

Manuale dell'amministratore di Symantec™ Data Loss Prevention

Versione 15.1

Ultimo aggiornamento: 06 agosto 2018



Manuale dell'amministratore di Symantec Data Loss Prevention

Versione della documentazione: 15.1

Note legali

Copyright © 2018 Symantec Corporation. Tutti i diritti riservati.

Symantec, CloudSOC, Blue Coat, il logo Symantec, il logo del segno di spunta, il logo Blue Coat e il logo a scudo sono marchi o marchi registrati di Symantec Corporation o di società affiliate negli Stati Uniti e altri Paesi. Gli altri nomi potrebbero essere marchi dei rispettivi proprietari.

Il presente prodotto Symantec può contenere programmi software di terze parti per i quali Symantec deve fornire attribuzione alle terze parti stesse ("Programmi di terze parti"). Alcuni dei programmi di terze parti sono disponibili con licenze Open Source o di software gratuito. Il contratto di licenza che accompagna il software non altera in alcun modo i diritti o gli obblighi eventuali derivanti da queste licenze Open Source o di software gratuito. Vedere l'appendice sull'informativa legale relativa a terzi di questa documentazione o il file Leggimi di TPIP che accompagna questo prodotto Symantec per maggiori informazioni sui programmi di terze parti.

Il prodotto descritto nel presente documento è distribuito in base alle condizioni di una licenza che ne limita l'utilizzo, la copia, la distribuzione e la decompilazione/decodificazione. Non è consentita la riproduzione anche parziale del documento in qualsiasi forma e con qualsiasi mezzo senza l'autorizzazione scritta di Symantec Corporation e degli eventuali licenzianti.

LA PRESENTE DOCUMENTAZIONE VIENE FORNITA COSÌ COM'È E VIENE NEGATA QUALSIASI GARANZIA, ESPLICITA O IMPLICITA, COMPRESE ANCHE E NON SOLO LE GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ, IDONEITÀ PER UNO SCOPO SPECIFICO O NON VIOLAZIONE DI DIRITTI ALTRUI NELLA MISURA MASSIMA CONSENTITA DALLA LEGGE. SYMANTEC CORPORATION NON SARÀ RESPONSABILE DI ALCUN TIPO DI DANNO INCIDENTALE O CONSEGUENZIALE COLLEGATO ALLA CONSEGNA, ALLE PRESTAZIONI O ALL'UTILIZZO DI QUESTA DOCUMENTAZIONE. LE INFORMAZIONI CONTENUTE NELLA PRESENTE DOCUMENTAZIONE SONO SOGGETTE A MODIFICA SENZA PREAVVISO.

Il Software e la Documentazione concessi in licenza sono ritenuti software commerciale per computer secondo le definizioni riportate nel FAR 12.212 e sono soggetti alle limitazioni di legge definite nel FAR Sezione 52.227-19 "Commercial Computer Software - Restricted Rights" e DFARS 227.7202 e successivi "Commercial Computer Software and Commercial Computer Software Documentation", per quanto applicabili, e nei regolamenti successivi, a prescindere dal fatto che siano forniti da Symantec come servizi in sede o host. Qualsiasi tipo di utilizzo, modifica, distribuzione, esecuzione, visualizzazione o divulgazione del software in licenza e della relativa documentazione da parte del Governo degli Stati Uniti potrà avvenire solo in conformità ai termini del presente contratto.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Sommario

Sezione 1	Guida introduttiva	71
Capitolo 1	Introduzione a Symantec Data Loss Prevention	72
	Informazioni sugli aggiornamenti al <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i>	72
	Informazioni su Symantec Data Loss Prevention	73
	Informazioni sulla piattaforma Enforce	75
	Informazioni su Network Monitor e Prevent	76
	Informazioni su Network Discover/Cloud Storage Discover	77
	Informazioni su Network Protect	77
	Informazioni su Endpoint Discover	78
	Informazioni su Endpoint Prevent	78
Capitolo 2	Guida introduttiva all'amministrazione di Symantec Data Loss Prevention	80
	Informazioni sull'amministrazione di Symantec Data Loss Prevention	80
	Informazioni sulla console di amministrazione di Enforce Server	81
	Accesso e disconnessione dalla console di amministrazione di Enforce Server	82
	Informazioni sull'account di amministrazione	83
	Esecuzione di attività di configurazione iniziale	83
	Modifica della password di amministratore	84
	Aggiunta di un account e-mail amministratore	85
	Modifica di un profilo utente	85
	Modifica della password	88
Capitolo 3	Utilizzo di lingue e impostazioni internazionali	89
	Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri	89
	Lingue supportate per il rilevamento	90
	Utilizzo di caratteri internazionali	92
	Informazioni su Symantec Data Loss Prevention supporti lingue	93
	Informazioni sulle impostazioni locali	94

Utilizzo di una lingua diversa dall'inglese sulla console di amministratore di Enforce Server	95
Uso dell'utilità supporto lingue	96

Sezione 2 Gestione della piattaforma di Enforce Server 100

Capitolo 4 Gestione dei servizi e delle impostazioni di Enforce Server 101

Informazioni sui servizi Symantec Data Loss Prevention	101
Informazioni sull'avvio e sull'arresto di servizi in Windows	102
Avvio di un Enforce Server su Windows	102
Arresto di un Enforce Server su Windows	103
Avvio di un server di rilevamento su Windows	103
Arresto di un server di rilevamento in Windows	104
Avvio dei servizi su installazioni Windows a un solo livello	104
Arresto dei servizi su installazioni Windows a un solo livello	104
Avvio e arresto di servizi in Linux	105
Avvio di un Enforce Server su Linux	105
Arresto di un Enforce Server su Linux	106
Avvio di un server di rilevamento su Linux	106
Arresto del server di rilevamento su Linux	107
Avvio dei servizi su installazioni Linux a un solo livello	107
Arresto dei servizi su installazioni Linux a un solo livello	107

Capitolo 5 Gestione di ruoli e utenti 109

Informazioni sul controllo degli accessi basato sul ruolo	109
Informazioni sulla configurazione di ruoli e utenti	110
Informazioni sui ruoli consigliati per l'organizzazione	111
Ruoli inclusi con i pacchetti di soluzioni	112
Ruoli di configurazione	114
Configurazione degli account utente	123
Configurazione delle impostazioni di imposizione delle password	127
Reimpostazione della password di amministratore	128
Gestione e aggiunta di ruoli	129
Gestione e aggiunta di utenti	129
Informazioni sull'autenticazione degli utenti	130
Configurazione dell'autenticazione dell'utente	134
Informazioni sull'autenticazione SAML	134
Configurazione dell'autenticazione	135
URL bypass dell'amministratore	136

	Impostazione e configurazione del metodo di autenticazione	137
	Impostazione della configurazione dell'autenticazione SAML	138
	Generazione o download dei metadati SAML di Enforce (provider di servizi)	139
	Configurare Enforce Server come provider di servizi SAML in IDP (creare un'applicazione nel provider di identità)	139
	Esportazione dei metadati IDP in DLP	140
	Configurazione dell'autenticazione di Active Directory	140
	Configurazione dell'autenticazione basata su moduli	141
	Configurazione dell'autenticazione del certificato	141
	Integrazione di Active Directory per autenticazione utente	141
	Creazione del file di configurazione per l'integrazione con Active Directory	142
	Verifica della connessione di Active Directory	144
	Informazioni sulla configurazione dell'autenticazione del certificato	145
	Configurazione dell'autenticazione del certificato per la console di amministrazione di Enforce Server	147
	Aggiunta di certificati dell'autorità di certificazione (CA) all'archivio Attendibilità Tomcat	149
	Mapping dei valori di nome comune (CN) agli account utente di Symantec Data Loss Prevention	152
	Informazioni sui controlli di revoca dei certificati	153
	Risoluzione dei problemi di autenticazione del certificato	159
	Disattivazione dell'autenticazione tramite password e dell'accesso basato sui moduli	160
Capitolo 6	Connessione alle directory di gruppo	161
	Creazione di connessioni ai server LDAP	161
	Configurazione delle connessioni a server di directory	162
	Pianificazione dell'indicizzazione del server di directory	164
Capitolo 7	Gestione di credenziali archiviate	167
	Informazioni sull'archivio credenziali	167
	Aggiunta di nuove credenziali all'archivio credenziali	168
	Configurazione delle credenziali endpoint	168
	Gestione delle credenziali nell'archivio credenziali	169
	Gestione di credenziali archiviate	169

Capitolo 8	Gestione di eventi e messaggi di sistema	171
	Informazioni sugli eventi di sistema	171
	Report di eventi di sistema	172
	Utilizzo dei report di sistema salvati	175
	Dettagli eventi di server e rivelatori	176
	Configurazione di attivazioni e soglie evento	177
	Informazioni sulle risposte agli eventi di sistema	180
	Attivazione di un server syslog	182
	Informazioni sugli avvisi di sistema	183
	Configurazione di Enforce Server per l'invio di avvisi tramite e-mail	183
	Configurazione degli avvisi di sistema	185
	Informazioni sulla verifica registri	187
	Messaggi e codici di eventi di sistema	187
Capitolo 9	Gestione del database di Symantec Data Loss Prevention	215
	Utilizzo di strumenti diagnostici di database di Symantec Data Loss Prevention	215
	Visualizzazione di allocazione spazi tabelle e file di dati	216
	Regolazione delle soglie di avviso per l'utilizzo dello spazio tabella in database di grande dimensioni	217
	Creazione di un report di database	217
	Visualizzazione dei dettagli della tabella	218
	Controllo della preparazione del database all'aggiornamento	219
	Preparazione dello strumento di preparazione aggiornamento	220
	Creazione dell'account database dello strumento Preparazione aggiornamento	221
	Esecuzione dello strumento di preparazione aggiornamento per Symantec Data Loss Prevention versione 14.x e 15.0	222
	Esame dei risultati di Preparazione aggiornamento	224
Capitolo 10	Utilizzo di Symantec Information Centric Encryption	225
	Informazioni su SymantecInformation Centric Encryption	225
	Informazioni sull'utilità Symantec ICE	226
	Panoramica sull'implementazione delle funzionalità di Information Centric Encryption	227
	Configurazione di Enforce Server per connettersi al cloud ICE Symantec	229

Capitolo 11	Utilizzo di Symantec Information Centric Tagging	231
	Informazioni sull'integrazione di Information Centric Tagging con Data Loss Prevention	231
	Panoramica dei passaggi per associare Information Centric Tagging a Data Loss Prevention	232
	Integrazione di Enforce Server con il server ICT	233
	Informazioni sulle importazioni automatiche e statiche della tassonomia di classificazione ICT	233
	Utilizzo del servizio Web ICT per importazioni di tassonomia di classificazione pianificata	234
	Utilizzo di un file XML per importazioni di tassonomia di classificazione statica	234
	Importazione della tassonomia di classificazione ICT	235
	Modifica dell'URL del servizio Web ICT	235
Capitolo 12	Aggiunta di un nuovo modulo di prodotto	237
	Installazione di un nuovo file di licenza	237
	Informazioni sugli aggiornamenti del sistema	238
Sezione 3	Gestione dei server di rilevamento	239
Capitolo 13	Installazione e gestione di server di rilevamento e rilevatori di cloud	240
	Informazioni sulla gestione dei server Symantec Data Loss Prevention	241
	Attivazione del controllo dei processi avanzato	241
	Controlli server	242
	Configurazione di base di server	244
	Server Network Monitor - Configurazione di base	246
	Server Network Prevent for Email - Configurazione di base	248
	Server Network Prevent for Web - Configurazione di base	251
	Server Network Discover/Cloud Storage Discover e Network Protect - Configurazione di base	254
	Endpoint Server - Configurazione di base	255
	Monitoraggio a un solo livello - configurazione di base	256
	Server di classificazione - Configurazione base	266
	Modifica di un rilevatore	267
	Configurazione server e rivelatore—avanzata	267
	Aggiunta di un server di rilevazione	268

	Aggiunta di un rilevatore di cloud	270
	Eliminazione di un server	271
	Importazione di certificati SSL in Enforce o Discover server	272
	Informazioni sulla schermata Panoramica	273
	Configurazione di Enforce Server per l'utilizzo di un proxy per connettersi ai servizi cloud	274
	Panoramica dello stato di server e rivelatori	275
	Elenco degli eventi di errore e avviso recenti	277
	Schermata Dettagli server/rilevatore	277
	Impostazioni server avanzate	279
	Impostazioni rilevatore avanzate	328
	Informazioni sull'utilizzo dei bilanciamenti del carico in una distribuzione endpoint	332
Capitolo 14	Gestione di file di registro	335
	Informazioni sui file di registro	335
	File di registro operativi	336
	File di registro di debug	339
	Schermata per la raccolta e la configurazione di registri	345
	Configurazione del comportamento di registrazione di un server	345
	Raccolta dei registri e dei file di configurazione del server	351
	Informazioni sui codici di evento dei registri	355
	File di registro operativi e codici di evento di Network Prevent for Web	355
	Campi e file del registro di accesso di Network Prevent for Web	357
	File di registro di debug per il protocollo di Network Prevent for Web	359
	Livelli di registrazione di Network Prevent for Email	359
	Codici dei registri operativi di Network Prevent for Email	360
	Risposte e codici generati da Network Prevent for Email	364
Capitolo 15	Utilizzo delle utilità di Symantec Data Loss Prevention	367
	Informazioni sulle utilità di Symantec Data Loss Prevention	367
	Informazioni sulle utilità Endpoint	368
	Informazioni su DBPasswordChanger	369
	Sintassi DBPasswordChanger	369
	Esempio di utilizzo di DBPasswordChanger	370

Sezione 4	Creazione di politiche	371
Capitolo 16	Introduzione alle politiche	373
	Informazioni sulle politiche di Data Loss Prevention	373
	Componenti della politica	375
	Modelli di politica	376
	Pacchetti di soluzioni	377
	Gruppi di politiche	377
	Distribuzione di politiche	378
	Gravità delle politiche	379
	Privilegi di creazione politiche	380
	Profili dati	381
	Gruppi utente	382
	Importazione ed esportazione dei modelli politica	383
	Flusso di lavoro per l'implementazione di politiche	384
	Visualizzazione, stampa e download dei dettagli della politica	385
Capitolo 17	Panoramica di rilevazione di politica	387
	Rilevamento della perdita di dati	387
	Contenuto che può essere rilevato	388
	File che possono essere rilevati	388
	Protocolli che è possibile monitorare	388
	Eventi endpoint che possono essere rilevati	389
	Identità che possono essere rilevate	389
	Lingue che possono essere rilevate	389
	Tecnologie di rilevamento delle politiche di Data Loss Prevention	390
	Condizioni di corrispondenza di politiche	392
	Condizioni per la corrispondenza del contenuto	393
	Condizioni corrispondenze delle proprietà file	395
	Condizione di corrispondenza di protocolli per la rete	396
	Condizioni di corrispondenza endpoint	396
	Condizioni per la corrispondenza tra gruppi (identità)	397
	Messaggi di rilevamento e componenti di messaggio	398
	Condizioni di eccezione	400
	Condizioni composte	401
	Esecuzione del rilevamento di politiche	402
	Rilevamento in due fasi per DLP Agent.	403
Capitolo 18	Creazione di politiche dai modelli	405
	Creazione di una politica a partire da un modello	405
	Modelli di politica Applicazione normative statunitensi	408

Modelli di politica Regolamento generale per la protezione dei dati (GDPR)	410
Modelli di politica Applicazione normative internazionali	411
Modelli di politica Protezione dei dati di clienti e dipendenti	412
Modelli di politica Protezione dei dati riservati o classificati	413
Modelli di politiche Applicazione norme di sicurezza di rete	415
Modelli di politica Applicazione norme di utilizzo accettabile	415
Modello di politica Applicazione normative colombiane relative ai dati personali	417
Scelta di un profilo dati esatti	417
Scelta di un profilo documento indicizzato	419

Capitolo 19 Configurazione di politiche 421

Aggiunta di una nuova politica o di un modello di politica	421
Configurazione di politiche	422
Aggiunta di una regola a una politica	424
Configurazione di regole di politica	427
Definizione di gravità della regola	430
Configurazione del conteggio delle corrispondenze	431
Selezione dei componenti per la corrispondenza	433
Aggiunta di un'eccezione a una politica	434
Configurazione delle eccezioni di politica	437
Configurazione delle condizioni di corrispondenza composte	440
Limiti di immissione caratteri per la configurazione di politiche	442

Capitolo 20 Amministrazione delle politiche 443

Gestione e aggiunta di politiche	444
Gestione e aggiunta di gruppi di politiche	446
Creazione e modifica di gruppi di politiche	447
Importazione politiche	449
Informazioni sull'importazione di politiche	449
Informazioni sui riferimenti della politica	450
Esportazione delle politiche	451
Informazioni sull'esportazione della politica	451
Clonazione delle politiche	452
Importazione di modelli di politica	453
Esportazione del rilevamento di politiche come modello	454
Aggiunta di una regola di risposta automatica a una politica	455
Eliminazione di politiche e gruppi di politiche	456
Visualizzazione e stampa dei dettagli della politica	456
Download dei dettagli delle politiche	457
Risoluzione dei problemi delle politiche	458

Aggiornamento dei profili EDM e IDM alla versione più recente	458
Aggiornamento delle politiche dopo l'upgrade alla versione più recente	459

Capitolo 21	Best practice per la creazione di politiche	462
	Best practice per la creazione di politiche	462
	Sviluppo di una strategia di politiche che supporti gli obiettivi di protezione dei dati	464
	Utilizzo iniziale di un numero limitato di politiche	464
	Utilizzo dei modelli di politica modificati in base alle esigenze	465
	Utilizzare lo stato di corrispondenza appropriato per gli obiettivi di prevenzione della perdita di dati.	465
	Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze	466
	Iniziare con soglie di corrispondenza elevate per ridurre i falsi positivi	468
	Utilizzo di un numero limitato di eccezioni per restringere l'ambito di rilevamento	468
	Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza.	469
	Creazione di politiche per limitare l'effetto potenziale del rilevamento in due fasi	469
	Utilizzo dei gruppi di politiche per gestire il ciclo di vita delle politiche	471
	Best practice specifiche del rilevamento	471

Capitolo 22	Rilevamento del contenuto mediante Exact Data Matching (EDM)	473
	Introduzione all'Exact Data Matching (EDM)	473
	Informazioni sull'utilizzo di EDM per proteggere i contenuti	474
	Funzionalità della politica EDM	475
	Modelli di politica EDM	476
	Informazioni sul profilo dati esatti e sull'indice	478
	Informazioni sul file origine dati esatti	479
	Informazioni sulla pulizia del file origine dati esatti	480
	Informazioni sull'utilizzo di campi di sistema per la convalida di origini dati	480
	Informazioni sulla pianificazione degli indici	481
	Informazioni sulla condizione Il contenuto corrisponde ai dati esatti da	482
	Informazioni sull'eccezione Proprietario dati	482
	Informazioni su Directory Group Matching (DGM) con profilo	483

Informazioni sul rilevamento in due fasi per l'EDM	
sull'endpoint	484
Informazioni sull'upgrade delle distribuzioni EDM	484
Configurazione di profili dati esatti	484
Creazione del file origine dati esatti per EDM	486
Creazione del file origine dati esatti per l'eccezione Proprietario	
dati	487
Creazione del file origine dati esatti per DGM con profilo	487
Preparazione del file origine dati esatti per l'indicizzazione	488
Caricamento di file origine dati esatti in Enforce Server	490
Creazione e modifica di profili dati esatti	492
Mapping dei campi del profilo dati esatti	496
Utilizzo delle convalide dei criteri fornite dal sistema per i profili	
EDM	498
Pianificazione dell'indicizzazione di profili dati esatti	499
Gestione e aggiunta di profili dati esatti	501
Configurazione dei criteri EDM	502
Configurazione della condizione di politica Contenuto	
corrispondente a profilo dati esatti	503
Configurazione dell'eccezione Proprietario dati per le condizioni	
della politica EDM	505
Configurazione della condizione di politica di mittente/utente	
basato su una directory con profilo	506
Configurazione del destinatario in base a una condizione della	
politica Profiled Directory	507
Informazioni sulla configurazione dell'elaborazione del linguaggio	
naturale per cinese, giapponese e coreano per le politiche	
EDM.	508
Configurazione di impostazioni avanzate per i criteri EDM	509
Utilizzo della corrispondenza multitoken	513
Caratteristiche delle celle multitoken	513
Multitoken con spazi	514
Multitoken con parole non significative	515
Multitoken con caratteri in lingue miste	515
Multi-token con punteggiatura	516
Ulteriori esempi per celle multitoken con punteggiatura	517
Alcuni casi particolari di utilizzo per formati di dati riconosciuti dal	
sistema	520
Caratteri di punteggiatura multitoken	522
Esempi di varianti di totale corrispondenze	523
Esempio di corrispondenza di prossimità	525
Aggiornamento degli indici EDM alla versione più recente	527
Processo di aggiornamento con Remote EDM Indexer	528

Processo di aggiornamento con Enforce Server	530
Codici di errore per indice EDM obsoleto	531
Requisiti di memoria per EDM	532
Informazioni sui requisiti di memoria per EDM	532
Panoramica della memoria di configurazione e di indicizzazione dell'origine dati	533
Determinazione dei requisiti per indicizzatori locali e remoti	534
Requisiti di memoria del server di rilevazione	535
Aumento della memoria del server di rilevamento (lettore del file)	538
Utilizzo del foglio di elettronico dei requisiti di memoria EDM	539
Indicizzazione EDM remota	539
Informazioni su Remote EDM Indexer	540
Informazioni su SQL Preindexer	540
Requisiti di sistema per l'indicizzazione EDM remota	541
Flusso di lavoro per l'indicizzazione EDM remota	541
Informazioni sull'installazione e l'esecuzione delle utilità Remote EDM Indexer e SQL Preindexer	542
Creazione del modello di un profilo EDM per l'indicizzazione remota	543
Download e copia del file di profilo EDM in un sistema remoto	546
Generazione remota di file indice	546
Esempi di indicizzazione remota mediante il file origine dati	547
Esempi di indicizzazione remota con SQL Preindexer	548
Copia e caricamento di file di indice remoti su Enforce Server	549
Opzioni di comando di SQL Preindexer	550
Opzioni di comando di Remote EDM Indexer	552
Risoluzione dei problemi per gli errori di preindicizzazione	553
Risoluzione dei problemi dell'indicizzazione remota	554
Installazione di Remote EDM Indexer	556
Best practice per l'utilizzo dell'EDM	557
Verifica della presenza di almeno una colonna di dati univoci nell'origine dati	558
Eliminazione di colonne vuote e righe duplicate dal file origine dati	559
Rimozione di tipi di carattere ambigui dal file origine dati	560
Funzionamento della corrispondenza di celle multitoken	560
Mancato utilizzo del delimitatore virgola se l'origine dati ha campi numerici	561
Mappaggio delle colonne origine dati ai campi di sistema per utilizzare la convalida	561

Assicurarsi che l'origine dati sia pronta per l'indicizzazione	562
Sfruttamento dei modelli di politica EDM quando possibile	562
Inclusione delle intestazioni di colonna come prima riga del file origine dati	563
Verifica degli avvisi di sistema per ottimizzare la precisione del profilo	563
Utilizzo di parole non significative per escludere le parole comuni dal rilevamento	563
Utilizzo dell'indicizzazione pianificata per automatizzare gli aggiornamenti del profilo	564
Corrispondenza con 3 colonne in una condizione EDM per aumentare la precisione di rilevamento	565
Sfruttamento delle tuple di eccezione per evitare i falsi positivi	566
Utilizzare una clausola WHERE per individuare i record che soddisfano criteri specifici	566
Utilizzo del campo Corrispondenze minime per ottimizzare le regole EDM	566
Combinazione tra identificatori dati e regole EDM per limitare l'impatto del rilevamento in due fasi	567
Inclusione di un campo per l'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo	567
Utilizzo della DGM con profilo per il rilevamento di identità di Network Prevent for Web	567

Capitolo 23

Rilevamento del contenuto mediante Indexed Document Matching (IDM)

Introduzione a Indexed Document Matching (IDM)	569
Informazioni sull'utilizzo dell'IDM	569
Metodi di corrispondenza supportati da IDM	570
Tipi di rilevamento IDM	571
Informazioni sul profilo documenti indicizzati	572
Informazioni sull'origine dati del documento	573
Informazioni sul processo di indicizzazione	573
Informazioni sull'indicizzazione remota dei documenti	574
Informazioni sui file di indice del server e i file di indice dell'agente	575
Informazioni sulla distribuzione e sulla registrazione degli indici	576
Utilizzo di IDM per rilevare file esatti	578
Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali	579

Informazioni sull'utilizzo della condizione Contenuto corrispondente a firma documento	581
Informazioni sull'aggiunta del contenuto file parziale a una lista bianca	582
Configurazione di profili IDM e condizioni delle politiche	583
Preparazione di un'origine dati di documento per l'indicizzazione	583
Creazione di una lista bianca di contenuto di file da escludere dalla corrispondenza parziale	585
Gestione e aggiunta di profili documenti indicizzati	586
Creazione e modifica di profili di documento indicizzati	588
Configurazione della corrispondenza parziale del contenuto endpoint	590
Caricamento di un archivio di documenti in Enforce Server	591
Riferimento a un archivio documenti in Enforce Server	592
Utilizzo del percorso locale sul Enforce Server	594
Utilizzo dell'opzione di condivisione SMB remota per indicizzare le condivisioni di file	595
Utilizzo dell'opzione di condivisione SMB remota per indicizzare i documenti SharePoint	596
Filtraggio di documenti per nome di file	599
Filtraggio di documenti per dimensioni file	601
Pianificazione dell'indicizzazione di profili documento	602
Modifica delle proprietà predefinite dell'indicizzatore	603
Attivazione dell'IDM dell'agente	604
Stima dell'utilizzo di memoria dell'endpoint per Agent IDM	605
Configurazione della condizione di politica Contenuto corrispondente a firma documento	605
Best practice per l'utilizzo di IDM	607
Reindicizzazione dei profili IDM dopo un upgrade importante	608
Non comprimere i file nell'origine documento	608
Mancata indicizzazione di documenti vuoti	609
Preferenza della corrispondenza parziale alla corrispondenza esatta con DLP Agent	609
Informazioni sulle limitazioni della corrispondenza esatta	610
Utilizzare la lista bianca per escludere il contenuto non sensibile dalla corrispondenza parziale	611
Escludere documenti dall'indicizzazione per ridurre i falsi positivi.	611
Distinzione delle eccezioni IDM dalla lista bianca e dal filtro	612
Creazione di profili separati per indicizzare origini di documenti di grandi dimensioni	613

Utilizzo di WebDAV o CIFS per indicizzare le origini dati di documenti remoti	613
Utilizzo dell'indicizzazione pianificata per tenere aggiornati i profili	613
Utilizzo di regole IDM parallele per ottimizzare le soglie di corrispondenze	614
Indicizzazione EDM remota	615
Informazioni sull'Indicizzatore IDM remoto	615
Indicizzazione dell'origine dati del documento mediante l'edizione GUI (solo Windows)	616
Indicizzazione dell'origine dati del documento tramite file di proprietà	619
Indicizzazione dell'origine dati del documento tramite CLI	621
Pianificazione dell'indicizzazione remota con l'app Indicizzatore IDM remoto per Windows	623
Indicizzazione incrementale	626
Registrazione e risoluzione dei problemi	627
Copia del file di preindice sull'host di Enforce Server	628
Caricamento del file di indice remoto in Enforce Server	628

Capitolo 24

Rilevamento del contenuto mediante Vector Machine Learning (VML)	629
Introduzione a Vector Machine Learning (VML)	629
Informazioni sul profilo Vector Machine Learning	630
Informazioni sul contenuto sottoposto a training	630
Informazioni sui livelli percentuali di precisione di base da training	631
Informazioni sulla soglia di similarità e sul punteggio di somiglianza	632
Informazioni sull'utilizzo di profili VML non accettati nelle politiche	633
Configurazione dei profili VML e delle condizioni delle politiche	633
Creazione di nuovi profili VML	635
Utilizzo delle schede Profilo corrente e Area di lavoro temporanea	635
Caricamento dei documenti di esempio per il training	636
Training dei profili VML	638
Regolazione dell'assegnazione di memoria	640
Gestione dei documenti dei set di training	641
Gestione di profili VML	642
Modifica dei nomi e delle descrizioni per i profili VML	644

Configurazione della condizione Rileva utilizzando il profilo Vector	
Machine Learning	645
Configurazione delle eccezioni alla politica VML	646
Regolazione della soglia di similarità	647
Test e ottimizzazione dei profili VML	648
Proprietà per la configurazione del training	649
File di log per la risoluzione dei problemi del training VML e del	
rilevamento di politiche	652
Procedure ottimali per l'utilizzo di VML	653
Quando utilizzare VML	654
Quando non utilizzare il VML	655
Scelte consigliate per la definizione del set di training	656
Linee guida per le dimensioni del set di training	657
Scelte consigliate per il caricamento di documenti per il	
training	658
Linee guida per il dimensionamento del profilo	658
Scelte consigliate per accettare o rifiutare un profilo	659
Linee guida per l'accettazione o il rifiuto dei risultati del	
training	660
Consigli per la distribuzione di profili	661

Capitolo 25

Rilevamento del contenuto mediante	
Riconoscimento moduli - Riconoscimento di	
immagini riservate	662
Informazioni sul rilevamento Riconoscimento moduli	662
Come funziona il riconoscimento dei moduli	663
Configurazione del rilevamento Riconoscimento moduli	664
Preparazione di un archivio della galleria Riconoscimento	
moduli	664
Configurazione del profilo Riconoscimento moduli	666
Configurazione della regola di rilevamento di riconoscimento	
moduli	666
Configurazione della regola di eccezione Riconoscimento	
moduli	667
Gestione dei profili di Riconoscimento moduli	668
Impostazioni di server avanzate per il riconoscimento moduli	670
Visualizzazione di un incidente di Riconoscimento moduli	671

Capitolo 26	Rilevamento del contenuto mediante OCR - Riconoscimento di immagini riservate	672
	Informazioni sul rilevamento dei contenuti con il riconoscimento OCR	
	delle immagini riservate	673
	Tipi di rilevamento supportati per l'estrazione OCR	673
	Tipi di file supportati per l'estrazione OCR	674
	Requisiti di sistema del Server OCR	674
	Utilizzo del foglio di calcolo per la stima del dimensionamento per i server OCR	674
	Configurazione dei server OCR	674
	Installazione di una licenza di riconoscimento OCR delle immagini riservate	676
	Creazione di una configurazione OCR	676
	Utilizzo del motore OCR	678
	Ulteriori informazioni su lingue e dizionari	678
	Dizionari specializzati disponibili per l'estrazione del contenuto OCR	678
	Lingue supportate per l'estrazione OCR	679
	Visualizzazione di incidenti OCR nei report	680
Capitolo 27	Rilevamento del contenuto mediante identificatori di dati	681
	Introduzione agli identificatori di dati	681
	Identificatori di dati definiti dal sistema	682
	Estensione e personalizzazione di identificatori di dati	693
	Informazioni sulla configurazione dell'identificatore dati	694
	Informazioni sulle coperture degli identificatori di dati	694
	Informazioni sulle convalide facoltative per identificatori di dati	695
	Informazioni sui criteri dell'identificatore dati	695
	Informazioni sulle convalide criterio	696
	Informazioni sui normalizzatori di dati	696
	Informazioni sulla corrispondenza con diversi componenti	696
	Informazioni sul conteggio delle corrispondenze univoche	697
	Configurazione delle condizioni della politica dell'identificatore dati	697
	Flusso di lavoro per la configurazione delle politiche dell'identificatore dati	698
	Gestione e aggiunta degli identificatori dati	698
	Modifica degli identificatori dati	699

Configurazione della condizione Contenuto corrispondente a	
identificatore dati	700
Utilizzo delle coperture identificatore dati	702
Selezione di una copertura dell'identificatore di dati	703
Utilizzo delle convalide opzionali	719
Configurazione delle convalide opzionali	720
Caratteri accettabili per le convalide opzionali	721
Utilizzo del totale corrispondenze univoche	723
Configurazione del conteggio delle corrispondenze	
univoche	724
Modifica degli identificatori dati di sistema	725
Clonazione di un identificatore dati di sistema prima della sua	
modifica	726
Modifica dell'input di convalida dei criteri	727
Elenco delle convalide criterio che accettano dati di input	727
Modifica delle parole chiave per gli identificatori dati PII	
internazionali	728
Elenco di parole chiave per gli identificatori dati di sistema	
internazionali	729
Aggiornamento delle politiche per l'utilizzo dell'identificatore dati	
Social Security Number (SSN) statunitense	
randomizzato	747
Creazione di identificatori dati personalizzati	748
Flusso di lavoro per la creazione di identificatori di dati	
personalizzati	749
Configurazione degli identificatori dati personalizzati	751
Utilizzo della lingua dei criteri degli identificatori dati	751
Creazione di criteri di identificatore di dati per la corrispondenza	
con i dati	755
Utilizzo delle convalide criterio	755
Selezione di convalide dei criteri	763
Selezione di un normalizzatore di dati	764
Creazione di convalide con script personalizzati	765
Best practice per l'utilizzo degli identificatori dati	765
Utilizzo degli identificatori dati invece di espressioni regolari per	
migliorare la precisione	766
Clonare gli identificatori di dati definiti dal sistema prima della	
modifica per mantenere lo stato originale	767
Modifica delle definizioni dell'identificatore dati quando si desidera	
applicare l'ottimizzazione a livello globale	767
Possibilità di utilizzare parallelamente più coperture per rilevare	
gravità diverse dei dati riservati	768

Evitare la corrispondenza con la busta HTTP per ridurre i falsi positivi	768
Utilizzo dell'identificatore dati Social Security Number (SSN) statunitense randomizzato per rilevare i numeri di previdenza sociale	769
Utilizzo del conteggio corrispondenze univoche per migliorare l'accuratezza e facilitare le riparazioni	769

Capitolo 28

Rilevamento del contenuto mediante la corrispondenza di parole chiave	771
Introduzione alla corrispondenza con parole chiave	771
Informazioni sulla corrispondenza di parole chiave per le lingue cinese, giapponese e coreano (CJK)	772
Informazioni sulla prossimità di parole chiave	773
Sintassi della corrispondenza di parole chiave	773
Esempi di corrispondenza con parole chiave	775
Esempi di corrispondenze parole chiave per lingue cinese, giapponese e coreano	776
Informazioni sugli aggiornamenti degli elenchi relativi a medicinali, malattie e cure	777
Configurazione della corrispondenza di parole chiave	778
Configurazione della condizione Contenuto corrispondente a parola chiave	779
Attivazione e utilizzo della verifica dei token CJK per la corrispondenza di parole chiave sul server	781
Aggiornamento degli elenchi di parole chiave Medicinali, Malattie e Cure per le politiche HIPAA e Caldicott	782
Best practice per l'utilizzo della corrispondenza di parole chiave	784
Attivazione della verifica dei token sul server per ridurre i falsi positivi per il rilevamento delle parole chiave CJK	784
Aggiornamento degli elenchi di parole chiave per le politiche HIPAA e Caldicott.	785
Ottimizzazione degli elenchi di parole chiave per gli identificatori dati per migliorare la precisione della corrispondenza	785
Utilizzo della corrispondenza con parole chiave per il rilevamento di metadati del documento	786
Utilizzo di VML per generare e mantenere grandi dizionari di parole chiave	786

Capitolo 29	Rilevamento del contenuto mediante espressioni regolari	787
	Introduzione alla corrispondenza con espressioni regolari	787
	Informazioni sul motore aggiornato di espressione regolare	788
	Informazioni sulla scrittura di espressioni regolari	788
	Configurazione della condizione Contenuto corrispondente a espressione regolare	789
	Best practice per l'utilizzo della corrispondenza di espressioni regolari	791
	Quando utilizzare la corrispondenza di espressioni regolari	791
	Utilizzo dei caratteri look-ahead e look-behind per migliorare la precisione delle espressioni regolari	791
	Utilizzo moderato delle espressioni regolari per prestazioni efficienti	792
	Verifica delle espressioni regolari prima della distribuzione per migliorare l'accuratezza	792
Capitolo 30	Rilevamento del contenuto utilizzando la corrispondenza di classificazione	793
	Introduzione alla corrispondenza di classificazione	793
	Tipi di file supportati	794
	Funzionamento della corrispondenza dei tag	795
	Configurazione della condizione Classificazione corrispondenze contenuto	799
Capitolo 31	Rilevamento del contenuto di lingua internazionale	802
	Rilevazione del contenuto in lingua non inglese	802
	Best practice per il rilevamento di contenuti non in inglese	803
	Aggiornamento all'ultima versione di Data Loss Prevention	803
	Utilizzo di modelli di politica internazionali per la creazione di politiche	803
	Utilizzo di parole chiave personalizzate per gli identificatori di dati del sistema	804
	Attivazione della convalida token per la corrispondenza con parole chiave cinesi, giapponesi e coreane sul server	806
Capitolo 32	Rilevamento delle proprietà di file	808
	Introduzione al rilevamento di proprietà di file	808
	Informazioni sulla corrispondenza con tipi di file	808

Informazioni sul supporto dei formati di file per la corrispondenza dei tipi di file	809
Informazioni sull'identificazione di tipi di file personalizzati	809
Informazioni sulla corrispondenza di dimensione di file	810
Informazioni sulla corrispondenza del nome del file	811
Configurazione della corrispondenza delle proprietà del file	811
Configurazione della condizione Corrispondenza allegato messaggio o tipo file.	812
Configurazione della condizione Corrispondenza allegato messaggio o dimensioni file	813
Configurazione della condizione Corrispondenza allegato messaggio o nome file	815
Sintassi di corrispondenza dei nomi di file	816
Esempi di corrispondenza dei nomi file	816
Attivazione della condizione Firma tipi di file personalizzati nella console della politica	817
Configurazione della condizione Firma tipi di file personalizzati	817
Best practice per l'utilizzo di corrispondenza delle proprietà file	818
Utilizzo delle regole proprietà file composte per proteggere i file di progettazione e multimediali	819
Non utilizzo della corrispondenza del tipo di file per rilevare il contenuto	819
Calcolo corretto della dimensione del file per migliorare la precisione della corrispondenza	819
Uso dei criteri di espressione per la corrispondenza con i nomi file	819
Utilizzo degli script e dei plug-in per rilevare i tipi di file personalizzati	820

Capitolo 33	Rilevamento degli incidenti di rete	821
	Introduzione al monitoraggio di protocolli per la rete	821
	Configurazione della condizione Monitoraggio protocollo per il rilevamento nella rete	822
	Best practice per l'utilizzo della corrispondenza di protocolli di rete	823
	Uso di politiche distinte per specifici protocolli	823
	Considerazione del posizionamento in rete del server di rilevazione per il supporto della corrispondenza indirizzi IP	823

Capitolo 34	Rilevamento degli eventi endpoint	824
	Introduzione al rilevamento di eventi endpoint	824
	Informazioni sul monitoraggio del protocollo endpoint	824
	Informazioni sul monitoraggio della destinazione endpoint	825
	Informazioni sul controllo delle applicazioni endpoint	825
	Informazioni sul rilevamento della posizione dell'endpoint	826
	Informazioni sul rilevamento di dispositivi endpoint	826
	Configurazione delle condizioni di rilevamento eventi dell'endpoint	826
	Configurazione della condizione di monitoraggio dell'endpoint	827
	Configurazione della condizione Posizione endpoint	829
	Configurazione della condizione Classe o ID dispositivo endpoint	830
	Raccolta degli ID dispositivo endpoint per i dispositivi rimovibili	831
	Creazione e modifica delle configurazioni di dispositivi endpoint	832
	Best practice per l'utilizzo del rilevamento endpoint	833
Capitolo 35	Rilevamento delle identità descritte	835
	Introduzione alla corrispondenza con identità descritte	835
	Esempi di corrispondenza di identità descritti	835
	Configurazione delle condizioni della politica di corrispondenza con le identità descritte	836
	Informazioni sui criteri di mittente/destinatario riutilizzabili	837
	Configurazione della condizione Mittente/utente corrisponde a criterio	837
	Configurazione di un criterio mittente riutilizzabile	839
	Configurazione della condizione Destinatario corrispondente a criterio	840
	Configurazione di un criterio destinatario riutilizzabile	842
	Best practice per l'utilizzo della corrispondenza di identità descritte	843
	Definizione di criteri di identità precisi per la corrispondenza con utenti	843
	Specificare esattamente gli indirizzi e-mail per migliorare l'accuratezza	844
	Corrispondenza con domini anziché con indirizzi IP per migliorare l'accuratezza	844

Capitolo 36	Rilevamento delle identità sincronizzate	846
	Introduzione a Directory Group Matching (DGM) sincronizzato	846
	Informazioni sul rilevamento in due fasi per DGM sincronizzata	847
	Configurazione di gruppi di utenti	847
	Configurazione delle condizioni di politica di DGM sincronizzata	850
	Configurazione della condizione Mittente/utente basato su gruppo di server di directory	851
	Configurazione della condizione Destinatario basato su gruppo di server di directory	852
	Best practice per l'utilizzo di condizioni DGM sincronizzate	853
	Aggiornamento della directory al momento del salvataggio iniziale del gruppo di utenti	853
	Distinzione della DGM sincronizzata da altri tipi di rilevamento endpoint	853
Capitolo 37	Rilevamento delle identità con profilo	855
	Introduzione a Directory Group Matching (DGM) con profilo	855
	Informazioni sul rilevamento in due fasi per DGM con profilo	856
	Configurazione di profili dati esatti per DGM	856
	Configurazione delle condizioni di politica di DGM con profilo	857
	Configurazione del Mittente/Utente in base a una condizione della Profiled Directory	858
	Configurazione del destinatario in base a una condizione Profiled Directory	859
	Procedure ottimali per l'utilizzo di DGM con profilo	859
	Osservare le best practice EDM quando si implementa DGM con profili	859
	Inclusione di un campo per l'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo	860
	Utilizzo della DGM con profilo per il rilevamento di identità di Network Prevent for Web	860
Capitolo 38	Utilizzo di attributi contestuali per il Rilevamento applicazioni	861
	Introduzione a attributi contestuali per le applicazioni cloud	861
	Configurazione delle condizioni di attributo contestuale	861
	Categorie di attributo contestuale	862

Capitolo 39	Formati di file supportati per rilevamento	876
	Panoramica del supporto del formato di file di rilevamento	876
	Formati supportati per l'identificazione dei tipi di file	878
	Formati supportati per l'estrazione di contenuto	893
	Formati di elaborazione di testi supportati per l'estrazione di contenuto	894
	Formati di presentazione supportati per l'estrazione di contenuto	896
	Formati di foglio di calcolo supportati per l'estrazione di contenuto	897
	Formati di testo e markup supportati per l'estrazione di contenuto	898
	Formati e-mail supportati per l'estrazione di contenuto	898
	Formati CAD supportati per l'estrazione di contenuto	899
	Formati di grafica supportati per l'estrazione di contenuto	899
	Formati di database supportati per l'estrazione di contenuto	900
	Altri formati di file supportati per l'estrazione di contenuto	900
	Formati di incapsulamento supportati per l'estrazione di file secondari	901
	Formati di file supportati per l'estrazione di metadati	902
	Informazioni sul rilevamento dei metadati dei documenti	903
	Attivazione del rilevamento di metadati del server	904
	Attivazione del rilevamento dei metadati dell'endpoint	904
	Best practice per l'utilizzo del rilevamento di metadati	905
Capitolo 40	Libreria degli identificatori di dati del sistema	911
	Libreria degli identificatori di dati del sistema	917
	Numero di routing ABA	918
	Copertura ampia Numero di routing ABA	918
	Copertura media Numero di routing ABA	918
	Copertura limitata Numero di routing ABA	919
	Numero di identificazione fiscale argentino	920
	Copertura ampia numero di identificazione fiscale argentino	921
	Copertura media numero di identificazione fiscale argentino	921
	Copertura limitata del numero di identificazione fiscale argentino	922
	Australian Business Number (partita IVA australiana)	923
	Copertura ampia Australian Business Number	923
	Copertura media dell'Australian Business Number (partita IVA australiana)	924
	Copertura limitata Australian Business Number (partita IVA australiana)	925

Codice azienda australiano (ACN)	925
Copertura ampia dell'Australian Company Number (ACN, codice azienda australiano)	926
Copertura media Australian Company Number (ACN, codice azienda australiano)	926
Copertura limitata Australian Company Number (ACN, codice azienda australiano)	927
Numero Medicare australiano	927
Copertura ampia numero Medicare australiano	928
Copertura media numero Medicare australiano	929
Copertura limitata del numero Medicare australiano	929
Numero di passaporto australiano	930
Copertura ampia del numero di passaporto australiano	931
Copertura limitata del numero di passaporto australiano	931
Tax File Number (codice fiscale) australiano	932
Copertura ampia Tax File Number (codice fiscale) australiano	932
Copertura limitata Tax File Number (codice fiscale) australiano	933
Numero di passaporto austriaco	933
Copertura ampia del numero di passaporto austriaco	934
Copertura limitata del numero di passaporto austriaco	934
Numero di identificazione fiscale austriaco	935
Copertura ampia del numero di identificazione fiscale austriaco	935
Copertura limitata del numero di identificazione fiscale austriaco	936
Numero di partita IVA austriaco	936
Copertura ampia numero di partita IVA austriaco	937
Copertura media del numero di partita IVA austriaco	937
Copertura limitata del numero di partita IVA austriaco	938
Numero di previdenza sociale austriaco	939
Portata ampia del numero di previdenza sociale austriaco	939
Copertura media del numero di previdenza sociale austriaco	940
Copertura limitata del numero di previdenza sociale austriaco	940
Numero di identificazione nazionale belga	942
Copertura ampia numero di identificazione nazionale belga	943
Copertura media del numero di identificazione nazionale belga	943
Copertura limitata numero di identificazione nazionale belga	944
Numero di patente di guida belga	945

Copertura ampia del Numero di patente di guida belga	945
Copertura limitata del Numero di patente di guida belga	946
Numero di passaporto belga	947
Copertura ampia numero di passaporto belga	947
Copertura limitata numero di passaporto belga	948
Numero di identificazione fiscale belga	948
Copertura ampia del numero di identificazione fiscale belga	949
Copertura limitata del numero di identificazione fiscale belga	950
Numero di partita IVA belga	951
Copertura ampia numero di partita IVA belga	951
Copertura media del numero di partita IVA belga	952
Copertura limitata numero di partita IVA belga	952
Numero di conto bancario brasiliano	953
Copertura ampia del numero di conto bancario brasiliano	954
Copertura media numero di conto bancario brasiliano	954
Copertura limitata del numero di conto bancario brasiliano	954
Numero di tessera elettorale brasiliana	955
Copertura ampia numero di tessera elettorale brasiliana	956
Copertura media numero di tessera elettorale brasiliana	957
Copertura limitata numero di tessera elettorale brasiliana	958
Numero del Registro Nazionale delle Persone Giuridiche brasiliانو	959
Copertura ampia numero del Registro Nazionale delle Persone Giuridiche brasiliانو	960
Copertura media numero del Registro Nazionale delle Persone Giuridiche brasiliانو	960
Copertura limitata numero del Registro Nazionale delle Persone Giuridiche brasiliانو	961
Codice fiscale per persone fisiche brasiliانو (CPF)	962
Copertura ampia codice fiscale per persone fisiche brasiliانو (CPF)	962
Copertura media codice fiscale per persone fisiche brasiliانو (CPF)	963
Copertura limitata codice fiscale per persone fisiche brasiliانو (CPF)	963
Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica	964
Copertura ampia Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica	965
Copertura media Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica	965

Copertura limitata Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica	966
Numero di cittadinanza univoco bulgaro (EGN)	967
Copertura ampia numero di cittadinanza univoco bulgaro (EGN)	967
Copertura media numero di cittadinanza univoco bulgaro (EGN)	968
Copertura limitata numero di cittadinanza univoco bulgaro (EGN)	969
Burgerservicenummer	970
Copertura ampia Burgerservicenummer	970
Copertura limitata burgerservicenummer	971
Social Insurance Number (numero di previdenza sociale) canadese	971
Copertura ampia Social Insurance Number (numero di previdenza sociale) canadese	972
Copertura media Social Insurance Number (numero di previdenza sociale) canadese	973
Copertura limitata Social Insurance Number (numero di previdenza sociale) canadese	974
Numero di identificazione nazionale cileno	975
Copertura ampia numero di identificazione nazionale cileno	975
Copertura media numero di identificazione nazionale cileno	976
Copertura limitata numero di identificazione nazionale cileno	976
Numero di passaporto cinese	977
Copertura ampia numero di passaporto cinese	977
Copertura limitata numero di passaporto cinese	978
Codice Fiscale	979
Copertura ampia Codice Fiscale	979
Copertura limitata Codice Fiscale	979
Indirizzi colombiani	980
Copertura ampia indirizzi colombiani	980
Copertura limitata indirizzi colombiani	981
Numero di cellulare colombiano	983
Copertura ampia numero di cellulare colombiano	983
Copertura limitata numero di cellulare colombiano	984
Numero di identificazione personale colombiano	986
Copertura ampia numero di identificazione personale colombiano	986
Copertura limitata numero di identificazione personale colombiano	987
Tax Identification Number (codice fiscale) colombiano	988

Copertura ampia Tax Identification Number (codice fiscale)	
colombiano	988
Copertura limitata Tax Identification Number (codice fiscale)	
colombiano	989
Dati banda magnetica per carte di credito	990
Numero carta di credito	993
Copertura ampia Numero carta di credito	993
Copertura media numero carta di credito	994
Copertura limitata numero carta di credito	997
Numero CUSIP	1002
Copertura ampia Numero CUSIP	1002
Copertura media numero CUSIP	1003
Copertura limitata numero CUSIP	1004
Numero di identificazione personale ceco	1004
Copertura ampia del numero di identificazione personale	
ceco	1005
Copertura media numero di identificazione personale ceco	1005
Copertura limitata numero di identificazione personale ceco	1006
Numero di identificazione personale danese	1007
Copertura ampia del numero di identificazione personale	
danese	1008
Copertura media del numero di identificazione personale	
danese	1008
Copertura limitata numero di identificazione personale	
danese	1009
Numero di identificazione fiscale danese	1009
Copertura ampia del numero di identificazione fiscale	
danese	1010
Copertura media del numero di identificazione fiscale	
danese	1010
Copertura limitata del numero di identificazione fiscale	
danese	1011
Numero di partita IVA danese	1012
Copertura ampia del numero di partita IVA danese	1013
Copertura media del numero di partita IVA danese	1013
Copertura limitata del numero di partita IVA danese	1014
Numero patente di guida - Stato della California	1015
Copertura ampia Numero patente di guida - Stato della	
California	1015
Copertura media numero patente di guida - Stato della	
California	1016
Numero di patente di guida - Stati della Florida, del Michigan e del	
Minnesota	1016

Copertura ampia numero patente di guida - Stati Florida, Michigan, Minnesota	1017
Copertura media numero patente di guida - Stati della Florida, del Michigan e del Minnesota	1017
Numero patente di guida - Stato dell'Illinois	1018
Copertura ampia Numero patente di guida - Stato dell'Illinois	1019
Copertura media numero patente di guida - Stato dell'Illinois	1019
Numero patente di guida - Stato del New Jersey	1020
Copertura ampia per Numero patente di guida - Stato del New Jersey	1020
Copertura media numero patente di guida - Stato del New Jersey	1020
Numero patente di guida - Stato di New York	1021
Copertura ampia Numero patente di guida - Stato di New York	1022
Copertura media numero patente di guida - Stato di New York	1022
Numero di patente di guida - Stato di Washington	1023
Copertura ampia del numero di patente di guida - Stato di Washington	1023
Copertura media numero di patente di guida - Stato di Washington	1024
Copertura limitata numero di patente di guida - Stato di Washington	1024
Numero di patente di guida - Stato del Wisconsin	1025
Copertura ampia numero patente di guida - Stato del Wisconsin	1025
Copertura media numero patente di guida - Stato del Wisconsin	1026
Copertura limitata numero patente di guida - Stato del Wisconsin	1027
Numero DEA (Drug Enforcement Agency)	1027
Copertura ampia del numero DEA (Drug Enforcement Agency)	1028
Copertura media numero DEA (Drug Enforcement Agency)	1028
Copertura limitata numero DEA (Drug Enforcement Agency)	1029
Numero di patente di guida finlandese	1029
Copertura ampia del numero di patente di guida finlandese	1030
Copertura media del numero patente di guida finlandese	1030
Copertura limitata del numero di patente di guida finlandese	1031
Numero di previdenza sociale europea della Finlandia	1032

Copertura ampia del numero di previdenza sociale europea della Finlandia	1032
Copertura limitata del numero di previdenza sociale europea della Finlandia	1033
Numero di passaporto finlandese	1034
Copertura ampia del numero di passaporto finlandese	1034
Copertura limitata del numero di passaporto finlandese	1035
Numero di identificazione fiscale finlandese	1035
Copertura ampia del numero di identificazione fiscale finlandese	1036
Copertura media del numero di identificazione fiscale finlandese	1036
Copertura limitata del numero di identificazione fiscale finlandese	1037
Numero di partita IVA finlandese	1038
Copertura ampia del numero di partita IVA finlandese	1038
Copertura media del numero di partita IVA finlandese	1039
Copertura limitata del numero di partita IVA finlandese	1039
Codice identificativo personale finlandese	1040
Copertura ampia codice identificativo personale finlandese	1040
Copertura media codice identificativo personale finlandese	1041
Copertura limitata codice identificativo personale finlandese	1041
Numero di patente di guida francese	1042
Copertura ampia del numero di patente di guida francese	1042
Copertura limitata del numero di patente di guida francese	1043
Numero di previdenza sociale francese	1044
Copertura ampia del numero di previdenza sociale francese	1044
Copertura limitata del numero di previdenza sociale francese	1044
Numero di identificazione fiscale francese	1045
Copertura ampia del numero di identificazione fiscale francese	1045
Copertura limitata del numero di identificazione fiscale francese	1046
Numero di partita IVA francese	1047
Copertura ampia numero di partita IVA francese	1047
Copertura media del numero di partita IVA francese	1048
Copertura limitata numero di partita IVA francese	1048
Codice INSEE francese	1049
Copertura ampia codice INSEE francese	1050
Copertura limitata codice INSEE francese	1050
Numero di passaporto francese	1051
Copertura ampia Numero di passaporto francese	1051

Copertura limitata Numero di passaporto francese	1052
Numero di previdenza sociale francese	1052
Copertura ampia del numero di previdenza sociale francese	1053
Copertura media numero di previdenza sociale francese	1053
Copertura limitata del numero di previdenza sociale francese	1054
Numero di passaporto tedesco	1054
Copertura ampia numero di passaporto tedesco	1055
Copertura media del numero di passaporto tedesco	1055
Copertura limitata numero di passaporto tedesco	1056
Numero di identificazione personale tedesco	1056
Copertura ampia numero di identificazione personale tedesco ... 1 0 5 7	
Copertura media numero di identificazione personale tedesco	1057
Copertura limitata numero di identificazione personale tedesco	1058
Numero di patente di guida tedesca	1059
Copertura ampia del numero di patente di guida tedesca	1059
Copertura limitata del numero di patente di guida tedesca	1059
Numero di identificazione fiscale tedesco	1060
Copertura ampia numero di identificazione fiscale tedesco	1061
Copertura media numero di identificazione fiscale tedesco	1061
Copertura limitata del numero di identificazione fiscale tedesco	1062
Numero di partita IVA tedesca	1063
Copertura ampia numero di partita IVA tedesca	1063
Copertura media del numero di partita IVA tedesca	1064
Copertura limitata numero di partita IVA tedesca	1064
Codice fiscale della Grecia (AMKA)	1065
Copertura ampia del codice fiscale della Grecia (AMKA)	1066
Copertura media codice fiscale della Grecia (AMKA)	1066
Copertura limitata codice fiscale della Grecia (AMKA)	1066
Codice fiscale greco (AFM)	1067
Copertura ampia del codice fiscale greco (AFM)	1067
Copertura media codice fiscale greco (AFM)	1068
Copertura limitata codice fiscale greco (AFM)	1068
Healthcare Common Procedure Coding System (codice CPT HCPCS).	1069
Copertura media Healthcare Common Procedure Coding System (codice CPT HCPCS).	1070
Copertura limitata Healthcare Common Procedure Coding System (codice CPT HCPCS)	1071

Numero di assicurazione sanitaria	1072
Copertura ampia del numero di assicurazione sanitaria	1073
Copertura media del numero di assicurazione sanitaria	1074
Copertura limitata del numero di assicurazione sanitaria	1074
ID Hong Kong	1076
Copertura ampia dell'ID Hong Kong	1076
Copertura limitata ID Hong Kong	1077
Numero di previdenza sociale ungherese	1078
Copertura ampia numero di previdenza sociale ungherese	1078
Copertura media del numero di previdenza sociale ungherese	1078
Copertura limitata numero di previdenza sociale ungherese	1079
Numero di identificazione fiscale ungherese	1080
Copertura ampia del numero di identificazione fiscale ungherese	1080
Copertura media numero di identificazione fiscale ungherese	1080
Copertura limitata numero di identificazione fiscale ungherese	1081
Numero di partita IVA ungherese	1082
Copertura ampia numero di partita IVA ungherese	1082
Copertura media del numero di partita IVA ungherese	1083
Copertura limitata numero di partita IVA ungherese	1083
IBAN paesi centrali	1084
Copertura ampia IBAN paesi centrali	1085
Copertura limitata dell'IBAN paesi centrali	1086
IBAN paesi orientali	1088
Copertura ampia dell'IBAN paesi orientali	1089
Copertura limitata IBAN paesi orientali	1091
IBAN paesi occidentali	1094
Copertura ampia dell'IBAN paesi occidentali	1094
Copertura limitata IBAN paesi occidentali	1096
Numero tessera Aadhaar indiana	1098
Copertura ampia Numero tessera Aadhaar indiana	1099
Copertura media Numero tessera Aadhaar indiana	1099
Copertura limitata Numero tessera Aadhaar indiana	1100
Codice di identificazione fiscale indiano (PAN)	1100
Copertura ampia codice di identificazione fiscale indiano (PAN)	1101
Copertura limitata del codice di identificazione fiscale indiano (PAN)	1101
Numero di carta di identità indonesiana (KTP)	1102

Copertura ampia numero di carta di identità indonesiana (KTP)	1102
Copertura media numero di carta di identità indonesiana (KTP)	1103
Copertura limitata del numero di carta di identità indonesiana (KTP)	1103
Numero IMEI	1104
Copertura ampia del numero IMEI	1104
Copertura media numero IMEI	1105
Copertura limitata numero IMEI	1105
Codice ISIN (International Securities Identification Number)	1106
Copertura ampia codice ISIN (International Securities Identification Number)	1107
Copertura media codice ISIN (International Securities Identification Number)	1107
Copertura limitata Codice ISIN (International Securities Identification Number)	1108
Indirizzo IP	1108
Copertura ampia indirizzo IP	1109
Copertura media indirizzo IP	1109
Copertura limitata dell'indirizzo IP	1110
Indirizzo IPv6	1110
Copertura ampia dell'indirizzo IPv6	1111
Copertura media indirizzo IPv6.	1111
Copertura limitata dell'indirizzo IPv6	1112
Numero di passaporto irlandese	1113
Copertura ampia del numero di passaporto irlandese	1113
Copertura limitata del numero di passaporto irlandese	1114
Numero di identificazione fiscale irlandese	1114
Copertura ampia del numero di identificazione fiscale irlandese	1115
Copertura media numero di identificazione fiscale irlandese	1116
Copertura limitata del numero di identificazione fiscale irlandese	1117
Numero di partita IVA irlandese	1118
Copertura ampia del numero di partita IVA irlandese	1119
Copertura media del numero di partita IVA irlandese	1120
Copertura limitata del numero di partita IVA irlandese	1120
Numero personale di servizio pubblico irlandese	1121
Copertura ampia del numero personale di servizio pubblico irlandese (PPS)	1122
Copertura media del numero personale di servizio pubblico irlandese (PPS)	1122

Copertura limitata numero personale di servizio pubblico irlandese (PPS)	1123
Numero di identificazione personale israeliano	1124
Copertura ampia del Numero di identificazione personale israeliano	1124
Copertura media del Numero di identificazione personale israeliano	1124
Copertura limitata Numero di identificazione personale israeliano	1125
Numero di patente di guida italiana	1126
Copertura ampia del numero di patente di guida italiana	1126
Copertura limitata del numero di patente di guida italiana	1127
Numero di previdenza sociale italiano	1127
Copertura ampia del numero di previdenza sociale italiano	1128
Copertura limitata del numero di previdenza sociale italiano	1128
Numero di passaporto italiano	1129
Copertura ampia del numero di passaporto italiano	1130
Copertura limitata del numero di passaporto italiano	1130
Numero di partita IVA italiano	1131
Copertura ampia numero di partita IVA italiana	1131
Copertura media del numero di partita IVA italiana	1132
Copertura limitata numero di partita IVA italiana	1132
Numero di patente di guida giapponese	1133
Copertura ampia del numero di patente di guida giapponese	1133
Copertura media del numero di patente di guida giapponese	1134
Copertura limitata del numero di patente di guida giapponese	1134
Numero di passaporto giapponese	1135
Copertura ampia Numero di passaporto giapponese	1135
Copertura limitata Numero di passaporto giapponese	1136
Numero di identificazione giapponese (Juki Net)	1137
Copertura ampia numero di identificazione giapponese (Juki Net)	1137
Copertura media numero di identificazione giapponese (Juki Net)	1138
Copertura limitata numero di identificazione giapponese (Juki Net)	1138
Numero di identificazione personale giapponese - Aziendale	1139
Copertura ampia numero di identificazione personale giapponese - Aziendale	1139
Copertura limitata numero di identificazione personale giapponese - Aziendale	1140
Numero di identificazione personale giapponese - Personale	1141

Copertura ampia del numero di identificazione personale	
giapponese - Personale	1141
Copertura media del numero di identificazione personale	
giapponese - Personale	1142
Copertura limitata del numero di identificazione personale	
giapponese - Personale	1142
Numero di passaporto coreano	1143
Copertura ampia Numero di passaporto coreano	1144
Copertura limitata Numero di passaporto coreano	1144
Numero di registrazione anagrafica coreano per stranieri.	1145
Copertura ampia Numero di registrazione anagrafica coreano per	
stranieri	1146
Copertura media Numero di registrazione anagrafica coreano per	
stranieri	1146
Copertura limitata Numero di registrazione anagrafica coreano	
per stranieri	1147
Numero di registrazione anagrafica coreano per coreani	1148
Copertura ampia Numero di registrazione anagrafica coreano per	
coreani	1148
Copertura media Numero di registrazione anagrafica coreano per	
coreani	1149
Copertura limitata Numero di registrazione anagrafica coreano	
per coreani	1150
Numero di identificazione personale lettone	1151
Copertura ampia del numero di identificazione personale	
lettone	1151
Copertura media del numero di identificazione personale	
lettone	1151
Copertura limitata del numero di identificazione personale	
lettone	1152
Numero di identificazione lussemburghese (RNPP)	1153
Copertura ampia numero di identificazione lussemburghese	
(RNPP)	1153
Copertura media numero di identificazione lussemburghese	
(RNPP)	1154
Copertura limitata del numero di identificazione lussemburghese	
(RNPP)	1154
Numero di passaporto lussemburghese	1155
Copertura ampia del numero di passaporto lussemburghese	1156
Copertura limitata numero di passaporto lussemburghese	1156
Numero di identificazione fiscale lussemburghese	1157
Copertura ampia del numero di identificazione fiscale	
lussemburghese	1157

Numero di conto bancario esteso messicano (CLABE)	1176
Copertura ampia numero di conto bancario esteso messicano (CLABE)	1176
Copertura media numero di conto bancario esteso messicano (CLABE)	1177
Copertura limitata del numero di conto bancario esteso messicano (CLABE)	1177
National Drug Code (NDC, codici identificativi dei farmaci)	1178
Copertura ampia National Drug Code (NDC, codici identificativi dei farmaci)	1179
Copertura media National Drug Code (NDC)	1179
Copertura limitata National Drug Code (NDC, codici identificativi dei farmaci)	1180
Numero NPI	1181
Copertura ampia del numero NPI	1181
Copertura media numero NPI	1181
Copertura limitata numero NPI	1182
Numero di patente di guida dei Paesi Bassi	1183
Copertura ampia del numero di patente di guida dei Paesi Bassi	1183
Copertura limitata del numero di patente di guida dei Paesi Bassi	1183
Numero di passaporto dei Paesi Bassi	1184
Copertura ampia numero di passaporto dei Paesi Bassi	1184
Copertura limitata numero di passaporto dei Paesi Bassi	1185
Numero di identificazione fiscale dei Paesi Bassi	1185
Copertura ampia del numero di identificazione fiscale dei Paesi Bassi	1186
Copertura media del numero di identificazione fiscale dei Paesi Bassi	1186
Copertura limitata del numero di identificazione fiscale dei Paesi Bassi	1187
Numero di partita IVA dei Paesi Bassi	1189
Copertura ampia numero di partita IVA dei Paesi Bassi	1189
Copertura media del numero di partita IVA dei Paesi Bassi	1190
Copertura limitata numero di partita IVA dei Paesi Bassi	1190
Codice di assistenza sanitaria della Nuova Zelanda (NHI)	1191
Copertura ampia codice di assistenza sanitaria della Nuova Zelanda (NHI)	1191
Copertura media del codice di assistenza sanitaria della Nuova Zelanda (NHI)	1192
Copertura limitata del codice di assistenza sanitaria della Nuova Zelanda (NHI)	1192

Numero di identificazione personale norvegese	1193
Copertura ampia del numero di identificazione personale norvegese	1194
Copertura media numero di identificazione personale norvegese	1194
Copertura media numero di identificazione personale norvegese	1195
Documento di identità cinese	1196
Copertura ampia documento di identità cinese	1196
Copertura limitata del documento di identità cinese	1196
Numero di carta di identità polacca	1197
Copertura ampia numero di carta di identità polacca	1197
Copertura media numero di carta di identità polacca	1198
Copertura limitata numero di carta di identità polacca	1198
Codice statistico polacco (REGON)	1199
Copertura ampia codice statistico polacco (REGON)	1200
Copertura media codice statistico polacco (REGON)	1200
Copertura limitata codice statistico polacco (REGON)	1200
Codice fiscale polacco (PESEL)	1201
Copertura ampia codice fiscale polacco (PESEL)	1202
Copertura media codice fiscale polacco (PESEL)	1202
Copertura limitata del codice fiscale polacco (PESEL)	1202
Numero di identificazione fiscale polacco (NIP)	1203
Copertura ampia numero di identificazione fiscale polacco (NIP)	1204
Copertura media numero di identificazione fiscale polacco (NIP)	1204
Copertura limitata numero di identificazione fiscale polacco (NIP)	1205
Numero di patente di guida portoghese	1206
Copertura ampia del numero di patente di guida portoghese	1206
Copertura limitata del numero di patente di guida portoghese	1207
Numero di identificazione nazionale portoghese	1208
Copertura ampia numero di identificazione nazionale portoghese	1208
Copertura media numero di identificazione nazionale portoghese	1209
Copertura limitata numero di identificazione nazionale portoghese	1210
Numero di passaporto portoghese	1211
Copertura ampia del numero di passaporto portoghese	1211
Copertura limitata del numero di passaporto portoghese	1212

Numero di identificazione fiscale portoghese	1212
Copertura ampia del numero di identificazione fiscale portoghese	1213
Copertura media del numero di identificazione fiscale portoghese	1213
Copertura limitata del numero di identificazione fiscale portoghese	1214
Numero di partita IVA portoghese	1215
Copertura ampia del numero di partita IVA portoghese	1216
Copertura media del numero di partita IVA portoghese	1216
Copertura limitata del numero di partita IVA portoghese	1217
Social Security Number (SSN) statunitense randomizzato	1218
Copertura media Social Security Number (SSN) statunitense randomizzato	1219
Copertura limitata Social Security Number (SSN) statunitense randomizzato	1220
Numero di identificazione nazionale rumeno	1221
Copertura ampia del numero di identificazione nazionale rumeno	1221
Copertura media del numero di identificazione nazionale rumeno	1222
Copertura limitata numero di identificazione nazionale rumeno	1222
Numero di identificazione personale rumeno (CNP)	1223
Copertura ampia del numero di identificazione personale rumeno (CNP)	1224
Copertura media numero di identificazione personale rumeno (CNP)	1224
Copertura limitata numero di identificazione personale rumeno (CNP)	1224
Numero di passaporto russo interno	1225
Copertura ampia numero di passaporto russo interno	1226
Copertura limitata numero di passaporto russo interno	1226
Numero di identificazione fiscale russo (INN)	1227
Copertura ampia numero di identificazione fiscale russo (INN)	1227
Copertura media numero di identificazione fiscale russo (INN)	1228
Copertura limitata numero di identificazione fiscale russo (INN)	1228
Identificatore di dati NRIC Singapore	1229
Numero di identificazione nazionale slovacco	1230

Copertura ampia del numero di identificazione nazionale slovacco	1230
Copertura media del numero di identificazione nazionale slovacco	1231
Copertura limitata numero di identificazione nazionale slovacco	1232
Numero identificativo cittadini della Slovenia	1233
Copertura ampia del numero identificativo cittadini della Slovenia	1234
Copertura media del numero identificativo dei cittadini della Slovenia	1234
Copertura limitata del numero identificativo dei cittadini della Slovenia	1235
Numero di identificazione personale sudafricano	1235
Copertura ampia numero di identificazione personale sudafricano	1236
Copertura media numero di identificazione personale sudafricano	1236
Copertura limitata del numero di identificazione personale sudafricano	1237
Numero di patente di guida spagnola	1238
Copertura ampia del numero di patente di guida spagnola	1238
Copertura limitata del numero di patente di guida spagnola	1239
Numero di partita IVA spagnolo	1240
Copertura ampia del numero di partita IVA spagnolo	1240
Copertura media del numero di partita IVA spagnolo	1241
Copertura limitata del numero di partita IVA spagnolo	1242
Numero di conto cliente spagnolo	1243
Copertura ampia numero di conto cliente spagnolo	1243
Modello copertura media numero di conto cliente spagnolo	1244
Copertura limitata numero di conto cliente spagnolo	1244
Numero di DNI spagnolo	1245
Copertura ampia del numero di DNI spagnolo	1245
Copertura limitata del numero di DNI spagnolo	1246
Numero di passaporto spagnolo	1247
Copertura ampia Numero di passaporto spagnolo	1247
Copertura limitata Numero di passaporto spagnolo	1248
Numero di previdenza sociale spagnolo	1249
Copertura ampia numero di previdenza sociale spagnolo	1249
Copertura media del numero di previdenza sociale spagnolo	1249
Copertura limitata numero di previdenza sociale spagnolo	1250
Codice fiscale spagnolo (CIF)	1251

Copertura ampia del codice fiscale spagnolo (CIF)	1251
Copertura media codice fiscale spagnolo (CIF)	1252
Copertura limitata codice fiscale spagnolo (CIF)	1252
Numero di patente di guida svedese	1254
Copertura ampia del numero di patente di guida svedese	1254
Copertura media del numero patente di guida svedese	1254
Copertura limitata del numero di patente di guida svedese	1255
Numero di identificazione fiscale svedese	1256
Copertura ampia del numero di identificazione fiscale svedese	1256
Copertura media del numero di identificazione fiscale svedese	1257
Copertura limitata del numero di identificazione fiscale svedese	1257
Numero di partita IVA svedese	1258
Copertura ampia del numero di partita IVA svedese	1259
Copertura media del numero di partita IVA svedese	1259
Copertura limitata del numero di partita IVA svedese	1260
Numero di passaporto svedese	1260
Copertura ampia Numero di passaporto svedese	1261
Copertura limitata Numero di passaporto svedese	1261
Numero di identificazione personale svedese	1262
Copertura ampia del numero di identificazione personale svedese	1262
Copertura media del numero di identificazione personale svedese	1263
Copertura limitata numero di identificazione personale svedese	1264
Codice SWIFT	1265
Copertura ampia Codice SWIFT	1265
Copertura limitata codice SWIFT	1266
Numero AHV svizzero	1267
Copertura ampia numero di previdenza sociale svizzero (AHV)	1268
Copertura limitata del numero AHV svizzero	1268
Numero di previdenza sociale svizzero (AHV)	1269
Copertura ampia del numero di codice fiscale svizzero (AHV)	1269
Copertura media del numero di previdenza sociale svizzero (AHV)	1270
Copertura limitata numero di previdenza sociale svizzero (AHV)	1270
ID ROC Taiwan	1271

Copertura ampia ID RDC Taiwan	1272
Copertura limitata dell'ID RDC Taiwan	1272
Numero di identificazione personale thailandese	1273
Copertura ampia del numero di identificazione personale thailandese	1273
Copertura media numero di identificazione personale thailandese	1273
Copertura limitata codice identificativo personale thailandese	1274
Numero di identificazione turco	1275
Copertura ampia del numero di identificazione turco	1275
Copertura media del numero di identificazione turco	1276
Copertura limitata di numero di identificazione turco	1276
Coordinate bancarie di un numero di conto britannico	1277
Copertura ampia delle Coordinate bancarie di un numero di conto britannico.	1277
Copertura media delle coordinate bancarie di un numero di conto britannico	1278
Copertura limitata delle coordinate bancarie di un numero di conto britannico	1278
Numero di patente di guida britannica	1279
Copertura ampia numeri delle patenti di guida britanniche	1280
Copertura media numero patente di guida britannica	1280
Copertura limitata del numero di patente di guida britannica	1281
Numero di tessera elettorale britannico	1282
Numero NHS (National Health Service) del Regno Unito	1282
Copertura media Numero NHS (National Health Service) britannico	1283
Copertura limitata numero NHS (National Health Service) britannico	1284
Numero di previdenza sociale britannico	1285
Copertura ampia Numero di previdenza sociale britannico	1285
Copertura media numero di previdenza sociale britannico	1286
Copertura limitata numero di previdenza sociale britannico	1286
Numero di passaporto britannico	1287
Copertura ampia Numero di passaporto britannico	1287
Copertura media numero di passaporto britannico	1288
Copertura limitata numero di passaporto britannico	1288
Codice fiscale britannico	1289
Copertura ampia codice fiscale britannico	1289
Copertura media codice fiscale britannico	1290
Copertura limitata codice fiscale britannico	1290
Numero di partita IVA britannico (VAT)	1291
Copertura ampia del numero di partita IVA britannico (VAT)	1291

Copertura media del numero di partita IVA britannico (VAT)	1292
Copertura limitata del numero di partita IVA britannico (VAT)	1293
Passaporto ucraino (interno)	1294
Copertura ampia del passaporto ucraino (interno)	1295
Copertura limitata del passaporto ucraino (interno)	1295
Carta di identità ucraina	1296
Copertura ampia della carta di identità ucraina	1296
Copertura media della carta di identità ucraina	1297
Copertura limitata della carta di identità ucraina	1297
Passaporto ucraino (internazionale)	1298
Copertura ampia del passaporto ucraino (internazionale)	1298
Copertura limitata del passaporto ucraino (internazionale)	1299
Numero di identificazione personale degli Emirati Arabi Uniti	1300
Copertura ampia numero di identificazione personale degli Emirati Arabi Uniti	1300
Copertura media numero di identificazione personale degli Emirati Arabi Uniti	1301
Copertura limitata numero di identificazione personale degli Emirati Arabi Uniti	1301
US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)	1302
Copertura ampia US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)	1303
Copertura media US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)	1303
Copertura limitata US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)	1304
Numero di passaporto statunitense	1305
Copertura ampia Numero di passaporto statunitense	1305
Copertura limitata Numero di passaporto statunitense	1306
Social Security Number (SSN) statunitense	1307
Copertura ampia del numero di previdenza sociale (SSN) statunitense	1307
Copertura media Social Security Number (SSN) statunitense	1308
Copertura limitata Social Security Number (SSN) statunitense	1309
Codici di avviamento postale Zip+4 statunitensi	1310
Copertura ampia Codici di avviamento postale Zip+4 statunitensi	1310
Copertura media Codici di avviamento postale Zip+4 statunitensi	1311

Copertura limitata Codici di avviamento postale Zip+4	
statunitensi	1311
Numero di identificazione nazionale venezuelano	1312
Copertura ampia numero di identificazione nazionale	
venezuelano	1313
Copertura media numero di identificazione nazionale venezuelano	
.....	1313
Copertura limitata del numero di identificazione nazionale	
venezuelano	1314

Capitolo 41	Libreria dei modelli di politica	1316
	Modello della politica Relazione Caldicott	1319
	Modello della politica Numeri di previdenza sociale (SIN)	
	canadesi	1321
	Modello di politica CAN-SPAM Act	1321
	Modello della politica della legge colombiana sulla protezione dei dati	
	personali 1581	1322
	Modello politica Siti caricamento spyware comuni	1323
	Modello di politica Comunicazioni con i concorrenti	1323
	Modello della politica Documenti riservati	1324
	Modello della politica Numeri di carta di credito	1325
	Modello di politica Protezione dei dati dei clienti	1325
	Modello della politica Data Protection Act 1998 (legge sulla protezione	
	dei dati del 1998)	1327
	Modello della politica Direttive UE sulla protezione dei dati	1329
	Modello di politica Classificazione GENSER Defense Message System	
	(DMS)	1331
	Modello della politica Documenti di progettazione	1332
	Modello di politica Protezione dei dati dei dipendenti	1333
	Modello della politica Dati crittografati	1335
	Modello di politica Export Administration Regulations (EAR)	1335
	Modello di politica FACTA 2003 (regole Red Flag)	1337
	Modello di politica Informazioni finanziarie	1340
	Modello della politica Siti Web non consentiti	1341
	Modello politica Gioco d'azzardo	1342
	Regolamento generale per la protezione dei dati (attività bancarie e	
	finanza)	1342
	Regolamento generale per la protezione dei dati (identità	
	digitale)	1364
	Regolamento generale per la protezione dei dati (identificazione	
	governativa)	1365

Regolamento generale per la protezione dei dati (sanità e assicurazioni)	1389
Regolamento generale per la protezione dei dati (profilo personale)	1401
Regolamento generale per la protezione dei dati (viaggi)	1404
Modello di politica Gramm-Leach-Bliley	1414
Modello di politica HIPAA e HITECH (incluso PHI)	1416
Modello di politica Human Rights Act (legge sui diritti umani) del 1998	1421
Modello di politica Sostanze illegali	1421
Modello della politica Codici identificativi dei contribuenti (ITIN)	1422
Modello di politica International Traffic in Arms Regulations (ITAR)	1422
Modello della politica File multimediali	1424
Medicare e Medicaid (incluso PHI)	1424
Modello della politica Contratti di acquisizione e fusione	1426
Modello di politica Regola NASD 2711 e regole NYSE 351 e 472	1427
Modello di politica Regola NASD 3010 e regola NYSE 342	1428
Modello di politica Linee guida sulla sicurezza del NERC per le società elettriche	1430
Modello della politica Diagrammi di rete	1432
Modello della politica Sicurezza di rete	1433
Modello di politica Linguaggio offensivo	1433
Modello di politica OFAC (Ufficio per il Controllo dei Fondi Stranieri)	1433
Modello di politica Memorandum OMB 06-16 e disposizioni FIPS 199	1436
Modello della politica File di password	1437
Modello della politica Payment Card Industry (PCI) Data Security Standard	1437
Modello di politica PIPEDA	1439
Modello di politica Informazioni sui prezzi	1441
Modello della politica Dati di progetto	1441
Modello di politica File multimediali proprietari	1441
Modello della politica Documenti di pubblicazione	1442
Modello politica Linguaggio razzista	1443
Modello della politica File con restrizioni	1443
Modello della politica Destinatari con restrizioni	1443
Modello della politica Curriculum	1444
Modello della politica Sarbanes-Oxley	1445
Modello della politica Normativa sull'imparzialità della trasparenza SEC	1447
Modello di politica Linguaggio sessualmente esplicito	1449

Modello di politica Codice sorgente	1450
Modello di privacy dei dati relativi allo stato	1451
Modello della politica Codici SWIFT	1455
Modello della politica Compatibilità Symantec DLP e Prevenzione	1455
Modello della politica Numeri Patente di guida del Regno Unito	1456
Modello politica Numeri di tessera elettorale britannici	1456
Modello della politica Numero NHS (National Health Service) britannico	1457
Modello della politica Numeri di previdenza sociale britannici	1457
Modello della politica Numeri di passaporto britannici	1457
Modello di politica Codici fiscali britannici	1458
Marchi di controllo dei servizi di intelligence degli Stati Uniti (CAPCO) e modello della politica DCID 1/7	1458
Modello di politica Social Security Number statunitense	1460
Modello della politica Violenza e armi	1460
Modello della politica di Webmail	1460
Modello di politica Attività della bacheca messaggi di Yahoo	1462
Modello di politica Yahoo e MSN Messenger sulla porta 80	1463

Sezione 5 Regole delle regola di risposta di politica 1466

Capitolo 42 Risposta alle violazioni di politica	1467
Informazioni sulle regole di risposta	1468
Informazioni sulle azioni di regola di risposta	1468
Azioni delle regole di risposta per tutti i server di rilevamento	1469
Azioni delle regole di risposta per il rilevamento di endpoint	1470
Azioni delle regole di risposta per il rilevamento di Network Prevent	1471
Azioni delle regole di risposta per il rilevamento di Network Protect	1472
Azioni di regole di risposta per rilevamento archiviazione cloud	1473
Azioni di regole di risposta per rilevatori Applicazioni cloud e dispositivo API	1474
Informazioni sui tipi di esecuzione delle regole di risposta	1478
Informazioni sulle regole di risposta automatica	1478
Informazioni sulle regole di risposta smart	1479
Informazioni sulle condizioni delle regole di risposta	1480
Informazioni sulla priorità di esecuzione delle azioni di regola di risposta	1481

	Informazioni sui privilegi di creazione di regole di risposta	1485
	Implementazione di regole di risposta	1486
	Best practice per le regole di risposta	1487
Capitolo 43	Configurazione e gestione delle regole di risposta	1489
	Gestione di regole di risposta	1489
	Aggiunta di una nuova regola di risposta	1490
	Configurazione di regole di risposta	1491
	Informazioni sulle regole di risposta smart	1492
	Configurazione delle condizioni della regola di risposta	1492
	Configurazione delle azioni di regola di risposta	1493
	Modifica dell'ordinamento delle regole di risposta	1497
	Informazioni sulla rimozione di regole di risposta	1498
Capitolo 44	Condizioni di regole di risposta	1499
	Configurazione dello condizione di risposta Posizione endpoint	1499
	Configurazione della condizione di risposta del dispositivo endpoint	1500
	Configurazione della condizione di risposta Tipo di incidente	1501
	Configurazione della condizione di risposta Numero corrispondenza incidenti	1503
	Configurazione della condizione di risposta Monitoraggio protocollo o endpoint	1504
	Configurazione della condizione di risposta Gravità	1506
Capitolo 45	Azioni di regole di risposta	1508
	Configurazione dell'azione Aggiungi nota	1510
	Configurazione dell'azione Limita conservazione dati incidenti	1510
	Conservazione dei dati per gli incidenti degli endpoint	1511
	Eliminazione dei dati per gli incidenti di rete	1512
	Configurazione del registro a un'azione del server Syslog	1513
	Configurazione dell'azione Invia notifica e-mail	1514
	Configurazione dell'azione di FlexResponse server	1516
	Configurazione dell'azione Imposta attributo	1517
	Configurazione dell'azione Imposta stato	1518
	Configurazione dell'azione di risposta Classifica contenuto Enterprise Vault	1519
	Configurazione delle categorie di conservazione disponibili per la classificazione	1521

Configurazione dell'azione Archiviazione cloud: aggiungi tag visivo	1523
Configurazione dell'azione Archiviazione cloud: quarantena	1523
Configurazione dell'azione di risposta smart Quarantena	1525
Configurazione dell'azione di risposta smart alla Quarantena SharePoint	1525
Configurazione dell'azione di risposta smart Ripristina file	1528
Configurazione dell'azione Interrompi collegamenti nei dati a riposo	1528
Configurazione dell'azione Azione personalizzata su dati a riposo	1529
Configurazione dell'azione Elimina dati a riposo	1530
Configurazione dell'azione Crittografia dati a riposo	1531
Configurazione dell'azione Esegui DRM su dati a riposo	1531
Configurazione dell'azione Metti in quarantena dati a riposo	1532
Configurazione dell'azione Marca dati a riposo	1533
Configurazione dell'azione Impedisci download, copia, stampa	1534
Configurazione dell'azione Rimuovi accesso collaboratore	1534
Configurazione dell'azione Imposta accesso collaboratore in Modifica	1535
Configurazione dell'azione Imposta accesso collaboratore in Anteprima	1535
Configurazione dell'azione Imposta accesso collaboratore in Lettura	1536
Configurazione dell'azione Imposta accesso file in Lettura completa	1537
Configurazione di Imposta accesso file in Modifica interna	1537
Configurazione dell'azione Imposta accesso file in Lettura interna	1538
Configurazione dell'azione Aggiungi autenticazione a due fattori	1539
Configurazione dell'azione Blocca dati in movimento	1539
Configurazione dell'azione Azione personalizzata su dati in movimento	1540
Configurazione dell'azione Crittografia dati in movimento	1541
Configurazione dell'azione Esegui DRM su dati in movimento	1541
Configurazione dell'azione Metti in quarantena dati in movimento	1542
Configurazione dell'azione Cancella dati in movimento	1543
Configurazione dell'azione Endpoint: FlexResponse	1544
Configurazione dell'azione Endpoint Discover: metti file in quarantena	1545
Configurazione dell'azione Endpoint Prevent: blocca	1547
Configurazione dell'azione Endpoint Prevent: crittografia	1550
Configurazione dell'azione Endpoint Prevent: notifica	1554
Configurazione dell'azione Endpoint Prevent: operazione annullata dall'utente	1557

Configurazione dell'azione Network Prevent for Web: Blocca richiesta FTP	1560
Configurazione dell'azione Network Prevent for Web: blocca HTTP/HTTPS	1560
Configurazione dell'azione Network Prevent: blocca messaggio SMTP	1562
Configurazione dell'azione Network Prevent: modifica messaggio SMTP	1563
Configurazione dell'azione Network Prevent for Web: rimuovi contenuto HTTP/HTTPS	1564
Configurazione dell'azione Network Protect: copia file	1565
Configurazione dell'azione Network Protect: metti file in quarantena	1566
Configurazione dell'azione Network Protect: crittografa file	1567

Sezione 6 Risoluzione e gestione degli incidenti 1569

Capitolo 46 Risoluzione di incidenti 1570

Informazioni sulla riparazione degli incidenti	1570
Risoluzione di incidenti	1573
Esecuzione di regole di risposta smart	1574
Comandi delle azioni di riparazione degli incidenti	1575
Variabili azione di risposta	1576
Variabili generali di incidente	1576
Variabili di incidenti di Network Monitor e Network Prevent	1577
Variabili di incidente di Discover	1578
Variabili di incidente endpoint	1578
Variabili di incidente dei connettori cloud	1579

Capitolo 47 Risoluzione di incidenti di rete 1580

Elenco degli incidenti di rete	1580
Elenco incidenti di rete - Azioni	1583
Elenco di incidenti di rete - Colonne	1585
Istantanea incidente di rete	1586
Istantanea incidente di rete - Intestazione e navigazione	1587
Istantanea incidente di rete—Informazioni generali	1587
Istantanea incidente di rete - Corrispondenze	1590
Istantanea incidente di rete - Attributi	1591
Report riepilogo rete	1591

Capitolo 48	Risoluzione di incidenti endpoint	1594
	Informazioni sugli elenchi di incidenti endpoint	1594
	Istantanea ticket Endpoint	1597
	Creazione di report su regole di risposta di Endpoint Prevent	1602
	Informazioni specifiche al protocollo o alla destinazione degli incidenti Endpoint	1604
	Report di riepilogo sugli incidenti endpoint	1605
Capitolo 49	Risoluzione di incidenti di rilevazione	1608
	Informazioni sui report per Network Discover	1608
	Informazioni sui report incidente per Network Discover/Cloud Storage Discover	1610
	Report incidente di Discover	1610
	Elenchi di incidenti di Discover	1611
	Azioni relative a incidenti di Discover	1611
	Voci sugli incidenti di Discover	1613
	Istantanea incidente di Discover	1615
	Report riepilogativi di Discover	1618
Capitolo 50	Utilizzo di incidenti connettore cloud	1619
	Informazioni sui report incidente delle applicazioni	1619
	Elenco di incidenti applicazione	1621
	Voci sugli incidenti delle applicazioni	1621
	Azioni incidente delle applicazioni	1623
	Istantanea incidente delle applicazioni	1624
	Report riepilogativi delle applicazioni	1628
Capitolo 51	Gestione e report degli incidenti	1630
	Informazioni sui report Symantec Data Loss Prevention	1632
	Informazioni sulle strategie per l'utilizzo di report	1633
	Impostazione delle preferenze di report	1634
	Informazioni sui report degli incidenti	1635
	Informazioni sui report dashboard e i riepiloghi executive	1637
	Visualizzazione di dashboard	1639
	Creazione di report di dashboard	1639
	Configurazione report della dashboard	1641
	Scelta dei report da includere in un dashboard	1642
	Informazioni sui report riepilogativi	1643
	Visualizzazione di report riepilogativi	1643
	Creazione di report riepilogativi	1644
	Visualizzazione degli incidenti	1645

Informazioni su report e dashboard personalizzati	1646
Utilizzo di IT Analytics per la gestione di incidenti	1648
Report di filtraggio	1648
Salvataggio dei report di incidente personalizzati	1649
Pianificazione dei report di incidente personalizzati	1650
Opzioni di pianificazione di consegna per i report di incidente e di sistema	1652
Opzioni di pianificazione di consegna per i report del dashboard	1654
Utilizzo del widget della data per pianificare i report	1656
Modifica dei dashboard e dei report personalizzati	1656
Esportazione dei report di incidente	1656
Campi esportati per Network Monitor	1657
Campi esportati per Network Discover/Cloud Storage Discover	1658
Campi esportati per Endpoint Discover	1659
Eliminazione di incidenti	1660
Informazioni sul processo di eliminazione incidente	1662
Configurazione della pianificazione del processo di eliminazione incidenti	1662
Avvio e arresto di processi di eliminazione incidenti	1663
Uso della cronologia processi di eliminazione	1664
Informazioni su come contrassegnare automaticamente gli incidenti da eliminare	1665
Informazioni sulla creazione dei report di incidente per contrassegnare automaticamente gli incidenti per l'eliminazione	1666
Configurazione del contrassegno automatico degli incidenti da eliminare	1667
Gestione del processo di contrassegno automatico degli incidenti da eliminare	1668
Risoluzione dei problemi relativi al contrassegno automatico degli incidenti da eliminare	1668
Eliminazione dei dashboard e dei report personalizzati	1669
Caratteristiche report incidenti più comuni	1669
Navigazione della pagina dei report incidente	1670
Filtro report incidente e opzioni di riepilogo	1671
Invio dei report degli incidenti tramite e-mail	1672
Stampa di report di incidenti	1673
Scheda della cronologia delle istantanee incidente	1673
Scheda note istantanea incidente	1674
Sezione attributi istantanea incidente	1674
Scheda Correlazioni dell'istantanea incidente	1674
Sezione Politica dell'istantanea incidente	1675
Sezione delle corrispondenze delle istantanee di incidenti	1675

	Sezione Informazioni accesso dell'istantanea incidente	1676
	Personalizzazione della pagina dell'istantanea incidente	1677
	Informazioni sui filtri e sulle opzioni di riepilogo per i report	1677
	Filtri generali per i report	1679
	Opzioni di riepilogo per i report di incidente	1682
	Opzioni di filtro avanzate per i report	1687
Capitolo 52	Come nascondere incidenti	1696
	Informazioni su come nascondere gli incidenti	1696
	Come nascondere gli incidenti	1697
	Visualizzazione di incidenti nascosti	1697
	Come impedire che gli incidenti vengano nascosti	1698
	Eliminazione degli incidenti nascosti	1699
Capitolo 53	Utilizzo di dati di incidente	1700
	Informazioni sugli attributi di stato incidente.	1700
	Configurazione di attributi e valori di stato	1702
	Configurazione di gruppi di stati	1703
	Esporta archivio Web	1704
	Esporta archivio Web - Crea archivio	1705
	Esporta archivio Web - Tutti gli eventi recenti	1706
	Informazioni sugli attributi personalizzati	1706
	Informazioni sull'uso di attributi personalizzati	1708
	Metodi di inserimento di attributi personalizzati	1708
	Configurazione di attributi personalizzati	1709
	Impostazione di attributi personalizzati	1709
	Impostazione manuale dei valori degli attributi personalizzati	1710
Capitolo 54	Utilizzo del rischio dell'utente	1712
	Informazioni sui rischi utente	1712
	Informazioni sulle origini dati dell'utente	1714
	Definizione di attributi personalizzati per i dati utente	1715
	Importazione dei dati dell'utente	1716
	Informazioni sull'identificazione degli utenti in incidenti Web	1721
	Abilitare l'identificazione degli utenti e la configurazione della pianificazione di mapping.	1722
	Controllare dello stato dei controller di dominio	1723
	Visualizzazione dell'elenco utenti	1724
	Visualizzazione dei dettagli dell'utente	1724
	Utilizzo del riepilogo rischi utente	1725

Capitolo 55	Implementazione dei plug-in di ricerca	1727
	Informazioni sui plug-in di ricerca	1727
	Tipi di plug-in di ricerca	1728
	Informazioni sui parametri di ricerca	1731
	Informazioni sulla distribuzione di plug-in	1732
	Informazioni sul concatenamento di plug-in	1732
	Informazioni sull'aggiornamento dei plug-in di ricerca	1733
	Implementazione e test dei plug-in di ricerca	1733
	Gestione e configurazione dei plug-in di ricerca	1735
	Creazione di nuovi plug-in di ricerca	1736
	Selezione dei parametri di ricerca	1737
	Attivazione dei plug-in di ricerca	1742
	Concatenamento dei plug-in di ricerca	1742
	Ricaricamento dei plug-in di ricerca	1743
	Risoluzione dei problemi relativi ai plug-in di ricerca	1743
	Configurazione della registrazione dettagliata per i plug-in di ricerca	1744
	Configurazione di proprietà di plug-in avanzate	1745
	Configurazione del plug-in di ricerca CSV	1747
	Requisiti per la creazione del file CSV	1748
	Definizione del percorso di file CSV	1750
	Scelta del delimitatore di file CSV	1750
	Selezione del set di caratteri per il file CSV	1750
	Mapping di attributi e chiavi di parametro a campi CSV	1750
	Esempio di mapping di attributi CSV	1752
	Test e risoluzione dei problemi del plug-in di ricerca CSV	1753
	Esercitazione del plug-in di ricerca CSV	1754
	Configurazione dei plug-in di ricerca LDAP	1757
	Requisiti per le connessioni del server LDAP	1758
	Mapping degli attributi ai dati LDAP	1758
	Esempi di mapping attributi per LDAP	1759
	Test e risoluzione dei problemi dei plug-in di ricerca LDAP	1760
	Esercitazione del plug-in di ricerca LDAP	1760
	Configurazione dei plug-in di ricerca di script	1762
	Scrittura di script per i plug-in di ricerca script	1763
	Definizione del comando script	1764
	Definizione degli argomenti	1765
	Attivazione delle opzioni stdin e stdout	1765
	Abilitazione del filtraggio del protocollo incidenti per gli script	1766
	Attivazione e crittografia delle credenziali script	1767
	Concatenamento di più plug-in di ricerca script	1769
	Esercitazione del plug-in di ricerca Script	1770

	Script di esempio	1771
	Configurazione dei plug-in di ricerca personalizzati (precedenti) migrati	1773
Sezione 7	Controllo e prevenzione di perdita di dati nella rete	1775
Capitolo 56	Implementazione di Network Monitor	1776
	Implementazione di Network Monitor	1776
	Informazioni sul supporto IP v6 per Network Monitor	1778
	Scelta di un metodo di acquisizione dei pacchetti di rete	1779
	Informazioni sull'installazione e sulla configurazione di software di acquisizione dei pacchetti	1780
	Installazione di WinPcap su una piattaforma Windows	1781
	Aggiornamento del driver delle schede Endace	1781
	Installazione e aggiornamento della scheda di rete e del software del driver Napatech	1781
	Configurazione del server Network Monitor	1787
	Attivazione dell'elaborazione GET con Network Monitor	1789
	Creazione di una politica per Network Monitor	1789
	Test di Network Monitor	1790
Capitolo 57	Implementazione di Network Prevent for Email	1791
	Implementazione di Network Prevent for Email	1791
	Informazioni sull'integrazione di Mail Transfer Agent (MTA)	1793
	Configurazione di Network Prevent for Email Server per modalità di riflessione o inoltro	1793
	Configurazione delle tabelle IP di Linux per reindirizzare il traffico da una porta con restrizioni	1798
	Configurazione di uno o più MTA di upstream	1799
	Creazione di una politica per Network Prevent for Email	1800
	Informazioni sulle intestazioni dei dati relativi alle violazioni delle politiche	1802
	Attivazione delle intestazioni dei dati sulle violazioni della politica	1802
	Test di Network Prevent for Email	1803
Capitolo 58	Implementazione di Network Prevent for Web	1805
	Implementazione di Network Prevent for Web	1805
	Configurazione del server Network Prevent for Web	1807
	Informazioni sulla configurazione di server proxy	1810

	Configurazione di servizi in modalità di richiesta e risposta	1811
	Configurazione di uno o più server proxy	1812
	Attivazione dell'elaborazione GET per Network Prevent for Web	1812
	Creazione di politiche per Network Prevent for Web	1813
	Test di Network Prevent for Web	1815
	Informazioni di risoluzione dei problemi per Network Prevent for Web	
	Server	1815
Sezione 8	Individuazione della posizione di archiviazione dei dati riservati	1817
Capitolo 59	Informazioni su Network Discover	1819
	Informazioni su Network Discover/Cloud Storage Discover	1819
	Funzionamento di Network Discover/Cloud Storage Discover	1821
Capitolo 60	Impostazione e configurazione di Network Discover	1823
	Impostazione e configurazione di Network Discover/Cloud Storage Discover	1823
	Modifica della configurazione del server Network Discover/Cloud Storage Discover	1824
	Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover	1826
	Modifica di un target di Network Discover/Cloud Storage Discover esistente	1828
Capitolo 61	Opzioni di configurazione target di scansione Network Discover	1829
	Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover	1830
	Configurazione dei campi obbligatori per i target di Network Discover	1832
	Pianificazione delle scansioni di Network Discover/Cloud Storage Discover	1833
	Autenticazione tramite password per il contenuto sottoposto a scansione Network Discover	1835
	Gestione delle autorizzazioni di archiviazione cloud	1836
	Fornitura delle credenziali di autorizzazione dell'archiviazione cloud Box	1837
	Password crittografate nei file di configurazione	1840

Impostazione di Network Discover/Cloud Storage Discover filtri per includere o escludere oggetti dalla scansione	1840
Filtraggio dei target di Discover per dimensione dell'oggetto	1843
Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica	1844
Ottimizzazione delle risorse con le opzioni di limitazione delle scansioni di Network Discover/Cloud Storage Discover	1847
Creazione di un inventario delle posizioni di dati riservati non protetti	1849

Capitolo 62

Gestione delle scansioni target di Network Discover	1852
Gestione delle scansioni target di Network Discover/Cloud Storage Discover	1853
Gestione di target Network Discover/Cloud Storage Discover	1853
Informazioni sull'elenco dei target di scansione di Network Discover/Cloud Storage Discover	1854
Utilizzo dei target di scansione di Network Discover/Cloud Storage Discover	1855
Rimozione dei target di scansione di Network Discover/Cloud Storage Discover	1856
Gestione delle cronologie di scansione di Network Discover/Cloud Storage Discover	1856
Informazioni sulle cronologie di scansione Discover e Endpoint Discover	1857
Gestione delle cronologie scansioni di Network Discover/Cloud Storage Discover	1859
Eliminazione delle scansioni di Network Discover/Cloud Storage Discover	1859
Informazioni sui dettagli di scansione di rilevamento	1860
Uso dei dettagli scansione di Network Discover/Cloud Storage Discover	1864
Gestione di server Network Discover/Cloud Storage Discover	1864
Visualizzazione dello stato dei server Network Discover/Cloud Storage Discover	1864
Informazioni sull'ottimizzazione delle scansioni di Network Discover/Cloud Storage Discover	1865
Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali	1868
Informazioni sulle scansioni incrementali	1869
Scansione di elementi nuovi o modificati con scansioni incrementali	1870

Informazioni sulla gestione delle scansioni incrementali	1871
Scansione di elementi nuovi o modificati con scansioni differenziali	1872
Configurazione delle scansioni parallele di target di Network Discover/Cloud Storage Discover	1873
Informazioni sulla scansione della griglia	1874
Configurazione della scansione della griglia	1876
Rinnovo dei certificati di comunicazione griglia per i server di rilevamento Discover	1878
Migrazione di una scansione di rilevamento da un server singolo a una griglia	1880
Linee guida per le prestazioni della scansione della griglia	1881
Risoluzione dei problemi delle scansioni di griglia	1882

Capitolo 63

Utilizzo dei plug-in FlexResponse server per riparare gli incidenti	1885
Informazioni sulla piattaforma FlexResponse server	1885
Utilizzo dei plug-in personalizzati di FlexResponse server per riparare gli incidenti	1887
Distribuzione di un plug-in di FlexResponse server	1888
Aggiunta di un plug-in FlexResponse server al file delle proprietà dei plug-in	1889
Creazione di un file di proprietà per configurare un plug-in di FlexResponse server	1891
Individuazione di incidenti per la riparazione manuale	1894
Utilizzo dell'azione di un plug-in di FlexResponse server per riparare un incidente manualmente	1895
Verifica dei risultati di un'azione di risposta agli incidenti	1896
Risoluzione dei problemi relativi a un plug-in di FlexResponse server	1897

Capitolo 64

Configurazione delle scansioni dell'archiviazione cloud Box utilizzando un server di rilevamento on-site	1899
Configurazione delle scansioni dei target di archiviazione cloud Box utilizzando un server di rilevazione on-site	1899
Configurazione delle scansioni dei target di archiviazione cloud Box	1900
Ottimizzazione della scansione dell'archiviazione cloud di Box	1903
Configurazione delle opzioni di riparazione per target di archiviazione cloud Box	1904

Capitolo 65	Impostazione di scansioni di condivisioni file	1906
	Impostazione delle scansioni di file system	1906
	Target del file system supportati	1907
	Rilevamento automatico di server e condivisioni prima di configurare un target File system	1908
	Utilizzo delle scansioni di enumerazione di radici di contenuti	1909
	Risoluzione dei problemi relativi alle scansioni di enumerazione di radici di contenuti	1913
	Rilevamento automatico di condivisioni file aperte	1914
	Informazioni sul rilevamento automatico dello stato di riparazione incidente	1915
	Risoluzione dei problemi di rilevamento della riparazione automatizzata degli incidenti	1916
	Opzioni di configurazione per il rilevamento automatico della risoluzione degli incidenti	1917
	Esclusione delle cartelle DFS interne	1920
	Configurazione delle scansioni delle cartelle personali di Microsoft Outlook (file .pst)	1921
	Configurazione delle scansioni del file system	1922
	Ottimizzazione della scansione del target del file system	1926
	Configurazione di Network Protect per condivisioni file	1928
Capitolo 66	Impostazione delle scansioni di database Lotus Notes	1931
	Impostazione delle scansioni del server di database di IBM (Lotus) Notes	1931
	Target di IBM (Lotus) Notes supportati	1932
	Configurazione ed esecuzione di scansioni IBM (Lotus) Notes	1932
	Configurazione delle opzioni di scansione della configurazione della modalità IBM (Lotus) Notes DIIOP	1936
Capitolo 67	Impostazione delle scansioni di database SQL	1938
	Impostazione delle scansioni del server di database SQL	1938
	Target di database SQL supportati	1939
	Configurazione ed esecuzione di scansioni database SQL	1940
	Installazione del driver JDBC per target di SQL Database.	1943
	Proprietà di configurazione scansione database SQL	1944

Capitolo 68	Impostazione delle scansioni di server SharePoint	1946
	Impostazione delle scansioni di server SharePoint	1946
	Informazioni sulle scansioni di server SharePoint	1947
	Target del server SharePoint supportati	1949
	Privilegi di accesso per le scansioni SharePoint	1949
	Informazioni sugli insiemi di mapping di accesso alternativo	1949
	Configurazione ed esecuzione delle scansioni dei server SharePoint	1950
	Configurazione Network Protect per i server SharePoint	1956
	Installazione della soluzione SharePoint su front end Web in un gruppo	1958
	Attivazione della scansione SharePoint senza installare la soluzione SharePoint	1960
	Configurazione delle scansioni SharePoint per l'uso dell'autenticazione Kerberos	1961
	Risoluzione dei problemi delle scansioni di SharePoint	1962
Capitolo 69	Impostazione delle scansioni di server Exchange	1965
	Impostazione della scansione di server di repository Exchange	1965
	Informazioni sulle scansioni di server Exchange	1966
	Destinazioni Exchange Server supportate	1967
	Configurazione della scansioni del server Exchange	1968
	Configurazione delle scansioni Exchange per utilizzare l'autenticazione Kerberos	1972
	Configurazioni di esempio e casi di utilizzo per le scansioni Exchange	1974
	Risoluzione dei problemi delle scansioni di Exchange	1975
Capitolo 70	Informazioni sui rilevatori Network Discover	1976
	Configurazione della scansione di server di Microsoft Exchange	1976
	Funzionamento dei rilevatori di Network Discover	1977
	Risoluzione dei problemi dei rilevatori	1978
	Processi del rilevatore	1980
	Struttura delle directory di installazione del rilevatore	1981
	File di configurazione del sistema di scansione	1982
	Opzioni di configurazione del controller del rilevatore	1983

Capitolo 71	Impostazione della scansione di file system	1985
	Impostazione della scansione remota di file system	1986
	Target supportati del rilevatore file system	1987
	Installazione dei rilevatori file system	1988
	Avvio della scansione del file system	1990
	Installazione di rilevatori file system invisibile dalla riga di comando	1992
	Opzioni di configurazione per i rilevatori file system	1992
	Configurazione di esempio per la scansione dell'unità C su un computer Windows	1994
	Configurazione di esempio per la scansione della directory /usr in UNIX	1994
	Esempio di configurazione per la scansione con filtri di inclusione	1994
	Esempio di configurazione per la scansione con filtri di esclusione	1995
	Esempio di configurazione per la scansione con filtri di inclusione e esclusione	1996
	Esempio di configurazione per la scansione con filtri di data	1996
	Esempio di configurazione per la scansione con filtri di dimensione di file	1997
	Esempio di configurazione per le scansioni che ignorano collegamenti simbolici su sistemi UNIX	1997
Capitolo 72	Impostazione della scansione di server Web	1998
	Configurazione di una scansione remota di Web Server	1998
	Target supportati del Web Server (rilevatore)	1999
	Installazione di rilevatori Web Server	2000
	Avvio delle scansioni del server Web	2002
	Opzioni di configurazione per i rilevatori Web Server	2003
	Configurazione di esempio per una scansione del sito Web senza autenticazione	2006
	Esempio di configurazione per la scansione di un sito Web con autenticazione di base	2006
	Configurazione di esempio per una scansione del sito Web con autenticazione basata sulla forma	2006
	Esempio di configurazione per una scansione di siti Web con NTLM	2007
	Esempio di filtraggio di URL per una scansione di siti Web	2007
	Esempio di filtraggio in base alla data per una scansione di siti Web	2008

Capitolo 73	Impostazione della scansione di archivi Documentum	2009
	Configurazione della scansione remota degli archivi Documentum	2009
	Target Documentum (rilevatore) supportati	2010
	Installazione dei rilevatori di Documentum	2010
	Avvio di scansioni Documentum	2013
	Opzioni di configurazione per i rilevatori di Documentum	2014
	Configurazione di esempio per la scansione di tutti i documenti in un archivio Documentum	2016
Capitolo 74	Impostazione della scansione di archivi Livelink	2018
	Configurazione della scansione remota degli archivi OpenText (Livelink)	2018
	Target del rilevatore OpenText (Livelink) supportati	2019
	Creazione di un'origine dati ODBC per SQL Server	2019
	Installazione di rilevatori Livelink	2020
	Avvio delle scansioni di OpenText (Livelink)	2022
	Opzioni di configurazione per rilevatori Livelink	2024
	Configurazione di esempio per la scansione di un database LiveLink	2025
Capitolo 75	Impostazione dei servizi Web per target di scansione personalizzati	2026
	Configurazione dei servizi Web per target di scansione personalizzati	2026
	Informazioni sulla configurazione della lingua di definizione del servizio Web (WSDL)	2027
	Esempio di un client Java di servizi Web	2027
	Codice campione Java per l'esempio di Servizi Web	2029

Sezione 9	Individuazione e prevenzione di perdita di dati su endpoint	2032
Capitolo 76	Panoramica di Symantec Data Loss Prevention per endpoint	2033
	Informazioni sull'individuazione e prevenzione della perdita di dati su endpoint	2033
	Linee guida per la creazione di politiche endpoint	2035
Capitolo 77	Riepilogo di DLP Agent per supporto Mac	2038
	Informazioni sul supporto a livello di funzionalità di DLP Agent	2038
	Installazione dell'agente Mac e dettagli sulle funzionalità degli strumenti	2039
	Supporto di installazione agente Mac	2039
	Funzionalità degli strumenti per endpoint Mac	2040
	Caratteristiche di gestione dell'agente Mac	2040
	Posizione endpoint agente Mac	2041
	Funzionalità gruppi agente Mac	2041
	Panoramica delle tecnologie di rilevamento dell'agente Mac e delle funzionalità di creazione di politiche	2041
	Tecnologie di rilevazione dell'agente Mac	2042
	Funzionalità della regola di risposta della politica dell'agente Mac	2047
	Supporto di monitoraggio dell'agente Mac	2061
	Funzionalità dispositivo di archiviazione rimovibile agente Mac	2049
	Funzionalità degli Appunti supportate su agenti Mac	2051
	Funzionalità e-mail dell'agente Mac	2052
	Funzionalità del browser dell'agente Mac	2053
	Funzionalità Controllo applicazioni dell'agente Mac	2054
	Funzionalità Copia in condivisione di rete per agente Mac	2056
	Filtro dall'agente Mac in base alle funzionalità delle proprietà del file	2056
	Filtro dall'agente Mac in base alle funzionalità delle proprietà del rete	2057
	Caratteristiche delle impostazioni dell'agente avanzate di Endpoint Prevent per l'agente Mac	2057
	Funzionalità dei target Endpoint Discover per Mac	2058
	Supporto Endpoint Discover per file system Mac	2059

Supporto di impostazioni agente avanzate di Endpoint Discover per Mac	2059
--	------

Capitolo 78 Utilizzo di Endpoint Prevent 2060

Informazioni sul monitoraggio di Endpoint Prevent	2060
Informazioni sul monitoraggio di dispositivi di archiviazione rimovibili	2061
Informazioni sul monitoraggio della rete endpoint	2063
Informazioni sul controllo CD/DVD	2064
Informazioni sul monitoraggio di stampa/fax	2065
Informazioni sul monitoraggio della condivisione di rete	2066
Informazioni sul monitoraggio degli Appunti	2067
Informazioni sul controllo applicazioni	2067
Informazioni sul controllo applicazioni dell'archiviazione cloud	2068
Informazioni sul supporto del desktop virtuale con Endpoint Prevent	2069
Informazioni sulla RRC	2072
Informazione sulla creazione di politiche per Endpoint Prevent	2073
Informazioni sul monitoraggio di politiche con regole di risposta per Endpoint Server	2073
Come implementare Endpoint Prevent	2076
Configurazione della posizione dell'endpoint	2076
Informazioni sulle regole di risposta di Endpoint Prevent con impostazioni locali differenti	2078

Capitolo 79 Utilizzo di Endpoint Discover 2080

Funzionamento di Endpoint Discover	2080
Informazioni sulla scansione di Endpoint Discover	2080
Informazioni sulla scansione degli endpoint target	2081
Informazioni sulla scansione completa di Endpoint Discover	2082
Informazioni sulla scansione incrementale di Endpoint Discover	2082
Informazioni sulle scansioni parallele negli endpoint target	2084
Ottimizzazione della scansione per le prestazioni dell'endpoint	2085
Preparazione dell'impostazione di Endpoint Discover	2086
Creazione di un gruppo di politiche per Endpoint Discover	2086
Creazione di una politica per Endpoint Discover	2087
Aggiunta di una regola per Endpoint Discover	2088
Impostazione e configurazione di Endpoint Discover	2089
Creazione di una scansione Endpoint Discover	2089

Creazione di un nuovo target Endpoint Discover	2091
Informazioni sui filtri di Endpoint Discover	2096
Configurazione delle impostazioni timeout scansione di Endpoint Discover	2104
Gestione delle scansioni target Endpoint Discover	2105
Informazioni sulla gestione delle scansioni Endpoint Discover	2105
Informazioni sui dettagli della scansione Endpoint Discover di endpoint target	2106
Informazioni sulla risoluzione degli incidenti Endpoint Discover	2108
Informazioni sui report endpoint	2108

Capitolo 80 Utilizzo delle configurazioni agente 2110

Informazioni sulle configurazioni dell'agente	2110
Informazioni sulla clonazione delle configurazioni agente	2111
Aggiunta e modifica di configurazioni agente	2111
Impostazioni di canale	2112
Impostazioni di Filtri canale	2115
Impostazioni di Device Control	2125
Impostazioni dell'agente	2126
Impostazioni agente avanzate	2133
Impostazione di canali specifici da monitorare in base alla posizione dell'endpoint	2179
Applicazione di configurazioni agente a un gruppo di agenti	2179
Configurazione dello stato di connessione dell'agente	2180

Capitolo 81 Utilizzo di gruppi di agenti 2181

Informazioni sui gruppi di agenti	2181
Sviluppo di una strategia per distribuire gruppi di agenti	2182
Panoramica del processo di distribuzione del gruppo di agenti	2183
Creazione e gestione degli attributi dell'agente	2184
Creazione di un nuovo attributo dell'agente	2185
Definizione di un filtro di ricerca per la creazione di attributi definiti dall'utente	2186
Verifica le ricerche dell'attributo con lo strumento Attribute Query Resolver	2187
Applicazione di un attributo nuovo o modificato agli agenti	2188
Annullare le modifiche apportate agli attributi dell'agente	2188
Modifica degli attributi agente definiti dall'utente	2188
Visualizzazione e gestione dei gruppi di agenti	2189
Condizioni gruppo di agenti	2190

	Creazione di un nuovo gruppo di agenti	2190
	Aggiornamento delle configurazioni obsolete dell'agente	2191
	Assegnazione delle configurazioni per distribuire i gruppi	2192
	Verificare che le assegnazioni dei gruppi siano corrette	2192
	Visualizzazione dei conflitti di gruppo	2192
	Modifica dei gruppi	2193
Capitolo 82	Gestione di Symantec DLP Agent	2194
	Informazioni sull'amministrazione di Symantec DLP Agent	2194
	Schermata Panoramica agente	2195
	Informazioni sugli eventi di agente	2214
	Informazioni sulla rimozione di Symantec DLP Agent	2222
	Informazioni sui registri DLP Agent	2226
	Impostazione dei livelli di registro per un agente di endpoint	2226
	Informazioni sulla gestione delle password dell'agente	2227
	Creazione di una nuova password di disinstallazione dell'agente o degli strumenti di Endpoint	2228
	Modifica della password esistente di disinstallazione dell'agente o degli strumenti di Endpoint	2229
	Conservazione delle password esistenti di disinstallazione dell'agente o degli strumenti di Endpoint	2229
Capitolo 83	Utilizzo del controllo applicazioni	2231
	Informazioni sul controllo delle applicazioni	2231
	Modifica delle impostazioni di controllo delle applicazioni	2232
	Controllo delle applicazioni di messaggistica istantanea su endpoint Mac	2235
	Elenco delle applicazioni CD/DVD	2235
	Informazioni sull'aggiunta di applicazioni	2236
	Aggiunta di un'applicazione Windows	2237
	Utilizzo dello strumento GetApplInfo	2240
	Aggiunta di un'applicazione macOS	2241
	Definizione dei nomi binari delle applicazioni macOS	2244
	Come ignorare applicazioni macOS	2245
	Informazioni sul monitoraggio Accesso ai file di applicazione	2245
	Implementazione del monitoraggio Accesso ai file di applicazione	2246
Capitolo 84	Utilizzo di Endpoint FlexResponse	2248
	Informazioni su Endpoint FlexResponse	2248
	Distribuzione di Endpoint FlexResponse	2250

	Informazioni sulla distribuzione di plug-in Endpoint FlexResponse agli endpoint	2251
	Distribuzione dei plug-in di Endpoint FlexResponse con una procedura di installazione invisibile	2252
	Informazioni sull'utilità Endpoint FlexResponse	2252
	Distribuzione del plug-in Endpoint FlexResponse mediante l'utilità Endpoint FlexResponse	2254
	Attivazione di Endpoint FlexResponse su Enforce Server	2255
	Disinstallazione di un plug-in Endpoint FlexResponse mediante l'utilità Endpoint FlexResponse	2256
	Recupero di un plug-in Endpoint FlexResponse da un endpoint specifico	2256
	Recupero di un elenco di plug-in di Endpoint FlexResponse da un endpoint	2257
Capitolo 85	Utilizzo degli strumenti Endpoint	2259
	Informazioni sugli strumenti di endpoint	2259
	Utilizzo di strumenti endpoint con Windows 7/8.1/10	2261
	Arresto dell'agente e dei servizi watchdog su endpoint Windows	2261
	Utilizzo degli strumenti Endpoint con macOS	2262
	Interruzione del servizio dell'agente degli endpoint Mac	2262
	Ispezione dei file di database utilizzati dall'agente	2263
	Visualizzazione dei file di registro estesi	2265
	Informazioni sulle utilità ID periferica	2266
	Avvio dei DLP Agent eseguiti negli endpoint Mac	2270
Sezione 10	Monitoraggio della perdita di dati in applicazioni cloud	2271
Capitolo 86	Utilizzo con Rilevamento applicazioni	2272
	Informazioni su Rilevamento applicazioni	2272
	Gestione di Rilevamento applicazioni	2273
Capitolo 87	Utilizzo con Cloud Service for Email	2279
	Informazioni su Cloud Service for Email	2279
	Aggiornamento di domini di posta nella console di amministrazione di Enforce Server	2280
	Informazioni sull'aggiornamento di domini di posta nella console di amministrazione di Enforce Server	2280

Crittografia delle e-mail cloud con Symantec Information Centric	
Encryption	2282
Implementazione di ICE con Cloud Service for Email	2283
Configurazione di Enforce Server per comunicare con il servizio	
ICE	2284
Creazione di regole di risposta per la crittografia ICE	2285
Informazioni sulla decrittografia di e-mail con crittografia	
ICE	2287
Visualizzazione dei dettagli sugli incidenti ICE	2287

Sezione 11 Monitoraggio della perdita di dati mediante dispositivi DLP 2291

Capitolo 88 Implementazione e utilizzo di dispositivi DLP	2292
Informazioni sui dispositivi DLP	2292
Informazioni su come ottenere i file e le licenze di attivazione del	
dispositivo	2293
Acquisizione dei file di attivazione e di licenza per il dispositivo	
virtuale	2293
Acquisizione dei file di licenza per il dispositivo hardware DLP	
S500-10	2295
Informazioni sull'interfaccia da riga di comando (CLI)	2296
Informazioni su ottimizzazione delle prestazioni e dimensionamento	
per i dispositivi	2296

Capitolo 89 Distribuzione dei dispositivi DLP	2297
Panoramica della distribuzione per il dispositivo virtuale	2297
Configurazione del dispositivo virtuale	2299
Panoramica della distribuzione per il dispositivo hardware	
DLP-S500	2302
Configurazione del dispositivo DLP-S500	2303
Aggiunta di un dispositivo	2305
Configurare il dispositivo Rilevamento API per le app degli	
sviluppatori	2306

Capitolo 90 Attività di post-distribuzione	2307
Dissociazione o reimpostazione di un dispositivo DLP	2307
Aggiornamento del software del dispositivo	2308
File di registro e registrazione per i dispositivi	2310

Indice 2311

Guida introduttiva

- [Capitolo 1. Introduzione a Symantec Data Loss Prevention](#)
- [Capitolo 2. Guida introduttiva all'amministrazione di Symantec Data Loss Prevention](#)
- [Capitolo 3. Utilizzo di lingue e impostazioni internazionali](#)

Introduzione a Symantec Data Loss Prevention

Il capitolo contiene i seguenti argomenti:

- Informazioni sugli aggiornamenti al Manuale dell'amministratore di Symantec Data Loss Prevention
- Informazioni su Symantec Data Loss Prevention
- Informazioni sulla piattaforma Enforce
- Informazioni su Network Monitor e Prevent
- Informazioni su Network Discover/Cloud Storage Discover
- Informazioni su Network Protect
- Informazioni su Endpoint Discover
- Informazioni su Endpoint Prevent

Informazioni sugli aggiornamenti al *Manuale dell'amministratore di Symantec Data Loss Prevention*

Questa guida viene aggiornata occasionalmente man mano che nuove informazioni diventano disponibili. È possibile trovare l'ultima versione del *Manuale dell'amministratore di Symantec Data Loss Prevention* al seguente collegamento del centro di supporto Symantec:

<http://www.symantec.com/docs/DOC9261>.

Iscriverti all'articolo del centro di supporto per ricevere notifiche quando sono disponibili aggiornamenti.

La seguente tabella fornisce la cronologia degli aggiornamenti a questa versione del *Manuale dell'amministratore di Symantec Data Loss Prevention*:

Tabella 1-1 Cronologia delle modifiche al *Manuale dell'amministratore di Symantec Data Loss Prevention*

Data	Descrizione
11 luglio 2018	Dettagli aggiornati sull'aggiunta di identità utente che le applicazioni di archiviazione cloud devono ignorare. Corretto ortografia dello strumento <code>start_agent</code> . Corretta la posizione dello strumento <code>uninstall_agent</code> per endpoint macOS. Corretti i percorsi del file di registro per sistemi Microsoft Windows. Dettagli aggiornati per la crittografia delle e-mail cloud con Symantec ICE.

Informazioni su Symantec Data Loss Prevention

Symantec Data Loss Prevention consente di:

- Rilevare e individuare informazioni confidenziali nel repository di archiviazione cloud, in file e Web server, nei database, sui dispositivi mobili e negli endpoint (laptop e desktop)
- Proteggere le informazioni confidenziali tramite quarantena
- Monitorare il traffico di rete per la trasmissione dei dati confidenziali
- Monitorare l'uso di dati sensibili su endpoint
- Impedire la trasmissione di dati confidenziali a posizioni esterne
- Applicare automaticamente le politiche di protezione dei dati e della crittografia

Symantec Data Loss Prevention comprende i seguenti componenti:

- Enforce Server
Vedere ["Informazioni sulla piattaforma Enforce"](#) a pagina 75.
Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.
Vedere ["Informazioni sulla console di amministrazione di Enforce Server"](#) a pagina 81.
- Network Discover/Cloud Storage Discover
Vedere ["Informazioni su Network Discover/Cloud Storage Discover"](#) a pagina 77.
- Network Protect
Vedere ["Informazioni su Network Protect"](#) a pagina 77.
- Network Monitor
Vedere ["Informazioni su Network Monitor e Prevent"](#) a pagina 76.
- Network Prevent
Vedere ["Informazioni su Network Monitor e Prevent"](#) a pagina 76.

- Endpoint Discover
 Vedere ["Informazioni su Endpoint Discover"](#) a pagina 78.
- Endpoint Prevent
 Vedere ["Informazioni su Endpoint Prevent"](#) a pagina 78.

I moduli Discover, Protect, Monitor e Prevent possono essere usati da soli o in combinazione. Indipendentemente da quali prodotti autonomi vengano utilizzati, Enforce Server viene sempre fornito per la gestione centrale. Tenere presente che il modulo Network Protect richiede il modulo Network Discover/Cloud Storage Discover.

A ciascun modulo di prodotto sono associati server di rilevamento e rilevatori di cloud corrispondenti:

- Il server Network Discover/Cloud Storage Discover individua i dati confidenziali esposti su una vasta gamma di archivi di dati aziendali, compresi:
 - Archiviazione cloud Box
 - File server
 - Database
 - Microsoft SharePoint
 - IBM Lotus Notes
 - EMC Documentum
 - LiveLink
 - Microsoft Exchange
 - Server Web
 - Altri archivi di dati

Se si dispone di una licenza a per Network Protect, questo server è anche in grado di copiare e mettere in quarantena i dati sensibili sui file server e nell'archiviazione cloud Box, come specificato nelle politiche.

Vedere ["Informazioni su Network Discover/Cloud Storage Discover"](#) a pagina 77.

- Il server Network Monitor monitora il traffico sulla rete.
 Vedere ["Informazioni su Network Monitor e Prevent"](#) a pagina 76.
- Il server Network Prevent for Email blocca le e-mail che contengono dati sensibili.
 Vedere ["Informazioni su Network Monitor e Prevent"](#) a pagina 76.
- Il server Network Prevent for Web blocca gli invii HTTP e i trasferimenti FTP che contengono dati sensibili.
 Vedere ["Informazioni su Network Monitor e Prevent"](#) a pagina 76.
- L'Endpoint Server monitora e impedisce l'uso improprio dei dati confidenziali sugli endpoint.

Vedere ["Informazioni su Endpoint Discover"](#) a pagina 78.

Vedere ["Informazioni su Endpoint Prevent"](#) a pagina 78.

L'architettura distribuita di Symantec Data Loss Prevention consente alle organizzazioni di:

- Eseguire gestione e reporting centralizzati.
- Gestire centralmente le politiche di sicurezza dei dati una volta e distribuirle immediatamente nell'intera suite Symantec Data Loss Prevention.
- Adeguare la prevenzione della perdita di dati in relazione alla dimensione dell'organizzazione.

Informazioni sulla piattaforma Enforce

Symantec Data Loss Prevention Enforce Server è la piattaforma di gestione centrale che consente di definire, distribuire e applicare politiche di sicurezza e di prevenzione delle perdite di dati. La console di amministrazione di Enforce Server fornisce un'interfaccia centralizzata basata sul Web per distribuire i server di rilevamento, creare le politiche, riparare gli incidenti e gestire il sistema.

Vedere ["Informazioni su Symantec Data Loss Prevention"](#) a pagina 73.

La piattaforma Enforce fornisce le seguenti funzionalità:

- Creare e distribuire politiche accurate di prevenzione delle perdite di dati. È possibile scegliere tra varie tecnologie di rilevamento, definire le regole e specificare le azioni da includere nelle politiche di prevenzione della perdita di dati. Utilizzando i modelli di politica normativi e di best practice forniti, è possibile soddisfare i requisiti di conformità normativa, protezione dei dati e uso accettabile e risolvere minacce per la sicurezza specifiche.

Vedere ["Informazioni sulle politiche di Data Loss Prevention"](#) a pagina 373.

Vedere ["Rilevamento della perdita di dati"](#) a pagina 387.

- Distribuire e imporre automaticamente politiche di prevenzione della perdita di dati. È possibile automatizzare le opzioni di imposizione delle politiche per la notifica, il flusso di lavoro di riparazione, il blocco e la crittografia.
- Misurare la riduzione di rischio e dimostrare la conformità. Le funzionalità di reporting di Enforce Server consentono di creare report operativi che individuano l'andamento della riduzione del rischio nel tempo. È anche possibile creare report di conformità per soddisfare i requisiti normativi di conformità.

Vedere ["Informazioni sui report Symantec Data Loss Prevention"](#) a pagina 1632.

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

- Consentire una riparazione rapida. In base alla gravità dell'incidente, è possibile automatizzare l'intero processo di riparazione utilizzando il reporting dettagliato degli incidenti e l'automazione del flusso di lavoro. I controlli degli accessi basati su ruolo

consentono alle singoli unità e reparti aziendali di esaminare e risolvere gli incidenti pertinenti alle loro attività o ai loro impiegati.

Vedere ["Informazioni sulla riparazione degli incidenti"](#) a pagina 1570.

Vedere ["Risoluzione di incidenti"](#) a pagina 1573.

- Salvaguardare la privacy dei dipendenti. È possibile utilizzare Enforce Server per esaminare gli incidenti senza rivelare l'identità del mittente o il contenuto di messaggio. In questo modo, le società multinazionali possono soddisfare i requisiti legali sul monitoraggio dei dipendenti dell'Unione Europea e sul trasferimento dei dati personali oltre i confini nazionali. Vedere ["Informazioni sul controllo degli accessi basato sul ruolo"](#) a pagina 109.

Informazioni su Network Monitor e Prevent

I prodotti di prevenzione e monitoraggio dei dati di rete Symantec Data Loss Prevention comprendono:

- **Network Monitor**
 Network Monitor acquisisce e analizza il traffico sulla rete. Rileva dati riservati e metadati di traffico significativi sui protocolli specificati. Ad esempio, SMTP, FTP, HTTP e diversi protocolli di messaggistica istantanea. È possibile configurare un server Network Monitor per monitorare i protocolli personalizzati e utilizzare diversi filtri (per protocollo) per filtrare il traffico a basso rischio.
- **Network Prevent for Email**
 Network Prevent for Email si integra con gli MTA standard e i servizi e-mail ospitati per fornire gestione di posta SMTP attiva in linea. Le politiche distribuite su Network Prevent for Email Server in linea indirizzano il server di posta hop successivo per bloccare, reindirizzare o assegnare tag a messaggi e-mail. Questi blocchi sono basati su contenuti specifici e altri attributi di messaggi. La comunicazione tra MTA e Network Prevent for Email Server può essere protetta, se necessario, tramite TLS.
 Implementare Network Monitor, esaminare gli incidenti acquisiti e affinare le politiche di conseguenza, prima di implementare Network Prevent for Email.
 Consultare la *Guida all'integrazione di Symantec Data Loss Prevention MTA per Network Prevent for Email*.
- **Network Prevent for Web**
 Per la gestione delle richieste Web attive in linea, Network Prevent for Web si integra con un server proxy FTP, HTTP o HTTPS. Questa integrazione utilizza Internet Content Adaptation Protocol (ICAP). Network Prevent for Web Server rileva i dati riservati in contenuti HTTP, HTTPS o FTP. In questo caso, provoca il rifiuto delle richieste da parte del proxy o rimuove il contenuto HTML, come specificato dalle politiche responsabili.

Informazioni su Network Discover/Cloud Storage Discover

Network Discover/Cloud Storage Discover esegue la scansione ad alta velocità di repository di archiviazione cloud, condivisioni di file in rete, server di contenuto Web, database, archivi di documenti e sistemi endpoint per rilevare i dati e i documenti a rischio. Network Discover/Cloud Storage Discover consente alle società di comprendere esattamente dove i dati riservati sono a rischio e di ridurre significativamente le perdite di dati.

Network Discover/Cloud Storage Discover consente alle organizzazioni di:

- Evidenziare i dati riservati non protetti. Network Discover/Cloud Storage Discover rende possibile l'individuazione accurata dei dati a rischio presenti nelle reti aziendali. Sarà quindi poi possibile informare i proprietari di file server condivisi affinché proteggano i dati.
- Ridurre la proliferazione di dati riservati. Network Discover/Cloud Storage Discover consente di rilevare la diffusione delle informazioni riservate in tutta la società e riduce il rischio di perdite di dati.
- Automatizzare analisi e verifiche. Network Discover/Cloud Storage Discover semplifica le analisi di sicurezza dei dati e le verifiche di conformità. Consente in effetti agli utenti di eseguire automaticamente la scansione di dati riservati, come pure verificare le politiche di controllo degli accessi e di crittografia.
- Durante la riparazione degli incidenti, Veritas Data Insight consente alle organizzazioni di risolvere il problema dell'identificazione di proprietari di dati e parti responsabili delle informazioni a causa di metadati o informazioni di tracciatura incompleti o imprecisi. Vedere la *Guida all'implementazione di Symantec Data Loss Prevention Data Insight*.
- Per fornire ulteriore flessibilità nella riparazione degli incidenti di Network Discover/Cloud Storage Discover, utilizzare i plug-in o l'API FlexResponse disponibili. Consultare il *Manuale per sviluppatori della piattaforma FlexResponse di Symantec Data Loss Prevention*, o contattare i servizi professionali Symantec per un elenco dei plug-in.

Vedere ["Informazioni su Symantec Data Loss Prevention"](#) a pagina 73.

Informazioni su Network Protect

Network Protect riduce i rischi rimuovendo dati riservati esposti, proprietà intellettuale e informazioni classificate da condivisioni di file aperte su server di rete o computer desktop. Non esiste un server Network Protect distinto; il modulo del prodotto Network Protect aggiunge funzionalità di protezione al server Network Discover.

Network Protect consente alle organizzazioni di:

- Applicare tag visivi al contenuto nell'archiviazione cloud Box. Network Protect può applicare un tag di testo ai file che violano le politiche contenuti nell'archiviazione cloud Box.

- Mettere in quarantena file esposti. Network Protect può spostare automaticamente i file che violano le politiche in un'area di quarantena che ricrea la struttura dei file di origine per un agevole reperimento degli stessi. Facoltativamente, Symantec Data Loss Prevention può collocare un file di testo marker nella posizione originale del file con la violazione. Il file marker può indicare dove e perché il file originale è stato messo in quarantena.
- Copiare file esposti o sospetti. Network Protect può copiare automaticamente i file che violano le politiche in un'area di quarantena. L'area di quarantena può ricreare la struttura dei file di origine per un agevole reperimento degli stessi, e lasciare il file originale dove si trova.
- Ripristinare file di quarantena. Network Protect può ripristinare facilmente i file in quarantena nella posizione originale o in una nuova posizione.
- Applicare politiche di controllo degli accessi e di crittografia. Network Protect assicura dinamicamente la conformità della forza lavoro alle politiche di crittografia e controllo degli accessi.

Vedere ["Informazioni su Symantec Data Loss Prevention"](#) a pagina 73.

Vedere ["Configurazione di Network Protect per condivisioni file"](#) a pagina 1928.

Informazioni su Endpoint Discover

Endpoint Discover rileva dati riservati su endpoint desktop o laptop. Consiste di almeno un Endpoint Server e almeno un Symantec DLP Agent eseguito su un endpoint. È possibile avere molti Symantec DLP Agent connessi a un singolo Endpoint Server. Mediante i Symantec DLP Agent è possibile:

- Rilevare dati riservati nel file system endpoint.
- Raccogliere dati su quell'attività.
- Inviare incidenti all'Endpoint Server.
- Inviare dati all'Endpoint Server associato per l'analisi, se necessario.

Vedere ["Informazioni su Endpoint Prevent"](#) a pagina 78.

Vedere ["Informazioni su Symantec Data Loss Prevention"](#) a pagina 73.

Informazioni su Endpoint Prevent

Endpoint Prevent rileva i dati riservati e ne impedisce il trasferimento da computer endpoint desktop o portatili. Include almeno un Endpoint Server e tutti i Symantec DLP Agent in esecuzione sui sistemi endpoint a cui è connesso. È possibile avere molti Symantec DLP Agent connessi a un singolo Endpoint Server. Endpoint Prevent esegue il rilevamento sui seguenti trasferimenti di dati:

- Controllo delle applicazioni
- CD/DVD
- Appunti
- E-mail/SMTP
- Unità rimovibili eSATA
- FTP
- HTTP/HTTPS
- IM
- Condivisioni di rete
- Stampa/Fax
- Dispositivi rimovibili USB

Vedere ["Informazioni su Endpoint Discover"](#) a pagina 78.

Vedere ["Informazioni su Symantec Data Loss Prevention"](#) a pagina 73.

Guida introduttiva all'amministrazione di Symantec Data Loss Prevention

Il capitolo contiene i seguenti argomenti:

- [Informazioni sull'amministrazione di Symantec Data Loss Prevention](#)
- [Informazioni sulla console di amministrazione di Enforce Server](#)
- [Accesso e disconnessione dalla console di amministrazione di Enforce Server](#)
- [Informazioni sull'account di amministrazione](#)
- [Esecuzione di attività di configurazione iniziale](#)
- [Modifica della password di amministratore](#)
- [Aggiunta di un account e-mail amministratore](#)
- [Modifica di un profilo utente](#)
- [Modifica della password](#)

Informazioni sull'amministrazione di Symantec Data Loss Prevention

Il sistema Symantec Data Loss Prevention è composto da un Enforce Server e uno o più server di rilevamento.

Enforce Server archivia tutte le configurazioni di sistema, le politiche, i report salvati, le altre informazioni di Symantec Data Loss Prevention e gestisce tutte le attività.

L'amministrazione del sistema viene eseguita dalla console di amministrazione dell'Enforce Server alla quale è possibile accedere tramite i browser Web Firefox o Internet Explorer. La console Enforce verrà visualizzata dopo l'accesso.

Vedere ["Informazioni sulla console di amministrazione di Enforce Server"](#) a pagina 81.

Dopo il completamento della procedura di installazione nella *Guida di installazione di Symantec Data Loss Prevention*, è necessario eseguire le attività di configurazione iniziale di Symantec Data Loss Prevention. Queste sono attività essenziali che è necessario eseguire prima che il sistema possa cominciare a monitorare i dati sulla rete.

Vedere ["Esecuzione di attività di configurazione iniziale"](#) a pagina 83.

Informazioni sulla console di amministrazione di Enforce Server

Amministrare il sistema Symantec Data Loss Prevention tramite la console di amministrazione Enforce Server.

L'utente Amministratore può visualizzare e accedere a tutte le parti della console di amministrazione. Altri utenti possono visualizzare solo le parti a cui i relativi ruoli garantiscono l'accesso. L'account utente con cui è stato effettuato l'accesso viene visualizzato nella parte superiore destra dello schermo.



Al primo accesso alla console di amministrazione, viene visualizzata la pagina **principale** predefinita. Tutti gli utenti possono modificare la pagina **principale** predefinita tramite il pulsante di selezione relativo.





Vedere [Tabella 2-1](#) a pagina 81.

Per navigare nel sistema, selezionare gli elementi da uno dei quattro cluster menu (**Pagina iniziale**, **Incidenti**, **Gestisci** e **Sistema**).

Nella porzione superiore destra della console di amministrazione sono presenti le seguenti icone di operazione e navigazione:

Tabella 2-1 Icone di operazione e navigazione della console di amministrazione

Icona	Descrizione
	Guida. Fare clic su questa icona per accedere alla guida in linea sensibile al contesto per la pagina corrente.
	Selezionare questa pagina come pagina iniziale . Se lo schermo corrente non può essere selezionato come pagina iniziale , questa icona non è disponibile.

Icona	Descrizione
	Tornare alla schermata precedente. Symantec consiglia di utilizzare tale pulsante Indietro invece del pulsante Indietro del browser. L'utilizzo del pulsante Indietro del browser può portare a un comportamento imprevisto e non è consigliato.
	Aggiornare la schermata. Symantec consiglia di utilizzare tale pulsante Aggiorna invece del pulsante Ricarica o Aggiorna . L'utilizzo dei pulsanti del browser può portare a un comportamento imprevisto e non è consigliato.
	Stampare il report corrente. Se i contenuti dello schermo corrente non possono essere inviati alla stampante, questa icona non è disponibile.
	Inviare per e-mail il report corrente a uno o più destinatari. Se i contenuti dello schermo corrente non possono essere inviati come e-mail, questa icona non è disponibile.

Vedere ["Accesso e disconnessione dalla console di amministrazione di Enforce Server"](#) a pagina 82.

Accesso e disconnessione dalla console di amministrazione di Enforce Server

Se è stato assegnato più di un ruolo, è possibile accedere solo con un ruolo alla volta. È necessario specificare il nome del ruolo e il nome utente all'accesso.

Come accedere a Enforce Server

- 1 Nell'host di Enforce Server, aprire un browser e puntarlo all'URL del server (come indicato dall'amministratore di Symantec Data Loss Prevention).
- 2 Nella schermata di accesso di Symantec Data Loss Prevention, immettere il nome utente nel campo **Nome utente**. Per il ruolo di amministratore, il nome utente è sempre `Administrator`. Gli utenti con più ruoli devono specificare il nome del ruolo e il nome utente nel formato `role\user` (ad esempio, `ReportViewer\bsmith`). Se non è così, Symantec Data Loss Prevention assegna all'utente un ruolo al momento dell'accesso.

Vedere ["Ruoli di configurazione"](#) a pagina 114.

- 3 Nel campo **Password**, digitare la password. Per l'amministratore al primo accesso, questa password è quella creata durante l'installazione.

Per i dettagli dell'installazione, consultare il *Manuale di installazione di Symantec Data Loss Prevention*.

- 4 Fare clic sul pulsante di **accesso**.

Viene visualizzata la console di amministrazione di Enforce Server. L'amministratore può accedere a tutte le parti della console di amministrazione, ma un altro utente può visualizzare solo le parti autorizzate per quel ruolo particolare.

Per disconnettersi da Enforce Server

- 1 Fare clic sul pulsante di **disconnessione** nella parte superiore destra dello schermo.
- 2 Fare clic su **OK** per confermare.

Symantec Data Loss Prevention visualizza un messaggio che conferma la corretta disconnessione.

Vedere ["Modifica di un profilo utente"](#) a pagina 85.

Informazioni sull'account di amministrazione

Il sistema Symantec Data Loss Prevention è preconfigurato con un account amministratore permanente. Tenere presente che il nome distingue maiuscole e minuscole e non può essere modificato. Durante l'installazione si è configurata una password per l'account di amministratore.

Per ulteriori informazioni, consultare il *Manuale di installazione di Symantec Data Loss Prevention*.

Soltanto l'amministratore può visualizzare o modificare l'account di amministratore. Le opzioni di ruolo non vengono visualizzate nella schermata di **configurazione dell'amministratore**, perché l'amministratore ha sempre accesso a ogni parte del sistema.

Vedere ["Modifica della password di amministratore"](#) a pagina 84.

Vedere ["Aggiunta di un account e-mail amministratore"](#) a pagina 85.

Esecuzione di attività di configurazione iniziale

Dopo il completamento della procedura di installazione nella *Guida di installazione di Symantec Data Loss Prevention*, è necessario eseguire le attività di configurazione iniziale di Symantec Data Loss Prevention. Queste sono attività essenziali che è necessario eseguire prima che il sistema possa cominciare a monitorare i dati sulla rete.

- Modificare la password dell'amministratore in una password univoca che nessun altro conosce e aggiungere un indirizzo e-mail per l'account utente dell'amministratore in modo da ricevere notifiche su vari eventi di sistema.
Vedere ["Informazioni sull'account di amministrazione"](#) a pagina 83.
- Aggiungere e configurare i server di rilevamento.
Vedere ["Aggiunta di un server di rilevazione"](#) a pagina 268.
Vedere ["Configurazione di base di server"](#) a pagina 244.
- Aggiungere tutti gli account utente necessari oltre a quelli forniti dal pacchetto di soluzioni di Symantec Data Loss Prevention.
- Esaminare i modelli di politica forniti con il pacchetto di soluzioni di Symantec Data Loss Prevention per conoscerne il contenuto e i requisiti di dati. Modificare le politiche o crearne di nuove come necessario.
- Aggiungere i profili di dati che si intende associare alle politiche.
I profili di dati non sono sempre richiesti. Questa fase è necessaria solo se si ha una licenza per i profili di dati e si intende utilizzarli nelle politiche.

Modifica della password di amministratore

Durante l'installazione, è stata creata una password di amministratore generica. Quando si accede per la prima volta, è necessario modificare la password con una password segreta e univoca.

Per ulteriori informazioni, consultare il *Manuale di installazione di Symantec Data Loss Prevention*.

Le password fanno distinzione tra maiuscole e minuscole e devono contenere almeno otto caratteri.

Notare che è possibile configurare Symantec Data Loss Prevention in modo da richiedere password efficaci. Le password efficaci sono password progettate specificamente per essere difficili da identificare. La politica di password viene configurata dalla schermata **Sistema > Impostazioni > Generale > Configura**.

Quando la password scade, Symantec Data Loss Prevention visualizza la finestra di rinnovo password all'accesso successivo. Quando viene visualizzata la finestra di rinnovo password, digitare la vecchia password, quindi digitare quella nuova e confermarla.

Vedere ["Configurazione degli account utente"](#) a pagina 123.

Per modificare la password di amministratore

- 1 Accedere come amministratore.
- 2 Fare clic su **Profilo** nell'angolo superiore destro della console di amministrazione.
- 3 Nella schermata **Modifica profilo** :

- Digitare la nuova password nel campo **Nuova password**.
- Ridigitare la nuova password nel campo **Immettere di nuovo la nuova password**.
Le due nuove password devono essere uguali.

Notare che le password fanno distinzione tra maiuscole e minuscole.

4 Fare clic su **Salva**.

Vedere ["Informazioni sull'account di amministrazione"](#) a pagina 83.

Vedere ["Informazioni sulla console di amministrazione di Enforce Server"](#) a pagina 81.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Aggiunta di un account e-mail amministratore

È possibile specificare un indirizzo e-mail per ricevere messaggi relativi all'account amministratore.

Per aggiungere o modificare un account e-mail amministratore

- 1** Fare clic su **Profilo** nell'angolo superiore destro della console di amministrazione.
- 2** Digitare l'indirizzo e-mail amministratore nuovo (o modificato) nel campo **Indirizzo e-mail**.

Gli indirizzi e-mail devono includere un nome di dominio completo. Ad esempio:

`my_name@acme.com`.

3 Fare clic su **Salva**.

Vedere ["Informazioni sull'account di amministrazione"](#) a pagina 83.

Vedere ["Informazioni sulla console di amministrazione di Enforce Server"](#) a pagina 81.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Modifica di un profilo utente

Gli utenti del sistema possono utilizzare la schermata **Profilo** per configurare i loro indirizzi e-mail, password e lingue.

Nella schermata **Profilo** gli utenti possono anche specificare le preferenze relative ai report.

Per visualizzare la schermata **Profilo**, fare clic sull'elenco a discesa nella parte destra della console di amministrazione di Enforce Server, quindi selezionare **Profilo**.

La schermata **Profilo** include le seguenti sezioni:

- **Autenticazione**. Usare questa sezione per cambiare la propria password o selezionare l'autenticazione del certificato, se disponibile.

- **Generale.** Usare questa sezione per specificare il proprio indirizzo e-mail, scegliere una lingua e visualizzare l'home page selezionata.
- **Preferenze report.** Usare questa sezione per specificare la codifica di testo, il delimitatore CSV e le preferenze di esportazione XML.
- **Ruoli.** Questa sezione visualizza il proprio ruolo. Da notare che questa sezione non viene visualizzata per l'amministratore perché l'amministratore è autorizzato a eseguire tutti i ruoli.

Sezione Autenticazione

Per cambiare la password

- 1 Digitare la nuova password nel campo **Nuova password**.
- 2 Ridigitare la nuova password nel campo **Immettere di nuovo la nuova password**.
- 3 Fare clic su **Salva**.

Per usare l'autenticazione del certificato

- 1 Se l'autenticazione del certificato è disponibile, selezionare **Usa autenticazione del certificato**.
- 2 Immettere il nome comune (CN) LDAP nel campo **Nome comune (CN)**.
- 3 Fare clic su **Salva**.

Sezione Generale

All'accesso successivo, utilizzare la nuova password.

Vedere ["Modifica della password"](#) a pagina 88.

Per specificare un nuovo indirizzo e-mail

- 1 Nel campo **Indirizzo e-mail** immettere il proprio indirizzo e-mail.
- 2 Fare clic su **Salva**.

Ogni utente di Symantec Data Loss Prevention può scegliere quale lingua e quali impostazioni locali usare tra quelle disponibili.

Per scegliere una lingua per un uso individuale

- 1 Fare clic sull'opzione accanto alla lingua scelta.
- 2 Fare clic su **Salva**.

La console di amministrazione di Enforce Server viene visualizzata nella nuova lingua.

La scelta di un'altra lingua non ha effetto sul rilevamento delle violazioni della politica. Il rilevamento viene eseguito su tutto il contenuto scritto in qualsiasi lingua supportata indipendentemente dalla lingua scelta per il profilo.

Vedere ["Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri"](#) a pagina 89.

Le lingue disponibili vengono determinate all'installazione del prodotto e con l'aggiunta successiva di supporti lingua per Symantec Data Loss Prevention. L'effetto di scegliere un'altra lingua varia come segue:

- Solo impostazioni locali. Se la lingua scelta include il messaggio *Traduzioni non disponibili*, date e numeri sono visualizzati nei formati appropriati per la lingua. Report ed elenchi sono ordinati conformemente a quella lingua, ma menu, etichette, schermate e guida della console di amministrazione non sono tradotti e rimangono in inglese.

Vedere ["Informazioni sulle impostazioni locali"](#) a pagina 94.

- Tradotto. La lingua scelta non visualizza il messaggio *Traduzioni non disponibili*. In questo caso, oltre al formato di numeri, date e ordinamento, menu, etichette, schermate della console di amministrazione, e in alcuni casi la guida, sono tradotti nella lingua scelta.

Vedere ["Informazioni su Symantec Data Loss Prevention supporti lingue"](#) a pagina 93.

Sezione Preferenze report

Per selezionare la codifica di testo

- 1 Selezionare un'opzione di codifica di testo:

- **Usa codifica predefinita browser.** Selezionare questa casella per specificare che i file di testo usano la stessa codifica del browser.
- Menu a discesa. Fare clic su un'opzione di codifica nel menu a discesa per selezionarla.

- 2 Fare clic su **Salva**.

La nuova codifica di testo viene applicata ai file CSV esportati. Questa codifica consente di selezionare la codifica di testo corrispondente alla codifica prevista dalle applicazioni CSV.

Per selezionare un delimitatore CSV

- 1 Scegliere uno dei delimitatori dal menu a discesa.

- 2 Fare clic su **Salva**.

Il nuovo delimitatore viene applicato al successivo elenco di valori separati da virgola (CSV) esportato.

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

Vedere ["Esportazione dei report di incidente"](#) a pagina 1656.

Per selezionare i dettagli dell'esportazione XML

- 1 **Includi violazioni incidente nell'esportazione XML.** Se questa casella è selezionata, i report esportati in XML includono le corrispondenze evidenziate in ogni istantanea incidente.
- 2 **Includi cronologia incidenti nell'esportazione XML.** Se questa casella è selezionata, i report esportati in XML includono i dati della cronologia incidenti contenuti nella scheda **Cronologia** di ogni istantanea incidente.
- 3 Fare clic su **Salva**.

Le selezioni vengono applicate al report successivo esportato in XML.

Se nessuna casella è selezionata, il report XML esportato contiene solo le informazioni di base sugli incidenti.

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

Vedere ["Esportazione dei report di incidente"](#) a pagina 1656.

Modifica della password

Quando la password scade, Symantec Data Loss Prevention mostra la finestra di rinnovo della password al momento dell'accesso successivo. Quando compare la finestra di rinnovo della password, inserire la nuova password e confermarla.

Quando la password scade, il sistema richiede di indicarne una nuova al successivo tentativo di accesso. Se viene richiesto di modificare la password, viene visualizzata la finestra di **Rinnovo password**.

Per modificare la password nella finestra Rinnovo password

- 1 Digitare la vecchia password nel campo **Vecchia password** della finestra **Rinnovo password**.
- 2 Digitare la nuova password nel campo **Nuova password** della finestra **Modifica della password**.
- 3 Digitare di nuovo la nuova password nel campo **Digita di nuovo la nuova password** della finestra di **Modifica della password**.

All'accesso successivo, utilizzare la nuova password.

È possibile anche cambiare in qualunque momento la password dalla schermata **Profilo**.

Vedere ["Modifica di un profilo utente"](#) a pagina 85.

Vedere ["Informazioni sull'account di amministrazione"](#) a pagina 83.

Vedere ["Accesso e disconnessione dalla console di amministrazione di Enforce Server"](#) a pagina 82.

Utilizzo di lingue e impostazioni internazionali

Il capitolo contiene i seguenti argomenti:

- [Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri](#)
- [Lingue supportate per il rilevamento](#)
- [Utilizzo di caratteri internazionali](#)
- [Informazioni su Symantec Data Loss Prevention supporti lingue](#)
- [Informazioni sulle impostazioni locali](#)
- [Utilizzo di una lingua diversa dall'inglese sulla console di amministrazione di Enforce Server](#)
- [Uso dell'utilità supporto lingue](#)

Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri

Symantec Data Loss Prevention supporta completamente distribuzioni internazionali offrendo un vasto numero di opzioni di localizzazione e lingue:

- Rilevamento della violazione e creazione della politica in molte lingue.
Le lingue supportate possono essere utilizzate in parole chiave, identificatori dati, espressioni regolari, profili dati esatti (EDM) e profili documenti (IDM).
Vedere "[Lingue supportate per il rilevamento](#) " a pagina 90.
- Operazione su versioni dell'interfaccia utente multilingua (MUI) e localizzate dei sistemi operativi di Windows.

- Set di caratteri internazionali. Per visualizzare e lavorare con set di caratteri internazionali, il sistema su cui viene visualizzata la console di amministrazione di Enforce Server deve possedere le funzionalità appropriate.
Vedere ["Utilizzo di caratteri internazionali"](#) a pagina 92.
- Formati di numeri e date basati su impostazioni internazionali, nonché ordini per elenchi e report.
Vedere ["Informazioni sulle impostazioni locali"](#) a pagina 94.
- Sistema di guida e interfaccia utente localizzata (UI). I supporti lingue per Symantec Data Loss Prevention forniscono versioni specifiche di una lingua della console di amministrazione Enforce Server. Possono inoltre fornire versioni specifiche di una lingua del sistema della Guida in linea.

Nota: Tali supporti lingue vengono aggiunti separatamente seguendo l'installazione iniziale del prodotto.

- Documentazione localizzata del prodotto.
- Pop-up di notifica specifiche di una lingua. I pop-up di notifica dell'endpoint vengono visualizzati nella lingua di visualizzazione selezionata sull'endpoint anziché nella lingua di impostazione internazionale del sistema. Ad esempio, se le impostazioni internazionali del sistema sono impostate su inglese e l'utente imposta la lingua di visualizzazione su tedesco, il pop-up di notifica viene visualizzato in tedesco.

Nota: Un pop-up di notifica di lingua misto viene visualizzato se la lingua delle impostazioni internazionali utente non corrisponde alla lingua utilizzata nella regola di risposta.

Lingue supportate per il rilevamento

Symantec Data Loss Prevention supporta molte lingue per il rilevamento. È possibile definire politiche che rilevano e segnalano accuratamente le violazioni trovate nel contenuto in queste lingue.

Tabella 3-1 Lingue supportate da Symantec Data Loss Prevention

Lingua	Versione 14.x	Versione 14.6	Versione 15.0	Versione 15.1
Arabo	Sì	Sì	Sì	Sì
Portoghese (Brasile)	Sì	Sì	Sì	Sì
Cinese (tradizionale)	Sì	Sì	Sì	Sì

Lingua	Versione 14.x	Versione 14.6	Versione 15.0	Versione 15.1
Cinese (semplificato)	Sì	Sì	Sì	Sì
Ceco	Sì	Sì	Sì	Sì
Danese	Sì	Sì	Sì	Sì
Olandese	Sì	Sì	Sì	Sì
Inglese	Sì	Sì	Sì	Sì
Finlandese	Sì	Sì	Sì	Sì
Francese	Sì	Sì	Sì	Sì
Tedesco	Sì	Sì	Sì	Sì
Greco	Sì	Sì	Sì	Sì
Ebraico	Sì	Sì	Sì	Sì
Ungherese	Sì	Sì	Sì	Sì
Italiano	Sì	Sì	Sì	Sì
Giapponese	Sì	Sì	Sì	Sì
Coreano	Sì	Sì	Sì	Sì
Norvegese	Sì	Sì	Sì	Sì
Polacco	Sì	Sì	Sì	Sì
Portoghese	Sì	Sì	Sì	Sì
Rumeno	Sì	Sì	Sì	Sì
Russo	Sì	Sì	Sì	Sì
Spagnolo	Sì	Sì	Sì	Sì
Svedese	Sì	Sì	Sì	Sì
Turco	Sì*	Sì*	Sì*	Sì*

* Symantec Data Loss Prevention non può essere installato su un sistema operativo Windows in lingua turca e non è possibile scegliere il turco come impostazioni locali alternative.

Per informazioni supplementari su specifiche lingue, vedere le *Note sulla versione di Symantec Data Loss Prevention*.

Questo supporto non include quanto segue:

- Supporto tecnico fornito in una lingua diversa dall'inglese. Sebbene Symantec Data Loss Prevention supporti una particolare lingua, ciò non implica che il supporto tecnico sia fornito in quella lingua.
- Interfaccia utente amministrativa e documentazione localizzate. Il supporto per una lingua non implica che l'interfaccia utente o la documentazione del prodotto sia stata localizzata in quella lingua. Tuttavia, anche senza un'interfaccia utente localizzata, parti della stessa definite dall'utente, come i messaggi di notifica sull'endpoint, possono ancora essere localizzate in qualsiasi lingua digitando il testo appropriato nell'interfaccia.
- Contenuto localizzato. Le parole chiave sono utilizzate in varie aree del prodotto, tra cui i modelli di politica e gli identificatori di dati. Il supporto per una lingua non implica che queste parole chiave siano state tradotte in quella lingua. Gli utenti possono tuttavia aggiungere parole chiave in una nuova lingua mediante la console di amministrazione di Enforce Server.
- Nuovi tipi di file, protocolli, applicazioni o codifiche. Il supporto per una lingua non implica l'assistenza per qualsiasi nuovo tipo di file, protocollo, applicazione o codifica che possono risultare prevalenti in quella lingua o regione.
- Normalizzazione specifica di una lingua. Un esempio di normalizzazione è considerare come uguali le versioni accentate e non accentate di un carattere. Il prodotto realizza già una serie di normalizzazioni, tra cui la normalizzazione Unicode standard che dovrebbe coprire la stragrande maggioranza dei casi. Tuttavia, non significa che tutte le normalizzazioni potenziali sono incluse.
- Normalizzazione e convalida specifica di un'area geografica. Un esempio è la consapevolezza che il prodotto ha del formato dei numeri di telefono nordamericani, che consente di considerare come uguali differenti versioni di un numero e di identificare i numeri non validi nei file di origine EDM. Il supporto per una lingua non implica questo tipo di funzionalità per quella lingua o area geografica.

Gli elementi in queste categorie sono gestiti come singoli potenziamenti del prodotto specifici di una lingua o di un'area geografica. Contattare il supporto tecnico Symantec per informazioni supplementari sui potenziamenti relativi alle lingue o sulle lingue non elencate.

Vedere ["Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri"](#) a pagina 89.

Utilizzo di caratteri internazionali

È possibile utilizzare varie lingue in Symantec Data Loss Prevention, in base a:

- Set di caratteri basato sul sistema operativo installato nel computer in cui si visualizza la console di amministrazione di Enforce Server
- Capacità del browser in uso

Ad esempio, un report incidente su una scansione di dati in lingua russa conterrà caratteri cirillici. Per visualizzare quel report, il computer e il browser utilizzati per accedere alla console di amministrazione di Enforce Server devono essere in grado di visualizzare tali caratteri. Di seguito sono riportate alcune linee guida:

- Se il computer utilizzato per accedere alla console di amministrazione di Enforce Server ha un sistema operativo localizzato per una particolare lingua, è necessario poter visualizzare e utilizzare un set di caratteri che supporta quella lingua.
- Se il sistema operativo del computer usato per accedere alla console di amministrazione non è localizzato per una particolare lingua, è possibile che sia necessario un supporto lingua supplementare. Questo supporto supplementare viene aggiunto al computer utilizzato per accedere alla console di amministrazione, non a Enforce Server.
 - In un sistema Windows, si aggiunge un supporto lingua supplementare utilizzando **Pannello di controllo > Opzioni internazionali e della lingua > Lingue (scheda) - Supporto lingua supplementare** per aggiungere font per alcuni set di caratteri.
- Può anche essere necessario configurare il browser per integrare i caratteri che si desidera visualizzare e immettere.

Nota: La console di amministrazione di Enforce Server supporta dati codificati UTF-8.

- In un sistema Windows, può anche essere necessario utilizzare la scheda **Lingue – Supporto lingua supplementare** in **Pannello di controllo > Opzioni internazionali e della lingua** per aggiungere font per alcuni set di caratteri.

Vedere le *Note sulla versione di Symantec Data Loss Prevention* per problemi noti relativi a specifiche lingue.

Vedere ["Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri"](#) a pagina 89.

Informazioni su Symantec Data Loss Prevention supporti lingue

I supporti lingue per Symantec Data Loss Prevention consentono di localizzare il prodotto per una particolare lingua sui sistemi Windows. Dopo che un supporto lingue è stato aggiunto a Symantec Data Loss Prevention, gli amministratori possono specificarlo come impostazione predefinita per l'intero sistema. Se gli amministratori rendono più supporti lingue disponibili per l'utilizzo, i singoli utenti possono scegliere la lingua con cui desiderano lavorare.

Vedere ["Utilizzo di una lingua diversa dall'inglese sulla console di amministrazione di Enforce Server"](#) a pagina 95.

I supporti lingue forniscono quanto segue:

- Le impostazioni locali della lingua selezionata diventano disponibili per amministratori e utenti finali nella schermata di **Configurazione** dell'Enforce Server.
- Schermate, voci di menu, comandi e messaggi di Enforce Server sono nella lingua scelta.
- La guida in linea di Symantec Data Loss Prevention può essere visualizzata nella lingua scelta.

I supporti lingue per Symantec Data Loss Prevention sono disponibili in [Symantec File Connect](#).

Attenzione: Quando si installa una nuova versione di Symantec Data Loss Prevention, tutti i supporti lingue installati vengono eliminati. Per una nuova versione localizzata di Symantec Data Loss Prevention, è necessario eseguire l'upgrade a una nuova versione del supporto lingue.

Vedere ["Informazioni sulle impostazioni locali"](#) a pagina 94.

Vedere ["Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri"](#) a pagina 89.

Informazioni sulle impostazioni locali

Le impostazioni locali sono installate insieme a un supporto lingue.

Le impostazioni locali:

- Visualizzano date e numeri nei formati appropriati alla lingua e all'area geografica in questione.
- Ordinano alfabeticamente elenchi e report in base alle colonne di testo, quali "nome politica" o "proprietario file" secondo le regole della impostazioni locali.

Un amministratore può anche configurare impostazioni locali supplementari per singoli utenti. Queste impostazioni locali supplementari devono essere supportate soltanto dalla versione di Java richiesta.

Per un elenco di queste impostazioni locali, vedere

<http://www.oracle.com/technetwork/java/javase/javase7locales-334809.html>.

Le impostazioni locali possono essere specificate all'installazione del prodotto, come descritto nella *Guida di installazione di Symantec Data Loss Prevention*. Possono anche essere configurate in un secondo momento utilizzando l'utilità supporto lingue.

Vedere ["Utilizzo di una lingua diversa dall'inglese sulla console di amministrazione di Enforce Server"](#) a pagina 95.

Vedere ["Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri"](#) a pagina 89.

Utilizzo di una lingua diversa dall'inglese sulla console di amministrazione di Enforce Server

L'uso di impostazioni locali e lingue è specificato mediante la console di amministrazione di Enforce Server in base ai seguenti ruoli:

- Amministratore di Symantec Data Loss Prevention. Specifica che una delle lingue disponibili deve essere la lingua predefinita del sistema e imposta le impostazioni locali.
- Singolo utente di Symantec Data Loss Prevention. Sceglie quali impostazioni locali usare.

Nota: L'aggiunta di molteplici supporti lingue potrebbe alterare leggermente le prestazioni di Enforce Server, a seconda del numero di lingue e di personalizzazioni presenti. Questo si verifica in quanto per ogni lingua è necessario costruire e gestire un set aggiuntivo di indici.

Avvertimento: Non modificare il database NLS_LANGUAGE e le impostazioni NLS_TERRITORY di Oracle.

Vedere ["Informazioni su Symantec Data Loss Prevention supporti lingue"](#) a pagina 93.

Vedere ["Informazioni sulle impostazioni locali"](#) a pagina 94.

Un amministratore di Symantec Data Loss Prevention specifica quale delle lingue disponibili è la lingua predefinita del sistema.

Per scegliere la lingua predefinita per tutti gli utenti

- 1 In Enforce Server, accedere a **Sistema > Impostazioni > Generale** e fare clic su **Configura**.

Viene visualizzata la schermata **Modifica impostazioni generali**.

- 2 Scorrere fino alla sezione **Lingua** della schermata **Modifica impostazioni generali** e fare clic sul pulsante accanto alla lingua da usare come lingua predefinita del sistema.
- 3 Fare clic su **Salva**.

Ogni utente di Symantec Data Loss Prevention può scegliere quale lingua e quali impostazioni locali usare aggiornando il proprio profilo.

Vedere ["Modifica di un profilo utente"](#) a pagina 85.

Gli amministratori possono usare l'utilità supporto lingue per aggiornare le lingue disponibili.

Vedere ["Uso dell'utilità supporto lingue"](#) a pagina 96.

Vedere ["Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri"](#) a pagina 89.

Nota: Se Enforce Server è eseguito su un host Linux, è necessario installare i caratteri della lingua sul computer host utilizzando l'applicazione Package Manager di Linux. Il nome di un pacchetto di caratteri di una lingua comincia con `fonts-<nome_lingua>`. Ad esempio, `fonts-japanese-0.20061016-4.el5.noarch`

Uso dell'utilità supporto lingue

Per avere a disposizione specifiche impostazioni locali per Symantec Data Loss Prevention, si aggiungono supporti lingue mediante l'utilità supporto lingue.

Eseguire l'utilità supporto lingue dalla riga di comando. Il suo eseguibile, `LanguagePackUtility.exe`, risiede nella directory `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\bin` in Windows e nella directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/bin` in Linux.

Per utilizzare l'utilità di supporto lingue, è necessario disporre delle autorizzazioni di lettura, scrittura ed esecuzione su tutti le cartelle e le sottocartelle in `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1`. Se si esegue l'utilità su Linux, è necessario essere un utente root.

Per visualizzare la guida per l'utilità, come l'elenco delle opzioni valide e dei relativi flag, digitare `LanguagePackUtility` senza flag.

Nota: L'esecuzione dell'utilità supporto lingue provoca un'interruzione di 20 secondi dei servizi `SymantecDLPManager` e `SymantecDLPIncidentPersister`. Tutti gli utenti che sono connessi alla console di amministrazione di Enforce Server vengono disconnessi automaticamente. Al termine degli aggiornamenti, l'utilità riavvia i servizi automaticamente e gli utenti può connettersi di nuovo alla console di amministrazione.

I supporti lingue per Symantec Data Loss Prevention possono essere ottenuti da Symantec [File Connect](#).

Per aggiungere un supporto lingue (Windows)

- 1 Informare gli altri utenti che tutti coloro che utilizzano la console di amministrazione di Enforce Server devono salvare il loro lavoro e disconnettersi.
- 2 Eseguire l'utilità di supporto lingue con il flag `-a` seguito dal nome del file ZIP per quel supporto lingue. Digitare:

```
LanguagePackUtility -a filename
```

dove *filename* è il percorso completo e il nome del file ZIP del supporto lingue.

Ad esempio, se il file zip del supporto lingue giapponese si trova in `c:\temp`, aggiungerlo digitando:

```
LanguagePackUtility -a c:\temp\Symantec_DLP_15.1_Japanese.zip
```

Per aggiungere molteplici supporti lingue durante la stessa sessione, specificare molteplici nomi di file, separati da spazi, ad esempio:

```
LanguagePackUtility -a  
c:\temp\Symantec_DLP_15.1_Japanese.zip  
Symantec_DLP_15.1_Chinese.zip
```

- 3 Accedere alla console di amministrazione di Enforce Server e confermare che l'opzione della nuova lingua è disponibile nella schermata **Modifica impostazioni generali**. A questo proposito, accedere a **Sistema > Impostazioni > Generale > Configura > Modifica impostazioni generali**.

Per aggiungere un supporto lingue (Linux)

- 1 Informare gli altri utenti che tutti coloro che utilizzano la console di amministrazione di Enforce Server devono salvare il loro lavoro e disconnettersi.
- 2 Aprire una sessione terminale per l'host di Enforce Server e passare a `DLP_system_account` eseguendo il comando seguente:

```
su - DLP_system_account
```

- 3 Eseguire il seguente comando:

```
DLP_home/Protect/bin/LanguagePackUtility -a <path to language pack zip file>
```

- 4 Accedere alla console di amministrazione di Enforce Server e confermare che l'opzione della nuova lingua è disponibile nella schermata **Modifica impostazioni generali**. A questo proposito, accedere a **Sistema > Impostazioni > Generale > Configura > Modifica impostazioni generali**.

Per rimuovere un supporto lingue

- 1 Informare gli utenti che tutti coloro che utilizzano la console di amministrazione di Enforce Server devono salvare il loro lavoro e disconnettersi.
- 2 Eseguire l'utilità di supporto lingue con il flag `-r` seguito dal codice di impostazioni locali Java del supporto lingue da rimuovere. Digitare:

```
LanguagePackUtility -r locale
```

dove *locale* è un codice di impostazioni locali Java valido che corrisponde a un supporto lingue di Symantec Data Loss Prevention.

Ad esempio, per rimuovere il supporto lingue francese digitare:

```
LanguagePackUtility -r fr_FR
```

Per rimuovere molteplici supporti lingue durante la stessa sessione, specificare molteplici nomi di file, separati da spazi.

- 3 Accedere alla console di amministrazione di Enforce Server e confermare che il supporto lingue non è più disponibile nella schermata **Modifica impostazioni generali**. A questo proposito, accedere a **Sistema > Impostazioni > Generale > Configura > Modifica impostazioni generali**.

L'eliminazione di un supporto lingue ha i seguenti effetti:

- Gli utenti non possono più selezionare le impostazioni locali del supporto lingue rimosso.

Nota: Se le impostazioni locali del supporto lingue sono supportate dalla versione di Java necessaria per eseguire Symantec Data Loss Prevention, l'amministratore può specificarle successivamente come impostazioni alternative per tutti gli utenti che ne hanno bisogno.

- Le impostazioni locali vengono ripristinate ai valori predefiniti configurati dall'amministratore.
- Se la lingua rimossa era quella predefinita del sistema, vengono ripristinate le impostazioni della lingua inglese.

Per cambiare o aggiungere delle impostazioni locali

- 1 Informare gli utenti che tutti coloro che utilizzano la console di amministrazione di Enforce Server devono salvare il loro lavoro e disconnettersi.
- 2 Eseguire l'utilità di supporto lingue con il flag `-c` seguito dal codice di impostazioni locali Java per le impostazioni locali che si desidera modificare o aggiungere. Digitare:

```
LanguagePackUtility -c locale
```

dove *locale* è un codice locale valido riconosciuto da Java, come `pt_PT` per il portoghese.

Ad esempio, per passare al portoghese brasiliano digitare:

```
LanguagePackUtility -c pt_BR
```

- 3 Accedere alla console di amministrazione di Enforce Server e confermare che le nuove impostazioni locali alternative sono ora disponibili nella schermata **Modifica impostazioni generali**. A questo proposito, accedere a **Sistema > Impostazioni > Generale > Configura > Modifica impostazioni generali**.

Se si specificano impostazioni locali per le quali non esiste un supporto lingue, il messaggio "Translations not available" viene visualizzato accanto al nome delle impostazioni locali. Ciò significa che la formattazione e l'ordinamento sono appropriati per le impostazioni locali, ma che le schermate e la guida in linea della console di amministrazione di Enforce Server non sono tradotti.

Nota: Gli amministratori possono mettere a disposizione degli utenti le impostazioni locali di una sola lingua supplementare non basata su un supporto lingue di Symantec Data Loss Prevention installato precedentemente.

Vedere ["Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri"](#) a pagina 89.

Gestione della piattaforma di Enforce Server

- [Capitolo 4. Gestione dei servizi e delle impostazioni di Enforce Server](#)
- [Capitolo 5. Gestione di ruoli e utenti](#)
- [Capitolo 6. Connessione alle directory di gruppo](#)
- [Capitolo 7. Gestione di credenziali archiviate](#)
- [Capitolo 8. Gestione di eventi e messaggi di sistema](#)
- [Capitolo 9. Gestione del database di Symantec Data Loss Prevention](#)
- [Capitolo 10. Utilizzo di Symantec Information Centric Encryption](#)
- [Capitolo 11. Utilizzo di Symantec Information Centric Tagging](#)
- [Capitolo 12. Aggiunta di un nuovo modulo di prodotto](#)

Gestione dei servizi e delle impostazioni di Enforce Server

Il capitolo contiene i seguenti argomenti:

- [Informazioni sui servizi Symantec Data Loss Prevention](#)
- [Informazioni sull'avvio e sull'arresto di servizi in Windows](#)
- [Avvio e arresto di servizi in Linux](#)

Informazioni sui servizi Symantec Data Loss Prevention

I servizi Symantec Data Loss Prevention potrebbero essere interrotti e avviati periodicamente. Questa sezione fornisce una breve descrizione di ogni servizio e la modalità di avvio e interruzione dei servizi sulle piattaforme supportate.

I servizi Symantec Data Loss Prevention per Enforce Server sono descritti nella seguente tabella:

Tabella 4-1 Servizi Symantec Data Loss Prevention

Nome servizio	Descrizione
Symantec DLP Manager	Fornisce i servizi di gestione e reporting centralizzati per Symantec Data Loss Prevention. Se si dispone di più di 50 politiche, 50 server di rilevamento o agenti 50.000, aumentare il <code>Max Memory</code> per questo servizio da 2048 a 4096. È possibile regolare questa impostazione nel file <code>SymantecDLPManager.conf</code> .
Controller server di rilevamento Symantec DLP	Controlla i server di rilevamento. Se si dispone di più di 50 politiche, 50 server di rilevamento o agenti 50.000, aumentare il <code>Max Memory</code> Per questo servizio da 1024 a 2048. È possibile regolare questa impostazione nel file <code>SymantecDLPDetectionServerController.conf</code> .
Symantec DLP Notifier	Fornisce le notifiche del database.
Symantec DLP Incident Persister	Consente di scrivere gli incidenti nel database.

Vedere ["Informazioni sull'avvio e sull'arresto di servizi in Windows"](#) a pagina 102.

Informazioni sull'avvio e sull'arresto di servizi in Windows

Le procedure per l'avvio e l'arresto dei servizi variano in base alle configurazioni dell'installazione e tra Enforce e server di rilevamento.

- Vedere ["Avvio di un Enforce Server su Windows"](#) a pagina 102.
- Vedere ["Arresto di un Enforce Server su Windows"](#) a pagina 103.
- Vedere ["Avvio di un server di rilevamento su Windows"](#) a pagina 103.
- Vedere ["Arresto di un server di rilevamento in Windows"](#) a pagina 104.
- Vedere ["Avvio dei servizi su installazioni Windows a un solo livello"](#) a pagina 104.
- Vedere ["Arresto dei servizi su installazioni Windows a un solo livello"](#) a pagina 104.

Avvio di un Enforce Server su Windows

Utilizzare la procedura seguente per avviare i servizi di Symantec Data Loss Prevention su un Enforce Server di Windows.

Per avviare i servizi Symantec Data Loss Prevention su un Enforce Server di Windows

- 1 Sul computer che ospita Enforce Server, accedere a **Start > Tutti i programmi > Strumenti di amministrazione > Servizi** per aprire il menu dei servizi di Windows.
- 2 Avviare i servizi di Symantec Data Loss Prevention nel seguente ordine:
 - SymantecDLPNotifier
 - SymantecDLPManager
 - SymantecDLPIncidentPersister
 - SymantecDLPDetectionServerController (se applicabile)

Nota: Avviare il servizio SymantecDLPNotifier prima di avviare altri servizi.

Vedere ["Arresto di un Enforce Server su Windows"](#) a pagina 103.

Arresto di un Enforce Server su Windows

Utilizzare la procedura seguente per arrestare i servizi di Symantec Data Loss Prevention su un Enforce Server di Windows.

Per arrestare i servizi di Symantec Data Loss Prevention su un Enforce Server di Windows.

- 1 Sul computer che ospita Enforce Server, accedere a **Start > Tutti i programmi > Strumenti di amministrazione > Servizi** per aprire il menu dei servizi di Windows.
- 2 Dal menu dei servizi di Windows, arrestare tutti i servizi Symantec Data Loss Prevention in esecuzione, nel seguente ordine:
 - SymantecDLPDetectionServerController (se applicabile)
 - SymantecDLPIncidentPersister
 - SymantecDLPManager
 - SymantecDLPNotifier

Vedere ["Avvio di un Enforce Server su Windows"](#) a pagina 102.

Avvio di un server di rilevamento su Windows

Per avviare i servizi Symantec Data Loss Prevention su un server di rilevamento Windows

- 1 Sul computer che ospita il server di rilevamento, accedere a **Start > Tutti i programmi > Strumenti di amministrazione > Servizi** per aprire il menu dei servizi di Windows.
- 2 Avviare il servizio SymantecDLPDetectionServer

Vedere ["Arresto di un server di rilevamento in Windows"](#) a pagina 104.

Arresto di un server di rilevamento in Windows

Utilizzare la procedura seguente per arrestare i servizi di Symantec Data Loss Prevention su un server di rilevamento di Windows.

Per arrestare i servizi di Symantec Data Loss Prevention su un server di rilevamento di Windows.

- 1 Sul computer che ospita il server di rilevamento, accedere a **Start > Tutti i programmi > Strumenti di amministrazione > Servizi** per aprire il menu dei servizi di Windows.
- 2 Dal menu **Servizi**, arrestare tutti i servizi Symantec Data Loss Prevention in esecuzione, che potrebbero includere il servizio `SymantecDLPDetectionServer`.

Vedere ["Avvio di un server di rilevamento su Windows"](#) a pagina 103.

Avvio dei servizi su installazioni Windows a un solo livello

Utilizzare la procedura seguente per avviare i servizi di Symantec Data Loss Prevention su un'installazione Windows a un solo livello.

Per avviare i servizi Symantec Data Loss Prevention su un'installazione Windows a un solo livello.

- 1 Sul computer che ospita il server Symantec Data Loss Prevention, accedere a **Start > Tutti i programmi > Strumenti di amministrazione > Servizi** per aprire il menu dei servizi di Windows.
- 2 Avviare Symantec Data Loss Prevention nel seguente ordine:
 - `SymantecDLPNotifier`
 - `SymantecDLPManager`
 - `SymantecDLPIncidentPersister`
 - `SymantecDLPDetectionServerController` (se applicabile)
 - `SymantecDLPDetectionServer`

Nota: Avviare il servizio `SymantecDLPNotifier` prima di avviare altri servizi.

Vedere ["Arresto dei servizi su installazioni Windows a un solo livello"](#) a pagina 104.

Arresto dei servizi su installazioni Windows a un solo livello

Utilizzare la procedura seguente per arrestare i servizi di Symantec Data Loss Prevention su un'installazione Windows a un solo livello.

Per arrestare i servizi Symantec Data Loss Prevention su un'installazione Windows a un solo livello.

- 1 Sul computer che ospita il server Symantec Data Loss Prevention, accedere a **Start > Tutti i programmi > Strumenti di amministrazione > Servizi** per aprire il menu dei servizi di Windows.
- 2 Dal menu dei servizi di Windows, arrestare tutti i servizi Symantec Data Loss Prevention in esecuzione, nel seguente ordine:
 - SymantecDLPDetectionServer
 - SymantecDLPDetectionServerController (se applicabile)
 - SymantecDLPIncidentPersister
 - SymantecDLPLManager
 - SymantecDLPNotifier

Vedere ["Avvio dei servizi su installazioni Windows a un solo livello"](#) a pagina 104.

Avvio e arresto di servizi in Linux

Le procedure per l'avvio e l'arresto dei servizi variano in base alle configurazioni dell'installazione e tra Enforce e server di rilevamento.

- Vedere ["Avvio di un Enforce Server su Linux"](#) a pagina 105.
- Vedere ["Arresto di un Enforce Server su Linux"](#) a pagina 106.
- Vedere ["Avvio di un server di rilevamento su Linux"](#) a pagina 106.
- Vedere ["Arresto del server di rilevamento su Linux"](#) a pagina 107.
- Vedere ["Avvio dei servizi su installazioni Linux a un solo livello"](#) a pagina 107.
- Vedere ["Arresto dei servizi su installazioni Linux a un solo livello"](#) a pagina 107.

Avvio di un Enforce Server su Linux

Utilizzare la procedura seguente per avviare i servizi di Symantec Data Loss Prevention su un Enforce Server Linux.

Per avviare i servizi di Symantec Data Loss Prevention su un Enforce Server Linux

- 1 Sul computer che ospita Enforce Server, accedere come utente principale.
- 2 Avviare il servizio Symantec DLP Notifier eseguendo il seguente comando:

```
service SymantecDLPNotifier start
```

- 3 Avviare i servizi Symantec Data Loss Prevention rimanenti, eseguendo il seguente comando:

```
service SymantecDLPManager start  
service SymantecDLPIncidentPersister start  
service SymantecDLPDetectionServerController start
```

Vedere ["Arresto di un Enforce Server su Linux"](#) a pagina 106.

Arresto di un Enforce Server su Linux

Utilizzare la procedura seguente per arrestare i servizi di Symantec Data Loss Prevention su un Enforce Server di Linux.

Per arrestare i servizi di Symantec Data Loss Prevention su un Enforce Server di Linux

- 1 Sul computer che ospita Enforce Server, accedere come utente principale.
- 2 Arrestare tutti i servizi Symantec Data Loss Prevention in esecuzione eseguendo il seguente comando:

```
service SymantecDLPIncidentPersisterh stop  
service SymantecDLPManager stop  
service SymantecDLPDetectionServerController stop  
service SymantecDLPNotifier stop
```

Vedere ["Avvio di un Enforce Server su Linux"](#) a pagina 105.

Avvio di un server di rilevamento su Linux

Utilizzare la procedura seguente per avviare i servizi di Symantec Data Loss Prevention su un server di rilevazione Linux.

Per avviare i servizi Symantec Data Loss Prevention su un server di rilevazione Linux

- 1 Sul computer che ospita il server di rilevamento, accedere come utente principale.
- 2 Avviare il servizio Symantec Data Loss Prevention eseguendo il seguente comando:

```
service SymantecDLPDetectionServer start
```

Vedere ["Arresto del server di rilevamento su Linux"](#) a pagina 107.

Arresto del server di rilevamento su Linux

Effettuare la seguente procedura per arrestare i servizi di Symantec Data Loss Prevention su un server Linux.

Per arrestare i servizi Symantec Data Loss Prevention su un server di rilevamento Linux

- 1 Sul computer che ospita il server di rilevamento, accedere come utente principale.
- 2 Arrestare il servizio Symantec Data Loss Prevention eseguendo il seguente comando:

```
service SymantecDLPDetectionServer stop
```

Vedere ["Avvio di un server di rilevamento su Linux"](#) a pagina 106.

Avvio dei servizi su installazioni Linux a un solo livello

Utilizzare la procedura seguente per avviare i servizi di Symantec Data Loss Prevention su un'installazione Linux a un solo livello.

Per avviare i servizi Symantec Data Loss Prevention su un'installazione Linux a un solo livello.

- 1 Sul computer che ospita le applicazioni del server Symantec Data Loss Prevention, accedere come utente principale.
- 2 Avviare il servizio Symantec DLP Notifier eseguendo il seguente comando:

```
service SymantecDLPNotifier start
```

- 3 Avviare i servizi Symantec Data Loss Prevention rimanenti eseguendo il seguente comando:

```
service SymantecDLPManager start  
service SymantecDLPDetectionServer start  
service SymantecDLPIncidentPersister start  
service SymantecDLPDetectionServerController start
```

Vedere ["Arresto dei servizi su installazioni Linux a un solo livello"](#) a pagina 107.

Arresto dei servizi su installazioni Linux a un solo livello

Utilizzare la procedura seguente per arrestare i servizi di Symantec Data Loss Prevention su un'installazione Linux a un solo livello.

Per arrestare i servizi di Symantec Data Loss Prevention su un'installazione Linux a un solo livello

- 1 Sul computer che ospita i server Symantec Data Loss Prevention accedere come utente principale.
- 2 Arrestare tutti i servizi Symantec Data Loss Prevention in esecuzione eseguendo il seguente comando:

```
service SymantecDLPIncidentPersister stop
service SymantecDLPManger stop
service SymantecDLPDetectionServer stop
service SymantecDLPDetectionServerController stop
service SymantecDLPNotifier stop
```

Vedere ["Avvio dei servizi su installazioni Linux a un solo livello"](#) a pagina 107.

Gestione di ruoli e utenti

Il capitolo contiene i seguenti argomenti:

- Informazioni sul controllo degli accessi basato sul ruolo
- Informazioni sulla configurazione di ruoli e utenti
- Informazioni sui ruoli consigliati per l'organizzazione
- Ruoli inclusi con i pacchetti di soluzioni
- Ruoli di configurazione
- Configurazione degli account utente
- Configurazione delle impostazioni di imposizione delle password
- Reimpostazione della password di amministratore
- Gestione e aggiunta di ruoli
- Gestione e aggiunta di utenti
- Informazioni sull'autenticazione degli utenti
- Configurazione dell'autenticazione dell'utente
- Integrazione di Active Directory per autenticazione utente
- Informazioni sulla configurazione dell'autenticazione del certificato

Informazioni sul controllo degli accessi basato sul ruolo

&pn.SuiteNameShort utilizza il controllo degli accessi in base ai ruoli per definire le modalità di accesso degli utenti alle funzionalità del prodotto. Ad esempio, un ruolo potrebbe consentire

agli utenti di visualizzare report, ma impedire agli utenti di creare politiche o di eliminare incidenti. In alternativa, un ruolo potrebbe consentire agli utenti di creare regole di risposta ma non regole di eliminazione.

I ruoli determinano cosa può visualizzare e fare un utente nella console di amministrazione di Enforce Server. Ad esempio, il ruolo Report è un ruolo specifico incluso nella maggior parte dei pacchetti della soluzione Symantec Data Loss Prevention. Gli utenti nel ruolo Report possono visualizzare incidenti e creare politiche, nonché configurare target di Discover (se è in esecuzione un Discover Server). Tuttavia, gli utenti nel ruolo Report non possono creare dati esatti o profili di documento. Inoltre, gli utenti nel ruolo Report non possono eseguire le attività di amministrazione del sistema. Quando un utente accede al sistema nel ruolo Report, i moduli **Gestisci > Profili dati** e **Sistema > Gestione accesso** nella console di amministrazione dell'Enforce Server non sono visibili a questo utente.

È possibile assegnare un utente a più di un ruolo. L'appartenenza a più ruoli consente a un utente di eseguire diversi tipi di attività nel sistema. Ad esempio, si può assegnare all'utente responsabile della gestione della sicurezza delle informazioni (InfoSec Manager) l'appartenenza a due ruoli: ISR (primo risponditore sicurezza delle informazioni) e ISM (responsabile sicurezza delle informazioni). L'InfoSec Manager può accedere al sistema come primo risponditore (ISR) o responsabile (ISM), a seconda delle attività da eseguire. L'InfoSec Manager vede solo i componenti dell'Enforce Server appropriati per quelle attività.

È anche possibile combinare ruoli e gruppi di politiche per limitare le politiche e i server di rilevamento che un utente può configurare. Ad esempio, è possibile associare un ruolo al gruppo di politiche dell'Ufficio europeo. Questo ruolo concede l'accesso alle politiche progettate solo per l'Ufficio europeo.

Vedere ["Distribuzione di politiche"](#) a pagina 378.

Gli utenti con più ruoli devono specificare quello desiderato al momento dell'accesso. Considerare ad esempio un caso in cui si assegna l'utente denominato User01 a due ruoli: Report e System Admin. Se User volesse accedere al sistema per amministrarlo, potrebbe accedere con la sintassi seguente: **Login:** `System Admin\User0101`

Vedere ["Accesso e disconnessione dalla console di amministrazione di Enforce Server"](#) a pagina 82.

L'utente Amministratore (creato durante l'installazione) ha accesso a ogni parte del sistema e pertanto non è un membro di alcun ruolo di controllo degli accessi.

Vedere ["Informazioni sull'account di amministrazione"](#) a pagina 83.

Informazioni sulla configurazione di ruoli e utenti

Quando si installa Enforce Server, si crea un utente amministratore predefinito che ha accesso a tutti i ruoli. Se si importa un pacchetto di soluzioni in Enforce Server, questo pacchetto include vari ruoli e utenti predefiniti.

Vedere ["Informazioni sull'account di amministrazione"](#) a pagina 83.

È tuttavia possibile che si voglia aggiungere altri ruoli e utenti a Enforce Server. Quando si aggiungono ruoli e utenti, è necessario considerare le seguenti linee guida:

- Determinare i ruoli necessari per i propri utenti aziendali e per i requisiti e le procedure di sicurezza delle informazioni dell'organizzazione.
 Vedere ["Informazioni sui ruoli consigliati per l'organizzazione"](#) a pagina 111.
- Esaminare i ruoli creati all'installazione di un pacchetto di soluzioni. È probabilmente possibile utilizzare alcuni di questi ruoli (o le versioni modificate degli stessi) per gli utenti nell'organizzazione.
 Vedere ["Ruoli inclusi con i pacchetti di soluzioni"](#) a pagina 112.
- Se necessario, modificare i ruoli del pacchetto di soluzioni e crearne di nuovi.
 Vedere ["Ruoli di configurazione"](#) a pagina 114.
- Creare gli utenti e assegnare ad ognuno uno o più ruoli.
 Vedere ["Configurazione degli account utente"](#) a pagina 123.
- Gestire ruoli e utenti e rimuovere quelli non utilizzati.
 Vedere ["Gestione e aggiunta di ruoli"](#) a pagina 129.
 Vedere ["Gestione e aggiunta di utenti"](#) a pagina 129.

Informazioni sui ruoli consigliati per l'organizzazione

Per determinare i ruoli di più utili per l'organizzazione, esaminare i processi aziendali e requisiti di sicurezza.

La maggior parte delle aziende e organizzazioni ritengono fondamentale i seguenti ruoli quando implementano il sistema Symantec Data Loss Prevention:

- **Amministratore di sistema**
 Questo ruolo consente l'accesso al modulo **Sistema** e alle opzioni di menu associate nella console di amministrazione di Enforce Server. Gli utenti con questo ruolo possono monitorare e gestire Enforce Server e i server di rilevamento. Gli utenti con questo ruolo possono anche distribuire server di rilevamento ed eseguire scansioni di rilevamento. Tuttavia, gli utenti con questo ruolo non possono visualizzare informazioni dettagliate sugli incidenti o creare politiche. Tutti i pacchetti di soluzioni creano il ruolo Amministratore di sistema con privilegi di amministratore di sistema.
- **Amministratore utenti**
 Questo ruolo assegna agli utenti il diritto di gestire utenti e ruoli. Di solito questo ruolo non assegna altri accessi o privilegi. Per evitare un uso improprio, si consiglia di non assegnare questo ruolo a più di due persone nell'organizzazione (principale e backup).
- **Amministratore delle politiche**

Questo ruolo assegna agli utenti il diritto di gestire le politiche e le regole di risposta. Di solito questo ruolo non assegna altri accessi o privilegi. Per evitare un uso improprio, si consiglia di non assegnare questo ruolo a più di due persone nell'organizzazione (principale e backup).

- **Autore di politiche**

Questo ruolo consente l'accesso al modulo **Politiche** e alle opzioni di menu associate nella console di amministrazione di Enforce Server. Questo ruolo è adatto per i responsabili della sicurezza delle informazioni che tengono traccia degli incidenti e rispondono alle tendenze dei rischi. Un responsabile della sicurezza delle informazioni può creare nuove politiche o modificarne di esistenti per impedire la perdita di dati. Tutti i pacchetti di soluzioni creano il ruolo di manager Infosec (InfoSec Manager, ISM) che dispone di privilegi per la creazione delle politiche.

- **Risponditore degli incidenti**

Questo ruolo consente l'accesso al modulo **Incidenti** e alle opzioni di menu associate nella console di amministrazione di Enforce Server. Gli utenti in questo ruolo possono tenere traccia e riparare gli incidenti. Le aziende hanno spesso almeno due ruoli per il risponditore degli incidenti che forniscono due livelli di privilegi per la visualizzazione e la risposta agli incidenti.

Il risponditore di primo livello può visualizzare informazioni generiche sugli incidenti ma non può accedere ai dettagli dell'incidente (ad esempio l'identità del mittente o del destinatario). Può anche eseguire alcune operazioni di riparazione, come inoltrare l'incidente o informare il trasgressore delle politiche di sicurezza dell'azienda. Il risponditore di secondo livello potrebbe essere il destinatario dell'inoltro, visualizzare i dettagli dell'incidente e modificare gli attributi personalizzati. Un risponditore di terzo livello potrebbe creare le regole di risposta, creare le politiche e creare i gruppi di politiche.

Tutti i pacchetti di soluzioni creano il ruolo risponditore Infosec (InfoSec Responder, ISR). Questo ruolo serve da risponditore di primo livello. È possibile utilizzare il ruolo ISM (manager InfoSec) per fornire l'accesso di secondo livello.

È probabile che la propria azienda richieda variazioni di questi ruoli, come pure di altri ruoli. Per ulteriori informazioni su questi e altri ruoli possibili, consultare le descrizioni dei ruoli importati con i pacchetti di soluzioni.

Vedere ["Ruoli inclusi con i pacchetti di soluzioni"](#) a pagina 112.

Ruoli inclusi con i pacchetti di soluzioni

I vari pacchetti di soluzioni offerti con Symantec Data Loss Prevention creano ruoli e utenti quando installati. Per tutti i pacchetti di soluzioni, è disponibile un set di ruoli e utenti standard. Ruoli e utenti possono variare a seconda del pacchetto di soluzioni importato.

La tabella seguente riassume i ruoli del pacchetto di soluzioni di servizi finanziari. Questi ruoli sono in massima parte gli stessi ruoli presenti in altri pacchetti di soluzioni di Symantec Data Loss Prevention.

Vedere [Tabella 5-1](#) a pagina 113.

Tabella 5-1 Ruoli del pacchetto di soluzioni di servizi finanziari

Nome ruolo	Descrizione
Compliance	<p>Responsabile della conformità:</p> <ul style="list-style-type: none"> ■ Gli utenti in questo ruolo possono visualizzare, riparare ed eliminare incidenti, cercare attributi e modificare tutti gli attributi personalizzati. ■ Questo ruolo completo fornisce agli utenti i privilegi per garantire il rispetto delle norme di conformità. Consente inoltre agli utenti di sviluppare strategie per la riduzione dei rischi a livello di unità operative e di visualizzare le tendenze degli incidenti e le valutazioni dei rischi.
Exec	<p>Dirigente:</p> <ul style="list-style-type: none"> ■ Gli utenti in questo ruolo possono visualizzare, riparare ed eliminare incidenti, cercare attributi e visualizzare tutti gli attributi personalizzati. ■ Questo ruolo fornisce agli utenti privilegi di accesso per prevenire il rischio di perdite di dati a livello di macro. Gli utenti in questo ruolo possono esaminare le tendenze dei rischi e la metrica delle prestazioni, come pure dashboard di incidenti.
HRM	<p>Responsabile risorse umane:</p> <ul style="list-style-type: none"> ■ Gli utenti in questo ruolo possono visualizzare, riparare ed eliminare incidenti, cercare attributi e modificare tutti gli attributi personalizzati. ■ Questo ruolo fornisce agli utenti privilegi di accesso per rispondere agli incidenti di sicurezza relativi alle violazioni da parte di impiegati.
Investigator	<p>Investigatore di incidenti:</p> <ul style="list-style-type: none"> ■ Gli utenti in questo ruolo possono visualizzare, riparare ed eliminare incidenti, cercare attributi e modificare tutti gli attributi personalizzati. ■ Questo ruolo fornisce agli utenti i privilegi di accesso per cercare dettagli di incidenti, compreso l'inoltro di incidenti per l'analisi scientifica. Gli utenti in questo ruolo possono anche indagare su specifici dipendenti.

Nome ruolo	Descrizione
ISM	Responsabile sicurezza informazioni: <ul style="list-style-type: none">■ Gli utenti in questo ruolo possono visualizzare, riparare ed eliminare incidenti. Possono cercare attributi, modificare tutti gli attributi personalizzati, creare politiche e regole di risposta.■ Questo ruolo fornisce agli utenti privilegi di risposta agli incidenti di secondo livello. Gli utenti possono gestire incidenti riassegnati nel team addetto alla sicurezza delle informazioni.
ISR	Risponditore sicurezza informazioni: <ul style="list-style-type: none">■ Gli utenti in questo ruolo possono visualizzare, riparare ed eliminare incidenti, cercare attributi e visualizzare o modificare alcuni attributi personalizzati. Non hanno accesso ai dettagli delle identità di destinatari o mittenti.■ Questo ruolo fornisce agli utenti privilegi di risposta agli incidenti di primo livello. Gli utenti possono visualizzare gli incidenti di politiche, trovare processi di business interrotti e richiedere l'assistenza del team di riparazione per riparare gli incidenti.
Report	Creazione di report e politiche <ul style="list-style-type: none">■ Gli utenti in questo ruolo possono visualizzare e riparare incidenti e creare politiche. Non hanno accesso ai dettagli degli incidenti.■ Questo ruolo fornisce un singolo ruolo per la creazione di politiche e la gestione dei rischi di perdite di dati.
Amministratore di sistema	Amministratore di sistema <ul style="list-style-type: none">■ Gli utenti in questo ruolo possono amministrare il sistema e gli utenti del sistema, nonché visualizzare incidenti. Non hanno accesso ai dettagli degli incidenti.

Ruoli di configurazione

Ogni utente Symantec Data Loss Prevention è assegnato a uno o più ruoli che definiscono i privilegi e i diritti che l'utente possiede all'interno del sistema. Un ruolo utente determina i privilegi di amministrazione del sistema, i diritti di creazione politiche, l'accesso agli incidenti e altro ancora. Se un utente è un membro di più ruoli, deve specificare il ruolo quando accede, ad esempio: **Accesso:** Sys Admin/sysadmin01.

Vedere ["Informazioni sul controllo degli accessi basato sul ruolo"](#) a pagina 109.

Vedere ["Informazioni sulla configurazione di ruoli e utenti"](#) a pagina 110.

Per configurare un ruolo

- 1 Accedere alla schermata **Sistema > Gestione accesso > Ruoli**.
- 2 Fare clic su **Aggiungi ruolo**.

Viene visualizzata la schermata **Configura ruolo** con le seguenti schede: **Generale**, **Accesso incidenti**, **Gestione politiche** e **Utenti**.

- 3 Nella scheda **Generale** :

- Immettere un **Nome** univoco per il ruolo. Il campo del nome distingue tra maiuscole e minuscole ed è limitato a 30 caratteri. Il nome che si immette deve essere corto e significativo. Utilizzare il campo **Descrizione** per annotare il nome del ruolo e spiegarne lo scopo più dettagliatamente. Il nome e la descrizione del ruolo vengono visualizzati nella schermata **Elenco dei ruoli**.
- Nella sezione **Privilegi utente**, è possibile concedere privilegi utente per il ruolo.
Privilegi di **Sistema** :

Amministrazione utente (super utente)

Selezionare l'opzione **Amministrazione utente** per consentire agli utenti di creare ruoli e utenti aggiuntivi in Enforce Server.

Amministrazione server

Selezionare l'opzione **Amministrazione server** per consentire agli utenti di eseguire le seguenti funzioni:

- Configurare i server di rilevamento.
- Creare e gestire i profili di dati per Exact Data Matching (EDM), Riconoscimento moduli, Indexed Document Matching (IDM) e Vector Machine Learning (VML).
- Configurare e assegnare gli attributi di incidente.
- Configurare impostazioni di sistema.
- Configurare regole di risposta.
- Creare gruppi di politiche.
- Configurare protocolli di riconoscimento.
- Visualizzare report di eventi di sistema e di traffico.
- Importare politiche.

Nota: La selezione di **Amministrazione server** fornisce inoltre i privilegi Gestione agente.

Gestione agente	<p>Selezionare l'opzione Gestione agente per consentire agli utenti di eseguire le seguenti funzioni:</p> <ul style="list-style-type: none"> ■ Esaminare lo stato dell'agente ■ Esaminare gli eventi dell'agente ■ Gestire gli agenti ed eseguire attività di risoluzione dei problemi ■ Eliminare, riavviare e arrestare gli agenti ■ Modificare l'Endpoint Server a cui si connettono gli agenti ■ Estrarre i registri dell'agente ■ Accedere ai report riepilogativi dell'agente ■ Aggiungere e aggiornare configurazioni dell'agente ■ Gestire e creare gruppi di agenti ■ Visualizzare i conflitti dei gruppi di agenti ■ Esaminare i registri del server ■ Gestire i registri del server, che include l'annullamento della raccolta di registri, la configurazione dei registri e il download e l'eliminazione di registri
------------------------	---

Privilegio **Persone** :

Reporting utente (riepilogo rischi, istantanea utente)	<p>Selezionare l'opzione Reporting utente per consentire agli utenti di visualizzare il riepilogo dei rischi dell'utente.</p> <p>Nota: Il privilegio Incidente > Visualizza è concesso automaticamente per tutti i tipi di incidente per gli utenti con il privilegio Reporting utente.</p> <p>Vedere "Informazioni sui rischi utente" a pagina 1712.</p>
--	--

- Nella sezione **Incidenti**, agli utenti in questo ruolo si concedono i seguenti privilegi di incidente. Queste impostazioni si applicano a tutti i report di incidenti nel sistema, inclusi il quadro generale, il riepilogo incidenti, l'elenco di incidenti e le istantanee incidente.

Visualizza

Selezionare l'opzione **Visualizza** per consentire agli utenti in questo ruolo di visualizzare incidenti di violazione della politica.

È possibile personalizzare l'accesso alla visualizzazione degli incidenti selezionando diverse opzioni per **Azioni** e **Visualizza attributi** come indicato di seguito:

- Per impostazione predefinita l'opzione **Visualizza** è attivata (selezionata) per tutti i tipi di incidenti: **Incidenti di rete**, **Incidenti di rilevazione** e **Incidenti endpoint**.
- Per limitare l'accesso alla visualizzazione solo a determinati tipi di incidente, selezionare (evidenziare) il tipo di incidente per il quale si desidera autorizzare la visualizzazione per questo ruolo. (Per effettuare selezioni multiple tenere premuto il tasto Ctrl.) Se un ruolo non consente a un utente di visualizzare parte di un report di incidente, l'opzione viene sostituita con "Non autorizzato" o è vuota.

Nota: Se si revoca un privilegio di visualizzazione incidenti per un ruolo, il sistema elimina tutti i report salvati per tale ruolo associati al privilegio revocato. Ad esempio, se si revoca (deseleziona) il privilegio di visualizzazione degli incidenti di rete, il sistema elimina qualsiasi report di incidente di rete salvato associato al ruolo.

Azioni

Effettuare una selezione tra le seguenti **Azioni** per personalizzare le azioni che un utente può eseguire quando si verifica un incidente:

- **Ripara incidenti**

Il privilegio consente agli utenti di modificare lo stato o la gravità di un incidente, impostare un proprietario di dati, aggiungere un commento alla cronologia incidenti, impostare le opzioni **Non nascondere** e **Consenti nascondi** ed eseguire le azioni delle regole di risposta. Inoltre, se si sta utilizzando l'API di reporting e aggiornamento incidenti, selezionare questo privilegio per riparare gli attributi di posizione e di stato.

- **Regole di risposta smart da eseguire**

Specificare quali regole di risposta smart è possibile eseguire sulla base del ruolo. Le regole di risposta smart configurate sono elencate nella colonna Disponibile sulla sinistra. Per esporre una regola di risposta smart per l'esecuzione da parte di un utente di questo ruolo, selezionarla e fare clic sulla freccia per aggiungerla alla colonna sul lato destro. Utilizzare il tasto CTRL per selezionare più regole.

- **Esegui ricerca attributi**

Consente agli utenti di cercare attributi di incidenti da origini esterne e popolare i loro valori per la riparazione di incidenti.

- **Elimina incidenti**

Consente agli utenti di eliminare un incidente.

- **Nascondi incidenti**

Consente agli utenti di nascondere un incidente.

- **Visualizza incidenti**

Consente agli utenti di ripristinare incidenti nascosti precedentemente.

- **Esporta archivio Web**

Consente agli utenti di esportare un report che il sistema compila da un archivio Web di incidenti.

- **Esporta XML**

Consente agli utenti di esportare un report di incidenti in formato XML.

- **Invia report incidente come allegato CSV tramite e-mail**

Consente agli utenti di inviare tramite e-mail come allegato un report contenente un elenco di dettagli di incidente separati da virgola.

**API di reporting e
aggiornamento
incidenti**

Effettuare una selezione tra i seguenti privilegi utente per consentire l'accesso a clienti di Web Services che utilizzano l'API di reporting e aggiornamento incidenti o l'API di reporting obsoleta:

■ **Reporting incidente**

Consente ai client di service Web di recuperare dettagli di incidente.

■ **Aggiornamento incidente**

Consente ai client di Web service aggiornare dettagli di incidente.
(Non si applica ai client che utilizzano l'API di reporting obsoleta.)

Per ulteriori informazioni, consultare il *Manuale per sviluppatori dell'API di reporting e aggiornamento incidenti Symantec Data Loss Prevention*.

Visualizza attributi Effettuare una selezione per il campo **Visualizza attributi** per impostare quali attributi vengono visualizzati nella vista Incidenti per le violazioni della politica che gli utenti del ruolo possono visualizzare.

Gli attributi **Condivisi** sono comuni a tutti i tipi di incidenti:

- **Corrispondenze**
Il testo evidenziato del messaggio che ha violato la politica viene visualizzato nella scheda **Corrispondenze** della schermata Istantanea incidente.
- **Cronologia**
La cronologia degli incidenti.
- **Corpo**
Il corpo del messaggio.
- **Allegati**
I nomi di tutti gli allegati o file.
- **Mittente**
Il mittente del messaggio.
- **Destinatari**
I destinatari del messaggio.
- **Oggetto**
L'oggetto del messaggio.
- **Messaggio originale**
Controlla se il messaggio originale che ha provocato l'incidente di violazione della politica può essere visualizzato.

Nota: Per visualizzare un allegato correttamente, deve essere selezionata sia l'opzione Allegato sia l'opzione "Messaggio originale".

Gli attributi **Endpoint** sono specifici dei ticket Endpoint:

- **Nome utente**
Il nome dell'utente di endpoint.
- **Nome computer**
Il nome del computer in cui l'agente di endpoint è installato.

Gli attributi **Discover** sono specifici per gli incidenti di rilevazione:

- **Proprietario file**
Il nome del proprietario del file di cui viene eseguita la scansione.
- **Posizione**
La posizione del file di cui viene eseguita la scansione.

Attributi personalizzati

L'elenco **Attributi personalizzati** include tutti gli attributi personalizzati configurati dall'amministratore di sistema, se presenti.

- Selezionare **Visualizza tutto** se si desidera che gli utenti siano in grado di visualizzare tutti i valori degli attributi personalizzati.
- Selezionare **Modifica tutto** se si desidera che gli utenti possano modificare tutti i valori degli attributi personalizzati.
- Per limitare la visualizzazione e modifica da parte degli utenti a determinati attributi personalizzati, deselezionare le caselle di controllo **Visualizza tutto** e **Modifica tutto** e selezionare singolarmente la casella **Visualizza** e/o **Modifica** per ogni attributo personalizzato che si desidera rendere visualizzabile o modificabile.

Nota: Se si seleziona **Modifica** per un attributo personalizzato, la casella di controllo **Visualizza** viene selezionata automaticamente (pertanto è visualizzata in grigio). Se si desidera che gli utenti in questo ruolo siano in grado di visualizzare tutti i valori degli attributi personalizzati, selezionare **Visualizza tutto**.

- Nella sezione **Discover**, è possibile concedere a utenti di questo ruolo i seguenti privilegi:

Reporting rischi cartelle

Questo privilegio consente agli utenti di visualizzare report di rischi cartelle. Fare riferimento a *Guida all'implementazione di Symantec Data Loss Prevention Data Insight*.

Nota: Questo privilegio è disponibile solo per licenze di Symantec Data Loss Prevention Data Insight.

Enumerazione radici contenuti

Questo privilegio consente agli utenti di configurare ed eseguire scansioni di enumerazione di radici di contenuti. Per ulteriori informazioni sulle scansioni di enumerazione di radici di contenuti, Vedere "[Utilizzo delle scansioni di enumerazione di radici di contenuti](#)" a pagina 1909.

- 4 Nella scheda **Accesso incidenti**, configurare tutte le condizioni (filtri) sui tipi di incidenti che gli utenti in questo ruolo possono visualizzare.

Nota: È necessario selezionare l'opzione **Visualizza** nella scheda **Generale** per fare in modo che le impostazioni nella scheda **Accesso incidenti** abbiano effetto.

Per aggiungere una condizione di Accesso incidenti:

- Fare clic su **Aggiungi condizione**.
- Selezionare il tipo di condizione e i relativi parametri da sinistra a destra come durante la scrittura di una frase. (Notare che il primo elenco a discesa in una condizione

contiene condizioni fornite dal sistema alfabetizzate associate a qualsiasi attributo personalizzato).

Selezionare ad esempio **Gruppo di politiche** dal primo elenco a discesa, selezionare **È uno qualsiasi dei seguenti valori** dal secondo elenco e **Gruppo di politiche predefinite** dalla casella di riepilogo finale. Queste impostazioni consentono agli utenti di visualizzare solo quegli incidenti che il gruppo di politiche predefinito ha rilevato.

- 5 Nella scheda **Gestione politiche**, selezionare uno dei seguenti privilegi di politica per il ruolo:

- **Importa politiche**

Questo privilegio consente agli utenti di importare file di politica che sono stati esportati da un Enforce Server.

Per concedere questo privilegio, il ruolo deve anche disporre dei privilegi **Amministrazione server**, **Crea politiche**, **Crea regole di risposta** e **Tutti i gruppi di politiche**.

- **Politiche autore**

Questo privilegio consente agli utenti di aggiungere, modificare ed eliminare politiche all'interno dei gruppi di politiche selezionati.

Esso consente inoltre agli utenti di modificare identificatori di dati del sistema e di creare identificatori di dati personalizzati.

Esso consente agli utenti di creare e modificare gruppi di utenti.

Questo privilegio non consente agli utenti di creare o gestire profili di dati. Questa attività richiede privilegi di amministratore di Enforce Server.

- **Controllo scansione di rilevamento**

Consente agli utenti in questo ruolo di creare target di Discover, di eseguire scansioni e di visualizzare Discover Server.

- **Gestione credenziali**

Consente agli utenti di creare e modificare le credenziali che il sistema richiede per accedere a sistemi target ed eseguire scansioni di rilevamento.

- **Gruppi di politiche**

Selezionare **Tutti i gruppi di politiche** solo se gli utenti in questo ruolo necessitano di accedere a tutti i gruppi di politiche esistenti e a tutti quelli che verranno creati in futuro.

In caso contrario è possibile selezionare singoli gruppo di politiche o **Gruppo di politiche predefinite**.

Nota: Queste opzioni non concedono il diritto di creare, modificare o eliminare gruppi di politiche. Soltanto gli utenti di cui il ruolo include il privilegio Amministrazione server possono operare con gruppi di politiche.

- **Regole di risposta autore**

Consente agli utenti in questo ruolo di creare, modificare ed eliminare le regole di risposta.

Nota: Gli utenti non possono modificare o creare regole di risposta per la riparazione di politiche a meno che non si selezioni l'opzione **Regole di risposta autore**.

Nota: Se si impedisce agli utenti di creare regole di risposta non si impedisce loro di eseguirle. Ad esempio, un utente senza privilegi di creazione di regole di risposta può ancora eseguire regole di risposta smart da un elenco di incidente o da un'istantanea incidente.

- 6 Nella scheda **Utenti**, selezionare tutti gli utenti a cui assegnare questo ruolo. Se non si sono ancora configurati utenti, è possibile assegnare utenti a ruoli dopo avere creato gli utenti.
- 7 Fare clic su **Salva** per salvare il ruolo creato di recente sul database di Enforce Server.

Configurazione degli account utente

Gli account utente sono ciò che gli utenti utilizzano per accedere al sistema ed eseguire operazioni. Il ruolo a cui appartiene l'account utente limita ciò che l'utente può fare nel sistema.

Per configurare un account utente:

- 1 Nella console di amministrazione di Enforce Server, selezionare **Sistema > Gestione accesso > Utenti DLP** per creare un nuovo account utente o per riconfigurarne uno esistente. Oppure fare clic su **Profilo** per riconfigurare l'account utente a cui si è attualmente collegati.
- 2 Fare clic su **Aggiungi utente DLP** per aggiungere un nuovo utente, oppure fare clic sul nome di un utente esistente per modificare la configurazione di tale utente.
- 3 Immettere un nome per un nuovo account utente nel campo **Nome**.
 - Il nome dell'account utente deve essere compreso tra 8 e 30 caratteri, fa distinzione tra maiuscole e minuscole e non può contenere barre rovesciate (\).
 - Se si utilizza l'autenticazione del certificato, il valore del campo **Nome** non deve necessariamente corrispondere al nome comune (CN) dell'utente. Tuttavia, è possibile scegliere di utilizzare lo stesso valore sia per **Nome** che per **Nome comune (CN)**, in modo da poter individuare facilmente la configurazione per un CN specifico. La console di amministrazione di Enforce Server mostra solo il valore del campo **Nome** nell'elenco degli utenti configurati.

- Se state utilizzando l'autenticazione Active Directory, il nome di account utente deve corrispondere al nome dell'account utente Active Directory. Si noti che tutti i nomi utente Symantec Data Loss Prevention fanno distinzione tra maiuscole e minuscole, anche se i nomi utente Active Directory non lo fanno. Gli utenti di Active Directory dovranno immettere il nome dell'account con distinzione tra maiuscole e minuscole quando effettuano l'accesso alla console di amministrazione di Enforce Server. Vedere ["Integrazione di Active Directory per autenticazione utente"](#) a pagina 141.

- 4 Configurare la sezione **Autenticazione** della pagina **Configura utente**. Su questa pagina sono disponibili soltanto le opzioni attivate.

Opzione	Istruzioni
Usa Mapping Single Sign-On	Se l'autenticazione SAML risulta attivata, l'utente può eseguire l'accesso tramite Mapping Single Sign-On sulla pagina Configura utente .
Usa accesso tramite Password	<p>Selezionare questa opzione per utilizzare l'autenticazione tramite password e consentire all'utente di eseguire l'accesso tramite la pagina di accesso della console di amministrazione di Enforce Server. Questa opzione è richiesta se l'account utente verrà utilizzato per un client del servizio Web API di reporting.</p> <p>Se si seleziona questa opzione, è necessario digitare anche la password dell'utente nei campi Password e Immettere di nuovo la password. La password deve avere almeno otto caratteri e fa distinzione tra maiuscole e minuscole. Per motivi di sicurezza, la password è oscurata e i caratteri vengono visualizzati come asterischi.</p> <p>Se si configurano impostazioni avanzate per la password, l'utente deve specificare una password difficile da indovinare. Inoltre, la password può scadere in una determinata data e l'utente deve impostarne una nuova periodicamente.</p> <p>Vedere "Configurazione delle impostazioni di imposizione delle password" a pagina 127.</p> <p>È possibile scegliere l'autenticazione tramite password anche se si utilizza l'autenticazione del certificato. Se utilizzate l'autenticazione del certificato, è possibile facoltativamente disattivare l'accesso dalla pagina di accesso della console di amministrazione di Enforce Server.</p> <p>Vedere "Disattivazione dell'autenticazione tramite password e dell'accesso basato sui moduli" a pagina 160.</p> <p>Symantec Data Loss Prevention autentica tutti i client dell'API di reporting che utilizzano l'autenticazione tramite password. Se si configura Symantec Data Loss Prevention in modo che utilizzi l'autenticazione del certificato, qualsiasi account utente utilizzato per accedere al servizio Web API di reporting deve avere una password valida. Consultare la <i>Guida degli sviluppatori dell'API di reporting Symantec Data Loss Prevention</i>.</p> <p>Nota: Se si configura l'integrazione delle Active Directory con Enforce Server, gli utenti effettuano l'autenticazione tramite le rispettive password di Active Directory. In questo caso il campo della password non viene visualizzato nella schermata Utenti.</p> <p>Vedere "Integrazione di Active Directory per autenticazione utente" a pagina 141.</p>

Opzione	Istruzioni
Usa autenticazione del certificato	<p>Selezionare questa opzione in modo da utilizzare l'autenticazione del certificato e consentire all'utente di scegliere l'accesso Single Sign-On automaticamente con un certificato generato da un'infrastruttura chiave privata (PKI) separata. Questa opzione è disponibile solo se è stato configurato manualmente il supporto dell'autenticazione del certificato.</p> <p>Vedere "Informazioni sull'autenticazione degli utenti" a pagina 130.</p> <p>Vedere "Informazioni sulla configurazione dell'autenticazione del certificato" a pagina 145.</p> <p>Se si seleziona questa opzione, è necessario specificare il valore del nome comune (CN) per l'utente nel campo Nome comune (CN). Il valore CN compare nel campo Oggetto del certificato dell'utente, che è generato dal PKI. I nomi comuni utilizzano generalmente il formato, <i>first_name last_name identification_number</i>.</p> <p>Enforce Server utilizza il valore CN per mappare il certificato a questo account utente. Se un certificato autenticato contiene il valore specificato CN, tutti gli altri attributi di questo account utente, quali il ruolo e le preferenze di reporting predefiniti, vengono applicati quando l'utente effettua l'accesso.</p> <p>Nota: Non è possibile specificare lo stesso valore di Nome comune (CN) in più account utente Nome comune (CN).</p>
Account disattivato	<p>Selezionare questa opzione per impedire all'utente di accedere alla console di amministrazione di Enforce Server. Questa opzione disattiva l'accesso per l'account utente indipendentemente dal meccanismo di autenticazione utilizzato.</p> <p>Per sicurezza, dopo un certo numero di tentativi di accesso non riusciti, il sistema disattiva automaticamente l'account e impedisce l'accesso all'utente. In questo caso l'opzione Account disattivato è selezionata. Per riattivare l'account utente e consentire all'utente di collegarsi al sistema, deselezionare l'opzione.</p>
5	<p>Se necessario, immettere un Indirizzo e-mail e selezionare una Lingua per l'utente nella sezione Generale della pagina. La selezione della Lingua dipende dal supporto lingue installato.</p>
6	<p>Nella sezione Preferenze report della schermata Utenti, specificare le preferenze relative al modo in cui l'utente riceve i report sugli incidenti, compresi Codifica file di testo e Delimitatore CSV.</p> <p>Se il ruolo assegna il privilegio per l'esportazione XML, è possibile scegliere di includere le violazioni e la cronologia incidenti nell'esportazione XML.</p>
7	<p>Nella sezione Ruoli, selezionare i ruoli disponibili per questo utente in modo da assegnare i privilegi di accesso a dati e incidenti.</p> <p>È necessario assegnare all'utente almeno un ruolo per accedere alla console di amministrazione di Enforce Server.</p> <p>Vedere "Ruoli di configurazione" a pagina 114.</p>

- 8 Selezionare **Ruolo predefinito** da assegnare a questo utente al momento dell'accesso.

Il ruolo predefinito viene applicato se nessun ruolo specifico è richiesto quando l'utente esegue l'accesso.

Ad esempio, la console di amministrazione di Enforce Server usa il ruolo predefinito se l'utente utilizza l'accesso Single Sign-On con autenticazione del certificato o la pagina di accesso.

Nota: I singoli utenti possono modificare il loro ruolo predefinito facendo clic su **Profilo** e selezionando un'opzione diversa dal menu **Ruolo predefinito**. Il nuovo ruolo predefinito viene applicato all'accesso successivo.

Vedere ["Informazioni sull'autenticazione degli utenti"](#) a pagina 130.

- 9 Fare clic su **Salva** per salvare la configurazione utente.

Nota: Una volta salvato un nuovo utente, non è possibile modificarne il nome utente.

- 10 Gestire utenti e ruoli secondo le necessità.

Vedere ["Gestione e aggiunta di ruoli"](#) a pagina 129.

Vedere ["Gestione e aggiunta di utenti"](#) a pagina 129.

Configurazione delle impostazioni di imposizione delle password

Nella schermata **Sistemi > Impostazioni > Generale** è possibile imporre agli utenti di usare password efficaci. Le password efficaci devono contenere almeno otto caratteri, almeno un numero e almeno una lettera maiuscola. Le password efficaci non possono avere più di due caratteri ripetuti consecutivi. L'imposizione delle password efficaci viene applicata a tutto il sistema. Gli utenti esistenti che non hanno una password efficace devono aggiornare i loro profili all'accesso seguente.

È anche possibile imporre agli utenti di cambiare le loro password a intervalli regolari. In questo caso, alla fine dell'intervallo specificato, il sistema forza gli utenti a creare una nuova password.

Se si utilizza l'autenticazione Active Directory, queste impostazioni sono applicate solo alla password amministratore. Tutte le altre password di account utente sono create con Active Directory.

Vedere ["Integrazione di Active Directory per autenticazione utente"](#) a pagina 141.

Per configurare le impostazioni di autenticazione avanzate

- 1 Accedere a **Sistema > Impostazioni > Generale** e fare clic su **Configura**.
- 2 Per imporre password efficaci, accedere alla sezione **Autenticazione utente DLP** e selezionare **Password efficace obbligatoria**.

Symantec Data Loss Prevention richiede agli utenti esistenti che non hanno password efficaci di crearne una all'accesso seguente.
- 3 Per impostare il periodo di validità delle password, digitare un numero (che rappresenta il numero di giorni) nel campo **Periodo di rotazione password**.

Per rendere illimitata la validità di una password, digitare 0 (il carattere zero).

Reimpostazione della password di amministratore

Symantec Data Loss Prevention fornisce l'utilità `AdminPasswordReset` per reimpostare la password dell'amministratore. Non esiste un metodo per recuperare una password perduta, ma è possibile usare questa utilità per assegnare una nuova password. È inoltre possibile usare l'utilità se i meccanismi di autenticazione del certificato sono disattivati e non è stata ancora definita una password per l'account di amministratore.

Per usare l'utilità `AdminPasswordReset` è necessario specificare la password per il database Enforce Server. Attenersi alla seguente procedura per reimpostare la password.

Per reimpostare la password di amministratore per l'accesso basato sui moduli

- 1 Accedere al computer con Enforce Server utilizzando l'account creato durante l'installazione di Symantec Data Loss Prevention.

Nota: Non modificare le autorizzazioni o l'appartenenza di qualsiasi file di configurazione di un altro account radice o di amministratore.

- 2 Passare alla directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/bin` (**Linux**) o `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\bin` (**Windows**). Se Symantec Data Loss Prevention è stato installato in una directory differente, sostituire il percorso corretto.
- 3 Eseguire l'utilità `AdminPasswordReset` utilizzando la seguente sintassi:

```
AdminPasswordReset -dbpass oracle_password -newpass new_administrator_password
```

Sostituire *oracle_password* con la password del database Enforce Server e sostituire *new_administrator_password* con la password da impostare.

Gestione e aggiunta di ruoli

La schermata **Sistema > Gestione accesso > Ruoli** consente di visualizzare un elenco alfabetico dei ruoli definiti per la propria organizzazione.

I ruoli elencati in questa schermata consentono di visualizzare le seguenti informazioni:

- **Nome** - Il nome del ruolo
- **Descrizione** - Una breve descrizione del ruolo.

Supponendo che si disponga dei privilegi appropriati, è possibile visualizzare, aggiungere e modificare i ruoli nel modo seguente:

- Aggiungere un nuovo ruolo o modificarne uno esistente.
Fare clic su **Aggiungi ruolo** per aggiungere un nuovo ruolo al sistema.
Fare clic su un punto qualsiasi della riga o sull'icona a forma di **matita** (estrema destra) per modificare quel ruolo
Vedere "[Ruoli di configurazione](#)" a pagina 114.
- Fare clic sulla **X rossa** (estrema destra) per eliminare il ruolo; una finestra di dialogo confermerà l'eliminazione.

Prima di modificare o eliminare i ruoli, attenersi alle seguenti linee guida:

- Se si cambiano i privilegi di un ruolo, gli utenti con quel ruolo attualmente collegati al sistema non sono interessati. Ad esempio, se si rimuove il privilegio di modifica per un ruolo, gli utenti attualmente collegati continuano ad avere l'autorizzazione di modificare gli attributi personalizzabili per quella sessione. Tuttavia, all'accesso successivo, le modifiche apportate a quel ruolo verranno confermate e quegli utenti non potranno più modificare gli attributi personalizzabili.
- Se si revoca un privilegio di visualizzazione di un incidente per un ruolo, Enforce Server elimina automaticamente qualsiasi report salvato associato al privilegio revocato. Ad esempio, se si revoca il privilegio di visualizzare gli incidenti di rete, il sistema elimina qualsiasi report di incidente di rete salvato associato al nuovo ruolo con restrizioni.
- Prima di poter eliminare un ruolo, è necessario assicurarsi che non vi siano utenti connessi a quel ruolo.
- Quando si elimina un ruolo, si eliminano tutti i report condivisi salvati dall'utente in quel ruolo.

Vedere "[Gestione e aggiunta di utenti](#)" a pagina 129.

Gestione e aggiunta di utenti

La schermata **Sistema > Gestione accesso > Utenti DLP** elenca tutti gli account utente attivi nel sistema.

Le seguenti informazioni sono elencate per ogni account utente:

- **Nome utente** - Il nome che l'utente digita per connettersi a Enforce Server
- **E-mail** - L'indirizzo e-mail dell'utente
- **Accesso** - Il ruolo dell'utente

Supponendo che si disponga di privilegi appropriati, è possibile aggiungere, modificare o eliminare account nel modo seguente:

- Aggiungere un nuovo account utente o modificarne uno esistente.
 Fare clic su **Aggiungi** per aggiungere un nuovo utente al sistema.
 Fare clic su un punto qualsiasi della riga o sull'icona a forma di **matita** (estrema destra) per visualizzare quell'account utente.
 Vedere ["Configurazione degli account utente"](#) a pagina 123.
- Fare clic sull'icona **X rossa** (estrema destra) per eliminare l'account utente; una finestra di dialogo conferma l'eliminazione.

Nota: L'account di amministratore viene creato all'installazione e non può essere rimosso dal sistema.

Nota: Quando si elimina un account utente, si eliminano anche tutti i report privati salvati associati a quell'utente.

Vedere ["Gestione e aggiunta di ruoli"](#) a pagina 129.

Informazioni sull'autenticazione degli utenti

Le opzioni di autenticazione dell'accesso alla console di gestione di Enforce Server includono SAML, basata su moduli, Active Directory/Kerberos e certificato.

Tabella 5-2 fornisce le descrizioni di questi meccanismi per autenticare gli utenti nella console di amministrazione di Enforce Server:

Tabella 5-2 Meccanismi di autenticazione di Enforce Server

Meccanismo di autenticazione	Meccanismo di accesso	Descrizione
Autenticazione SAML	Single Sign-On	<p>Con l'autenticazione SAML, la console di amministrazione di Enforce Server autentica ciascun utente convalidando l'e-mail, il nome utente o altri attributi dell'utente che corrispondono agli attributi utilizzati da Identity Provider.</p> <p>Quando SAML è attivato, gli utenti accedono all'URL della console di amministrazione di Enforce Server e sono reindirizzati alla pagina di accesso di Identity Provider, dove immettono le loro credenziali. Dopo che sono stati autenticati con Identity Provider, i loro attributi sono inviati a Enforce Server. Enforce Server cerca di trovare un utente con gli attributi corrispondenti. Se l'utente viene trovato, è connesso alla console di amministrazione di Enforce Server.</p> <p>File di modello di configurazione utilizzato: springSecurityContext-SAML.xml</p> <p>Vedere "Informazioni sull'autenticazione SAML" a pagina 134.</p>
Autenticazione tramite password	Accesso basato sui moduli	<p>Con l'autenticazione tramite password, la console di amministrazione di Enforce Server autentica ciascun utente determinando se la combinazione di nome utente e password fornita corrisponde a un account utente attivo nella configurazione di Enforce Server. Un account utente attivo viene autenticato se gli è stato assegnato un ruolo valido.</p> <p>Gli utenti immettono le credenziali nella pagina di accesso della console di amministrazione di Enforce Server e le invia su una connessione HTTP al contenitore Tomcat che ospita la console di amministrazione.</p> <p>Con l'autenticazione tramite password è necessario configurare il nome utente e la password di ciascun account utente direttamente nella console di amministrazione di Enforce Server. È inoltre necessario che ciascun account utente disponga di almeno un ruolo assegnato.</p> <p>File di modello di configurazione utilizzato: springSecurityContext-Form.xml</p> <p>Vedere "Gestione e aggiunta di utenti" a pagina 129.</p>

Meccanismo di autenticazione	Meccanismo di accesso	Descrizione
Autenticazione Active Directory	Accesso basato sui moduli	<p>Con l'autenticazione Microsoft Active Directory, la console di amministrazione di Enforce Server valuta dapprima il nome utente fornito per determinare se il nome esiste in un server Active Directory configurato. Se il nome utente esiste in Active Directory, la password fornita per l'utente viene valutata in base alla password Active Directory. Eventuali password configurate nella configurazione di Enforce Server vengono ignorate.</p> <p>Con l'autenticazione Active Directory è necessario configurare un account utente per ciascun utente Active Directory nuovo nella console di amministrazione di Enforce Server. Quando si esegue l'upgrade a Symantec Data Loss Prevention 15, gli utenti esistenti non devono essere configurati nuovamente.</p> <p>Non è necessario immettere una password per un account utente Active Directory. È possibile passare all'autenticazione Active Directory dopo che si sono già creati account utente nel sistema. Tuttavia solo i nomi utente esistenti che corrispondono ai nomi utente Active Directory rimangono validi dopo il passaggio.</p> <p>File di modello di configurazione utilizzato: <code>springSecurityContext-Kerberos.xml</code></p> <p>Vedere "Verifica della connessione di Active Directory" a pagina 144.</p>

Meccanismo di autenticazione	Meccanismo di accesso	Descrizione
Autenticazione del certificato	Single Sign-On dall'interfaccia PKI	<p>L'autenticazione del certificato consente a un utente di accedere automaticamente alla console di amministrazione di Enforce Server mediante un certificato client X.509. Questo certificato viene generato dall'infrastruttura a chiave pubblica (PKI). Per utilizzare il Single Sign-On basato sul certificato, è necessario attivare dapprima l'autenticazione del certificato come descritto in questa sezione.</p> <p>Vedere "Configurazione dell'autenticazione del certificato per la console di amministrazione di Enforce Server" a pagina 147.</p> <p>Il certificato client deve venire consegnato a Enforce Server quando un browser del client esegue l'handshake SSL con la console di amministrazione di Enforce Server. Ad esempio è possibile utilizzare un lettore di smart card e middleware con il browser per presentare automaticamente un certificato a Enforce Server. In alternativa è possibile ottenere un certificato X.509 da un'autorità di certificazione e caricarlo su un browser configurato per inviare il certificato a Enforce Server.</p> <p>Quando un utente accede alla console di amministrazione di Enforce Server, l'infrastruttura PKI consegna automaticamente il certificato dell'utente al contenitore Tomcat che ospita la console di amministrazione. Il contenitore Tomcat convalida il certificato client mediante le autorità di certificazione configurate nell'archivio Attendibilità Tomcat.</p> <p>File di modello di configurazione utilizzato: <code>springSecurityContext-Certificate.xml</code></p> <p>Vedere "Aggiunta di certificati dell'autorità di certificazione (CA) all'archivio Attendibilità Tomcat" a pagina 149.</p> <p>La console di amministrazione di Enforce Server utilizza il certificato convalidato per determinare se il certificato è stato revocato.</p> <p>Vedere "Informazioni sui controlli di revoca dei certificati" a pagina 153.</p> <p>Se il certificato è valido e non è stato revocato, Enforce Server utilizza il nome comune (CN) del certificato per determinare se tale CN è mappato a un account utente attivo con un ruolo nella configurazione di Enforce Server. Per ogni utente che accede alla console di amministrazione di Enforce Server con il Single Sign-On basato sul certificato, è necessario creare un account utente in Enforce Server che definisca il valore CN dell'utente corrispondente. È inoltre necessario assegnare uno o più ruoli validi all'account utente.</p>

Alcuni punti importanti da tenere in considerazione quando si configura l'autenticazione SAML.

- È necessario riavviare il manager quando si cambia il metodo di autenticazione degli utenti in SAML. Cambiando questo criterio di mapping nel file `springSecurityContext` per SAML senza riavviare il manager, gli utenti perdono la sincronizzazione, poiché il sistema continua a utilizzare la versione precedente del file. Ad esempio, se si modificano i criteri di mapping da nome utente a indirizzo e-mail è necessario riavviare il manager.
- È necessario rimappare ciascun utente quando si cambiano i criteri di mapping degli utenti in SAML. Cambiando i criteri di mapping, si invalida il mapping corrente degli utenti.
- È necessario convalidare la sintassi XML prima di riavviare il manager. Alcuni caratteri come "&" che possono far parte di un attributo utente rendono non valido l'XML. È necessario sostituire questi caratteri con la relativa stringa XML con escape. Ad esempio, anziché "&" utilizzare "&".
- Non eliminare nessun nodo XML nei file XML.
- I nomi di attributo in XML devono corrispondere esattamente (comprese le maiuscole/minuscole) ai nomi di attributo in Identity Provider.
- Quando si passa dall'autenticazione basata su moduli all'autenticazione SAML, è necessario esaminare ciascun utente e disattivare l'accesso tramite password per gli utenti di servizi non Web.
- Quando si passa dall'autenticazione del certificato all'autenticazione SAML, assicurarsi che il valore `ClientAuth` in `server.xml` sia impostato su `false`.

Vedere ["Configurazione dell'autenticazione dell'utente"](#) a pagina 134.

Configurazione dell'autenticazione dell'utente

Informazioni sull'autenticazione SAML

È ora disponibile l'autenticazione degli utenti SAML (Security Assertion Markup Language) per accedere alla console di amministrazione di Enforce Server. SAML è a un formato di dati a standard aperto basato su XML per lo scambio dei dati di autenticazione e autorizzazione tra i provider di servizi e i provider di identità. DLP è il provider di servizi.

Prima di utilizzare SAML, è necessario configurare il provider di servizi e il provider di identità e mappare gli attributi dell'utente per identificare l'utente.

Sono disponibili tre tipi di mapping: tramite e-mail, tramite nome utente e tramite gli attributi personalizzati dell'utente. Quando si utilizza SAML, l'accesso NOME UTENTE\RUOLO per gli utenti locali non è supportato.

Symantec supporta i seguenti provider di identità, sia on-site sia cloud:

- SAM (Symantec Access Manager)
- Okta

■ SSOCircle

Per aggiornamenti sugli IDP supportati, consultare la *Symantec Data Loss Prevention Guida ai requisiti di sistema* all'indirizzo <http://www.symantec.com/docs/doc10602>.

Vedere "Configurazione dell'autenticazione" a pagina 135.

Configurazione dell'autenticazione

Tabella 5-3 mostra un riepilogo delle attività di configurazione con collegamenti a ulteriori informazioni su ciascun passaggio.

Tabella 5-3 Passaggi di configurazione dell'autenticazione

Passaggio	Operazione	Ulteriori informazioni
Passaggio 1	Modificare il file contestuale Spring per il metodo di autenticazione.	Vedere "Impostazione e configurazione del metodo di autenticazione" a pagina 137.
Passaggio 2	Impostare la configurazione dell'autenticazione.	<p>Per SAML: Vedere "Impostazione della configurazione dell'autenticazione SAML" a pagina 138.</p> <p>Per Active Directory/Kerberos: Vedere "Configurazione dell'autenticazione di Active Directory" a pagina 140.</p> <p>Per l'autenticazione basata su moduli: Vedere "Configurazione dell'autenticazione basata su moduli" a pagina 141.</p> <p>Per il certificato: Vedere "Configurazione dell'autenticazione del certificato" a pagina 141.</p>
Passaggio 3	Riavviare Enforce Server.	Vedere "Informazioni sui servizi Symantec Data Loss Prevention" a pagina 101.

Passaggio	Operazione	Ulteriori informazioni
Passaggio 4	Per SAML, generare e scaricare i metadati SAML del provider di servizi. La console di amministrazione di Enforce Server è il provider di servizi.	Vedere "Generazione o download dei metadati SAML di Enforce (provider di servizi)" a pagina 139.
Passaggio 5	Per SAML, configurare Enforce come provider di servizi SAML con il provider di identità.	Vedere "Configurare Enforce Server come provider di servizi SAML in IDP (creare un'applicazione nel provider di identità)" a pagina 139.
Passaggio 6	Per SAML, scaricare i metadati Identity Provider.	Vedere "Esportazione dei metadati IDP in DLP" a pagina 140.
Passaggio 7	Completare il processo riavviando Enforce Server.	Vedere "Informazioni sui servizi Symantec Data Loss Prevention" a pagina 101.
Passaggio 8	Accedere alla console di amministrazione di Enforce Server con l'URL bypass dell'amministratore.	Vedere "URL bypass dell'amministratore" a pagina 136.

Nota: La console di amministrazione di Enforce Server (il provider di servizi in SAML) e IDP scambiano messaggi utilizzando le impostazioni nella configurazione. Assicurarsi che le impostazioni coincidano con la configurazione e le capacità di IDP. Impostazioni non coincidenti causano problemi al sistema.

È necessario riavviare due volte Enforce Server: una volta dopo aver impostato la configurazione dell'autenticazione nel file `springSecurityContext.xml` e una volta dopo aver scaricato il file dei metadati IDP e sostituito il contenuto di `idp-metadata.xml` con i metadati di IDP nella directory di installazione di Enforce.

Vedere ["URL bypass dell'amministratore"](#) a pagina 136.

URL bypass dell'amministratore

L'URL bypass dell'amministratore, `https://<hostnameOrIp>/ProtectManager/admin/Logon`, consente di aggirare l'autenticazione SAML. È possibile accedere alla console di amministrazione di Enforce Server e utilizzare l'autenticazione basata sui moduli per configurare gli utenti. È necessario immettere questo URL nel browser, non è possibile accedervi attraverso l'interfaccia utente della console di amministrazione di Enforce Server.

Nota: È disponibile un solo accesso attivo con l'URL bypass.

Vedere ["Impostazione e configurazione del metodo di autenticazione"](#) a pagina 137.

Impostazione e configurazione del metodo di autenticazione

Questi passaggi presentano una panoramica delle attività comuni per impostare e configurare tutti i metodi di autenticazione. I passaggi aggiuntivi o le modifiche per ogni metodo sono spiegati in Ultime passaggi dopo la configurazione iniziale del file di modello.

Nota: I file che è necessario modificare sono commentati con dettagli utili durante il processo di aggiornamento.

Per configurazione il metodo di autenticazione

- 1 Eliminare (o rinominare) il file `springSecurityContext.xml` in `[directory di installazione]/Protect/tomcat/webapps/ProtectManager/WEB-INF/`.
- 2 Accedere alla cartella `[directory di installazione]/Protect/tomcat/webapps/ProtectManager/security/template` e selezionare il file del modello di configurazione adatto al metodo di autenticazione utilizzato:
 - `SpringSecurityContext-SAML.xml` per configurazioni dell'autenticazione SAML
 - `springSecurityContext-Form.xml` per configurazioni dell'autenticazione basata su moduli e certificato client
 - `SpringSecurityContext-Certificate.xml` per l'autenticazione basata solo su certificato del client
 - `springSecurityContext-Kerberos.xml` per le configurazioni dell'autenticazione Active Directory/Kerberos
- 3 Copiare il file selezionato nella cartella `[directory di installazione]/Protect/tomcat/webapps/ProtectManager/WEB-INF/`.
- 4 Rinominare il file in `springSecurityContext.xml`.
- 5 Configurare il file `springSecurityContext.xml`:
- 6 Ultime passaggi:
 - SAML: per istruzioni su come impostare la configurazione dell'autenticazione SAML, consultare [Impostazione della configurazione dell'autenticazione SAML](#).
 - Basato su moduli: se il file di modello copiato è per l'autenticazione basata su moduli, non ci sono impostazioni aggiuntive da configurare. La sezione **Autenticazione utente**

DLP delle **Impostazioni generali** ora indica che il metodo di autenticazione degli utenti è **Basato su moduli**.

- **Certificato client:** per attivare l'autenticazione del certificato client, impostare `clientAuth` su `want` o su `true` in `<InstallDirectory>/Protect/tomcat/config/server.xml`. La sezione **Autenticazione utente DLP** delle **Impostazioni generali** ora indica che il metodo di autenticazione degli utenti è **Certificato**.
- **Active Directory:** per attivare l'autenticazione di Active Directory, sostituire il valore `krbConfLocation` in

```
[directory di
installazione]/Protect/tomcat/webapps/ProtectManager/WEB-INF/springSecurityContext.xml
```

con il percorso del file `krb5.ini`.

La sezione **Autenticazione utente DLP** delle **Impostazioni generali** ora indica che il metodo di autenticazione degli utenti è **Active Directory**. È possibile configurare l'elenco dei domini nella sezione **Autenticazione utente DLP** della pagina **Impostazioni generali**.

Nota: Non è più possibile eseguire la configurazione iniziale di Active Directory tramite la console di amministrazione di Enforce Server.

Vedere ["Impostazione della configurazione dell'autenticazione SAML"](#) a pagina 138.

Impostazione della configurazione dell'autenticazione SAML

Ottenere informazioni su IDP, come la sua scelta dei metodi di autenticazione, gli identificatori dell'utente disponibili, gli attributi dell'utente disponibili e i metadati del provider di servizi richiesti.

Aprire `[directory di installazione]/Protect/tomcat/webapps/ProtectManager/WEB-INF/` e impostare la proprietà `entityBaseURL` sull'URL di Enforce: `https://<nome host o IP>/ProtectManager`.

Nota: A meno che non si desideri solo accedere alla console di amministrazione di Enforce Server dal computer host, non utilizzare `localhost` come nome host.

Impostare il valore della proprietà `"nameID"` modificando il valore `property name ="nameID"` nel file Spring su un identificatore di nome come `emailAddress`, `WindowsDomainQualified` o un altro `nameID` supportato da IDP. Forniamo qui un esempio per l'indirizzo e-mail:

```
<property name="nameID"
value=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" />
```

È possibile utilizzare una combinazione di attributi dell'utente restituiti da IDP per identificare un utente di Data Loss Prevention. In questo caso, è possibile impostare la proprietà `userAttributes`. Ad esempio:

```
<bean id=userLookupService" class="com.vontu.login.spring.VontuSAMLUserDetailsService">
  <!--
    <property name="user Attributes">
      <set>
        <value>UserName</value>
        <value>EmailAddress</value>
        <value>EmployeeID</value>
      </set>
    </property>
```

Generazione o download dei metadati SAML di Enforce (provider di servizi)

Per scaricare i metadati SAML di Enforce

- 1 Riavviare Enforce Server.
- 2 Accedere come amministratore utilizzando l'URL bypass. A questo URL bypass si accede direttamente: non è necessario accedere alla console di amministrazione di Enforce Server.
- 3 Accedere a **Sistema > Impostazioni > Generale** e andare alla sezione **Autenticazione utente DLP**.
- 4 Fare clic sul collegamento a destra di **Il file di configurazione SAML per l'IDP si trova in** per scaricare i metadati.

Vedere ["Configurare Enforce Server come provider di servizi SAML in IDP \(creare un'applicazione nel provider di identità\)"](#) a pagina 139.

Configurare Enforce Server come provider di servizi SAML in IDP (creare un'applicazione nel provider di identità)

Questi passaggi variano a seconda dell'IDP utilizzato. Questa è una rapida panoramica della procedura se si utilizza Symantec VIP Access Manager come IDP:

Per configurare Enforce Server come provider di servizi SAML in IDP creare un'applicazione

- 1 Accedere come amministratore alla console di amministrazione di VIP Access Manager.
- 2 Fare clic su un modello generico.

- 3 Dare un nome al connettore.
- 4 Selezionare la politica dell'accesso come SSO (Single Sign-On).
- 5 Configurare il portale selezionando un'icona per il sito (questa icona compare sul dashboard del provider di identità).
- 6 Caricare i metadati di Enforce Server.

Vedere ["Esportazione dei metadati IDP in DLP"](#) a pagina 140.

Esportazione dei metadati IDP in DLP

Scaricare i metadati IDP e sostituire il contenuto del file `idp-metadata.xml` in `<installdirectory>/Protect/tomcat/webapps/ProtectManager/security/idp-metadata.xml` con i metadati IDP scaricati.

Vedere ["Configurazione dell'autenticazione di Active Directory"](#) a pagina 140.

Configurazione dell'autenticazione di Active Directory

Se il file modello copiato è per l'autenticazione Kerberos/Active Directory, aprire `<InstallDirectory>/Protect/tomcat/webapps/ProtectManager/WEB-INF/springSecurityContext.xml` in un editor di testo. Questo è il file `springSecurityContext-Kerberos.xml` precedentemente rinominato `springSecurityContext.xml`. Impostare il valore `krbConfLocation` sul file di autenticazione Kerberos. Ad esempio:

```
<!-- Set krbConfLocation in System prooperties -->
<bean class="org.springframework.security.kerberos.authentication.sun.
GlobalJunJaasKerberosConfig">
    <!-- krb5 configuration file location.
    For example C:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Pro
    or
    /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config/krb5.conf on L
    -->
    property name="krbConfLocation" value="C:\Program Files\Symantec\Data Loss Prevent
    \config\krb5.ini"/>
</bean>
```

Vedere ["Impostazione e configurazione del metodo di autenticazione"](#) a pagina 137.

Vedere ["Configurazione dell'autenticazione basata su moduli"](#) a pagina 141.

Vedere ["Integrazione di Active Directory per autenticazione utente"](#) a pagina 141.

Configurazione dell'autenticazione basata su moduli

Dopo aver copiato il file di modello per l'autenticazione basata su moduli, non ci sono impostazioni aggiuntive da configurare.

Vedere ["Configurazione dell'autenticazione del certificato"](#) a pagina 141.

Configurazione dell'autenticazione del certificato

Dopo aver copiato il file di modello per l'autenticazione basata sul certificato client, andare al file `<Directory di installazione>/Protect/tomcat/config/server.xml` e impostare il valore `client auth` su `want` o `true`.

Vedere ["Generazione o download dei metadati SAML di Enforce \(provider di servizi\)"](#) a pagina 139.

Integrazione di Active Directory per autenticazione utente

È possibile configurare Enforce Server per utilizzare Microsoft Active Directory per l'autenticazione utente.

Dopo essere passati all'autenticazione Active Directory, è necessario definire gli utenti nella console di amministrazione di Enforce Server. Se i nomi utente immessi nella console di amministrazione corrispondono agli utenti Active Directory, il sistema associa ogni nuovo account utente alle password Active Directory. È possibile passare all'autenticazione Active Directory dopo la creazione di account utente nel sistema. Solo i nomi utente esistenti che corrispondono ai nomi utente Active Directory rimangono validi dopo il passaggio.

Gli utenti devono utilizzare le password Active Directory all'accesso. Si noti che tutti i nomi utente Symantec Data Loss Prevention fanno distinzione tra maiuscole e minuscole, anche se i nomi utente Active Directory non lo fanno. È possibile passare all'autenticazione Active Directory dopo la creazione di nomi utente in Symantec Data Loss Prevention. Tuttavia, gli utenti devono ancora utilizzare il nome utente Symantec Data Loss Prevention con distinzione maiuscole/minuscole all'accesso.

Per utilizzare l'autenticazione Active Directory

- 1 Verificare che l'host Enforce Server sia sincronizzato con orario con il server Active Directory.

Nota: Assicurarsi che l'orologio nell'host Active Directory sia sincronizzato con uno scarto di massimo cinque minuti con l'orologio dell'host Enforce Server.

- 2 (Solo Linux) Assicurarsi che i seguenti RPM Red Hat siano installati sull'host Enforce Server:
 - `krb5-workstation`
 - `krb5-libs`
 - `pam_krb5`
- 3 Creare il file di configurazione `krb5.ini` (o `krb5.conf` per Linux) che offre a Enforce Server informazioni sulla struttura di dominio Active Directory e gli indirizzi server Active Directory.
Vedere ["Creazione del file di configurazione per l'integrazione con Active Directory"](#) a pagina 142.
- 4 Confermare che Enforce Server possa comunicare con il server Active Directory.
Vedere ["Verifica della connessione di Active Directory"](#) a pagina 144.
- 5 Configurare Symantec Data Loss Prevention per utilizzare l'autenticazione Active Directory.

Creazione del file di configurazione per l'integrazione con Active Directory

È necessario creare un file di configurazione `krb5.ini` (o `krb5.conf` su Linux) per fornire a Symantec Data Loss Prevention informazioni sulla struttura dei domini Active Directory e sulla posizione dei server. Questo passaggio è necessario se sono presenti più domini Active Directory. Tuttavia, anche se la struttura di Active Directory comprende solo un dominio, è comunque raccomandato di creare questo file. L'utilità `kinit` usa questo file per confermare che Symantec Data Loss Prevention può comunicare con il server di Active Directory.

Nota: Se si esegue Symantec Data Loss Prevention su Linux, verificare il collegamento di Active Directory utilizzando l'utilità `kinit`. È necessario rinominare il file `krb5.ini` in `krb5.conf`. L'utilità `kinit` richiede che il file sia nominato `krb5.conf` su Linux. Symantec Data Loss Prevention suppone che si utilizzi `kinit` per verificare il collegamento di Active Directory e indica di rinominare il file in `krb5.conf`.

Symantec Data Loss Prevention fornisce un file `krb5.ini` di esempio che è possibile modificare per l'utilizzo con il sistema in uso. Il file di esempio è memorizzato in `SymantecDLP\Protect\config` (ad esempio, `\Program Files\Symantec\Data Loss Prevention\Enforce Server\Protect\config` su Windows o `/opt/Symantec/DataLossPrevention/Protect/config` su Linux). Se si esegue Symantec Data Loss Prevention su Linux, Symantec raccomanda di rinominare il file in `krb5.conf`. Il file di esempio, che è diviso in due sezioni, ha questo aspetto:

```
[libdefaults]
    default_realm = TEST.LAB
[realms]
    ENG.COMPANY.COM = {
        kdc = engAD.eng.company.com
    }
    MARK.COMPANY.COM = {
        kdc = markAD.eng.company.com
    }
    QA.COMPANY.COM = {
        kdc = qaAD.eng.company.com
    }
```

La sezione `[libdefaults]` identifica il dominio predefinito. Le aree di autenticazione Kerberos corrispondono ai domini di Active Directory. La sezione `[realms]` definisce un server di Active Directory per ogni dominio. Nell'esempio precedente, il server di Active Directory per `ENG.COMPANY.COM` è `engAD.eng.company.com`.

Per creare il file `krb5.ini` o `krb5.conf`

- 1 Accedere a `SymantecDLP\Protect\config` e individuare il file di esempio `krb5.ini`. Ad esempio, individuare il file in `\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (su Windows) o `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config` (su Linux).
- 2 Copiare il file di esempio `krb5.ini` nella directory `c:\windows` (su Windows) o nella directory `/etc` (su Linux). Se si esegue Symantec Data Loss Prevention su Linux, pianificare una verifica del collegamento di Active Directory utilizzando lo strumento da riga di comando `kinit`. Rinominare il file in `krb5.conf`.

Vedere ["Verifica della connessione di Active Directory"](#) a pagina 144.

- 3 Aprire il file `krb5.ini` o `krb5.conf` in un editor di testo.

- 4 Sostituire il valore di esempio `default_realm` con il nome completo del dominio predefinito. (Il valore per `default_realm` deve essere tutto in lettere maiuscole.) Ad esempio, modificare il valore in modo che abbia l'aspetto seguente:

```
default_realm = MYDOMAIN.LAB
```

- 5 Sostituire gli altri nomi di dominio di esempio con i nomi dei domini reali. I nomi di dominio devono essere tutti in lettere maiuscole. Ad esempio, sostituire `ENG.COMPANY.COM` con `ADOMAIN.COMPANY.COM`.
- 6 Sostituire i valori di esempio `kdc` con i nomi host o gli indirizzi IP dei server Active Directory. Assicurarsi di seguire il formato specificato, in cui le parentesi aperte sono seguite immediatamente da un'interruzione di riga. Ad esempio, sostituire `engAD.eng.company.com` con `ADserver.eng.company.com` e così via.
- 7 Rimuovere tutte le voci `kdc` inutilizzate dal file di configurazione. Ad esempio, se sono presenti solo due domini oltre a quello predefinito, eliminare la voce `kdc` inutilizzata.
- 8 Salvare il file.

Verifica della connessione di Active Directory

`kinit` è uno strumento da riga di comando che è possibile utilizzare per confermare che il server di Active Directory risponde alle richieste. Inoltre verifica che Enforce Server abbia accesso al server di Active Directory. Per le installazioni Microsoft Windows, l'utilità viene installata dal programma di installazione Symantec Data Loss Prevention nella directory `C:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\jre\bin`. Per le installazioni Linux, l'utilità fa parte della distribuzione di Red Hat Enterprise Linux e si trova nella seguente posizione: `/usr/kerberos/bin/kinit`. È anche possibile scaricare Java SE 6 e individuare lo strumento `kinit` in `\java_home\jdk1.6.0\bin`.

Se si esegue Enforce Server su Linux, utilizzare l'utilità `kinit` per verificare l'accesso daa Enforce Server al server di Active Directory. Rinominare il file `krb5.ini` in `krb5.conf`. L'utilità `kinit` richiede che il file sia nominato `krb5.conf` su Linux.

Per verificare la connessione al server Active Directory

- 1 Sull'host di Enforce Server, accedere alla riga di comando e passare alla directory in cui si trova `kinit`.
- 2 Scrivere un comando `kinit` utilizzando un nome utente e una password noti come parametri. La password è visibile in chiaro quando la si digita nella riga di comando. Ad esempio, scrivere quanto segue:

```
kinit kchatterjee mypwd10#
```

La prima volta che si contatta Active Directory, potrebbe verificarsi un errore per il quale non è possibile trovare il file `krb5.conf` o `krb5.ini` nella posizione prevista. In Windows, l'errore ha un aspetto simile al seguente:

```
krb_error 0 Could not load configuration file c:\winnt\krb5.ini  

(The system cannot find the file specified) No error.
```

In questo caso, copiare il file `krb5.conf` o `krb5.ini` nella posizione prevista ed eseguire nuovamente il comando `kinit` indicato sopra.

- 3 A seconda della risposta del server di Active Directory al comando, effettuare una delle seguenti azioni:
 - Se il server di Active Directory indica di aver creato correttamente un ticket Kerberos, continuare a configurare Symantec Data Loss Prevention.
 - Se viene visualizzato un messaggio di errore, rivolgersi all'amministratore di Active Directory.

Informazioni sulla configurazione dell'autenticazione del certificato

L'autenticazione del certificato consente a un utente di connettersi automaticamente alla console di amministrazione di Enforce Server mediante un certificato client generato dall'infrastruttura a chiave pubblica (PKI). Quando un utente accede alla console di amministrazione di Enforce Server, l'infrastruttura PKI consegna automaticamente il certificato dell'utente al contenitore Tomcat che ospita la console di amministrazione. Il contenitore Tomcat convalida il certificato client mediante le autorità di certificazione configurate nell'archivio Attendibilità Tomcat.

Il certificato client viene consegnato al computer Enforce Server quando un browser del client esegue l'handshake con Enforce Server. Ad esempio, alcuni browser potrebbero essere configurati per funzionare con un lettore di smart card per la presentazione del certificato. In alternativa, è possibile caricare il certificato X.509 in un browser e configurare il browser per l'invio del certificato a Enforce Server.

Se il certificato è valido, la console di amministrazione di Enforce Server può anche determinare se il certificato è stato revocato.

Vedere ["Informazioni sui controlli di revoca dei certificati"](#) a pagina 153.

Se il certificato è valido, Enforce Server utilizza il nome comune (CN) del certificato per determinare se tale CN è mappato su un account utente attivo con un ruolo nella configurazione di Enforce Server.

Nota: Alcuni browser inseriscono nella cache il certificato client di un utente e fanno accedere automaticamente l'utente alla console di amministrazione dopo che l'utente ha scelto di disconnettersi. In questo caso, per completare il processo di disconnessione gli utenti devono chiudere la finestra del browser.

La seguente tabella descrive i passaggi necessari per usare l'autenticazione del certificato con Symantec Data Loss Prevention.

Tabella 5-4 Procedura per la configurazione dell'autenticazione del certificato

Fase	Azione	Descrizione
1	Attivare l'autenticazione del certificato sul computer Enforce Server.	È possibile configurare un Enforce Server esistente per consentire l'autenticazione. Enforce Server applica per impostazione predefinita l'autenticazione basata su moduli. Vedere "Configurazione dell'autenticazione del certificato per la console di amministrazione di Enforce Server" a pagina 147.
2	Aggiungere i certificati dell'autorità di certificazione (CA) per impostare la catena di attendibilità.	È possibile aggiungere i certificati CA all'archivio Attendibilità Tomcat con l'utilità <code>keytool</code> di Java per aggiungere manualmente i certificati a un'istanza di Enforce Server esistente. Vedere "Aggiunta di certificati dell'autorità di certificazione (CA) all'archivio Attendibilità Tomcat" a pagina 149.
3	(Facoltativo) Cambiare la password dell'archivio Attendibilità Tomcat.	Il programma di installazione di Symantec Data Loss Prevention configura ogni nuova installazione di Enforce Server con una password predefinita dell'archivio Attendibilità Tomcat. Seguire queste istruzioni per configurare una password sicura. Vedere "Modifica della password dell'archivio Attendibilità Tomcat" a pagina 151.

Fase	Azione	Descrizione
4	Mappare i valori nome comune certificato (CN) su account utente Enforce Server.	Vedere "Mapping dei valori di nome comune (CN) agli account utente di Symantec Data Loss Prevention" a pagina 152.
5	Configurare Enforce Server per il controllo della revoca del certificato.	Vedere "Informazioni sui controlli di revoca dei certificati" a pagina 153.
6	Verificare l'accesso a Enforce Server mediante un accesso Single Sign-On basato sul certificato.	Vedere "Risoluzione dei problemi di autenticazione del certificato" a pagina 159.
7	(Facoltativo) Disattivare l'accesso basato sui moduli.	Per utilizzare l'accesso Single Sign-On basato sul certificato per tutti gli accessi a Enforce Server, disattivare l'accesso basato sui moduli. Vedere "Disattivazione dell'autenticazione tramite password e dell'accesso basato sui moduli" a pagina 160.

Configurazione dell'autenticazione del certificato per la console di amministrazione di Enforce Server

L'autenticazione basata su moduli è disponibile per impostazione predefinita in Enforce Server. È necessario aggiungere manualmente l'autenticazione del certificato. Seguire questa procedura per attivare manualmente l'autenticazione basata su modulo e certificato in un'installazione di Symantec Data Loss Prevention.

Per attivare l'autenticazione basata su moduli e certificato per gli utenti della console di amministrazione di Enforce Server

- 1 Accedere al computer con Enforce Server utilizzando l'account creato durante l'installazione di Symantec Data Loss Prevention.

Nota: Non modificare le autorizzazioni o l'appartenenza di qualsiasi file di configurazione di un altro account radice o di amministratore.

- 2 Copiare il file corrispondente `springSecurityContext.xml` nella directory WEB-INF di Tomcat.
- 3 Aprire il file `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\tomcat\conf\server.xml` (Windows) o `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/tomcat/conf/server.xml` (Linux) e cambiare il valore di `ClientAuth` da `false` a `want`. Salvare il file.

- 4 Riavviare Enforce Server. Questa modifica al file `server.xml` modificato al precedente passaggio seleziona la casella di controllo **Usa autenticazione del certificato** nell'interfaccia utente della console di amministrazione di Enforce Server.
- 5 Accedere alla console di amministrazione di Enforce Server e andare a **Sistema > Gestione accesso > Utenti DLP**.
- 6 Selezionare **Usa autenticazione del certificato** e indicare il mapping CN corrispondente.
- 7 Aggiungere i certificati CA all'archivio attendibilità Tomcat utilizzando l'utilità keytool di Java.

Vedere ["Aggiunta di certificati dell'autorità di certificazione \(CA\) all'archivio Attendibilità Tomcat"](#) a pagina 149.

Assicurarsi di avere installato tutti i certificati necessari e che gli utenti possano accedere con l'autenticazione del certificato.

- 8 Ora l'utente dispone dell'autenticazione basata su moduli e su certificato.

[Informazioni sui controlli di revoca dei certificati](#)

Seguire questa procedura per attivare l'autenticazione del certificato in Symantec Data Loss Prevention.

Per attivare l'autenticazione del certificato per gli utenti della console di amministrazione di Enforce Server

- 1 Accedere al computer con Enforce Server utilizzando l'account creato durante l'installazione di Symantec Data Loss Prevention.

Nota: Non modificare le autorizzazioni o l'appartenenza di qualsiasi file di configurazione di un altro account radice o di amministratore.

- 2 Copiare il file corrispondente `springSecurityContext.xml` nella directory WEB-INF di Tomcat.
- 3 Aprire il file `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\tomcat\conf\server.xml` (Windows) o `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/tomcat/conf/server.xml` (Linux) e cambiare il valore di `ClientAuth` da `false` a `true`. Salvare il file.
- 4 Riavviare Enforce Server. Questa modifica al file `server.xml` modificato al precedente passaggio seleziona la casella di controllo **Usa autenticazione del certificato** nell'interfaccia utente della console di amministrazione di Enforce Server.
- 5 Accedere alla console di amministrazione di Enforce Server e andare a **Sistema > Gestione accesso > Utenti DLP**.

- 6 Selezionare **Usa autenticazione del certificato** e indicare il mapping **Nome comune (CN)** corrispondente.

- 7 Aggiungere i certificati CA all'archivio attendibilità Tomcat utilizzando l'utilità keytool di Java.

Vedere ["Aggiunta di certificati dell'autorità di certificazione \(CA\) all'archivio Attendibilità Tomcat"](#) a pagina 149.

Assicurarsi di avere installato tutti i certificati necessari e che gli utenti possano accedere con l'autenticazione del certificato.

- 8 Solo per l'autenticazione del client, copiare il file
`springSecurityContext-Certificate.xml` da `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\tomcat\webapps\ProtectManager\security\template` (Windows)
 o `opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/tomcat/webapps/ProtectManager/WEB-INF` (Linux) e rinominarlo in `springSecurityContext.xml`.

- 9 Aprire il file `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\tomcat\conf\server.xml` (Windows) o
`/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/tomcat/conf/server.xml` e cambiare il valore di `ClientAuth` da `want` a `true`.

Riavviare Enforce Server.

Ora l'utente dispone solamente dell'autenticazione basata su certificato.

Vedere ["Aggiunta di certificati dell'autorità di certificazione \(CA\) all'archivio Attendibilità Tomcat"](#) a pagina 149.

Aggiunta di certificati dell'autorità di certificazione (CA) all'archivio Attendibilità Tomcat

Per usare l'autenticazione del certificato con Symantec Data Loss Prevention è necessario aggiungere all'archivio Attendibilità Tomcat tutti i certificati CA richiesti per l'autenticazione degli utenti nel sistema. Per Symantec Data Loss Prevention 15.0 e versioni successive, è possibile importare i certificati CA in Enforce Server solo utilizzando l'utilità keytool di Java. Ciascun certificato X.509 va fornito in formato Distinguished Encoding Rules (DER) in un file `.cer`. Se per la catena di certificati sono necessarie più autorità di certificazione, è necessario aggiungere più file `.cer`.

Per aggiungere certificati CA all'archivio Attendibilità Tomcat

- 1 Accedere al computer con Enforce Server utilizzando l'account creato durante l'installazione di Symantec Data Loss Prevention.

Nota: Non modificare le autorizzazioni o l'appartenenza di qualsiasi file di configurazione di un altro account radice o di amministratore.

- 2 Passare alla directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/tomcat/conf` (Linux) o `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\tomcat\conf` (Windows). Se Symantec Data Loss Prevention è stato installato in una directory differente, sostituire il percorso corretto.
- 3 Copiare tutti i file di certificato (file `.cer`) che si desidera importare nella directory `conf` sul computer Enforce Server.
- 4 Mediante l'utilità `keytool` installata con Symantec Data Loss Prevention aggiungere un certificato all'archivio attendibilità Tomcat. Per i sistemi Windows, immettere:

```
c:\Program Files\Symantec\Data Loss Prevention\Enforce Server\jre\bin\keytool -import -trustcacerts
    -alias CA_CERT_1
    -file certificate_1.cer
    -keystore .\truststore.jks
```

Per i sistemi Linux, immettere:

```
/opt/Symantec/DataLossPrevention/jre/bin/keytool -import -trustcacerts
    -alias CA_CERT_1
    -file certificate_1.cer
    -keystore ./truststore.jks
```

Nei questi comandi, sostituire `CA_CERT_1` con un alias unico corrispondente al certificato che si importa. Sostituire a `certificate_1.cer` il nome del file certificato copiato nel computer Enforce Server.

- 5 Immettere la password nell'archivio chiavi quando l'utilità `keytool` la richiede. La password predefinita dell'archivio chiavi è `protect`.
- 6 Ripetere questi passaggi per installare tutti i file di certificato necessari per completare la catena di certificati.
- 7 Interrompere e riavviare il servizio Symantec DLP Manager per applicare le modifiche.
- 8 Se non è stata ancora modificata la password predefinita dell'archivio chiavi Tomcat, modificarla ora.

Vedere ["Modifica della password dell'archivio Attendibilità Tomcat"](#) a pagina 151.

Modifica della password dell'archivio Attendibilità Tomcat

Quando si installa Symantec Data Loss Prevention, l'archivio Attendibilità Tomcat usa `protect` come password predefinita. Attenersi alla seguente procedura per assegnare una password sicura all'archivio Attendibilità Tomcat quando si utilizza l'autenticazione del certificato.

Per cambiare la password dell'archivio Attendibilità Tomcat

- 1 Accedere al computer con Enforce Server utilizzando l'account creato durante l'installazione di Symantec Data Loss Prevention.

Nota: Non modificare le autorizzazioni o l'appartenenza di qualsiasi file di configurazione di un altro account radice o di amministratore.

- 2 Passare alla directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/tomcat/conf` (Linux) o `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\tomcat\conf` (Windows). Se Symantec Data Loss Prevention è stato installato in una directory differente, sostituire il percorso corretto.
- 3 Utilizzare l'utilità `keytool` installata con Symantec Data Loss Prevention per cambiare la password dell'archivio Attendibilità Tomcat. Per i sistemi Windows, immettere:

```
c:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\jre\bin\keytool -storepasswd
-new new_password -keystore ./truststore.jks
```

Per i sistemi Linux, immettere:

```
/opt/Symantec/DataLossPrevention/Enforce Server/15.1/jre/bin/keytool -storepasswd
-new new_password -keystore ./truststore.jks
```

Sostituire `new_password` con una password sicura.

- 4 Immettere la password corrente nell'archivio chiavi quando l'utilità `keytool` richiede di eseguire questa operazione. La password predefinita è `protect`.
- 5 Passare alla directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/tomcat/conf` (Linux) o `c:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\tomcat\conf` (Windows) directory. Se Symantec Data Loss Prevention è stato installato in una directory differente, sostituire il percorso corretto.
- 6 Aprire il file `server.xml` con un editor di testo.

- 7 Nella seguente linea del file, modificare la voce `truststorePass="protect"` per specificare la nuova password:

```
<Connector URIEncoding="UTF-8" acceptCount="100" clientAuth="want"
debug="0" disableUploadTimeout="true" enableLookups="false"
keystoreFile="conf/.keystore" keystorePass="protect"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25"
port="443" scheme="https" secure="true" sslProtocol="TLS"
truststoreFile="conf/truststore.jks" truststorePass="protect"/>
```

Sostituire *protect* con la nuova password definita nel comando `keytool`.

- 8 Salvare le modifiche e uscire dall'editor di testo.
- 9 Passare alla directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config` (**Linux**) o `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (**Windows**). Se Symantec Data Loss Prevention è stato installato in una directory differente, sostituire il percorso corretto.
- 10 Aprire il file `Manager.properties` con un editor di testo.

Aggiungere la seguente riga nel file per specificare la nuova password:

```
com.vontu.manager.tomcat.truststore.password = password
```

Sostituire *password* con la nuova password. Non racchiudere la password tra virgolette.

- 11 Salvare le modifiche e uscire dall'editor di testo.
- 12 Aprire il file `server.xml` con un editor di testo.
- 13 Modificare (o, se non presente, aggiungere) la seguente riga nel file per specificare la nuova password:

```
com.vontu.manager.tomcat.truststore.password = password
```

Sostituire *password* con la nuova password. Non racchiudere la password tra virgolette.

- 14 Salvare le modifiche e uscire dall'editor di testo.
- 15 Interrompere e riavviare il servizio Symantec DLP Manager per applicare le modifiche.

Mapping dei valori di nome comune (CN) agli account utente di Symantec Data Loss Prevention

Ogni utente che accede alla console di amministrazione di Enforce Server con il Single Sign-On basato sul certificato deve disporre di un account utente attivo nella configurazione di Enforce Server. L'account utente associa il valore di nome comune (CN) del certificato client dell'utente a uno o più ruoli nella console di amministrazione di Enforce Server. È possibile mappare un valore CN a un solo account utente di Enforce Server.

L'account utente creato non richiede una password separata per la console di amministrazione di Enforce Server. È possibile configurare facoltativamente una password se si desidera consentire all'utente di accedere anche dalla pagina di accesso della console di amministrazione di Enforce Server. Se si attiva l'autenticazione tramite password e l'utente non fornisce un certificato quando il browser ne richiede uno, viene visualizzata la pagina di accesso di Enforce Server. Se l'autenticazione tramite password è disattivata e l'utente non fornisce un certificato si verifica un errore di accesso.

Per eseguire l'accesso utilizzando il Single Sign-On con l'autenticazione del certificato, un account utente attivo deve identificare il valore CN dell'utente e deve avere un ruolo valido assegnato in Enforce Server. Se si desidera impedire a un utente di accedere alla console di amministrazione di Enforce Server senza revocare il certificato client dell'utente, disattivare o eliminare l'account utente di Enforce Server associato.

Vedere ["Configurazione degli account utente"](#) a pagina 123.

Informazioni sui controlli di revoca dei certificati

Durante la gestione dell'infrastruttura a chiave pubblica può essere necessario revocare il certificato di un client con la CA. Ad esempio è possibile che occorra revocare un certificato se un dipendente lascia la società o se le credenziali di un dipendente vanno perse o vengono rubate. Quando si revoca un certificato, la CA utilizza uno o più elenchi di certificati revocati (CRL) per pubblicare i certificati che non sono più validi. Symantec Data Loss Prevention supporta inoltre l'utilizzo di un risponditore OCSP (Online Certificate Status Protocol, protocollo di stato del certificato in linea), che i clienti possono usare per determinare se un dato certificato è stato revocato. Il risponditore OCSP può essere implementato come servizio sul server CA o come server OCSP separato.

Nota: Per impostazione predefinita, il controllo della revoca dei certificati è disattivato. È necessario attivarlo e configurarlo. Vedere ["Configurazione dei controlli di revoca dei certificati"](#) a pagina 155.

OCSP è il primo meccanismo che Symantec Data Loss Prevention utilizza per eseguire i controlli di revoca dei certificati. Dopo che il contenitore Tomcat ha stabilito che un certificato client è valido, Enforce Server invia una richiesta OCSP a un risponditore OCSP designato per determinare se il certificato è stato revocato. Le informazioni utilizzate per contattare il risponditore OCSP possono venire fornite in due modi diversi:

- Mediante il campo di accesso alle informazioni di autorità (AIA) in un certificato client. Il certificato client può includere l'URL del risponditore OCSP in un campo AIA. Di seguito è riportato un esempio di un campo AIA che definisce un risponditore OCSP:

```
[1]Authority Info Access Access Method=On-line
Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
Alternative Name: URL=http://my_ocsp_responder
```

Questo metodo viene comunemente utilizzato quando si configura una CA interna in modo che fornisca il servizio di risponditore OCSP. Se il risponditore OCSP specificato nel campo AIA è direttamente accessibile dal computer con Enforce Server, non è necessaria alcuna configurazione aggiuntiva per eseguire i controlli di revoca. Tuttavia, se il risponditore OCSP è accessibile solo da un server proxy, è necessario configurare le impostazioni del server proxy nella configurazione di Symantec Data Loss Prevention.

- Mediante il file di configurazione OCSP. In alternativa è possibile configurare manualmente le proprietà del risponditore OCSP con il file di configurazione `manager-certauth.security`. Se si sceglie di utilizzare questo file, la configurazione nel file ignora eventuali informazioni presenti nel campo AIA di un certificato client. Questo metodo viene comunemente utilizzato se si desidera usare un risponditore OCSP locale invece di quello specificato nel campo AIA o se i certificati client non includono un campo AIA.

Vedere ["Configurazione manuale delle proprietà del risponditore OCSP"](#) a pagina 158.

Nota: se il risponditore OCSP configurato in questo file non utilizza il certificato CA per firmare le risposte, è necessario aggiungere il certificato del risponditore OCSP all'archivio attendibilità Tomcat.

Vedere ["Aggiunta di certificati dell'autorità di certificazione \(CA\) all'archivio Attendibilità Tomcat"](#) a pagina 149.

Se lo stato di revoca di un certificato non può essere determinato con OCSP, Symantec Data Loss Prevention recupera gli elenchi di revoca da un CRLDP (Certificate Revocation List Distribution Point, punto di distribuzione dell'elenco di certificati evocati). Per controllare la revoca con un CRLDP, il certificato client deve includere un campo del punto di distribuzione CRL. Di seguito è riportata una definizione del campo CRDLP di esempio:

```
[1]CRL Distribution Point
Distribution Point Name:
Full Name: URL=http://my_crl_dp
```

Nota: Symantec Data Loss Prevention non supporta la definizione di CRLDP con un URL LDAP.

Se il punto di distribuzione CRL è definito in ogni certificato ed Enforce Server può accedere direttamente al server, non è necessaria alcuna configurazione aggiuntiva per eseguire i controlli di revoca. Se il punto di distribuzione CRL è accessibile solo da un server proxy, è

necessario configurare le impostazioni del server proxy nella configurazione di Symantec Data Loss Prevention.

Vedere ["Accesso al responder OCSP o CRLDP mediante un proxy"](#) a pagina 157.

Indipendentemente dal metodo di controllo di revoca utilizzato, è necessario attivare i controlli di revoca dei certificati sul computer con Enforce Server. I controlli di verifica dei certificati sono attivati per impostazione predefinita se si seleziona l'installazione del certificato durante l'installazione di Enforce Server. Se si è aggiornata un'installazione di Symantec Data Loss Prevention esistente, la revoca del certificato non è attivata per impostazione predefinita.

Vedere ["Configurazione dei controlli di revoca dei certificati"](#) a pagina 155.

Se il computer con Enforce Server deve utilizzare un proxy per accedere al servizio di risponditore OCSP, è necessario configurare le impostazioni proxy sul computer con Enforce Server.

Vedere ["Accesso al responder OCSP o CRLDP mediante un proxy"](#) a pagina 157.

Se si sta utilizzando OCSP per i controlli di revoca, ma i campi AIA del certificato client non specificano un risponditore OCSP valido, è necessario configurare manualmente le proprietà del risponditore OCSP nel file di configurazione `manager-certauth.security`.

Vedere ["Configurazione manuale delle proprietà del risponditore OCSP"](#) a pagina 158.

Configurazione dei controlli di revoca dei certificati

Quando si attivano i controlli di revoca dei certificati, Symantec Data Loss Prevention usa OCSP per determinare se ciascun certificato client è stato revocato dall'autorità di certificazione. Se lo stato del certificato non può essere determinato con OCSP, Symantec Data Loss Prevention usa un CRLDP per determinare lo stato di revoca.

Seguire questa procedura per attivare i controlli di revoca dei certificati.

Per configurare i controlli di revoca dei certificati

- 1 Verificare che il risponditore OCSP sia configurato nel campo AIA di ogni certificato o nel file `manager-certauth.security`.
Vedere ["Informazioni sui controlli di revoca dei certificati"](#) a pagina 153.
Vedere ["Configurazione manuale delle proprietà del risponditore OCSP"](#) a pagina 158.
- 2 Verificare che il CRLDP sia definito nel campo del punto di distribuzione CRL di ciascun certificato client.
- 3 Accedere al computer con Enforce Server utilizzando l'account creato durante l'installazione di Symantec Data Loss Prevention.

Nota: Non modificare le autorizzazioni o l'appartenenza di qualsiasi file di configurazione di un altro account radice o di amministratore.

- 4 Passare alla directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config (Linux)` o `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config (Windows)`. Se Symantec Data Loss Prevention è stato installato in una directory differente, sostituire il percorso corretto.
- 5 Aprire il file `SymantecDLPManager.conf` con un editor di testo.
- 6 Per consentire i controlli di revoca certificati aggiungere o modificare la seguente riga del file:

```
wrapper.java.additional.19=-Dcom.sun.net.ssl.checkRevocation=true
```

Per disattivare le verifiche, impostare il valore su `false`.

- 7 Per configurare manualmente il server risponditore OCSP, anziché utilizzare il campo AIA nei certificati client, modificare la seguente riga del file:

```
wrapper.java.additional.20=-Djava.security.properties=../config/manager-certauth.security
```

Attivare tale riga del file anche per disattivare i controlli di revoca OCSP. È quindi possibile configurare una proprietà in `manager-certauth.security` per disattivare le verifiche OCSP.

Verificare che il parametro di configurazione indichi il file di configurazione OCSP specificato. Modificare sempre il file `manager-certauth.security` esistente anziché creare un nuovo file.

Vedere "[Configurazione manuale delle proprietà del risponditore OCSP](#)" a pagina 158.

- 8 Per consentire il controllo di revoca mediante CRLDP, aggiungere la seguente riga nel file o eliminare il commento alla riga per attivarla:

```
wrapper.java.additional.22=-Dcom.sun.security.enableCRLDP=true
```

Questa opzione è attivata per impostazione predefinita nelle nuove installazioni di Symantec Data Loss Prevention.

- 9 Se si utilizzano i controlli di revoca CRLDP, facoltativamente è possibile configurare la durata della cache mediante la proprietà:

```
wrapper.java.additional.22=-Dsun.security.certpath.ldap.cache.lifetime=30
```

Questo parametro specifica la durata in secondi nella cache degli elenchi di revoca ottenuti da un punto di distribuzione CRL. Una volta trascorso tale tempo, alla successiva richiesta di autenticazione viene eseguita una ricerca per aggiornare la cache. La durata nella cache predefinita è pari a 30 secondi. Specificare 0 per disattivare la cache o -1 per archiviare indefinitamente i risultati della cache.

- 10 Interrompere e riavviare il servizio Symantec DLP Manager per applicare le modifiche.

Accesso al responder OCSP o CRLDP mediante un proxy

Symantec consiglia di consentire l'accesso diretto dal computer Enforce Server a tutti i server responder OCSP e ai server CRLDP necessari per eseguire i controlli di revoca dei certificati. Se il risponditore OCSP o i server CRLDP sono accessibili solo mediante un proxy, è necessario configurare le impostazioni proxy sul computer Enforce Server.

Quando si configura un proxy, Enforce Server utilizza la configurazione proxy per tutte le connessioni HTTP, ad esempio per le connessioni create per la connessione a un server Data Insight per il recupero di certificati. Verificare con l'amministratore proxy prima di configurare queste impostazioni proxy e considerare la possibilità di consentire l'accesso diretto ai server CRDLP e OCSP ove possibile.

Per configurare le impostazioni proxy per un responder OCSP o un server CRLDP

- 1 Verificare che il risponditore OCSP sia configurato nel campo AIA di ogni certificato. Vedere ["Informazioni sui controlli di revoca dei certificati"](#) a pagina 153.
- 2 Verificare che il CRLDP sia definito nel campo del punto di distribuzione CRL di ciascun certificato client.
- 3 Accedere al computer con Enforce Server utilizzando l'account creato durante l'installazione di Symantec Data Loss Prevention.

Nota: Non modificare le autorizzazioni o l'appartenenza di qualsiasi file di configurazione di un altro account radice o di amministratore.

- 4 Passare alla directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config (Linux)` o `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config (Windows)`. Se Symantec Data Loss Prevention è stato installato in una directory differente, sostituire il percorso corretto.
- 5 Aprire il file `SymantecDLPManager.conf` con un editor di testo.
- 6 Aggiungere o modificare le seguenti proprietà di configurazione per identificare il proxy:

```
wrapper.java.additional.22=-Dhttp.proxyHost=myproxy.mydomain.com
wrapper.java.additional.23=-Dhttp.proxyPort=8080
wrapper.java.additional.24=-Dhttp.nonProxyHosts=hosts
```

Sostituire a *myproxy.mydomain.com* e *8080* il nome host e la porta del server proxy. Sostituire *hosts* con uno o più risponditori OCSP accessibili per l'uso se il proxy non è disponibile. È possibile includere nomi host server, nomi di dominio completi o indirizzi IP separati da un carattere pipe. Ad esempio:

```
wrapper.java.additional.24=-Dhttp.nonProxyHosts=ocsp-server|
127.0.0.1|DataInsight_Server_Host
```

- 7 Salvare le modifiche al file di configurazione.
- 8 Interrompere e riavviare il servizio Symantec DLP Manager per applicare le modifiche.

Configurazione manuale delle proprietà del risponditore OCSP

Facoltativamente è possibile modificare il file `manager-certauth.security` per configurare i parametri di connessione OCSP del sistema. Per impostazione predefinita questo file attiva i controlli OCSP, ma tutte le altre opzioni sono commentate e inattive. Se si rimuove il commento da uno o più parametri del file, tali parametri sovrascrivono la configurazione OCSP presente nei campi AIA di un certificato client.

Vedere ["Informazioni sui controlli di revoca dei certificati"](#) a pagina 153.

Nota: Se il risponditore OCSP configurato in questo file non utilizza il certificato CA per firmare le risposte, sarà necessario aggiungere il certificato del risponditore OCSP all'archivio Attendibilità Tomcat.

Vedere ["Aggiunta di certificati dell'autorità di certificazione \(CA\) all'archivio Attendibilità Tomcat"](#) a pagina 149.

`manager-certauth.security` si trova nella directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config` (Linux) o `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (Windows). Modificare sempre il file `manager-certauth.security` esistente anziché creare un nuovo file. Può risultare utile creare un backup del file prima di effettuare le modifiche per conservare il contenuto originale. `manager-certauth.security` contiene informazioni aggiuntive su questi parametri.

Il file contiene i seguenti parametri.

Tabella 5-5 Parametri di configurazione OCSP

Parametro di configurazione con esempio	Descrizione
<code>ocsp.enable=true</code>	Questo parametro abilita OCSP per i controlli di revoca se la revoca del certificato è abilitata anche nel file <code>SymantecDLPManager.properties</code> . Questo parametro è attivato per impostazione predefinita per tutte le installazioni di Symantec Data Loss Prevention. Disattivare la proprietà se si desidera usare solo i controlli CRLDP anziché i controlli OCSP.
<code>ocsp.responderURL=http://ocsp.example.net:80</code>	Definisce l'URL del risponditore OCSP. Se non si definisce questo parametro, l'URL viene ricavato dal campo AIA nel certificato client, se disponibile.

Parametro di configurazione con esempio	Descrizione
<code>ocsp.responderCertSubjectName=CN=OCSP Responder, O=XYZ Corp</code>	<p>Definisce il nome oggetto del certificato che corrisponde al risponditore OCSP. Per impostazione predefinita, Symantec Data Loss Prevention suppone che il certificato dell'emittente del certificato client corrisponda al certificato del risponditore OCSP. Se non si usa questa configurazione predefinita, è necessario identificare il certificato del risponditore OCSP in un altro modo. È anche necessario aggiungere il certificato del risponditore OCSP all'archivio Attendibilità Tomcat.</p> <p>Vedere "Aggiunta di certificati dell'autorità di certificazione (CA) all'archivio Attendibilità Tomcat" a pagina 149.</p> <p>Se non è possibile identificare esattamente il certificato del risponditore OCSP utilizzando solo il nome oggetto, utilizzare entrambi i parametri <code>ocsp.responderCertIssuerName</code> e <code>ocsp.responderCertSerialNumber</code> anziché <code>ocsp.responderCertSubjectName</code>. Se si definisce <code>ocsp.responderCertSubjectName</code>, gli altri due parametri della tabella vengono ignorati.</p>
<code>ocsp.responderCertIssuerName=CN=Enterprise CA, O=XYZ Corp</code>	<p>Utilizzare questo parametro insieme a <code>ocsp.responderCertSerialNumber</code> per identificare il certificato del risponditore OCSP. Questo parametro definisce l'emittente del certificato del risponditore OCSP.</p> <p>Se si usa questo parametro, evitare di utilizzare anche il parametro <code>ocsp.responderCertSubjectName</code>.</p>
<code>ocsp.responderCertSerialNumber=2A:FF:00</code>	<p>Utilizzare questo parametro insieme a <code>ocsp.responderCertIssuerName</code> per identificare il certificato del risponditore OCSP. Questo parametro definisce il numero di serie del certificato del risponditore OCSP.</p> <p>Se si usa questo parametro, evitare di utilizzare anche il parametro <code>ocsp.responderCertSubjectName</code>.</p>

Risoluzione dei problemi di autenticazione del certificato

Per impostazione predefinita Symantec Data Loss Prevention registra ogni richiesta riuscita di connessione alla console di amministrazione di Enforce Server. Symantec Data Loss Prevention registra inoltre un messaggio di errore se una richiesta di accesso viene effettuata senza fornire un certificato o se un certificato valido presenta un CN non mappabile a un account utente valido nella configurazione di Enforce Server.

Nota: Se l'autenticazione del certificato non riesce mentre il browser stabilisce una connessione HTTPS alla console di amministrazione di Enforce Server, Symantec Data Loss Prevention non è in grado di registrare un messaggio di errore.

È possibile registrare facoltativamente ulteriori informazioni sulle verifiche di revoca certificato aggiungendo o annullando il commento alla seguente proprietà di sistema nel file

`SymantecDLPManager.conf`:

```
wrapper.java.additional.90=-Djava.security.debug=certpath
```

`SymantecDLPManager.conf` si trova nella directory `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (Windows) o `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config` (Linux). Tutti i messaggi di debug sono registrati in `c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs\debug\SymantecDLPManager.log` (Windows) o `/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/debug/SymantecDLPManager.log` (Linux).

Disattivazione dell'autenticazione tramite password e dell'accesso basato sui moduli

L'accesso basato sui moduli con l'autenticazione tramite password può essere utilizzato come meccanismo di accesso di fallback mentre si configura e si testa l'autenticazione del certificato. Dopo aver configurato l'autenticazione del certificato è possibile disattivare l'accesso basato su moduli e l'autenticazione basata su password. L'infrastruttura a chiave pubblica gestisce tutte le richieste di accesso.

Dopo aver configurato il nome comune (CN) con moduli e certificato attivati, è possibile passare al solo certificato sostituendo il file `springSecurityContext.xml` con il file `springSecurityContext-Certificate.xml` e riavviando Enforce Server. L'accesso basato sui moduli viene quindi disattivato completamente.

Nota: La disattivazione dell'accesso basato sui moduli disattiva questa funzionalità per tutti gli utenti, compresi quelli con i privilegi di amministratore. In alternativa è possibile disattivare l'accesso basato sui moduli o l'autenticazione del certificato per un singolo utente mediante la configurazione dell'account di tale utente.

Vedere ["Configurazione degli account utente"](#) a pagina 123.

Se successivamente si attiva l'accesso basato sui moduli, ma per l'account utente dell'amministratore non è configurata una password, è possibile reimpostare la password dell'amministratore. Reimpostare la password utilizzando l'utilità `AdminPasswordReset`.

Vedere ["Reimpostazione della password di amministratore"](#) a pagina 128.

Connessione alle directory di gruppo

Il capitolo contiene i seguenti argomenti:

- [Creazione di connessioni ai server LDAP](#)
- [Configurazione delle connessioni a server di directory](#)
- [Pianificazione dell'indicizzazione del server di directory](#)

Creazione di connessioni ai server LDAP

Symantec Data Loss Prevention supporta connessioni a server di directory conformi a LDAP quali Microsoft Active Directory (AD). Una connessione directory di gruppo specifica come Enforce Server o Discovery Server si connette al server di directory.

La connessione al server di directory deve essere stabilita prima della creazione di gruppi di utenti in Enforce Server. Enforce Server o Discover Server utilizza la connessione per ottenere dettagli relativi ai gruppi. Se la connessione non viene creata non è possibile definire **Gruppi utente**. La connessione non è permanente, ma è possibile configurarla per la sincronizzazione a intervalli specificati. Il server di directory contiene tutte informazioni necessarie per creare i **Gruppi utente**.

Vedere ["Gruppi utente"](#) a pagina 382.

Nota: Se si utilizza un server di directory che contiene un certificato di autenticazione autofirmato, è necessario aggiungere il certificato a Enforce Server o Discover Server. Se il server di directory usa un certificato pre-autorizzato, questo viene aggiunto automaticamente a Enforce Server o Discover Server. Vedere ["Importazione di certificati SSL in Enforce o Discover server"](#) a pagina 272.

Per creare una connessione directory di gruppo

- 1 Accedere alla schermata **Sistema > Impostazioni > Connessioni directory**.
- 2 Fare clic su **Aggiungi connessione**.
- 3 Configurare la connessione directory.

Vedere "[Configurazione delle connessioni a server di directory](#)" a pagina 162.

Configurazione delle connessioni a server di directory

La pagina **Connessioni directory** è la home page per la configurazione delle connessioni a server di directory. Dopo avere definito la connessione di una directory, è possibile creare uno o più gruppi di utenti.

Vedere "[Configurazione di gruppi di utenti](#)" a pagina 847.

Tabella 6-1 Configurazione delle connessioni a server di directory

Passaggio	Azione	Descrizione
1	Accedere alla pagina Connessioni directory (se non è già visualizzata).	Questa pagina è accessibile da Sistema > Impostazioni > Connessioni directory .
2	Fare clic su Crea nuova connessione .	Questa azione consente di visualizzare la pagina Configura connessione directory .
3	Immettere un nome per la connessione al server di directory.	Nome connessione è il nome definito dall'utente per la connessione. Viene visualizzato nella home page Connessioni directory dopo che la connessione è stata configurata.
4	Specificare i parametri di rete per la connessione al server di directory.	La Tabella 6-2 fornisce informazioni dettagliate su questi parametri. Immettere o specificare i seguenti parametri: <ul style="list-style-type: none"> ■ Nome host del computer su cui è installato il server di directory. ■ Porta sul server di directory che supporta le connessioni. ■ DN di base (nome univoco) del server di directory. ■ Metodo di crittografia per la connessione: Nessuno o Protetto.
5	Specificare la modalità di autenticazione per la connessione al server di directory.	La Tabella 6-3 fornisce informazioni dettagliate sulla configurazione dei parametri di autenticazione.

Passaggio	Azione	Descrizione
6	Fare clic su Prova connessione per verificare la connessione.	Se la connessione non funziona correttamente, il sistema restituisce un messaggio di errore in cui viene descritto il problema.
7	Fare clic su Salva per salvare la configurazione della connessione della direzione.	Il sistema indicizza automaticamente il server di directory dopo che si è creata, provata e salvata la connessione al server di directory.
8	Selezionare la scheda Stato indice e replica .	Assicurarsi che il server di directory sia stato indicizzato. Dopo qualche tempo (a seconda della dimensione della query del server di directory) Stato replica dovrebbe essere "Completato <data> <ora>". Se lo stato non è visualizzato come completato, assicurarsi di avere configurato e provato correttamente la connessione di directory. Contattare l'amministratore del server di directory per assistenza.
9	Selezionare la scheda Impostazioni indice .	È possibile regolare la pianificazione dell'indicizzazione del server di directory in base alle esigenze nella scheda Impostazioni indice . Vedere "Pianificazione dell'indicizzazione del server di directory" a pagina 164.

Tabella 6-2 Parametri di rete della connessione di directory

Parametri di rete	Descrizione
Nome host	Immettere il nome host del server di directory. Ad esempio: enforce.dlp.symantec.com È necessario immettere il nome completo (FQN) del server di directory. Non utilizzare l'indirizzo IP.
Porta	Immettere la porta di connessione per il server di directory. Ad esempio: 389 Solitamente la porta è 389 o 636 per le connessioni protette.
DN di base	Immettere il DN di base per il server di directory. Questo campo accetta l'immissione di un solo server di directory. Ad esempio: dc=enforce,dc=dlp,dc=symantec,dc=com La stringa DN di base non può contenere spazi. DN di base è il nome univoco di base del server di directory. Solitamente questo nome è il nome di dominio del server di directory. Il parametro DN di base definisce la profondità iniziale della ricerca del server di directory.

Parametri di rete	Descrizione
Metodo di crittografia	<p>Selezionare l'opzione Protetto se si desidera che la comunicazione tra il server di directory ed Enforce Server venga crittografata tramite SSL.</p> <p>Nota: se si sceglie di utilizzare una connessione protetta, può essere necessario importare il certificato SSL del server di directory nell'archivio chiavi di Enforce Server. Vedere "Importazione di certificati SSL in Enforce o Discover server" a pagina 272.</p>

Tabella 6-3

Parametri di autenticazione della connessione di directory

Autenticazione	Descrizione
Autenticazione	Selezionare l'opzione Autenticazione per connettersi al server di directory utilizzando la modalità di autenticazione. Controllare Connetti con credenziali per aggiungere il nome utente e la password per eseguire l'autenticazione al server di directory.
Nome utente	<p>Per eseguire l'autenticazione con Active Directory, utilizzare uno dei seguenti metodi:</p> <ul style="list-style-type: none"> ■ Nome di dominio e utente, ad esempio: <code>Domain\username</code> ■ Nome utente e di dominio, ad esempio: <code>username@domain.com</code> ■ Nome utente e di dominio completamente distinti (senza spazi), ad esempio: <code>cn=username,cn=Users,dc=domain,dc=com</code> <p>Per autenticarti con un altro tipo di server di directory:</p> <ul style="list-style-type: none"> ■ Una sintassi differente potrebbe essere necessaria, ad esempio: <code>uid=username,ou=people,o=company</code>
Password	<p>Immettere la password per l'utente specificato nel campo precedente.</p> <p>La password è oscurata quando viene inserita.</p>

Pianificazione dell'indicizzazione del server di directory

Ogni connessione di directory viene impostata in modo da indicizzare automaticamente il server LDAP configurato **una volta** alle 00:00 il giorno dopo la creazione della connessione iniziale. È possibile modificare la pianificazione di indicizzazione in modo da specificare quando e con quale frequenza viene sincronizzato l'indice.

Ogni connessione del server di directory viene impostata in modo da indicizzare automaticamente il gruppo di utenti configurato, ospitato sul server di directory **una volta** alle 00:00 il giorno dopo la creazione della connessione iniziale.

Dopo avere creato, testato e salvato la connessione del server di directory, il sistema indicizza automaticamente tutti i gruppi di utenti ospitati nella directory di cui si è stabilita la connessione.

È possibile modificare questa impostazione e pianificare l'indicizzazione ogni giorno, settimana o mese.

Per pianificare l'indicizzazione della directory di gruppo

- 1 Selezionare una connessione del server di directory di gruppo esistente nella schermata **Sistema > Impostazioni > Connessioni directory**. In alternativa creare una nuova connessione.

Vedere ["Configurazione delle connessioni a server di directory"](#) a pagina 162.

- 2 Regolare le impostazioni di indice in base alla pianificazione desiderata.

Vedere [Tabella 6-4](#) a pagina 165.

Tabella 6-4 Pianificazione dell'indicizzazione del server di directory di gruppo e visualizzazione dello stato

Impostazioni indice	Descrizione
Indicizzare il server di directory una volta.	L'impostazione Una volta è selezionata per impostazione predefinita e indicizza automaticamente il server di directory alle 00:00 il giorno dopo la creazione della connessione iniziale. È possibile modificare la pianificazione di indicizzazione Una volta predefinita. A questo scopo specificare quando e con quale frequenza è necessario ricreare l'indice.
Indicizzare il server di directory giornalmente.	Selezionare l'opzione Ogni giorno per pianificare l'indice giornalmente. Specificare l' ora del giorno e, facoltativamente, la durata Fino a per questa pianificazione.
Indicizzare il server di directory settimanalmente.	Selezionare l'opzione Ogni settimana per pianificare l'indicizzazione una volta alla settimana. Specificare il giorno della settimana per l'indicizzazione. Specificare l' ora per l'indicizzazione. Specificare facoltativamente la durata Fino a per questa pianificazione.
Indicizzare il server di directory mensilmente.	Specificare il giorno del mese per l'indicizzazione della directory e l' ora . Specificare facoltativamente la durata Fino a per questa pianificazione.

Impostazioni indice	Descrizione
Visualizzare lo stato di indicizzazione e replica.	<p>Selezionare la scheda Stato indice e replica per visualizzare lo stato del processo di indicizzazione.</p> <ul style="list-style-type: none"> ■ Stato di indicizzazione Visualizza la data e l'ora dell'indice pianificato successivo. ■ Nome server di rilevamento Visualizza il server di rilevamento in cui è distribuito il profilo del gruppo di utenti. ■ Stato replica ■ Visualizza la data e l'ora della sincronizzazione più recente con il server di directory di gruppo.

Gestione di credenziali archiviate

Il capitolo contiene i seguenti argomenti:

- [Informazioni sull'archivio credenziali](#)
- [Aggiunta di nuove credenziali all'archivio credenziali](#)
- [Configurazione delle credenziali endpoint](#)
- [Gestione delle credenziali nell'archivio credenziali](#)
- [Gestione di credenziali archiviate](#)

Informazioni sull'archivio credenziali

Una credenziale di autenticazione può essere archiviata come credenziale con nome in un archivio credenziali centrale. La credenziale può essere definita una sola volta e essere utilizzata come riferimento da un numero qualsiasi di target di Discover. Le password vengono crittografate prima di essere archiviate.

L'archivio credenziali semplifica la gestione delle modifiche a nomi utente e password.

È possibile aggiungere, eliminare o modificare credenziali archiviate.

Vedere ["Aggiunta di nuove credenziali all'archivio credenziali"](#) a pagina 168.

Vedere ["Gestione delle credenziali nell'archivio credenziali"](#) a pagina 169.

La schermata Gestione credenziali è accessibile agli utenti con il privilegio "Gestione credenziale".

Le credenziali archiviate possono essere usate quando si modifica o crea un target di Discover.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Aggiunta di nuove credenziali all'archivio credenziali

È possibile aggiungere nuove credenziali all'archivio credenziali. Successivamente è possibile fare riferimento a queste credenziali con i nomi delle credenziali.

Per aggiungere una credenziale archiviata

- 1 Fare clic su **Sistema > Impostazioni > Credenziali** e fare clic su **Aggiungi credenziale**.
- 2 Immettere le seguenti informazioni:

Nome credenziale	Immettere il nome della credenziale archiviata. Il nome deve essere univoco nell'archivio credenziali e viene utilizzato solo per identificare la credenziale.
Nome utente di accesso	Immettere il nome utente per l'autenticazione.
Password di accesso	Immettere la password per l'autenticazione.
Immettere di nuovo la password di accesso	Immettere di nuovo la password.

- 3 Fare clic su **Salva**.
- 4 È possibile in seguito modificare o eliminare le credenziali dall'archivio credenziali.

Vedere ["Gestione delle credenziali nell'archivio credenziali"](#) a pagina 169.

Vedere ["Configurazione delle credenziali endpoint"](#) a pagina 168.

Configurazione delle credenziali endpoint

È necessario aggiungere le credenziali all'archivio delle credenziali prima di potere accedere alle credenziali per Endpoint FlexResponse o la regola di risposta di quarantena di Endpoint Discover. Le credenziali vengono archiviate in una cartella crittografata su tutti gli endpoint connessi a Endpoint Server. Poiché tutti gli endpoint archiviano le credenziali, è necessario prestare attenzione al tipo di credenziali che si archivia. Utilizzare credenziali che non possono accedere ad altre aree del sistema. Prima di potere utilizzare le credenziali dell'endpoint, è necessario attivare Enforce Server in modo che le riconosca.

Per creare le credenziali endpoint

- 1 Selezionare **Sistema > Impostazioni > Generale**.
- 2 Fare clic su **Configura**.

- 3 Nella sezione **Gestione credenziali** assicurarsi che sia selezionata la casella di controllo **Consenti credenziali salvate negli agenti di endpoint**.
- 4 Fare clic su **Salva**.
- 5 Selezionare **Sistema > Impostazioni > Credenziali**.
- 6 Fare clic su **Aggiungi credenziale**.
- 7 Nella sezione **Generale** immettere i dettagli della credenziale da aggiungere.
- 8 In **Autorizzazioni d'uso** selezionare **Server e agenti di endpoint (documenti indicizzati, target di Discover, regole di risposta endpoint)**.
- 9 Fare clic su **Salva**.

Vedere ["Informazioni sull'archivio credenziali"](#) a pagina 167.

Vedere ["Configurazione dell'azione Endpoint Discover: metti file in quarantena"](#) a pagina 1545.

Gestione delle credenziali nell'archivio credenziali

È possibile eliminare o modificare una credenziale archiviata.

Per eliminare una credenziale archiviata

- 1 Fare clic su **Sistema > Impostazioni > Credenziali**. Individuare il nome della credenziale archiviata che si desidera rimuovere.
- 2 Fare clic sull'icona di cancellazione a destra del nome. Una credenziale può essere eliminata solo se non vi sono attualmente riferimenti alla stessa in un target di Discover o in un profilo di documenti indicizzati.

Per modificare una credenziale archiviata

- 1 Fare clic su **Sistema > Impostazioni > Credenziali**. Individuare il nome della credenziale archiviata che si desidera modificare.
- 2 Fare clic sull'icona di modifica (matita) a destra del nome.
- 3 Aggiornare il nome utente o la password.
- 4 Fare clic su **Salva**.
- 5 Se si modifica la password per una determinata credenziale, la nuova password viene utilizzata per tutte le scansioni di Discover successive che usano tale credenziale.

Gestione di credenziali archiviate

Una credenziale di autenticazione può essere archiviata in un archivio credenziali centrale. Può essere definita una volta come credenziale e quindi essere utilizzata come riferimento da un numero qualsiasi di target di Network Discover/Cloud Storage Discover.

Archiviare le credenziali di autenticazione in un archivio centrale per semplificare la gestione delle modifiche di nome utente e password.

È possibile aggiungere, eliminare o modificare le credenziali archiviate.

Per aggiungere una credenziale archiviata

- 1 In **Sistema > Impostazioni > Credenziali** fare clic su **Aggiungi credenziale**.
- 2 Immettere le seguenti informazioni:

Nome credenziale	Immettere il nome della credenziale archiviata. Il nome deve essere univoco nell'archivio credenziali e viene utilizzato solo per identificare la credenziale.
Nome utente di accesso	Immettere il nome utente per l'autenticazione.
Password di accesso	Immettere la password per l'autenticazione.
Immettere di nuovo la password di accesso	Immettere di nuovo la password.

- 3 Fare clic su **Salva**.

Per eliminare una credenziale archiviata

- 1 In **Sistema > Impostazioni > Credenziali** individuare il nome della credenziale archiviata che si desidera rimuovere.
- 2 Fare clic sull'icona di eliminazione a destra del nome. Una credenziale può essere eliminata solo se non vi sono attualmente riferimenti alla stessa in un target di Discover o in un profilo di documenti indicizzati.

Per modificare una credenziale archiviata

- 1 In **Sistema > Impostazioni > Credenziali** individuare il nome della credenziale archiviata che si desidera modificare.
- 2 Fare clic sull'icona di modifica (matita) a destra del nome.
- 3 Aggiornare il nome utente o la password.
- 4 Fare clic su **Salva**.
- 5 Se si modifica la password per una determinata credenziale, la nuova password viene utilizzata per tutte le scansioni di Discover successive che usano tale credenziale.

Vedere ["Autenticazione tramite password per il contenuto sottoposto a scansione Network Discover"](#) a pagina 1835.

Gestione di eventi e messaggi di sistema

Il capitolo contiene i seguenti argomenti:

- [Informazioni sugli eventi di sistema](#)
- [Report di eventi di sistema](#)
- [Utilizzo dei report di sistema salvati](#)
- [Dettagli eventi di server e rivelatori](#)
- [Configurazione di attivazioni e soglie evento](#)
- [Informazioni sulle risposte agli eventi di sistema](#)
- [Attivazione di un server syslog](#)
- [Informazioni sugli avvisi di sistema](#)
- [Configurazione di Enforce Server per l'invio di avvisi tramite e-mail](#)
- [Configurazione degli avvisi di sistema](#)
- [Informazioni sulla verifica registri](#)
- [Messaggi e codici di eventi di sistema](#)

Informazioni sugli eventi di sistema

Gli eventi di sistema correlati all'installazione di Symantec Data Loss Prevention vengono monitorati, segnalati e registrati. Gli eventi di sistema comprendono le notifiche di Cloud Operations per i servizi cloud.

I report degli eventi di sistema vengono visualizzati nella console di amministrazione di Enforce Server:

- I cinque eventi di sistema più recenti di gravità Avviso o Gravità vengono elencati nella schermata **Panoramica** (**Sistema > Server e rilevatori > Panoramica**).
Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.
- È possibile visualizzare report su tutti gli eventi di sistema di qualsiasi gravità accedendo a **Sistema > Server e rilevatori > Eventi**.
Vedere ["Report di eventi di sistema"](#) a pagina 172.
- Gli eventi di sistema recenti per uno specifico server di rilevamento o servizio cloud sono elencati nella schermata **Dettagli server/rilevatore** per tale server o rilevatore.
Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.
- Fare clic su un evento nell'elenco eventi per accedere alla schermata **Dettagli evento** per tale evento. La schermata **Dettagli evento** fornisce ulteriori informazioni sull'evento.
Vedere ["Dettagli eventi di server e rivelatori"](#) a pagina 176.

Gli eventi di sistema possono richiamare l'attenzione dell'utente in tre modi:

- Report di eventi di sistema visualizzati sulla console di amministrazione
- Messaggi e-mail di avviso di sistema
Vedere ["Informazioni sugli avvisi di sistema"](#) a pagina 183.
- Funzionalità Syslog
Vedere ["Attivazione di un server syslog"](#) a pagina 182.

Alcuni eventi di sistema richiedono una risposta.

Vedere ["Informazioni sulle risposte agli eventi di sistema"](#) a pagina 180.

Per restringere il campo di interesse della gestione degli eventi è possibile:

- Utilizzare i filtri nei diversi metodi di notifica degli eventi di sistema.
Vedere ["Report di eventi di sistema"](#) a pagina 172.
- Configurare le soglie di eventi di sistema per singoli server.
Vedere ["Configurazione di attivazioni e soglie evento"](#) a pagina 177.




Report di eventi di sistema

Per visualizzare tutti gli eventi di sistema, accedere alla schermata dei report sugli eventi di sistema (**Sistema > Server e rilevatori > Eventi**). Questa schermata elenca gli eventi, un evento per riga. L'elenco contiene gli eventi che corrispondono all'intervallo di dati selezionato e a tutte le altre opzioni di filtro elencate nella barra **Filtri applicati**. Per ogni evento, le seguenti informazioni sono visualizzate:

Tabella 8-1

Eventi	Descrizione
Tipo	Il tipo (la gravità) dell'evento. Il tipo può essere uno qualsiasi di quelli elencati in Tabella 8-2 .
Orario	La data e l'ora dell'evento.
Server	Il nome del server in cui si è verificato l'evento.
Host	L'indirizzo IP o il nome host del server su cui si è verificato l'evento.
Codice	Un numero che identifica il tipo di evento. Consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per ulteriori informazioni sui numeri dei codici evento.
Riepilogo	Una breve descrizione dell'evento. Fare clic sul riepilogo per ulteriori informazioni sull'evento.

Tabella 8-2 Tipi di eventi di sistema

Evento	Descrizione
	Informazioni di sistema
	Avviso
	Grave

È possibile scegliere tra varie opzioni di gestione dei report.

Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.

Fare clic su un evento qualsiasi nell'elenco per accedere alla schermata **Dettagli evento** per quell'evento. La schermata **Dettagli evento** fornisce ulteriori informazioni sull'evento.

Vedere ["Dettagli eventi di server e rivelatori"](#) a pagina 176.

Poiché l'elenco di eventi può essere lungo, sono a disposizione dei filtri per selezionare solo gli eventi a cui si è interessati. Per impostazione predefinita, solo il filtro Data è attivato ed è inizialmente impostato su Tutte le date. Il filtro Data seleziona gli eventi in base alla data in cui gli eventi si sono verificati.

Per filtrare l'elenco degli eventi di sistema per data di occorrenza

- 1 Accedere alla sezione Filtro della schermata relativa ai report di eventi e selezionare una delle opzioni per l'intervallo di date.
- 2 Fare clic su **Applica**.
- 3 Selezionare **Personalizza** dall'elenco di date per specificare la data di inizio e quella di fine.

Oltre al filtro per intervallo di date, è anche possibile applicare filtri avanzati. I filtri avanzati sono cumulativi con il filtro di data corrente. Ciò significa che gli eventi sono elencati solo se corrispondono al filtro avanzato e rientrano nell'intervallo di date corrente. Possono essere applicati filtri avanzati multipli. Se i filtri multipli sono applicati, gli eventi sono elencati solo se corrispondono a tutti i filtri e all'intervallo di date.

Per applicare filtri avanzati supplementari

- 1 Fare clic su **Filtri avanzati e riepilogo**.
- 2 Fare clic su **Aggiungi filtro**.
- 3 Scegliere il filtro che si desidera utilizzare dal elenco a discesa più a sinistra. I filtri disponibili sono elencati in [Tabella 8-3](#).
- 4 Scegliere l'operatore del filtro dall'elenco a discesa nel mezzo.

Nota: È possibile usare il valore del filtro **Cloud Operations** per visualizzare gli eventi di Cloud Operations per i rivelatori.

Per ogni filtro avanzato è possibile specificare un operatore di filtro **È uno qualsiasi dei seguenti valori** o **Non è alcuno dei seguenti valori**.

- 5 Immettere il valore o i valori del filtro nella casella di testo a destra, o fare clic su un valore nell'elenco per selezionarlo.
 - Per selezionare molteplici valori da un elenco, mantenere premuto il tasto CTRL e fare clic su ogni valore.
 - Per selezionare un intervallo di valori da un elenco, fare clic sul primo, quindi mantenere premuto il tasto MAIUSC e fare clic sull'ultimo valore nell'intervallo desiderato.
- 6 (Opzionale) Specificare altri filtri avanzati, se necessario.
- 7 Dopo aver specificato un filtro o un set di filtri, fare clic su **Applica**.

Fare clic sulla X rossa per eliminare un filtro avanzato.

La barra **Filtri applicati** elenca i filtri che sono utilizzati per elaborare l'elenco di eventi visualizzato. Tenere presente che i filtri multipli sono cumulativi. Affinché un evento sia visualizzato sull'elenco deve superare tutti i filtri applicati.

I seguenti filtri avanzati sono disponibili:

Tabella 8-3 Opzioni di filtri avanzate per eventi di sistema

Filtro	Descrizione
Codice evento	Filtra gli eventi per i numeri di codice che identificano ogni tipo di evento. È possibile filtrare per singolo numero di codice o per molteplici numeri di codice separati da virgole (2121, 1202, 1204). Non è possibile filtrare per intervalli di numeri di codice o in base agli operatori Maggiore di o Minore di.
Tipo evento	Filtra gli eventi per tipo di gravità dell'evento (Informazioni, Avviso o Gravità).
Server	Filtra gli enti per nome del server su cui si è verificato l'evento.

Nota: Un piccolo sottoinsieme dei parametri che attivano gli eventi di sistema ha soglie che possono essere configurate. Questi parametri devono essere regolati solo su consiglio del supporto Symantec. Prima di modificare queste impostazioni, è necessario comprendere perfettamente le implicazioni in gioco. I valori predefiniti sono appropriati per la maggior parte delle installazioni.

Vedere ["Configurazione di attivazioni e soglie evento"](#) a pagina 177.

Vedere ["Informazioni sugli eventi di sistema"](#) a pagina 171.

Vedere ["Dettagli eventi di server e rivelatori"](#) a pagina 176.

Vedere [" Utilizzo dei report di sistema salvati"](#) a pagina 175.

Vedere ["Configurazione di attivazioni e soglie evento"](#) a pagina 177.

Vedere ["Informazioni sugli avvisi di sistema"](#) a pagina 183.

Utilizzo dei report di sistema salvati

La schermata **Report di sistema** elenca i report di sistema e relativi agli agenti che sono stati precedentemente salvati. Per visualizzare la schermata **Report di sistema**, fare clic su **Sistema > Report di sistema**. Utilizzare questa schermata per lavorare con i report di sistema salvati.

Per creare un report di sistema salvato

- 1 Accedere a una delle seguenti schermate:
 - Eventi di sistema (**Sistema > Eventi**)

- Panoramica degli agenti (**Sistema > Agenti > Panoramica**)
- Eventi degli agenti (**Sistema > Agenti > Eventi**)

Vedere ["Informazioni sulla console di amministrazione di Enforce Server"](#) a pagina 81.

- 2 Selezionare i filtri e riepiloghi per il report personalizzato.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

- 3 Selezionare **Report > Salva con nome**.

- 4 Immettere le informazioni del report salvato.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

- 5 Fare clic su **Salva**.

La schermata **Report di sistema** include due sezioni:

- In **Evento di sistema - Report salvati** sono elencati i report di sistema salvati.
- In **Gestione agente - Report salvati sono elencati i report sugli agenti salvati**.

Per ogni report salvato è possibile eseguire le seguenti operazioni:

- Condividere il report. Fare clic su **Condividi** per consentire ad altri utenti di Symantec Data Loss Prevention con lo stesso ruolo di condividere il report. La condivisione del report non può essere annullata; dopo che un report è stato condiviso non può essere reso privato. Dopo che un report è stato condiviso, tutti gli utenti con il quale è stato condiviso possono visualizzare, modificare o eliminare il report.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

- Cambiare il nome o la descrizione del report. Fare clic sull'icona della matita a destra del nome del report per modificarlo.
- Modificare la pianificazione di report. Fare clic sull'icona del calendario a destra del nome del report per modificare la pianificazione della consegna del report e i destinatari a cui viene inviato.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Vedere ["Opzioni di pianificazione di consegna per i report di incidente e di sistema"](#) a pagina 1652.

- Eliminare il report. Fare clic sulla X rossa a destra del nome di report per eliminare il report.

Dettagli eventi di server e rivelatori

Per visualizzare la schermata **Dettagli eventi di server e rivelatori**, accedere a **Sistema > Server e rivelatori > Eventi** e fare clic su uno degli eventi elencati.

Vedere ["Report di eventi di sistema"](#) a pagina 172.

La schermata **Dettagli eventi di server e rivelatori** visualizza tutte le informazioni disponibili per l'evento selezionato. Le informazioni in questa schermata non sono modificabili.

La schermata **Dettagli eventi di server e rivelatori** è divisa in due sezioni: **Generale** e **Messaggio**.

Tabella 8-4 Dettagli evento - Generale

Elemento	Descrizione
Tipo	L'evento è uno dei seguenti tipi: <ul style="list-style-type: none">■ Informazioni: informazioni sul sistema.■ Avviso: un problema che non è abbastanza grave per generare un errore.■ Grave: un errore che richiede attenzione immediata.
Orario	La data e l'ora dell'evento.
Server o rivelatore	Il nome del server o del rivelatore.
Host	Il nome host o l'indirizzo IP del server.

Tabella 8-5 Dettagli evento - Messaggio

Elemento	Descrizione
Codice	Un numero che identifica il tipo di evento. Vedere "Messaggi e codici di eventi di sistema" a pagina 187.
Riepilogo	Una breve descrizione dell'evento.
Dettaglio	Informazioni dettagliate sull'evento.

Vedere ["Informazioni sugli eventi di sistema"](#) a pagina 171.

Vedere ["Report di eventi di sistema"](#) a pagina 172.

Vedere ["Informazioni sugli avvisi di sistema"](#) a pagina 183.

Configurazione di attivazioni e soglie evento

Un piccolo sottoinsieme dei parametri che attivano gli eventi di sistema ha soglie che possono essere configurate. Questi parametri sono configurati separatamente per ogni server di rilevamento o rivelatore. Questi parametri devono essere regolati solo su consiglio del supporto Symantec. Prima di modificare queste impostazioni, è necessario comprendere perfettamente le implicazioni. I valori predefiniti sono appropriati per la maggior parte delle installazioni.

Vedere ["Informazioni sugli eventi di sistema"](#) a pagina 171.

Per visualizzare e modificare i parametri configurabili che attivano gli eventi di sistema

- 1 Accedere alla schermata **Panoramica (Sistema > Server e rilevatori > Panoramica)**.
- 2 Fare clic sul nome di un server di rilevamento o di un rilevatore per visualizzare la schermata **Dettagli server/rilevatore** di tale server.
- 3 Fare clic su **Impostazioni server/rilevatore**.

Viene visualizzata la schermata **Impostazioni server/rilevatore avanzate** per tale server.

- 4 Modificare i parametri configurabili, se necessario.

Tabella 8-6 Parametri configurabili che attivano gli eventi

Parametro	Descrizione	Evento
BoxMonitor.DiskUsageError	Indica la quantità di spazio su disco piena (in percentuale) che attiva un evento di sistema grave. Ad esempio, un evento grave si verifica se un server di rilevamento è installato sull'unità C e il valore dell'errore dello spazio su disco è 90. Il server di rilevamento crea un evento di sistema grave quando l'utilizzo dell'unità C è del 90% o superiore. Il valore predefinito è 90.	Spazio su disco insufficiente
BoxMonitor.DiskUsageWarning	Indica la quantità di spazio su disco piena (in percentuale) che attiva un evento di sistema di avviso. Ad esempio, un evento di avviso si verifica se il server di rilevamento è installato sull'unità C e il valore di avviso dello spazio su disco è 80. Quindi, il server di rilevamento genera un evento di sistema di avviso quando l'utilizzo dell'unità C è dell'80% o superiore. Il valore predefinito è 80.	Spazio su disco insufficiente
BoxMonitor.MaxRestartCount	Indica il numero di volte in cui un processo di sistema può essere riavviato in un'ora prima della generazione di un evento di sistema grave. Il valore predefinito è 3.	<i>nome processo</i> riavviato troppe volte

Parametro	Descrizione	Evento
IncidentDetection.MessageWaitSevere	Indica il numero di minuti che i messaggi devono attendere per l'elaborazione prima che un evento di sistema grave relativo ai tempi di attesa del messaggio venga inviato. Il valore predefinito è 240.	Tempo di attesa messaggi lungo
IncidentDetection.MessageWaitWarning	Indica il numero di minuti che i messaggi devono attendere per l'elaborazione prima che un evento di sistema grave relativo ai tempi di attesa del messaggio venga inviato. Il valore predefinito è 60.	Tempo di attesa messaggi lungo
IncidentWriter.BacklogInfo	Indica il numero degli incidenti che possono essere messi in coda prima della generazione di un evento di sistema di informazioni. Questo tipo di backlog indica solitamente che gli incidenti non vengono elaborati o non vengono elaborati correttamente poiché il sistema è rallentato o interrotto. Il valore predefinito è 1000.	N. incidenti in coda
IncidentWriter.BacklogWarning	Indica il numero degli incidenti che possono essere messi in coda prima della generazione di un evento di sistema di avviso. Questo tipo di backlog indica solitamente che gli incidenti non vengono elaborati o non vengono elaborati correttamente poiché il sistema è rallentato o interrotto. Il valore predefinito è 3000.	N. incidenti in coda
IncidentWriter.BacklogSevere	Indica il numero di incidenti che possono essere messi in coda prima della generazione di un evento di sistema grave. Questo tipo di backlog indica solitamente che gli incidenti non vengono elaborati o non vengono elaborati correttamente poiché il sistema è rallentato o interrotto. Il valore predefinito è 10000.	N. incidenti in coda

Informazioni sulle risposte agli eventi di sistema

Gli eventi di sistema possono richiamare l'attenzione dell'utente in tre modi:

- Report di eventi di sistema visualizzati sulla console di amministrazione
- Messaggi e-mail di avviso di sistema
Vedere ["Informazioni sugli avvisi di sistema"](#) a pagina 183.
- Funzionalità Syslog
Vedere ["Attivazione di un server syslog"](#) a pagina 182.

Nella maggior parte dei casi, il riepilogo degli eventi di sistema e le informazioni dettagliate devono fornire abbastanza informazioni da dirigere le fasi di analisi e riparazione. La seguente tabella fornisce alcuni linee guida generali in merito alla risposta agli eventi di sistema.

Tabella 8-7 Risposte agli eventi di sistema

Evento sistema o categoria	Risposta appropriata
Spazio su disco insufficiente	<p>Se questo evento viene segnalato su un server di rilevamento, riciclare i servizi di Symantec Data Loss Prevention sul server di rilevamento. Il server di rilevamento può avere perso la connessione con Enforce Server. Il server di rilevamento mette quindi in coda i relativi incidenti localmente e riempie il disco.</p> <p>Se questo evento viene segnalato su un Enforce Server, verificare lo stato dei servizi di Oracle e Symantec DLP Incident Persister. È possibile che venga segnalato uno spazio su disco insufficiente se gli incidenti non vengono trasferiti correttamente dal file system al database. Questo evento può anche indicare la necessità di aggiungere spazio su disco supplementare.</p>
Spazio tabella quasi pieno	<p>Aggiungere file di dati supplementari al database. Quando il disco rigido è all'80% della capacità, si consiglia di utilizzare un disco più capiente invece di aggiungere file di dati supplementari.</p> <p>Consultare il <i>Manuale di installazione di Symantec Data Loss Prevention</i>.</p>
Gestione licenze e controllo delle versioni	Contattare il supporto Symantec.

Evento sistema o categoria	Risposta appropriata
Il servizio di monitoraggio non risponde	<p>Riavviare il servizio del Server di rilevamento di Symantec DLP. Se l'evento persiste, verificare le connessioni di rete. Assicurarsi che il computer che ospita il server delle rilevazioni sia acceso collegandosi a esso. È possibile collegarsi con servizi terminali o un altro metodo di connessione desktop remoto. Se necessario, contattare il supporto Symantec.</p> <p>Vedere "Informazioni sui servizi Symantec Data Loss Prevention" a pagina 101.</p>
Invio di avviso o report pianificato non riuscito.	Accedere a Sistema > Impostazioni > Generale e assicurarsi che le impostazioni nelle sezioni Report e avvisi e SMTP siano configurate correttamente. Verificare la connettività tra Enforce Server e il server SMTP. Contattare il supporto Symantec.
Accensione chiave automatica non riuscita	Contattare il supporto Symantec.
Le chiavi di crittografia non corrispondono	Contattare il supporto Symantec.
Tempo di attesa messaggi lungo	<p>Aumentare la capacità del server di rilevamento aggiungendo più CPU o sostituendo il computer con uno più potente.</p> <p>Diminuire il carico sul server di rilevamento. È possibile diminuire il carico applicando filtri di traffico configurati per rilevare meno incidenti. È anche possibile ridirigere porzioni del traffico su altri server di rilevamento.</p> <p>Aumentare i tempi di attesa della soglia se tutti i seguenti elementi sono veri:</p> <ul style="list-style-type: none"> ■ Questo messaggio viene visualizzato durante le ore di punta. ■ Il tempo di attesa del messaggio scende a zero prima del picco seguente. ■ È possibile che avvengano simili ritardi nell'elaborazione dei messaggi.
process_name viene riavviato troppe volte	Verificare il processo accedendo a Sistema > Server > Panoramica . Per consultare i singoli processi in questa schermata, occorre attivare il controllo dei processi accedendo in Sistema > Impostazioni > Generale > Configura .

Evento sistema o categoria	Risposta appropriata
N. incidenti in coda	<p>Analizzare il motivo per cui gli incidenti riempiono la coda.</p> <p>I motivi più probabili sono i seguenti:</p> <ul style="list-style-type: none">■ Problemi di connessione. Risposta: assicurarsi che la comunicazione tra l'Endpoint Server e il server di rilevamento sia stabile.■ Larghezza di banda della connessione insufficiente per il numero di incidenti generati (tipico per le connessioni WAN). Risposta: valutare la possibilità di modificare le politiche (configurando i filtri) in modo che generino meno incidenti.

Attivazione di un server syslog

La funzionalità Syslog eventi di sistema gravi a un server syslog. I server Syslog consentono agli amministratori di sistema di filtrare e indirizzare le notifiche di eventi di sistema a un livello più granulare. Gli amministratori di sistema che utilizzano regolarmente il syslog per il monitoraggio dei loro sistemi possono preferire l'utilizzo del syslog al posto degli avvisi. Syslog può essere preferito se il volume di avvisi è troppo ingombrante per l'e-mail.

La funzionalità Syslog è un'opzione on/off. Se il syslog è attivo, tutti gli eventi gravi vengono inviati al server syslog.

Per attivare la funzionalità syslog

- 1 Accedere alla directory `\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` in Windows o alla directory `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config` su Linux.
- 2 Aprire il file `Manager.properties`.
- 3 Rimuovere il commento dalla riga `#systemevent.syslog.host=` eliminando il simbolo `#` dall'inizio della riga e immettere il nome host o l'indirizzo IP del server syslog.
- 4 Rimuovere il commento dalla riga `#systemevent.syslog.port=` eliminando il simbolo `#` dall'inizio della riga. Immettere il numero di porta che dovrebbe accettare connessioni dal servizio Enforce Server. Il valore predefinito è 514.
- 5 Rimuovere il commento dalla riga `#systemevent.syslog.format= [{0}] {1} - {2}` eliminando il simbolo `#` dall'inizio della riga. Quindi definire il formato del messaggio di evento di sistema da inviare al server syslog:

Se la riga è senza commenti e senza modifiche, i messaggi di notifica vengono inviati nel seguente formato: [nome server] riepilogo - dettagli. Le variabili di formato sono le seguenti:

- {0}: il nome del server in cui si è verificato l'evento.

- {1}: il riepilogo dell'evento
- {2}: i dettagli dell'evento

Ad esempio, la seguente configurazione specifica che le notifiche degli eventi di sistema gravi vengono inviate a un host di syslog denominato server1 che utilizza la porta 600.

```
systemevent.syslog.host=server1  
systemevent.syslog.port=600  
systemevent.syslog.format= [{0}] {1} - {2}
```

Utilizzando questo esempio, una notifica di evento spazio su disco insufficiente da Enforce Server su un host denominato dlp-1 avrebbe questo aspetto:

```
dlp-1 Low disk space - Hard disk space for  
incident data storage server is low. Disk usage is over 82%.
```

Vedere ["Informazioni sugli eventi di sistema"](#) a pagina 171.

Informazioni sugli avvisi di sistema

Gli avvisi di sistema sono messaggi di posta elettronica inviati agli indirizzi designati quando si verifica un particolare evento di sistema. Definire quali avvisi utilizzare per l'installazione (se disponibili). Gli avvisi vengono specificati e modificati nella schermata **Configura avviso**, visualizzabile selezionando **Sistema > Server e rilevatori > Avvisi > Aggiungi avviso**.

Gli avvisi possono essere specificati in base alla gravità dell'evento, al nome del server, al codice di evento o a una combinazione di questi fattori. Gli avvisi possono essere inviati per qualsiasi evento di sistema.

L'e-mail che viene generata dall'avviso ha una riga oggetto che inizia con `Symantec Data Loss Prevention System Alert` seguita da un breve riepilogo dell'evento. Il corpo dell'e-mail contiene le stesse informazioni visualizzate nella schermata **Dettagli evento** per fornire informazioni complete sull'evento.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Vedere ["Configurazione degli avvisi di sistema"](#) a pagina 185.

Vedere ["Dettagli eventi di server e rivelatori"](#) a pagina 176.

Configurazione di Enforce Server per l'invio di avvisi tramite e-mail

Per inviare avvisi tramite e-mail relativi agli eventi di sistema specificati, Enforce Server deve essere configurato in modo da supportare l'invio di avvisi e report. Questa sezione descrive

come specificare il formato del report e come configurare Symantec Data Loss Prevention in modo da comunicare con un server SMTP.

Dopo il completamento della configurazione qui descritta, è possibile programmare l'invio di report specifici e creare avvisi di sistema specifici.

Per configurare Symantec Data Loss Prevention in modo da inviare avvisi e report

- 1 Accedere a **Sistema > Impostazioni > Generale** e fare clic su **Configura**.

Viene visualizzata la schermata **Modifica impostazioni generali**.

- 2 Nella sezione **Report e avvisi**, selezionare uno dei metodi di distribuzione seguenti:

- **Invia report come collegamenti; accesso richiesto per la visualizzazione.** Symantec Data Loss Prevention invia i messaggi di posta elettronica con i collegamenti ai report. È necessario accedere a Enforce Server per visualizzare i report.

Nota: I report con i dati degli incidenti non possono essere distribuiti se questa opzione è impostata.

- **Invia dati di report tramite e-mail.** Symantec Data Loss Prevention invia messaggi e-mail e allega i dati dei report.

- 3 Immettere il nome del dominio di Enforce Server o l'indirizzo IP nel campo **Nome completo del manager**.

Se inviate i report come collegamenti, Symantec Data Loss Prevention utilizza il nome del dominio come base dell'URL nell'e-mail del report.

Non specificare un numero di porta a meno che Enforce Server non sia stato modificato in modo da essere eseguito su una porta diversa da quella predefinita (443).

- 4 Se si desidera che i destinatari degli avvisi visualizzino eventuali incidenti correlati, selezionare la casella di controllo **Correlazioni attivate**.

Quando le correlazioni sono attive, gli utenti le visualizzano nella schermata **Istantanea incidente**.

- 5 Nella sezione **SMTP**, identificare il server SMTP da utilizzare per l'invio di avvisi e report.

Immettere le informazioni corrispondenti nei campi specificati:

- **Server:** il nome host o l'indirizzo IP del server SMTP che Symantec Data Loss Prevention utilizza per inviare report programmati ed eventi di sistema.
- **E-mail del sistema:** l'indirizzo e-mail del mittente dell'avviso. Symantec Data Loss Prevention specifica questo indirizzo e-mail come il mittente di tutti i messaggi e-mail in uscita. Il dipartimento IT potrebbe richiedere che l'e-mail di sistema sia un indirizzo e-mail valido sul server SMTP.

- ID utente: se il server SMTP lo richiede, digitare un nome utente valido per accedere al server. Ad esempio, immettere `DOMAIN\bsmith`.
- Password: se il server SMTP lo richiede, digitare la password per l'ID utente.

6 Fare clic su **Salva**.

Vedere ["Informazioni sugli avvisi di sistema"](#) a pagina 183.

Vedere ["Configurazione degli avvisi di sistema"](#) a pagina 185.

Vedere ["Informazioni sugli eventi di sistema"](#) a pagina 171.

Configurazione degli avvisi di sistema

È possibile configurare Symantec Data Loss Prevention per inviare un avviso tramite e-mail ogni volta che individua un evento di sistema specificato. Gli avvisi possono essere specificati in base alla gravità dell'evento, al nome del server, al codice di evento o a una combinazione di questi fattori. Gli avvisi possono essere inviati per qualsiasi evento di sistema.

Vedere ["Informazioni sugli avvisi di sistema"](#) a pagina 183.

Enforce Server deve essere configurato per inviare avvisi e report.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Gli avvisi vengono specificati e modificati nella schermata **Configura avviso** in **Sistema > Server > Avvisi**, quindi selezionare **Aggiungi avviso** per creare un nuovo avviso o fare clic sul nome di un avviso esistente per modificarlo.

Per creare o modificare un avviso

- 1 Accedere alla schermata **Avvisi** (**Sistema > Server e rilevatori > Avvisi**).
- 2 Fare clic sulla scheda **Aggiungi avviso** per creare un nuovo avviso o sul nome di un avviso per modificarlo.
Viene visualizzata la schermata **Configura avviso**.
- 3 Compilare o modificare il nome dell'avviso. Il nome dell'avviso viene visualizzato nella riga dell'oggetto del messaggio di avviso inviato tramite e-mail.
- 4 Compilare o modificare la descrizione dell'avviso.
- 5 Fare clic su **Aggiungi condizione** per specificare una condizione che attiverà l'allarme.

Ogni volta che si fa clic su **Aggiungi condizione** è possibile aggiungere un'altra condizione. Se si specificano più condizioni, per poter attivare l'avviso è necessario che ognuna di esse si verifichi.

Fare clic sulla X rossa accanto a una condizione per rimuoverla da un avviso esistente.

- 6 Immettere l'indirizzo e-mail a cui inviare l'avviso. Separare più indirizzi utilizzando le virgole.
- 7 Limitare il numero massimo degli invii dell'avviso in un'ora inserendo un numero nella casella **Max per ora**.

Se non si inserisce un numero in questa casella, non vi sarà alcun limite sul numero di volte che questo avviso potrà essere inviato. Si consiglia di limitare gli avvisi a uno o due per ora e di inserire un numero maggiore per gli invii successivi, se necessario. Se viene specificato un numero elevato o nessun numero, le cassette postali del destinatario potrebbero essere sovraccaricate da avvisi continui.

- 8 Fare clic su **Salva** per completare l'azione.

Viene visualizzato l'elenco Avvisi.

Per attivare un avviso, è possibile specificare tre tipi di condizioni:

- Tipo evento: la gravità dell'evento.
- Server: il server associato all'evento.
- Codice evento: codice numerico che identifica un tipo particolare di evento.

Per ogni tipo di condizione, è possibile scegliere uno dei due operatori:

- È uno qualsiasi dei seguenti valori
- Non è alcuno dei seguenti valori

Per ogni tipo di condizione, specificare gli appropriati parametri:

- Tipo evento. È possibile selezionare un tipo o una combinazione di tipi tra **Informazioni**, **Avviso**, **Grave**. Fare clic su un tipo di evento per specificarlo. Per specificare più tipi, tenere premuto il tasto Ctrl facendo clic sui tipi di evento. È possibile specificare uno, due o tutti e tre i tipi.
- Server. È possibile selezionare uno o più server dall'elenco dei server disponibili. Fare clic sul nome del server per specificarlo. Per specificare più server, tenere premuto il tasto Ctrl facendo clic sui nomi dei server. È possibile specificare il numero di server desiderato.
- Codice evento. Immettere il codice numerico. Per immettere più codici numerici, separarli con virgole o utilizzare il tasto Ripristina per immettere ciascun codice in una riga separata. Vedere ["Messaggi e codici di eventi di sistema"](#) a pagina 187.

Combinando più condizioni, è possibile definire gli avvisi che riguardano numerose condizioni di sistema.

Nota: Se si definisce più di una condizione, le condizioni verranno trattate come se fossero collegate dall'operatore booleano "AND". Ciò significa che Enforce Server invia l'avviso solo se tutte le condizioni vengono soddisfatte. Ad esempio, se si definisce una condizione di tipo di evento e una condizione server, Enforce Server invia l'avviso solo se si verifica l'evento specificato sul server indicato.

Vedere ["Informazioni sugli avvisi di sistema"](#) a pagina 183.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Vedere ["Report di eventi di sistema"](#) a pagina 172.

Informazioni sulla verifica registri

L'installazione di Symantec Data Loss Prevention include diversi file di registro. Questi file forniscono informazioni sulla comunicazione del server, su Enforce Server nonché sul funzionamento del server di rilevamento, sul rilevamento incidenti, ecc.

Per impostazione predefinita, i registri per Enforce Server e il server di rilevamento vengono archiviati nelle seguenti directory:

- **Windows:** `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs`
- **Linux:** `/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/`

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Vedere anche il *Manuale di manutenzione del sistema di Symantec Data Loss Prevention* per informazioni aggiuntive sull'utilizzo dei registri.

Messaggi e codici di eventi di sistema

Gli eventi di sistema di Symantec Data Loss Prevention sono monitorati, segnalati e registrati. Ogni evento è identificato dal numero di codice elencato nelle tabelle.

Vedere ["Informazioni sugli eventi di sistema"](#) a pagina 171.

I report e gli elenchi di eventi di sistema possono essere filtrati in base ai codici di evento.

Vedere ["Report di eventi di sistema"](#) a pagina 172.

Nota: I numeri racchiusi tra parentesi graffe come {0}, indicano stringhe di testo inserite dinamicamente nel nome o nel messaggio descrittivo dell'evento.

Tabella 8-8 Eventi generali del server di rilevamento

Codice	Riepilogo	Descrizione
1000	Monitoraggio avviato	Tutti i processi di monitoraggio sono stati avviati.
1001	Monitoraggio locale avviato	Tutti i processi di monitoraggio sono stati avviati.
1002	Monitoraggio avviato	Alcuni processi di monitoraggio sono disattivati e non sono stati avviati.
1003	Monitoraggio locale avviato	Alcuni processi di monitoraggio sono disattivati e non sono stati avviati.
1004	Monitoraggio arrestato	Tutti i processi di monitoraggio sono stati arrestati.
1005	Monitoraggio locale arrestato	Tutti i processi di monitoraggio sono stati arrestati.
1006	Impossibile avviare {0}	Impossibile avviare il processo {0}. Per ulteriori informazioni, consultare i file di registro.
1007	{0} riavviato troppe volte	Il processo {0} è stato riavviato {1} volte negli ultimi {2} minuti.
1008	{0} inattivo	Interruzione del processo {0} prima del completamento della procedura di avvio.
1010	{0} riavviato	Il processo {0} è stato riavviato dopo un arresto imprevisto.
1011	{0} riavviato	{0} è stato riavviato perché non rispondeva.
1012	Impossibile avviare {0}	Impossibile eseguire il binding al socket di datagramma di arresto. Un nuovo tentativo verrà effettuato in seguito.
1013	{0} riavviato	Il binding al socket di arresto è stato eseguito.
1014	Spazio su disco insufficiente	Lo spazio sull'hard disk è insufficiente. L'uso del disco del server Symantec Data Loss Prevention è superiore al {0}%.

Tabella 8-9 Eventi di Endpoint Server

Codice	Riepilogo	Descrizione
1100	Aggregatore avviato	Nessuna
1101	Avvio aggregatore non riuscito	Errore di avvio dell'aggregatore. {0} Non verranno rilevati incidenti.
1102	Comunicazione con agenti non legacy disattivate	L'archivio Attendibilità e l'archivio chiavi SSL non sono configurati per questo server endpoint. Configurare la pagina del server per configurare l'archivio Attendibilità e l'archivio chiavi SSL.

Tabella 8-10 Eventi di configurazione di rilevamento

Codice	Riepilogo	Descrizione
1200	Politica caricata	"{0}" Politica "{0}" v{1} ({2}) caricata correttamente.
1201	{0} politiche caricate	Nessuna
1202	Nessuna politica caricata	Nessuna politica rilevante trovata. Non verrà rilevato alcun incidente. 1203 Politica "{0}" scaricata La politica "{0}" è stata scaricata.
1204	Politica "{0}" aggiornata	La politica "{0}" è stata aggiornata. La versione corrente della politica è {1}. Canali attivi: {2}.
1205	Limite di incidenti raggiunto per la politica "{0}"	La politica "{0}" ha trovato incidenti in più di {1} messaggi nelle ultime {2} ore. La politica non verrà applicata fino a che non viene modificata o fino alla scadenza del periodo per la reimpostazione di {2} ore.
1206	Tempo di attesa messaggi lungo	Il tempo di attesa dei messaggi è {0}:{1}:{2}:{3}.
1207	Impossibile caricare il profilo Vector Machine Learning	Impossibile caricare il profilo di Vector Machine Learning [{0}]. Per ulteriori informazioni, vedere i file di registro del server.
1208	Impossibile scaricare il profilo Vector Machine Learning	Impossibile scaricare il profilo di Vector Machine Learning [{0}]. Per ulteriori informazioni, vedere i file di registro del server.
1209	Profilo Vector Machine Learning caricato	Il profilo Vector Machine Learning [{0}] è stato caricato.
1210	Profilo Vector Machine Learning scaricato	Il profilo Vector Machine Learning [{0}] è stato scaricato.
1211	Training per Vector Machine Learning completato	Il training per il profilo Vector Machine Learning [{0}] è stato completato
1212	Training per Vector Machine Learning non riuscito	Il training per il profilo Vector Machine Learning [{0}] non è riuscito
1213	Timeout di {0} messaggi in Rilevamento di recente	Timeout di {0} messaggi in Rilevamento negli ultimi {1} minuti. Per ulteriori informazioni, attivare i file di registro di traccia esecuzione di Rilevamento.
1214	Rilevate regole di espressioni regolari con criteri non validi	Il set di politiche contiene regole di espressioni regolari con criteri non validi. Per ulteriori informazioni, vedere FileReader.log.

Tabella 8-11 Eventi di File Reader

Codice	Riepilogo	Descrizione
1301	File Reader avviato	Nessuna
1302	Avvio di File Reader non riuscito	Errore di avvio di File Reader. {0} Non verranno rilevati incidenti.
1303	Impossibile eliminare la cartella	File Reader non è riuscito a eliminare la cartella "{0}" nel file system. Identificare la causa poiché questo problema provocherà un malfunzionamento del sistema.
1304	Canale attivato	Il canale di monitoraggio "{0}" è stato attivato.
1305	Canale disattivato	Il canale di monitoraggio "{0}" è stato disattivato. 1306 Licenza ricevuta. {0}.
1306	Licenza ricevuta.	Nessuna
1307	avviato	Il processo è stato avviato.
1308	inattivo	Il processo è inattivo.

Tabella 8-12 Eventi ICAP

Codice	Riepilogo	Descrizione
1400	Canale ICAP configurato	Il canale è in modalità {0}
1401	Licenza non valida	Il canale ICAP non dispone di una licenza o la licenza è scaduta. Nessun incidente verrà rilevato o evitato mediante il canale ICAP.
1402	Rimozione contenuto non corretta	La regola di configurazione alla riga {0} è obsoleta o scritta in un formato di grammatica non appropriato. Rimuoverla dal file di configurazione o aggiornarla.
1403	Errore di memoria esaurita (Prevenzione Web) durante l'elaborazione del messaggio	Si è verificato un errore di memoria esaurita durante l'elaborazione della richiesta sulla connessione ID{0}. Modificare la configurazione per il carico del traffico.
1404	Limitazione host	Qualsiasi host (client ICAP) può connettersi al server ICAP.
1405	Errore di limitazione host	Impossibile ottenere l'indirizzo IP dell'host {0}.
1406	Errore di limitazione host	Impossibile ottenere l'indirizzo IP di qualsiasi host in Icap.AllowHosts.
1407	Traccia protocollo attivata	Sono state attivate le tracce disponibili in {0}.

Codice	Riepilogo	Descrizione
1408	Fattore di bilanciamento del carico non valido	Icap.LoadBalanceFactor è configurato su 0. Verrà considerato il valore 1.

Tabella 8-13 Eventi MTA

Codice	Riepilogo	Descrizione
1500	Licenza non valida	Il canale SMTP Prevent non dispone di una licenza o la licenza è scaduta. Nessun incidente sarà rilevato o evitato mediante il canale SMTP Prevent.
1501	Errore nell'indirizzo di binding	Impossibile eseguire il binding di {0}. Per ulteriori informazioni, verificare l'indirizzo configurato o il file di registro RequestProcessor. 1502 Errore di restrizione di MTA Impossibile risolvere l'host {0}.
1503	Tutti gli MTA con restrizioni	MTA client con restrizioni, ma nessun host risolto. Per ulteriori informazioni, verificare il file di registro RequestProcessor e correggere l'impostazione RequestProcessor.AllowHosts per questo server Prevent.
1504	Handshake TLS con downstream non riuscito	Handshake TLS con MTA downstream {0} non riuscito. Per ulteriori informazioni, consultare i file di registro Smtpprevent e RequestProcessor.
1505	Handshake TLS con downstream completato	Handshake TLS con MTA downstream {0} completato.

Tabella 8-14 Eventi dell'induttore di file

Codice	Riepilogo	Descrizione
1600	Cartella override non valida	Il canale di monitoraggio {0} ha una cartella di origine non valida: {1} Cartella utilizzata: {2}
1601	Cartella di origine non valida	Il canale di monitoraggio {0} ha una cartella di origine non valida: {1} Il canale è disattivato.

Tabella 8-15 Eventi di scansione di file

Codice	Riepilogo	Descrizione
1700	Avvio scansione non riuscito	Il target di Discover con ID {0} non esiste. 1701 Scansione terminata {0}
1702	Scansione completata	Il target di Discover "{0}" ha completato una scansione.

Codice	Riepilogo	Descrizione
1703	Avvio scansione non riuscito	{0}
1704	Elenco di condivisioni con errori	{0}
1705	Scansione pianificata non riuscita	Avvio di una scansione pianificata del target di Discover {0} non riuscito. {1}
1706	Sospensione scansione non riuscita	{0}
1707	Ripresa della scansione non riuscita	{0}
1708	Sospensione scansione pianificata non riuscita	La sospensione pianificata per la scansione del target di Discover {0} non è riuscita. {1}
1709	Ripresa scansione pianificata non riuscita	La sospensione pianificata per la scansione del target di Discover {0} non è riuscita. {1}
1710	Timeout durata massima scansione	Si è verificato il timeout del target di Discover "{0}" a causa della durata massima della scansione.
1711	Timeout durata massima scansione non riuscito	Timeout di durata massima per la scansione: {0}. Si è tuttavia verificato un errore durante il tentativo di interruzione della scansione.
1712	Timeout inattività scansione	Si è verificato il timeout di inattività della scansione per il target di Discover "{0}".
1713	Timeout inattività scansione non riuscito	Timeout di durata massima di inattività per la scansione: {0}. Si è tuttavia verificato un errore durante il tentativo di interruzione della scansione.
1714	Scansione terminata - Stato server non valido	La scansione del target di Discover "{0}" è terminata con lo stato "{1}" in quanto il Discover Server {2} associato è passato inaspettatamente allo stato "{3}".
1715	Scansione terminata - Server rimosso	La scansione del target di Discover "{0}" è stata interrotta in quanto il Discover Server {1} associato non è più disponibile.
1716	Scansione terminata - Server riassegnato	La scansione del target di Discover "{0}" è stata interrotta in quanto il Discover Server {1} associato sta già eseguendo la scansione dei target di Discover "{2}".
1717	Scansione terminata - Transizione non riuscita	Impossibile gestire il cambiamento dello stato del Discover Server {1} durante la scansione del target di Discover "{0}". Per ulteriori informazioni, consultare i file di registro.

Codice	Riepilogo	Descrizione
1718	Avvio scansione non riuscito	Avvio della scansione del target di Discover "{0}" non riuscito. Per una descrizione dettagliata dell'errore, consultare i file di registro.
1719	Avvio scansione non riuscito a causa di un tipo di target non supportato	La scansione del target di Discover "{0}" non è riuscita in quanto il tipo di target non è più supportato.

Tabella 8-16 Eventi di archiviazione esterna di allegati incidenti

Codice	Riepilogo	Descrizione
1750	Migrazione allegati incidenti avviata	La migrazione degli allegati incidenti dal database alla directory di archiviazione esterna è stata avviata.
1751	Migrazione allegati incidenti completata	La migrazione degli allegati incidenti dal database alla directory di archiviazione esterna è stata completata.
1752	Migrazione allegati incidenti non riuscita	Non è possibile migrare uno o più allegati incidenti dal database alla directory di archiviazione esterna. Per ulteriori informazioni, consultare il file di registro di Incident Persister. Dopo la risoluzione dell'errore, riavviare il servizio <code>SymantecDLPIncidentPersister</code> per riprendere la migrazione.
1753	Errore di migrazione allegati incidenti.	Si sono verificati uno o più errori durante la migrazione degli allegati incidenti dal database alla directory di archiviazione esterna. Per ulteriori informazioni, consultare il file di registro di Incident Persister. La migrazione continuerà e un nuovo tentativo verrà effettuato in seguito per l'allegato con errori.
1754	Impossibile aggiornare la pianificazione dell'eliminazione di allegati incidenti	Non è possibile aggiornare la pianificazione per l'eliminazione di allegati incidenti nella directory esterna. Per ulteriori informazioni, consultare il file di registro di Incident Persister.
1755	Eliminazione allegati incidenti avviata	L'eliminazione di allegati incidenti obsoleti dalla directory di archiviazione esterna è stata avviata.
1756	Eliminazione allegati incidenti completata	L'eliminazione di allegati incidenti obsoleti dalla directory di archiviazione esterna è stata completata.
1757	Eliminazione allegati incidenti non riuscita	Non è possibile eliminare uno o più allegati incidenti dalla directory di archiviazione esterna. Per ulteriori informazioni, consultare il file di registro di Incident Persister.

Codice	Riepilogo	Descrizione
1758	Directory di archiviazione esterna di allegati incidenti non accessibile	La directory di archiviazione esterna di allegati incidenti non è accessibile. Per ulteriori informazioni, consultare il file di registro di Incident Persister.
	Directory di archiviazione esterna di allegati incidenti accessibile	La directory di archiviazione esterna di allegati incidenti è accessibile.

Tabella 8-17 Eventi di Incident Persister e writer incidenti

Codice	Riepilogo	Descrizione
1800	Incident Persister non è in grado di elaborare l'incidente	Memoria esaurita in Incident Persister durante l'elaborazione dell'incidente {0}.
1801	Elaborazione incidente {0} con Incident Persister non riuscita	
1802	Ricevuto incidente danneggiato	È stato ricevuto un incidente danneggiato che è stato rinominato in {0}.
1803	Politica non configurata correttamente	Alla politica "{0}" non è associato il livello di gravità.
1804	Impossibile avviare Incident Persister	Non è possibile avviare Incident Persister. L'accesso alla cartella degli incidenti {0} non è riuscito. Verificare le autorizzazioni per la cartella.
1805	Incident Persister non è in grado di accedere alla	Incident Persister non è in grado di accedere alla cartella degli incidenti {0}. Verificare le autorizzazioni per la cartella.
1806	Avvio elaborazione regola di risposta non riuscito	L'avvio dell'elaborazione della regola di risposta {0} non è riuscito.
1807	Impossibile eseguire l'elaborazione della regola di risposta	L'esecuzione runtime del comando della regola di risposta non è riuscita con l'errore: {0}.
1808	Impossibile scrivere l'incidente	L'eliminazione del file temporaneo {0} obsoleto non è riuscita.
1809	Impossibile scrivere l'incidente	La ridenominazione del file incidente {0} temporaneo non è riuscita.
1810	Impossibile elencare gli incidenti	Non è possibile elencare i file incidente nella cartella {0}. Verificare le autorizzazioni per la cartella.
1811	Errore di invio dell'incidente	Si è verificato un errore imprevisto durante l'invio di un incidente. {0} Per ulteriori informazioni, consultare il file di registro del writer incidenti.

Codice	Riepilogo	Descrizione
1812	Writer incidenti arrestato	Non è possibile eliminare il file incidente {0} dopo l'invio. Eliminare il file manualmente, correggere il problema e riavviare il writer incidenti.
1813	Impossibile elencare gli incidenti	Non è possibile elencare i file incidente nella cartella {0}. Verificare le autorizzazioni per la cartella.
1814	Backlog della coda di incidenti	{0} incidenti nella coda di questo server.
1815	Spazio su disco insufficiente sul server incidenti	Lo spazio sull'hard disk per il server di archiviazione di dati sugli incidenti è insufficiente. L'uso del disco è superiore al {0}%.
1816	Impossibile aggiornare le statistiche della politica	L'aggiornamento delle statistiche della politica {0} non è riuscito.
1817	Limite massimo di incidenti giornalieri superato	Il numero massimo di incidenti giornalieri per la politica {0} è stato superato. Non verranno generati altri incidenti.
1818	Dimensione file incidente troppo grande: l'incidente è stato reso persistente con un numero limitato di componenti e/o violazioni	La dimensione del file incidente è troppo grande. L'incidente è stato reso parzialmente persistente con messageID {0}, nome file incidente {1}.
1821	Elaborazione di un incidente ricevuto dal gateway cloud non riuscita	Si è verificato un errore imprevisto durante l'invio di un incidente {0}

Tabella 8-18 Eventi di installazione o aggiornamento

Codice	Riepilogo	Descrizione
1900	Caricamento pacchetto di aggiornamento non riuscito	Si è verificato un errore di connessione al database durante il caricamento del pacchetto di aggiornamento {0}.
1901	Aggiornamento software non riuscito	L'aggiornamento del software dal pacchetto {0} non è riuscito. Consultare il file di registro del servizio di aggiornamento.

Tabella 8-19 Eventi di password di attivazione delle chiavi

Codice	Riepilogo	Descrizione
2000	Errori di attivazione delle chiavi	L'attivazione delle chiavi con la nuova password di attivazione non è riuscita. Il rilevamento basato sui profili dati esatti verrà disattivato.

Codice	Riepilogo	Descrizione
2001	Impossibile aggiornare la password di attivazione delle chiavi.	La password di attivazione delle chiavi non verrà aggiornata perché le chiavi di crittografia non sono attivate. Exact Data Matching verrà disattivato.

Tabella 8-20 Codice di eventi di reimpostazione della password amministratore

Codice	Riepilogo	Descrizione
2099	Password amministratore reimpostata	La password amministratore è stata reimpostata dallo strumento di reimpostazione password.

Tabella 8-21 Eventi di politica e amministratore di Manager

Codice	Riepilogo	Descrizione
2100	Amministratore salvato	Le impostazioni dell'amministratore sono state salvate.
2101	Origine dati rimossa	L'origine dati con ID {0} è stata rimossa da {1}.
2102	Origine dati salvata	L'origine dati {0} è stata salvata da {1}.
2103	Origine documento rimossa	L'origine documento con ID {0} è stata rimossa da {1}.
2104	Origine documento salvata	L'origine documento {0} è stata salvata da {1}.
2105	Nuovo protocollo creato	Il nuovo protocollo {0} è stato creato da {1}.
2106	Ordine protocollo modificato	Il protocollo {0} è stato spostato in {1} da {2}.
2107	Protocollo rimosso	Il protocollo {0} è stato rimosso da {1}.
2108	Protocollo salvato	Il protocollo {0} è stato modificato da {1}.
2109	Utente rimosso	L'utente con ID {0} è stato rimosso da {1}.
2110	Utente salvato	L'utente {0} è stato salvato da {1}.
2111	Rilevata ricerca in esecuzione	L'esecuzione di uno dei plug-in di ricerca di attributi non è stata completata normalmente e un thread è ancora in esecuzione nel sistema. Potrebbe essere necessario riavviare il manager.
2112	Plug-in di ricerca di attributi personalizzati caricati	Sono stati caricati i seguenti plug-in di ricerca di attributi: {0}.
2113	Nessun plug-in di ricerca di attributi personalizzati caricato	Non è stato trovato alcun plug-in di ricerca di attributi personalizzati.

Codice	Riepilogo	Descrizione
2114	Ricerca di attributi personalizzati non riuscita	Timeout del plug-in di ricerca {0}. Il plug-in non è stato caricato.
2115	Ricerca di attributi personalizzati non riuscita	La creazione di istanze del plug-in di ricerca {0} non è riuscita. Il plug-in non è stato caricato. Messaggio di errore: {1}
2116	Politica modificata	La politica {0} è stata modificata da {1}.
2117	Politica rimossa	La politica {0} è stata rimossa da {1}.
2118	Invio di avviso o report pianificato non riuscito. {0}	configurato da {1} contiene i seguenti indirizzi e-mail non raggiungibili: {2}. Gli indirizzi non sono corretti o il server di e-mail non consente l'invio a tali indirizzi.
2119	Impostazioni di sistema modificate	Le impostazioni di sistema sono state modificate da {0}.
2120	Impostazioni di posizioni endpoint modificate	Le impostazioni di posizioni endpoint sono state modificate da {0}.
2121	Account "{1}" bloccato	Il numero massimo di {0} tentativi di accesso consecutivi è stato superato per l'account "{1}" e di conseguenza l'account è stato bloccato.
2122	Azioni FlexResponse caricate	Sono state caricate le seguenti azioni FlexResponse: {0}.
2123	Nessuna azione FlexResponse caricata.	Non è stata trovata alcuna azione FlexResponse.
2124	Rilevata azione FlexResponse in esecuzione.	L'esecuzione di uno dei plug-in FlexResponse non è stata completata normalmente e un thread è ancora in esecuzione nel sistema. Potrebbe essere necessario riavviare il manager.
2125	Impostazioni di Data Insight modificate.	Le impostazioni di Data Insight sono state modificate da {0}.
2126	Configurazione agente creata	La configurazione agente {0} è stata creata da {1}.
2127	Configurazione agente modificata	La configurazione agente {0} è stata modificata da {1}.
2128	Configurazione agente rimossa	La configurazione agente {0} è stata rimossa da {1}.
2129	Configurazione agente applicata	La configurazione agente {0} è stata applicata a Endpoint Server {1} da {2}.
2130	Origine connessione directory rimossa	L'origine della connessione alla directory con ID {0} è stata rimossa da {1}.

Codice	Riepilogo	Descrizione
2131	Origine connessione directory salvata	L'origine della connessione alla directory {0} è stata salvata da {1}.
2132	Attività di risoluzione dei problemi agente	L'attività di risoluzione dei problemi agente di tipo {0} è stata creata dall'utente {1}.
2133	File di autorità di certificazione generato.	È stato generato il file di autorità di certificazione {0}.
2134	File di autorità di certificazione danneggiato.	Il file di autorità di certificazione {0} è danneggiato.
2135	Password modificata per il file di autorità di certificazione.	La password per il file di autorità di certificazione {0} è stata modificata. Il nuovo file di autorità di certificazione è {1}.
2136	Archivio chiavi server generato.	L'archivio chiavi server {0} è stato generato per Endpoint Server {1}.
2137	Archivio chiavi server mancante o danneggiato.	L'archivio chiavi server {0} per Endpoint Server {1} non è presente o è danneggiato.
2138	Archivio Attendibilità server generato.	L'archivio Attendibilità server {0} è stato generato per Endpoint Server {1}.
2139	Archivio Attendibilità server mancante o danneggiato.	L'archivio Attendibilità server {0} per Endpoint Server {1} non è presente o è danneggiato.
2140	Certificati client e chiave generati.	Certificati client e chiave generati.
2141	Pacchetto di installazione agente generato.	È stato generato il pacchetto di installazione agente per le piattaforme {0}.

Tabella 8-22 Eventi relativi alle gestione delle licenze e all'attivazione delle chiavi di Enforce

Codice	Riepilogo	Descrizione
2200	Contratto di licenza con l'utente finale accettato	Il contratto di licenza con l'utente finale di Symantec Data Loss Prevention è stato accettato da {0}, {1}, {2}.
2201	Licenza non valida	Nessuna
2202	Licenza scaduta	Una o più licenze del prodotto sono scadute. Alcune funzionalità del sistema potrebbero essere disattivate. Verificare lo stato delle licenze nella pagina delle impostazioni del sistema.

Codice	Riepilogo	Descrizione
2203	La licenza sta per scadere	Una o più licenze del prodotto scadranno tra breve. Verificare lo stato delle licenze nella pagina delle impostazioni del sistema.
2204	Nessuna licenza	La licenza non esiste, è scaduta o non è valida. Non verrà rilevato alcun incidente.
2205	Chiavi attivate	Le chiavi di crittografia sono state attivate dalla chiave master.
2206	Attivazione chiavi non riuscita	L'attivazione manuale delle chiavi di crittografia non è riuscita. Per ulteriori informazioni, consultare i file di registro di Enforce Server. Non sarà possibile creare nuovi profili dati esatti.
2207	Attivazione chiavi automatica	Le chiavi crittografiche sono state attivate automaticamente.
2208	Attivazione chiavi manuale necessaria	L'attivazione automatica delle chiavi crittografiche non è configurata. L'accesso come amministratore è necessario per attivare le chiavi crittografiche. I profili dati esatti non saranno creati fino all'accesso dell'amministratore.

Tabella 8-23 Eventi Manager principali

Codice	Riepilogo	Descrizione
2300	Spazio su disco insufficiente	Lo spazio sull'hard disk è insufficiente. L'uso del disco di Symantec Data Loss Prevention Enforce Server è superiore al {0}%.
2301	Spazio tabella quasi pieno	Lo spazio tabella Oracle {0} è pieno per più del {1}%.
2302	{0} non risponde	L'heartbeat del server di rilevamento {0} non è stato aggiornato per almeno 20 minuti.
2303	Configurazione di monitoraggio modificata	La configurazione di monitoraggio {0} è stata modificata da {1}.
2304	Aggiornamento del sistema caricato	È stato caricato un aggiornamento del sistema che ha effetto sui componenti seguenti: {0}.
2305	Server SMTP non raggiungibile.	Server SMTP non raggiungibile. Non è possibile inviare avvisi o report pianificati.
2306	Enforce Server avviato	Enforce Server è stato avviato.
2307	Enforce Server arrestato	Enforce Server è stato arrestato.

Codice	Riepilogo	Descrizione
2308	Eccezione nel programma di aggiornamento stato di monitoraggio	Si è verificata un'eccezione generale nel programma di aggiornamento dello stato di monitoraggio. Per ulteriori informazioni, consultare i file di registro di Enforce Server.
2309	Aggiornamento statistiche sistema non riuscito	Non è possibile aggiornare le statistiche sull'uso del disco e del database di Enforce Server. Per ulteriori informazioni, consultare i file di registro di Enforce Server.
2310	Errore di aggregazione statistiche	Si è verificato un errore generale nell'attività di riepilogo delle statistiche. Per ulteriori informazioni, consultare i file di registro di Enforce Server.
2311	Versioni non corrispondenti	La versione di Enforce è {0} mentre quella del monitor è {1}.
2312	Eliminazione incidenti non riuscita	Eliminazione incidenti non riuscita.
2313	Eliminazione incidenti completata	L'eliminazione degli incidenti è stata eseguita per {0} e {1} incidenti sono stati eliminati.
2314	Eliminazione dati endpoint non riuscita	Eliminazione dati endpoint non riuscita.
2315	Spazio su disco insufficiente sul server incidenti	Lo spazio sull'hard disk per il server di archiviazione di dati sugli incidenti è insufficiente. L'uso del disco è superiore al {0}%.
2316	Più di {0} incidenti attualmente contenuti nel database	Più di {0} incidenti persistenti possono ridurre le prestazioni del database.
2318	Processo per contrassegnare gli incidenti da eliminare avviato.	Processo per contrassegnare gli incidenti da eliminare avviato.
2319	Processo per contrassegnare gli incidenti da eliminare terminato.	Processo per contrassegnare gli incidenti da eliminare terminato.

Tabella 8-24 Eventi di supporto per le versioni di Monitor

Codice	Riepilogo	Descrizione
2320	Versione obsoleta	Il server di rilevamento non è supportato quando la relativa versione è antecedente di almeno due versioni a quella di Enforce Server. La versione di Enforce è {0} e quella di questo server di rilevamento è {1}. Eseguire l'upgrade di questo server di rilevamento.

Codice	Riepilogo	Descrizione
2321	Versione meno recente della versione di Enforce	Enforce non sarà utilizzabile con questo server di rilevamento e non sarà in grado di inviargli aggiornamenti. Gli incidenti del server di rilevamento saranno ricevuti ed elaborati normalmente. La versione di Enforce è {0} e quella di questo server di rilevamento è {1}.
2322	Versione meno recente della versione di Enforce	Le funzionalità presenti nelle versioni più recenti di Enforce relative a questo tipo di server di rilevamento non sono supportate da questo server di rilevamento. La versione di Enforce è {0} e quella di questo server di rilevamento è {1}.
2323	Versione secondaria meno recente della versione secondaria di Enforce	Le funzionalità presenti nelle versioni più recenti di Enforce relative a questo tipo di server di rilevamento non sono supportate da questo server di rilevamento. La versione di Enforce è {0} e quella di questo server di rilevamento è {1}. Eseguire l'upgrade di questo server di rilevamento.
2324	Versione più recente della versione di Enforce	Il server di rilevamento non è supportato quando la relativa versione è più recente della versione di Enforce Server. La versione di Enforce è {0} e quella di questo server di rilevamento è {1}. Eseguire l'upgrade di Enforce o il downgrade del server di rilevamento.

Tabella 8-25 Eventi di reporting di Manager

Codice	Riepilogo	Descrizione
2400	Esportazione archivio Web completata	L'archivio "{0}" per l'utente {1} è stato creato.
2401	Esportazione archivio Web annullata	L'archivio {0} per l'utente {1} è stato annullato.
2402	Esportazione archivio Web non riuscita	La creazione dell'archivio {0} per l'utente {1} non è riuscita. Il report specificato include più di {2} incidenti.
2403	Esportazione archivio Web non riuscita	La creazione dell'archivio {0} per l'utente {1} non è riuscita. Si è verificato un errore in corrispondenza dell'incidente {2}.
2404	Impossibile eseguire il report pianificato	Il report pianificato {0} non è valido ed è stato rimosso.
2405	Impossibile eseguire il report pianificato	Nel report pianificato {0} di proprietà di {1} si è verificato un errore: {2}.
2406	Pianificazione report disattivata	Non è possibile eseguire il report pianificato {0} di proprietà di {1} in quanto la pianificazione di report è disattivata.

Codice	Riepilogo	Descrizione
2407	Pianificazione report disattivata	Non è possibile eseguire il report pianificato in quanto la pianificazione di report è disattivata.
2408	Impossibile eseguire il report pianificato	Non è possibile connettersi al server di posta durante il recapito del report pianificato {0}{1}.
2409	Impossibile eseguire il report pianificato	L'utente {0} non è più nel ruolo {1} a cui il report pianificato {2} appartiene. La pianificazione è stata eliminata.
2410	Impossibile eseguire il report pianificato	Non è possibile eseguire il report pianificato {0} per l'utente {1} in quanto l'account è bloccato.
2411	Report pianificato inviato	Il report pianificato {0} di proprietà di {1} è stato inviato.
2412	Esportazione XML del report non riuscita	Esportazione XML del report da parte dell'utente [{0}] non riuscita.
2420	Impossibile eseguire la distribuzione del report pianificato da parte del proprietario dei dati	Il proprietario dei dati non può distribuire il report {0} (id={1}) poiché l'invio dei dati del report è stato disattivato.
2421	Distribuzione report da parte del proprietario dei dati non riuscita	La distribuzione del report {0} (id={1}) da parte del proprietario dei dati non è riuscita.
2422	Distribuzione report da parte del proprietario dei dati completata	La distribuzione del report {0} (id={1}) da parte del proprietario dei dati è stata completata con {2} incidenti per {3} proprietari dei dati. L'esportazione di {4} incidenti per {5} proprietari dei dati non è riuscita.
2423	Distribuzione report al proprietario dei dati non completata	La dimensione massima consentita per la distribuzione del report {1} (id={2}) al proprietario dei dati "{0}" è stata superata. Solo i primi {3} incidenti sono stati inviati a "{0}".

Tabella 8-26 Eventi di messaggistica

Codice	Riepilogo	Descrizione
2500	Errore imprevisto durante l'elaborazione di un messaggio	Si è verificato un errore imprevisto in {0} durante l'elaborazione di un messaggio. Per ulteriori informazioni, vedere il file di registro.
2501	Limitazione memoria disattivata	{0} x {1} byte devono essere disponibili per la limitazione della memoria. Sono disponibili solo {2} byte. La limitazione della memoria è stata disattivata.

Tabella 8-27 Eventi di comunicazione dei server di rilevamento

Codice	Riepilogo	Descrizione
2600	Errore di comunicazione	Si è verificato un errore imprevisto durante l'invio di {1} aggiornamenti a {0}. {2} Per ulteriori informazioni, vedere i file di registro del controller di monitoraggio.
2650	Errore di comunicazione (VML)	Si è verificato un errore imprevisto durante l'invio del set di configurazione degli aggiornamenti di profilo {0} a {1} {2}. Per ulteriori informazioni, consultare i file di registro del controller di monitoraggio.

Tabella 8-28 Eventi del Controller di monitoraggio

Codice	Riepilogo	Descrizione
2700	Controller di monitoraggio avviato	Il servizio Controller di monitoraggio è stato avviato.
2701	Controller di monitoraggio arrestato	Il servizio Controller di monitoraggio è stato arrestato.
2702	Aggiornamento trasferito a {0}	Il pacchetto di aggiornamento {1} è stato trasferito al server di rilevamento {0}.
2703	Trasferimento dell'aggiornamento completato	Il pacchetto di aggiornamento {0} è stato trasferito a tutti i server di rilevamento.
2704	Aggiornamento di {0} non riuscito	Il trasferimento del pacchetto di aggiornamento al server di rilevamento {0} non è riuscito.
2705	Trasferimento file di configurazione completato	Il file di configurazione {0} è stato trasferito al server di rilevamento.
2706	Richiesta di caricamento registri inviata.	La richiesta di caricamento registri {0} è stata inviata.
2707	Impossibile inviare la richiesta di caricamento registri	Si è verificato un errore recuperabile durante il tentativo di invio della richiesta di caricamento registri {0}.
2708	Impossibile inviare la richiesta di caricamento registri	Si è verificato un errore irrecuperabile durante il tentativo di invio della richiesta di caricamento registri {0}.
2709	Certificato integrato utilizzato	Il certificato integrato è utilizzato per assicurare la comunicazione tra Enforce Server e i server di rilevamento.
2710	Certificato generato dall'utente utilizzato	Il certificato generato dall'utente è utilizzato per assicurare la comunicazione tra Enforce Server e i server di rilevamento.

Codice	Riepilogo	Descrizione
2711	Ora non corrispondente tra Enforce e Monitor. Questo problema può influire su alcune funzionalità nel sistema.	Ora non corrispondente tra Enforce e Monitor. È consigliabile impostare l'ora nel Monitor mediante la sincronizzazione automatica dell'ora.
2712	Connesso al rilevatore di cloud	Connesso al rilevatore di cloud.
2713	Rilevatore di cloud disconnesso	Errore {0} - Verificare le impostazioni di rete.

Tabella 8-29 Eventi di acquisizione del pacchetto

Codice	Riepilogo	Descrizione
2800	Directory di spool non valida configurata per acquisizione del pacchetto	L'acquisizione del pacchetto è stata configurata con una directory di spool: {0}. Questa directory non ha privilegi di scrittura. Verificare le autorizzazioni per la directory e il file di configurazione del monitor. Al termine, riavviare il monitor.
2801	Invio elenco di NIC non riuscito. {0}	{0}.

Tabella 8-30 Eventi e messaggi dell'indice EDM

Codice	Riepilogo	Descrizione
2900	Ricerca profilo EDM non riuscita	{0}.
2901	Chiavi non attivate	Exact Data Matching verrà disattivato fino all'attivazione delle chiavi di crittografia.
2902	Cartella di indicizzazione non accessibile	Impossibile elencare file nella cartella di indicizzazione {0}. Verificare la configurazione e le autorizzazioni per la cartella.
2903	Cartella di indicizzazione creata	La cartella di indicizzazione {0} specificata nella configurazione non esisteva ed è stata creata.
2904	Cartella di indicizzazione non valida	La cartella di indicizzazione {0} specificata nella configurazione non esiste.
2905	Creazione profilo dati esatti non riuscita	Il file di dati per il profilo dati esatti "{0}" non è stato creato. Per ulteriori informazioni, consultare i file di registro di Enforce Server.
2906	Indicizzazione annullata	La creazione del profilo di database "{0}" è stata annullata.
2907	Replica annullata	La replica del profilo di database "{0}" versione {1} al server {2} è stata annullata.

Codice	Riepilogo	Descrizione
2908	Replica non riuscita	La connessione al database è stata interrotta durante la replica del profilo di database {0} al server {1}.
2909	Replica non riuscita	Si è verificato un errore di database durante la replica del profilo di database {0} al server {1}.
2910	Impossibile rimuovere il file di indice	L'eliminazione del file di indice {1} del profilo di database {0} non è riuscita.
2911	Impossibile rimuovere il file di indice	L'eliminazione del file di indice {1} del profilo di database {0} non è riuscita.
2912	Impossibile rimuovere il file orfano	La rimozione del file di indice del profilo di database orfano {0} non è riuscita.
2913	Replica non riuscita	La replica del profilo di database {0} al server {2} non è riuscita.{1} Per ulteriori informazioni, consultare il file di registro del controller di monitoraggio.
2914	Replica completata	La replica del profilo di database {0} al server {2} è stata completata. Il file {1} è stato trasferito correttamente.
2915	Replica completata	La replica del profilo di database {0} al server {2} è stata completata. I file {1} sono stati trasferiti correttamente.
2916	Profilo database rimosso	Il profilo di database {0} è stato rimosso. Il file {1} è stato eliminato.
2917	Profilo database rimosso	Il profilo di database {0} è stato rimosso. I file {1} sono stati eliminati correttamente.
2918	Profilo database caricato	Il profilo di database {0} è stato caricato da {1}.
2919	Profilo database non caricato	Il profilo di database {0} non è stato caricato.
2920	Impossibile caricare il profilo database	{2} Non verrà rilevato alcun incidente in base al profilo di database "{0}" versione {1}.
2921	Caricamento profilo database non riuscito	{2} Il caricamento del profilo di database "{0}" versione {1} potrebbe non riuscire in futuro senza il riavvio del server di rilevamento.
2922	Impossibile trovare contenuto registrato	Il contenuto registrato con ID {0} non è stato trovato nel database durante l'indicizzazione.
2923	Errore di database	Si è verificato un errore di database durante l'indicizzazione. {0}

Codice	Riepilogo	Descrizione
2924	Arresto del processo durante l'indicizzazione	Il processo è stato arrestato durante l'indicizzazione. È possibile che una parte del contenuto registrato non sia stata creata.
2925	Politica non accurata	In base a {1}, la politica "{0}" presenta una o più regole con una precisione di rilevazione non soddisfacente. {2}
2926	Profilo dati esatti creato	{0} creato dal file "{1}". Righe elaborate: {2} Righe non valide: {3} Il profilo dati esatto verrà replicato in tutti i server Symantec Data Loss Prevention.
2927	Sincronizzazione gruppo utenti "{0}" non riuscita	Le seguenti directory di gruppi di utenti sono state rimosse/rinominate nel server di directory e non sono state sincronizzate: {1}. Aggiornare la pagina Gruppo utenti "{2}" per riflettere tali modifiche.
2928	Uno o più profili EDM sono obsoleti e devono essere reindicizzati	Verificare la pagina "Gestisci > Profili dati > Dati esatti". I seguenti profili DM sono obsoleti: {0}.

Tabella 8-31 Eventi e messaggi dell'indice IDM

Codice	Riepilogo	Descrizione
3000	{0}	{1} Il profilo documento non è stato creato.
3001	Indicizzazione annullata	La creazione del profilo documento "{0}" è stata annullata.
3002	Replica annullata	La replica del profilo documento "{0}" versione {1} nel server {2} è stata annullata.
3003	Replica non riuscita	La connessione al database è stata interrotta durante la replica del profilo documento "{0}" versione {1} nel server {2}.
3004	Replica non riuscita	Si è verificato un errore di database durante la replica del profilo documento "{0}" versione {1} nel server {2}.
3005	Impossibile rimuovere il file di indice	L'eliminazione del file di indice {2} del profilo documento "{0}" versione {1} non è riuscita.
3006	Impossibile rimuovere il file di indice	L'eliminazione dei file di indice {2} del profilo documento "{0}" versione {1} non è riuscita.
3007	Impossibile rimuovere il file orfano	{0}

Codice	Riepilogo	Descrizione
3008	Replica non riuscita	La replica del profilo documento "{0}" versione {1} nel server {3} non è riuscita. {2}\nPer ulteriori informazioni, consultare il file di registro del controller di monitoraggio.
3009	Replica completata	La replica del profilo documento "{0}" versione {1} nel server {3} è stata completata. Il file {2} è stato trasferito correttamente.
3010	Replica completata	La replica del profilo documento "{0}" versione {1} nel server {3} è stata completata.\nI file {2} sono stati trasferiti correttamente.
3011	Profilo documento rimosso	Il profilo documento "{0}" versione {1} è stato rimosso. Il file {2} è stato eliminato.
3012	Profilo documento rimosso	Il profilo documento "{0}" versione {1} è stato rimosso. I file {2} sono stati eliminati correttamente.
3013	Profilo documento caricato	Il profilo documento "{0}" versione {1} da {2} è stato caricato.
3014	Profilo documento scaricato	Il profilo documento "{0}" versione {1} è stato scaricato.
3015	Impossibile caricare il profilo documento	{2}Nessun incidente verrà rilevato in base al profilo documento "{0}" versione {1}.
3016	Impossibile scaricare il profilo documento	{2} È possibile che il profilo documento "{0}" versione {1} non venga ricaricato in futuro senza il riavvio del monitor.
3017	Profilo documento creato	"{0}" creato da "{1}". Vi sono {2} file accessibili nella radice di contenuti. {3} Il profilo contiene l'indice per {4} documenti. {5} Il profilo documento verrà ora replicato in tutti i server Symantec Data Loss Prevention.
3018	Profilo documento	È stata raggiunta la dimensione massima per {0}. Sono stati indicizzati solo {1} documenti su {2}.
3019	Nessun documento da indicizzare	L'origine documento "{0}" non ha trovato file da indicizzare.
3020	Profilo documento creato	"{0}" creato da "{1}". Vi sono {2} file accessibili nella radice di contenuti. {3} Il profilo contiene l'indice per {4} documenti. Rispetto all'ultima indicizzazione: {5} nuovi documenti aggiunti, {6} documenti aggiornati, {7} documenti non modificati e {8} documenti rimossi. Il profilo documento verrà ora replicato in tutti i server Symantec Data Loss Prevention.
3021	Nessun documento da indicizzare	Il nuovo profilo IDM remoto per l'origine "{0}" è identico alla versione importata precedente.

Codice	Riepilogo	Descrizione
3022	Conversione profilo	Il profilo IDM {0} è stato convertito in {1} nell'endpoint.
3023	Utilizzo della memoria per profili IDM endpoint	La dimensione ottenuta sommando la dimensione del profilo IDM {0} e quella dei profili già distribuiti è troppo grande per l'endpoint. Sarà disponibile solo una corrispondenza esatta.

Tabella 8-32 Eventi di ricerca di attributi

Codice	Riepilogo	Descrizione
3100	Attributi non validi rilevati con il plug-in di ricerca di script	Attributi non validi o non sicuri passati da Standard In sono stati rimossi durante l'esecuzione dello script. Per ulteriori informazioni, consultare i file di registro.
3101	Attributi non validi rilevati con il plug-in di ricerca di script	Attributi non validi o non sicuri passati da Standard Out sono stati rimossi durante l'esecuzione dello script. Per ulteriori informazioni, consultare i file di registro.

Tabella 8-33 Eventi di stub di Monitor

Codice	Riepilogo	Descrizione
3200	AggregatorStub avviato	Nessuna
3201	{0} aggiornato	Elenco di aggiornamenti: {1}.
3202	Archivio {0} inizializzato	Elementi iniziali: {1}.
3203	{0} ricevuti	Dimensione: {1} byte.
3204	FileReaderStub avviato	Nessuna
3205	IncidentWriterStub avviato	Utilizzata cartella di incidenti di prova {0}.
3206	Configurazione ricevuta per {0}	{1}.
3207	PacketCaptureStub avviato	Nessuna
3208	RequestProcessorStub avviato	Nessuna
3209	Impostazioni avanzate ricevute	Nessuna
3210	Impostazioni aggiornate	Impostazioni aggiornate: {0}.
3211	Impostazioni avanzate caricate	Nessuna
3212	UpdateServiceStub avviato	Nessuna

Codice	Riepilogo	Descrizione
3213	DetectionServerDatabaseStub avviato	Nessuna

Tabella 8-34 Eventi di acquisizione del pacchetto

Codice	Riepilogo	Descrizione
3300	Acquisizione del pacchetto avviata	L'acquisizione del pacchetto è stata avviata.
3301	Impossibile avviare l'acquisizione sul dispositivo {0}	Il dispositivo {0} è configurato per l'acquisizione, ma non è stato inizializzato. Per ulteriori informazioni, consultare PacketCapture.log.
3302	Impossibile elevare il livello di privilegi di PacketCapture	Non è stato possibile elevare il livello di privilegi di PacketCapture. È probabile che alcune attività di inizializzazione non riusciranno. Verificare la proprietà e le autorizzazioni del file eseguibile di PacketCapture.
3303	Impossibile abbassare il livello di privilegi di PacketCapture	È ancora possibile ripristinare i privilegi root dopo tale operazione. PacketCapture verrà arrestato.
3304	L'acquisizione del pacchetto è stata riavviata in quanto è disponibile ulteriore spazio su disco	L'acquisizione del pacchetto è stata riavviata poiché ulteriore spazio è disponibile sulle unità disco rigido del monitor.
3305	L'acquisizione del pacchetto è stata arrestata a causa del limite di spazio su disco	L'elaborazione dei pacchetti con acquisizione del pacchetto è stata arrestata in quanto lo spazio disponibile sulle unità disco rigido del monitor è insufficiente.
3306	Driver Endace DAG non disponibile	L'acquisizione del pacchetto non è riuscita ad attivare il supporto per il dispositivo Endace. Per ulteriori informazioni, consultare PacketCapture.log.
3307	Driver PF_RING non disponibile	L'acquisizione del pacchetto non è riuscita ad attivare i dispositivi che utilizzano l'interfaccia PF_RING. Per ulteriori informazioni, consultare PacketCapture.log e i file di registro del sistema in uso.
3308	Driver PACKET_MMAP non disponibile	L'acquisizione del pacchetto non è riuscita ad attivare i dispositivi che utilizzano l'interfaccia PACKET_MMAP. Per ulteriori informazioni, consultare PacketCapture.log e i file di registro del sistema in uso.

Codice	Riepilogo	Descrizione
3309	{0} non disponibile	L'acquisizione del pacchetto non è riuscita a caricare {0}. Non è disponibile alcuna interfaccia di acquisizione nativa. Per ulteriori informazioni, consultare PacketCapture.log.
3310	Traffico {0} non acquisito	Il traffico {0} non è stato acquisito negli ultimi {1} secondi. Verificare i filtri di protocollo e il traffico inviato alla NIC di monitoraggio.
3311	Impossibile creare la directory	Impossibile creare la directory {0} : {1}.

Tabella 8-35 Eventi di raccolta dei registri

Codice	Riepilogo	Descrizione
3400	Impossibile aggiungere file al file zip	I file richiesti per la raccolta non sono stati scritti su un file di archivio.
3401	Impossibile inviare la raccolta di file di registro	I file richiesti per la raccolta non sono stati inviati.
3402	Impossibile leggere le proprietà di registrazione	Un file di proprietà non è stato letto. Le modifiche alla configurazione della registrazione non sono state applicate.
3403	Impossibile decomprimere il pacchetto di configurazione registri	Il file zip contenente le modifiche alla configurazione della registrazione non è stato decompresso. Le modifiche alla configurazione non saranno applicate.
3404	Impossibile trovare file da raccogliere	Non sono stati trovati file per l'ultima richiesta di raccolta registri inviata al server.
3405	Creazione file non riuscita	Non è stato possibile creare file per la raccolta di file di registro endpoint.
3406	Limite di utilizzo del disco superato	Impossibile creare file a causa di spazio su disco insufficiente.
3407	Limite massimo di file aperti superato	Impossibile creare file in quanto è già stato raggiunto il limite massimo di file aperti.

Tabella 8-36 Eventi di Enforce SPC

Codice	Riepilogo	Descrizione
3500	Server SPC registrato.	Server SPC registrato. ID istanza prodotto [{0}].
3501	La registrazione del server SPC è stata annullata.	La registrazione del server SPC è stata annullata. ID istanza prodotto [{0}].

Codice	Riepilogo	Descrizione
3502	Certificato autofirmato generato.	Certificato autofirmato generato. Alias certificato [{0}].

Tabella 8-37 Eventi di origini dati di utenti Enforce

Codice	Riepilogo	Descrizione
3600	Importazione utente completata.	L'importazione dell'utente dall'origine {0} è stata completata.
3601	Importazione utente non riuscita.	L'importazione dell'utente dell'origine dati {0} non è riuscita.
3602	Dati utente relativi a incidenti aggiornati	I dati utente relativi a {0} eventi incidente esistenti sono stati aggiornati.

Tabella 8-38 Eventi relativi alla distribuzione di elementi di catalogo

Codice	Riepilogo	Descrizione
3700	Impossibile scrivere l'elemento di catalogo	L'eliminazione del file temporaneo {0} obsoleto non è riuscita.
3701	Impossibile rinominare l'elemento di catalogo	La ridenominazione del file elemento di catalogo temporaneo {0} non è riuscita.
3702	Impossibile elencare elementi di catalogo	Non è possibile elencare file di elementi di catalogo nella cartella {0}. Verificare le autorizzazioni per la cartella.
3703	Errore di invio di elementi di catalogo	Si è verificato un errore imprevisto durante l'invio di un elemento di catalogo.{0}Per ulteriori informazioni, consultare il file di registro di File Reader.
3704	Impossibile eliminare file con File Reader.	L'eliminazione del file catalogo {0} dopo l'invio non è riuscita.\nEliminare il file manualmente, correggere il problema e riavviare File Reader.
3705	Impossibile elencare file di elementi di catalogo	Non è possibile elencare file di elementi di catalogo nella cartella {0}. Verificare le autorizzazioni per la cartella.
3706	Configurazione non valida.	La proprietà {0} è stata configurata con un valore {1} non valido. Assicurarsi di specificare un valore corretto.
3707	Scansione non riuscita: impossibile aggiornare il catalogo di rilevamento riparazioni	Timeout dell'aggiornamento del catalogo di rilevamento riparazioni dopo {0} secondi per il target {1}.

Tabella 8-39 Eventi del database di server di rilevamento

Codice	Riepilogo	Descrizione
3800	DetectionServerDatabase avviato	Nessuna
3801	Avvio di DetectionServerDatabase non riuscito	Errore di avvio di DetectionServerDatabase. Motivo: {0}.
3802	Porta non valida per DetectionServerDatabase	Impossibile recuperare la porta per il processo DetectionServerDatabase per l'ascolto della connessione. Motivo: {0}. Verificare se l'impostazione del file di proprietà ha un numero di porta valido.

Tabella 8-40 Eventi del livello di comunicazione endpoint

Codice	Riepilogo	Descrizione
3900	Errore di comunicazione interno.	Errore di comunicazione interno. Per informazioni sugli errori, vedere {0}. Viene eseguita la ricerca della stringa {1}.
3901	Eventi di sistema eliminati.	È stato superato il limite di eventi di sistema. {0} eventi sono stati eliminati. Codice di errore interno = {1}.

Tabella 8-41 Codici di eventi di comunicazione dell'agente

Codice	Riepilogo	Descrizione
4000	Errore nell'handshaker agente	Errore nell'handshaker agente. Per informazioni sugli errori, vedere {0}. Viene eseguita la ricerca della stringa {1}.

Tabella 8-42 Eventi di errore dell'applicazione relativi al livello di comunicazione della replica del controller di monitoraggio

Codice	Riepilogo	Descrizione
4050	Errore di persistenza batch di dati agente	Si è verificato un errore imprevisto durante l'operazione per rendere persistenti i dati agente: {0}. Per ulteriori informazioni, consultare i file di registro del controller di monitoraggio.
4051	Errore di persistenza batch attributi di stato per agenti	Non è stato possibile rendere persistenti i dati di attributi di stato per {0} agenti. Per ulteriori informazioni, consultare i file di registro del controller di monitoraggio.
4052	Persistenza batch eventi per agenti	Non è stato possibile rendere persistenti i dati di eventi per {0} agenti. Per ulteriori informazioni, consultare i file di registro del controller di monitoraggio.

Tabella 8-43 Codici di evento relativi ai servizi Web di Enforce Server

Codice	Riepilogo	Descrizione
4101	Errore nel database di servizi di esecuzione regole di risposte durante il recupero della richiesta	Il recupero della richiesta non è riuscito nemmeno dopo {0} tentativi. La connessione al database è ancora inattiva. Il servizio verrà arrestato.

Tabella 8-44 Eventi di registrazione al servizio cloud

Codice	Riepilogo	Descrizione
4200	Registrazione al servizio cloud: certificato client ricevuto da Symantec Managed PKI Service	Registrazione al servizio cloud: certificato client ricevuto da Symantec Managed PKI Service.
4201	Registrazione al servizio cloud: errore di richiesta del certificato client a Symantec Managed PKI Service	ERRORE {0}.
4205	Il certificato di Symantec Managed PKI Service scade tra {0} giorni	Il certificato di Symantec Managed PKI Service scade tra {0} giorni.
4206	Certificato di Symantec Managed PKI Service scaduto	Certificato di Symantec Managed PKI Service scaduto.
4210	Errore nel pacchetto di registrazione al servizio cloud	Contenuto file di registrazione non valido.
4211	Errore nel pacchetto di registrazione al servizio cloud	File di registrazione mancante nel pacchetto ZIP.
4212	Pacchetto di registrazione rilevatore di cloud non valido	Le informazioni sul rilevatore non corrispondono alla configurazione esistente.

Tabella 8-45 Codice di evento del rilevatore di cloud

Codice	Riepilogo	Descrizione
4300	Rilevatore di cloud creato in Enforce	Rilevatore di cloud {0} creato in Enforce.

Tabella 8-46 Codice di evento relativi ai profili di gruppi di utenti

Codice	Riepilogo	Descrizione
4400	Uno o più profili di gruppi di utenti non sono aggiornati e devono essere reindicizzati.	Per ulteriori informazioni, visitare la pagina Gestisci > Politiche > Gruppi utenti . I seguenti profili di gruppi di utenti non sono aggiornati: {0}.

Tabella 8-47 Codice di evento di Cloud Operations

Codice	Riepilogo	Descrizione
4701	Eventi o notifiche di Cloud Operations	Cloud Operations ha emesso un evento o una notifica sul servizio cloud.

Gestione del database di Symantec Data Loss Prevention

Il capitolo contiene i seguenti argomenti:

- [Utilizzo di strumenti diagnostici di database di Symantec Data Loss Prevention](#)
- [Visualizzazione di allocazione spazi tabelle e file di dati](#)
- [Visualizzazione dei dettagli della tabella](#)
- [Controllo della preparazione del database all'aggiornamento](#)

Utilizzo di strumenti diagnostici di database di Symantec Data Loss Prevention

La console di amministrazione di Enforce Server consente di visualizzare informazioni diagnostiche sugli spazi tabelle e sulle tabelle del proprio database per consentire una migliore gestione delle risorse di database. È possibile verificare quanto sono pieni gli spazi tabelle e le tabelle e se i file nelle tabelle sono estendibili automaticamente per contenere più dati. Queste informazioni possono aiutare a gestire il database e a comprendere in quali casi è opportuno attivare la funzionalità di estensione automatica di Oracle su file di dati e in quali altri è meglio gestire le risorse di database in altro modo. È anche possibile generare un report di database dettagliato da condividere con il supporto tecnico Symantec per richiedere assistenza in merito alla risoluzione dei problemi di database.

È possibile visualizzare l'allocazione degli spazi tabelle, inclusi dimensione, utilizzo memoria, estensibilità, stato e numero di file in ogni spazio tabella. È anche possibile visualizzare il nome, la dimensione e l'impostazione di estensione automatica per ogni file di uno spazio

tabella. Inoltre, è possibile visualizzare allocazioni a livello di tabelle per tabelle di dati di incidente, altre tabelle, indici e tabelle di oggetti localizzatori (LOB).

È possibile generare un report di database completo in formato HTML da condividere in qualunque momento con il supporto tecnico Symantec facendo clic su **Ottieni report completo**. I dati nel report possono aiutare il supporto tecnico Symantec a risolvere i problemi del proprio database.

Vedere ["Creazione di un report di database"](#) a pagina 217.

Visualizzazione di allocazione spazi tabelle e file di dati

È possibile visualizzare allocazioni spazi tabelle e file di dati nella pagina **Riepilogo spazi tabelle database** (**Sistema > Database > Riepilogo spazi tabelle**).

Nella pagina **Riepilogo spazi tabelle database** sono visualizzate le seguenti informazioni:

- **Nome** : il nome dello spazio tabella.
- **Dimensioni** : le dimensioni dello spazio tabella in megabyte.
- **Usati (%)** : la percentuale dello spazio tabella attualmente in uso. Questa percentuale viene calcolata in base ai valori **Usati (MB)** e **Dimensione**. Non tiene in considerazione il valore **Estendibile fino a (MB)**.
- **Usati (MB)** : la quantità dello spazio tabella attualmente in uso, in megabyte.
- **Estendibile fino a (MB)** : le dimensioni a cui lo spazio tabella può essere esteso. Questo valore è basato sulle impostazioni Estensione automatica dei file all'interno dello spazio tabella.
- **Stato** : lo stato corrente dello spazio tabella secondo la percentuale dello spazio tabella attualmente in uso, in base alle soglie di avviso. Se state utilizzando le impostazioni di soglia di avviso predefinite, lo stato è:
 - **OK** : lo spazio tabella è pieno per meno dell'80% o lo spazio tabella può essere automaticamente esteso.
 - **Avviso** : lo spazio tabella è pieno per una percentuale tra l'80 e il 90%. Se viene visualizzato un avviso in uno spazio tabella, considerare l'ipotesi di attivare l'estensione automatica sui file di dati nello spazio tabella o di estendere il valore massimo per l'estensibilità automatica dei file di dati.
 - **Grave** : lo spazio tabella è pieno oltre il 90%. Se viene visualizzato un avviso grave in uno spazio tabella, attivare l'estensione automatica sui file di dati nello spazio tabella, estendere il valore massimo per l'estensibilità automatica dei file di dati o determinare se è possibile eliminare alcuni dati nello spazio tabella.

- **Numero di file** : il numero di file di dati nello spazio tabella.

Selezionare uno spazio tabella dall'elenco per visualizzare i dettagli relativi ai file contenuti. La vista del file dello spazio tabella visualizza le seguenti informazioni:

- **Nome** : il nome del file.
- **Dimensioni** : le dimensioni del file, in megabyte.
- **Estendibile automaticamente** : consente di specificare se il file viene esteso automaticamente in base all'impostazione di estensione automatica del file nel database Oracle.
- **Estendibile fino a (MB)** : le dimensioni massime a cui il file può essere esteso, in megabyte.
- **Percorso** : il percorso del file.

Regolazione delle soglie di avviso per l'utilizzo dello spazio tabella in database di grande dimensioni

Se il database contiene molti dati (1 terabyte o più), è possibile regolare le soglie di avviso per l'utilizzo dello spazio tabella. Per database di grandi dimensioni, Symantec consiglia di regolare la soglia di **Avviso** sull'85% pieno e la soglia **Grave** sul 95% pieno. Per database più grandi è possibile impostare queste soglie su valori ancora superiori. È possibile specificare questi valori nel file `Manager.properties`.

Per regolare le soglie di avviso dell'utilizzo dello spazio tabella

- 1 Aprire il file **Manager.properties** in un editor di testo.
- 2 Impostare le soglie di **Avviso** e **Grave** sui seguenti valori:

```
com.vontu.manager.tablespaceThreshold.warning=85  
com.vontu.manager.tablespaceThreshold.severe=95
```
- 3 Salvare le modifiche nel file **Manager.properties** e chiuderlo.
- 4 Riavviare il servizio Symantec DLP Manager per applicare le modifiche.

Creazione di un report di database

È possibile generare un report di database completo in formato HTML in qualsiasi momento facendo clic su **Ottieni report completo** nella pagina **Riepilogo spazi tabelle database**. Il report database include le seguenti informazioni:

- Informazioni dettagliate sul database
- Distribuzione dei dati di incidente
- Distribuzione di dati di messaggio

- Informazioni sul gruppo di politiche
- Informazioni sulla politica
- Informazioni sull'agente endpoint
- Informazioni del server di rilevamento (monitor)

Il supporto tecnico Symantec può richiedere questo report per avere indicazioni utili alla risoluzione di problemi di database.

Per generare un report di database

- 1 Accedere a **Sistema > Database > Riepilogo spazi tabelle**.
- 2 Fare clic su **Ottieni report completo**.
- 3 Per la creazione del report è necessario attendere qualche minuto. Per visualizzare il collegamento al report, aggiornare la schermata dopo qualche minuto.
- 4 Per aprire o salvare il report, fare clic sul collegamento sopra la tabella **Allocazioni spazi tabelle**. Per praticità il collegamento include il timestamp del report.
- 5 Nella finestra di dialogo **Apri file** scegliere se aprire il file o salvarlo.
- 6 Per visualizzare il report, aprirlo in un browser Web o in un editor di testo.
- 7 Per aggiornare il report, fare clic su **Aggiorna report completo**.

Visualizzazione dei dettagli della tabella

È possibile visualizzare allocazioni a livello di tabella nella pagina **Dettagli tabella database** (**Sistema > Database > Dettagli tabella**). La visualizzazione di allocazioni a livello di tabella può essere utile dopo una grande eliminazione di dati per visualizzare la deallocazione di spazio all'interno di segmenti di database. È possibile aggiornare le informazioni visualizzate in questa pagina facendo clic su **Aggiorna dati tabella** in qualunque momento.

La pagina **Dettagli tabella database** visualizza le allocazioni a livello di tabella in una delle quattro schede:

- **Tabelle incidenti** : questa scheda elenca tutte le tabelle di dati di incidente nello schema del database Symantec Data Loss Prevention. La scheda visualizza le seguenti informazioni:
 - **Nome tabella** : il nome della tabella.
 - **Nello spazio tabella** : il nome dello spazio tabella che contiene la tabella.
 - **Dimensioni (MB)** : le dimensioni della tabella, in megabyte.
 - **% riempimento** : la percentuale della tabella attualmente in uso.
- **Altre tabelle** : questa scheda elenca tutte le altre tabelle nello schema. La scheda visualizza le seguenti informazioni:

- **Nome tabella** : il nome della tabella.
- **Nello spazio tabella** : il nome dello spazio tabella che contiene la tabella.
- **Dimensioni (MB)** : le dimensioni della tabella, in megabyte.
- **% riempimento** : la percentuale della tabella attualmente in uso.
- **Indici** : questa tabella elenca tutti gli indici nello schema. La scheda visualizza le seguenti informazioni:
 - **Nome indice** : il nome dell'indice.
 - **Nome tabella** : il nome della tabella che contiene l'indice.
 - **Nello spazio tabella** : il nome dello spazio tabella che contiene la tabella.
 - **Dimensioni (MB)** : le dimensioni della tabella, in megabyte.
 - **% riempimento** : la percentuale della tabella attualmente in uso.
- **Segmenti LOB** : questa tabella elenca tutte le tabelle di oggetti localizzatori nello schema. La scheda visualizza le seguenti informazioni:
 - **Nome tabella** : il nome della tabella.
 - **Nome colonna** : il nome della colonna di tabella contenente i dati LOB.
 - **Nello spazio tabella** : il nome dello spazio tabella che contiene la tabella.
 - **Dimensioni segmento LOB (MB)** : le dimensioni del segmento LOB, in megabyte.
 - **Dimensioni indice LOB** : le dimensioni dell'indice LOB, in megabyte.
 - **% riempimento** : la percentuale della tabella attualmente in uso.

Nota: Il valore di percentuale di utilizzo per ogni tabella visualizza la percentuale di tabella attualmente in uso come riportato dal database di Oracle in blu scuro. Include inoltre un intervallo di percentuale di utilizzo stimata supplementare in blu chiaro. Symantec Data Loss Prevention calcola questo intervallo in base all'utilizzo della spazio tabella.

Controllo della preparazione del database all'aggiornamento

Utilizzare lo strumento Preparazione aggiornamento per confermare che il database Oracle è pronto a eseguire l'upgrade alla versione successiva di Symantec Data Loss Prevention.

Lo strumento Preparazione aggiornamento testa i seguenti punti nello schema del database:

- Versione di Oracle

- Patch di Oracle
- Autorizzazioni
- Spazi tabelle
- Schema esistente rispetto allo schema standard
- Real Application Cluster
- Change Data Capture
- Colonne virtuali
- Tabelle partizionate
- Overflow numerico
- Spazio temporaneo di Oracle

Tabella 9-1 elenca le attività completate per eseguire lo strumento.

Tabella 9-1 Utilizzo dello strumento Preparazione aggiornamento

Passaggio	Operazione	Dettagli
1	Individuare la versione più recente dello strumento.	Vedere "Preparazione dello strumento di preparazione aggiornamento" a pagina 220.
2	Creare l'account database dello strumento Preparazione aggiornamento.	Vedere "Creazione dell'account database dello strumento Preparazione aggiornamento" a pagina 221.
3	Eseguire lo strumento.	Vedere "Esecuzione dello strumento di preparazione aggiornamento per Symantec Data Loss Prevention versione 14.x e 15.0" a pagina 222.
4	Esaminare i risultati di Preparazione aggiornamento.	Vedere "Esame dei risultati di Preparazione aggiornamento" a pagina 224.

Preparazione dello strumento di preparazione aggiornamento

La preparazione dello strumento di preparazione aggiornamento include il download dello strumento e il suo spostamento nell'Enforce Server.

Per preparare lo strumento di preparazione aggiornamento

- ◆ È possibile ottenere la versione più recente dello strumento (per le versioni principali e secondarie di Symantec Data Loss Prevention) in Download software.

Il nome file dello strumento è `Symantec_DLP_15.1_Update_Readiness_Tool_15.`

`1.0-1.zip`. La versione dello strumento cambia quando vengono distribuiti strumenti aggiornati.

Symantec consiglia di scaricare lo strumento nella directory `DLPDownloadHome\15.1\`.

Nota: Esaminare il file Leggimi incluso nello strumento per vedere l'elenco delle versioni di Symantec Data Loss Prevention che lo strumento può testare.

Vedere ["Controllo della preparazione del database all'aggiornamento"](#) a pagina 219.

Creazione dell'account database dello strumento Preparazione aggiornamento

Per poter eseguire lo strumento Preparazione aggiornamento, è necessario creare un account database.

Per creare il nuovo account database dello strumento Preparazione aggiornamento

- 1 Accedere alla cartella `/script` in cui è stato estratto lo strumento Preparazione aggiornamento.

- 2 Avviare SQL*Plus:

```
sqlplus /nolog
```

- 3 Eseguire lo script `oracle_create_user.sql`:

```
SQL> @oracle_create_user.sql
```

- 4 Nella richiesta **Please enter the password for sys user** (Immettere la password per l'utente sys), immettere la password per l'utente SYS.
- 5 Nella richiesta **Please enter sid** (Immettere il sid), immettere un nome utente.
- 6 Nella richiesta **Please enter required username to be created** (Immettere il nome utente necessario da creare), immettere un nome per il nuovo account database di Preparazione aggiornamento.
- 7 Nella richiesta **Please enter a password for the new username** (Immettere una password per il nuovo nome utente), immettere una password per il nuovo account database di Preparazione aggiornamento.

Utilizzare le seguenti linee guida per creare una password accettabile:

- Le password non possono contenere più di 30 caratteri.
- Le password non possono contenere virgolette doppie, virgole o barre rovesciate.
- Evitare di utilizzare il carattere &.
- Le password distinguono tra maiuscole e minuscole per impostazione predefinita. È possibile modificare la distinzione maiuscole/minuscole attraverso un'impostazione di configurazione di Oracle.
- Se la password utilizza caratteri speciali diversi da `_#` o `$`, o se comincia con un numero, è necessario racchiuderla tra virgolette doppio durante la configurazione.

Conservare il nome utente e la password in un luogo sicuro per riferimento futuro. Utilizzare nome utente e password per eseguire lo strumento Preparazione aggiornamento.

- 8 Come utente sysdba del database, concedere l'autorizzazione per *nome utente dello schema* di Symantec Data Loss Prevention per i seguenti oggetti di database:

```
sqlplus sys/[schema user name] as sysdba  
GRANT READ,WRITE ON directory DATA_PUMP_DIR TO [schema user name];  
GRANT SELECT ON dba_registry_history TO [schema user name];  
GRANT SELECT ON dba_temp_free_space TO [schema user name];
```

Vedere ["Preparazione dello strumento di preparazione aggiornamento"](#) a pagina 220.

Vedere ["Controllo della preparazione del database all'aggiornamento"](#) a pagina 219.

Esecuzione dello strumento di preparazione aggiornamento per Symantec Data Loss Prevention versione 14.x e 15.0

Dopo aver individuato lo strumento di preparazione aggiornamento, eseguirlo dal prompt dei comandi sul server in cui è installato Enforce Server.

Per eseguire lo strumento Preparazione aggiornamento

- 1 Da una finestra di comando, accedere alla directory in cui è stato estratto lo strumento Preparazione aggiornamento.
- 2 Eseguire lo strumento Preparazione aggiornamento utilizzando il seguente comando:

```
java UpdateReadinessTool
--username <schema user name>
--password <password>
--sid <database_system_id>
--readiness_username <readiness_username>
--readiness_password <readiness_password>
[--quick]
```

La seguente tabella identifica i comandi:

<code><schema user name></code>	Il nome utente dello schema Symantec Data Loss Prevention.
<code><password></code>	La password dello schema Symantec Data Loss Prevention.
<code><database_system_id></code>	L'ID di sistema del database (SID), in genere "protect".
<code><readiness_username></code>	L'account utente del database dello strumento Preparazione aggiornamento creato. Vedere "Creazione dell'account database dello strumento Preparazione aggiornamento" a pagina 221.
<code><readiness_password></code>	La password per l'account utente del database dello strumento Preparazione aggiornamento creato.
<code>[--quick]</code>	Il comando facoltativo esegue solo il controllo degli oggetti di database e ignora il test di preparazione aggiornamento.

Al termine del test, i risultati si trovano in un file di registro nella directory `/output`. Questa directory si trova dove è stato estratto lo strumento Preparazione aggiornamento. Se non si include `[--quick]` quando si esegue lo strumento, il completamento del test può richiedere fino a un'ora. È possibile verificare lo stato del test esaminando i file di registro nella directory `/output`.

Vedere ["Preparazione dello strumento di preparazione aggiornamento"](#) a pagina 220.

Vedere ["Esame dei risultati di Preparazione aggiornamento"](#) a pagina 224.

Esame dei risultati di Preparazione aggiornamento

Dopo l'esecuzione, lo strumento Preparazione aggiornamento restituisce i risultati dei test in un file di registro. [Tabella 9-2](#) elenca i risultati riassunti nel file di registro.

Tabella 9-2 Risultati di Preparazione aggiornamento

Stato	Descrizione
Riuscito	Gli elementi visualizzati in questa sezione sono confermati e pronti per l'aggiornamento.
Avviso	Se non corretti, gli elementi visualizzati in questa sezione possono impedire il corretto upgrade del database.
Errore	Questi elementi impediscono il completamento dell'upgrade e devono essere corretti.

Vedere ["Controllo della preparazione del database all'aggiornamento"](#) a pagina 219.

Utilizzo di Symantec Information Centric Encryption

Il capitolo contiene i seguenti argomenti:

- [Informazioni su SymantecInformation Centric Encryption](#)
- [Informazioni sull'utilità Symantec ICE](#)
- [Panoramica sull'implementazione delle funzionalità di Information Centric Encryption](#)
- [Configurazione di Enforce Server per connettersi al cloud ICE Symantec](#)

Informazioni su SymantecInformation Centric Encryption

Symantec Information Centric Encryption (ICE) è una soluzione di riduzione del rischio che consente a dipendenti, partner e individui affidabili di condividere in modo sicuro le e-mail e i file della società. Symantec ICE può aiutare a rilevare le e-mail e i file riservati e a crittografarli affinché siano accessibili solo agli utenti autorizzati.

Le tecnologie di crittografia tipiche possono portare alla perdita di dati dopo la decrittografia delle e-mail o dei file. Una volta decrittografati, possono essere inviati ad altri individui e non sono più protetti. Tuttavia, la tecnologia di crittografia di ICE crittografa e protegge le e-mail e i file per la loro intera esistenza, indipendentemente dalla posizione.

Quando si determina che una e-mail o un file è riservato o di particolare importanza, ICE la crittografia avviene automaticamente sul posto utilizzando la libreria e i servizi di crittografia di ICE. Una volta crittografato, solo gli utenti autorizzati possono leggerlo.

ICE inoltre comprende la Information Centric Encryption Cloud Console, che fornisce informazioni sull'utilizzo delle e-mail e dei file crittografati da ICE. È possibile monitorare chi accede a queste e-mail e file, da dove viene effettuato l'accesso e come vengono utilizzati. È inoltre possibile utilizzare ICE Cloud Console per impostare autorizzazioni di gruppo specifiche. È possibile impostare le autorizzazioni per il salvataggio, la condivisione e la modifica di e-mail e file per gruppi di politiche. È inoltre possibile revocare l'accesso a e-mail e file singoli o revocare i diritti di accesso a e-mail e file per specifici gruppi di politiche.

Il modo e il tipo di protezione dipende dalla soluzione Symantec integrata con ICE. ICE è progettato per estendere la crittografia end-to-end a più prodotti Symantec, migliorare la protezione dei messaggi di posta elettronica e dei file. [\[Unresolved xref\]](#) elenca i modi più comuni in cui è possibile utilizzare ICE con prodotti Symantec.

Informazioni sull'utilità Symantec ICE

L'utilità Symantec ICE consente a un utente autorizzato di decrittografare un file crittografato da ICE. Se un utente tenta di accedere a un file protetto da ICE, l'utilità ICE richiede l'autenticazione dell'utente. Se l'utente è autenticato, l'utilità ICE decrittografa il file. Inoltre, l'utilità ICE applica i set di autorizzazioni assegnati all'utente nella ICE Cloud Console. Ad esempio, se la stampa è stata disattivata per l'utente o il gruppo di politiche, l'utente non può stampare il documento.

Nota: Nei dispositivi mobili, l'utilità ICE si chiama ICE Workspace. È possibile ottenere ICE Workspace con l'app VIP Access for Mobile.

L'utilità ICE è sensibile al contesto, ossia riconosce l'ambiente di un utente. L'utilità ICE può essere distribuita in due tipi di ambienti: ambienti gestiti e ambienti non gestiti.

- Negli ambienti gestiti, l'organizzazione fornisce e mantiene i dispositivi da cui gli utenti accedono ai file protetti.
Negli ambienti gestiti, l'utilità ICE sfrutta le politiche e i controlli di sicurezza stabiliti dall'organizzazione sui dispositivi degli utenti. In questo ambiente, l'utilità ICE concede all'utente una maggiore flessibilità per la decrittografia e l'utilizzo di file protetti. I file si aprono nella loro app nativa e l'utente ha pieno accesso al file per modificare, condividere, salvare, salvare con nome e stampare il file. Gli utenti devono autenticarsi almeno una volta ogni 180 giorni.
La versione gestita dell'utilità ICE funziona allo stesso modo sulle piattaforme Windows e macOS; tuttavia, la versione di Windows del pacchetto di installazione dell'utilità ICE include anche l'agente ICT. Gli utenti possono installare l'agente ICT solo se ICT è stato implementato e il pacchetto di installazione dell'agente ICT è stato configurato correttamente.
- Negli ambienti non gestiti, come quelli dei partner o quelli in cui i dipendenti utilizzano i propri dispositivi, non è possibile controllare direttamente i dispositivi degli utenti.

Poiché non è possibile controllare direttamente la sicurezza dei dispositivi degli utenti negli ambienti non gestiti, l'utilità ICE fornisce sicurezza aggiuntiva. L'utilità ICE impone restrizioni più rigorose sulla disponibilità e la modalità di decrittografia di un file e consente un maggiore controllo del contenuto tramite set di autorizzazioni.

Quando gli utenti tentano di aprire un file protetto su un dispositivo senza l'utilità ICE, viene richiesto di scaricare l'utilità ICE.

Gli utenti devono autenticarsi ogni 24 ore la prima volta che tentano di accedere a un file crittografato.

- In Windows, i tipi di file supportati vengono aperti nella loro app nativa, ma vengono imposte le autorizzazioni assegnate all'utente. In questo modo, se la stampa è stata limitata per l'utente o il gruppo di politiche, l'utente non può stampare il file.
File che ICE non supporta aperti nella loro app nativa, ma ICE non applica le autorizzazioni.
- In macOS, i tipi di file supportati vengono aperti nella loro app nativa, se l'autorizzazione **Modifica** è attivata nella Information Centric Encryption Cloud Console. Tuttavia, se le autorizzazioni includono **blocco del contenuto** o restrizioni di **stampa**, tali file vengono aperti nell'applicazione Mac Preview in modalità di sola visualizzazione. Per i formati Office, i file crittografati da ICE lanciano l'applicazione Microsoft Office. Se l'utente non dispone di Microsoft Office installato, i documenti Word vengono aperti in Mac TextEdit e i file Excel e PowerPoint vengono aperti in Mac Preview.
Su iOS, i tipi di file supportati vengono aperti in modalità di sola visualizzazione indipendentemente dalle autorizzazioni assegnate all'utente.

In tutti gli ambienti, quando l'utente ha terminato con il file, l'utilità ICE lo crittografa di nuovo, assicurando la sicurezza del file per tutta la sua esistenza.

Nota: Se a un utente è consentito salvare il file con un nuovo nome, il nuovo file non è crittografato.

Panoramica sull'implementazione delle funzionalità di Information Centric Encryption

I passaggi di alto livello per l'implementazione di Information Centric Encryption con Symantec Data Loss Prevention vengono forniti in [Tabella 10-1](#). I passaggi specifici dell'attività sono forniti negli argomenti indicati nella colonna Dettagli.

Per ulteriori informazioni su Information Centric Encryption, fare riferimento alla *Guida alla distribuzione di Symantec Information Centric Encryption* all'indirizzo <http://www.symantec.com/docs/DOC9707>.

Tabella 10-1 Panoramica sull'implementazione delle funzionalità di Information Centric Encryption

Passaggio	Azione	Dettagli
1	A seconda delle esigenze di sicurezza dell'organizzazione, installare una o entrambe le seguenti licenze: <ul style="list-style-type: none"> ■ Network Protect ICE ■ Endpoint Prevent ICE 	Vedere "Installazione di un nuovo file di licenza" a pagina 237.
2	Configurare Enforce Server per connettersi al cloud ICE Symantec.	Vedere "Configurazione di Enforce Server per connettersi al cloud ICE Symantec" a pagina 229.
3	Configurare le azioni di regola di risposta della politica per proteggere i file riservati utilizzando la crittografia di ICE.	<p>Vedere "Configurazione dell'azione Endpoint Prevent: crittografia" a pagina 1550.</p> <p>Vedere "Configurazione dell'azione Network Protect: crittografia file" a pagina 1567.</p> <p>Vedere "Configurazione dell'azione di FlexResponse server" a pagina 1516.</p>
4	Configurare Network Protect per attivare la protezione della crittografia di ICE per i target di scansione supportati.	Vedere "Configurazione di Network Protect per condivisioni file" a pagina 1928.
5	Configurare le azioni della regola di risposta della politica di Cloud Service for Email per proteggere e-mail ed allegati sensibili o allegati di e-mail sensibili utilizzando la crittografia ICE.	Vedere "Crittografia delle e-mail cloud con Symantec Information Centric Encryption" a pagina 2282.

Passaggio	Azione	Dettagli
6	<p>Attivare la crittografia ICE in Endpoint Prevent per proteggere i file riservati che vengono memorizzati</p> <ul style="list-style-type: none"> ■ sugli endpoint ■ nei dispositivi rimovibili connessi agli endpoint ■ in applicazioni di archiviazione cloud 	<p>Vedere "Impostazioni di Crittografia incentrata sulle informazioni per i DLP Agent" a pagina 2133.</p> <p>Vedere "Configurazione Network Protect per i server SharePoint" a pagina 1956.</p>
7	<p>Scaricare e installare l'utilità ICE su tutti i dispositivi gestiti all'interno dell'organizzazione. L'utilità ICE è necessaria affinché gli utenti possano accedere ai file crittografati da ICE.</p> <p>Gli utenti di dispositivi non gestiti dovranno scaricare e installare l'utilità ICE quando tentano di accedere ai file crittografati da ICE per la prima volta su un dispositivo particolare.</p>	<p>L'utilità ICE è scaricabile da Symantec FileConnect.</p> <p>Vedere "Informazioni sull'utilità Symantec ICE" a pagina 226.</p>

Configurazione di Enforce Server per connettersi al cloud ICE Symantec

Dopo aver installato la licenza ICE Endpoint Prevent o la licenza ICE Network Protect, oppure dopo aver caricato il pacchetto di registrazione del Servizio cloud DLP per e-mail, è necessario configurare l'Enforce Server per connettersi al cloud ICE Symantec. Questo passaggio è un requisito indispensabile per attivare le funzioni relative alla crittografia; per configurarlo si utilizza la console di configurazione di Enforce Server.

Vedere ["Installazione di un nuovo file di licenza"](#) a pagina 237.

Per configurare Enforce Server per connettersi al cloud ICE Symantec:

- 1 Accedere a **Sistema > Impostazioni > Generale** e fare clic su **Configura**.
- 2 Nella schermata **Modifica impostazioni generali**, scorrere fino alla sezione **Impostazioni di accesso a cloud ICE Symantec**.

3 Digitare i seguenti dettagli del cloud ICE Symantec nei campi forniti:

- ID cliente
- ID dominio
- URL servizio
- ID utente servizio
- Password servizio

Nota: Ottenere queste informazioni dalla pagina **Impostazioni > Configurazione avanzata > Servizi esterni** della console del cloud ICE. La password di servizio è visibile solo quando si autorizza un servizio esterno per la prima volta. Se la password di servizio è stata persa, il solo modo per vederla è di ottenerne una nuova.

4 Fare clic su **Salva**.

5 Per attivare e configurare la funzionalità ICE in Symantec Data Loss Prevention, effettuare una o più delle seguenti operazioni, a seconda delle licenze ICE installate:

- Configurare Network Protect per attivare la protezione con crittografia di ICE per i target di scansione supportati.
Vedere "[Configurazione di Network Protect per condivisioni file](#)" a pagina 1928.
- Configurare Cloud Service for Email per consentire la crittografia della posta elettronica ICE di Office 365 e Gmail nel cloud.
Vedere la *Guida all'implementazione di Cloud Service for Email* nel centro di supporto Symantec <http://www.symantec.com/docs/DOC9008>.
- Attivare la crittografia ICE in Endpoint Prevent per proteggere i file riservati archiviati
 - su endpoint
 - nei dispositivi rimovibili connessi agli endpoint
 - in applicazioni di archiviazione cloudVedere "[Impostazioni di Crittografia incentrata sulle informazioni per i DLP Agent](#)" a pagina 2133.

Utilizzo di Symantec Information Centric Tagging

Il capitolo contiene i seguenti argomenti:

- [Informazioni sull'integrazione di Information Centric Tagging con Data Loss Prevention](#)
- [Panoramica dei passaggi per associare Information Centric Tagging a Data Loss Prevention](#)
- [Integrazione di Enforce Server con il server ICT](#)
- [Importazione della tassonomia di classificazione ICT](#)
- [Modifica dell'URL del servizio Web ICT](#)

Informazioni sull'integrazione di Information Centric Tagging con Data Loss Prevention

Symantec Information Centric Tagging (ICT) è un prodotto di classificazione di dati che definisce e supporta l'applicazione di tag e filigrane a e-mail e file. Information Centric Tagging fa inoltre parte dell'Information Centric Security Module (ICSM) con licenza separata. ICSM offre anche la protezione dei dati mediante opzioni di crittografia, tra cui Symantec Information Centric Encryption (ICE), che possono essere associate a determinati tag.

La tassonomia di classificazione dei dati è una gerarchia di tag configurati a livello di società-ambito. Gli utenti finali applicano i tag a e-mail e file considerati riservati in base alla politica aziendale.

In Data Loss Prevention 15.1, è possibile importare la tassonomia di classificazione ICT nel database di Data Loss Prevention. È necessario eseguire l'importazione dalla console di amministrazione utilizzando il servizio Web ICT o un metodo statico basato su file XML. È possibile pianificare l'importazione o eseguirla subito.

Una tassonomia importata è un prerequisito per la creazione di regole di rilevamento mediante l'opzione *Classificazione corrispondenze contenuto*. Le regole si creano selezionando i tag visualizzati sulla console di amministrazione. Il contenuto contrassegnato da tag viene rilevato nei metadati di e-mail e file supportati.

Per ulteriori informazioni, consultare la documentazione relativa a Information Centric Tagging qui:

https://support.symantec.com/en_US/article.DOC11006.html

Vedere "Panoramica dei passaggi per associare Information Centric Tagging a Data Loss Prevention" a pagina 232.

Panoramica dei passaggi per associare Information Centric Tagging a Data Loss Prevention

La procedura avanzata per l'integrazione di Symantec Information Centric Tagging con Symantec Data Loss Prevention è disponibile in [Tabella 11-1](#). I passaggi specifici dell'attività sono forniti negli argomenti indicati nella colonna Dettagli.

Tabella 11-1 Panoramica delle funzionalità di implementazione di Information Centric Tagging

Passaggio	Azione	Dettagli
1	Se si utilizza Symantec Data Loss Prevention 15.0 per definire le regole di rilevamento per cui sono stati immessi manualmente tag Information Centric Tagging, Symantec raccomanda di eliminare tali regole.	
2	Integrare l'Enforce Server con il server ICT definendo le proprie credenziali server ICT e l'URL del servizio Web ICT o un nome del percorso del file XML.	Vedere " Integrazione di Enforce Server con il server ICT " a pagina 233.
3	Pianificare o attivare l'importazione della tassonomia di classificazione Information Centric Tagging.	Vedere " Importazione della tassonomia di classificazione ICT " a pagina 235.
4	Definire le regole di rilevamento utilizzando la tassonomia importata.	Vedere " Configurazione della condizione Classificazione corrispondenze contenuto " a pagina 799.

Integrazione di Enforce Server con il server ICT

Per integrare Enforce Server con il server ICT, definire le impostazioni del server ICT. Le impostazioni del server ICT includono le credenziali del server ICT e l'URL del servizio Web ICT o un nome percorso XML.

Per definire le impostazioni del server Information Centric Tagging

- 1 Nella console di amministrazione di Enforce Server, accedere a **Sistema > Impostazioni > Information Centric Tagging**.
- 2 Per attivare le impostazioni, fare clic su **Modifica**.
- 3 Nel campo **Credenziali server**, selezionare le credenziali server ICT dal menu a discesa. Il nome di credenziale rappresenta il nome utente e la password di accesso per il server ICT.

Per aggiungere la credenziale al menu, accedere alla pagina **Credenziali** nella console di amministrazione e inserire la credenziale. Le credenziali devono essere un account utente di Windows con privilegi di accesso al database SQL ICT.

Vedere ["Aggiunta di nuove credenziali all'archivio credenziali"](#) a pagina 168.

- 4 Nel campo **URL servizio Web ICT**, digitare l'URL del servizio Web ICT o un nome percorso per il file XML.

Vedere ["Informazioni sulle importazioni automatiche e statiche della tassonomia di classificazione ICT"](#) a pagina 233.

Se si modifica l'URL del servizio Web ICT: Vedere ["Modifica dell'URL del servizio Web ICT"](#) a pagina 235.

Informazioni sulle importazioni automatiche e statiche della tassonomia di classificazione ICT

È possibile utilizzare il servizio Web ICT per le importazioni automatiche e pianificate della tassonomia di classificazione ICT. Se non è possibile utilizzare il servizio Web ICT - può darsi che il firewall in uso sia restrittivo o esista una politica in Enforce Server che non permette aggiornamenti del database da processi esterni - in alternativa è possibile importare una versione statica della tassonomia, basata su XML. Per questi metodi è possibile eseguire l'importazione immediatamente, anziché pianificarla.

Vedere ["Utilizzo del servizio Web ICT per importazioni di tassonomia di classificazione pianificata"](#) a pagina 234.

Vedere ["Utilizzo di un file XML per importazioni di tassonomia di classificazione statica"](#) a pagina 234.

Utilizzo del servizio Web ICT per importazioni di tassonomia di classificazione pianificata

Per utilizzare il servizio Web ICT per le importazioni di tassonomia di classificazione ICT

- ◆ Nella pagina **Information Centric Tagging**, nel campo **URL servizio Web ICT** digitare l'URL del servizio Web ICT.

La sintassi dell'URL è

`http://<server_ict>/ICT/Admin-Webservice/Classifications.asmx.`

Nota: L'utilizzo del servizio Web richiede la connettività di rete sulla porta 80 tra Enforce Server e il server Information Centric Tagging.

Utilizzo di un file XML per importazioni di tassonomia di classificazione statica

Per importare la tassonomia ICT utilizzando un file XML

- 1 Accedere al server ICT come utente Windows con privilegi di accesso al database SQL ICT.
- 2 Utilizzare il browser Internet Explorer sul server per cercare il servizio Web ICT. L'URL del servizio Web utilizza questa sintassi:
`http://<server_ict>/ICT/Admin-Webservice/Classifications.asmx`
- 3 Eseguire l'operazione `GetAllClassifications`.

Nella scheda **Classificazioni**, fare clic su **Richiama**.

- 4 Selezionare e copiare l'intero XML risultante dalla finestra del browser IE e salvarlo in un file di testo.
- 5 Rilasciare il file in un punto qualsiasi di Enforce Server.

Nota: Questo passaggio richiede l'autorizzazione di amministratore (scrittura) per Enforce Server.

- 6 Nella pagina **Information Centric Tagging**, nel campo **URL servizio Web ICT** immettere il nome del percorso XML anziché l'URL. Un esempio di nome percorso XML è:

`file://Programmi/Symantec/Data Loss Prevention Enforce /
Server/15.1/Protect/config/ICT.xml`

Importazione della tassonomia di classificazione ICT

È possibile stabilire una pianificazione di importazione giornaliera o eseguire un'importazione immediata.

Per impostare una pianificazione di sincronizzazione per l'importazione di tassonomia di classificazione ICT

- ◆ Nella pagina **Information Centric Tagging**, dai due menu a discesa del campo **Sincronizza ogni giorno alle** selezionare l'ora e minuti per l'importazione. La sincronizzazione del servizio Web ICT verrà eseguita ogni giorno.

Per eseguire un'importazione immediata della tassonomia di classificazione ICT

- ◆ Nella pagina **Information Centric Tagging**, per attivare un'importazione immediata fare clic su **Sincronizza ora**.

Dopo l'esecuzione di una sincronizzazione, la tassonomia importata viene visualizzata nella pagina **Information Centric Tagging** nelle colonne **Organizzazione**, **Ambito**, **Sensibilità** e **Livello**. Fare clic su qualsiasi colonna per ordinarla.

Si tenga presente che quando si risincronizza la tassonomia, qualsiasi tassonomia esistente viene eliminata e sostituita con quella nuova.

Tenere presente che in Information Centric Tagging, una volta creata una classificazione, questa non può essere eliminata. Le politiche di rilevamento di Data Loss Prevention esistenti continueranno a funzionare, anche se viene eseguita una nuova importazione. Tuttavia, l'amministratore ICT può apportare modifiche alle classificazioni. Di conseguenza, col passare del tempo è necessario riesaminare le politiche esistenti. Aggiornarle o eliminarle e ricrearle, se necessario, in modo da rispecchiare i tag società-ambito-livello. L'esame deve includere anche i nomi delle politiche, se sono indicativi dei tag in rilevamento.

Modifica dell'URL del servizio Web ICT

La necessità di modificare l'URL del servizio Web ICT è rara; tuttavia, se si modifica il nome del server di Information Centric Tagging, ad esempio, ed è necessario modificare l'URL, consultare [Tabella 11-2](#) per conoscere le azioni necessarie.

Tabella 11-2 Implicazioni della modifica dell'URL servizio Web ICT

Circostanza	Azione
Non è ancora stata sincronizzata un'importazione di classificazione ICT con questo URL.	Modificare l'URL senza eseguire altre azioni. Fare clic su Modifica per attivare il campo URL servizio Web ICT . Apportare la modifica e fare clic su Salva .

Circostanza	Azione
Un'importazione di classificazione ICT è stata sincronizzata con questo URL e il nuovo URL indica ancora la stessa tassonomia di prima.	Modificare l'URL senza eseguire altre azioni.
L'URL è stato utilizzato per sincronizzare un'importazione di classificazione ICT, ma il nuovo URL indica una tassonomia differente.	<p>Se sono già in uso regole di rilevamento:</p> <ol style="list-style-type: none"> 1 Eliminare tutti gli incidenti generati da tali regole. 2 Eliminare le regole di rilevamento che utilizzano l'opzione <i>Classificazione corrispondenze contenuto</i>. 3 Definire nuove regole utilizzando la tassonomia risultante dall'utilizzo del nuovo URL del servizio Web ICT.

Aggiunta di un nuovo modulo di prodotto

Il capitolo contiene i seguenti argomenti:

- [Installazione di un nuovo file di licenza](#)
- [Informazioni sugli aggiornamenti del sistema](#)

Installazione di un nuovo file di licenza

Quando si acquista Symantec Data Loss Prevention per la prima volta, si passa a una versione successiva, o si acquistano moduli supplementari del prodotto, è necessario installare uno o più file di licenza di Symantec Data Loss Prevention. I file di licenza hanno nomi nel formato `nome.slf`.

È anche possibile immettere un file di licenza per un solo modulo per iniziare e in seguito immettere i file di licenza per ulteriori moduli.

Per installare una licenza:

- 1 Scaricare il nuovo file di licenza.

Per informazioni sul download e l'estrazione del file di licenza, vedere il documento *Come ottenere il software Symantec Data Loss Prevention*, disponibile nel sito Symantec Software Downloads.

- 2 Accedere a **Sistema > Impostazioni > Generale** e fare clic su **Configura**.
- 3 Nella schermata **Modifica impostazioni generali**, scorrere fino alla sezione **Licenza**.

- 4 Nel campo **Installa licenza**, cercare il nuovo file di licenza di Symantec Data Loss Prevention scaricato, quindi fare clic su **Salva** per accettare i termini e le condizioni del contratto di licenza con l'utente finale (EULA) per il software e installare la licenza.

Nota: Se non si accettano i termini e le condizioni dell'EULA, non è possibile installare il software.

- 5 Per attivare completamente le funzionalità relative alla licenza del nuovo prodotto, riavviare il servizio Symantec DLP Manager.

Vedere ["Informazioni sui servizi Symantec Data Loss Prevention"](#) a pagina 101.

L'elenco **Licenza corrente** visualizza le seguenti informazioni per ogni licenza del prodotto:

- **Prodotto** - Il nome del singolo prodotto Symantec Data Loss Prevention
- **Conteggio** - Il numero di utenti che possono utilizzare il prodotto in base alla licenza
- **Stato** - Lo stato corrente del prodotto
- **Scadenza** - La data di scadenza della licenza per il prodotto

Un mese prima della **Scadenza** della licenza, appaiono messaggi di avviso sulla schermata di **Sistema > Server > Panoramica**. Quando si vede un messaggio sulla scadenza della licenza, contattare Symantec per acquistare una nuova chiave di licenza prima che la licenza corrente scada.

Informazioni sugli aggiornamenti del sistema

Il pulsante **Upgrade sistema** nella schermata **Panoramica** avvia il caricamento e l'upgrade del sistema a una versione più recente di Symantec Data Loss Prevention.

Per informazioni sull'aggiornamento del software Symantec Data Loss Prevention, consultare il *Manuale di upgrade di Symantec Data Loss Prevention*.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Gestione dei server di rilevamento

- [Capitolo 13. Installazione e gestione di server di rilevamento e rilevatori di cloud](#)
- [Capitolo 14. Gestione di file di registro](#)
- [Capitolo 15. Utilizzo delle utilità di Symantec Data Loss Prevention](#)

Installazione e gestione di server di rilevamento e rilevatori di cloud

Il capitolo contiene i seguenti argomenti:

- [Informazioni sulla gestione dei server Symantec Data Loss Prevention](#)
- [Attivazione del controllo dei processi avanzato](#)
- [Controlli server](#)
- [Configurazione di base di server](#)
- [Modifica di un rilevatore](#)
- [Configurazione server e rivelatore—avanzata](#)
- [Aggiunta di un server di rilevazione](#)
- [Aggiunta di un rilevatore di cloud](#)
- [Eliminazione di un server](#)
- [Importazione di certificati SSL in Enforce o Discover server](#)
- [Informazioni sulla schermata Panoramica](#)
- [Configurazione di Enforce Server per l'utilizzo di un proxy per connettersi ai servizi cloud](#)
- [Panoramica dello stato di server e rivelatori](#)
- [Elenco degli eventi di errore e avviso recenti](#)
- [Schermata Dettagli server/rilevatore](#)

- [Impostazioni server avanzate](#)
- [Impostazioni rilevatore avanzate](#)
- [Informazioni sull'utilizzo dei bilanciamenti del carico in una distribuzione endpoint](#)

Informazioni sulla gestione dei server Symantec Data Loss Prevention

I rilevatori di cloud e i server Symantec Data Loss Prevention sono gestiti dalla schermata **Sistema > Server e rilevatori > Panoramica**. Questa schermata fornisce una panoramica del sistema, compreso lo stato del server e gli eventi di sistema recenti. Visualizza informazioni di riepilogo su tutti i server Symantec Data Loss Prevention, un elenco di eventi di avviso ed errori recenti e informazioni sulla licenza. In questa schermata è possibile aggiungere o rimuovere i server di rilevamento.

- Fare clic sul nome di un server per visualizzarne la schermata **Dettagli server/rilevatore**, dalla quale è possibile controllare e configurare il server.

Vedere ["Installazione di un nuovo file di licenza"](#) a pagina 237.

Vedere ["Informazioni sulla console di amministrazione di Enforce Server"](#) a pagina 81.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Vedere ["Aggiunta di un server di rilevazione"](#) a pagina 268.

Vedere ["Aggiunta di un rilevatore di cloud"](#) a pagina 270.

Vedere ["Eliminazione di un server"](#) a pagina 271.

Vedere ["Controlli server"](#) a pagina 242.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Attivazione del controllo dei processi avanzato

Controllo dei processi avanzato di Symantec Data Loss Prevention consente di avviare o interrompere i singoli processi server dalla console di amministrazione Enforce Server. Non è necessario avviare o interrompere un intero server. Questa funzionalità può essere utile per il debug. Quando Controllo dei processi avanzato è disattivato (per impostazione predefinita), ogni schermata **Dettagli server/rilevatore** mostra solo lo stato dell'intero server. Quando si attiva Controllo dei processi avanzato, la sezione **Generale** della schermata **Dettagli server/rilevatore** mostra singoli processi.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Per consentire il Controllo dei processi avanzato

- 1 Accedere a **Sistema > Impostazioni > Generale** e fare clic su **Configura**.
Viene visualizzata la schermata **Modifica impostazioni generali**.
- 2 Scorrere verso il basso fino alla sezione **Controllo dei processi** e selezionare la casella **Controllo dei processi avanzato**.
- 3 Fare clic su **Salva**.

[Tabella 13-1](#) descrive i singoli processi e i server su cui sono in esecuzione una volta attivato il controllo dei processi.

Tabella 13-1 Processi avanzati

Processo	Descrizione	Controllo
Controller di monitoraggio	Il controller di monitoraggio controlla il server di rilevazione.	Lo Stato MonitorController è disponibile per Enforce Server.
Lettore file	Il processo del lettore file rileva gli incidenti.	Lo Stato FileReader è disponibile per tutti i server di rilevazione.
Writer incidenti	Il processo writer incidenti invia incidenti a Enforce Server.	Lo Stato IncidentWriter è disponibile per tutti i server di rilevazione, a meno che non siano parte di un'installazione a un solo livello, nel qual caso è disponibile solo un processo writer incidenti.
Acquisizione del pacchetto	Il processo Acquisizione del pacchetto acquisisce flussi di rete.	Lo Stato PacketCapture è disponibile per Network Monitor.
Processore richiesta	Il processore richiesta elabora le richieste SMTP.	Lo Stato RequestProcessor è disponibile per Network Prevent for Email.
Endpoint Server	Il processo Endpoint Server interagisce con Symantec DLP Agent.	Lo Stato EndpointServer è disponibile per Endpoint Prevent.
Database server di rilevazione	Il processo del database del server di rilevazione è utilizzato per il rilevamento di riparazione degli incidenti automatici.	Lo Stato DetectionServerDatabase è disponibile per Network Discover.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Controlli server

I server e i loro processi sono controllati dalla schermata **Dettagli server/rilevatore**.







- Per raggiungere la schermata **Dettagli server/rilevatore** per un server particolare, accedere alla schermata **Sistema > Server e rilevatori > Panoramica** e fare clic sul nome del server, del rilevatore o del dispositivo nell'elenco.

Vedere "**Schermata Dettagli server/rilevatore**" a pagina 277.

Lo stato del server e dei suoi processi compare nella sezione **Generale** della schermata **Dettagli server/rilevatore**. I pulsanti **Avvia**, **Ricicla** e **Arresta** controllano le operazioni del server e dei processi.

Lo stato corrente del server compare nella sezione **Generale** della schermata **Dettagli server/rilevatore**. I valori possibili sono:

Tabella 13-2 Valori di stato del server

Icona	Stato
	Avvio in corso - In fase di avvio.
	In esecuzione - In esecuzione senza errori.
	Selezionato in esecuzione - Alcuni processi sul server sono interrotti o hanno errori. Per visualizzare gli stati di singoli processi, è necessario dapprima attivare l'opzione Controllo dei processi avanzato nella schermata Impostazioni di sistema .
	Arresto in corso - In fase di arresto.
	Arrestato - Completamente fermo.
	Sconosciuto - Nel server si è verificato uno dei seguenti errori:

- **Avvia**. Per avviare un server o un processo, fare clic su **Avvia**.
- **Ricicla**. Per arrestare e riavviare un server, fare clic su **Ricicla**.
- **Arresta**. Per arrestare un server o un processo, fare clic su **Arresta**.
- Per interrompere un processo durante la procedura di avvio, fare clic su **Termina**.
- Per riavviare un dispositivo, fare clic su **Riavvia**.

Nota: Lo stato e i controlli per i singoli processi del server sono visualizzati solo se il Controllo dei processi avanzato è attivato per Enforce Server. Per attivare il Controllo dei processi avanzato, accedere a **Sistema > Impostazioni > Generale > Configura**, selezionare la casella **Controllo dei processi avanzato** e fare clic su **Salva**.

- Per aggiornare lo stato, fare clic sull'icona **Aggiorna** nella parte in alto a destra della schermata, come necessario.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Vedere ["Report di eventi di sistema"](#) a pagina 172.

Vedere ["Dettagli eventi di server e rivelatori"](#) a pagina 176.

Configurazione di base di server

La configurazione di Enforce Server viene eseguita mediante il menu **Sistema > Impostazioni > Generale**.

I server di rilevazione sono configurati nella schermata **Configura server** di ogni server.

Per configurare un server

- 1 Accedere alla schermata **Sistema > Server e rilevatori > Panoramica**.
- 2 Fare clic sul nome del server nell'elenco.

Viene visualizzata la schermata **Dettagli server/rilevatore** di quel server. Nella parte superiore sinistra di una schermata **Dettagli server/rilevatore** sono disponibili i seguenti pulsanti:

- **Fine**. Fare clic su **Fine** per ritornare alla schermata precedente.
- **Configura**. Fare clic su **Configura** per specificare una configurazione di base per questo server.
- **Impostazioni server**. Fare clic su **Impostazioni server** per specificare parametri di configurazione avanzata per questo server. Prestare attenzione quando si modificano le impostazioni avanzate del server. Si consiglia di consultare il supporto Symantec prima di modificare qualsiasi impostazione avanzata.

Vedere ["Configurazione server e rivelatore—avanzata"](#) a pagina 267.

Per informazioni sulla configurazione avanzata di server, vedere la guida in linea di Symantec Data Loss Prevention.

- 3 Fare clic su **Configura** o **Impostazioni server** per visualizzare uno schermata di configurazione per quel tipo di server.
- 4 Specificare o cambiare le impostazioni sulla schermata come necessario, quindi fare clic su **Salva**.

Fare clic su **Annulla** per ritornare alla schermata precedente senza cambiare alcuna impostazione.

Nota: Un server deve essere riciclato prima che le nuove impostazioni diventino effettive.

Vedere ["Controlli server"](#) a pagina 242.

La schermata **Configura server** include una sezione **Generale** per tutti i server di rilevazione che contiene i seguenti parametri:

- **Nome.** Il nome che si assegna al server. Questo nome appare nella console di amministrazione di Enforce Server (**Sistema > Server e rilevatori > Panoramica**). Il nome non deve includere più di 255 caratteri.
- **Host.** Il nome host o l'indirizzo IP del sistema che ospita il server. I nomi host devono essere completi. Se l'host ha più di un indirizzo IP, specificare l'indirizzo in cui il server di rilevazione ascolta le connessioni a Enforce Server.
- **Porta.** Il numero di porta usato dal server di rilevazione per comunicare con Enforce Server. La porta predefinita è 8100.

Per i monitor a un solo livello, il campo **Host** nella pagina **Configura server** presenta l'indirizzo IP locale 127.0.0.1. Non è possibile modificare questo valore.

Le altre parti della schermata **Configura server** variano a seconda del tipo di server.

Vedere ["Server Network Monitor - Configurazione di base"](#) a pagina 246.

Vedere ["Server Network Discover/Cloud Storage Discover e Network Protect - Configurazione di base"](#) a pagina 254.

Vedere ["Server Network Prevent for Email - Configurazione di base"](#) a pagina 248.

Vedere ["Server Network Prevent for Web - Configurazione di base"](#) a pagina 251.

Vedere ["Endpoint Server - Configurazione di base"](#) a pagina 255.

Vedere ["Monitoraggio a un solo livello - configurazione di base"](#) a pagina 256.

Vedere ["Server di classificazione - Configurazione base"](#) a pagina 266.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Server Network Monitor - Configurazione di base

I server di rilevamento sono configurati nella schermata **Configura server** di ogni server. Per visualizzare la schermata **Configura server**, accedere alla schermata **Panoramica (Sistema > Server e rilevatori > Panoramica)** e fare clic sul nome del server nell'elenco. Viene visualizzata la schermata **Dettagli server/rilevatore** di quel server. Fare clic su **Configura** per visualizzare la schermata **Configura server**.

La schermata **Configura server** di un server Network Monitor contiene una sezione generale e due schede:

- Sezione **Generale**. Utilizzare questa sezione per specificare nome, host e porta del server. Vedere ["Configurazione di base di server"](#) a pagina 244.
- Scheda **Acquisizione del pacchetto**. Utilizzare questa scheda per configurare le impostazioni di acquisizione dei pacchetti di rete.
- Scheda **Copia regola SMTP**. Utilizzare questa scheda per modificare la cartella di origine da cui il server recupera i file dei messaggi SMTP.

La parte superiore di **Acquisizione del pacchetto** definisce i parametri generali di acquisizione del pacchetto. Fornisce i seguenti campi:

Campo	Descrizione
Sovrascrittura cartella di origine	La cartella di origine è la directory utilizzata dal server per il buffering dei flussi di rete prima che li elabori. L'impostazione raccomandata è di lasciare vuoto il campo Sovrascrittura cartella di origine per accettare l'impostazione predefinita. Per specificare una directory di buffer personalizzata, digitare il percorso completo della directory.
Interfacce di rete	<p>Selezionare le schede di interfaccia di rete da utilizzare per il monitoraggio. Per il monitoraggio è necessario aver installato un software NIC WinPcap sul server di Network Monitor.</p> <p>Vedere il <i>Manuale di installazione di Symantec Data Loss Prevention</i> per ulteriori informazioni sui NIC.</p>

La sezione **Protocollo di Acquisizione del pacchetto** specifica i tipi di traffico di rete (per protocollo) da acquisire. Inoltre specifica gli eventuali parametri personalizzati da applicare. Questa sezione elenca i protocolli standard concessi in licenza da Symantec e gli eventuali protocolli TCP personalizzati aggiunti.

Per monitorare un protocollo particolare, selezionare la casella corrispondente. Quando si configura un server per la prima volta, le impostazioni per ciascuno dei protocolli selezionati sono ereditate dalle impostazioni dei protocolli a livello di sistema. Configurare queste

impostazioni accedendo a **Sistema > Impostazioni > Protocollo**. Le impostazioni predefinite a livello di sistema sono elencate come **Standard**.

Per informazioni sull'utilizzo di impostazioni a livello di sistema, vedere la guida in linea di Symantec Data Loss Prevention.

Per sovrascrivere le impostazioni di filtro ereditate per un protocollo, fare clic sul nome del protocollo. Le seguenti impostazioni personalizzate sono disponibili (alcune impostazioni potrebbero non essere disponibili per alcuni protocolli):

- Filtro IP
- Filtro mittente L7
- Filtro destinatario L7
- Filtro contenuti
- Profondità di ricerca (pacchetti)
- Frequenza di campionamento
- Attesa massima prima della scrittura
- Attesa massima prima del rilascio
- Numero massimo di pacchetti flusso
- Dimensione minima flusso
- Dimensione massima flusso
- Intervallo segmento
- Timeout di notifica di assenza traffico (il valore massimo per questa impostazione è 360.000 secondi)

Utilizzare **Copia regola SMTP** per modificare la cartella di origine da cui questo server recupera i file dei messaggi SMTP. È possibile modificare la cartella di origine immettendo il percorso completo a una cartella.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Vedere ["Controlli server"](#) a pagina 242.

Oltre alle impostazioni disponibili nella schermata **Configura server**, è possibile specificare le impostazioni avanzate per questo server. Per specificare parametri di configurazione avanzati, fare clic su **Impostazioni server** nella schermata **Dettagli server/rilevatore** del server.

Prestare attenzione quando si modificano le impostazioni avanzate del server. Contattare il supporto Symantec prima di modificare qualsiasi impostazione avanzata.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Consultare la guida in linea di Symantec Data Loss Prevention per informazioni sulle impostazioni avanzate.

Server Network Prevent for Email - Configurazione di base

I server di rilevamento sono configurati nella schermata **Configura server** di ogni server. Per visualizzare la schermata **Configura server**, accedere alla schermata **Panoramica (Sistema > Server e rilevatori > Panoramica)** e fare clic sul nome del server nell'elenco. Viene visualizzata la schermata **Dettagli server/rilevatore** di quel server. Fare clic su **Configura** per visualizzare la schermata **Configura server**.

La schermata **Configura server** di un server Network Prevent for Email include una sezione **Generale** e una scheda **SMTP inline**. La sezione **Generale** consente di specificare il nome, l'host e la porta del server.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Utilizzare la scheda **SMTP inline** per configurare differenti funzionalità del server &pn.NetworkPreventEmail:

Campo	Descrizione
Modalità di prova	La modalità di prova consente di verificare le funzionalità di prevenzione senza bloccare le richieste. Quando la modalità di prova è selezionata, il server rileva gli incidenti e crea report incidenti, ma non blocca alcun messaggio. Deselezionare questa opzione per bloccare i messaggi che violano le politiche di Symantec Data Loss Prevention.
Password archivio chiavi	Se si utilizza l'autenticazione TLS in una configurazione modalità di inoltro, digitare la password corretta per il file di archivio chiavi.
Configurazione hop successivo	<p>Selezionare Rifletti per eseguire il server Network Prevent for Email in modalità di riflessione.</p> <p>Selezionare Inoltro per attivare la modalità di inoltro.</p> <p>Nota: Se si seleziona Inoltro è necessario anche selezionare Abilita ricerca MX o Disabilita ricerca MX per configurare il metodo usato per determinare l'agente MTA dell'hop successivo.</p>

Campo

Abilita ricerca MX

Descrizione

Questa opzione si applica solo alle configurazioni della modalità di inoltra.

Selezionare **Abilita ricerca MX** per eseguire una query DNS su un nome di dominio e ottenere i record di scambio di posta (MX) per il server. Il server Network Prevent for Email utilizza i record MX restituiti per selezionare l'indirizzo del server di posta dell'hop successivo.

Se si seleziona **Abilita ricerca MX**, aggiungere anche uno o più nomi di dominio nella casella di testo **Immetti domini**. Ad esempio:

`companyname.com`

Il server Network Prevent for Email esegue query di record MX per i nomi di dominio specificati.

Nota: È necessario includere almeno una voce valida nella casella di testo **Immetti domini** per configurare correttamente il comportamento delle modalità di inoltra.

Campo	Descrizione
Disabilita ricerca MX	<p>Questo campo riguarda solo le configurazioni della modalità di inoltro.</p> <p>Selezionare Disabilita ricerca MX se si desidera specificare il nome host o l'indirizzo IP esatto di uno o più MTA dell'hop successivo. Il server Network Prevent for Email utilizza i nomi host o gli indirizzi specificati e non esegue una ricerca di record MX.</p> <p>Se si seleziona Disabilita ricerca MX, aggiungere anche uno o più nomi di host o indirizzi IP per gli MTA degli hop successivi nella casella di testo Immetti nomi host. È possibile specificare più voci posizionando ognuna di esse su una linea separata. Ad esempio:</p> <pre>smtp1.companyname.com smtp2.companyname.com smtp3.companyname.com</pre> <p>Il server Network Prevent for Email prova sempre a utilizzare il primo MTA specificato nell'elenco. Se tale MTA non è disponibile, il server Network Prevent for Email prova la successiva voce disponibile nell'elenco.</p> <p>Nota: È necessario includere almeno una voce valida nella casella di testo Immetti nome host per configurare correttamente il comportamento delle modalità di inoltro.</p>

Per ulteriori informazioni sulla configurazione di opzioni del server Network Prevent for Email, consultare la *Guida all'integrazione MTA di Symantec Data Loss Prevention per Network Prevent for Email*.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Vedere ["Controlli server"](#) a pagina 242.

Oltre alle impostazioni disponibili nella schermata **Configura server**, è possibile specificare le impostazioni avanzate per questo server. Per specificare parametri di configurazione avanzati, fare clic su **Impostazioni server** nella schermata **Dettagli server/rilevatore** del server.

Prestare attenzione quando si modificano le impostazioni avanzate del server. Contattare il supporto Symantec prima di modificare qualsiasi impostazione avanzata.

Vedere "**Impostazioni server avanzate**" a pagina 279.

Consultare la guida in linea di Symantec Data Loss Prevention per informazioni sulle impostazioni avanzate.

Server Network Prevent for Web - Configurazione di base

I server di rilevazione sono configurati nella schermata **Configura server** di ogni server. Per visualizzare la schermata **Configura server**, accedere alla schermata **Panoramica (Sistema > Server e rilevatori > Panoramica)** e fare clic sul nome del server nell'elenco. Viene visualizzata la schermata **Dettagli server/rilevatore** di quel server. Fare clic su **Configura** per visualizzare la schermata **Configura server**.

La schermata **Configura Server** del server Network Prevent for Web è divisa in una sezione generale, una sezione Amministrazione Symantec Encryption Server e due schede:

- Sezione **Generale**. Questa sezione consente di specificare nome, host e porta del server.
- Sezione **Amministrazione Symantec Encryption Server**. Questa sezione specifica il **Nome Symantec Encryption Server**, la **Porta protocollo servizio universale** e la **Credenziale**.
- Scheda **ICAP**. Questa scheda permette di configurare l'Internet Content Adaptation Protocol (ICAP). Usare la scheda ICAP per configurare traffico di rete basato su web.

La scheda **ICAP** è divisa in quattro sezioni:

- La sezione **Modalità di prova** consente di verificare la politica di prevenzione senza bloccare il traffico. Quando è selezionata la modalità di prova, il server rileva gli incidenti e crea report incidente, ma non blocca alcun traffico. Questa opzione consente di testare le politiche senza bloccare il traffico. Selezionare la casella per attivare la modalità di prova.
- Fare clic sulla casella nella sezione **Configurazione sicurezza** per attivare l'ICAP protetto con il server Blue Coat ProxySG. È inoltre necessario disporre di un archivio chiavi configurato e fornire la password dell'archivio chiavi quando si attiva l'ICAP protetto. Per istruzioni sull'impostazione della configurazione del client ICAP protetto con Blue Coat ProxySG, consultare la documentazione di Blue Coat ProxySG in www.symantec.com/docs/DOC10187.html.
- La sezione **Filtraggio richieste** configura i criteri di filtraggio del traffico:

Campo	Descrizione
Ignora richieste inferiori a	Consente di specificare la dimensione di corpo minima delle richieste HTTP per l'ispezione su questo server. Il valore predefinito è 4096 byte. Le richieste HTTP con corpi più piccoli di questo numero non sono ispezionate.
Ignora richieste da host o domini	Immettere i nomi host o i domini le cui richieste devono essere escluse tramite i filtri (ignore). Immettere un nome host o dominio per riga.
Ignora richieste da agenti utente	Immettere i nomi degli agenti utente le cui richieste devono essere escluse tramite i filtri (ignore). Immettere un agente per riga.

- La sezione **Filtro risposte** configura i criteri di filtraggio per la gestione delle risposte HTTP:

Campo	Descrizione
Ignora risposte inferiori a	Immettere la dimensione di corpo minima delle richieste HTTP per l'ispezione su questo server. Il valore predefinito è 4096 byte. Le risposte HTTP con i corpi più piccoli di questo numero non vengono ispezionate.
Ispeziona tipo di contenuto	Specificare i tipi di contenuto MIME che il server deve monitorare. Per impostazione predefinita, questo campo contiene valori di tipo contenuto per i formati Microsoft Office, PDF e testo semplice standard. È possibile aggiungere altri valori del tipo di contenuto MIME. Immettere tipi di contenuti separati su righe separate. Ad esempio, per ispezionare file Excel immettere application/vnd.ms-excel .
Ignora risposte da host o domini	Immettere i nomi di host o i domini di cui devono essere ignorate le risposte. Immettere un nome host o dominio per riga.

Campo	Descrizione
Ignora risposte da agenti utente	Immettere i nomi di agenti utente di cui devono essere ignorate le risposte. Immettere un agente utente per riga.
<ul style="list-style-type: none"> Fare clic sulla scheda Motore OCR per aggiungere un profilo Configurazione motore OCR. Scorrere verso il basso per selezionare una configurazione. Vedere "Informazioni sul rilevamento dei contenuti con il riconoscimento OCR delle immagini riservate" a pagina 673. Vedere "Creazione di una configurazione OCR" a pagina 676. La sezione Connessione configura le impostazioni per la connessione ICAP tra un server proxy HTTP e il server Network Prevent for Web: 	

Campo	Descrizione
Porta TCP	Specificare il numero di porta TCP che questo server deve utilizzare per ascoltare le richieste ICAP. Lo stesso valore deve essere configurato sul proxy HTTP che invia le richieste ICAP a questo server. Il valore consigliato è 1344.
Numero massimo di richieste	Immettere il numero massimo di connessioni di richieste ICAP simultanee. Il valore predefinito è 25.
Numero massimo di risposte	Immettere il numero massimo di connessioni di risposte ICAP simultanee dal proxy HTTP o dai proxy consentiti. Il valore predefinito è 25.
Backlog connessione	Immettere il numero massimo di connessioni in attesa consentite. Per ogni connessione in attesa un utente è in attesa davanti al browser. Il valore minimo è 1.

Vedere ["Configurazione del server Network Prevent for Web"](#) a pagina 1807.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Vedere ["Controlli server"](#) a pagina 242.

Oltre alle impostazioni disponibili nella schermata **Configura server**, è possibile specificare le impostazioni avanzate per questo server. Per specificare parametri di configurazione avanzati, fare clic su **Impostazioni server** nella schermata del server **Dettagli server/rilevatore**.

Prestare attenzione quando si modificano le impostazioni avanzate del server. Contattare il supporto Symantec prima di modificare qualsiasi impostazione avanzata.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Consultare la guida in linea di Symantec Data Loss Prevention per informazioni sulle impostazioni avanzate del server.

Server Network Discover/Cloud Storage Discover e Network Protect - Configurazione di base

I server di rilevazione sono configurati nella schermata **Configura server** di ogni server. Per visualizzare la schermata **Configura** per un server, accedere alla schermata **Sistema > Server e rilevatori > Panoramica** e fare clic sul nome del server nell'elenco. Viene visualizzata la schermata **Dettagli server/rilevatore** di quel server. Fare clic su **Configura**. Viene visualizzata la schermata **Configura server** del server.

Vedere ["Modifica della configurazione del server Network Discover/Cloud Storage Discover"](#) a pagina 1824.

La schermata **Configura server** di un server Network Discover contiene una sezione generale e una scheda:

- Sezione **Generale**. Questa sezione consente di specificare nome, host e porta del server. Vedere ["Configurazione di base di server"](#) a pagina 244.

- Scheda **Discover**. Questa scheda consente di modificare il numero di scansioni parallele eseguite su questo Discover Server.

Il numero massimo può essere aumentato in qualunque momento. Dopo l'aumento, tutte le scansioni in coda eseguibili nel server Network Discover vengono avviate. Il numero può essere diminuito solo se nel server Network Discover non sono in esecuzione scansioni. Prima di ridurre il numero, sospendere o arrestare tutte le scansioni in esecuzione sul server.

Per visualizzare le scansioni in esecuzione sui server Network Discover, accedere a **Gestisci > Scansione Discover > Target di Discover**.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Vedere ["Controlli server"](#) a pagina 242.

Oltre alle impostazioni disponibili nella schermata **Configura server**, è anche possibile specificare impostazioni avanzate per questo server. Per specificare parametri di configurazione avanzati, fare clic su **Impostazioni server** nella schermata **Dettagli server/rilevatore**. Prestare attenzione quando si modificano le impostazioni avanzate del server. Si consiglia di consultare il supporto Symantec prima di modificare qualsiasi impostazione avanzata.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Endpoint Server - Configurazione di base

I server di rilevazione sono configurati nella schermata **Configura server** di ogni server. Per visualizzare la schermata **Configura** per un server, accedere alla schermata **Sistema > Server e rilevatori > Panoramica** e fare clic sul nome del server. Viene visualizzata la schermata **Dettagli server/rilevatore** per quel server. Fare clic su **Configura** per visualizzare la schermata **Configura server** per quel server.

Vedere ["Aggiunta di un server di rilevazione"](#) a pagina 268.

La schermata **Configura server** per un Endpoint Server include una sezione generale e le schede seguenti:

- **Generale.** In questa sezione è possibile specificare nome del server, host e porta.
Vedere ["Configurazione di base di server"](#) a pagina 244.
- **Agente.** Questa sezione consente di aggiungere certificati di sicurezza a Endpoint Server.
Vedere ["Aggiunta e modifica di configurazioni agente"](#) a pagina 2111.

Listener di agente. Usare questa sezione per configurare Endpoint Server per l'ascolto delle connessioni da Symantec DLP Agent:

Campo	Descrizione
Indirizzo di binding	Immettere l'indirizzo IP su cui Endpoint Server ascolta le comunicazioni da Symantec DLP Agent. L'indirizzo IP predefinito è 0.0.0.0 e consente a Endpoint Server di ascoltare su tutti gli indirizzi IP host.
Porta	Immettere la porta sulla quale Endpoint Server ascolta le comunicazioni da Symantec DLP Agent. Nota: Molti sistemi Linux limitano le porte inferiori a 1024 all'accesso root. Endpoint Server non può essere configurato per ascoltare le connessioni da Symantec DLP Agent a queste porte su sistemi Linux.

Nota: Se si utilizza la modalità FIPS 140-2 per la comunicazione tra Endpoint Server e i DLP Agent, non utilizzare la suite per crittografia Diffie-Hellman (DH). Le suite per crittografia combinate impediscono all'agente e a Endpoint Server di comunicare. È possibile confermare la suite per crittografia corrente con l'impostazione **EndpointCommunications.SSLCipherSuites** nella pagina **Impostazioni server**. Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Monitoraggio a un solo livello - configurazione di base

I server di rilevazione sono configurati nella schermata **Configura server** di ogni server. Per visualizzare la schermata **Configura server**, accedere alla schermata **Sistema > Server e rilevatori > Panoramica** e fare clic sul nome del server nell'elenco. Viene visualizzata la schermata **Dettagli server/rilevatore** di quel server. Fare clic su **Configura** per visualizzare la schermata **Configura server**.

Il **Monitoraggio a un solo livello** è un server di rilevamento che comprende le funzionalità di rilevamento dei server di rilevamento Network Monitor, Network Discover/Cloud Storage Discover, Network Prevent for Web, Network Prevent for Email, Endpoint Prevent e Endpoint Discover. Ciascuno di questi tipi di server di rilevamento è associato a uno o più "canali" di rilevamento. La distribuzione di singoli server semplifica l'amministrazione di Symantec Data Loss Prevention e riduce i costi di manutenzione e hardware per le organizzazioni di piccole dimensioni o per le filiali di imprese più grandi che trarrebbero vantaggio dalle distribuzioni in loco di Symantec Data Loss Prevention.

Configurazione dei canali per Network Monitor

Network Monitor utilizza due canali: **Acquisizione del pacchetto** e **Copia regola SMTP**. Per configurare Network Monitor, immettere le informazioni di configurazione in entrambe le schede **Acquisizione del pacchetto** e **Copia regola SMTP** nella schermata **Configura server**.

Per configurare le schede **Acquisizione del pacchetto** e **Copia regola SMTP**

- 1 Facoltativo: nella scheda **Acquisizione del pacchetto** della schermata **Configura server**, specificare la **Sovrascrittura cartella di origine**.

La cartella di origine è la directory utilizzata dal server per il buffering dei flussi di rete prima che li elabori. L'impostazione raccomandata è di lasciare vuoto il campo **Sovrascrittura cartella di origine** per accettare l'impostazione predefinita. Per specificare una directory di buffer personalizzata, digitare il percorso completo della directory.

- 2 Selezionare le **Interfacce di rete**.

Selezionare le schede di interfaccia di rete da utilizzare per il monitoraggio.

Vedere il *Manuale di installazione di Symantec Data Loss Prevention* per ulteriori informazioni sui NIC.

- 3 Nella sezione **Protocollo**, selezionare la casella di ciascun tipo di traffico di rete da acquisire.

Quando si configura un server per la prima volta, le impostazioni per ciascuno dei protocolli selezionati sono ereditate dalle impostazioni dei protocolli a livello di sistema. Configurare queste impostazioni accedendo a **Sistema > Impostazioni > Protocollo**. Le impostazioni predefinite a livello di sistema sono elencate come **Standard**. Per sovrascrivere le impostazioni di filtro ereditate per un protocollo, fare clic sul nome del protocollo. Le seguenti impostazioni personalizzate sono disponibili (alcune impostazioni potrebbero non essere disponibili per alcuni protocolli):

- Filtro IP
- Filtro mittente L7
- Filtro destinatario L7
- Filtro contenuti
- Profondità di ricerca (pacchetti)
- Frequenza di campionamento
- Attesa massima prima della scrittura
- Attesa massima prima del rilascio
- Numero massimo di pacchetti flusso
- Dimensione minima flusso
- Dimensione massima flusso
- Intervallo segmento
- Timeout di notifica di assenza traffico (il valore massimo per questa impostazione è 360.000 secondi)

- 4 Facoltativo: nella scheda **Copia regola SMTP**, specificare la **Sovrascrittura cartella di origine** per modificare la cartella di origine da cui questo server recupera i file dei messaggi SMTP.

È possibile modificare la cartella di origine immettendo il percorso completo a una cartella. Lasciare vuoto questo campo per usare la cartella di origine predefinita.

Configurazione del canale per Network Discover/Cloud Storage Discover

Network Discover/Cloud Storage Discover utilizza il canale **Discover**. Nella scheda **Discover**, è possibile modificare il numero di scansioni parallele eseguite nel Monitoraggio a un solo livello inserendo un numero nel campo **Numero massimo di scansioni parallele**.

Nota: Se si prevede di utilizzare la funzionalità di scansione della griglia per distribuire il carico di lavoro di scansione tra più server di rilevamento, mantenere il valore predefinito (1).

Il numero massimo può essere aumentato in qualunque momento. Dopo l'aumento, tutte le scansioni in coda eseguibili nel server Network Discover vengono avviate. Il numero può essere diminuito solo se nel server Network Discover non sono in esecuzione scansioni. Prima di ridurre il numero, sospendere o arrestare tutte le scansioni in esecuzione sul server.

Configurazione del canale per Network Prevent for Web

Network Prevent for Web utilizza il canale **ICAP**. La scheda di configurazione del canale ICAP è divisa in quattro sezioni: **Filtraggio richieste**, **Filtraggio risposte** e **Connessione**.

Per configurare la scheda ICAP

- 1 Verificare o modificare l'impostazione **Modalità di prova**. **Modalità di prova** consente di verificare la prevenzione senza bloccare le richieste in tempo reale. Se si seleziona **Modalità di prova**, Symantec Data Loss Prevention rileva gli incidenti e indica che ha bloccato una comunicazione HTTP, ma non blocca la comunicazione.
- 2 Verificare o modificare le opzioni di filtraggio per le richieste dei client HTTP (agenti utente). Le opzioni della sezione **Filtraggio richieste** sono le seguenti:

Ignora richieste inferiori a

Specifica la dimensione minima del corpo delle richieste HTTP per l'ispezione. (l'impostazione predefinita è 4096 byte). Ad esempio, le stringhe di ricerca digitate in motori di ricerca quali Yahoo o Google sono in genere brevi. È possibile regolare questo valore per escludere tali ricerche dall'ispezione.

Ignora richieste senza allegati

Fa sì che il server ispezioni solo le richieste che contengono allegati. Questa opzione può essere utile se l'interesse maggiore riguarda richieste associate alla pubblicazione di file riservati.

Ignora richieste a host o domini

Fa sì che il server ignori le richieste inviate agli host o ai domini specificati. Questa opzione può essere utile se si prevede molto traffico HTTP tra i domini della sede aziendale e delle filiali. È possibile digitare uno o più nomi host o di dominio (ad esempio www.azienda.com), ciascuno su una riga distinta.

Ignora richieste da agenti utente

Fa sì che il server ignori le richieste provenienti dagli agenti utente (client HTTP) specificati. Questa opzione può essere utile se l'organizzazione usa un programma o una lingua (quale Java) che fa frequenti richieste HTTP. È possibile digitare uno o più valori dell'agente utente, ciascuno su una riga distinta.

- 3 Verificare o modificare le opzioni di filtro per le risposte dei server Web. Le opzioni della sezione **Filtraggio risposte** sono le seguenti:

Ignora risposte inferiori a

Specifica la dimensione minima del corpo delle risposte HTTP ispezionate da questo server (l'impostazione predefinita è 4096 byte).

Ispeziona tipo di contenuto

Specifica i tipi di contenuti MIME che Symantec Data Loss Prevention deve controllare nelle risposte. Per impostazione predefinita, questo campo contiene valori di tipo contenuto per i formati Microsoft Office, PDF e testo semplice. Per aggiungerne altri, digitare un tipo di contenuto MIME per riga. Ad esempio digitare `application/word2013` affinché Symantec Data Loss Prevention analizzi i file Microsoft Word 2013.

Si tenga presente che in genere è più efficiente specificare i tipi di contenuto MIME a livello del proxy Web.

Ignora risposte da host o domini

Fa sì che il server ignori le risposte provenienti dagli host o dai domini specificati. È possibile digitare uno o più nomi host o di dominio (ad esempio `www.azienda.com`), ciascuno su una riga distinta.

Ignora risposte da agenti utente

Fa sì che il server ignori le risposte inviate agli agenti utente (client HTTP) specificati. È possibile digitare uno o più valori dell'agente utente, ciascuno su una riga distinta.

- 4 Verificare o modificare le impostazioni per la connessione ICAP tra il server proxy HTTP e il server Web Prevent. Le opzioni della sezione **Connessione** sono le seguenti:

Porta TCP	Specifica il numero della porta TCP sulla quale il server riceve le richieste ICAP. Questo numero deve corrispondere al valore configurato sul proxy HTTP che invia le richieste ICAP a questo server. Il valore consigliato è 1344.
Numero massimo di richieste	Specifica il numero massimo di connessioni di richiesta ICAP simultanee dal proxy HTTP. Il valore predefinito è 25.
Numero massimo di risposte	Specifica il numero massimo di connessioni di risposta ICAP simultanee dal/dai proxy HTTP. Il valore predefinito è 25.
Backlog connessione	Specifica il numero di connessioni in attesa consentite. Una connessione in attesa è un utente che attende una risposta HTTP dal browser. Il valore minimo è 1. Se il proxy HTTP riceve un numero eccessivo di richieste (o risposte), le gestisce in base alla configurazione del proxy. È possibile configurare il proxy HTTP in modo da bloccare tutte le richieste (o tutte le risposte) che superano il numero limite.

Configurazione del canale per Network Prevent for Email

Network Prevent for Email utilizza il canale **SMTP inline**. La scheda di configurazione SMTP inline è divisa in tre sezioni: **Numero massimo di connessioni**, **Configurazione sicurezza** e **Configurazione hop successivo**.

Per configurare la scheda SMTP inline

- 1 Verificare o modificare l'impostazione **Modalità di prova**. **Modalità di prova** consente di verificare la prevenzione senza bloccare le richieste in tempo reale. Se si seleziona **Modalità di prova**, Symantec Data Loss Prevention rileva gli incidenti e indica che ha bloccato una comunicazione HTTP, ma non blocca la comunicazione.
- 2 Verificare o modificare il **Numero massimo di connessioni**. Per impostazione predefinita, il numero massimo di connessioni è 12.

- 3 Se si utilizza l'autenticazione TLS in una configurazione modalità di inoltro, digitare la password corretta per il file di archivio chiavi nel campo **Password archivio chiavi** della sezione **Configurazione sicurezza**.

- 4 Nella sezione Configurazione hop successivo, configurare la modalità di riflessione o di inoltra modificando i seguenti campi:

Campo	Descrizione
Configurazione hop successivo	<p>Selezionare Rifletti per operare il server Network Prevent for Email in modalità di riflessione.</p> <p>Selezionare Avanti per operare in modalità di inoltra.</p> <p>Nota: Se si seleziona Avanti, è necessario selezionare anche Abilita ricerca MX o Disabilita ricerca MX per configurare il metodo impiegato per determinare l'MTA dell'hop successivo.</p>
Abilita ricerca MX	<p>Questa opzione si applica solo alle configurazioni della modalità di inoltra.</p> <p>Selezionare Abilita ricerca MX per eseguire una query DNS su un nome di dominio e ottenere i record di scambio di posta (MX) per il server. Il server Network Prevent for Email utilizza i record MX restituiti per selezionare l'indirizzo del server di posta dell'hop successivo.</p> <p>Se si seleziona Abilita ricerca MX, aggiungere anche uno o più nomi di dominio nella casella di testo Immetti domini. Ad esempio:</p> <p><code>companyname.com</code></p> <p>Il server Network Prevent for Email esegue query di record MX per i nomi di dominio specificati.</p> <p>Nota: È necessario includere almeno una voce valida nella casella di testo Immetti domini per configurare correttamente il comportamento delle modalità di inoltra.</p>

Campo	Descrizione
Disabilita ricerca MX	<p>Questo campo si applica solo alle configurazioni della modalità di inoltro.</p> <p>Selezionare Disabilita ricerca MX se si desidera specificare il nome host o l'indirizzo IP esatto di uno o più MTA dell'hop successivo. Il server Network Prevent for Email utilizza i nomi host o gli indirizzi specificati e non esegue una ricerca di record MX.</p> <p>Se si seleziona Disabilita ricerca MX, aggiungere anche uno o più nomi di host o indirizzi IP per gli MTA degli hop successivi nella casella di testo Immetti nomi host. È possibile specificare più voci posizionando ognuna di esse su una linea separata. Ad esempio:</p> <pre>smtp1.companyname.com smtp2.companyname.com smtp3.companyname.com</pre> <p>Network Prevent for Email Server prova sempre a indirizzarsi verso il primo MTA che viene specificato nell'elenco. Se tale MTA non è disponibile, il server Network Prevent for Email prova la successiva voce disponibile nell'elenco.</p> <p>Nota: È necessario includere almeno una voce valida nella casella di testo Immetti nome host per configurare correttamente il comportamento delle modalità di inoltro.</p>

Configurazione del canale per Endpoint

Endpoint utilizza il canale Endpoint. È possibile configurare il canale Endpoint nella scheda **Agente**.

Per configurare la scheda Agente

- ◆ Configurare i campi **Listener di agente** :

Campo	Descrizione
Indirizzo di binding	Immettere l'indirizzo IP su cui Endpoint Server ascolta le comunicazioni da Symantec DLP Agent. L'indirizzo IP predefinito è 0.0.0.0 e consente a Endpoint Server di ascoltare su tutti gli indirizzi IP host.
Porta	Immettere la porta sulla quale Endpoint Server ascolta le comunicazioni da Symantec DLP Agent.

Configurazione di impostazioni server avanzate per il Monitoraggio a un solo livello

Poiché il Monitoraggio a un solo livello esegue più canali nello stesso server di rilevazione, è necessario modificare alcune Impostazioni server avanzate per ottenere le migliori prestazioni dal sistema.

Per modificare le Impostazioni server avanzate nel Monitoraggio a un solo livello

- 1 Accedere all'Enforce Server come amministratore.
- 2 Accedere a **Sistema > Server e rilevatori > Panoramica**.
Viene visualizzata la pagina **Panoramica**.
- 3 Fare clic sulla riga del server di rilevamento Monitoraggio a un solo livello.
Viene visualizzata la pagina **Dettagli server/rilevatore**.
- 4 Fare clic su **Impostazioni server**.
Viene visualizzata la pagina **Dettagli server/rilevatore - Impostazioni avanzate**.
- 5 Modificare le seguenti impostazioni:

Impostazione	Valore
MessageChain.NumChains	32
MessageChain.CacheSize	32
PacketCapture.NUMBER_BUFFER_POOL_PACKETS	1.200.000
PacketCapture.NUMBER_SMALL_POOL_PACKETS	1.000.000

- 6 Fare clic su **Salva**.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Vedere ["Controlli server"](#) a pagina 242.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Consultare la guida in linea di Symantec Data Loss Prevention per informazioni sulle impostazioni avanzate del server.

Server di classificazione - Configurazione base

I server di rilevazione sono configurati nella schermata **Configura server** di ogni server. Per visualizzare la schermata **Configura server**, accedere alla schermata **Panoramica (Sistema > Server e rilevatori > Panoramica)** e fare clic sul nome del server nell'elenco. Viene visualizzata la schermata **Dettagli server/rilevatore** per il server. Fare clic su **Configura** per visualizzare lo schermo **Configura server**.

La schermata **Configura server** per un server di classificazione è divisa in due sezioni:

- Sezione **Generale**. Questa sezione specifica il nome del server, l'host e la porta utilizzati per la comunicazione con Enforce Server.
Vedere ["Configurazione di base di server"](#) a pagina 244.
- Sezione **Classificazione**. Questa sezione specifica le proprietà di connessione che il filtro Data Classification for Enterprise Vault utilizza per comunicare con il server di classificazione.

Utilizzare i campi della sezione **Classificazione** per configurare le proprietà di connessione del server:

Numero massimo di sessioni

Immettere il numero massimo di sessioni simultanee che il server di classificazione può accettare dai filtri Data Classification for Enterprise Vault. Il valore predefinito è 12. Il numero massimo delle sessioni che un server di classificazione può supportare dipende dalla CPU e dalla memoria disponibile nel server. Per ulteriori informazioni, consultare la *Guida all'implementazione di Symantec Enterprise Vault Data Classification Services*.

Timeout sessione (in millisecondi)

Immettere il numero massimo di sessioni millisecondi per i quali un filtro Data Classification for Enterprise Vault può restare in attesa che il server di classificazione termini la sessione. Il valore predefinito è 30000 millisecondi.

Porta servizio di classificazione

Specificare il numero della porta sulla quale il server di classificazione accetta le connessioni dai filtri Data Classification for Enterprise Vault. La porta predefinita è 10080.

Nota: Il server di classificazione viene utilizzato solo con la soluzione Symantec Enterprise Vault Data Classification, che ha una licenza separata da quella di Symantec Data Loss Prevention. È necessario configurare il filtro Enterprise Vault Data Classification Services e il server di classificazione in modo che comunichino tra loro. Per ulteriori informazioni, consultare la *Guida all'implementazione di Symantec Enterprise Vault Data Classification Services*.

Modifica di un rilevatore

È possibile modificare il nome del rilevatore sulla schermata **Dettagli server/rilevatore**.

Modifica del nome di un rilevatore

- 1 Accedere a **Sistema > Server e rilevatori > Panoramica** e fare clic sul nome del rilevatore. Viene visualizzata la schermata **Dettagli server/rilevatore**.
- 2 Fare clic su **Modifica**. Viene visualizzata la pagina **Modifica rilevatore**.
- 3 Immettere un nuovo nome per il rilevatore nel campo **Nome rilevatore**.
- 4 Fare clic su **Salva**.

Configurazione server e rivelatore—avanzata

Symantec Data Loss Prevention fornisce le impostazioni di configurazione avanzate per ogni rilevatore o server di rilevamento nel sistema.

Nota: Contattare il supporto Symantec prima di modificare qualsiasi impostazione avanzata. In caso di errori durante la modifica delle impostazioni avanzate, è possibile ridurre drasticamente le prestazioni o anche disattivare interamente il server.

Per modificare un'impostazione di configurazione avanzata per un rilevatore o un server di rilevazione

- 1 Accedere a **Sistema > Server e rilevatori > Panoramica** e fare clic sul nome del server di rilevazione.
 Viene visualizzata la schermata **Dettagli server/rilevatore** di quel server.
- 2 Fare clic su **Impostazioni server** o **Impostazioni rilevatore**, come appropriato.
 Viene visualizzata la schermata **Dettagli server/rilevatore - Impostazioni avanzate**.
 Per informazioni sulla configurazione avanzata di server, vedere la guida in linea di Symantec Data Loss Prevention.
 Vedere ["Impostazioni server avanzate"](#) a pagina 279.
- 3 Con l'orientamento del supporto di Symantec, modificare le impostazioni appropriate.
- 4 Fare clic su **Salva**.
 Le modifiche a queste impostazioni su tale schermata solitamente non ha effetto fino al riavvio del server.
 Vedere ["Configurazione di base di server"](#) a pagina 244.

Aggiunta di un server di rilevazione

Aggiungere i server di rilevazione che si desidera al Symantec Data Loss Prevention sistema dalla schermata di **Sistema > Server e rilevatori > Panoramica**.

È possibile aggiungere i seguenti tipi di server:

- Server di Network Monitor, che controlla il traffico di rete.
- Server di Network Discover/Cloud Storage Discover, che ispeziona nei dati memorizzati le violazioni della politica.
- Server di Network Prevent for Email, che impedisce le violazioni SMTP.
- Server di Cloud Prevent for Email, che impedisce le violazioni del traffico di Microsoft Office 365 Exchange.
- Server di Network Prevent for Web, che impedisce le violazioni del server proxy ICAP quali FTP, HTTP e HTTPS.
- Endpoint Prevent, che controlla i Symantec DLP Agent che controllano ed esplorano gli endpoint.
- Server a un solo livello: selezionando l'opzione Server a un solo livello, i server di rilevamento in licenza vengono installati nello stesso host di Enforce Server. Il server a un solo livello esegue il rilevamento per i seguenti prodotti (è necessario avere una licenza

per ciascuno): Network Monitor, Network Discover, Network Prevent for Email, Network Prevent for Web, ed Endpoint Prevent.

Nota: Symantec consiglia di applicare la stessa configurazione hardware e software a tutti i server di rilevamento che si intende utilizzare per le scansioni della griglia. Symantec Data Loss Prevention supporta le scansioni della griglia con un massimo di 11 server di rilevamento partecipanti.

Per aggiungere un server di rilevamento

- 1 Accedere alla schermata di **Panoramica sistema** (**Sistema > Server e rilevatori > Panoramica**).
Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.
- 2 Fare clic su **Aggiungi server**.
Viene visualizzata la schermata **Aggiungi server**.
- 3 Selezionare il tipo di server che si desidera installare e fare clic su **Avanti**.
Compare la schermata **Configura server** per quel server di rilevazione.
- 4 Per eseguire la configurazione del server di base, utilizzare la schermata **Configura server**, quindi fare clic su **Salva** al termine.
Vedere ["Server Network Monitor - Configurazione di base"](#) a pagina 246.
Vedere ["Server Network Prevent for Email - Configurazione di base"](#) a pagina 248.
Vedere la *Guida all'implementazione di Symantec Data Loss Prevention Cloud Prevent for Microsoft Office 365* per maggiori informazioni.
Vedere ["Server Network Prevent for Web - Configurazione di base"](#) a pagina 251.
Vedere ["Server Network Discover/Cloud Storage Discover e Network Protect - Configurazione di base"](#) a pagina 254.
Vedere ["Endpoint Server - Configurazione di base"](#) a pagina 255.
Vedere ["Monitoraggio a un solo livello - configurazione di base"](#) a pagina 256.
- 5 Per ritornare alla schermata **Panoramica sistema**, fare clic su **Fine**.
Il nuovo server viene visualizzato nella lista **Server e rilevatori** con lo stato **Sconosciuto**.
- 6 Fare clic sul server per visualizzare la schermata **Dettagli server/rilevatore**.
Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.
- 7 Fare clic su **[Ricicla]** per riavviare il server.

- 8 Fare clic su **Fine** per ritornare alla schermata **Panoramica sistema**.

Quando il server ha finito il riavvio, il suo stato è **In esecuzione**.

- 9 Se necessario, fare clic su **Impostazioni server** nella schermata **Dettaglio server/rilevatore** per eseguire la configurazione del server avanzata.

Vedere "[Impostazioni server avanzate](#)" a pagina 279.

Per informazioni sulla configurazione avanzata di server, vedere la guida in linea di Symantec Data Loss Prevention.

Vedere "[Configurazione di base di server](#)" a pagina 244.

Aggiunta di un rilevatore di cloud

Un rilevatore di cloud è un servizio di rilevamento Symantec Data Loss Prevention distribuito nel cloud Symantec. Dopo la configurazione da parte di Symantec del servizio di rilevamento nel cloud, Symantec invia all'utente un pacchetto di registrazione. Questo pacchetto contiene le informazioni necessarie per configurare la connessione da Enforce Server on-site al servizio di rilevamento nel cloud Symantec.

Il pacchetto di registrazione è un archivio ZIP. Per motivi di sicurezza, il file ZIP non estratto dovrebbe essere salvato in una posizione non accessibile da altri utenti. Ad esempio, in un sistema Microsoft Windows, salvare il pacchetto in una cartella come:

```
c:\Users\username\downloads
```

In un sistema Linux, salvare il pacchetto in una directory come:

```
/home/username/
```

Consultare la documentazione del rilevatore di cloud per informazioni più dettagliate sul processo di registrazione.

Dopo aver salvato il pacchetto di registrazione, registrare il rilevatore di cloud per attivare la comunicazione tra di esso ed Enforce Server on-site.

Per registrare un rilevatore di cloud

- 1 Accedere all'Enforce Server come amministratore.
- 2 Accedere a **Sistema > Server e rilevatori > Panoramica**.
Viene visualizzata la pagina **Panoramica**.
- 3 Fare clic su **Aggiungi rilevatore cloud**.
Viene visualizzata la pagina **Aggiungi rilevatore cloud**.
- 4 Fare clic su **Sfoglia** nel campo **File pacchetto di registrazione**.

- 5 Individuare il file del pacchetto di registrazione salvato, quindi immettere un nome nel campo **Nome rilevatore**.
- 6 Fare clic su **Registra rilevatore**.
Viene visualizzato lo schermo Dettagli server/rilevatore.
- 7 Se necessario, fare clic su **Impostazioni rilevatore** nella schermata **Dettagli server/rilevatore** per eseguire la configurazione avanzata del rilevatore.
Vedere "[Impostazioni rilevatore avanzate](#)" a pagina 328.
- 8 Fare clic su **Fine**.

Possono essere necessari diversi minuti perché la console di amministrazione Enforce Server mostri che l'esecuzione del rilevatore di cloud è in corso. Per verificare che il rilevatore sia stato aggiunto, verificare la pagina **Sistema > Server e rilevatori > Panoramica**. Il rilevatore dovrebbe essere visualizzato nell'elenco **Server e rilevatori** con lo stato **Connesso**.

Eliminazione di un server

Vedere la *Guida di installazione di Symantec Data Loss Prevention* appropriata per informazioni su come disinstallare Symantec Data Loss Prevention da un server.

La console di amministrazione di Enforce Server elenca i server di rilevamento registrati nella console stessa nella schermata **Sistema > Server e rilevatori > Panoramica**. Se Symantec Data Loss Prevention viene disinstallato da un server di rilevamento o il server è stato arrestato o disconnesso dalla rete, lo stato viene visualizzato come Sconosciuto nella console.

Un server di rilevamento può essere rimosso (annullamento della registrazione) da una console di amministrazione di Enforce Server. Quando un server di rilevamento è stato rimosso da un Enforce Server, i relativi servizi Symantec Data Loss Prevention continuano a funzionare. Ciò significa che quando la registrazione di un server di rilevamento viene annullata da Enforce, il server continua a funzionare, a meno che non venga arrestato. In altre parole, anche se viene rimosso da una console di amministrazione di Enforce Server, un server di rilevazione continua a funzionare. Gli incidenti che rileva sono memorizzati sul server di rilevazione. Se un server di rilevazione viene registrato di nuovo in un Enforce Server, gli incidenti rilevati e memorizzati vengono inoltrati all'Enforce Server.

Per rimuovere (annullare la registrazione) un server di rilevazione dall'Enforce Server

- 1 Accedere a **Sistema > Server e rilevatori > Panoramica**.
Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.
- 2 Nella sezione **Server e rilevatori** della schermata, fare clic sulla X rossa sulla riga dello stato del server per rimuoverlo da questa console di amministrazione di Enforce Server.
Vedere ["Controlli server"](#) a pagina 242.
- 3 Fare clic su **OK** per confermare.
La riga dello stato del server viene rimossa dall'elenco Panoramica sistema.

Importazione di certificati SSL in Enforce o Discover server

È possibile importare certificati SSL nell'archivio chiavi attendibile Java degli Enforce o Discover Server. Il certificato SSL può essere autofirmato (server) o emesso da un'autorità di certificazione nota.

Potrebbe essere necessario importare un certificato SSL per eseguire connessioni protette ai server esterni come Active Directory (AD). Se un'autorità riconosciuta ha firmato il certificato del server esterno, il certificato viene automaticamente aggiunto a Enforce Server. Se il certificato del server è autofirmato, è necessario importarlo manualmente in Enforce Server o Discover Server.

Tabella 13-3 Importazione di un certificato SSL in Enforce Server o Discover Server

Passaggio	Descrizione
1	Copiare il file di certificato che si desidera importare nel computer Enforce Server o Discover Server.
2	Passare alla directory <code>c:\Programmi\Symantec\Data Loss Prevention\Server JRE\1.8.0_162\lib\security</code> sul computer Enforce Server o Discover Server.
3	<p>Eseguire l'utilità <code>keytool</code> con l'opzione <code>-importcert</code> per importare il certificato della chiave pubblica nell'archivio chiavi di Enforce Server o Discover Server:</p> <pre>keytool -importcert -alias new_endpointgroup_alias -keystore ..\lib\security\cacerts -file my-domaincontroller.crt</pre> <p>In questo comando di esempio, <code>new_endpointgroup_alias</code> è un nuovo alias da assegnare al certificato importato e <code>my-domaincontroller.crt</code> è il percorso al certificato.</p>

Passo	Descrizione
4	<p>Quando richiesto, immettere la password per l'archivio chiavi.</p> <p>Per impostazione predefinita, la password è changeit. Se lo si desidera, è possibile modificare la password quando richiesto.</p> <p>Per modificare la password, utilizzare: <code>keytool -storepassword -alias new_endpointgroup_alias -keystore ..\lib\security\cacerts</code></p>
5	Fare clic su Sì quando viene chiesto se si considera attendibile il certificato.
6	Riavviare Enforce Server o Discover Server.

Vedere ["Configurazione delle connessioni a server di directory"](#) a pagina 162.

Informazioni sulla schermata Panoramica

Per accedere alla schermata **Panoramica sistema**, selezionare **Sistema > Server e rilevatori > Panoramica**. Questa schermata fornisce una rapida istantanea dello stato del sistema.

Elenca le informazioni su Enforce Server e su ogni server di rilevamento, rilevatore di cloud o dispositivo registrato.

La schermata **Panoramica sistema** offre le seguenti funzionalità:

- Il pulsante **Aggiungi server** è utilizzato per registrare un server di rilevazione. Quando si visualizza questa schermata per la prima volta dopo l'installazione, solo Enforce Server è elencato. È necessario registrare i vari server di rilevazione con il pulsante **Aggiungi server**. Dopo la registrazione dei server di rilevamento, questi sono elencati nella sezione **Server e rilevatori** della schermata.

Vedere ["Aggiunta di un server di rilevazione"](#) a pagina 268.

- Il pulsante **Aggiungi rilevatore cloud** è utilizzato per registrare un rivelatore di cloud. Quando si visualizza questa schermata per la prima volta dopo l'installazione, solo Enforce Server è elencato. È necessario registrare i rilevatori di cloud con il pulsante **Aggiungi rilevatore cloud**. Dopo la registrazione dei rilevatori di cloud, questi sono elencati nella sezione **Server e rilevatori** della schermata.

- Il pulsante **Aggiungi dispositivo** è utilizzato per registrare un dispositivo. Quando si visualizza questa schermata per la prima volta dopo l'installazione, solo Enforce Server è elencato. È necessario registrare i dispositivi con il pulsante **Aggiungi dispositivo**. Dopo la registrazione dei dispositivi, questi sono elencati nella sezione **Server e rilevatori** della schermata.

Vedere ["Aggiunta di un dispositivo"](#) a pagina 2305.

- Il pulsante **Preparazione sistema e aggiornamento dispositivi** è utilizzato per accedere alla schermata **Preparazione sistema e aggiornamento dispositivi** in cui è possibile eseguire dei test per confermare l'aggiornamento del database e dei dispositivi.
- Il pulsante **Upgrade** consente l'upgrade di Symantec Data Loss Prevention a una versione più recente.
Vedere ["Informazioni sugli aggiornamenti del sistema"](#) a pagina 238.
Vedere anche il *Manuale di aggiornamento di Symantec Data Loss Prevention* appropriato.
- La sezione **Server e rilevatori** della schermata visualizza informazioni riepilogative sullo stato di ogni server, rilevatore o dispositivo. Può anche essere utilizzata per rimuovere (annullare la registrazione) di un server, un rilevatore o un dispositivo.
Vedere ["Panoramica dello stato di server e rivelatori"](#) a pagina 275.
- La sezione **Eventi di errore e avviso recenti** mostra gli ultimi cinque eventi con livello di gravità errore o avviso di tutti i server elencati nella sezione **Server e rilevatori**.
Vedere ["Elenco degli eventi di errore e avviso recenti"](#) a pagina 277.
- La sezione **Licenza** della schermata elenca i singoli prodotti di Symantec Data Loss Prevention per i quali si dispone di una licenza d'uso.
Vedere ["Configurazione di base di server"](#) a pagina 244.
Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Configurazione di Enforce Server per l'utilizzo di un proxy per connettersi ai servizi cloud

Per configurare Enforce Server per l'utilizzo di un proxy per connettersi ai servizi cloud, è necessario impostare il proxy seguendo le istruzioni del produttore dello stesso. Quindi configurare Enforce Server per supportare l'utilizzo del proxy. Dopo aver impostato il proxy, utilizzare queste istruzioni per completare la configurazione.

Per configurare Enforce Server per l'utilizzo di un proxy per connettersi al servizio cloud







- 1 Accedere a **Sistema > Impostazioni > Generale** e fare clic su **Configura**. Viene visualizzata la schermata **Modifica impostazioni generali**.
- 2 Nella sezione **Applica a proxy del cloud**, selezionare una delle seguenti categorie di proxy:
 - **Nessun proxy o proxy trasparente**, oppure
 - **Proxy manuale**
- 3 Se si sceglie **Proxy manuale**, vengono visualizzati i campi **URL**, **Porta** e **Proxy autenticato**.
 - Immettere l'URL del proxy HTTP per il servizio cloud ottenuto da Symantec.

- Immettere un numero di porta.
- 4 Se si utilizza un proxy autenticato, immettere anche
 - un ID utente
 - una password
- 5 Fare clic su **Salva**.
- 6 Riavviare il Controller del server di rilevamento di Symantec DLP.

Panoramica dello stato di server e rivelatori

Per accedere alla sezione **Server e rivelatori** della schermata **Panoramica sistema**, selezionare **Sistema > Server e rivelatori > Panoramica**. Questa sezione della schermata fornisce una rapida panoramica dello stato del sistema.

Tabella 13-4 Stati di server e rivelatori

Icona	Stato	Descrizione
	Avvio in corso	Il server è in fase di avvio.
	In esecuzione	L'esecuzione del server è normale e senza errori.
	Selezionato in esecuzione	Alcuni processi di Symantec Data Loss Prevention sul server sono stati arrestati o presentano errori. Per visualizzare gli stati di singoli processi, è necessario dapprima attivare l'opzione Controllo dei processi avanzato nella schermata Impostazioni di sistema . Vedere " Attivazione del controllo dei processi avanzato " a pagina 241.
	Arresto in corso	Il server sta arrestando i servizi di Symantec Data Loss Prevention. Vedere " Informazioni sui servizi Symantec Data Loss Prevention " a pagina 101.
	Arrestato	Tutti i processi di Symantec Data Loss Prevention sono stati arrestati.
	Sconosciuto	Il server presenta uno dei seguenti errori: <ul style="list-style-type: none"> ■ Enforce Server non è raggiungibile dal server. ■ Symantec Data Loss Prevention non è installato sul server. ■ Una chiave di licenza non è stata configurata per Enforce Server. ■ C'è un problema con le autorizzazioni dell'account di Symantec Data Loss Prevention in Windows.

Per ogni server, vengono visualizzate anche le informazioni descritte di seguito. È anche possibile fare clic su un qualsiasi nome di server per visualizzare la schermata **Dettagli server/rilevatore** per quel server.

Tabella 13-5 Ulteriori informazioni sullo stato di server e rilevatori

Nome colonna	Descrizione
Messaggi (ultimi 10 sec)	Il numero di messaggi elaborati negli ultimi 10 secondi.
Messaggi (ultime 24 ore)	Il numero di messaggi elaborati nelle ultime 24 ore.
Incidenti (ultime 24 ore)	Il numero di incidenti elaborati nelle ultime 24 ore. Per gli Endpoint Server, il numero di incidenti e messaggi non corrispondono. Questo perché l'elaborazione dei messaggi viene eseguita sull'endpoint e non su Endpoint Server. Tuttavia, il numero di incidenti continua ad aumentare.
Coda incidenti	Per Enforce Server, si tratta del numero di incidenti nel database, anche se non hanno ancora uno stato. Questo numero cambia ogni volta che si aggiorna la schermata. Per gli altri tipi di server, questo è il numero di incidenti non ancora registrati su Enforce Server. Questo numero viene aggiornato approssimativamente ogni 30 secondi. Se si arresta il server, questo è l'ultimo numero aggiornato dal server. Presumibilmente gli incidenti sono ancora nella cartella degli incidenti.
Tempo di attesa messaggi	L'intervallo di tempo necessario per elaborare un messaggio dopo la registrazione nel sistema. Questi dati si applicano all'ultimo messaggio elaborato. Se il server che ha elaborato l'ultimo messaggio è disconnesso, il valore è N/D.

Per visualizzare informazioni dettagliate su un server o un rivelatore

- ◆ Fare clic su qualsiasi nome di server per visualizzare ulteriori informazioni su quel server.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Per rimuovere un server o un rivelatore da un Enforce Server

- ◆ Fare clic sulla X rossa del server e confermare la decisione.



Nota: La rimozione (l'annullamento della registrazione) di un server comporta la disconnessione dello stesso da Enforce Server, ma non l'arresto del server di rilevazione.

Vedere ["Eliminazione di un server"](#) a pagina 271.

Elenco degli eventi di errore e avviso recenti

La sezione **Eventi di errore e avviso recenti** della schermata **Sistema > Server e rilevatori > Panoramica** mostra gli ultimi cinque eventi con gravità di errore o avviso per i server elencati nella sezione **Server e rilevatori**.

Tabella 13-6 Informazioni sugli eventi di errore e avviso recenti

Nome colonna	Descrizione
Tipo	  Il triangolo giallo indica un avviso, l'ottagono rosso indica un errore.
Orario	La data e l'ora in cui si è verificato l'evento.
Server	Il nome del server in cui si è verificato l'evento.
Host	L'indirizzo IP o il nome del computer in cui si trova il server. Il nome del server e quello dell'host potrebbero coincidere.
Codice	Il codice evento di sistema. La colonna Messaggio fornisce il testo del codice. Gli elenchi di eventi possono essere filtrati per numero di codice.
Messaggio	Un riassunto del messaggio di errore o di avviso associato a questo codice di evento.

- Per visualizzare un elenco di tutti gli eventi di errore e avviso, fare clic su **Mostra tutto**.
- Per visualizzare la schermata **Dettagli evento** per ulteriori informazioni su quell'evento particolare, fare clic su un evento.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Vedere ["Report di eventi di sistema"](#) a pagina 172.

Vedere ["Dettagli eventi di server e rivelatori"](#) a pagina 176.

Schermata Dettagli server/rilevatore

La schermata **Dettagli server/rilevatore** fornisce informazioni dettagliate relative a un singolo server, rilevatore o dispositivo selezionato. La schermata **Dettagli server/rilevatore** serve anche a controllare e configurare un server, rilevatore o dispositivo.

Per visualizzare la schermata **Dettagli server/rilevatore** per un determinato server o rilevatore

- 1 Accedere alla schermata **Sistema > Server e rilevatori > Panoramica**.
- 2 Fare clic sul nome del server di rilevamento, del rilevatore o del dispositivo nell'elenco **Server e rilevatori**.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

La schermata **Dettagli server/rilevatore** è divisa in sezioni. Le sezioni elencate di seguito visualizzano tutti i tipi di server, rilevatore e dispositivo. Il sistema visualizza le sezioni in base al tipo di rilevamento.

Tabella 13-7 Informazioni visualizzate nella schermata Dettagli server

Sezioni visualizzate in Dettagli server	Descrizione
Generale	<p>La sezione Generale identifica il server, visualizza lo stato del sistema e le statistiche e fornisce dei controlli per avviare e arrestare il server e i suoi processi.</p> <p>Vedere "Controlli server" a pagina 242.</p>
Configurazione	<p>La sezione Configurazione visualizza i Canali, Gruppi di politiche, Configurazione agente, Dispositivo utente e Stato configurazione per il server di rilevamento.</p>
Tutti gli agenti	<p>La sezione Tutti gli agenti visualizza un riassunto di tutti gli agenti assegnati a un Endpoint Server.</p> <p>Fare clic sul numero accanto allo stato di un agente per vederne i dettagli nella schermata Sistema > Agenti > Panoramica > Report riepilogativi.</p> <p>Nota: Il sistema visualizza la sezione Riepilogo agente solo per un Endpoint Server.</p>
Eventi di errore e avviso recenti	<p>La sezione Eventi di errore e avviso recenti visualizza i cinque eventi Avviso o Grave più recenti che si sono verificati su questo server.</p> <p>Fare clic su un evento per vederne i dettagli. Fare clic su Mostra tutto per visualizzare tutti gli eventi di errore e avviso.</p> <p>Vedere "Informazioni sugli eventi di sistema" a pagina 171.</p>
Tutti gli eventi recenti	<p>La sezione Tutti gli eventi recenti visualizza tutti gli eventi di tutte le gravità che si sono verificati su questo server nelle ultime 24 ore.</p> <p>Fare clic su un evento per vederne i dettagli. Fare clic su Mostra tutto per visualizzare tutti gli eventi del server di rilevamento.</p>

Sezioni visualizzate in Dettagli server	Descrizione
Profili dati esatti distribuiti	La sezione Profili dati esatti distribuiti elenca gli eventuali Dati esatti o Profili documento distribuiti al server di rilevamento. Il sistema visualizza la versione dell'indice nel profilo. Vedere " Profili dati " a pagina 381.

Vedere "[Informazioni sulla schermata Panoramica](#)" a pagina 273.

Vedere "[Configurazione di base di server](#)" a pagina 244.

Vedere "[Controlli server](#)" a pagina 242.

Vedere "[Report di eventi di sistema](#)" a pagina 172.

Vedere "[Dettagli eventi di server e rivelatori](#)" a pagina 176.

Impostazioni server avanzate

Fare clic su **Impostazioni server** nella schermata del server di rilevamento **Sistema > Server e rilevatori > Panoramica > Dettagli server/rilevatore** per modificare le impostazioni su quel server.

Prestare attenzione quando si modificano queste impostazioni su un server. Contattare il supporto Symantec prima di modificare qualsiasi impostazione nella schermata. Le modifiche a queste impostazioni normalmente non entrano in vigore fino a dopo il riavvio del server.

Non è possibile modificare le impostazioni per Enforce Server dalla schermata **Dettagli server/rilevatore**. Nella schermata **Dettagli server/rilevatore - Impostazioni avanzate** vengono visualizzati solo server di rilevamento e rilevatori.

Nota: Se si cambiano le impostazioni avanzate del server agli Endpoint Server in un ambiente con bilanciamento del carico, è necessario applicare le stesse modifiche a tutti gli Endpoint Server nell'ambiente con bilanciamento del carico.

Tabella 13-8 Impostazioni avanzate dei server di rilevamento

Impostazioni	Impostazione predefinita	Descrizione
BoxMonitor.Channels	Varia	<p>I valori fanno distinzione tra maiuscole e minuscole e vengono separati con virgola se multipli.</p> <p>Sebbene sia possibile configurare qualsiasi mix di configurazioni, le configurazioni ufficialmente supportate sono le seguenti:</p> <ul style="list-style-type: none"> ■ Server Network Monitor: Acquisizione del pacchetto, Copia regola ■ Discover Server: Discover ■ Endpoint Server: Endpoint ■ Network Prevent for Email: SMTP inline ■ Network Prevent for Web: ICAP
BoxMonitor.DetectionServerDatabase	attivato	<p>Attiva il processo di BoxMonitor per avviare il database Automated Incident Remediation Tracking sul server di rilevamento. Se lo si imposta su <code>off</code>, è necessario avviare manualmente il database di tracciamento delle risoluzioni.</p>
BoxMonitor.DetectionServerDatabaseMemory	-Xrs -Xms300M -Xmx1024M	<p>È possibile utilizzare qualsiasi combinazione di flag di memoria JVM.</p>
BoxMonitor.DiskUsageError	90	<p>La quantità di spazio su disco occupata (in percentuale) che attiverà un evento di sistema grave. Ad esempio, se Symantec Data Loss Prevention è installato sull'unità C e questo valore è di 90, il server di rilevamento crea un evento di sistema grave quando l'utilizzo dell'unità C è superiore al 90%.</p>

Impostazioni	Impostazione predefinita	Descrizione
BoxMonitor.DiskUsageWarning	80	La quantità di spazio su disco occupata (in percentuale) che attiverà un evento di sistema di avviso. Ad esempio, se Symantec Data Loss Prevention è installato sull'unità C e questo valore è di 80 , il server di rilevamento crea un evento di sistema di avviso quando l'utilizzo dell'unità C è superiore all'80%.
BoxMonitor.EndpointServer	attivato	Attiva l'Endpoint Server.
BoxMonitor.EndpointServerMemory	-Xrs -Xms300M -Xmx4096M	È possibile utilizzare qualsiasi combinazione di flag di memoria JVM. Ad esempio: -Xrs -Xms300m -Xmx1024m .
BoxMonitor.FileReader	attivato	Se disattivato, BoxMonitor non può avviare FileReader, ma quest'ultimo può comunque essere avviato manualmente.
BoxMonitor.FileReaderMemory	-Xrs -Xms1200M -Xmx4G	Argomenti della riga di comando della JVM FileReader.
BoxMonitor.HeartbeatGapBeforeRestart	960000	L'intervallo di tempo (in millisecondi) in cui BoxMonitor attende un processo di monitoraggio (ad esempio FileReader, IncidentWriter) per segnalare l'heartbeat. Se l'heartbeat non viene ricevuto entro questo intervallo di tempo, BoxMonitor riavvia il processo.
BoxMonitor.IncidentWriter	attivato	Se disattivato, BoxMonitor non può avviare IncidentWriter in modalità a due livelli, ma quest'ultimo può ancora essere avviato manualmente. Questa impostazione non ha effetto nella modalità a un livello.

Impostazioni	Impostazione predefinita	Descrizione
BoxMonitor.IncidentWriterMemory	-Xrs	Argomenti della riga di comando della JVM IncidentWriter. Ad esempio: -Xrs
BoxMonitor.InitialRestartWaitTime	5000	L'intervallo di tempo in millisecondi che BoxMonitor attende dopo il riavvio di un processo di monitoraggio, ad esempio FileReader o IncidentWriter.
BoxMonitor.MaxRestartCount	3	Il numero di volte in cui un processo può essere riavviato in un'ora prima della generazione di un evento di sistema GRAVE.
BoxMonitor.MaxRestartCountDuringStartup	5	Il numero massimo di volte in cui il server di monitoraggio tenterà di riavviarsi autonomamente.
BoxMonitor.PacketCapture	attivato	Se disattivato, BoxMonitor non può avviare PacketCapture, ma quest'ultimo può ancora essere avviato manualmente. Il canale PacketCapture deve essere attivato affinché questa impostazione funzioni.
BoxMonitor.PacketCaptureDirectives	-Xrs	Parametri della riga di comando di PacketCapture (in Java). Ad esempio: -Xrs
BoxMonitor.ProcessLaunchTimeout	30000	L'intervallo di tempo (in millisecondi) per avviare un processo di monitoraggio (ad esempio FileReader).
BoxMonitor.ProcessShutdownTimeout	45000	L'intervallo di tempo (in millisecondi) assegnato a ogni processo di monitoraggio per effettuare un arresto normale. Se il processo è ancora in esecuzione al termine dell'intervallo di tempo, BoxMonitor tenta di interrompere il processo.

Impostazioni	Impostazione predefinita	Descrizione
BoxMonitor.RequestProcessor	attivato	Se disattivato, BoxMonitor non può avviare RequestProcessor, ma quest'ultimo può ancora essere avviato manualmente. Il canale SMTP inline deve essere attivato affinché questa impostazione funzioni.
BoxMonitor.RequestProcessorMemory	-Xrs -Xms300M -Xmx1300M	È possibile utilizzare qualsiasi combinazione di flag di memoria JVM. Ad esempio: -Xrs -Xms300M -Xmx1300M
BoxMonitor.RmiConnectionTimeout	15000	L'intervallo di tempo (in millisecondi) concesso per stabilire il collegamento all'oggetto RMI.
BoxMonitor.RmiRegistryPort	37329	La porta TCP in cui BoxMonitor avvia il registro RMI.
BoxMonitor.StatisticsUpdatePeriod	10000	Le statistiche di monitoraggio vengono aggiornate dopo questo intervallo di tempo (in millisecondi).
Classification.WebServiceLogRetentionDats	7	Specifica il numero di giorni per i quali vengono conservati registri di servizi web di classificazione.
ContentExtraction.DefaultCharsetForSubFileName	N/D	Definisce il set di caratteri predefinito che viene utilizzato nella decodifica del nome file secondario se la conversione del set di caratteri non riesce.

Impostazioni	Impostazione predefinita	Descrizione
ContentExtraction.EnableMetaData	disattivato	Consente il rilevamento sui metadati del file. Se l'impostazione è attiva , è possibile rilevare i metadati per file Microsoft Office e PDF. Per i file Microsoft Office, sono supportati i metadati OLE, i quali includono i campi Titolo, Oggetto, Autore e Parole chiave. Per i file PDF, solo i metadati del dizionario informazioni documento sono supportati, i quali includono campi come Autore, Titolo, Oggetto, Creazione e Date di aggiornamento. Il contenuto Extensible Metadata Platform (XMP) non è rilevato. Tenere presente che l'attivazione di questa opzione di rilevamento metadati può generare falsi positivi.

Impostazioni	Impostazione predefinita	Descrizione
ContentExtraction.ImageExtractorEnabled	1	<p>Consente di regolare o disattivare l'estrazione dei contenuti per Riconoscimento moduli.</p> <p>L'impostazione predefinita, 1, carica il plug-in Image Extractor su richiesta. Se vengono usate una o più regole di Riconoscimento moduli, il plug-in Dynamic Image Extractor viene caricato automaticamente nel server di rilevamento quando si ricevono gli aggiornamenti della politica corrispondenti. Quando si eliminano o disattivano regole di Riconoscimento moduli, il caricamento del plug-in viene annullato automaticamente. Questa opzione impedisce l'esecuzione del plug-in Dynamic Image Extractor se non si utilizza Riconoscimento moduli.</p> <p>Immettere 0 per disattivare il plug-in Image Extractor. Questa impostazione impedisce a Riconoscimento moduli di estrarre immagini, disattivando di fatto la funzionalità.</p> <p>Immettere 2 se si desidera caricare il plug-in Image Extractor all'apertura del servizio di estrazione del contenuto dopo l'avvio di server di rilevamento. Il plug-in continua a funzionare indipendentemente dal fatto che siano o non siano state configurate politiche di Riconoscimento moduli.</p>
ContentExtraction.LongContentSize	1M	<p>Se il componente del messaggio supera queste dimensioni (in byte), <code>ContentExtraction.LongTimeout</code> viene utilizzato al posto di <code>ContentExtraction.ShortTimeout</code>.</p>

Impostazioni	Impostazione predefinita	Descrizione
ContentExtraction.LongTimeout	Varia	<p>Il valore predefinito per questa impostazione varia in base al tipo di server di rilevamento (60.000 o 120.000).</p> <p>L'intervallo di tempo (in millisecondi) a disposizione di <code>ContentExtractor</code> per elaborare un documento più grande di <code>ContentExtraction.LongContentSize</code>. Se il documento non viene elaborato entro il tempo specificato, viene segnalato come non elaborato. Questo valore deve essere maggiore di <code>ContentExtraction.ShortTimeout</code> e minore di <code>ContentExtraction.RunawayTimeout</code>.</p>
ContentExtraction.MarkupAsText	disattivato	<p>Consente di ignorare l'estrazione di contenuti per file con estensione XML o HTML. Dovrebbe essere utilizzato in casi come pagine Web contenenti dati nel blocco intestazione o script. Il valore predefinito è Off.</p>
ContentExtraction.MaxContentSize	30M	<p>La dimensione massima (in MB) del documento che può essere elaborato da <code>ContentExtractor</code>.</p>
ContentExtraction.MaxNumImagesToExtract	10	<p>Il numero massimo di immagini da estrarre dai file PDF e dai documenti TIFF a più pagine.</p>

Impostazioni	Impostazione predefinita	Descrizione
ContentExtraction.RunawayTimeout	300.000	L'intervallo di tempo (in millisecondi) a disposizione di ContentExtractor per completare l'elaborazione di qualsiasi documento. Se ContentExtractor non completa l'elaborazione di un determinato documento entro questi limiti, verrà considerato instabile e il processo verrà riavviato. Questo valore deve essere considerevolmente maggiore di <code>ContentExtraction.LongTimeout</code> .
ContentExtraction.ShortTimeout	30.000	L'intervallo di tempo (in millisecondi) a disposizione di ContentExtractor per elaborare un documento più piccolo di <code>ContentExtraction.LongContentSize</code> . Se il documento non viene elaborato entro il tempo specificato, viene segnalato come non elaborato. Questo valore deve essere minore di <code>ContentExtraction.LongTimeout</code> .
ContentExtraction.TemporaryDirectory		Specifica la directory per i file temporanei di estrazione del contenuto.

Impostazioni	Impostazione predefinita	Descrizione
ContentExtraction.TrackedChanges	disattivato	<p>Consente il rilevamento del contenuto modificato nel tempo (contenuto Revisioni) nei documenti di Microsoft Office.</p> <p>Nota: L'utilizzo dell'opzione precedente potrebbe ridurre il tasso di accuratezza per identificatori dati e IDM. Il valore predefinito è impostato su Off (non consentire).</p> <p>Per indicizzare il contenuto modificato nel tempo, impostare <code>ContentExtraction.TrackedChanges=on</code> nel file <code>Indexer.properties</code>. Il valore predefinito e l'impostazione consigliata è off.</p>

Impostazioni	Impostazione predefinita	Descrizione
DDM.MaxBinMatchSize	30.000.000	<p>La dimensione massima (in byte) utilizzata per generare l'hash MD5 per una corrispondenza binaria esatta in un IDM. Questa impostazione non dovrebbe essere modificata. Per consentire il corretto funzionamento di IDM, devono essere rispettate le seguenti condizioni:</p> <ul style="list-style-type: none"> ■ Questa impostazione deve essere esattamente identica all'impostazione <code>max_bin_match_size</code> su Enforce Server nel file <code>indexer.properties</code>. ■ Questa impostazione deve essere inferiore o uguale al valore <code>FileReader.FileMaxSize</code> ■ Questa impostazione deve essere minore di o uguale al valore <code>ContentExtraction.MaxContentSize</code> su Enforce Server nel file <code>indexer.properties</code>. <p>Nota: La modifica del primo o terzo elemento nell'elenco richiede la reindicizzazione di tutti i file IDM.</p>
Detection.EncodingGuessingDefaultEncoding	ISO-8859-1	Specifica la codifica di backup presupposta per un flusso di byte.
Detection.EncodingGuessingEnabled	attivato	Designa se è necessario identificare la codifica di flussi di byte sconosciuti.
Detection.EncodingGuessingMinimumConfidence	50	Specifica il livello di sicurezza richiesto per l'ipotesi di codifica dei flussi di byte sconosciuti.

Impostazioni	Impostazione predefinita	Descrizione
Detection.MessageTimeout ReportIntervalInSeconds	3600	Il numero dei secondi tra ogni evento di sistema pubblicato per visualizzare il numero dei messaggi scaduti di recente. Questi eventi di sistema sono pianificati per essere pubblicati a cadenza fissa, ma verranno saltati se non sono presenti messaggi scaduti nel periodo specifico.
DI.MaxViolations	100	Specifica il numero massimo di violazioni consentite con gli identificatori di dati.
Discover.CountAllFilteredItems	false	<p>Fornisce statistiche di scansione più accurate contando gli elementi nelle cartelle saltate a causa dei filtri.</p> <p>Impostando il valore su false si attivano i filtri di percorso ottimizzati di Discover, che migliorano le prestazioni ma a volte possono generare un comportamento imprevisto del filtro. I filtri ottimizzati normalizzano le barre, troncano le stringhe di filtro prima dei caratteri jolly e rimuovono le barre finali. Di conseguenza, la stringa di filtro /Car*tella corrisponderà a /Folder, ma anche a /FolXYZ.</p> <p>Impostare questo valore su true per disattivare i filtri di percorso ottimizzati di Discover.</p>
Discover.Exchange.FollowRedirects	true	Specifica se seguire i reindirizzamenti. Symantec Data Loss Prevention segue i reindirizzamenti solo dalla cartella principale pubblica.
Discover.Exchange.ScanHiddenItems	false	Se impostato su true, esegue la scansione di elementi nascosti in repository Exchange.

Impostazioni	Impostazione predefinita	Descrizione
Discover.Exchange.UseSecureHttpConnections	true	Specifica se i collegamenti a repository Exchange e Active Directory sono sicuri quando si utilizza il crawler dei servizi Web di Exchange.
Discover.IgnorePstMessageClasses	IPM.Appointment, IPM.Contact, IPM.Task, REPORT. IPM. Note.DR, REPORT. IPM. Note.IPNRN	Questa impostazione specifica un elenco di classi di messaggi .pst separate da virgola. Tutti gli elementi in un file .pst che hanno una classe di messaggio nell'elenco verranno ignorati (non verrà effettuato nessun tentativo di estrarre l'elemento .pst). Questa impostazione fa distinzione tra maiuscole e minuscole.
Discover.IncludePstMessageClasses	IPM.Note	Questa impostazione specifica un elenco di classi di messaggi .pst separate da virgola. Tutti gli elementi in un file .pst che hanno una classe di messaggio nell'elenco verranno inclusi. Una volta definite entrambe le impostazioni di inclusione ed esclusione, Discover.IncludePstMessageClasses ha la precedenza.
Discover.PollInterval	10000	Specifica a quale intervallo di tempo (in millisecondi) Enforce recupera i dati dal monitoraggio Discover durante la scansione.
Discover.Sharepoint.FetchACL	true	Spegne ACL recuperando le scansioni SharePoint integrate. Il valore predefinito è true (attivato).
Discover.Sharepoint.SocketTimeout	60000	Fissa il valore di timeout della connessione socket (in millisecondi) tra il server Network Discover e il target SharePoint.

Impostazioni	Impostazione predefinita	Descrizione
Discover.ValidateSSLCertificates	false	<p>Impostare su true per attivare la convalida dei certificati SSL per le connessioni HTTPS per target SharePoint ed Exchange. Quando la convalida è attivata, la scansione dei server SharePoint o Exchange effettuata con certificati autofirmati o non attendibili non riesce. Se l'applicazione Web SharePoint o il server Exchange sono firmati da un certificato emesso da un'Autorità di certificazione (CA), il certificato del server o il certificato CA del server deve risiedere nell'archivio chiavi attendibile di Java utilizzato da Discover Server. Se il certificato non risiede nell'archivio chiavi, è necessario importarlo manualmente utilizzando l'utilità <code>keytool</code>.</p> <p>Vedere "Importazione di certificati SSL in Enforce o Discover server" a pagina 272.</p>
EDM.HighlightAllMatchesInProximity	false	<p>Se false (scelta predefinita), il sistema evidenzia il numero minimo delle corrispondenze, a partire da quella più a sinistra. Ad esempio, se la politica EDM è configurata per abbinare 3 campi della colonna su 8 nell'indice, verranno evidenziate solo le prime 3 corrispondenze nell'istanza incidente.</p> <p>Se true, il sistema evidenzia tutte le corrispondenze presenti nella finestra di prossimità, compresi i duplicati. Ad esempio, se la politica è configurata per abbinare 3 corrispondenze su 8 e sono presenti 7 corrispondenze all'interno della finestra di prossimità, il sistema evidenzia tutte le 7 corrispondenze nell'istanza incidente.</p>

Impostazioni	Impostazione predefinita	Descrizione
EDM.MatchCountVariant	3	<p>Specifica come vengono conteggiate le corrispondenze.</p> <ul style="list-style-type: none"> ■ 1 - Conteggia il numero totale di set di token con corrispondenza. ■ 2 - Conteggia il numero di set di token univoci con corrispondenza. ■ 3 - Conteggia il numero di superset univoci di set di token. (predefinito) <p>Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.</p>
EDM.MaximumNumberOfMatchesToReturn	100	<p>Definisce un limite superiore per il numero di corrispondenze restituite da ciascuna ricerca indice RAM.</p> <p>Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.</p>
EDM.RunProximityLogic	true	<p>Se true, esegue il controllo di prossimità del token.</p> <p>Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.</p>
EDM.SimpleTextProximityRadius	35	<p>Numero di token valutati insieme quando il controllo di prossimità è attivato.</p> <p>Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.</p>
EDM.TokenVerifierEnabled	false	<p>Se attivata (true), il server convalida i token per le parole chiave in lingua cinese, giapponese e coreana (CJK).</p> <p>Per impostazione predefinita è disattivata (false).</p>

Impostazioni	Impostazione predefinita	Descrizione
EndpointCommunications. AllConnInboundDataThrottleInKBPS	0	<p>Se attivata, limita la velocità di trasferimento di tutto il traffico in entrata in kilobyte al secondo.</p> <p>Per impostazione predefinita è disattivata.</p> <p>La modifica a questa impostazione viene applicata a tutte le nuove connessioni. Le modifiche non hanno effetto sulle connessioni esistenti.</p>
EndpointCommunications. AllConnOutboundDataThrottleInKBPS	0	<p>Se attivata, limita la velocità di trasferimento di tutto il traffico in uscita in kilobyte al secondo.</p> <p>Per impostazione predefinita è disattivata.</p> <p>La modifica a questa impostazione viene applicata a tutte le nuove connessioni. Le modifiche non hanno effetto sulle connessioni esistenti.</p>

Impostazioni	Impostazione predefinita	Descrizione
EndpointCommunications. ApplicationHandshakeTimeoutInSeconds	60	<p>Il tempo massimo di attesa del server per ogni roundtrip durante le comunicazioni di handshake dell'applicazione prima di interrompere la connessione tra server e agente.</p> <p>Si applica alla durata del periodo tra il momento in cui l'agente accetta la connessione TCP e il momento in cui l'agente riceve il messaggio di handshake. Questa durata include handshake SSL e la ricezione da parte dell'agente delle intestazioni HTTP. Se il processo supera la durata specificata, la connessione si interrompe.</p> <p>La modifica a questa impostazione viene applicata a tutte le nuove connessioni. Le modifiche non hanno effetto sulle connessioni esistenti.</p>
EndpointCommunications.MaxActiveAgentsPerServer	90000	<p>Imposta il numero massimo di agenti associati a un determinato server in un qualsiasi momento.</p> <p>Questa impostazione viene implementata dopo il riavvio successivo di Endpoint Server.</p>
EndpointCommunications. MaxActiveAgentsPerServerGroup	150000	<p>Imposta il numero massimo di agenti che verranno associati a un determinato gruppo di server dietro lo stesso bilanciamento del carico in un qualsiasi momento. Usato per le dimensioni massime delle cache per le funzionalità endpoint interne.</p> <p>Questa impostazione viene implementata dopo il riavvio successivo di Endpoint Server.</p>

Impostazioni	Impostazione predefinita	Descrizione
EndpointCommunications.MaxConcurrentConnections	90000	<p>Imposta il numero massimo di connessioni simultanee consentite.</p> <p>La modifica a questa impostazione viene applicata a tutte le nuove connessioni. Le modifiche non hanno effetto sulle connessioni esistenti.</p>
EndpointCommunications.MaxConnectionLifetimeInSeconds	86400 (1 giorno)	<p>Imposta il tempo massimo consentito a una connessione per rimanere aperta. Non impostare le connessioni in modo tale che rimangano aperte per un periodo di tempo indefinito. Le connessioni con chiusura impostata garantiscono un aggiornamento frequente delle chiavi di sessione SSL aumentando così la sicurezza. Questo timeout si applica solo durante la fase di funzionamento normale della connessione, dopo le fasi di handshake SSL e di handshake dell'applicazione di una connessione.</p> <p>Questa impostazione viene implementata immediatamente in tutte le connessioni.</p>
EndpointCommunications.ShutdownTimeoutInMillis	5000 (5 secondi)	<p>Imposta il tempo massimo di attesa per la chiusura normale delle connessioni durante l'arresto prima di doverne forzare la chiusura.</p> <p>Questa impostazione viene implementata immediatamente in tutte le connessioni.</p>

Impostazioni	Impostazione predefinita	Descrizione
EndpointCommunications.SSLCipherSuites	TLS_RSA_WITH_AES_128_CBC_SHA	<p>Elenca le suite per la crittografia SSL consentite. Immettere più voci separate da virgole.</p> <p>La modifica a questa impostazione viene applicata a tutte le nuove connessioni. Le modifiche non hanno effetto sulle connessioni esistenti. È necessario riavviare Endpoint Server per implementare le modifiche. Vedere "Controlli server" a pagina 242.</p> <p>Se si utilizza la modalità FIPS 140-2 per la comunicazione tra Endpoint Server e i DLP Agent, non utilizzare la suite per crittografia Diffie-Hellman (DH). Le suite per crittografia combinate impediscono all'agente e all'Endpoint Server di comunicare.</p>
EndpointCommunications.SSLSessionCacheTimeoutInSeconds	86400	<p>Imposta la durata massima della voce sessione SSL nella cache di sessione dello SSL.</p> <p>L'impostazione predefinita corrisponde a un giorno. Questa impostazione viene implementata dopo il riavvio successivo di Endpoint Server.</p>
EndpointMessageStatistics.MaxFileDetectionCount	100	<p>Il numero massimo di volte in cui verrà eseguita la scansione di un file valido. Il file non deve causare un incidente. Se viene superato il numero massimo, viene generato un evento di sistema che consiglia di filtrare il file.</p>

Impostazioni	Impostazione predefinita	Descrizione
EndpointMessageStatistics.MaxFolderDetectionCount	1800	Il numero massimo di volte in cui verrà eseguita la scansione di una cartella valida. La cartella non deve causare un incidente. Se viene superato il numero massimo, viene generato un evento di sistema che consiglia di filtrare il file.
EndpointMessageStatistics.MaxMessageCount	2000	Il numero massimo di volte in cui verrà eseguita la scansione di un messaggio valido. Il messaggio non deve causare un incidente. Se viene superato il numero massimo, viene generato un evento di sistema che consiglia di filtrare il file.
EndpointMessageStatistics.MaxSetSize	3	L'elenco massimo degli host visualizzati da dove provengono file, cartelle e messaggi validi. Quando un evento di sistema per EndpointMessageStatistics. MaxFileDetectionCount, EndpointMessageStatistics. MaxFolderDetectionCount, o EndpointMessageStatistics. MaxMessageCount è generato, Symantec Data Loss Prevention elenca i computer host dove gli eventi di sistema sono stati generati. Questa impostazione limita il numero degli host visualizzati nell'elenco.
EndpointServer.Discover.ScanStatusBatchInterval	60000	L'intervallo di tempo in millisecondi in cui Endpoint Server accumula gli stati di scansione di Endpoint Discover prima di inviarli come batch a Endpoint Server.

Impostazioni	Impostazione predefinita	Descrizione
EndpointServer.Discover.ScanStatusBatchSize	1000	<p>Il numero degli stati di scansione accumulati dall'aggregatore prima di inviarli come batch a Enforce Server. Endpoint Server inoltra un batch di stati a Enforce Server quando il conteggio degli stati raggiunge il valore configurato.</p> <p>Il batch viene inoltrato a Enforce Server quando vengono raggiunte le soglie delle seguenti impostazioni:</p> <ul style="list-style-type: none"> ■ EndpointServer.Discover.ScanStatusBatchInterval ■ EndpointServer.Discover.ScanStatusBatchSize
EndpointServer.EndpointSystemEventQueueSize	20000	<p>Il numero massimo degli eventi di sistema che possono essere archiviati nella coda dell'agente endpoint da inviare a Endpoint Server. Se si interrompe la connessione al database o se altri avvenimenti provocano un numero elevato di eventi di sistema, tutti gli eventi di sistema supplementari che si verificano dopo il raggiungimento del numero massimo consentito vengono eliminati. Questo valore può essere regolato secondo i requisiti di memoria.</p>
EndpointServer.MaxPercentageMemToStoreEndpointFiles	60	<p>La quantità massima (in percentuale) di memoria da destinare all'archiviazione dei file di cache shadow.</p>
EndpointServer.MaxTimeToKeepEndpointFilesOpen	20000	<p>L'intervallo di tempo (in minuti) in cui il file endpoint viene tenuto aperto o la dimensione del file può superare l'impostazione <code>EndpointServer.MaxEndpointFileSize</code>, a seconda di quale evento si verifica per primo.</p>

Impostazioni	Impostazione predefinita	Descrizione
EndpointServer.MaxTimeToWaitForWriter	1000	Il tempo massimo (in millisecondi) di attesa dell'agente per collegarsi al server.
EndpointServer.NoOfRecievers	15	Il numero di ricevitori del file di cache shadow di endpoint.
EndpointServer.NoOfWriters	10	Il numero di utenti scrittura del file di cache shadow di endpoint.
FileReader.MaxFileSize	30M	La dimensione massima (in MB) di un messaggio da elaborare. I messaggi più grandi vengono troncati e ridotti a questa dimensione. Per elaborare file grandi di grandi dimensioni, accertarsi che questo valore sia uguale o maggiore del valore di ContentExtraction.MaxContentSize .
FileReader.MaxFileSystemCrawlerMemory	30M	La memoria massima assegnata al crawler del file system. Se questo valore è minore di <code>FileReader.MaxFileSize</code> , allora viene assegnato il maggiore tra i due valori.
FileReader.MaxReadGap	15	Il tempo in cui un processo secondario può raccogliere dati ma non leggere tutto prima di interrompere l'invio di heartbeat.
FileReader.ScheduledInterval	1000	L'intervallo di tempo (in millisecondi) tra i controlli della cartella di ricezione da parte del filereader. Ciò influisce solo sui canali Copia regola, Acquisizione del pacchetto e File system.

Impostazioni	Impostazione predefinita	Descrizione
FileReader.TempDirectory	Percorso a una directory sicura come specificato nel filereader <code>.temp.Attributo io.dir</code> nel <code>FileReader.properties</code>	Una directory sicura sul server di rilevamento in cui archiviare i file temporanei per il lettore di file.
FormRecognition.ALIGNMENT_COEFFICIENT	85.00	Una soglia su una scala da 0 a 100 che indica la corrispondenza tra un'immagine e la forma galleria indicizzata al fine di creare un incidente.
FormRecognition.CANONICAL_FORM_WIDTH	930	La larghezza in pixel a cui tutte le immagini vengono ridimensionate internamente per il riconoscimento della forma.
Icap.AllowHosts	qualsiasi	Il valore predefinito "qualsiasi" consente a tutti i sistemi di stabilire una connessione al server Network Prevent for Web sulla porta di servizio ICAP. Se si sostituisce "qualsiasi" con l'indirizzo IP o il nome di dominio completo (FQDN) di uno o più sistemi, limita le connessioni ICAP solo ai sistemi designati. Per designare più sistemi, separare gli indirizzi IP FQDN con delle virgole.
Icap.AllowStreaming	false	Se true, l'output ICAP viene trasmesso in streaming direttamente al proxy senza eseguire prima il buffering della richiesta ICAP.

Impostazioni	Impostazione predefinita	Descrizione
Icap.BindAddress	0.0.0.0	L'Indirizzo IP a cui si lega un listener del server Network Prevent for Web. Quando BindAddress è configurato, il server risponderà solo a una connessione a quell'indirizzo IP. Il valore predefinito di 0.0.0.0 è un carattere jolly che consente di ascoltare tutti gli indirizzi disponibili, compreso 127.0.0.1.
Icap.BufferSize	3K	La dimensione (in kilobyte) del buffer di memoria usato per lo streaming e la segmentazione della richiesta ICAP. Lo streaming può essere eseguito solo se la richiesta è superiore di FileReader.MaxFileSize e se la richiesta ha un'intestazione relativa alla lunghezza del contenuto.
Icap.DisableHealthCheck	false	Se true, disattiva l'autoverifica periodica ICAP. Se false, attiva l'autoverifica periodica ICAP. Questa impostazione è utile per il debug per rimuovere l'accumulo di file prodotto dalle richieste di autoverifica dai registri.
Icap.EnableIncidentSuppression	true	Attiva la cache di soppressione incidente per il traffico ICAP tablet Gmail.
Icap.EnableTrace	false	Se impostata su true, l'analisi di debug del protocollo è attivata quando una cartella viene specificata utilizzando l'impostazione Icap.TraceFolder.

Impostazioni	Impostazione predefinita	Descrizione
Icap.ExchangeActiveSyncCommandsToInspect	SendMail	Un elenco di comandi ActiveSync separati da virgole e con distinzione tra maiuscole e minuscole che deve essere inviato tramite rilevamento Symantec Data Loss Prevention. Se questo parametro viene lasciato vuoto, il supporto ActiveSync è disattivato. Se questo parametro viene impostato su "qualsiasi", tutti i comandi ActiveSync vengono ispezionati.
Icap.IncidentSuppressionCacheCleanupInterval	120000	L'intervallo di tempo in millisecondi in cui eseguire il thread di pulizia della cache di soppressione incidente.
Icap.IncidentSuppressionCacheTimeout	120000	Il tempo in millisecondi per invalidare la voce di cache di soppressione incidente.
Icap.LoadBalanceFactor	1	Il numero dei server proxy Web con cui Network Prevent for Webserver è in grado di comunicare. Ad esempio, se il server è configurato per comunicare con 3 proxy, impostare il valore <code>Icap.LoadBalanceFactor</code> su 3.
Icap.PoolFolder		Questo valore è necessario per pool ICAP.
Icap.TraceFolder		Il nome completo della cartella o della directory in cui sono memorizzati i dati della traccia di debug del protocollo quando l'impostazione <code>Icap.EnableTrace</code> è configurata su true. Per impostazione predefinita, il valore per questa impostazione viene lasciato vuoto.

Impostazioni	Impostazione predefinita	Descrizione
ImagePreclassifier.ENABLE_FORM_RECOGNITION_PRECLASSIFIER	true	Determina quali tipi di immagini sono elaborate per il riconoscimento moduli. Se true , Symantec Data Loss Prevention filtra le fotografie a colori, immagini come logo, firme e-mail e altre immagini che non sono caratteristiche dei moduli. Se false , Symantec Data Loss Prevention elabora tutte le immagini.
ImagePreclassifier.ENABLE_OCR_PRECLASSIFIER	true	Determina quali tipi di immagini sono elaborate per il riconoscimento ottico dei caratteri (OCR). Se true , Symantec Data Loss Prevention filtra le fotografie a colori, immagini come logo, firme e-mail e altre immagini che non includono testo significativo. Se false , Symantec Data Loss Prevention elabora tutte le immagini.
ImageRecognition.NUM_WORKER_THREADS	2	Il numero di thread nel pool usato dal processo di rilevamento del riconoscimento di immagini. Il valore per questa impostazione deve essere uguale a metà del numero dei core fisici nel sistema.
IncidentDetection.IncidentLimitResetTime	86400000	Specifica il periodo di tempo (in millisecondi) usato dall'impostazione IncidentDetection. MaxIncidentsPerPolicy . L'impostazione predefinita 86400000 corrisponde un giorno.

Impostazioni	Impostazione predefinita	Descrizione
IncidentDetection.MaxContentLength	2000000	Si applica solo alle regole di espressione regolare. In base al componente, solo il primo numero di caratteri MaxContentLength è sottoposto a scansione per le violazioni. Il valore predefinito (2.000.000) è equivalente a > 1000 pagine di testo tipico. Il limitatore esiste per impedire alle regole di espressione regolare di impiegare troppo tempo.
IncidentDetection.MaxIncidentsPerPolicy	10000	Definisce il numero massimo di incidenti individuati da una politica specifica su un monitoraggio particolare all'interno di un determinato periodo di tempo in IncidentDetection. IncidentTimeLimitResetTime. Il valore predefinito è 10.000 incidenti per politica per limite di tempo.
IncidentDetection.MessageWaitSevere	240	Il numero di minuti di attesa prima che un evento di sistema grave relativo ai tempi di attesa del messaggio venga inviato.
IncidentDetection.MessageWaitWarning	60	Il numero di minuti di attesa prima che un evento di sistema avviso relativo ai tempi di attesa del messaggio venga inviato.

Impostazioni	Impostazione predefinita	Descrizione
IncidentDetection.MinNormalizedSize	30	Questa impostazione si applica al rilevamento IDM. DEVE essere mantenuta sincronizzata all'impostazione corrispondente nel file Indexer.properties su Enforce Server (si applica all'indicizzazione). Il rilevamento derivativo si applica solo ai messaggi quando il contenuto normalizzato è superiore a questa impostazione. Se la dimensione del contenuto normalizzato è inferiore a quella di questa impostazione, il rilevamento IDM ha una corrispondenza binaria diretta.
IncidentDetection.patternConditionMaxViolations	100	Il numero massimo di corrispondenze segnalate da un server di rilevamento. Il server di rilevamento non segnala le corrispondenze superiori al valore del parametro IncidentDetection. patternConditionMaxViolations anche se presenti.

Impostazioni	Impostazione predefinita	Descrizione
IncidentDetection.StopCachingWhenMemoryLowerThan	400M	<p>Istruisce il rilevamento in modo che smetta di memorizzare il contenuto in formato token e crittografico nella cache tra le esecuzioni della regola se la memoria JVM disponibile scende al di sotto di questo valore (in megabyte). Impostare questo attributo su 0 consente di memorizzare nella cache indipendentemente dalla memoria disponibile e non è consigliata perché potrebbero verificarsi OutOfMemoryErrors.</p> <p>Impostando questo attributo a un valore vicino o superiore al valore dell'opzione -Xmx in BoxMonitor.FileReaderMemory, la memorizzazione nella cache verrà disattivata.</p> <p>Tenere presente che impostare un valore troppo basso può avere ripercussioni gravi sulle prestazioni.</p>
IncidentDetection.TrialMode	false	<p>Impedire alla modalità di prova di generare incidenti di prevenzione senza un'impostazione di prevenzione.</p> <p>Se true, gli incidenti SMTP derivanti dai canali Copia regola e Acquisizione del pacchetto vengono visualizzati come se fossero stati bloccati e gli incidenti HTTP derivanti dal canale Acquisizione del pacchetto vengono visualizzati come se fossero stati bloccati.</p>
IncidentWriter.BacklogInfo	1000	<p>Il numero di incidenti raccolti nel registro prima che venga generato un messaggio con informazioni sul numero di messaggi.</p>

Impostazioni	Impostazione predefinita	Descrizione
IncidentWriter.BacklogSevere	10000	Il numero di incidenti raccolti nel registro prima che venga generato un messaggio di livello grave sul numero di messaggi.
IncidentWriter.BacklogWarning	3000	Il numero di incidenti raccolti nel registro prima che venga generato un messaggio di livello avviso sul numero di messaggi.
IncidentWriter.ResolveIncidentDNSNames	false	Se true, solo i nomi host dei destinatari vengono individuati dall'IP.
IncidentWriter.ShouldEncryptContent	true	Se true, il monitoraggio crittograferà il corpo di ogni messaggio, il componente del messaggio e il componente compromesso prima della scrittura sul disco o dell'invio a Enforce.
Keyword.TokenVerifierEnabled	false	Per impostazione predefinita è disattivata (false). Se attivato (true), il server convalida i token per le parole chiave nelle lingue asiatiche (cinese, giapponese e coreano). Vedere "Attivazione e utilizzo della verifica dei token CJK per la corrispondenza di parole chiave sul server" a pagina 781.
L7.cleanHttpBody	true	Se true, i riferimenti di entità HTML vengono sostituiti dagli spazi.

Impostazioni	Impostazione predefinita	Descrizione
L7.DefaultBATV	Standard	<p>Questa impostazione determina lo schema di tag utilizzato da Network Prevent for Email per interpretare i tag BATV (Bounce Address Tag Validation) nell'intestazione MAIL DA di un messaggio. Se è impostata su "Standard" (valore predefinito), Network Prevent usa lo schema di tag descritto nella specifica BATV:</p> <p>http://tools.ietf.org/html/draft-levine-mass-batv-02</p> <p>Modificare l'impostazione su "Ironport" per attivare la compatibilità con l'implementazione di proxy di IronPort del tag BATV.</p>
L7.DefaultUrlEncodedCharset	UTF-8	<p>Definisce il set di caratteri predefinito che viene utilizzato nella decodifica dei parametri di ricerca o nel corpo con codifica URL in assenza delle informazioni sul set di caratteri dall'intestazione.</p>
L7.discardDuplicateMessages	true	<p>Se true, il monitoraggio ignora i messaggi duplicati basati sul messageId.</p>

Impostazioni	Impostazione predefinita	Descrizione
L7.ExtractBATV	true	<p>Se true (valore predefinito), Network Prevent for Email interpreta i tag BATV (Bounce Address Tag Validation) presenti nell'intestazione MAIL DA di un messaggio. Ciò consente a Network Prevent di includere un indirizzo significativo del mittente negli incidenti che sono generati dai messaggi con tag BATV. Se false, Network Prevent for Email non interpreta i tag BATV e un messaggio che contiene i tag BATV può generare un incidente con un indirizzo illeggibile del mittente.</p> <p>Vedere http://tools.ietf.org/html/draft-levine-mass-batv-02 per ulteriori informazioni sulla specifica BATV.</p>
L7.httpClientIdHeader	X-Forwarded-For	Il nome dell'intestazione dell'identificatore del mittente.
L7.MAX_NUM_HTTP_HEADERS	30	Se un messaggio HTTP contiene più righe di intestazione di quelle specificate, viene eliminato.
L7.maxWordLength	30	Lunghezza massima delle parole (in caratteri) consentita nell'estrazione delle stringhe UTCP.
L7.messageIDCacheCleanupInterval	600000	Periodo di tempo durante il quale il messageID rimane memorizzato nella cache. Il sistema non memorizzerà nella cache i messaggi duplicati durante questo periodo di tempo se l'impostazione L7.discardDuplicateMessages è impostata su true.

Impostazioni	Impostazione predefinita	Descrizione
L7.minSizeOfGetUrl	100	<p>La dimensione minima dell'URL GET da elaborare. Le azioni HTTP GET non vengono sottoposte a verifica da parte di Symantec Data Loss Prevention per le violazioni di politica se il numero dei byte nell'URL è inferiore al valore di questa impostazione. Ad esempio, con il valore predefinito 100, non viene eseguito alcun controllo di rilevazione quando un browser visualizza il sito web di Symantec all'indirizzo: http://www.symantec.com/index.jsp. Il motivo è che l'URL contiene solo 33 caratteri, ovvero un numero inferiore ai 100 caratteri minimi.</p> <p>Nota: Altri tipi di richiesta, ad esempio POST o PUT, non vengono interessati da L7.minSizeofGetURL. Affinché Symantec Data Loss Prevention ispezioni le azioni GET, l'impostazione L7.processGets deve essere impostata su true.</p>
L7.processGets	true	<p>Se true, le richieste GET vengono elaborate. Se false, le richieste GET non vengono elaborate. Tenere presente che questa impostazione interagisce con l'impostazione L7.minSizeofGetURL.</p>
Lexer.IncludePunctuation InWords	true	<p>Se true, durante il rilevamento sono considerati i caratteri di punteggiatura interni a un token.</p> <p>Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.</p>

Impostazioni	Impostazione predefinita	Descrizione
Lexer.MaximumNumber OfTokens	30000	Numero massimo dei token estratti da ogni componente messaggio per il rilevamento. Applicabile a tutte le tecnologie di rilevamento nelle quali l'applicazione di token è obbligatoria (EDM, DGM con profilo e criteri di sistema supportati da tali tecnologie). L'incremento del valore predefinito può determinare l'esaurimento della memoria e il riavvio del server di rilevamento. Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.
Lexer.Validate	true	Se true, esegue la convalida specifica per il criterio del sistema. Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.
MessageChain.ArchiveTimedOutStreams	false	Specifica se i messaggi devono essere archiviati nella cartella temporanea
MessageChain.CacheSize	8	Limita il numero dei messaggi che possono essere inseriti nella coda nelle catene di messaggi.
MessageChain.ContentDumpEnabled	false	Se impostato su true, ogni messaggio che entra nella catena di messaggi di rilevazione viene archiviato in \${SymantecDLP.temp.dir}/dump. Questa impostazione è pensata per la risoluzione di problemi e il debug.
MessageChain.MaximumComponentTime	60.000	L'intervallo di tempo (in millisecondi) consentito prima che qualsiasi componente della catena venga riavviato.

Impostazioni	Impostazione predefinita	Descrizione
MessageChain.MaximumFailureTime	360000	Numero di millisecondi che devono trascorrere prima che il file reader venga riavviato. Viene tenuto traccia di ciò una volta che l'errore della catena di messaggi viene rilevato e che la catena di messaggi stessa non è stata recuperata.
MessageChain.MaximumMessageTime	Varia	Questa impostazione varia tra 600.000 e 1.800.000 in base al tipo di server di rilevamento. L'intervallo di tempo massimo (in millisecondi) in cui un messaggio può rimanere in una catena di messaggi.
MessageChain.MemoryThrottlerReservedBytes	200.000.000	Numero di byte disponibili richiesti prima che un messaggio venga inviato tramite la catena di messaggi. Questa impostazione può evitare problemi di memoria insufficiente. Il valore predefinito è 200 MB. La limitazione può essere disattivata impostando questo valore su 0.
MessageChain.MinimumFailureTime	30000	Numero di millisecondi che devono trascorrere prima che il guasto di una catena di messaggi venga tracciato. Alla fine il guasto impone di riavviare la catena di messaggi o il file reader.

Impostazioni	Impostazione predefinita	Descrizione
MessageChain.NumChains	Varia	<p>Questo numero varia a seconda del tipo di server di rilevamento. Può essere 4 o 8.</p> <p>Numero di messaggi in parallelo che verranno elaborati dal file reader. L'impostazione di questo numero su un valore superiore a 8 (con le altre impostazioni predefinite) è sconsigliata. Un'impostazione più alta non incrementa sostanzialmente le prestazioni e comporta un rischio molto maggiore di esaurimento della memoria. L'impostazione su un valore inferiore a 8 (talvolta su 1) risulta utile per l'elaborazione di file di grandi dimensioni, ma può rallentare considerevolmente le prestazioni del sistema.</p>
MessageChain.StopProcessing WhenMemoryLowerThan	200M	<p>Istruisce il rilevamento in modo che interrompa il drill-down e l'elaborazione di file secondari se la memoria JVM disponibile scende al di sotto di questo valore. Impostando questo attributo su 0, l'elaborazione di file secondari verrà forzata, indipendentemente dalla memoria disponibile. Impostando questo attributo su un valore vicino o superiore al valore dell'opzione <code>-Xmx</code> in <code>BoxMonitor.FileReaderMemory</code>, l'elaborazione dei file secondari verrà disattivata correttamente.</p>

Impostazioni	Impostazione predefinita	Descrizione
OCR.ENABLE_AUTO_LANGUAGE_DETECTION	true	Se true , questa impostazione consente di estrarre il testo più rapidamente, identificando automaticamente la lingua o le lingue in un'immagine, anziché elaborando ogni lingua nella configurazione OCR. Se false , il motore OCR estrae il testo utilizzando ogni lingua nella configurazione OCR, rallentando l'estrazione del testo, ma migliorando la precisione.
OCR.ENABLE_SPELL_CHECK	true	Se true , questa impostazione consente di estrarre il testo in modo più accurato utilizzando dizionari ortografici interni al motore OCR. Se false , l'accuratezza del testo estratto potrebbe essere ridotta.
PacketCapture.DISCARD_HTTP_GET	true	Se true , elimina i flussi GET HTTP.
PacketCapture.DOES_DISCARD_TRIGGER_STREAM_DUMP	false	Se true , la prima volta che si riceve un messaggio di scarto viene creato il dump di un elenco di tcpstreams in un file di output nella directory del registro.
PacketCapture.ENDACE_BIN_PATH		Per consentire l'acquisizione del pacchetto tramite una scheda Endace, immettere il percorso per la directory Endace <code>/bin</code> . Tenere presente che le variabili di ambiente (ad esempio <code>%ENDACE_HOME%</code>) non possono essere utilizzate in questa impostazione. Ad esempio: <code>/usr/local/bin</code>

Impostazioni	Impostazione predefinita	Descrizione
PacketCapture.ENDACE_LIB_PATH		Per consentire l'acquisizione del pacchetto tramite una scheda Endace, immettere il percorso della directory Endace /lib . Tenere presente che le variabili di ambiente (ad esempio <code>%ENDACE_HOME%</code>) non possono essere utilizzate in questa impostazione. Ad esempio: <code>/usr/local/lib</code>
PacketCapture.ENDACE_XILINX_PATH		Per consentire l'acquisizione del pacchetto tramite una scheda Endace, immettere il percorso della directory Endace/xilinx. Tenere presente che le variabili di ambiente (ad esempio <code>%ENDACE_HOME%</code>) non possono essere utilizzate in questa impostazione. Ad esempio: <code>/usr/local/dag/xilinx</code>
PacketCapture.Filter	tcp ip proto 47 (vlan && (tcp ip proto 47))	Quando vengono impostati sul valore predefinito, tutti i pacchetti non TCP vengono esclusi e non inviati a Network Monitor. Il valore predefinito può essere ignorato utilizzando il formato di filtro tcpdump illustrato nel programma tcpdump. Questa impostazione consente agli specialisti di creare filtri più precisi (IP di origine e di destinazione per le porte indicate).
PacketCapture.INPUT_SOURCE_FILE	/dummy.dmp	Percorso e nome completo del file di entrata.
PacketCapture.IS_ARCHIVING_PACKETS	false	NON UTILIZZARE QUESTO CAMPO. Impostazione diagnostica che crea i dump di pacchetti acquisiti in packetcapture per il riutilizzo in un secondo momento. Questa funzionalità non è supportata e non presenta una verifica degli errori normale. Può provocare riavvii ripetuti su pcap.

Impostazioni	Impostazione predefinita	Descrizione
PacketCapture.IS_ENDACE_ENABLED	false	Per attivare l'acquisizione dei pacchetti tramite una scheda Endace, impostare questo valore su true.
PacketCapture.IS_FTP_RETR_ENABLED	false	Se true, FTP GETS e FTP PUTS vengono elaborati. Se false, vengono elaborati solo FTP PUTS.
PacketCapture.IS_INPUT_SOURCE_FILE	false	Se true, legge continuamente nei pacchetti da un file formattato tcpdump indicato in INPUT_SOURCE_FILE. Impostarlo su dag quando viene installata una scheda Endace.
PacketCapture.IS_NAPATECH_ENABLED	false	Per attivare l'acquisizione dei pacchetti tramite una scheda Napatech, impostare questo valore su true. L'impostazione predefinita è false.
PacketCapture.KERNEL_BUFFER_SIZE_I686	64M	Per le piattaforme Linux a 32 bit, questa impostazione specifica la quantità di memoria assegnata per eseguire il buffering dei pacchetti di rete. Specificare K per kilobyte o M per megabyte. Non specificare un valore superiore a 128M.
PacketCapture.KERNEL_BUFFER_SIZE_Win32	16M	Per le piattaforme Windows a 32 bit, questa impostazione specifica la quantità di memoria assegnata per eseguire il buffering dei pacchetti di rete. Specificare K per kilobyte o M per megabyte.
PacketCapture.KERNEL_BUFFER_SIZE_X64	64M	Per le piattaforme Windows a 64 bit, questa impostazione specifica la quantità di memoria assegnata per eseguire il buffering dei pacchetti di rete. Specificare K per kilobyte o M per megabyte.

Impostazioni	Impostazione predefinita	Descrizione
PacketCapture.KERNEL_BUFFER_SIZE_X86_64	64M	Per le piattaforme Linux a 64 bit, questa impostazione specifica la quantità di memoria assegnata per eseguire il buffering dei pacchetti di rete. Specificare K per kilobyte o M per megabyte. Non specificare un valore più grande di 64M.
PacketCapture.MAX_FILES_PER_DIRECTORY	30000	Una volta elaborato il numero specificato di flussi di file, viene creata una nuova directory.
PacketCapture.MBYTES_LEFT_TO_DISABLE_CAPTURE	1000	Se la quantità di spazio su disco (in MB) disponibile sull'unità drop_pcap scende al di sotto di questa specifica, l'acquisizione dei pacchetti viene sospesa. Ad esempio, se questo numero è 100, il pcap smetterà di scrivere i file drop_pcap quando sono disponibili meno di 100 MB sull'unità installata
PacketCapture.MBYTES_REQUIRED_TO_RESTART_CAPTURE	1500	La quantità di spazio su disco (in MB) necessaria sull'unità drop_pcap prima che l'acquisizione dei pacchetti riprenda dopo l'interruzione a causa della mancanza di spazio. Ad esempio, se questo valore è 150 e l'acquisizione dei pacchetti è sospesa, l'acquisizione dei pacchetti riprende quando sono disponibili più di 150 MB sull'unità drop_pcap.
PacketCapture.NAPATECH_TOOLS_PATH		Questa impostazione specifica la posizione della directory degli strumenti di Napatech. Questa directory non è impostata per impostazione predefinita. Se l'acquisizione dei pacchetti è attivata per Napatech, immettere il percorso qualificato della directory di installazione degli strumenti di Napatech.

Impostazioni	Impostazione predefinita	Descrizione
PacketCapture.NO_TRAFFIC_ALERT_PERIOD	86.400	Il tempo di aggiornamento (in secondi), tra nessun messaggio di avviso di traffico. Nessun evento di sistema di traffico viene creato per un dato protocollo in questo periodo di tempo. Ad esempio, se questo valore è impostato su 24*60*60 secondi, ogni giorno viene inviato un nuovo messaggio se non è presente traffico per un dato protocollo. Non confonderlo con il timeout del traffico per protocollo, che esprime il periodo di tempo senza traffico prima di inviare il primo avviso.
PacketCapture.NUMBER_BUFFER_POOL_PACKETS	600000	Il numero di buffer di pacchetto preassegnati di dimensioni standard utilizzati per eseguire il buffering e ordinare il traffico in entrata.
PacketCapture.NUMBER_JUMBO_POOL_PACKETS	1	Il numero di buffer di pacchetto preassegnati di grandi dimensioni utilizzati per eseguire il buffering e ordinare il traffico in entrata.
PacketCapture.NUMBER_SMALL_POOL_PACKETS	200000	Il numero di buffer di pacchetto preassegnati di piccole dimensioni utilizzati per eseguire il buffering e ordinare il traffico in entrata.
PacketCapture.RING_CAPTURE_LENGTH	1518	Controlla la quantità di dati pacchetto acquisiti. Il valore di default di 1518 è sufficiente per catturare le reti Ethernet ed Ethernet tipiche su VLAN con tag 802.1Q.

Impostazioni	Impostazione predefinita	Descrizione
PacketCapture.RING_DEVICE_MEM	67108864	<p>Questa impostazione è obsoleta. Utilizzare invece l'impostazione PacketCapture.KERNEL_BUFFER_SIZE_I686 (per le piattaforme Linux a 32 bit) o l'impostazione PacketCapture.KERNEL_BUFFER_SIZE_X86_64 (per le piattaforme Linux a 64 bit).</p> <p>Specifica la quantità di memoria (in byte) da assegnare ai pacchetti di buffer per ciascun dispositivo. (Il valore predefinito di 67108864 è equivalente a 64MB.)</p>
PacketCapture.SIZE_BUFFER_POOL_PACKETS	1540	La dimensione dei pacchetti di pool di buffer standard.
PacketCapture.SIZE_JUMBO_POOL_PACKETS	10000	La dimensione dei pacchetti di pool di buffer molto grandi.
PacketCapture.SIZE_SMALL_POOL_PACKETS	150	La dimensione dei pacchetti di pool di buffer piccoli.
PacketCapture.SPOOL_DIRECTORY		La directory in cui effettuare lo spooling dei flussi con molti pacchetti. Questa impostazione è definita dall'utente.
PacketCapture.STREAM_WRITE_TIMEOUT	5000	L'intervallo di tempo (in millisecondi) tra ogni conteggio (timeout di scrittura di StreamManager)

Impostazioni	Impostazione predefinita	Descrizione
RequestProcessor.AddDefaultHeader	true	Se vero, aggiunge un'intestazione predefinita a ogni e-mail elaborata (quando si lavora in modalità SMTP inline). L'intestazione predefinita è <code>RequestProcessor.DefaultHeader</code> . Questa intestazione viene aggiunta a tutti i messaggi che passano attraverso il sistema, ovvero, se viene reindirizzato, se viene aggiunta un'altra intestazione, se il messaggio non presenta violazioni della politica, verrà aggiunta tale intestazione.
RequestProcessor.AddHeaderOnMessageTimeout	false	Il valore predefinito imposta il sistema per continuare a inviare i messaggi se c'è un timeout del messaggio. Se impostato su true , l'X-Header "X-Symantec-DLP: Message timed out (potential Enforce System event 1213)" viene inserito nel messaggio e-mail. L'MTA downstream utilizza queste informazioni di intestazione per gestire il messaggio, e il messaggio del registro mostra "Passed message through due to timeout, with added timeout header".
RequestProcessor.AllowExtensions	8BITMIME VRFY DSN HELP PIPELINING SIZE ENHANCEDSTATUSCODES STARTTLS	Questa impostazione elenca le estensioni del protocollo SMTP che Network Prevent for Email può utilizzare per comunicare con gli altri MTA.

Impostazioni	Impostazione predefinita	Descrizione
RequestProcessor.AllowHosts	qualsiasi	Il valore predefinito “qualsiasi” consente a tutti i sistemi di stabilire una connessione al server Network Prevent for Email sulla porta di servizio SMTP. Se si sostituisce “qualsiasi” con l'indirizzo IP o il nome di dominio completo (FQDN) di uno o più sistemi, limita le connessioni SMTP solo ai sistemi designati. Per designare i sistemi multipli, separare gli indirizzi con virgole. Utilizzare solo una virgola per separare gli indirizzi; non inserire spazi tra gli indirizzi.
RequestProcessor.AllowUnauthenticatedConnections	false	Il valore di default fa in modo che gli MTA debbano eseguire l'autenticazione con Network Prevent for Email per la comunicazione TLS.
RequestProcessor.Backlog	12	Il backlog specificato dal processore richiesta per il listener del socket del server.
RequestProcessor.BindAddress	0.0.0.0	L'Indirizzo IP a cui si lega un listener del server Network Prevent for Email. Quando BindAddress è configurato, il server risponderà solo a una connessione a quell'indirizzo IP. Il valore predefinito di 0.0.0.0 è un carattere jolly che consente di ascoltare tutti gli indirizzi disponibili, compreso 127.0.0.1.

Impostazioni	Impostazione predefinita	Descrizione
RequestProcessor.BlockStatusCodeOverride	5.7.1	<p>Consente di forzare il codice di stato ESMTP inviato all'MTA upstream durante l'esecuzione di una regola di risposta di blocco.</p> <p>I valori accettati sono 5.7.0 e 5.7.1. Se vengono immessi altri valori, questa impostazione eseguirà il fallback al valore predefinito di 5.7.1.</p> <p>L'utilizzo del valore 5.7.0 (con stato di sicurezza altro o non definito) è preferito quando il server di rilevamento interagisce con l'e-mail Office365, perché il valore 5.7.1 fornisce un contesto sbagliato per il caso di uso Office365.</p>
RequestProcessor.CacheCleanupInterval	120000	Specifica l'intervallo dopo il quale le risposte memorizzate nella cache vengono eliminate. Le unità sono in millisecondi.
RequestProcessor.CachedMessageTimeout	120000	Specifica il periodo di tempo dopo la generazione in cui una data risposta presente nella cache venga eliminata da essa. Le unità sono in millisecondi.
RequestProcessor.CacheEnabled	false	Consente di memorizzare nella cache le risposte dei messaggi SMTP duplicati. La cache è stata aggiunta nell'ambito della soluzione cloud per supportare la suddivisione della busta.

Impostazioni	Impostazione predefinita	Descrizione
RequestProcessor.DefaultCommandTimeout	300	Specifica il numero di secondi in cui Network Prevent for Email aspetta una risposta ad un comando SMTP prima di chiudere le connessioni agli MTA upstream e downstream. Il valore predefinito è 300 secondi. Questa impostazione non si applica al comando "." (la fine di un comando DATA). Non modificare il valore predefinito senza consultare prima il supporto di Symantec.
RequestProcessor.DefaultPassHeader	X-CFilter-Loop: Reflected	Si tratta dell' intestazione predefinita che verrà aggiunta se RequestProcessor.AddDefaultPassHeader è impostato su true, quando si lavora in modalità SMTP inline. Deve avere un formato di intestazione valido; si consiglia l' intestazione in formato X.
RequestProcessor.DotCommandTimeout	600	Specifica il numero di secondi in cui Network Prevent for Email aspetta una risposta al comando "." (la fine di un comando DATA) prima di chiudere le connessioni con gli MTA upstream e downstream. Il valore predefinito è 600 secondi. Non modificare il valore predefinito senza consultare prima il supporto di Symantec.
RequestProcessor.ForwardConnectionTimeout	20000	Il valore di timeout da utilizzare quando si esegue l' inoltrato a un MTA.
RequestProcessor.KeyManagementAlgorithm	SunX509	L' algoritmo della gestione delle chiavi utilizzato nella comunicazione TLS.
RequestProcessor.MaxLineSize	1048576	La dimensione massima (in byte) delle righe di dati attese da un MTA esterno. Se le righe di dati sono più grandi, vengono ridotte a questa dimensione.

Impostazioni	Impostazione predefinita	Descrizione
RequestProcessor.Mode	ESMTP	Specifica la modalità di protocollo da utilizzare (SMTP o ESMTP).
RequestProcessor.MTAResubmitPort	10026	Questo è il numero di porta utilizzato dal processore richiesta nell'MTA per inviare nuovamente il messaggio SMTP.
RequestProcessor.NumberOfDNSAttempts	4	Il numero massimo di query DNS che Network Prevent for Email esegue quando tenta di ottenere i record di scambio di posta (MX) per un dominio. Network Prevent for Email utilizza questa impostazione solo se sono state attivate le ricerche di record MX.
RequestProcessor.RPLTimeout	360000	Tempo massimo in millisecondi consentito per l'elaborazione dei messaggi di posta elettronica da parte di un server Prevent. Tutti i messaggi di posta elettronica non elaborati durante questo intervallo di tempo vengono passati dal server.
RequestProcessor.ServerSocketPort	10025	Il numero di porta che il monitor SMTP deve utilizzare per ascoltare le connessioni provenienti dagli MTA.
RequestProcessor.TagHighestSeverity	false	Quando impostato su true, al messaggio viene aggiunta un'ulteriore intestazione e-mail che indica la gravità più alta di tutte le politiche violate. Ad esempio, se l'e-mail viola una politica con gravità HIGH (alta) e una politica con gravità LOW (bassa), visualizzerà: X-DLP-MAX-Severity:HIGH.

Impostazioni	Impostazione predefinita	Descrizione
RequestProcessor.TagPolicyCount	false	Quando impostato su true, al messaggio viene aggiunta un'ulteriore intestazione e-mail che indica il numero totale di politiche violate. Ad esempio, se il messaggio viola 3 politiche viene aggiunta l'intestazione X-DLP-Policy-Count: 3.
RequestProcessor.TagScore	false	Quando impostato su true, al messaggio viene aggiunta un'ulteriore intestazione e-mail che indica il numero totale di politiche violate dal messaggio. I punteggi sono calcolati utilizzando la formula: Alta=4, Media=3, Bassa=2 e Informazioni=1. Ad esempio, se un messaggio viola tre politiche, una con gravità media e due con gravità bassa viene aggiunta l'intestazione X-DLP-Score: 7.
RequestProcessor.TrustManagementAlgorithm	PKIX	L'algoritmo della gestione dell'attendibilità che Network Prevent for Email utilizza quando convalida i certificati per la comunicazione TLS. È possibile specificare facoltativamente un algoritmo integrato del gestore dell'attendibilità Java (ad esempio SunX509 o SunPKIX) o un algoritmo personalizzato appositamente sviluppato.
RequestProcessorListener.ServerSocketPort	12355	La porta TCP locale che FileReader utilizzerà per ascoltare le connessioni provenienti da RequestProcessor o su un server Network Prevent.

Impostazioni	Impostazione predefinita	Descrizione
ServerCommunicator.CONNECT_DELAY_POST_WAKEUP_OR_POST_VPN_SECONDS	60	Il tempo di ritardo (in secondi) dopo il quale un server di rilevamento che torna online tenta di riconnettersi all'Enforce Server. Il valore predefinito è 60 secondi. La gamma per questa impostazione è di 30 - 600 secondi.
SocketCommunication.BufferSize	8K	La dimensione del buffer che Network Prevent for Web utilizza per elaborare le richieste ICAP. Aumentare il valore predefinito solo se è necessario elaborare le richieste ICAP superiori a 8K. Determinate caratteristiche, ad esempio l'autenticazione di Active Directory, possono richiedere un aumento delle dimensioni del buffer.
UnicodeNormalizer.AsianCharRanges	predefinito	Può essere utilizzato per sovrascrivere la definizione predefinita dei caratteri che il motore di rilevamento considera asiatici. Deve essere default o un elenco di intervalli separati da virgole, ad esempio: 11A80-11F9,3200-321E
UnicodeNormalizer.Enabled	attivato	Può essere utilizzato per disattivare la normalizzazione Unicode. Immettere disattivato per disattivare.
UnicodeNormalizer.NewlineEliminationEnabled	attivato	Può essere utilizzato per disattivare l'eliminazione della nuova riga per lingue asiatiche. Immettere disattivato per disattivare.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.

Vedere ["Informazioni sulla schermata Panoramica"](#) a pagina 273.

Vedere ["Schermata Dettagli server/rilevatore"](#) a pagina 277.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Vedere ["Controlli server"](#) a pagina 242.

Impostazioni rilevatore avanzate

Fare clic su **Impostazioni rilevatore** nella schermata **Sistema > Server e rilevatori > Panoramica > Dettagli server/rilevatore** del rilevatore per modificare le impostazioni in tale server.

Prestare attenzione quando si modificano tali impostazioni in un rivelatore. Contattare il supporto Symantec prima di modificare qualsiasi impostazione nella schermata. Le modifiche a queste impostazioni solitamente non hanno effetto fino al riavvio del rilevatore.

Non è possibile modificare le impostazioni per Enforce Server dalla schermata **Dettagli server/rilevatore**. Nella schermata **Dettagli server/rilevatore - Impostazioni avanzate** vengono visualizzati solo server di rilevazione e rilevatori.

Tabella 13-9 Impostazioni avanzate rilevatore

Impostazione	Impostazione predefinita	Descrizione
ContentExtraction.EnableMetaData	off	Consente il rilevamento sui metadati del file. Se l'impostazione è attiva , è possibile rilevare i metadati per file Microsoft Office e PDF. Per i file Microsoft Office, sono supportati i metadati OLE, i quali includono i campi Titolo, Oggetto, Autore e Parole chiave. Per i file PDF, solo i metadati del dizionario informazioni documento sono supportati, i quali includono campi come Autore, Titolo, Oggetto, Creazione e Date di aggiornamento. Il contenuto Extensible Metadata Platform (XMP) non è rilevato. Tenere presente che l'attivazione di questa opzione di rilevamento metadati può generare falsi positivi.
ContentExtraction.MarkupAsText	off	Consente di ignorare l'estrazione di contenuti per file con estensione XML o HTML. Dovrebbe essere utilizzato in casi come pagine Web contenenti dati nel blocco intestazione o script. Il valore predefinito è Off.

Impostazione	Impostazione predefinita	Descrizione
ContentExtraction.TrackedChanges	off	<p>Consente il rilevamento del contenuto modificato nel tempo (contenuto Revisioni) nei documenti di Microsoft Office.</p> <p>Nota: L'utilizzo dell'opzione precedente potrebbe ridurre il tasso di accuratezza per identificatori dati e IDM. Il valore predefinito è impostato su Off (non consentire).</p> <p>Per indicizzare il contenuto modificato con il passare del tempo, impostare ContentExtraction.TrackedChanges=on nel file \Protect\config\Indexer.properties. Il valore predefinito e l'impostazione consigliata è ContentExtraction.TrackedChanges=off.</p>
DDM.MaxBinMatchSize	30.000.000	<p>La dimensione massima (in byte) utilizzata per generare l'hash MD5 per una corrispondenza binaria esatta in un IDM. Questa impostazione non dovrebbe essere modificata. Per consentire il corretto funzionamento di IDM, devono essere rispettate le seguenti condizioni:</p> <ul style="list-style-type: none"> ■ Questa impostazione deve essere esattamente identica all'impostazione max_bin_match_size su Enforce Server nel file indexer.properties. ■ Questa impostazione deve essere inferiore o uguale al valore FileReader.FileMaxSize. ■ Questa impostazione deve essere inferiore o uguale al valore ContentExtraction.MaxContentSize su Enforce Server nel file indexer.properties. <p>Nota: La modifica del primo o terzo elemento nell'elenco richiede la reindicizzazione di tutti i file IDM.</p>
Detection.EncodingGuessingDefaultEncoding	ISO-8859-1	Specifica la codifica di backup presupposta per un flusso di byte.
Detection.EncodingGuessingEnabled	on	Designa se è necessario identificare la codifica di flussi di byte sconosciuti.
Detection.EncodingGuessingMinimumConfidence	50	Specifica il livello di sicurezza richiesto per l'ipotesi di codifica dei flussi di byte sconosciuti.

Impostazione	Impostazione predefinita	Descrizione
DI.MaxViolations	100	Specifica il numero massimo di violazioni consentite con gli identificatori di dati.
EDM.MatchCountVariant	3	<p>Specifica come vengono conteggiate le corrispondenze.</p> <ul style="list-style-type: none"> ■ 1 - Conteggia il numero totale di set di token con corrispondenza. ■ 2 - Conteggia il numero di set di token univoci con corrispondenza. ■ 3 - Conteggia il numero di superset univoci di set di token. (predefinito) <p>Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.</p>
EDM.MaximumNumberOfMatchesToReturn	100	<p>Definisce un limite superiore per il numero di corrispondenze restituite da ciascuna ricerca indice RAM.</p> <p>Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.</p>
EDM.SimpleTextProximityRadius	35	<p>Numero di token valutati insieme quando il controllo di prossimità è attivato.</p> <p>Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.</p>
EDM.TokenVerifierEnabled	false	<p>Se attivata (true), il server convalida i token per le parole chiave in lingua cinese, giapponese e coreana (CJK).</p> <p>Per impostazione predefinita è disattivata (false).</p>
IncidentDetection.MaxContentLength	2000000	<p>Si applica solo alle regole di espressione regolare. In base al componente, solo il primo numero di caratteri MaxContentLength è sottoposto a scansione per le violazioni. Il valore predefinito (2.000.000) è equivalente a > 1000 pagine di testo tipico. Il limitatore esiste per impedire alle regole di espressione regolare di impiegare troppo tempo.</p>

Impostazione	Impostazione predefinita	Descrizione
IncidentDetection.MinNormalizedSize	30	Questa impostazione si applica al rilevamento IDM. Deve essere mantenuta sincronizzata all'impostazione corrispondente nel file <code>Indexer.properties</code> su Enforce Server (si applica all'indicizzazione). Il rilevamento derivativo si applica ai messaggi solo quando il contenuto normalizzato è maggiore di questa impostazione. Se la dimensione del contenuto normalizzato è inferiore a quella di questa impostazione, il rilevamento IDM ha una corrispondenza binaria diretta.
IncidentDetection.patternConditionMaxViolations	100	Il numero massimo di corrispondenze segnalate da un rilevatore. Il rilevatore non segnala le corrispondenze superiori al valore del parametro 'IncidentDetection.patternConditionMaxViolations', anche se presenti.
Keyword.TokenVerifierEnabled	false	Per impostazione predefinita è disattivata (false). Se attivato (true), il server convalida i token per le parole chiave nelle lingue asiatiche (cinese, giapponese e coreano). Vedere "Attivazione e utilizzo della verifica dei token CJK per la corrispondenza di parole chiave sul server" a pagina 781.
Lexer.IncludePunctuation InWords	true	Se true, durante il rilevamento sono considerati i caratteri di punteggiatura interni a un token. Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.
Lexer.MaximumNumber OfTokens	12000	Numero massimo dei token estratti da ogni componente messaggio per il rilevamento. Applicabile a tutte le tecnologie di rilevamento nelle quali l'applicazione di token è obbligatoria (EDM, DGM con profilo e criteri di sistema supportati da tali tecnologie). L'incremento del valore predefinito può determinare l'esaurimento della memoria e il riavvio del rilevatore. Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.

Impostazione	Impostazione predefinita	Descrizione
Lexer.Validate	true	Se true, esegue la convalida specifica per il criterio del sistema. Vedere " Configurazione di impostazioni avanzate per i criteri EDM " a pagina 509.
UnicodeNormalizer.AsianCharRanges	default	Può essere utilizzato per sovrascrivere la definizione predefinita dei caratteri che il motore di rilevamento considera asiatici. Deve essere default o un elenco di intervalli separati da virgole, ad esempio: 11A80-11F9,3200-321E
UnicodeNormalizer.Enabled	on	Può essere utilizzato per disattivare la normalizzazione Unicode. Immettere Off per disattivare.
UnicodeNormalizer.NewlineEliminationEnabled	on	Può essere utilizzato per disattivare l'eliminazione della nuova riga per lingue asiatiche. Immettere disattivato per disattivare.

Informazioni sull'utilizzo dei bilanciamenti del carico in una distribuzione endpoint

È possibile utilizzare un bilanciamento del carico per gestire più Endpoint Server o un pool di server. L'aggiunta di Endpoint Server a un pool di server con bilanciamento del carico consente a Symantec Data Loss Prevention di utilizzare una larghezza di banda inferiore e, al tempo stesso, gestire più agenti. Quando si configura un pool di server per gestire Endpoint Server e agenti, le impostazioni predefinite di Symantec Data Loss Prevention consentono la comunicazione tra server e agenti. Tuttavia esistono numerose impostazioni di bilanciamento del carico che possono influenzare la comunicazione di Endpoint Server e agenti. È possibile che sia necessario apportare modifiche alle impostazioni avanzate di agenti e server se il bilanciamento del carico utilizzato non usa le impostazioni predefinite.

Generalmente ai bilanciamenti del carico devono essere applicate le impostazioni seguenti per funzionare al meglio con Symantec Data Loss Prevention:

- Velocità effettiva di 1 Gbps
- Persistenza IP di origine. Imposta il tempo di persistenza in modo che sia maggiore del periodo di polling dell'agente.
- Periodo di timeout della sessione SSL di 24 ore

Gli Endpoint Server comunicano nel modo più efficiente con gli agenti quando il bilanciamento del carico è configurato per l'utilizzo della persistenza dell'IP di origine. (Questo nome di protocollo può variare a seconda delle marche del bilanciamento del carico.) L'utilizzo della persistenza dell'IP di origine in un'implementazione Symantec Data Loss Prevention garantisce che se un agente viene riavviato sulla stessa rete, si riconnette allo stesso Endpoint Server, indipendentemente dallo stato della sessione SSL. Inoltre, la persistenza dell'IP di origine utilizza meno larghezza di banda durante l'handshake SSL tra agenti e Endpoint Server. Questo protocollo consente inoltre di mantenere la coerenza della cache evento/attributo.

Per gli agenti che si connettono a Endpoint Server mediante proxy o NAT, l'affinità del server della sessione SSL è l'impostazione di bilanciamento del carico ottimale. Tuttavia, se questa impostazione viene utilizzata e l'agente viene riavviato o se l'identità della sessione memorizzata nella cache SSL viene eliminata, viene negoziata una nuova sessione SSL. La negoziazione di una nuova sessione SSL può far sì che l'agente si connetta a un monitor diverso con maggiore frequenza, il che potrebbe interferire con gli aggiornamenti dello stato dell'agente su Enforce Server.

Esaminare le impostazioni di connessione dell'agente se le impostazioni di connessione inattiva del bilanciamento del carico non sono quelle predefinite. L'impostazione di connessione inattiva del bilanciamento del carico può inoltre essere denominata intervallo di timeout di connessione, connessione inattiva pulita e così via a seconda del marchio del bilanciamento del carico.

È possibile valutare le impostazioni di Symantec Data Loss Prevention e di bilanciamento del carico nei due scenari seguenti:

- Impostazioni DLP predefinite. [Tabella 13-10](#)
- Impostazioni DLP non predefinite. [Tabella 13-11](#)

Nota: contattare il supporto Symantec prima di modificare le impostazioni avanzate predefinite di agenti e server.

Tabella 13-10 Scenario delle impostazioni di Symantec Data Loss Prevention predefinite

Descrizione	Risoluzione
A partire dalla versione 12.5, Symantec Data Loss Prevention utilizza connessioni non persistenti per impostazione predefinita. L'utilizzo di connessioni non persistenti comporta che gli Endpoint Server interrompano le connessioni con gli agenti dopo che questi ultimi sono rimasti inattivi per 30 secondi.	<p>Esaminare come il timeout di inattività dell'agente coincide con l'impostazione di connessione inattiva interrotta del bilanciamento del carico. Se il bilanciamento del carico è configurato in modo da interrompere le connessioni inattive dopo meno di 30 secondi, gli agenti vengono disconnessi prematuramente dagli Endpoint Server.</p> <p>Per risolvere il problema, effettuare una delle seguenti operazioni:</p> <ul style="list-style-type: none"> ■ Modificare l'impostazione di timeout di inattività dell'agente (EndpointCommunications.IDLE_TIMEOUT_IN_SECONDS.int) e specificare un valore inferiore all'impostazione di connessione inattiva interrotta del bilanciamento del carico. ■ Aumentare l'impostazione di heartbeat dell'agente (EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int) in modo che sia inferiore all'impostazione di connessione inattiva interrotta del bilanciamento del carico. L'utente deve inoltre aumentare l'impostazione di timeout in assenza di traffico (CommLayer.NO_TRAFFIC_TIMEOUT_IN_SECONDS.int) e specificare un valore superiore all'impostazione di heartbeat dell'agente.

Tabella 13-11 Scenario delle impostazioni di Symantec Data Loss Prevention non predefinite

Descrizione	Risoluzione
Considerare come le modifiche delle impostazioni di Symantec Data Loss Prevention predefinite influenzano il modo in cui il bilanciamento del carico gestisce le connessioni inattive e persistenti dell'agente. Ad esempio, se si modifica l'impostazione di timeout di inattività e si specifica 0 per creare una connessione persistente e si lascia l'impostazione di heartbeat predefinita dell'agente (270 secondi), è necessario considerare l'impostazione di connessione inattiva del bilanciamento del carico. Se l'impostazione di connessione inattiva del bilanciamento del carico è inferiore a 270 secondi, gli agenti vengono disconnessi prematuramente dagli Endpoint Server.	<p>Per risolvere il problema, effettuare una delle seguenti operazioni:</p> <ul style="list-style-type: none"> ■ Modificare l'heartbeat dell'agente (EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int) e le impostazioni di timeout in assenza di traffico (CommLayer.NO_TRAFFIC_TIMEOUT_IN_SECONDS.int) e specificare un valore inferiore all'impostazione di connessione inattiva del bilanciamento del carico. ■ Verificare che l'impostazione di timeout in assenza di traffico sia superiore all'impostazione di heartbeat.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.

Gestione di file di registro

Il capitolo contiene i seguenti argomenti:

- [Informazioni sui file di registro](#)
- [Schermata per la raccolta e la configurazione di registri](#)
- [Configurazione del comportamento di registrazione di un server](#)
- [Raccolta dei registri e dei file di configurazione del server](#)
- [Informazioni sui codici di evento dei registri](#)

Informazioni sui file di registro

Symantec Data Loss Prevention fornisce vari file di registro differenti che registrano informazioni sul comportamento del software. I file di registro rientrano in queste categorie:

- I file di registro operativi registrano informazioni dettagliate sulle attività che il software esegue e sugli errori che si verificano durante l'esecuzione delle stesse. È possibile usare il contenuto dei file di registro operativi per verificare che il software funziona come previsto. È anche possibile usare questi file per risolvere eventuali problemi di compatibilità tra il software e gli altri componenti del sistema.
Ad esempio, è possibile utilizzare i file di registro operativi per verificare che un server Network Prevent for Email comunica con un MTA specifico sulla rete.
Vedere ["File di registro operativi"](#) a pagina 336.
- I file di registro di debug registrano dettagli tecnici elaborati riguardanti i singoli processi o componenti software che costituiscono Symantec Data Loss Prevention. Il contenuto dei file di registro di debug non è inteso per l'uso nella diagnosi degli errori di configurazione del sistema o nella verifica della funzionalità del software. Non è necessario esaminare tali file per amministrare o verificare un'installazione di Symantec Data Loss Prevention. Tuttavia, il supporto Symantec può richiedere i file di registro di debug per risolvere un problema segnalato. Per impostazione predefinita, alcuni file di registro di debug non

vengono creati. Il supporto Symantec può spiegare come configurare il software per creare il file, se necessario.

Vedere ["File di registro di debug"](#) a pagina 339.

- I file di registro di installazione registrano informazioni sulle attività di installazione di Symantec Data Loss Prevention eseguite su un determinato computer. È possibile utilizzare questi file di registro per verificare un'installazione o correggere errori di installazione. I file di registro di installazione si trovano nelle seguenti posizioni:
 - Il registro di installazione di Symantec Data Loss Prevention si trova in
`installdir\SymantecDLP\.install4j\installation.log`.
 - Il registro di installazione per Oracle si trova in
`installdir\oracle_home\admin\protect\`.

Per ulteriori informazioni, consultare il *Manuale di installazione di Symantec Data Loss Prevention*.

File di registro operativi

Enforce Server e i server di rilevamento memorizzano file di registro operativi nella directory `c:\ProgramData\Symantec\Data Loss Prevention\<Enforce Server o Detection Server>\15.1\Protect\logs\` nelle installazioni Windows e nella directory `/var/log/Symantec/DataLossPrevention/<Enforce Server o Detection Server>/15.1/` nelle installazioni Linux. Un numero alla fine del nome di file di registro indica il totale (indicato come 0 in [Tabella 14-1](#)).

[Tabella 14-1](#) elenca e descrive i file di registro operativi di Symantec Data Loss Prevention.

Tabella 14-1 File di registro operativi

Nome di file di registro	Descrizione	Server
agentmanagement_webservices_access_0.log	Registra i tentativi di accesso riusciti e falliti al servizio Web API Gestione agente.	Enforce Server
agentmanagement_webservices_soap_0.log	Registra l'intera richiesta SOAP e la risposta per la maggior parte delle richieste al servizio Web API Gestione agente.	Enforce Server

Nome di file di registro	Descrizione	Server
boxmonitor_operational_0.log	<p>Il processo BoxMonitor sorveglia i processi del server di rilevamento che riguardano quel particolare tipo di server.</p> <p>Ad esempio, i processi eseguiti su Network Monitor sono file reader e acquisizione del pacchetto.</p> <p>Il file di registro di BoxMonitor è in genere molto piccolo e mostra come vengono eseguiti i processi dell'applicazione.</p>	Tutti i server di rilevamento
detection_operational_0.log	Il file di registro dell'operazione di rilevamento fornisce dettagli sulla configurazione del server di rilevamento e se sta funzionando correttamente.	Tutti i server di rilevamento
detection_operational_trace_0.log	<p>Il file di registro delle tracce di rilevamento fornisce dettagli su ogni messaggio elaborato dal server di rilevamento. Il file di registro include le seguenti informazioni:</p> <ul style="list-style-type: none"> ■ Le politiche applicate al messaggio ■ Le regole di politiche corrispondenti nel messaggio ■ Il numero di incidenti che il messaggio ha generato. 	Tutti i server di rilevamento
machinelearning_training_operational_0.log	Questo registro registra informazioni su attività, registri e file di configurazione richiamati all'avvio del processo di training VML.	Enforce Server
manager_operational_0.log.	Registra le informazioni sul processo di gestione di Symantec Data Loss Prevention, che implementa l'interfaccia utente della console di amministrazione di Enforce Server.	Enforce Server

Nome di file di registro	Descrizione	Server
monitorcontroller_operational_0.log	Registra un registro dettagliato delle connessioni tra Enforce Server e tutti i server di rilevamento. Fornisce dettagli sulle informazioni scambiate tra questi server, ad esempio se le politiche sono state distribuite o meno ai server di rilevazione.	Enforce Server
SmtpPrevent_operational0.log	Questo file di registro operativo è relativo solo a SMTP Prevent. È il registro primario per il rilevamento dello stato e dell'attività di un sistema Network Prevent for Email. Esaminare questo file per informazioni sulla comunicazione tra i MTA e il server di rilevamento.	Server di rilevamento di SMTP Prevent
WebPrevent_Access0.log	Questo file di registro di accesso contiene le informazioni sulle richieste elaborate dai server di rilevamento di Network Prevent for Web. È simile ai registri di accesso Web per un proxy server.	<ul style="list-style-type: none"> Server di rilevamento di Network Prevent for Web
WebPrevent_Operational0.log	Questo file di registro operativo informa sulla condizione operativa di Network Prevent for Web, ad esempio se è attivo o meno, e sulla gestione delle connessioni.	<ul style="list-style-type: none"> Server di rilevamento di Network Prevent for Web
webservices_access_0.log	Questo file di registro registra i tentativi di accesso riusciti e falliti al servizio Web Reporting incidente.	Enforce Server

Nome di file di registro	Descrizione	Server
webservices_soap_0.log	Contiene l'intera richiesta SOAP e la risposta per la maggior parte delle richieste al servizio Web API Reporting incidente. Questo registro registra tutte le richieste e le risposte salvo le risposte alle richieste binarie di incidenti. Per impostazione predefinita, questo file di registro non viene creato. Per ulteriori informazioni consultare la <i>Guida degli sviluppatori dell'API Reporting incidente di Symantec Data Loss Prevention</i> .	Enforce Server

Vedere ["File di registro operativi e codici di evento di Network Prevent for Web"](#) a pagina 355.

Vedere ["Campi e file del registro di accesso di Network Prevent for Web"](#) a pagina 357.

Vedere ["Livelli di registrazione di Network Prevent for Email"](#) a pagina 359.

Vedere ["Codici dei registri operativi di Network Prevent for Email"](#) a pagina 360.

Vedere ["Risposte e codici generati da Network Prevent for Email"](#) a pagina 364.

File di registro di debug

Enforce Server e i server di rilevamento memorizzano i file di registro di debug nella directory `c:\ProgramData\Symantec\Data Loss Prevention\<Enforce Server o Detection Server>\15.1\Protect\logs\` nelle installazioni Windows e nella directory `/var/log/Symantec/DataLossPrevention/<Enforce Server or Detection Server>/15.1/` nelle installazioni Linux. Un numero alla fine del nome di file di registro indica il totale (indicato come 0 nei file di registro di debug).

La tabella seguente elenca e descrive i file di registro di debug di Symantec Data Loss Prevention.

Tabella 14-2 File di registro di debug

Nome di file di registro	Descrizione	Server
Aggregator0.log	<p>Questo file descrive le comunicazioni tra il server di rilevamento e gli agenti.</p> <p>Esaminare questo registro per risolvere i seguenti problemi:</p> <ul style="list-style-type: none"> ■ Connessione agli agenti ■ Per determinare quali incidenti non sono visualizzati quando dovrebbero esserlo ■ Se si verificano eventi dell'agente imprevisti 	Server di rilevamento di endpoint
BoxMonitor0.log	<p>Questo file è in genere molto piccolo e mostra come i processi dell'applicazione vengono eseguiti. Il processo <code>BoxMonitor</code> sorveglia i processi del server di rilevazione che riguardano quel particolare tipo di server.</p> <p>Ad esempio, i processi eseguiti su Network Monitor sono file reader e acquisizione del pacchetto.</p>	Tutti i server di rilevamento
ContentExtractionAPI_FileReader.log	<p>Registra il comportamento del file reader API di estrazione del contenuto che invia le richieste all'host del plug-in. Il livello di registrazione predefinito è "Info" che è configurabile tramite <code>log4cxx_config_filereader.xml</code> nella directory <code>c:\Programmi\ Symantec\ Data Loss Prevention\ Detection Server\ 15.1\ Protect\config (Windows)</code> o nella directory <code>/opt/Symantec/ DataLossPrevention/ Detection Server/ 15.1/ Protect/config (Linux)</code>.</p>	Server di rilevamento
ContentExtractionAPI_Manager.log	<p>Registra il comportamento del manager API di estrazione del contenuto che invia le richieste all'host del plug-in. Il livello di registrazione predefinito è "Info" che è configurabile tramite <code>log4cxx_config_manager.xml</code> nella directory <code>c:\Programmi\ Symantec\ Data Loss Prevention\ Detection Server\ 15.1\ Protect\config (Windows)</code> o nella directory <code>/opt/Symantec/ DataLossPrevention/ Detection Server/ 15.1/ Protect/config (Linux)</code>.</p>	Enforce Server

Nome di file di registro	Descrizione	Server
ContentExtractionHost_FileReader.log	Registra il comportamento di host e plug-in del file reader di estrazione del contenuto. Il livello di registrazione predefinito è "Info" che è configurabile tramite log4cxx_config_filereader.xml nella directory c:\Programmi\ Symantec\ Data Loss Prevention\ Detection Server\ 15.1\ Protect\config (Windows) o nella directory /opt/Symantec/ DataLossPrevention/ Detection Server/ 15.1/ Protect/config (Linux).	Server di rilevamento
ContentExtractionHost_Manager.log	Registra il comportamento degli host e plug-in del manager di estrazione del contenuto. Il livello di registrazione predefinito è "Info" che è configurabile tramite log4cxx_config_manager.xml nella directory c:\Programmi\ Symantec\ Data Loss Prevention\ Detection Server\ 15.1\ Protect\config (Windows) o nella directory /opt/Symantec/ DataLossPrevention/ Detection Server/ 15.1/ Protect/config (Linux).	Enforce Server
DiscoverNative.log.0	Questo file di registro si trova in c:\Programmi\ Symantec\Data Loss Prevention\Detection Server\15.1\ Protect\logs\debug Questo file di registro contiene le istruzioni di registro emesse dal codice nativo Network Discover/Cloud Storage Discover. Contiene correntemente le informazioni relative alla scansione .pst. Questo file di registro viene applicato solo ai server Network Discover/Cloud Storage Discover eseguiti su piattaforme Windows. È possibile configurare questo registro nel file c:\Programmi\ Symantec\Data Loss Prevention\Detection Server\15.1\ Protect\ config\ DiscoverNativeLogging.properties.	Server di rilevamento di Discover
FileReader0.log	Questo file di registro riguarda il processo di file reader e contiene la registrazione specifica all'applicazione, che può essere utile nelle risoluzione di problemi relativi al rilevamento e alla creazione di incidenti. Un sintomo sono i timeout dell'estrattore di contenuto.	Tutti i server di rilevamento

Nome di file di registro	Descrizione	Server
flash_client_0.log	Registra i messaggi dei client Adobe Flex utilizzati per i report dei rischi delle cartelle da Network Discover.	Enforce Server
flash_server_remoting_0.log	Contiene i messaggi di registro di BlazeDS, un componente open source che risponde alle chiamate di procedure remote da un client Adobe Flex. Questo registro indica se Enforce Server ha ricevuto messaggi dal client Flash. Ai livelli di registrazione permissivi (BUONO, MIGLIORE, OTTIMO), i registri di BlazeDS contengono il contenuto delle richieste client al server e il contenuto delle risposte server al client	Enforce Server
IncidentPersister0.log	Questo file di registro riguarda il processo di Incident Persister. Questo processo legge gli incidenti dalla cartella di incidenti su Enforce Server e li scrive nel database. Esaminare questo registro se la dimensione della coda degli incidenti su Enforce Server (manager) diventa troppo grande. Questa situazione può essere osservata anche controllando la cartella degli incidenti su Enforce Server per vedere se è stato eseguito il backup degli incidenti.	Enforce Server
Indexer0.log	Questo file di registro contiene informazioni quando un profilo EDM o un profilo IDM è indicizzato. Inoltre comprende anche le informazioni che vengono raccolte quando si utilizza il processo di indicizzazione esterno. Se l'indicizzazione non riesce, consultare questo registro.	Enforce Server (o il computer dove è in esecuzione il processo di indicizzazione)
jdbc.log	Questo file di registro è una traccia delle chiamate JDBC al database. Per impostazione predefinita, la scrittura su questo registro è disattivata.	Enforce Server

Nome di file di registro	Descrizione	Server
machinelearning_native_filereader.log	Questo file di registro registra la classificazione della categoria di runtime (positiva e negativa) e i livelli di sicurezza associati per ogni messaggio rilevato da un profilo VML. Il livello di registrazione predefinito è "Info" che è configurabile tramite <code>\log4cxx_config_filereader.xml</code> nella directory <code>c:\Programmi\ Symantec\ Data Loss Prevention\ Detection Server\ 15.1\ Protect\config (Windows)</code> o nella directory <code>/opt/Symantec/ DataLossPrevention/ Detection Server/ 15.1/ Protect/config (Linux)</code> .	Server di rilevamento
machinelearning_training_0_0.log	Questo file di registro registra le percentuali di accuratezza di base nella fase di realizzazione per le valutazioni k-fold di tutti i profili VML.	Enforce Server
machinelearning_training_native_manager.log	Questo file di registro registra il numero totale delle funzionalità modellate nella fase di realizzazione per ogni training di profili VML eseguito. Il livello di registrazione predefinito è "Info" che è configurabile tramite <code>log4cxx_config_manager.xml</code> nella directory <code>c:\Programmi\ Symantec\ Data Loss Prevention\ Detection Server\ 15.1\ Protect\config (Windows)</code> o nella directory <code>/opt/Symantec/ DataLossPrevention/ Detection Server/ 15.1/ Protect/config (Linux)</code> .	Enforce Server
MonitorController0.log	Questo file di registro è un registro dettagliato delle connessioni tra Enforce Server e i server di rilevamento. Fornisce dettagli sulle informazioni scambiate tra questi server, ad esempio se le politiche sono state distribuite o meno ai server di rilevazione.	Enforce Server
PacketCapture.log	Questo file di registro riguarda il processo di acquisizione dei pacchetti che riassume i pacchetti nei messaggi e li scrive nella directory <code>drop_pcap</code> . Esaminare questo registro in caso di problemi con i pacchetti ignorati o se il traffico è inferiore al previsto. <code>PacketCapture</code> non è un processo Java, quindi non segue le stesse regole di registrazione degli altri processi di sistema di Symantec Data Loss Prevention.	Network Monitor

Nome di file di registro	Descrizione	Server
PacketCapture0.log	Questo file di registro descrive i problemi con le comunicazioni di <code>PacketCapture</code> .	Network Monitor
RequestProcessor0.log	Questo file di registro è relativo solo a SMTP Prevent. Il file di registro serve soprattutto nei casi in cui <code>Smtpprevent0.log</code> non è sufficiente.	Server di rilevamento di SMTP Prevent
ScanDetail-target-0.log	Dove <i>target</i> è il nome del target della scansione. Tutti gli spazi bianchi nel nome del target sono sostituiti da trattini. Questo file di registro riguarda la scansione del Discover Server. È un record file per file di ciò che si è verificato nella scansione. Se la scansione del file riesce, vengono mostrati l'esito e informazioni su percorso, dimensione, ora, proprietario e ACL del file sottoposto a scansione. Se non riesce, viene mostrato un avviso seguito dal nome di file.	Server di rilevamento di Discover
tomcat\localhost.data.log	Questi file di registro Tomcat contengono informazioni per qualsiasi azione relativa all'interfaccia utente. I registri includono gli errori dell'interfaccia utente, errori a livello di password all'accesso ed errori Oracle (ORA-#).	Enforce Server
SymantecDLPIncidentPersister.log	Questo file di registro contiene informazioni minime: solo <code>stdout</code> e <code>stderr</code> (eventi fatali).	Enforce Server
SymantecDLPManager.log	Questo file di registro contiene informazioni minime: solo <code>stdout</code> e <code>stderr</code> (eventi fatali).	Enforce Server
SymantecDLPMonitor.log	Questo file di registro contiene informazioni minime: solo <code>stdout</code> e <code>stderr</code> (eventi fatali).	Tutti i server di rilevamento
SymantecDLPMonitorController.log	Questo file di registro contiene informazioni minime: solo <code>stdout</code> e <code>stderr</code> (eventi fatali).	Enforce Server
SymantecDLPNotifier.log	Questo file di registro riguarda il servizio di notifica e le relative comunicazioni con Enforce Server e il servizio <code>MonitorController</code> . Esaminare questo file per verificare se il servizio <code>MonitorController</code> ha registrato una modifica della politica.	Enforce Server
SymantecDLPUpdate.log	Questo file di registro viene popolato quando si aggiorna Symantec Data Loss Prevention.	Enforce Server

Vedere ["File di registro di debug per il protocollo di Network Prevent for Web"](#) a pagina 359.

Vedere ["Livelli di registrazione di Network Prevent for Email"](#) a pagina 359.

Schermata per la raccolta e la configurazione di registri

Utilizzare la schermata **Sistema > Server e rilevatori > Registri** per raccogliere file di registro o configurare il comportamento della registrazione per qualsiasi server Symantec Data Loss Prevention. La schermata **Registri** include due schede che forniscono le seguenti funzionalità:

- **Aggregazione** - Utilizzare questa scheda per raccogliere file di registro e i file di configurazione da uno o più server Symantec Data Loss Prevention.
Vedere ["Raccolta dei registri e dei file di configurazione del server"](#) a pagina 351.
- **Configurazione** - Utilizzare questa scheda per configurare il comportamento di registrazione di base per un server Symantec Data Loss Prevention o per applicare un file di configurazione registri personalizzato a un server.
Vedere ["Configurazione del comportamento di registrazione di un server "](#) a pagina 345.

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Configurazione del comportamento di registrazione di un server

Utilizzare la scheda **Configurazione** della schermata **Sistema > Server e rilevatori > Registri** per modificare i parametri di configurazione della registrazione di tutti i server della distribuzione di Symantec Data Loss Prevention. Il menu **Seleziona impostazione registro diagnostico** fornisce impostazioni preconfigurate per i parametri di registrazione di Enforce Server e del server di rilevamento. È possibile selezionare un'impostazione preconfigurata per definire i livelli di registrazione comuni o per attivare la registrazione delle funzionalità più comuni del server. Il menu **Seleziona impostazione registro diagnostico** fornisce anche un'impostazione predefinita che reimposta i parametri di configurazione della registrazione sui valori predefiniti utilizzati al momento dell'installazione.

La [Tabella 14-3](#) descrive le impostazioni di registrazione preconfigurate disponibili per l'Enforce Server. La [Tabella 14-4](#) descrive le impostazioni preconfigurate disponibili per i server di rilevazione.

Se lo si desidera, è possibile caricare un file di configurazione della registrazione personalizzato creato o modificato utilizzando un editor di testo. Utilizzare la scheda **Aggregazione** per scaricare un file di configurazione della registrazione da personalizzare. È possibile caricare solo i file di configurazione che modificano le proprietà di registrazione (nomi di file che terminano con `Logging.properties`). Quando si carica un nuovo file di configurazione della

registrazione in un server, il server esegue prima il backup del file di configurazione esistente con lo stesso nome. Il nuovo file viene quindi copiato nella directory dei file di configurazione e le relative proprietà hanno effetto immediato.

Non è necessario riavviare il processo server per rendere effettive le modifiche apportate, a meno che non venga richiesto di farlo. A partire dalla versione corrente del software, solo le modifiche ai file `PacketCaptureNativeLogging.properties` e `DiscoverNativeLogging.properties` richiedono di riavviare il processo del server.

Vedere ["Controlli server"](#) a pagina 242.

Assicurarsi che il file di configurazione che si carica contenga definizioni di proprietà valide applicabili al tipo di server che si desidera configurare. Se si commettono errori durante il caricamento del file di configurazione della registrazione, utilizzare l'impostazione preconfigurata **Ripristina predefinite** per ripristinare la configurazione della registrazione allo stato dell'installazione originale.

La console di amministrazione di Enforce Server esegue solo una minima convalida dei file di configurazione che si caricano. Verifica che:

- I nomi dei file di configurazione corrispondano a nomi di file di configurazione effettivi.
- La registrazione a livello della radice sia attivata nel file di configurazione. Questa configurazione garantisce che le funzionalità di registrazione di base siano sempre disponibili per un server.
- Le proprietà nel file che definiscono i livelli di registrazione contengono solo valori validi (ad esempio `INFO`, `FINE` o `WARNING`).

Se il server rileva un problema con uno di questi elementi, visualizza un messaggio di errore e annulla il caricamento del file.

Se l'Enforce Server carica correttamente una modifica al file di configurazione della registrazione, la console di amministrazione indica che la modifica della configurazione è stata inviata. Se il server di rilevazione rileva dei problemi quando cerca di applicare la modifica della configurazione, registra un avviso di evento di sistema per indicare il problema.

Tabella 14-3 Impostazioni di registrazione preconfigurate per Enforce Server

Selezionare un valore per l'impostazione del registro diagnostico	Descrizione
Ripristina predefinite	Ripristina i parametri del file di registro sui valori predefiniti.

Selezionare un valore per l'impostazione del registro diagnostico	Descrizione
Registrazione SOAP dell'API Reporting incidente	<p>Registra l'intera richiesta SOAP e il messaggio di risposta per la maggior parte delle richieste al servizio Web API Reporting incidente. I messaggi registrati sono memorizzati nel file <code>webservices_soap.log</code>. Per avviare la registrazione in questo file, modificare il file <code>c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\ManagerLogging.properties (Windows)</code> o <code>/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config/ManagerLogging.properties (Linux)</code> per impostare la proprietà <code>com.vontu.enforce.reportingapi.webservice.log</code>.</p> <p><code>WebServiceSOAPLogHandler.level</code> su <code>INFO</code>.</p> <p>È possibile utilizzare il contenuto di <code>webservices_soap.log</code> per diagnosticare i problemi durante lo sviluppo di client del servizio Web API Reporting incidente. Per ulteriori informazioni consultare la <i>Guida degli sviluppatori dell'API Reporting incidente di Symantec Data Loss Prevention</i>.</p>
Registrazione ricerca attributi personalizzati	<p>Registra le informazioni diagnostiche ogni volta che l'Enforce Server utilizza un plug-in per compilare gli attributi personalizzati per un incidente. I plug-in di ricerca compilano i dati degli attributi personalizzati utilizzando LDAP, file CSV o altri archivi di dati. Le informazioni diagnostiche sono registrate nel file di registro Tomcat (<code>c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs\tomcat\localhost.data.log [Windows]</code> o <code>/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/tomcat/localhost.data.log [Linux]</code>) e <code>IncidentPersister_0.log</code>.</p> <p>Vedere "Informazioni sugli attributi personalizzati" a pagina 1706.</p> <p>Vedere "Informazioni sull'uso di attributi personalizzati" a pagina 1708.</p>

Tabella 14-4 Impostazioni di registrazione preconfigurate per i server di rilevamento

Selezionare un valore per l'impostazione del registro diagnostico	Il server di rilevamento usa	Descrizione
Ripristina predefinite	Tutti i server di rilevamento	Ripristina i parametri del file di registro sui valori predefiniti.
Registrazione tracce di rilevazione	Server Network Discover	Attiva la registrazione informativa per le scansioni Network Discover. Questi messaggi di registro vengono memorizzati in <code>FileReader0.log</code> .
Registrazione tracce di rilevamento	Tutti i server di rilevamento	<p>Registra informazioni su ogni messaggio elaborato dal server di rilevazione. Include informazioni quali:</p> <ul style="list-style-type: none">■ Le politiche applicate al messaggio■ Le regole di politiche corrispondenti nel messaggio■ Il numero di incidenti che il messaggio ha generato. <p>Quando si attiva Registrazione tracce di rilevamento i messaggi risultanti vengono memorizzati nel file <code>detection_operational_trace_0.log</code>.</p> <p>Nota: La registrazione delle tracce può generare un gran numero di dati e i dati sono memorizzati in formato di testo non crittografato. Utilizzare la registrazione delle tracce solo quando è necessario eseguire il debug di un determinato problema.</p>

Selezionare un valore per l'impostazione del registro diagnostico	Il server di rilevamento usa	Descrizione
Registrazione debug di acquisizione pacchetti	Server Network Monitor	<p>Attiva la registrazione di debug di base per l'acquisizione dei pacchetti con Network Monitor. Questa impostazione registra le informazioni nel file <code>PacketCapture.log</code>.</p> <p>Sebbene questo tipo di registrazione può produrre una grande quantità di dati, l'impostazione Registrazione debug di acquisizione pacchetti limita la dimensione del file di registro a 50 MB e il numero massimo di file di registro a 10.</p> <p>Se si applica questa impostazione di configurazione di registro a un server, è necessario riavviare il processo server per attivare la modifica.</p>
Registrazione Email Prevent	Server Network Prevent for Email	<p>Attiva la registrazione dei messaggi completi per i server Network Prevent for Email. Questa impostazione registra l'intero contenuto dei messaggi e include informazioni sull'esecuzione e il tracciamento degli errori. Le informazioni registrate sono memorizzate nel file <code>SmtpPrevent0.log</code>.</p> <p>Nota: La registrazione delle tracce può generare un gran numero di dati e i dati sono memorizzati in formato di testo non crittografato. Utilizzare la registrazione delle tracce solo quando è necessario eseguire il debug di un determinato problema.</p> <p>Vedere "Codici dei registri operativi di Network Prevent for Email" a pagina 360.</p> <p>Vedere "Risposte e codici generati da Network Prevent for Email" a pagina 364.</p>

Selezionare un valore per l'impostazione del registro diagnostico	Il server di rilevamento usa	Descrizione
Registrazione elaborazione messaggi ICAP Prevent	Server Network Prevent for Web	<p>Consente la registrazione relativa agli accessi e al funzionamento di Network Prevent for Web. Questa impostazione registra le informazioni nel file <code>FileReader0.log</code>.</p> <p>Vedere "File di registro operativi e codici di evento di Network Prevent for Web" a pagina 355.</p> <p>Vedere "Campi e file del registro di accesso di Network Prevent for Web" a pagina 357.</p>

Seguire questa procedura per modificare la configurazione della registrazione di un server Symantec Data Loss Prevention.

Per configurare le proprietà di registrazione per un server

- 1 Fare clic sulla scheda **Configurazione** se non è già selezionata.
- 2 Per configurare le proprietà di registrazione per un server di rilevamento, selezionare il nome del server dal menu **Selezionare un server di rilevamento**.
- 3 Per applicare impostazioni di registrazione preconfigurate a un server, selezionare il nome della configurazione dal menu **Selezionare una configurazione di diagnostica** accanto al server che si desidera configurare.

Vedere la [Tabella 14-3](#) e la [Tabella 14-4](#) per la descrizione delle configurazioni di diagnostica.

- 4 Se invece si desidera utilizzare un file di configurazione della registrazione personalizzato, fare clic su **Sfoggia...** accanto al server che si desidera configurare. Selezionare quindi il file di configurazione della registrazione da usare dalla finestra di dialogo **Carica file** e fare clic su **Apri**. I file di configurazione della registrazione caricati non hanno effetto su altre funzionalità del server.

Nota: Se il pulsante **Sfoggia** non è disponibile a causa di una selezione di menu precedente, fare clic su **Cancella modulo**.

- 5 Fare clic su **Configura registri** per applicare l'impostazione preconfigurata o il file di configurazione della registrazione personalizzato al server selezionato.
- 6 Verificare la presenza di avvisi di eventi di sistema che indicano un problema nell'applicazione delle modifiche alla configurazione in un server.

Vedere ["Schermata per la raccolta e la configurazione di registri"](#) a pagina 345.

Nota: I seguenti file di registro di debug vanno configurati senza utilizzare le funzionalità di registrazione disponibili tramite la console di amministrazione di Enforce Server:

`ContentExtractionAPI_FileReader.log`, `ContentExtractionAPI_Manager.log`,
`ContentExtractionHost_FileReader.log`, `ContentExtractionHost_Manager.log`,
`machinelearning_native_filereader.log` e

`machinelearning_training_native_manager.log`. Fare riferimento a ciascuno di questi file di registro nell'elenco dei file del registro di debug per i dettagli di configurazione. Vedere ["File di registro di debug"](#) a pagina 339.

Raccolta dei registri e dei file di configurazione del server

Usare la scheda **Raccolta** della schermata **Sistema > Server e rilevatori > Registri** per raccogliere i file di registro e i file di configurazione da uno o più server pn.SuiteNameShort;. È possibile raccogliere i file da un singolo server di rilevamento o da tutti i server di rilevamento come pure dal computer Enforce Server. È possibile limitare i file raccolti solo a quelli che sono stati aggiornati l'ultima volta in un intervallo di date specifico.

La console di amministrazione Enforce Server immagazzina tutti i file di registro e di configurazione che vengono raccolti in un singolo file ZIP sul computer Enforce Server. Se si recuperano i file da più server Symantec Data Loss Prevention i server e i file di ogni server vengono memorizzati in una sottodirectory separata del file ZIP.

Le caselle di controllo nella scheda **Raccolta** consentono di raccogliere diversi tipi di file dai server selezionati. [Tabella 14-5](#) descrive ogni tipo di file.

Tabella 14-5 Tipi di file per la raccolta

Tipo di file	Descrizione
Registri operativi	<p>I file di registro operativi registrano informazioni dettagliate sulle attività che il software esegue e sugli errori che si verificano durante l'esecuzione delle stesse. È possibile usare il contenuto dei file di registro operativi per verificare che il software funziona come previsto. È anche possibile usare questi file per risolvere eventuali problemi di compatibilità tra il software e gli altri componenti del sistema.</p> <p>Ad esempio, è possibile utilizzare i file di registro operativi per verificare che un server Network Prevent for Email comunica con un MTA specifico sulla rete.</p>
Registri di debug e di traccia	<p>I file di registro di debug registrano dettagli tecnici elaborati riguardanti i singoli processi o componenti software che costituiscono Symantec Data Loss Prevention. Il contenuto dei file di registro di debug non è inteso per l'uso nella diagnosi degli errori di configurazione del sistema o nella verifica della funzionalità del software. Non è necessario esaminare tali file per amministrare o verificare un'installazione di Symantec Data Loss Prevention. Tuttavia, il supporto Symantec può richiedere i file di registro di debug per risolvere un problema segnalato. Per impostazione predefinita, alcuni file di registro di debug non vengono creati. Il supporto Symantec può spiegare come configurare il software per creare il file, se necessario.</p>

Tipo di file	Descrizione
File di configurazione	<p>Usare l'opzione di File di configurazione per recuperare sia i file di configurazione della registrazione che i file di configurazione della funzionalità server.</p> <p>I file di configurazione della registrazione definiscono il livello globale di dettaglio della registrazione registrato nei file di registro del server. I file di configurazione della registrazione inoltre determinano se le funzionalità specifiche o gli eventi di sottosistema vengono registrati nei file di registro.</p> <p>Ad esempio, per impostazione predefinita la console Enforce non registra i messaggi SOAP generati dai client dei servizi web API di reporting incidente. Il file <code>ManagerLogging.properties</code> ha una proprietà che consente la registrazione per i messaggi SOAP.</p> <p>È possibile modificare molte proprietà comuni di configurazione di registrazione utilizzando i valori predefiniti disponibili nella scheda Configurazione.</p> <p>Se si desidera aggiornare a mano un file di configurazione della registrazione, usare la casella File di configurazione per scaricare i file di configurazione per un server. È possibile modificare le diverse proprietà della registrazione utilizzando di un editor di testo e poi usare la scheda Configurazione per caricare il file modificato sul server.</p> <p>Vedere "Configurazione del comportamento di registrazione di un server " a pagina 345.</p> <p>L'opzione File di configurazione recupera i file di configurazione della registrazione attivi e tutti i file di configurazione del registro di backup creati quando è stata usata la scheda Configurazione. Questa opzione inoltre recupera i file di configurazione della funzionalità server. I file di configurazione della funzionalità server riguardano vari aspetti di comportamento del server, quali la posizione di un server di Syslog o le impostazioni di comunicazione del server. È possibile raccogliere questi file di configurazione per contribuire a diagnosticare i problemi o verificare le impostazioni del server. Tuttavia, non è possibile usare la scheda Configurazione cambiare i file di configurazione della funzionalità server. È possibile usare la scheda solo per cambiare i file di configurazione della registrazione.</p>
Registri agente	<p>Usare l'opzione Registri agente per raccogliere il servizio del DLP Agent e i file di registro operativi da un server di rilevamento Endpoint Prevent. Questa opzione è disponibile solo per i server Endpoint Prevent. Per raccogliere i registri dell'agente utilizzando questa opzione, occorre aver prima estratto i file di registro da agenti specifici verso il server di rilevamento Endpoint Prevent utilizzando l'azione Estrai registri.</p> <p>Utilizzare la schermata Elenco agenti per selezionare singoli agenti e inviare i file di registro selezionati al server di rilevamento Endpoint Prevent. Quindi utilizzare l'opzione Registri agente in questa pagina per raccogliere i file di registro.</p> <p>Quando i registri vengono estratti dall'endpoint, vengono archiviati su Endpoint Server in un formato non crittografato. Dopo che i registri sono stati raccolti da Endpoint Server, vengono eliminati da Endpoint Server e archiviati solo su Enforce Server. È possibile raccogliere i registri da un solo endpoint alla volta.</p> <p>Vedere "Utilizzo della schermata Elenco agenti" a pagina 2197.</p>

File operativi, di debug, file di registro e di tracciamento vengono archiviati nella sottodirectory `server_identifier/logs` dell'archivio ZIP. `server_identifier` identifica il server che ha generato i file di registro e corrisponde a uno delle seguenti valori:

- Se si raccolgono i file di registro dall'Enforce Server, Symantec Data Loss Prevention sostituisce `server_identifier` con la stringa `Enforce`. Tenere presente che Symantec Data Loss Prevention non utilizza il nome localizzato dell'Enforce Server.
- Se il nome di un server di rilevamento comprende solo i caratteri ASCII, Symantec Data Loss Prevention usa il nome del server di rilevamento per il valore `server_identifier`.
- Se un nome del server di rilevamento contiene caratteri non-ASCII, Symantec Data Loss Prevention usa la stringa `DetectionServer-ID-id_number` per il valore `server_identifier`. `id_number` è un numero di identificazione univoco del server di rilevamento.

Se si raccolgono file di registro del servizio dell'agente o file di registro operativi da un server Endpoint Prevent i file vengono posizionati nella sottodirectory `server_identifier/agentlogs`. Ogni file di registro dell'agente usa il nome dell'agente singolo come prefisso del file di registro.

Seguire questa procedura per raccogliere i file di registro e registrare i file di configurazione dai server Symantec Data Loss Prevention.

Per raccogliere i file di registro da uno o più server

- 1 Fare clic sulla scheda **Raccolta** se non è già selezionata.
- 2 Usare il menu **Intervallo di date** per selezionare un intervallo di date per i file che si desidera raccogliere. Tenere presente che il processo di raccolta non taglia in alcun modo i file di registro scaricati. I limiti dell'intervallo di date hanno raccolto i file in quei file che sono stati aggiornati l'ultima volta nell'intervallo specificato.
- 3 Per raccogliere i file di registro dall'Enforce Server, selezionare una o più caselle di controllo accanto alla voce **Enforce Server** per indicare il tipo di file che si desidera raccogliere.
- 4 Per raccogliere i file di registro da uno o tutti i server di rilevamento, usare il menu **Seleziona un server di rilevamento** per selezionare il nome di un server di rilevamento o l'opzione **Raccogli i registri da tutti i server di rilevamento**. Quindi selezionare una o più caselle accanto al menu per indicare il tipo di file che si desidera raccogliere.
- 5 Fare clic su **Raccogli registri** per cominciare il processo di raccolta dei registri.

La console di amministrazione aggiunge una nuova voce al processo di raccolta dei registri nell'elenco **Raccolte registri precedenti** in fondo alla schermata. Se si stanno recuperando molti file di registro, può essere necessario ricaricare periodicamente la schermata per determinare quando il processo di raccolta del registro è completato.

Nota: È possibile eseguire solo un processo di raccolta di registri per volta.

- 6 Per annullare un processo di raccolta del registro attivo, fare clic su **Annulla** accanto alla voce della raccolta di registri. Può essere necessario annullare la raccolta del registro se uno o più server sono offline e il processo della raccolta non può essere completato. Quando si annulla la raccolta del registro, il file ZIP contiene solo i file che sono stati raccolti con successo.
- 7 Per scaricare i registri raccolti sul computer locale, cliccare su **Scarica** accanto alla voce di raccolta di registri.
- 8 Per rimuovere i file ZIP archiviati su Enforce Server, fare clic su **Elimina** accanto a una voce di raccolta dei registri.

Vedere ["Schermata per la raccolta e la configurazione di registri"](#) a pagina 345.

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Informazioni sui codici di evento dei registri

I messaggi dei file di registro operativi sono formattati per corrispondere il più possibile agli standard industriali dei vari protocolli utilizzati. Questi messaggi di registro contengono codici di evento che descrivono l'attività che il software stava cercando di eseguire quando il messaggio è stato registrato. I messaggi di registro sono in genere formattati come segue:

Timestamp [Log Level] (Event Code) Event description [event parameters]

- Vedere ["File di registro operativi e codici di evento di Network Prevent for Web"](#) a pagina 355.
- Vedere ["Codici dei registri operativi di Network Prevent for Email"](#) a pagina 360.
- Vedere ["Risposte e codici generati da Network Prevent for Email"](#) a pagina 364.

File di registro operativi e codici di evento di Network Prevent for Web

I nomi dei file di registro di Network Prevent for Web usano il formato

WebPrevent_OperationalX.log (dove X è un numero). Il numero di file archiviati e le relative dimensioni possono essere specificati cambiando i valori nel file

FileReaderLogging.properties. Questo file si trova nella directory

c:\Programmi\Symantec\Data Loss Prevention\Detection Server\15.1\Protect\config (Windows) o nella directory /opt/Symantec/DataLossPrevention/Detection Server/15.1/Protect/config (Linux). Per impostazione predefinita, i valori sono:

- `com.vontu.icap.log.IcapOperationalLogHandler.limit = 5000000`
- `com.vontu.icap.log.IcapOperationalLogHandler.count = 5`

[Tabella 14-6](#) elenca i codici dei registri operativi definiti da Network Prevent for Web per categoria. Il testo in corsivo contiene parametri di evento.

Tabella 14-6 Codici di stato per i registri operativi di Network Prevent for Web

Codice	Testo e descrizione
Eventi operativi	
1100	Starting Network Prevent for Web
1101	Shutting down Network Prevent for Web
Eventi di connettività	
1200	<p>Listening for incoming connections at <i>icap_bind_address:icap_bind_port</i></p> <p>Dove:</p> <ul style="list-style-type: none"> ■ <i>icap_bind_address</i> è l'indirizzo di binding di Network Prevent for Web che il server ascolta. Questo indirizzo è specificato con l'impostazione avanzata Icap.BindAddress. ■ <i>icap_bind_port</i> è la porta che il server ascolta. Questa porta è impostata nella pagina Server > Configura.
1201	<p>Connection (<i>id=conn_id</i>) opened from <i>host(icap_client_ip:icap_client_port)</i></p> <p>Dove:</p> <ul style="list-style-type: none"> ■ <i>conn_id</i> è l'ID di connessione assegnato a questa connessione. Questo ID può essere utile per le correlazioni tra molteplici registri. ■ <i>icap_client_ip</i> e <i>icap_client_port</i> sono l'indirizzo IP e la porta del proxy da cui è stata eseguita l'operazione di connessione a Network Prevent for Web.
1202	<p>Connection (<i>id=conn_id</i>) closed (<i>close_reason</i>)</p> <p>Dove:</p> <ul style="list-style-type: none"> ■ <i>conn_id</i> è l'ID di connessione assegnato all'operazione di connessione. ■ <i>close_reason</i> fornisce la ragione della chiusura della connessione.
1203	<p>Connection states: REQMOD=<i>N</i>, RESPMOD=<i>N</i>, OPTIONS=<i>N</i>, OTHERS=<i>N</i></p> <p>Dove <i>N</i> indica il numero di connessioni in ogni stato, quando il messaggio è stato registrato.</p> <p>Questo messaggio fornisce lo stato di sistema in termini di gestione delle connessioni. Viene registrato ogni volta che una connessione viene aperta o chiusa.</p>
Errori di connettività	

Codice	Testo e descrizione
5200	<p>Failed to create listener at <i>icap_bind_address:icap_bind_port</i></p> <p>Dove:</p> <ul style="list-style-type: none"> ■ <i>icap_bind_address</i> è l'indirizzo di binding di Network Prevent for Web che il server ascolta. Questo indirizzo può essere specificato con l'impostazione avanzata <code>Icap.BindAddress</code>. ■ <i>icap_bind_port</i> è la porta che il server ascolta. Questa porta è impostata nella pagina Server > Configura.
5201	<p>Connection was rejected from unauthorized host (<i>host_ip:port</i>)</p> <p>Dove <i>host_ip</i> e <i>port</i> sono l'indirizzo IP e la porta del sistema proxy da cui è stato eseguito un tentativo di connessione a Network Prevent for Web. Se l'host non è elencato nell'impostazione avanzata <code>Icap.AllowHosts</code>, non è in grado di generare una connessione.</p>

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Campi e file del registro di accesso di Network Prevent for Web

I nomi dei file di registro di Network Prevent for Web usano il formato `WebPrevent_AccessX.log` (dove X è un numero). Il numero di file archiviati e le relative dimensioni possono essere specificati cambiando i valori nel file `FileReaderLogging.properties`. Per impostazione predefinita, i valori sono:

- `com.vontu.icap.log.IcapAccessLogHandler.limit = 5000000`
- `com.vontu.icap.log.IcapAccessLogHandler.count = 5`

Un registro di accesso di Network Prevent for Web è simile al registro di accesso Web di un server proxy. Il formato dei messaggi del registro "start" è:

```
# Web Prevent starting: start_time
```

Dove il formato di `start_time` è `date:time`, per esempio: `13/Aug/2018:03:11:22:015-0700`.

Il formato dei messaggi descrittivi è:

```
# host_ip "auth_user" time_stamp "request_line" icap_status_code
request_size "referer" "user_agent" processing_time(ms) conn_id client_ip
client_port action_code icap_method_code traffic_source_code
```

Tabella 14-7 elenca i campi. I valori dei campi racchiusi tra virgolette in questo esempio lo sono nel messaggio. Se i valori dei campi non possono essere determinati, il messaggio mostra - o "" come valore predefinito.

Tabella 14-7 Campi del registro di accesso di Network Prevent for Web

Campi	Descrizione
host_ip	L'indirizzo IP dell'host che ha generato la richiesta.
auth_user	L'utente autorizzato per questa richiesta.
time_stamp	La data e l'ora in cui Network Prevent for Web riceve la richiesta.
request_line	La riga che rappresenta la richiesta.
icap_status_code	Codice di risposta ICAP che Network Prevent for Web invia per questa richiesta.
request_size	La dimensione della richiesta in byte.
referrer	Il valore di intestazione della richiesta che contiene l'URI da cui la richiesta è stata originata.
user_agent	L'agente utente associato alla richiesta.
processing_time (millisecondi)	Il tempo di elaborazione della richiesta in millisecondi. Questo valore comprende il tempo di ricezione, il tempo di ispezione del contenuto e quello di invio.
conn_id	L'ID di connessione associato alla richiesta.
client_ip	L'IP del client ICAP (proxy).
client_port	La porta del client ICAP (proxy).
action_code	<p>Un numero intero che rappresenta l'azione intrapresa da Network Prevent for Web. Il codice dell'azione è uno dei seguenti:</p> <ul style="list-style-type: none"> ■ 0 = UNKNOWN ■ 1 = ALLOW ■ 2 = BLOCK ■ 3 = REDACT ■ 4 = ERROR ■ 5 = ALLOW_WITHOUT_INSPECTION ■ 6 = OPTIONS_RESPONSE ■ 7 = REDIRECT

Campi	Descrizione
icap_method_code	Un numero intero che rappresenta il metodo ICAP associato alla richiesta. Il codice del metodo ICAP è uno dei seguenti: <ul style="list-style-type: none">■ -1 = ILLEGAL■ 0 = OPTIONS■ 1 = REQMOD■ 2 = RESPMOD■ 3 = LOG
traffic_source_code	Un numero intero che rappresenta l'origine del traffico di rete. Il codice del traffico di rete è uno dei seguenti: <ul style="list-style-type: none">■ 1 = WEB■ 2 = UNKNOWN

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

File di registro di debug per il protocollo di Network Prevent for Web

Per consentire la registrazione della tracce ICAP, impostare l'impostazione avanzata **icap.EnableTrace** su `true` e usare l'impostazione avanzata **icap.TraceFolder** per specificare una directory dove ricevere le tracce. Il servizio Symantec Data Loss Prevention deve essere riavviato per rendere effettiva la modifica.

I nomi dei file di tracce nella directory specificata sono nel formato: *timestamp-id_conn*. La prima riga di un file di traccia fornisce informazioni sulla porta e sull'IP host di connessione e un timestamp. I dati dei file letti dal socket sono visualizzati nel formato `<<timestamp number_of_bytes_read`. I dati scritti sul socket sono visualizzati nel formato `>>timestamp number_of_bytes_written`. L'ultima riga deve indicare che la connessione è stata chiusa.

Nota: La registrazione delle tracce produce una grande quantità di dati e quindi richiede una grande quantità di spazio di archiviazione sul disco. La registrazione delle tracce deve essere usata solo per il debug di un problema in quanto i dati scritti nel file sono in testo non crittografato.

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Livelli di registrazione di Network Prevent for Email

I nomi dei file di registro di Network Prevent for Email usano il formato `EmailPrevent_OperationalX.log` (dove *X* è un numero). Il numero di file archiviati e le relative

dimensioni possono essere specificati cambiando i valori nel file `FileReaderLogging.properties`. Per impostazione predefinita, i valori sono:

- `com.vontu.mta.log.SmtOperationalLogHandler.limit = 5000000`
- `com.vontu.mta.log.SmtOperationalLogHandler.count = 5`

A seconda dei diversi livelli di registrazione, i componenti del pacchetto `com.vontu.mta.rp` forniscono vari livelli di dettaglio. L'impostazione `com.vontu.mta.rp.level` specifica i livelli di registro nel file `RequestProcessorLogging.properties` memorizzato nel file `FileReaderLogging.properties`. Questo file si trova nella directory `c:\Programmi\Symantec\Data Loss Prevention\Detection Server\15.1\Protect\config` (Windows) o nella directory `/opt/Symantec/DataLossPrevention/Detection Server/15.1/Protect/config` (Linux). Ad esempio, `com.vontu.mta.rp.level = FINE` specifica il livello di dettaglio BUONO.

[Tabella 14-8](#) descrive i livelli di registrazione di Network Prevent for Email.

Tabella 14-8 Livelli di registrazione di Network Prevent for Email

Livello	Linee guida
NORMALE	Eventi generale: avvisi di connessione e disconnessione, informazioni sui messaggi che vengono elaborati per ogni connessione.
BUONO	Alcune informazioni supplementare per il tracciamento delle esecuzioni.
MIGLIORE	Flussi del comando Busta, intestazioni dei messaggi, risultati della rilevazione.
OTTIMO	Contenuto completo dei messaggi, tracciamento delle esecuzioni estremamente dettagliato e tracciamento degli errori.

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Codici dei registri operativi di Network Prevent for Email

[Tabella 14-9](#) elenca i codici dei registri operativi di Network Prevent for Email definiti per categoria.

Tabella 14-9 Codici di stato dei registri operativi di Network Prevent for Email

Codice	Descrizione
Eventi core	
1100	Starting Network Prevent for Email
1101	Shutting down Network Prevent for Email

Codice	Descrizione
1102	Reconnecting to FileReader (tid= <i>id</i>) Dove <i>id</i> è l'identificatore del thread. Il RequestProcessor tenta di ristabilire la connessione con il FileReader per il rilevamento.
1103	Reconnected to the FileReader successfully (tid= <i>id</i>) Il RequestProcessor è stato in grado di ristabilire la connessione al FileReader.
Errori core	
5100	Could not connect to the FileReader (tid= <i>id</i> timeout=.3s) Un tentativo di connessione al FileReader non è riuscito.
5101	FileReader connection lost (tid= <i>id</i>) La connessione del RequestProcessor al FileReader è stata interrotta.
Eventi di connettività	
1200	Listening for incoming connections (local= <i>hostname</i>) <i>Hostnames</i> è un indirizzo IP o un nome di dominio completo.
1201	Connection accepted (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i>) Dove <i>N</i> è l'identificatore della connessione.
1202	Peer disconnected (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i>)
1203	Forward connection established (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i>)
1204	Forward connection closed (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i>)
1205	Service connection closed (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> messages=1 time=0.14s)

Codice	Descrizione
Errori di connettività	
5200	Connection is rejected from the unauthorized host (tid= <i>id</i> local= <i>hostname:port</i> remote= <i>hostname:port</i>)
5201	Local connection error (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> reason= <i>Explanation</i>)
5202	Sender connection error (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> reason= <i>Explanation</i>)
5203	Forwarding connection error (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> reason= <i>Explanation</i>)
5204	Peer disconnected unexpectedly (tid= <i>id</i> cid= <i>N</i> local= <i>hostname:port</i> remote= <i>hostname:port</i> reason= <i>Explanation</i>)
5205	Could not create listener (address=local= <i>hostname:port</i> reason= <i>Explanation</i>)
5206	Authorized MTAs contains invalid hosts: <i>hostname</i> , <i>hostname</i> , ...
5207	MTA restrictions are active, but no MTAs are authorized to communicate with this host
5208	TLS handshake failed (reason= <i>Explanation</i> tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i>)
5209	TLS handshake completed (tid= <i>id</i> cid= <i>N</i> local= <i>hostname</i> remote= <i>hostname</i>)
5210	All forward hosts unavailable (tid= <i>id</i> cid= <i>N</i> reason= <i>Explanation</i>)

Codice	Descrizione
5211	DNS lookup failure (tid=id cid=N NextHop=hostname reason=Explanation)
5303	Failed to encrypt incoming message (tid=id cid=N local=hostname remote=hostname)
5304	Failed to decrypt outgoing message (tid=id cid=N local=hostname remote=hostname)

Eventi di messaggio

1300	<p>Message complete (cid=N message_id=3 dlp_id=message_identifier size=number sender=email_address recipient_count=N disposition=response estatus=statuscode rtime=N dtime=N mtime=N)</p> <p>Dove:</p> <ul style="list-style-type: none"> ■ Recipient_count è il numero totale di destinatari nei campi A, CC e CCN. ■ La risposta è la risposta Network Prevent for Email che può essere una di: PASS, BLOCK, BLOCK_AND_REDIRECT, REDIRECT, MODIFY, or ERROR. ■ Lo stato è un codice di stato Avanzato. Vedere "Risposte e codici generati da Network Prevent for Email" a pagina 364. ■ rtime è il tempo in secondi che Network Prevent for Email ha a disposizione per ricevere completamente il messaggio dal MTA che lo ha inviato. ■ dtime è il tempo in secondi che Network Prevent for Email ha a disposizione per eseguire il rilevamento sul messaggio. ■ mtime è il tempo totale in secondi che Network Prevent for Email ha a disposizione per elaborare gli errori di messaggio.
------	---

Errori di messaggio

5300	<p>Error while processing message (cid=N message_id=header_ID dlp_id=message_identifier size=0 sender=email_address recipient_count=N disposition=response estatus=statuscode rtime=N dtime=N mtime=N reason=Explanation)</p> <p>Dove header_ID è un'intestazione RFC 822 Message-Id se esistente.</p>
5301	Sender rejected during re-submit
5302	Recipient rejected during re-submit

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Risposte e codici generati da Network Prevent for Email

Network Prevent for Email genera le risposte descritte in questa sezione. Altre risposte di protocollo sono previste quando Network Prevent for Email trasmette risposte del flusso di comandi dall'agente MTA di inoltra a quello di invio. [Tabella 14-10](#) mostra le risposte generate in situazioni in cui Network Prevent deve ignorare l'agente MTA di ricezione. Mostra inoltre le situazioni in cui Network Prevent genera una specifica risposta a un evento che non è trasmesso dal downstream.

“Stato avanzato” è il codice di stato avanzato RFC1893 associato alla risposta.

Tabella 14-10 Risposte generate da Network Prevent for Email

Codice	Stato avanzato	Testo	Descrizione
250	2.0.0	Ok: Carry on.	Codice di operazione riuscita utilizzato da Network Prevent for Email.
221	2.0.0	Service closing.	Il normale codice di interruzione della connessione che Network Prevent for Email genera se una richiesta QUIT è ricevuta quando nessuna connessione MTA di inoltra è attiva.
451	4.3.0	Error: Processing error.	Questa risposta di errore “generale, temporaneo” viene emessa quando si ha una condizione di errore (potenzialmente) recuperabile. Questa risposta di errore viene emessa quando una risposta di errore più specifica non è disponibile. Le connessioni di inoltra vengono a volte chiuse e questa interruzione inattesa è occasionalmente dovuta a un codice 451, stato 4.3.0. Tuttavia, in questi casi, le connessioni di invio devono rimanere aperte a meno che l'agente MTA di invio sceglie di interromperle.
421	4.3.0	Fatal: Processing error. Closing connection.	Questa risposta di errore “generale, terminale” viene emessa quando si ha una condizione di errore irreversibile. Questo errore provoca l'interruzione immediata di qualsiasi connessione di invio o ricezione.
421	4.4.1	Fatal: Forwarding agent unavailable.	Un tentativo di connessione all'agente MTA di inoltra è stato rifiutato o non è riuscito.

Codice	Stato avanzato	Testo	Descrizione
421	4.4.2	Fatal: Connection lost to forwarding agent.	Chiusura della connessione. La connessione MTA di inoltra è stata interrotta e la conversazione con l'agente MTA di invio non è possibile. La chiusura si ha durante il buffering dell'intestazione o del corpo del messaggio. La connessione viene interrotta immediatamente.
451	4.4.2	Error: Connection lost to forwarding agent.	La connessione MTA di inoltra è stata interrotta e può eventualmente essere ripristinata. La connessione MTA di invio viene mantenuta a meno che l'agente MTA scelga di interromperla.
421	4.4.7	Error: Request timeout exceeded.	L'ultimo comando emesso non ha ricevuto una risposta entro l'intervallo di tempo definito in RequestProcessor.DefaultCommandTimeout. L'intervallo di tempo può essere quello definito in RequestProcessor.DotCommandTimeout se il comando emesso era ".". La connessione viene chiusa immediatamente.
421	4.4.7	Error: Connection timeout exceeded.	La connessione è rimasta inattiva (nessun comando attivamente in attesa di risposta) per un tempo superiore all'intervallo definito in RequestProcessor.DefaultCommandTimeout.
501	5.5.2	Fatal: Invalid transmission request.	Si è verificata una violazione fatale del protocollo SMTP (o dei vincoli sullo stesso). Non è previsto un cambiamento della violazione in seguito a un ulteriore tentativo di invio del messaggio. Questo messaggio viene generato solo in risposta a un singolo comando o riga di dati che supera i limiti definiti in RequestProcessor.MaxLineLength.
502	5.5.1	Error: Unrecognized command.	Definito ma non attualmente utilizzato.
550	5.7.1	User Supplied.	Questa combinazione di codice e stato indica che è stata attivata una regola di risposta di blocco. Il testo restituito è parte della definizione della regola di risposta.

Da notare che un codice 4xx e uno stato avanzato 4.x.x indicano un errore temporaneo. In tali casi, l'agente MTA può inviare di nuovo il messaggio al server Network Prevent for Email.

Un codice 5xx e uno stato avanzato 5.x.x indicano un errore permanente. In tali casi, l'agente MTA deve trattare il messaggio come non recapitabile.

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Utilizzo delle utilità di Symantec Data Loss Prevention

Il capitolo contiene i seguenti argomenti:

- [Informazioni sulle utilità di Symantec Data Loss Prevention](#)
- [Informazioni sulle utilità Endpoint](#)
- [Informazioni su DBPasswordChanger](#)

Informazioni sulle utilità di Symantec Data Loss Prevention

Symantec fornisce una suite di utilità che aiutano gli utenti a eseguire le attività da eseguire su base non regolare. Le utilità vengono solitamente utilizzate per eseguire risoluzione di problemi e operazioni di manutenzione. Inoltre vengono usate per preparare i dati e i file da utilizzare con il software Symantec Data Loss Prevention.

Le utilità di Symantec Data Loss Prevention vengono fornite per i sistemi operativi Windows e Linux. La riga di comando consente di eseguire utilità su entrambi i sistemi operativi. Le utilità funzionano in modo analogo indipendentemente dal sistema operativo.

[Tabella 15-1](#) descrive come e quando utilizzare ogni utilità.

Tabella 15-1 Utilità di Symantec Data Loss Prevention

Nome	Descrizione
DBPasswordChanger	Modifica la password crittografata che l'Enforce Server utilizza per connettersi al database di Oracle. Vedere "Informazioni su DBPasswordChanger" a pagina 369.
sslkeytool	Genera chiavi di autenticazione personalizzate per migliorare la sicurezza dei dati trasmessi tra l'Enforce Server e i server di rilevamento. Le chiavi di autenticazione personalizzate devono essere copiate in ogni server Symantec Data Loss Prevention. Vedere l'argomento "Informazioni sull'utilità sslkeytool e certificati del server" nel <i>Manuale di installazione di Symantec Data Loss Prevention</i> .
SQL Preindexer	Indicizza una database SQL o esegue una query SQL su specifiche tabelle di dati all'interno del database. Questa utilità è progettata per collegare in cascata il relativo output direttamente nell'utilità Indicizzatore EDM remoto. Vedere "Informazioni su SQL Preindexer" a pagina 540.
Indicizzatore EDM remoto	Converte un file di dati separati da virgole o delimitati da tabulazioni in un indice Exact Data Matching (EDM). L'utilità può essere eseguita su un computer remoto per fornire la stessa funzionalità di indicizzazione disponibile localmente sull'Enforce Server. Questa utilità vien utilizzata spesso con SQL Preindexer. L'SQL Preindexer può eseguire una query SQL e trasmettere i dati risultanti direttamente nell'Indicizzatore EDM remoto per creare un indice EDM. Vedere "Informazioni su Remote EDM Indexer" a pagina 540.

Informazioni sulle utilità Endpoint

[Tabella 15-2](#) descrive le utilità applicate ai prodotti Endpoint.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Tabella 15-2 Utilità Endpoint

Nome	Descrizione
Service_Shutdown.exe	Questa utilità consente a un amministratore di disattivare i servizi cane da guardia e agente in un endpoint. (Come misura di verifica delle alterazioni, non è possibile per un utente interrompere il servizio watchdog o agente.) Vedere "Arresto dell'agente e dei servizi watchdog su endpoint Windows" a pagina 2261.

Nome	Descrizione
Vontu_sqlite3.exe	Questa utilità fornisce un'interfaccia SQL che garantisce di visualizzare o modificare i file di database crittografati utilizzati da Symantec DLP Agent. Utilizzare questo strumento quando si desidera investigare o effettuare modifiche ai file Symantec Data Loss Prevention. Vedere "Ispezione dei file di database utilizzati dall'agente" a pagina 2263.
Logdump.exe	Questo strumento consente di visualizzare ii file di registro estesi di Symantec DLP Agent, nascosti per motivi di sicurezza. Vedere "Visualizzazione dei file di registro estesi" a pagina 2265.
Start_agent	Questa utilità consente a un amministratore di avviare gli agenti in esecuzione su endpoint Mac interrotti tramite l'attività di arresto. Vedere "Avvio dei DLP Agent eseguiti negli endpoint Mac" a pagina 2270.

Informazioni su DBPasswordChanger

Symantec Data Loss Prevention archivia le password crittografate sul database di Oracle in un file denominato `DatabasePassword.properties`, situato `inc:\SymantecDLP\Protect\config(Windows)` o `in/opt/SymantecDLP/Protect/config(Linux)`. Poiché i contenuti del file sono crittografati, non è possibile modificare direttamente il file. L'utilità DBPasswordChanger modifica le password di database Oracle archiviate che vengono utilizzate da Enforce Server.

Prima di potere utilizzare DBPasswordChanger per cambiare la password nel database Oracle è necessario:

- Arrestare Enforce Server.
- Modificare la password del database di Oracle mediante le utilità di Oracle.

Vedere ["Esempio di utilizzo di DBPasswordChanger"](#) a pagina 370.

Sintassi DBPasswordChanger

L'utilità DBPasswordChanger utilizza la seguente sintassi:

```
DBPasswordChanger password_file new_oracle_password
```

Tutti i parametri della riga di comando sono richiesti. La seguente tabella descrive ogni parametro di riga di comando.

Vedere ["Esempio di utilizzo di DBPasswordChanger"](#) a pagina 370.

Tabella 15-3 Parametri della riga di comando DBPasswordChanger

Parametro	Descrizione
<i>password_file</i>	Specifica il file che contiene la password crittografata. Per impostazione predefinita, il file è denominato <code>DatabasePassword.properties</code> ed è archiviato in <code>\SymantecDLP\Protect\config</code> (Windows) o <code>/opt/SymantecDLP/Protect/config</code> (Linux).
<i>new_oracle_password</i>	Specifica la nuova password di Oracle da crittografare e archiviare.

Esempio di utilizzo di DBPasswordChanger

Se Symantec Data Loss Prevention è stato installato nella posizione predefinita, l'utilità DBPasswordChanger si trova in `c:\SymantecDLP\Protect\bin` (Windows) o `/opt/SymantecDLP/Protect/bin` (Linux). Solo un amministratore (o radice) può eseguire DBPasswordChanger.

Ad esempio immettere:

```
DBPasswordChanger \SymantecDLP\Protect\bin\DatabasePassword.properties
protect_oracle
```

Vedere ["Sintassi DBPasswordChanger"](#) a pagina 369.

Creazione di politiche

- [Capitolo 16. Introduzione alle politiche](#)
- [Capitolo 17. Panoramica di rilevazione di politica](#)
- [Capitolo 18. Creazione di politiche dai modelli](#)
- [Capitolo 19. Configurazione di politiche](#)
- [Capitolo 20. Amministrazione delle politiche](#)
- [Capitolo 21. Best practice per la creazione di politiche](#)
- [Capitolo 22. Rilevamento del contenuto mediante Exact Data Matching \(EDM\)](#)
- [Capitolo 23. Rilevamento del contenuto mediante Indexed Document Matching \(IDM\)](#)
- [Capitolo 24. Rilevamento del contenuto mediante Vector Machine Learning \(VML\)](#)
- [Capitolo 25. Rilevamento del contenuto mediante Riconoscimento moduli - Riconoscimento di immagini riservate](#)
- [Capitolo 26. Rilevamento del contenuto mediante OCR - Riconoscimento di immagini riservate](#)
- [Capitolo 27. Rilevamento del contenuto mediante identificatori di dati](#)
- [Capitolo 28. Rilevamento del contenuto mediante la corrispondenza di parole chiave](#)
- [Capitolo 29. Rilevamento del contenuto mediante espressioni regolari](#)

- Capitolo 30. Rilevamento del contenuto utilizzando la corrispondenza di classificazione
- Capitolo 31. Rilevamento del contenuto di lingua internazionale
- Capitolo 32. Rilevamento delle proprietà di file
- Capitolo 33. Rilevamento degli incidenti di rete
- Capitolo 34. Rilevamento degli eventi endpoint
- Capitolo 35. Rilevamento delle identità descritte
- Capitolo 36. Rilevamento delle identità sincronizzate
- Capitolo 37. Rilevamento delle identità con profilo
- Capitolo 38. Utilizzo di attributi contestuali per il Rilevamento applicazioni
- Capitolo 39. Formati di file supportati per rilevamento
- Capitolo 40. Libreria degli identificatori di dati del sistema
- Capitolo 41. Libreria dei modelli di politica

Introduzione alle politiche

Il capitolo contiene i seguenti argomenti:

- [Informazioni sulle politiche di Data Loss Prevention](#)
- [Componenti della politica](#)
- [Modelli di politica](#)
- [Pacchetti di soluzioni](#)
- [Gruppi di politiche](#)
- [Distribuzione di politiche](#)
- [Gravità delle politiche](#)
- [Privilegi di creazione politiche](#)
- [Profili dati](#)
- [Gruppi utente](#)
- [Importazione ed esportazione dei modelli politica](#)
- [Flusso di lavoro per l'implementazione di politiche](#)
- [Visualizzazione, stampa e download dei dettagli della politica](#)

Informazioni sulle politiche di Data Loss Prevention

Le politiche vengono implementate per rilevare e impedire perdite di dati. Una politica di Symantec Data Loss Prevention combina regole di rilevamento e azioni di risposta. Se una regola di politica viene violata, il sistema genera un incidente che è possibile segnalare e riparare. Le regole di politica implementate sono basate sugli obiettivi di sicurezza delle informazioni. Le azioni intraprese in risposta alle violazioni delle politiche sono basate sui

requisiti di conformità dell'azienda. La console di amministrazione di Enforce Server fornisce un'interfaccia intuitiva, centralizzata e basata su Web per creare le politiche.

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

[Tabella 16-1](#) descrive le funzionalità di creazione di politiche fornite da Symantec Data Loss Prevention.

Tabella 16-1 Funzionalità di creazione delle politiche

Funzionalità	Descrizione
Generazione intuitiva delle politiche	<p>L'interfaccia del generatore di politiche supporta la logica booleana per la configurazione del rilevamento.</p> <p>È possibile combinare differenti metodi e tecnologie di rilevamento in una singola politica.</p> <p>Vedere "Rilevamento della perdita di dati" a pagina 387.</p> <p>Vedere "Best practice per la creazione di politiche" a pagina 462.</p>
Regole di risposta distinte	<p>Il sistema archivia le regole di risposta e le politiche come entità distinte.</p> <p>È possibile gestire e aggiornare le regole di risposta senza dover modificare le politiche; è possibile riutilizzare le regole di risposta nelle politiche.</p> <p>Vedere "Informazioni sulle regole di risposta" a pagina 1468.</p>
Reporting elaborato delle politiche	<p>Il sistema fornisce livelli di gravità per le violazioni delle politiche.</p> <p>È possibile segnalare la gravità globale di una violazione di politica in base alla gravità più elevata.</p> <p>Vedere "Gravità delle politiche" a pagina 379.</p>
Profiling centralizzato di dati e gruppi	<p>Il sistema archivia i profili di dati e gruppi separatamente dalle politiche.</p> <p>Questa separazione consente di gestire e aggiornare i profili senza modificare le politiche.</p> <p>Vedere "Profili dati" a pagina 381.</p> <p>Vedere "Gruppi utente" a pagina 382.</p>
Rilevamento di politiche basato su modelli	<p>Il sistema fornisce 65 modelli di politica predefiniti.</p> <p>È possibile utilizzare questi modelli per configurare e distribuire rapidamente le politiche.</p> <p>Vedere "Modelli di politica" a pagina 376.</p>
Condivisione di politiche	<p>Il sistema supporta l'importazione e l'esportazione di modelli di politica.</p> <p>È possibile condividere modelli di politica in ambienti e sistemi.</p> <p>Vedere "Importazione ed esportazione dei modelli politica" a pagina 383.</p>

Funzionalità	Descrizione
Controllo degli accessi basato sul ruolo	<p>Il sistema fornisce il controllo degli accessi basato sul ruolo per varie funzioni utente e amministrative.</p> <p>È possibile creare ruoli per la creazione di politiche, l'amministrazione di politiche e la creazione di regole di risposta.</p> <p>Vedere "Privilegi di creazione politiche" a pagina 380.</p>

Componenti della politica

Una politica valida ha almeno una regola di rilevamento o di gruppo con almeno una condizione di corrispondenza. Le regole di risposta sono componenti facoltativi della politica.

[Componenti della politica](#) descrive i componenti della politica Data Loss Prevention.

Tabella 16-2 Componenti della politica

Componente	Utilizzo	Descrizione
Gruppo di politiche	Obbligatorio	<p>Una politica deve essere assegnata a un singolo gruppo di politiche.</p> <p>Vedere "Gruppi di politiche" a pagina 377.</p>
Nome politica	Obbligatorio	<p>Il nome della politica deve essere unico all'interno del gruppo di politiche.</p> <p>Vedere "Gestione e aggiunta di politiche" a pagina 444.</p>
Regola politica	Obbligatorio	<p>Una politica valida deve contenere almeno una regola che dichiara almeno una condizione di corrispondenza.</p> <p>Vedere "Condizioni di corrispondenza di politiche" a pagina 392.</p>
Profilo dati	Può essere richiesto	<p>Le politiche Exact Data Matching (EDM), Indexed Document Matching (IDM), Vector Machine Learning (VML) e Riconoscimento moduli richiedono profili dati.</p> <p>Vedere "Profili dati" a pagina 381.</p>
Gruppo utenti	Può essere richiesto	<p>Una politica richiede un gruppo di utenti solo se un metodo di gruppo della politica lo richiede a sua volta.</p> <p>Le regole e le eccezioni DGM sincronizzate richiedono un gruppo di utenti.</p> <p>Vedere "Gruppi utente" a pagina 382.</p>
Descrizione politica	Opzionale	<p>Una descrizione della politica aiuta gli utenti a identificare lo scopo della politica.</p> <p>Vedere "Configurazione di politiche" a pagina 422.</p>

Componente	Utilizzo	Descrizione
Etichetta politica	Opzionale	Una descrizione della politica aiuta gli utenti aziendali di Veritas Data Insight a identificare lo scopo della politica quando utilizzano il portale self service. Vedere "Configurazione di politiche" a pagina 422.
Regola di risposta	Opzionale	Una politica può implementare una o più regole per segnalare e risolvere incidenti. Vedere "Informazioni sulle regole di risposta" a pagina 1468.
Eccezione della politica	Opzionale	Una politica può contenere una o più eccezioni per l'esclusione di dati dalla corrispondenza. Vedere "Condizioni di eccezione" a pagina 400.
Condizioni di corrispondenza composte	Opzionale	Una regola o un'eccezione della politica può implementare più condizioni di corrispondenza. Vedere "Condizioni composte" a pagina 401.

Modelli di politica

Symantec Data Loss Prevention fornisce modelli di politica per aiutare a distribuire rapidamente a politiche di rilevamento nella propria azienda. È possibile condividere le politiche su sistemi e ambienti importando ed esportando regole ed eccezioni di politica come modelli.

L'utilizzo dei modelli politica consente di risparmiare tempo ed evitare gli errori e le lacune di informazioni nelle politiche in quanto i metodi di rilevamento sono predefiniti. È possibile modificare un modello per creare una politica che soddisfi pienamente le proprie esigenze. È inoltre possibile esportare e importare i propri modelli di politica.

Alcuni modelli di politica sono basati su insiemi di norme ben noti, come Payment Card Industry Security Standard, Gramm-Leach-Bliley, California SB1386 e HIPAA. Altri modelli di politica sono più generici, come Protezione dei dati dei clienti, Protezione dei dati dei dipendenti e Dati crittografati. Benché i modelli basati su regolamenti possano aiutare ad affrontare i requisiti dei modelli rilevanti, consultare un legale per verificare la conformità.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

[Tabella 16-3](#) descrive i modelli di politica definiti dal sistema forniti da Symantec Data Loss Prevention.

Tabella 16-3 Modelli di politica definiti dal sistema

Tipo del modello di politica	Descrizione
Applicazione normative statunitensi	Vedere "Modelli di politica Applicazione normative statunitensi" a pagina 408.
Regolamento generale per la protezione dei dati	Vedere "Modelli di politica Regolamento generale per la protezione dei dati (GDPR)" a pagina 410.
Applicazione normative internazionali	Vedere "Modelli di politica Applicazione normative internazionali" a pagina 411.
Protezione dei dati di clienti e dipendenti	Vedere "Modelli di politica Protezione dei dati di clienti e dipendenti" a pagina 412.
Protezione dei dati riservati o classificati	Vedere "Modelli di politica Protezione dei dati riservati o classificati" a pagina 413.
Applicazione norme di sicurezza di rete	Vedere "Modelli di politiche Applicazione norme di sicurezza di rete" a pagina 415.
Applicazione norme di utilizzo accettabile	Vedere "Modelli di politica Applicazione norme di utilizzo accettabile" a pagina 415.
Modelli importati	Vedere "Importazione ed esportazione dei modelli politica" a pagina 383.

Pacchetti di soluzioni

Symantec Data Loss Prevention fornisce pacchetti di soluzioni per diversi settori. Un pacchetto di soluzioni contiene politiche configurate, regole di risposta, ruoli utente, report, protocolli e gli stati degli incidenti che supportano un particolare settore o organizzazione. Per un elenco dei pacchetti di soluzioni disponibili e istruzioni, consultare il capitolo 4 della guida *Symantec Data Loss Prevention Installation Guide*. È possibile importare un pacchetto di soluzioni nell'Enforce Server.

Dopo aver importato il pacchetto di soluzioni, iniziare esaminando le politiche. Per impostazione predefinita il pacchetto di soluzioni attiva le politiche che fornisce.

Vedere ["Gestione e aggiunta di politiche"](#) a pagina 444.

Gruppi di politiche

Le politiche vengono distribuite ai server di rilevamento utilizzando gruppi di politiche. I gruppi di politiche limitano le politiche, gli incidenti e i meccanismi di rilevamento accessibili a specifici utenti.

Ogni politica appartiene a un gruppo di politiche. Quando si configura una politica, la si assegna a un gruppo di politiche. È possibile modificare l'assegnazione a un gruppo di politiche, ma non assegnare una politica a più di un gruppo di politiche. I gruppi di politiche sono distribuiti a uno o più server di rilevamento.

Enforce Server è configurato con un singolo gruppo di politiche denominato **Gruppo di politiche predefinite**. Il sistema distribuisce il gruppo di politiche predefinito a tutti i server di rilevamento. Se si definisce una nuova politica, il sistema assegna la politica al gruppo di politiche predefinito, a meno che non si crei e si specifichi un gruppo di politiche differente. È possibile modificare il nome del gruppo di politiche predefinito. Un pacchetto di soluzioni crea vari gruppi di politiche e assegna politiche alle stesse.

Dopo avere creato un gruppo di politiche, è possibile collegare le politiche, i target di Discover e ruoli al gruppo di politiche. Quando si crea un target di Discover, è necessario associarlo a un singolo gruppo di politiche. Quando si associa un ruolo a particolari gruppi di politiche, è possibile limitare gli utenti in quel ruolo. Le politiche in quel gruppo individuano incidenti e li segnalano agli utenti nel ruolo assegnato a quel gruppo di politiche.

La relazione tra i gruppi di politiche e i server di rilevamento dipende dal tipo di server. È possibile distribuire un gruppo di politiche a uno o più Network Monitor, Network Prevent o Endpoint Server. I gruppi di politiche distribuiti a un Endpoint Server si applicano a qualsiasi DLP Agent registrato con quel server. Enforce Server associa automaticamente tutti i gruppi di politiche a tutti i server Network Discover.

Per Network Monitor e Network Prevent, ogni gruppo di politiche è assegnato a uno o più server Network Monitor, Network Prevent for Email o Network Prevent for Web. Per Network Discover, i gruppi di politiche sono assegnati a singoli target di Discover. Un singolo server di rilevamento può gestire tutti i gruppi di politiche necessari per eseguire la scansione dei relativi target. Per Endpoint Monitor, i gruppi di politiche sono assegnati a Endpoint Server e si applicano a tutti i DLP Agent registrati.

Vedere ["Gestione e aggiunta di gruppi di politiche"](#) a pagina 446.

Vedere ["Creazione e modifica di gruppi di politiche"](#) a pagina 447.

Distribuzione di politiche

È possibile usare i gruppi di politiche per organizzare e distribuire le politiche in modi diversi. Ad esempio, considerare una situazione in cui i server di rilevamento sono configurati in un sistema implementato in vari paesi. È possibile usare i gruppi di politiche per assicurarsi che un server di rilevamento esegua solo le politiche valide per una determinata località.

È possibile dedicare alcuni server di rilevamento al monitoraggio del traffico di rete interno e altri server al monitoraggio dei punti di uscita della rete. È possibile usare i gruppi di politiche per distribuire le politiche meno restrittive ai server che controllano il traffico interno. Allo stesso tempo, è possibile distribuire le politiche più rigorose ai server che controllano il traffico in uscita dalla rete.

È possibile usare i gruppi di politiche per organizzare politiche e incidenti in base a divisioni operative, dipartimenti, regioni geografiche o in base a qualsiasi altra unità organizzativa. Ad esempio i gruppi di politiche per dipartimenti specifici possono essere appropriati quando le responsabilità in materia di sicurezza sono distribuite tra vari gruppi. In tali casi i gruppi di politiche offrono un controllo degli accessi basato sui ruoli per la visualizzazione e la modifica degli incidenti. I gruppi di politiche vengono distribuiti in base alla suddivisione dei diritti di accesso richiesta all'interno della organizzazione (ad esempio per unità operativa).

È possibile usare i gruppi di politiche per l'assegnazione del server di rilevamento, che può essere più comune se i dipartimenti di sicurezza sono centralizzati. In tali casi è opportuno scegliere con cura l'assegnazione del server di rilevamento per ciascun ruolo e riportare il nome server nel nome del gruppo di politiche. Ad esempio, è possibile denominare i gruppi In entrata e In Uscita, Italia e Estero o Testing e Produzione.

Negli ambienti più complessi, è possibile considerare una combinazione dei seguenti gruppi di politiche per la distribuzione:

- Vendite e marketing - Stati Uniti
- Vendite e marketing - Europa
- Vendite e marketing - Asia
- Vendite e marketing - Australia, Nuova Zelanda
- Risorse umane - Stati Uniti
- Risorse umane - Internazionale
- Ricerca e sviluppo
- Servizio clienti

Infine è possibile usare i gruppi di politiche per testare le politiche prima della distribuzione negli ambienti di produzione, per gestire le politiche legacy e per importare ed esportare modelli di politica.

Vedere ["Gruppi di politiche"](#) a pagina 377.

Vedere ["Informazioni sul controllo degli accessi basato sul ruolo"](#) a pagina 109.

Gravità delle politiche

Quando si configura una regola di rilevamento, è possibile selezionare un livello di gravità delle politiche. È quindi possibile utilizzare le regole di risposta per intraprendere azioni in base a un livello di gravità. Ad esempio è possibile configurare una regola di risposta per intraprendere azioni dopo un numero specificato di violazioni di gravità alta.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Il livello di gravità predefinito è impostato su "Alta" a meno che non lo si cambi. Il livello di gravità predefinito si applica a qualsiasi condizione a cui corrisponda la regola di rilevamento. Ad esempio, se il livello di gravità predefinito è impostato su "Alta", ogni violazione della regola di rilevamento viene etichettata con questo livello di gravità. Se non si desidera applicare un tag a ogni violazione con una gravità specifica, è possibile definire i criteri in base ai quali è stabilito un livello di gravità. In questo caso il comportamento predefinito viene ignorato. Ad esempio è possibile definire il livello di gravità "Alta" da applicare solo dopo che è stato trovato un numero specificato di corrispondenze di condizioni.

Vedere ["Definizione di gravità della regola"](#) a pagina 430.

Inoltre è possibile definire più livelli di gravità per creare livelli per il reporting di gravità. Ad esempio è possibile impostare il livello di gravità "Alta" per 100 corrispondenze e il livello di gravità medio per 50 corrispondenze.

Tabella 16-4 Livelli di gravità delle regole

Livello di gravità regola	Descrizione
Alta	Se si verifica una corrispondenza di condizioni, viene etichettata con una gravità "Alta".
Media	Se si verifica una corrispondenza di condizioni, viene etichettata con una gravità "Media".
Bassa	Se si verifica una corrispondenza di condizioni, viene etichettata con una gravità "Bassa".
Informazioni	Se si verifica una corrispondenza di condizioni, viene etichettata con una gravità "Informazioni".

Privilegi di creazione politiche

Gli autori di politiche configurano e gestiscono le politiche e le relative regole ed eccezioni. Per creare politiche, un utente deve appartenere a un ruolo che assegna il privilegio di creazione politiche. Questo ruolo può essere espanso per includere la gestione dei gruppi di politiche, degli obiettivi di scansione e delle credenziali.

I privilegi di creazione di regole di risposta sono credenziali separate dai privilegi di creazione e amministrazione di politiche. A seconda delle esigenze aziendali, gli autori delle politiche possono disporre o meno di privilegi per la creazione di regole di risposta.

La [Tabella 16-5](#) descrive i privilegi tipici per i ruoli di creazione di politiche e regole di risposta.

Tabella 16-5 Privilegi di creazione politiche

Privilegio del ruolo	Descrizione
Crea politiche	Aggiungere, configurare e gestire le politiche. Aggiungere, configurare e gestire le regole e le eccezioni della politica. Importare ed esportare i modelli di politica. Modificare gli identificatori dati definiti dal sistema e creare identificatori dati personalizzati. Aggiungere, configurare e gestire i gruppi di utenti. Aggiungere regole di risposta alle politiche (ma non creare regole di risposta). Vedere "Informazioni sul controllo degli accessi basato sul ruolo" a pagina 109.
Amministrazione Enforce Server	Aggiungere, configurare e gestire i gruppi di politiche. Aggiungere, configurare e gestire i profili di dati. Vedere "Ruoli di configurazione" a pagina 114.
Crea regole di risposta	Aggiungere, configurare e gestire le regole di risposta (ma non aggiungerle alle politiche). Vedere "Informazioni sui privilegi di creazione di regole di risposta" a pagina 1485.

Profili dati

I Profili dati sono configurazioni definite dall'utente create per implementare le condizioni delle politiche Exact Data Matching (EDM), Indexed Document Matching (IDM), Form Recognition e Vector Machine Learning (VML).

Vedere ["Tecnologie di rilevamento delle politiche di Data Loss Prevention"](#) a pagina 390.

[Tabella 16-6](#) descrive i tipi di profili dati supportati dal sistema.

Tabella 16-6 Tipi di profili dati

Tipo di profilo dati	Descrizione
Profilo dati esatti	Per le politiche Exact Data Matching è richiesto un Profilo dati esatti. Il Profilo dati esatti contiene i dati che sono stati indicizzati da un'origine dati strutturata, ad esempio un database, un server di directory o un file CSV. Il Profilo dati esatti viene eseguito sul server di rilevamento. Se una politica EDM viene assegnata a un endpoint, il DLP Agent invia il messaggio al server di rilevamento per la valutazione (rilevamento in due fasi). Vedere "Informazioni sul profilo dati esatti e sull'indice" a pagina 478. Vedere "Introduzione a Directory Group Matching (DGM) con profilo" a pagina 855. Vedere "Informazioni sul rilevamento in due fasi per l'EDM sull'endpoint" a pagina 484.

Tipo di profilo dati	Descrizione
Profilo documento indicizzato	<p>Per le politiche Indexed Document Matching (IDM) viene utilizzato un Profilo documento indicizzato. Il Profilo documento indicizzato contiene i dati che sono stati indicizzati da una raccolta di documenti confidenziali. Il Profilo documento indicizzato viene eseguito sul server di rilevamento. Se una politica IDM viene assegnata a un endpoint, il DLP Agent invia il messaggio al server di rilevamento per la valutazione (rilevamento in due fasi).</p> <p>Vedere "Informazioni sul profilo documenti indicizzati" a pagina 572.</p>
Profilo Vector Machine Learning	<p>Per le politiche Vector Machine Learning (VML) viene utilizzato un Profilo Vector Machine Learning. Il Profilo Vector Machine Learning contiene un modello statistico delle funzionalità (parole chiave) estratte dal contenuto che si desidera proteggere. Il profilo VML viene caricato nella memoria dal server di rilevamento e dal DLP Agent. VML non richiede il rilevamento in due fasi.</p> <p>Vedere "Informazioni sul profilo Vector Machine Learning" a pagina 630.</p> <p>Vedere "Informazioni sul profilo Vector Machine Learning" a pagina 630.</p>
Profilo di riconoscimento moduli	<p>Per le politiche di riconoscimento moduli viene utilizzato un profilo di riconoscimento. Il profilo di riconoscimento moduli contiene le immagini vuote dei moduli che si desidera rilevare.</p> <p>Quando si configura un profilo, è necessario specificare il valore numerico che rappresenta la Soglia di riempimento. Si tratta di un valore compreso tra 1 e 10. 1 rappresenta un modulo completato in maniera minima e 10 un modulo completato totalmente. Se la soglia di riempimento viene raggiunta o superata, viene aperto un incidente.</p> <p>Vedere "Gestione dei profili di Riconoscimento moduli" a pagina 668.</p>

Gruppi utente

È possibile definire i gruppi utente in Enforce Server. I gruppi utente contengono informazioni sull'identità degli utenti, che vengono popolate mediante la sincronizzazione di Enforce Server con un server directory di gruppo (Microsoft Active Directory).

Per definire i Gruppi utente è necessario avere almeno privilegi di creazione politiche o di amministratore server. È necessario definire i Gruppi utente prima di sincronizzare gli utenti.

Una volta definito un gruppo utente è possibile popolarlo con gli utenti, i gruppi e le unità aziendali del server di directory. Dopo che il gruppo utente è stato popolato, lo si associa le regole o le eccezioni di rilevamento Utente/Mittente e Destinatario. La politica si applica solo ai membri del Gruppo utente.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

Vedere ["Configurazione delle connessioni a server di directory"](#) a pagina 162.

Vedere ["Configurazione di gruppi di utenti"](#) a pagina 847.

Importazione ed esportazione dei modelli politica

È possibile esportare e importare modelli di politica in Enforce Server. Questa funzionalità consente di condividere modelli di politica tra ambienti, conservare diverse versioni delle politiche esistenti e archiviare le politiche legacy.

Considerare uno scenario in cui l'utente e l'autore rifiniscono una politica su un sistema di test e poi esportano la politica come modello. È possibile importare questo modello di politica in un sistema di produzione per eseguire la distribuzione su uno o più server di rilevamento. In alternativa, se si desidera ritirare una politica, è possibile esportarla come modello per l'archiviazione, quindi rimuoverla dal sistema.

Vedere ["Importazione di modelli di politica"](#) a pagina 453.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Un modello di politica è un file XML. Il modello contiene i metadati della politica, nonché le regole e le eccezioni di rilevamento e del gruppo. Se un modello di politica contiene più di una condizione che richiede un profilo di dati, il sistema importa solo una di queste condizioni. Un modello di politica non include le regole di risposta della politica, o gli identificatori di dati modificati o personalizzati.

[Tabella 16-7](#) descrive i componenti del modello di politica.

Tabella 16-7 Componenti inclusi nei modelli di politica

Componente della politica	Descrizione	Incluso nel modello
Metadati della politica (nome, descrizione, etichetta)	Il nome del modello deve essere inferiore a 60 caratteri, altrimenti non appare nell'elenco Modelli importati .	Sì
Regole ed eccezioni Described Content Matching (DCM)	Se il modello contiene solo metodi DCM, viene importato come esportato senza modifiche.	Sì
Condizioni Exact Data Matching (EDM) e Indexed Document Matching (IDM)	Se il modello contiene più condizioni di corrispondenza EDM o IDM, solo una viene esportata. Se il modello contiene una condizione EDM e una condizione IDM, il sistema ignora l'IDM.	Sì
Gruppo utenti	I metodi del gruppo di utenti vengono mantenuti al momento dell'importazione solo se i gruppi di utenti esistono già sul target.	NO
Gruppo di politiche	I gruppi di politiche non vengono esportati. Al momento dell'importazione è possibile selezionare un gruppo di politiche locale, altrimenti il sistema assegna la politica al gruppo di politiche predefinito.	NO

Componente della politica	Descrizione	Incluso nel modello
Regole di risposta	È necessario definire e aggiungere le regole di risposta alle politiche dall'istanza di Enforce Server.	NO
Profili dati	Al momento dell'importazione è necessario fare riferimento a un profilo di dati definito localmente, altrimenti il sistema ignora gli eventuali metodi che richiedono un profilo di dati.	NO
Identificatori di dati personalizzati	Gli identificatori di dati modificati e personalizzati non vengono esportati.	NO
Protocolli personalizzati	I protocolli personalizzati non vengono esportati.	NO
Stato della politica	Lo stato della politica (Attivo/Sospeso) non viene esportato.	NO

Flusso di lavoro per l'implementazione di politiche

Le politiche definiscono il contenuto, incluso il contesto, e le identità che si desidera rilevare. Le politiche possono anche definire azioni di regola di risposta se una politica viene violata. La creazione di una politica riuscita è un processo che richiede un'analisi attenta e una configurazione adeguata per consentire di ottenere risultati ottimali.

Tabella 16-8 descrive il flusso di lavoro tipico per l'implementazione di politiche di Data Loss Prevention.

Tabella 16-8 Processo di implementazione di una politica

Azione	Descrizione
Acquisire familiarità con i diversi tipi di tecnologie e metodi di rilevazione che Symantec Data Loss Prevention offre e considerazioni per la creazione di politiche di prevenzione di perdita di dati.	Vedere "Rilevamento della perdita di dati" a pagina 387. Vedere "Tecnologie di rilevamento delle politiche di Data Loss Prevention" a pagina 390. Vedere "Condizioni di corrispondenza di politiche" a pagina 392. Vedere "Best practice per la creazione di politiche" a pagina 462.
Sviluppare una strategia di rilevazione della politica che definisce il tipo di dati che si desidera proteggere dalla perdita di dati.	Vedere "Sviluppo di una strategia di politiche che supporti gli obiettivi di protezione dei dati" a pagina 464.
Controllare i modelli di politica forniti con Symantec Data Loss Prevention e tutti i modelli che si importano manualmente o per pacchetto di soluzione.	Vedere "Modelli di politica" a pagina 376. Vedere "Pacchetti di soluzioni" a pagina 377.

Azione	Descrizione
Creare gruppi di politiche per controllare in che modo viene eseguito l'accesso alle politiche e in che modo queste vengono modificate e distribuite.	Vedere "Gruppi di politiche" a pagina 377. Vedere "Distribuzione di politiche" a pagina 378.
Per rilevare dati o contenuto esatti o dati non strutturati simili, creare uno o più profili di dati.	Vedere "Profili dati" a pagina 381.
Per rilevare le identità esatte da un server di directory sincronizzato (Active Directory), configurare uno o più gruppi di utenti.	Vedere "Gruppi utente" a pagina 382.
Configurare le condizioni per il rilevamento e regole ed eccezioni di gruppo.	Vedere "Creazione di una politica a partire da un modello" a pagina 405.
Verificare e ottimizzare le politiche.	Vedere "Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze" a pagina 466.
Aggiungere regole di risposta alla politica per effettuare un'azione quando la politica viene violata.	Vedere "Informazioni sulle regole di risposta" a pagina 1468.
Gestire le politiche nella propria azienda.	Vedere "Gestione e aggiunta di politiche" a pagina 444.

Visualizzazione, stampa e download dei dettagli della politica

Potrebbe essere necessario condividere dettagli di alto livello riguardo alle politiche con persone che non sono utenti Symantec Data Loss Prevention. Ad esempio, potrebbe essere richiesto di fornire dettagli relativi alla politica a un responsabile della sicurezza delle informazioni all'interno della propria azienda o al revisore esterno della sicurezza. Per facilitare tale operazione, è possibile visualizzare e stampare i dettagli della politica in un formato facilmente leggibile nella schermata **Elenco politiche**. La vista dei dettagli della politica non include alcuna nomenclatura tecnica o specifica personalizzazione in Symantec Data Loss Prevention. Consente di visualizzare il nome della politica, la descrizione, l'etichetta, il gruppo, lo stato, la versione e la data di ultima modifica della politica. Inoltre, visualizza il rilevamento e le regole di risposta per quella determinata politica.

Qualsiasi utente che dispone del privilegio Crea politiche per una data politica o un insieme di politiche può visualizzare e stampare i dettagli della politica.

Vedere ["Privilegi di creazione politiche"](#) a pagina 380.

[Tabella 16-9](#) descrive come utilizzare i dettagli della politica.

Tabella 16-9 Utilizzo dei dettagli della politica

Azione	Descrizione
Visualizzazione e stampa di dettagli di una singola politica.	Vedere " Visualizzazione e stampa dei dettagli della politica " a pagina 456.
Scaricare i dettagli per tutte le politiche.	Vedere " Download dei dettagli delle politiche " a pagina 457.

Panoramica di rilevazione di politica

Il capitolo contiene i seguenti argomenti:

- [Rilevamento della perdita di dati](#)
- [Tecnologie di rilevamento delle politiche di Data Loss Prevention](#)
- [Condizioni di corrispondenza di politiche](#)
- [Messaggi di rilevamento e componenti di messaggio](#)
- [Condizioni di eccezione](#)
- [Condizioni composte](#)
- [Esecuzione del rilevamento di politiche](#)
- [Rilevamento in due fasi per DLP Agent.](#)

Rilevamento della perdita di dati

Symantec Data Loss Prevention rileva i dati da praticamente qualsiasi tipo di messaggio o file, qualsiasi utente, mittente o destinatario, ovunque si trovino i dati o gli endpoint. È possibile utilizzare Data Loss Prevention per rilevare i contenuti e il contesto di dati all'interno dell'azienda. Definire e gestire le politiche di rilevamento dalla console di amministrazione Enforce Server centralizzata basata su Web.

Vedere ["Contenuto che può essere rilevato"](#) a pagina 388.

Vedere ["File che possono essere rilevati"](#) a pagina 388.

Vedere ["Protocolli che è possibile monitorare"](#) a pagina 388.

Vedere ["Eventi endpoint che possono essere rilevati"](#) a pagina 389.

Vedere ["Identità che possono essere rilevate"](#) a pagina 389.

Vedere ["Lingue che possono essere rilevate"](#) a pagina 389.

Contenuto che può essere rilevato

Symantec Data Loss Prevention rileva il contenuto di documenti e dati, tra cui testo, markup, presentazioni, fogli elettronici, file di archivio e il relativo contenuto, messaggi di posta elettronica, file di database, progetti e file grafica, file multimediali, moduli basati su immagini e altro. Ad esempio, il sistema può aprire un file compresso e cercare la parola chiave "riservato" in un documento di Microsoft Word che si trova nel file compresso. Se la parola chiave viene trovata, il motore di rilevamento contrassegna il messaggio come incidente.

Il rilevamento del contenuto è basato sul contenuto vero e proprio e non sul file. Un server di rilevamento può rilevare estratti o derivati di contenuto protetto o descritto. Questo contenuto può includere sezioni di documenti che sono state copiate e incollate in altri documenti o e-mail. Un server di rilevamento può anche identificare dati riservati in un formato di file differente dal file di origine. Ad esempio, se si crea l'impronta di un file Word riservato, il motore di rilevamento può trovare la corrispondenza con il contenuto inviato via e-mail in un collegamento PDF.

Vedere ["Condizioni per la corrispondenza del contenuto"](#) a pagina 393.

File che possono essere rilevati

Symantec Data Loss Prevention riconosce molti tipi di file e allegati in base al relativo contesto, ovvero tipo di file, nome di file e dimensione del file. Symantec Data Loss Prevention identifica più di 300 tipi di file, tra cui formati di elaborazione di testo, file multimediali, fogli elettronici, presentazioni, immagini, formati di incapsulamento, formati di crittografia e altri.

Per il rilevamento del tipo di file, il sistema non considera l'estensione di file. Ad esempio, il sistema riconosce un file di Microsoft Word anche se un utente cambia l'estensione in .txt. In questo caso, il motore di rilevamento controlla la firma binaria del file per identificare il tipo.

Vedere ["Condizioni corrispondenze delle proprietà file"](#) a pagina 395.

Protocolli che è possibile monitorare

Symantec Data Loss Prevention rileva i messaggi sulla rete identificando la firma di protocollo: e-mail (SMTP), Web (HTTP), trasferimento di file (FTP), newsgroup (NNTP), TCP, Telnet e SSL.

È possibile configurare un server di rilevamento per ascoltare sulle porte non predefinite le violazioni di perdita di dati. Ad esempio, se la rete trasmette il traffico Web sulla porta 81 anziché la porta 80, il sistema continua a riconoscere il contenuto trasmesso come HTTP.

Vedere ["Condizione di corrispondenza di protocolli per la rete"](#) a pagina 396.

Eventi endpoint che possono essere rilevati

Symantec Data Loss Prevention consente di individuare le violazioni di perdite di dati in varie destinazioni endpoint. Queste destinazioni comprendono l'unità locale, unità CD/DVD, dispositivi di archiviazione rimovibili, condivisioni file di rete, Appunti Windows, stampanti e fax e file di applicazioni. È anche possibile rilevare eventi di protocollo sull'endpoint per e-mail (SMTP), Web (HTTP) e trasferimento di file (FTP).

Ad esempio, DLP Agent (installato su ogni computer endpoint) può rilevare la copia di un file riservato in un dispositivo USB. Oppure DLP Agent può consentire la copia di file solo in una specifica classe di dispositivo USB che soddisfa i requisiti di crittografia dell'azienda.

Vedere ["Condizioni di corrispondenza endpoint"](#) a pagina 396.

Identità che possono essere rilevate

Symantec Data Loss Prevention consente di rilevare l'identità di utenti di dati, mittenti di messaggi e destinatari di messaggi utilizzando vari metodi. Questi metodi includono criteri di identità descritte e identità esatte con corrispondenze in un server di directory o in un database aziendale.

Ad esempio, è possibile rilevare messaggi e-mail inviati da un utente specifico, oppure consentire messaggi e-mail inviati a o da un gruppo specifico di utenti come definito nel server Microsoft Active Directory in uso.

Vedere ["Condizioni per la corrispondenza tra gruppi \(identità\)"](#) a pagina 397.

Lingue che possono essere rilevate

Symantec Data Loss Prevention fornisce un vasto supporto internazionale per il rilevamento di perdite di dati in molte lingue. Le lingue supportate sono la maggior parte delle lingue dell'Europa Occidentale e Centrale, l'ebreo, l'arabo, il cinese (semplificato e tradizionale), il giapponese, il coreano e altre ancora.

Il motore di rilevamento utilizza il formato Unicode. È possibile creare regole ed eccezioni di politiche localizzate utilizzando qualsiasi tecnologia di rilevamento in qualunque lingua supportata.

Vedere ["Lingue supportate per il rilevamento"](#) a pagina 90.

Vedere ["Rilevazione del contenuto in lingua non inglese"](#) a pagina 802.

Tecnologie di rilevamento delle politiche di Data Loss Prevention

Symantec Data Loss Prevention fornisce vari tipi di tecnologie di rilevamento per agevolare la creazione di politiche con cui rilevare perdite di dati. Ogni tipo di tecnologia di rilevamento fornisce funzionalità uniche. Spesso si combinano varie tecnologie nelle politiche per ottenere risultati di rilevamento accurati. Inoltre, Symantec Data Loss Prevention fornisce vari metodi per estendere il rilevamento di politiche e trovare corrispondenze con qualsiasi tipo di dati, contenuto o file.

Vedere ["Informazioni sulle politiche di Data Loss Prevention"](#) a pagina 373.

Vedere ["Best practice per la creazione di politiche"](#) a pagina 462.

[Tabella 17-1](#) elenca i vari tipi di tecnologie di rilevamento e le personalizzazioni fornite da Data Loss Prevention.

Tabella 17-1 Tecnologie di rilevamento di Data Loss Prevention

Tecnologia	Descrizione
Exact Data Matching (EDM)	Utilizzare EDM per rilevare informazioni che consentono l'identificazione dell'utente. Vedere "Introduzione all'Exact Data Matching (EDM)" a pagina 473.
Indexed Document Matching (IDM)	Utilizzare IDM per rilevare contenuto di file e file esatti e contenuto derivato. Vedere "Introduzione a Indexed Document Matching (IDM)" a pagina 569.
Vector Machine Learning (VML)	Utilizzare VML per rilevare contenuto di documenti simile. Vedere "Introduzione a Vector Machine Learning (VML)" a pagina 629.
Riconoscimento moduli	Utilizzare Riconoscimento moduli per rilevare immagini di moduli che appartengono a una galleria associata a una politica Riconoscimento moduli. Vedere "Informazioni sul rilevamento Riconoscimento moduli" a pagina 662.
Directory Group Matching (DGM)	Utilizzare DGM per rilevare identità esatte sincronizzate a partire da un server di directory o con profilo definito da un database. Vedere "Introduzione a Directory Group Matching (DGM) sincronizzato" a pagina 846. Vedere "Introduzione a Directory Group Matching (DGM) con profilo" a pagina 855.

Tecnologia	Descrizione
Described Content Matching (DCM)	<p>Utilizzare DCM per rilevare il contenuto e il contesto di messaggi, tra cui:</p> <ul style="list-style-type: none"> ■ Identificatori di dati per la corrispondenza con contenuto utilizzando criteri e convalide di dati precisi. Vedere "Introduzione agli identificatori di dati" a pagina 681. ■ Parole chiave per rilevare contenuto utilizzando parole chiave, frasi chiave e dizionari di parole chiave. Vedere "Introduzione alla corrispondenza con parole chiave" a pagina 771. ■ Espressioni regolari per rilevare caratteri, criteri e stringhe. Vedere "Introduzione alla corrispondenza con espressioni regolari" a pagina 787. ■ Proprietà di file per rilevare file per tipo, nome, dimensione e tipo. Vedere "Introduzione al rilevamento di proprietà di file" a pagina 808. ■ Criteri utente, mittente e destinatario per rilevare identità descritte. Vedere "Introduzione alla corrispondenza con identità descritte" a pagina 835. ■ Firme di protocollo per rilevare traffico di rete. Vedere "Introduzione al monitoraggio di protocolli per la rete" a pagina 821. ■ Destinazioni, dispositivi e protocolli per rilevare eventi endpoint. Vedere "Introduzione al rilevamento di eventi endpoint" a pagina 824.
Information Centric Tagging (ICT)	<ul style="list-style-type: none"> ■ Classificazioni per rilevare i tag Information Centric Tagging Vedere "Introduzione alla corrispondenza di classificazione" a pagina 793.

Tecnologia	Descrizione
Metodi di rilevamento di politiche personalizzati	<p>Data Loss Prevention fornisce metodi per la personalizzazione e l'estensione del rilevamento, tra cui:</p> <ul style="list-style-type: none"> ■ Identificatori di dati personalizzati Implementare i propri criteri di identificatori di dati e convalide definite dal sistema. Vedere "Introduzione agli identificatori di dati" a pagina 681. ■ Convalide script personalizzate per identificatori di dati Utilizzare il linguaggio di script di Symantec Data Loss Prevention per convalidare tipi di dati personalizzati. Vedere "Flusso di lavoro per la creazione di identificatori di dati personalizzati" a pagina 749. ■ Identificazione di tipi di file personalizzati Utilizzare il linguaggio di script di Symantec Data Loss Prevention per rilevare tipi di file personalizzati. Vedere "Informazioni sull'identificazione di tipi di file personalizzati" a pagina 809. ■ Rilevamento personalizzato di dispositivi endpoint Rilevare qualsiasi dispositivo endpoint mediante espressioni regolari. Vedere "Informazioni sul rilevamento di dispositivi endpoint" a pagina 826. ■ Rilevamento di protocolli di rete personalizzati Definire porte TCP personalizzate. Vedere "Introduzione al monitoraggio di protocolli per la rete" a pagina 821. ■ Estrazione di contenuto personalizzato Utilizzare un plug-in per identificare formati di file personalizzati ed estrarre contenuto di file per l'analisi mediante il server di rilevamento. Vedere "Panoramica del supporto del formato di file di rilevamento" a pagina 876.

Condizioni di corrispondenza di politiche

Symantec Data Loss Prevention fornisce vari tipi di condizioni di corrispondenza, ognuna delle quali offre funzionalità di rilevamento uniche. Le condizioni di corrispondenza vengono implementate nelle politiche come regole o eccezioni. Le regole di rilevamento utilizzano le condizioni per la corrispondenza con il contenuto o il contesto dei messaggi. Le regole di gruppo utilizzano le condizioni per la corrispondenza con le identità. È anche possibile utilizzare le condizioni come eccezioni delle politiche di gruppo e di rilevamento.

Vedere ["Condizioni di eccezione"](#) a pagina 400.

[Tabella 17-2](#) elenca i vari tipi di condizioni di corrispondenza di politiche presenti in Data Loss Prevention.

Tabella 17-2 Tipi di condizioni di corrispondenza di politiche

Tipo di condizione	Descrizione
Contenuto	Vedere "Condizioni per la corrispondenza del contenuto" a pagina 393.
Proprietà file	Vedere "Condizioni corrispondenze delle proprietà file" a pagina 395.
Protocollo	Vedere "Condizione di corrispondenza di protocolli per la rete" a pagina 396.
Endpoint	Vedere "Condizioni di corrispondenza endpoint" a pagina 396.
Gruppi (identità)	Vedere "Condizioni per la corrispondenza tra gruppi (identità)" a pagina 397.

Condizioni per la corrispondenza del contenuto

Symantec Data Loss Prevention fornisce varie condizioni per la corrispondenza del contenuto dei messaggi. Alcune condizioni per il contenuto richiedono un profilo dati e un indice associati. Per il rilevamento del contenuto, determinate condizioni consentono di definire la corrispondenza con i singoli componenti del messaggio, inclusi l'intestazione, il corpo, gli allegati e l'oggetto.

Vedere ["Messaggi di rilevamento e componenti di messaggio"](#) a pagina 398.

Vedere ["Contenuto che può essere rilevato"](#) a pagina 388.

La [Tabella 17-3](#) elenca le condizioni di corrispondenza del contenuto che è possibile utilizzare senza un profilo dati e un indice.

Tabella 17-3 Condizioni per la corrispondenza del contenuto

Tipo di regola contenuto	Descrizione
Contenuto corrispondente a espressione regolare	Stabilisce la corrispondenza con il contenuto indicato mediante espressioni regolari. Vedere "Introduzione alla corrispondenza con espressioni regolari" a pagina 787. Vedere "Configurazione della condizione Contenuto corrispondente a espressione regolare" a pagina 789.
Contenuto corrispondente a parola chiave	Stabilisce la corrispondenza con il contenuto indicato mediante parole chiave, frasi chiave e dizionari di parole chiave Vedere "Introduzione alla corrispondenza con parole chiave" a pagina 771. Vedere "Configurazione della condizione Contenuto corrispondente a parola chiave" a pagina 779.

Tipo di regola contenuto	Descrizione
Contenuto corrispondente a identificatore dati	<p>Stabilisce la corrispondenza con il contenuto indicato mediante criteri e convalide Identificatore dati.</p> <p>Vedere "Introduzione agli identificatori di dati" a pagina 681.</p> <p>Vedere "Configurazione della condizione Contenuto corrispondente a identificatore dati" a pagina 700.</p>
Classificazione corrispondenze contenuto	<p>Abbina i contenuti descritti utilizzando file ed e-mail con tag Information Centric Tagging.</p> <p>Vedere "Introduzione alla corrispondenza di classificazione" a pagina 793.</p>

La [Tabella 17-4](#) elenca le condizioni per la corrispondenza del contenuto che richiedono un profilo dati e un indice.

Vedere ["Profili dati"](#) a pagina 381.

Vedere ["Rilevamento in due fasi per DLP Agent."](#) a pagina 403.

Tabella 17-4 Condizioni per la corrispondenza del contenuto basate sull'indice

Tipo di regola contenuto	Descrizione
Il contenuto corrisponde ai dati esatti da un profilo dati esatti (EDM)	<p>Stabilisce la corrispondenza con i dati profilo esatti derivati da un'origine dati strutturata quale un database o un file CSV.</p> <p>Vedere "Introduzione all'Exact Data Matching (EDM)" a pagina 473.</p> <p>Vedere "Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti" a pagina 503.</p> <p>Nota: Questa condizione richiede il rilevamento in due fasi sull'endpoint. Vedere "Informazioni sul rilevamento in due fasi per l'EDM sull'endpoint" a pagina 484.</p>
Il contenuto corrisponde alla firma del documento di un profilo documento indicizzato (IDM)	<p>Stabilisce la corrispondenza esatta o parziale con file e contenuti di file mediante l'impronta digitale</p> <p>Vedere "Introduzione a Indexed Document Matching (IDM)" a pagina 569.</p> <p>Vedere "Configurazione della condizione di politica Contenuto corrispondente a firma documento" a pagina 605.</p> <p>Nota: Questa condizione richiede il rilevamento in due fasi sull'endpoint. Vedere "Informazioni sul profilo documenti indicizzati" a pagina 572.</p>

Tipo di regola contenuto	Descrizione
Rileva utilizzando il profilo Vector Machine Learning (VML)	<p>Stabilisce la corrispondenza del contenuto del file con caratteristiche simili al contenuto di esempio oggetto del training.</p> <p>Vedere "Introduzione a Vector Machine Learning (VML)" a pagina 629.</p> <p>Vedere "Configurazione della condizione Rileva utilizzando il profilo Vector Machine Learning" a pagina 645.</p>

Condizioni corrispondenze delle proprietà file

Symantec Data Loss Prevention fornisce varie condizioni per la corrispondenza con le proprietà dei file, inclusi il tipo di file, le dimensioni file e il nome file.

Vedere ["File che possono essere rilevati"](#) a pagina 388.

Tabella 17-5 Condizioni delle corrispondenze delle proprietà file

Tipo di condizione	Descrizione
Corrispondenza allegato messaggio o tipo file	<p>Rileva la corrispondenza con formati file e allegati di documenti specifici.</p> <p>Vedere "Informazioni sulla corrispondenza con tipi di file" a pagina 808.</p> <p>Vedere "Configurazione della condizione Corrispondenza allegato messaggio o tipo file." a pagina 812.</p>
Corrispondenza allegato messaggio o dimensioni file	<p>Rileva la corrispondenza con file o collegamenti di dimensioni superiori o inferiori a una dimensione specificata.</p> <p>Vedere "Informazioni sulla corrispondenza di dimensione di file" a pagina 810.</p> <p>Vedere "Configurazione della condizione Corrispondenza allegato messaggio o dimensioni file" a pagina 813.</p>
Corrispondenza allegato messaggio o nome file	<p>Rileva la corrispondenza con file o collegamenti con un nome specifico o caratteri jolly specifici.</p> <p>Vedere "Informazioni sulla corrispondenza del nome del file" a pagina 811.</p> <p>Vedere "Configurazione della condizione Corrispondenza allegato messaggio o nome file" a pagina 815.</p>
Proprietà e attributi messaggio/e-mail	<p>Classifica i messaggi e-mail di Microsoft Exchange in base a specifici attributi del messaggio (attributi MAPI).</p>

Tipo di condizione	Descrizione
Firma tipi di file personalizzati	Rileva la corrispondenza con tipi di file personalizzati sulla base della firma binaria mediante gli script. Vedere "Informazioni sull'identificazione di tipi di file personalizzati" a pagina 809. Vedere "Attivazione della condizione Firma tipi di file personalizzati nella console della politica" a pagina 817.

Condizione di corrispondenza di protocolli per la rete

Symantec Data Loss Prevention fornisce la condizione singola **Monitoraggio protocolli** per la corrispondenza del traffico di rete per le regole di rilevamento delle politiche e le eccezioni.

Vedere ["Protocolli che è possibile monitorare"](#) a pagina 388.

Tabella 17-6 Condizione di corrispondenza di protocolli per il monitoraggio della rete

Condizione di corrispondenza	Descrizione
Monitoraggio di protocolli	Cercare la corrispondenza degli incidenti sulla rete trasmessi utilizzando un protocollo specificato, tra cui SMTP, FTP, HTTP/S, IM e NNTP. Vedere "Introduzione al monitoraggio di protocolli per la rete" a pagina 821. Vedere "Configurazione della condizione Monitoraggio protocollo per il rilevamento nella rete" a pagina 822.

Condizioni di corrispondenza endpoint

Symantec Data Loss Prevention fornisce diverse condizioni per la corrispondenza di eventi endpoint.

Vedere ["Eventi endpoint che possono essere rilevati"](#) a pagina 389.

Tabella 17-7 Condizioni di corrispondenza endpoint

Condizione	Descrizione
Monitoraggio protocollo o endpoint	Cerca la corrispondenza dei messaggi endpoint trasmessi con un protocollo di trasporto specificato o quando i dati vengono spostati o copiati in una determinata destinazione. Vedere "Introduzione al rilevamento di eventi endpoint" a pagina 824. Vedere "Configurazione della condizione di monitoraggio dell'endpoint" a pagina 827.

Condizione	Descrizione
Classe o ID dispositivo endpoint	<p>Cerca la corrispondenza di eventi endpoint su dispositivi hardware specificati.</p> <p>Vedere "Introduzione al rilevamento di eventi endpoint" a pagina 824.</p> <p>Vedere "Configurazione della condizione Classe o ID dispositivo endpoint" a pagina 830.</p>
Posizione endpoint	<p>Cerca la corrispondenza di eventi endpoint a seconda che DLP Agent sia o meno sulla rete aziendale.</p> <p>Vedere "Introduzione al rilevamento di eventi endpoint" a pagina 824.</p> <p>Vedere "Configurazione della condizione Posizione endpoint" a pagina 829.</p>

Condizioni per la corrispondenza tra gruppi (identità)

Symantec Data Loss Prevention fornisce varie condizioni per definire la corrispondenza dell'identità di utenti e gruppi e di mittenti e destinatari di messaggi.

Le regole del criterio del destinatario e del mittente sono riutilizzabili da una politica all'altra. Le regole Directory Group Matching (DGM) consentono di definire la corrispondenza in base a mittenti e destinatari derivati da Directory (DGM sincronizzata) o da un profilo dati esatti (DGM con profilo).

Vedere ["Identità che possono essere rilevate"](#) a pagina 389.

Vedere ["Rilevamento in due fasi per DLP Agent."](#) a pagina 403.

Tabella 17-8 Regole di gruppo disponibili per la corrispondenza di identità

Regola di gruppo	Descrizione
Mittente/utente corrisponde a criterio	<p>Definisce la corrispondenza di mittenti e utenti di messaggi mediante indirizzo e-mail, ID utente, nome schermata IM e indirizzo IP.</p> <p>Vedere "Introduzione alla corrispondenza con identità descritte" a pagina 835.</p> <p>Vedere "Configurazione della condizione Mittente/utente corrisponde a criterio" a pagina 837.</p>
Destinatario corrisponde a criterio	<p>Definisce la corrispondenza di destinatari mediante e-mail, indirizzo IP o dominio Web.</p> <p>Vedere "Introduzione alla corrispondenza con identità descritte" a pagina 835.</p> <p>Vedere "Configurazione della condizione Destinatario corrispondente a criterio" a pagina 840.</p>

Regola di gruppo	Descrizione
Mittente/utente basato su gruppo di server di directory	<p>Definisce la corrispondenza di mittenti e utenti di messaggi da un server di directory sincronizzato.</p> <p>Vedere "Introduzione a Directory Group Matching (DGM) sincronizzato" a pagina 846.</p> <p>Vedere "Configurazione della condizione Mittente/utente basato su gruppo di server di directory" a pagina 851.</p>
Mittente/utente basato su una directory di: un profilo di dati esatto	<p>Definisce la corrispondenza di mittenti e utenti da un server di directory con profilo.</p> <p>Vedere "Introduzione a Directory Group Matching (DGM) con profilo" a pagina 855.</p> <p>Vedere "Configurazione del Mittente/Utente in base a una condizione della Profiled Directory" a pagina 858.</p> <p>Nota: Questa condizione richiede il rilevamento in due fasi sull'endpoint. Vedere "Informazioni sul rilevamento in due fasi per DGM con profilo" a pagina 856.</p>
Destinatario basato su gruppo di server di directory	<p>Definisce la corrispondenza di destinatari da un server di directory sincronizzato.</p> <p>Vedere "Introduzione a Directory Group Matching (DGM) sincronizzato" a pagina 846.</p> <p>Vedere "Configurazione della condizione Destinatario basato su gruppo di server di directory" a pagina 852.</p> <p>Nota: Questa condizione richiede il rilevamento in due fasi sull'endpoint. Vedere "Informazioni sul rilevamento in due fasi per DGM sincronizzata" a pagina 847.</p>
Destinatario basato su una directory di: un profilo di dati esatto	<p>Definisce la corrispondenza di destinatari da un server di directory con profilo.</p> <p>Vedere "Configurazione di profili dati esatti per DGM" a pagina 856.</p> <p>Vedere "Configurazione del destinatario in base a una condizione Profiled Directory" a pagina 859.</p> <p>Nota: Questa condizione richiede il rilevamento in due fasi sull'endpoint. Vedere "Informazioni sul rilevamento in due fasi per DGM con profilo" a pagina 856.</p>

Messaggi di rilevamento e componenti di messaggio

I server di rilevazione di Data Loss Prevention e DLP Agent ricevono i dati di input per l'analisi sotto forma di messaggi. Il sistema determina il tipo di messaggio, ad esempio, un'e-mail o un documento Word. A seconda del tipo di messaggio, il sistema analizza il contenuto del messaggio nei componenti (intestazione, oggetto, corpo, allegati), o lascia il messaggio intatto. Il sistema valuta il messaggio o i componenti del messaggio per verificare se vengono applicate condizioni per la corrispondenza della politica. Se una condizione viene applicata e supporta la corrispondenza del componente, il sistema confronta il contenuto con ogni componente del messaggio selezionato. Se la condizione non supporta la corrispondenza del componente, il sistema valuta l'intero messaggio in base alla condizione di corrispondenza.

Vedere ["Selezione dei componenti per la corrispondenza"](#) a pagina 433.

Le condizioni basate sul contenuto supportano la corrispondenza del componente trasversale. È possibile configurare le condizioni del contenuto DCM per cercare la corrispondenza in tutti i componenti del messaggio. La condizione EDM cerca la corrispondenza in busta, corpo e allegati del messaggio. Le condizioni del documento cercano la corrispondenza nel corpo e negli allegati del messaggio, fatta eccezione per Tipo file e Nome che cercano corrispondenza solo nell'allegato. Le condizioni di protocollo, endpoint e identità cercano la corrispondenza nell'intero messaggio, come tutte le condizioni valutate da DLP Agent. Il componente dell'oggetto viene applicato solo alle e-mail SMTP o ai messaggi NNTP.

[Tabella 17-9](#) riassume la corrispondenza del componente supportata da ogni tipo di condizione di corrispondenza.

Tabella 17-9 Componenti del messaggio per i quali eseguire la corrispondenza

Tipo condizione	Busta	Oggetto	Corpo	Allegati
Condizioni Described Content Matching (DCM) per rilevamento di contenuti: Parola chiave, Identificatore dati, Espressione regolare	corrispondenza	corrispondenza	corrispondenza	corrispondenza
Classificazioni di Information Centric Tagging (ICT) per il rilevamento di contenuto: Classificazione	corrispondenza			corrispondenza
Exact Data Matching (EDM)	corrispondenza		corrispondenza	corrispondenza
Indexed Document Matching (IDM)			corrispondenza	corrispondenza
Vector Machine Learning (VML)			corrispondenza	corrispondenza
Riconoscimento moduli				corrispondenza
Dimensione del file (DCM)			corrispondenza	corrispondenza
Tipo file e nome file (DCM)				corrispondenza
Protocollo (DCM)	corrispondenza (intero messaggio)			
Endpoint (DCM)	corrispondenza (intero messaggio)			
Identità (DCM e DGM)	corrispondenza (intero messaggio)			

Tipo condizione	Busta	Oggetto	Corpo	Allegati
Qualsiasi condizione valutata da DLP Agent				corrispondenza (intero messaggio)

Condizioni di eccezione

Symantec Data Loss Prevention fornisce eccezioni della politica per escludere messaggi e componenti dei messaggi dalla corrispondenza. È possibile usare le condizioni di eccezione per definire ulteriormente l'ambito delle regole di gruppo e di rilevamento.

Vedere ["Utilizzo di un numero limitato di eccezioni per restringere l'ambito di rilevamento"](#) a pagina 468.

Avvertimento: Non utilizzare più eccezioni composte in una singola politica. Il rilevamento potrebbe esaurire la memoria. Se si rileva che la politica richiede più eccezioni composte per produrre le corrispondenze, è necessario riconsiderare la progettazione delle condizioni di corrispondenza.

Il sistema valuta un messaggio o un componente del messaggio in arrivo rispetto alle eccezioni prima che rispetto alle regole della politica. Se l'eccezione supporta la corrispondenza su diversi componenti (eccezioni basate sul contenuto), può essere configurata per la corrispondenza con singoli componenti del messaggio. Altrimenti, l'eccezione rileverà la corrispondenza con l'intero messaggio.

Se un'eccezione viene soddisfatta, il sistema esclude l'intero messaggio o il componente del messaggio che comprende il contenuto che ha attivato l'eccezione. Il messaggio o il componente del messaggio escluso non è più disponibile per la valutazione rispetto alle regole della politica. Il sistema non scarta solo l'elemento di dati o il contenuto con il quale è stata rilevata la corrispondenza, bensì l'intero messaggio o componente del messaggio che contiene l'oggetto associato all'eccezione.

Nota: Symantec Data Loss Prevention non supporta le eccezioni di livello corrispondenza, ma solo le eccezioni di livello componente o messaggio.

Ad esempio, si consideri una politica con una regola di rilevamento che include una condizione e un'eccezione con una condizione. La regola rileva la corrispondenza con i messaggi contenenti allegati di Microsoft Word e genera un incidente per ogni corrispondenza. L'eccezione esclude dalla corrispondenza i messaggi con mittente `ceo@company.com`. Un e-mail con mittente `ceo@company.com` che contiene un allegato di Word viene escluso dalla corrispondenza e non attiva un incidente. L'eccezione di rilevamento che esclude i messaggi di `ceo@company.com`

ha la precedenza sulla condizione di corrispondenza con regola di rilevamento che altrimenti rileverebbe una corrispondenza con questo messaggio.

Vedere ["Esecuzione del rilevamento di politiche"](#) a pagina 402.

È possibile implementare come eccezione qualsiasi condizione, meno la condizione EDM II **contenuto corrisponde ai dati esatti da**. Inoltre Network Prevent for Web non supporta le eccezioni DGM sincronizzate. È possibile implementare IDM come eccezione, ma l'eccezione esclude dalla corrispondenza i file esatti, non i contenuti dei file. Per escludere i contenuti del file è necessario aggiungerli a una lista bianca. VML può essere usato come eccezione se il contenuto appartiene alla stessa categoria.

Vedere ["Aggiunta di un'eccezione a una politica"](#) a pagina 434.

Vedere ["Modello di politica CAN-SPAM Act"](#) a pagina 1321.

Vedere ["Creazione di una lista bianca di contenuto di file da escludere dalla corrispondenza parziale"](#) a pagina 585.

Condizioni composte

Una politica valida deve dichiarare almeno una regola che definisce almeno una condizione di corrispondenza. La condizione cerca la corrispondenza con i dati specificati per rilevare perdite di dati. Una regola con una singola condizione è una regola semplice. Facoltativamente, è possibile dichiarare molteplici condizioni in una singola regola di gruppo o di rilevamento. Una regola con molteplici condizioni è una condizione composta.

Per le condizioni composte, ogni condizione nella regola deve essere vera per generare una violazione. Quindi, per una singola politica che dichiara una regola con due condizioni, se una condizione è vera e l'altra no, il rilevamento non segnala una corrispondenza. Se entrambe le condizioni sono vere, il rilevamento segnala una corrispondenza, purché la regola sia configurata per conteggiare tutte le corrispondenze. In termini programmatici, due o più condizioni nella stessa regola sono unite con AND.

Come avviene con le regole, è possibile dichiarare più condizioni in una singola eccezione. In questo caso, tutte le condizioni nell'eccezione devono essere vere perché l'eccezione venga applicata.

Vedere ["Esecuzione del rilevamento di politiche"](#) a pagina 402.

Vedere ["Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza."](#) a pagina 469.

Vedere ["Condizioni di eccezione"](#) a pagina 400.

Esecuzione del rilevamento di politiche

È possibile includere qualsiasi combinazione di regole di rilevamento, regole di gruppo ed eccezioni in una singola politica. Un server di rilevamento valuta prima le eccezioni di politica. Se viene soddisfatta un'eccezione, l'intero messaggio o il componente del messaggio che corrisponde all'eccezione viene escluso e non è più disponibile per la corrispondenza di politiche.

Il server di rilevamento valuta le regole di rilevamento e di gruppo nella politica in base a una regola. In termini programmatici, se si dispone della definizione di una singola politica, la connessione tra le condizioni nella stessa regola o eccezione è AND (condizioni composte). La connessione tra due o più regole dello stesso tipo è OR (ad esempio, 2 regole di rilevamento). Però, se si combinano regole di tipo diverso in una singola politica (ad esempio, 1 regola di rilevamento e 1 regola di gruppo), la connessione tra le regole è AND. In questa configurazione entrambe le regole devono corrispondere per attivare un incidente. Tuttavia le condizioni di eccezione create nelle scheda "Rilevamento" e "Gruppi" sono connesse da una condizione OR implicita.

Vedere ["Condizioni composte"](#) a pagina 401.

Vedere ["Condizioni di eccezione"](#) a pagina 400.

La [Tabella 17-10](#) riepiloga la logica di esecuzione delle condizioni di politica per il server di rilevamento per varie configurazioni di politica.

Tabella 17-10 Logica di esecuzione delle condizioni di politica

Configurazione politica	Logica	Descrizione
Condizioni composte	AND	Se una singola regola o eccezione in una politica contiene due o più condizioni di corrispondenza, tutte le condizioni devono corrispondere.
Regole o eccezioni dello stesso tipo	OR	Se vi sono due regole di rilevamento in una singola politica, due regole di gruppo in una singola politica o due eccezioni dello stesso tipo (rilevamento o gruppo), le regole o le eccezioni sono indipendenti tra loro.
Regole di tipo diverso	AND	Se una o più regole di rilevamento vengono combinate con una o più regole di gruppo in una singola politica, le regole sono dipendenti.
Eccezioni di tipo diverso	OR	Se una o più eccezioni di rilevamento vengono combinate con una o più eccezioni di gruppo in una singola politica, le eccezioni sono indipendenti.

Rilevamento in due fasi per DLP Agent.

Symantec Data Loss Prevention usa un'architettura di rilevamento in due fasi per analizzare l'attività negli endpoint associata a determinate condizioni di corrispondenza basate su indice.

Il rilevamento in due fasi richiede la comunicazione e il trasferimento di dati tra DLP Agent e Endpoint Server per il rilevamento degli incidenti. Se una condizione di corrispondenza richiede il rilevamento in due fasi, la condizione non viene valutata localmente sull'endpoint da DLP Agent. DLP Agent invia i dati a Endpoint Server per la valutazione della politica.

Vedere ["Linee guida per la creazione di politiche endpoint"](#) a pagina 2035.

Con il rilevamento in due fasi la valutazione della politica registra un ritardo pari al tempo necessario per l'invio e la valutazione dei dati in Endpoint Server. Se DLP Agent non è collegato alla rete o non è in grado di comunicare con Endpoint Server, la condizione che richiede il rilevamento in due fasi non viene valutata fino a quando DLP Agent non si connette. Tale ritardo può ridurre le prestazioni di DLP Agent se il messaggio è un file o un allegato di grandi dimensioni.

Vedere ["Risoluzione dei problemi delle politiche"](#) a pagina 458.

Il rilevamento in due fasi ha implicazioni sui tipi di politiche create per gli endpoint. È possibile ridurre il potenziale collo di bottiglia rappresentato dal rilevamento in due fasi analizzando in dettaglio le condizioni di rilevamento che richiedono il rilevamento in due fasi e creando le politiche per l'endpoint che contribuiscano a eliminare o ridurre l'esigenza del rilevamento in due fasi.

Vedere ["Creazione di politiche per limitare l'effetto potenziale del rilevamento in due fasi"](#) a pagina 469.

La [Tabella 17-11](#) elenca le condizioni di rilevamento che richiedono il rilevamento in due fasi sull'endpoint.

Nota: Quando è attivato il rilevamento in due fasi, non è possibile combinare una regola di risposta Endpoint Prevent: notifica o Endpoint Prevent: blocca con condizioni di rilevamento in due fasi, incluse Exact Data Matching (EDM), Directory Group Matching (DGM) e Indexed Document Matching (IDM). Se si fa ciò, il sistema visualizza un avviso sia per la condizione di rilevamento sia per la regola di risposta.

Tabella 17-11 Condizioni di corrispondenza delle politiche che richiedono il rilevamento in due fasi

Tecnologia di rilevamento	Condizione di corrispondenza	Descrizione
Exact Data Matching (EDM)	Il contenuto corrisponde ai dati esatti da un profilo dati esatti	Vedere "Introduzione all'Exact Data Matching (EDM)" a pagina 473. Vedere "Informazioni sul rilevamento in due fasi per l'EDM sull'endpoint" a pagina 484.
Directory Group Matching (DGM) con profilo	Mittente/utente basato su una directory di un profilo dati esatti	Vedere "Introduzione a Directory Group Matching (DGM) con profilo" a pagina 855.
	Destinatario basato su una directory di un profilo dati esatti	Vedere "Informazioni sul rilevamento in due fasi per DGM con profilo" a pagina 856.
Directory Group Matching (DGM) sincronizzata	Destinatario basato su gruppo di server di directory	Vedere "Introduzione a Directory Group Matching (DGM) sincronizzato" a pagina 846. Vedere "Informazioni sul rilevamento in due fasi per DGM sincronizzata" a pagina 847.
Indexed Document Matching (IDM)	Il contenuto corrisponde alla firma del documento di un profilo documenti indicizzati	Vedere "Introduzione a Indexed Document Matching (IDM)" a pagina 569. Vedere "Rilevamento IDM in due fasi" a pagina 572. Nota: Il rilevamento in due fasi per IDM può essere implementato solo se è attivato su Endpoint Server (two_tier_idm = on). Se è attivato Endpoint IDM (two_tier_idm = off), il rilevamento in due fasi non viene utilizzato.

Creazione di politiche dai modelli

Il capitolo contiene i seguenti argomenti:

- [Creazione di una politica a partire da un modello](#)
- [Modelli di politica Applicazione normative statunitensi](#)
- [Modelli di politica Regolamento generale per la protezione dei dati \(GDPR\)](#)
- [Modelli di politica Applicazione normative internazionali](#)
- [Modelli di politica Protezione dei dati di clienti e dipendenti](#)
- [Modelli di politica Protezione dei dati riservati o classificati](#)
- [Modelli di politiche Applicazione norme di sicurezza di rete](#)
- [Modelli di politica Applicazione norme di utilizzo accettabile](#)
- [Modello di politica Applicazione normative colombiane relative ai dati personali](#)
- [Scelta di un profilo dati esatti](#)
- [Scelta di un profilo documento indicizzato](#)

Creazione di una politica a partire da un modello

È possibile creare una politica da un modello fornito dal sistema o da un modello importato in Enforce Server.

Vedere ["Modelli di politica"](#) a pagina 376.

Vedere ["Importazione ed esportazione dei modelli politica"](#) a pagina 383.

Tabella 18-1 Creazione di una politica a partire da un modello

Azione	Descrizione
Aggiungere una politica da un modello.	Vedere "Aggiunta di una nuova politica o di un modello di politica" a pagina 421.
Scegliere il modello che si desidera utilizzare.	<p>Nella schermata Gestisci > Politiche > Elenco politiche > Nuova politica - Elenco modelli, il sistema elenca tutti i modelli di politica.</p> <p>Categorie di modelli fornite dal sistema:</p> <ul style="list-style-type: none"> ■ Vedere "Modelli di politica Applicazione normative statunitensi" a pagina 408. ■ Vedere "Modelli di politica Regolamento generale per la protezione dei dati (GDPR)" a pagina 410. ■ Vedere "Modelli di politica Applicazione normative internazionali" a pagina 411. ■ Vedere "Modelli di politica Protezione dei dati di clienti e dipendenti" a pagina 412. ■ Vedere "Modelli di politica Protezione dei dati riservati o classificati" a pagina 413. ■ Vedere "Modelli di politiche Applicazione norme di sicurezza di rete" a pagina 415. ■ Vedere "Modelli di politica Applicazione norme di utilizzo accettabile" a pagina 415. ■ Vedere "Modello di politica Applicazione normative colombiane relative ai dati personali" a pagina 417. <p>I modelli importati vengono visualizzati individualmente dopo l'importazione:</p> <ul style="list-style-type: none"> ■ Vedere "Importazione di modelli di politica" a pagina 453.
Fare clic su Avanti per configurare la politica.	<p>Ad esempio, selezionare il modello di politica Webmail e fare clic su Avanti.</p> <p>Vedere "Configurazione di politiche" a pagina 422.</p>
Scegliere un profilo di dati (se richiesto).	<p>Se il modello si basa su uno o più profili di dati, il sistema richiede di selezionare:</p> <ul style="list-style-type: none"> ■ Profilo dati esatti Vedere "Scelta di un profilo dati esatti" a pagina 417. ■ Profilo documento indicizzato Vedere "Scelta di un profilo documento indicizzato" a pagina 419. <p>Se non si dispone di un profilo di dati, è possibile:</p> <ul style="list-style-type: none"> ■ Annullare il processo di definizione della politica, definire il profilo e ricominciare a creare la politica dal modello. ■ Fare clic su Avanti per configurare la politica. Al momento della creazione della politica, il sistema ignora le eventuali regole o eccezioni che si basano sul profilo di dati. <p>Nota: È necessario utilizzare un profilo se un modello lo richiede.</p>

Azione	Descrizione
Modificare il nome o la descrizione della politica (facoltativo).	<p>Se si intende modificare un modello definito dal sistema, è possibile cambiare il nome in modo da poterlo distinguere dall'originale.</p> <p>Vedere "Configurazione di politiche" a pagina 422.</p> <p>Nota: Se si desidera esportare la politica come modello, il nome della politica deve essere di meno di 60 caratteri. Se è più lungo, il modello non viene visualizzato nella sezione Modelli importati della schermata Elenco modelli.</p> <p>Nota: Il campo Etichetta politica è riservato al portale di supporto autonomo di Veritas Data Insight.</p>
Selezionare un gruppo di politiche (se necessario).	<p>Se è stato definito un gruppo di politiche, selezionarlo dall'elenco Gruppo di politiche.</p> <p>Vedere "Creazione e modifica di gruppi di politiche" a pagina 447.</p> <p>Se non è stato definito un gruppo di politiche, il sistema distribuisce la politica al Gruppo di politiche predefinite.</p>
Modificare le regole o le eccezioni della politica (se necessario).	<p>La schermata Configura politica visualizza le regole e le eccezioni (se presenti) fornite dalla politica.</p> <p>È possibile modificare, aggiungere e rimuovere le regole e le eccezioni della politica a seconda delle esigenze.</p> <p>Vedere "Configurazione di regole di politica" a pagina 427.</p> <p>Vedere "Configurazione delle eccezioni di politica" a pagina 437.</p>
Salvare la politica ed esportarla (facoltativo).	<p>Fare clic su Salva per salvare la politica.</p> <p>È possibile esportare il rilevamento di politiche come modello a scopo di condivisione o archiviazione.</p> <p>Vedere "Esportazione del rilevamento di politiche come modello" a pagina 454.</p> <p>Ad esempio, se si è cambiata la configurazione di un modello di politica definito dal sistema, è possibile esportarlo per condividerlo in altri ambienti.</p>
Testare e ottimizzare la politica (raccomandato).	<p>Testare e ottimizzare la politica utilizzando dei dati che la politica deve e non deve rilevare.</p> <p>Esaminare gli incidenti generati dalla politica. Definire ulteriormente le regole e le eccezioni della politica secondo necessità per ridurre i falsi positivi e i falsi negativi.</p>
Aggiungere una regola di risposta (facoltativo).	<p>Aggiungere regole di risposta alla politica per segnalare e riparare le violazioni.</p> <p>Vedere "Implementazione di regole di risposta" a pagina 1486.</p> <p>Nota: Le regole di risposta non sono incluse nei modelli di politica.</p>

Modelli di politica Applicazione normative statunitensi

Symantec Data Loss Prevention fornisce diversi modelli di politica a supporto delle linee guida relative all'applicazione delle normative statunitensi.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Tabella 18-2 Modelli di politica Applicazione normative statunitensi

Modello di politica	Descrizione
CAN-SPAM Act	Stabilisce i requisiti per l'invio di e-mail commerciali. Vedere "Modello di politica CAN-SPAM Act" a pagina 1321.
Classificazione GENSER Defense Message System (DMS)	Rileva le informazioni classificate come riservate. Vedere "Modello di politica Classificazione GENSER Defense Message System (DMS)" a pagina 1331.
Export Administration Regulations (EAR, normativa sulla gestione delle esportazioni)	Applica la normativa sulla gestione delle esportazioni del Dipartimento del Commercio statunitense. Vedere "Modello di politica Export Administration Regulations (EAR)" a pagina 1335.
FACTA 2003 (regole Red Flag)	Applica le sezioni 114 e 315 (o regole Red Flag) della normativa Fair and Accurate Credit Transactions Act (FACTA) del 2003. Vedere "Modello di politica FACTA 2003 (regole Red Flag)" a pagina 1337.
Gramm-Leach-Bliley	Questa politica limita la condivisione delle informazioni sul consumatore da parte degli istituti finanziari. Vedere "Modello di politica Gramm-Leach-Bliley" a pagina 1414.
HIPAA e HITECH (incluso PHI)	Questa politica applica l'Health Insurance Portability and Accountability Act (HIPAA - Legge sulla trasferibilità e gli obblighi di rendere conto in materia di copertura assicurativa) degli Stati Uniti. Vedere "Modello di politica HIPAA e HITECH (incluso PHI)" a pagina 1416.
International Traffic in Arms Regulations (ITAR, normativa sul traffico internazionale di armi)	Questa politica applica le disposizioni ITAR del Dipartimento di Stato degli Stati Uniti. Vedere "Modello di politica International Traffic in Arms Regulations (ITAR)" a pagina 1422.

Modello di politica	Descrizione
Medicare e Medicaid (incluso PHI)	Questa politica rileva le informazioni sanitarie protette (PHI) associate ai programmi Medicare e Medicaid degli Stati Uniti. Vedere "Medicare e Medicaid (incluso PHI)" a pagina 1424.
Regola NASD 2711 e regole NYSE 351 e 472	Questa politica protegge i nomi delle società coinvolte in un'offerta di azioni imminente. Vedere "Modello di politica Regola NASD 2711 e regole NYSE 351 e 472" a pagina 1427.
Regola NASD 3010 e regola NYSE 342	Questa politica monitora le comunicazioni tra gli operatori di borsa. Vedere "Modello di politica Regola NASD 3010 e regola NYSE 342" a pagina 1428.
Linee guida sulla sicurezza del NERC per le società elettriche	Questa politica rileva le informazioni che sono descritte nelle linee guida sulla sicurezza del NERC (North American Electric Reliability Council) per il settore elettrico. Vedere "Modello di politica Linee guida sulla sicurezza del NERC per le società elettriche" a pagina 1430.
OFAC (Ufficio per il Controllo dei Fondi Stranieri)	Questo modello rileva le comunicazioni che coinvolgono i gruppi OFAC mirati. Vedere "Modello di politica OFAC (Ufficio per il Controllo dei Fondi Stranieri)" a pagina 1433.
Memorandum OMB 06-16 e disposizioni FIPS 199	Questo modello rileva le informazioni che sono classificate come riservate. Vedere "Modello di politica Memorandum OMB 06-16 e disposizioni FIPS 199" a pagina 1436.
Payment Card Industry Data Security Standard	Questo modello rileva i dati dei numeri delle carte di credito. Vedere "Modello della politica Payment Card Industry (PCI) Data Security Standard" a pagina 1437.
Sarbanes-Oxley	Questo modello rileva i dati finanziari riservati. Vedere "Modello della politica Sarbanes-Oxley" a pagina 1445.
Normativa sull'imparzialità della trasparenza SEC	Questo modello rileva la divulgazione di informazioni finanziarie concrete. Vedere "Modello della politica Normativa sull'imparzialità della trasparenza SEC" a pagina 1447.

Modello di politica	Descrizione
Privacy dei dati relativi allo stato	Questo modello rileva le violazioni di riservatezza imposte dallo stato. Vedere "Modello di privacy dei dati relativi allo stato" a pagina 1451.
Marchi di controllo dei servizi di intelligence degli Stati Uniti (CAPCO) e DCID 1/7	Questo modello rileva i termini autorizzati per identificare le informazioni classificate nella US Intelligence Community. Vedere "Marchi di controllo dei servizi di intelligence degli Stati Uniti (CAPCO) e modello della politica DCID 1/7" a pagina 1458.

Modelli di politica Regolamento generale per la protezione dei dati (GDPR)

Il Regolamento generale per la protezione dei dati (GDPR) è un regolamento con cui la Commissione europea vuole rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. Tratta inoltre dell'esportazione dei dati personali all'esterno dell'UE. Gli obiettivi principali del GDPR sono di restituire ai cittadini il controllo sui propri dati personali e di semplificare le norme per le aziende internazionali unificando i regolamenti all'interno dell'UE. Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Symantec Data Loss Prevention fornisce numerosi modelli di politica per la conformità al Regolamento generale per la protezione dei dati (General Data Protection Regulation, GDPR).

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Tabella 18-3

Modello di politica	Descrizione
Regolamenti generali per la protezione dei dati (attività bancarie e finanza)	Questa politica protegge le informazioni personali identificabili relative ad attività bancarie e finanza. Vedere "Regolamento generale per la protezione dei dati (attività bancarie e finanza)" a pagina 1342.
Regolamento generale per la protezione dei dati (identità digitale)	Questa politica protegge le informazioni personali identificabili relative all'identità digitale. Vedere "Regolamento generale per la protezione dei dati (identità digitale)" a pagina 1364.
Regolamento generale per la protezione dei dati (identificazione governativa)	Questa politica protegge le informazioni personali identificabili relative all'identificazione governativa. Vedere "Regolamento generale per la protezione dei dati (identificazione governativa)" a pagina 1365.

Modello di politica	Descrizione
Regolamento generale per la protezione dei dati (sanità e assicurazioni)	Questa politica protegge le informazioni personali identificabili relative a sanità e assicurazioni. Vedere "Regolamento generale per la protezione dei dati (sanità e assicurazioni)" a pagina 1389.
Regolamento generale per la protezione dei dati (profilo personale)	Questa politica protegge le informazioni personali identificabili relative al profilo personale. Vedere "Regolamento generale per la protezione dei dati (profilo personale)" a pagina 1401.
Regolamento generale per la protezione dei dati (viaggi)	Questa politica protegge le informazioni personali identificabili relative ai viaggi. Vedere "Regolamento generale per la protezione dei dati (viaggi)" a pagina 1404.

Modelli di politica Applicazione normative internazionali

Symantec Data Loss Prevention fornisce vari modelli di politica per l'applicazione di normative internazionali.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Tabella 18-4 Modelli di politica Applicazione normative internazionali

Modello di politica	Descrizione
Relazione Caldicott	Questa politica protegge le informazioni dei pazienti britannici. Vedere "Modello della politica Relazione Caldicott" a pagina 1319.
Data Protection Act (legge sulla protezione dei dati) del 1998	Questa politica protegge le informazioni personali identificabili. Vedere "Modello della politica Data Protection Act 1998 (legge sulla protezione dei dati del 1998)" a pagina 1327.
Direttive UE sulla protezione dei dati	Questa politica rileva i dati personali a cui si fa riferimento nelle direttive UE. Vedere "Modello della politica Direttive UE sulla protezione dei dati" a pagina 1329. Nota: Le Direttive UE sulla protezione dei dati sono state sostituite dal Regolamento generale per la protezione dei dati (GDPR) il 25 maggio 2018. Vedere "Modelli di politica Regolamento generale per la protezione dei dati (GDPR)" a pagina 410.

Modello di politica	Descrizione
Human Rights Act (legge sui diritti umani) del 1998	Questa politica implementa l'articolo 8 della legge per i cittadini britannici. Vedere " Modello di politica Human Rights Act (legge sui diritti umani) del 1998 " a pagina 1421.
PIPEDA	Questa politica rileva i dati cliente dei cittadini canadesi. Vedere " Modello di politica PIPEDA " a pagina 1439.

Modelli di politica Protezione dei dati di clienti e dipendenti

Symantec Data Loss Prevention fornisce diversi modelli di politica Protezione dei dati di clienti e dipendenti.

Vedere "[Creazione di una politica a partire da un modello](#)" a pagina 405.

Tabella 18-5 Modelli di politica Protezione dei dati di clienti e dipendenti

Modello di politica	Descrizione
Numeri di previdenza sociale canadesi (SIN)	Questa politica rileva i criteri indicanti numeri di previdenza sociale canadesi. Vedere " Modello della politica Numeri di previdenza sociale (SIN) canadesi " a pagina 1321.
Numeri di carta di credito	Questa politica rileva i criteri indicanti numeri di carta di credito. Vedere " Modello della politica Numeri di carta di credito " a pagina 1325.
Protezione dei dati dei clienti	Questa politica rileva i dati dei clienti. Vedere " Modello di politica Protezione dei dati dei clienti " a pagina 1325.
Protezione dei dati dei dipendenti	Questa politica rileva i dati dei dipendenti. Vedere " Modello di politica Protezione dei dati dei dipendenti " a pagina 1333.
Codici identificativi dei contribuenti (ITIN)	Questa politica rileva i numeri di elaborazione delle imposte rilasciati dall'IRS. Vedere " Modello della politica Codici identificativi dei contribuenti (ITIN) " a pagina 1422.

Modello di politica	Descrizione
Codici SWIFT	Questa politica rileva i codici che le banche utilizzano per trasferire denaro oltre i confini nazionali. Vedere "Modello della politica Codici SWIFT" a pagina 1455.
Numeri delle patenti di guida britanniche	Questa politica rileva i numeri delle patenti di guida britanniche. Vedere "Modello della politica Numeri Patente di guida del Regno Unito" a pagina 1456.
Numeri di tessera elettorale britannici	Questa politica rileva i numeri delle tessere elettorali britanniche. Vedere "Modello politica Numeri di tessera elettorale britannici" a pagina 1456.
Numeri di previdenza sociale britannici	Questa politica rileva i numeri di previdenza sociale britannici. Vedere "Modello della politica Numeri di previdenza sociale britannici" a pagina 1457.
Numero NHS (National Health Service) britannico	Questa politica rileva i numeri di identificazione personale rilasciati dal servizio sanitario nazionale (NHS) britannico. Vedere "Modello della politica Numero NHS (National Health Service) britannico" a pagina 1457.
Numeri di passaporto britannici	Questa politica rileva i passaporti britannici validi. Vedere "Modello della politica Numeri di passaporto britannici" a pagina 1457.
Codici fiscali britannici	Questa politica rileva i codici fiscali britannici. Vedere "Modello di politica Codici fiscali britannici" a pagina 1458.
Social Security Number statunitensi	Questa politica rileva i criteri indicanti i Social Security Number statunitensi. Vedere "Modello di politica Social Security Number statunitense" a pagina 1460.

Modelli di politica Protezione dei dati riservati o classificati

Symantec Data Loss Prevention fornisce diversi modelli di politica per Protezione dei dati riservati o classificati.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Tabella 18-6 Modelli di politica Protezione dei dati riservati o classificati

Modello di politica	Descrizione
Documenti riservati	Questa politica rileva i documenti aziendali riservati. Vedere "Modello della politica Documenti riservati" a pagina 1324.
Documenti di progettazione	Questa politica rileva diversi tipi di documenti di progettazione. Vedere "Modello della politica Documenti di progettazione" a pagina 1332.
Dati crittografati	Questa politica rileva l'utilizzo della crittografia mediante una serie di metodi. Vedere "Modello della politica Dati crittografati" a pagina 1335.
Informazioni finanziarie	Questa politica rileva informazioni e dati finanziari. Vedere "Modello di politica Informazioni finanziarie" a pagina 1340.
Contratti di acquisizione e fusione	Questa politica rileva informazioni e comunicazioni relative alle attività di acquisizione e fusione imminenti. Vedere "Modello della politica Contratti di acquisizione e fusione" a pagina 1426.
Informazioni sui prezzi	Questa politica rileva informazioni specifiche su SKU e prezzi. Vedere "Modello di politica Informazioni sui prezzi" a pagina 1441.
Dati di progetto	Questa politica rileva le discussioni relative ai progetti riservati. Vedere "Modello della politica Dati di progetto" a pagina 1441.
File multimediali proprietari	Questa politica rileva diversi tipi di file audio e video. Vedere "Modello di politica File multimediali proprietari" a pagina 1441.
Documenti di pubblicazione	Questa politica rileva diversi tipi di documenti di pubblicazione. Vedere "Modello della politica Documenti di pubblicazione" a pagina 1442.
Curriculum	Questa politica rileva le ricerche di lavoro attive. Vedere "Modello della politica Curriculum" a pagina 1444.
Codice sorgente	Questa politica rileva diversi tipi di codice sorgente. Vedere "Modello di politica Codice sorgente" a pagina 1450.
Compatibilità Symantec DLP e prevenzione	Questa politica rileva eventuali comunicazioni relative a Symantec DLP o altri sistemi di prevenzione della perdita di dati e a un'eventuale prevenzione del rilevamento. Vedere "Modello della politica Compatibilità Symantec DLP e Prevenzione" a pagina 1455.

Modelli di politiche Applicazione norme di sicurezza di rete

Symantec Data Loss Prevention fornisce vari modelli di politica per Applicazione norme di sicurezza di rete.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Tabella 18-7 Modelli di politiche Applicazione norme di sicurezza di rete

Modello di politica	Descrizione
Siti caricamento spyware comuni	Questa politica rileva l'accesso ai siti Web di caricamento spyware comuni. Vedere "Modello politica Siti caricamento spyware comuni" a pagina 1323.
Diagrammi di rete	Questa politica rileva i diagrammi di rete dei computer. Vedere "Modello della politica Diagrammi di rete" a pagina 1432.
Sicurezza di rete	Questa politica rivela la prova di strumenti di hacking e piani di attacco. Vedere "Modello della politica Sicurezza di rete" a pagina 1433.
File di password	Questa politica rileva i formati di file di password. Vedere "Modello della politica File di password" a pagina 1437.

Modelli di politica Applicazione norme di utilizzo accettabile

Symantec Data Loss Prevention fornisce diversi modelli di politica per consentire l'utilizzo di informazioni accettabile.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Tabella 18-8 Modelli di politica Applicazione norme di utilizzo accettabile

Modello di politica	Descrizione
Comunicazioni con i concorrenti	Questa politica rileva le comunicazioni non consentite con i concorrenti. Vedere "Modello di politica Comunicazioni con i concorrenti" a pagina 1323.
Siti Web non consentiti	Questa politica rileva l'accesso ai siti Web specificati. Vedere "Modello della politica Siti Web non consentiti" a pagina 1341.

Modello di politica	Descrizione
Gioco d'azzardo	Questa politica rileva eventuali riferimenti al gioco d'azzardo. Vedere "Modello politica Gioco d'azzardo" a pagina 1342.
Sostanze illegali	Questa politica rileva le conversazioni relative a sostanze illegali e sostanze controllate. Vedere "Modello di politica Sostanze illegali" a pagina 1421.
File multimediali	Questa politica rileva diversi tipi di file audio e video. Vedere "Modello della politica File multimediali" a pagina 1424.
Linguaggio offensivo	Questa politica rileva l'utilizzo di linguaggio offensivo. Vedere "Modello di politica Linguaggio offensivo" a pagina 1433.
Linguaggio razzista	Questa politica rileva l'utilizzo di linguaggio razzista. Vedere "Modello politica Linguaggio razzista" a pagina 1443.
File con restrizioni	Questa politica rileva diversi tipi di file generalmente inadatti alla divulgazione al di fuori dell'azienda. Vedere "Modello della politica File con restrizioni" a pagina 1443.
Destinatari con restrizioni	Questa politica rileva le comunicazioni con i destinatari specificati. Vedere "Modello della politica Destinatari con restrizioni" a pagina 1443.
Linguaggio sessualmente esplicito	Questa politica rileva contenuto sessualmente esplicito. Vedere "Modello di politica Linguaggio sessualmente esplicito" a pagina 1449.
Violenza e armi	Questa politica rileva l'utilizzo di linguaggio violento e le discussioni in merito alle armi. Vedere "Modello della politica Violenza e armi" a pagina 1460.
Webmail	Questa politica rileva l'utilizzo di una serie di servizi di Webmail. Vedere "Modello della politica di Webmail" a pagina 1460.
Attività della bacheca messaggi di Yahoo	Questa politica rileva l'attività della bacheca messaggi di Yahoo. Vedere "Modello di politica Attività della bacheca messaggi di Yahoo" a pagina 1462.
Yahoo e MSN Messenger sulla porta 80	Questa politica rileva l'attività di Yahoo IM e MSN Messenger. Vedere "Modello di politica Yahoo e MSN Messenger sulla porta 80" a pagina 1463.

Modello di politica Applicazione normative colombiane relative ai dati personali

Symantec Data Loss Prevention fornisce i modelli di politica per l'applicazione delle normative colombiane relative ai dati personali.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Tabella 18-9 Modello di politica Applicazione normative colombiane relative ai dati personali

Modello di politica	Descrizione
Legge colombiana 1581 sulla protezione dei dati personali	<p>Questa politica rileva le violazioni alla legge colombiana 1581 sulla protezione dei dati personali.</p> <p>Vedere "Modello della politica della legge colombiana sulla protezione dei dati personali 1581" a pagina 1322.</p>

Scelta di un profilo dati esatti

Se il modello di politica selezionato implementa Exact Data Matching (EDM), il sistema richiede la selezione di un profilo dati esatti. [Tabella 18-10](#) elenca i modelli di politica basati sui profili dati esatti.

Se non si dispone di un profilo dati esatti, è possibile annullare la creazione della politica e definire un profilo. Oppure, è possibile scegliere di non usare un profilo dati esatti. In questo caso il sistema disattiva le regole di rilevamento EDM associate nel modello di politica. È possibile usare qualsiasi regola o eccezione DCM fornita dal modello di politica.

Vedere ["Introduzione all'Exact Data Matching \(EDM\)"](#) a pagina 473.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Per scegliere un profilo dati esatti

- 1 Selezionare **Profilo dati esatti** dall'elenco di profili disponibili.
- 2 Fare clic su **Avanti** per creare la politica dal modello.
Fare clic su **Indietro** per ritornare all'elenco di modelli di politica.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Nota: Quando il sistema richiede la selezione di un profilo dati esatti, vengono elencate le colonne di dati da includere nel profilo per fornire il più alto livello di accuratezza. Se i campi di dati nel profilo dati esatti non sono rappresentati nel modello di politica selezionato, il sistema visualizza quei campi per la corrispondenza con il contenuto quando si definisce la regola di rilevamento.

Tabella 18-10 Criteri di politica che implementano Exact Data Matching (EDM)

Criterio di politica	Descrizione
Relazione Caldicott	Vedere "Modello della politica Relazione Caldicott" a pagina 1319.
Protezione dei dati dei clienti	Vedere "Modello di politica Protezione dei dati dei clienti" a pagina 1325.
Data Protection Act (legge sulla protezione dei dati) del 1988	Vedere "Modello della politica Data Protection Act 1998 (legge sulla protezione dei dati del 1998)" a pagina 1327.
Protezione dei dati dei dipendenti	Vedere "Modello di politica Protezione dei dati dei dipendenti" a pagina 1333.
Direttive UE sulla protezione dei dati	Vedere "Modello della politica Direttive UE sulla protezione dei dati" a pagina 1329.
Export Administration Regulations (EAR, normativa sulla gestione delle esportazioni)	Vedere "Modello di politica Export Administration Regulations (EAR)" a pagina 1335.
FACTA 2003 (regole Red Flag)	Vedere "Modello di politica FACTA 2003 (regole Red Flag)" a pagina 1337.
Regolamenti generali per la protezione dei dati (attività bancarie e finanza)	Vedere "Regolamento generale per la protezione dei dati (attività bancarie e finanza)" a pagina 1342.
Regolamenti generali per la protezione dei dati (identità digitale)	Vedere "Regolamento generale per la protezione dei dati (identità digitale)" a pagina 1364.
Regolamenti generali per la protezione dei dati (identificazione governativa)	Vedere "Regolamento generale per la protezione dei dati (identificazione governativa)" a pagina 1365.
Regolamenti generali per la protezione dei dati (sanità e assicurazioni)	Vedere "Regolamento generale per la protezione dei dati (sanità e assicurazioni)" a pagina 1389.
Regolamenti generali per la protezione dei dati (profilo personale)	Vedere "Regolamento generale per la protezione dei dati (profilo personale)" a pagina 1401.
Regolamenti generali per la protezione dei dati (viaggi)	Vedere "Regolamento generale per la protezione dei dati (viaggi)" a pagina 1404.
Gramm-Leach-Bliley	Vedere "Modello di politica Gramm-Leach-Bliley" a pagina 1414.
HIPAA e HITECH (incluso PHI)	Vedere "Modello di politica HIPAA e HITECH (incluso PHI)" a pagina 1416.
Human Rights Act (legge sui diritti umani) del 1998	Vedere "Modello di politica Human Rights Act (legge sui diritti umani) del 1998" a pagina 1421.
International Traffic in Arms Regulations (ITAR, normativa sul traffico internazionale di armi)	Vedere "Modello di politica International Traffic in Arms Regulations (ITAR)" a pagina 1422.

Criterio di politica	Descrizione
Payment Card Industry Data Security Standard	Vedere "Modello della politica Payment Card Industry (PCI) Data Security Standard" a pagina 1437.
PIPEDA	Vedere "Modello di politica PIPEDA" a pagina 1439.
Informazioni sui prezzi	Vedere "Modello di politica Informazioni sui prezzi" a pagina 1441.
Curriculum	Vedere "Modello della politica Curriculum" a pagina 1444.
Privacy dei dati relativi allo stato	Vedere "Modello della politica Normativa sull'imparzialità della trasparenza SEC" a pagina 1447.

Scelta di un profilo documento indicizzato

Se il modello di politica scelto utilizza il rilevamento IDM, il sistema richiede la selezione di un profilo documento.

Vedere ["Introduzione a Indexed Document Matching \(IDM\)"](#) a pagina 569.

Per usare un profilo documento

- 1 Selezionare **Profilo documento** dall'elenco di profili disponibili.
- 2 Fare clic su **Avanti** per creare la politica dal modello.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Se non si dispone di un profilo documento, è possibile annullare la creazione della politica e definire il profilo documento. Oppure, è possibile scegliere di non usare un profilo documento. In questo caso il sistema disattiva tutte le regole o eccezioni IDM per l'istanza della politica. Se il modello di politica contiene regole o eccezioni DCM, è possibile usarle.

Vedere ["Informazioni sul profilo documenti indicizzati"](#) a pagina 572.

Tabella 18-11 Modelli di politica che implementano il rilevamento IDM

Modello di politica	Descrizione
CAN-SPAM Act (eccezione IDM)	Vedere "Modello di politica CAN-SPAM Act" a pagina 1321.
Regola NASD 2711 e regole NYSE 351 e 472	Vedere "Modello di politica Regola NASD 2711 e regole NYSE 351 e 472" a pagina 1427.
Linee guida sulla sicurezza del NERC per le società elettriche	Vedere "Modello di politica Linee guida sulla sicurezza del NERC per le società elettriche" a pagina 1430.
Sarbanes-Oxley	Vedere "Modello della politica Sarbanes-Oxley" a pagina 1445.

Modello di politica	Descrizione
Normativa sull'imparzialità della trasparenza SEC	Vedere " Modello della politica Normativa sull'imparzialità della trasparenza SEC " a pagina 1447.
Documenti riservati	Vedere " Modello della politica Documenti riservati " a pagina 1324.
Documenti di progettazione	Vedere " Modello della politica Documenti di progettazione " a pagina 1332.
Informazioni finanziarie	Vedere " Modello di politica Informazioni finanziarie " a pagina 1340.
Dati di progetto	Vedere " Modello della politica Dati di progetto " a pagina 1441.
File multimediali proprietari	Vedere " Modello di politica File multimediali proprietari " a pagina 1441.
Documenti di pubblicazione	Vedere " Modello della politica Documenti di pubblicazione " a pagina 1442.
Codice sorgente	Vedere " Modello di politica Codice sorgente " a pagina 1450.
Diagrammi di rete	Vedere " Modello della politica Diagrammi di rete " a pagina 1432.

Configurazione di politiche

Il capitolo contiene i seguenti argomenti:

- [Aggiunta di una nuova politica o di un modello di politica](#)
- [Configurazione di politiche](#)
- [Aggiunta di una regola a una politica](#)
- [Configurazione di regole di politica](#)
- [Definizione di gravità della regola](#)
- [Configurazione del conteggio delle corrispondenze](#)
- [Selezione dei componenti per la corrispondenza](#)
- [Aggiunta di un'eccezione a una politica](#)
- [Configurazione delle eccezioni di politica](#)
- [Configurazione delle condizioni di corrispondenza composte](#)
- [Limiti di immissione caratteri per la configurazione di politiche](#)

Aggiunta di una nuova politica o di un modello di politica

L'autore di una politica può definire una nuova politica da zero o a partire da un modello.

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

Per aggiungere una nuova politica o un modello di politica

- 1 Fare clic su **Nuovo** nella schermata **Gestisci > Politiche > Elenco politiche**.
Vedere ["Gestione e aggiunta di politiche"](#) a pagina 444.
- 2 Scegliere il tipo di politica che si desidera aggiungere alla schermata **Nuova politica**.
Selezionare **Aggiungere una politica vuota** per aggiungere una nuova politica vuota.
Vedere ["Componenti della politica"](#) a pagina 375.
Selezionare **Aggiungere una politica da un modello** per aggiungere una politica da un modello.
Vedere ["Modelli di politica"](#) a pagina 376.
- 3 Fare clic su **Avanti** per configurare la politica o il modello di politica.
Vedere ["Configurazione di politiche"](#) a pagina 422.
Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.
Fare clic su **Annulla** per non aggiungere una politica e ritornare alla schermata **Elenco politiche**.

Configurazione di politiche

La schermata **Gestisci > Politiche > Elenco politiche > Configura politica** è la pagina iniziale per la configurazione delle politiche.

[Tabella 19-1](#) descrive il flusso di lavoro per la configurazione delle politiche.

Tabella 19-1 Configurazione di politiche

Azione	Descrizione
Definire una nuova politica o modificare una politica esistente.	Aggiungere una nuova politica vuota. Vedere "Aggiunta di una nuova politica o di un modello di politica" a pagina 421. Creare una politica a partire da un modello. Vedere "Creazione di una politica a partire da un modello" a pagina 405. Selezionare una politica esistente nella schermata Gestisci > Politiche > Elenco politiche per modificarla. Vedere "Gestione e aggiunta di politiche" a pagina 444.

Azione	Descrizione
Immettere un nome e una descrizione per la politica.	<p>Il nome della politica deve essere univoco nel gruppo di politiche in cui si distribuisce la politica.</p> <p>Vedere "Limiti di immissione caratteri per la configurazione di politiche" a pagina 442.</p> <p>Nota: Il campo Etichetta politica è riservato al portale di supporto autonomo di Veritas Data Insight.</p>
Dall'elenco, selezionare il gruppo di politiche in cui la politica deve essere distribuita.	<p>Il gruppo di politiche predefinite è selezionato se nessun gruppo di politiche è configurato.</p> <p>Vedere "Creazione e modifica di gruppi di politiche" a pagina 447.</p>
Impostare lo stato della politica.	<p>È possibile attivare (impostazione predefinita) o disattivare una politica. Una politica disattivata viene distribuita ma non caricata nella memoria per rilevare incidenti.</p> <p>Vedere "Gestione e aggiunta di politiche" a pagina 444.</p>
Aggiungere una regola alla politica o modificare una regola esistente.	<p>Fare clic su Aggiungi regola per aggiungere una regola.</p> <p>Vedere "Aggiunta di una regola a una politica" a pagina 424.</p> <p>Selezionare una regola esistente per modificarla.</p>
Configurare la regola con una o più condizioni.	<p>Per una politica valida, è necessario configurare almeno una regola che dichiara almeno una condizione. Le eccezioni e le condizioni composte sono facoltative.</p> <p>Vedere "Configurazione di regole di politica" a pagina 427.</p>
Se lo si desidera, aggiungere una o più eccezioni di politica o modificare un'eccezione esistente.	<p>Fare clic su Aggiungi eccezione per aggiungere l'eccezione.</p> <p>Vedere "Aggiunta di un'eccezione a una politica" a pagina 434.</p> <p>Selezionare un'eccezione esistente per modificarla.</p>
Configurare qualsiasi eccezione.	<p>Vedere "Configurazione delle eccezioni di politica" a pagina 437.</p>
Salvare la configurazione della politica.	<p>Fare clic su Salva per salvare la configurazione della politica nel database di Enforce Server.</p> <p>Vedere "Componenti della politica" a pagina 375.</p>
Esportare la politica come modello.	<p>Se lo si desidera, è possibile esportare le regole e le eccezioni della politica come modello.</p> <p>Vedere "Esportazione del rilevamento di politiche come modello" a pagina 454.</p>

Azione	Descrizione
Aggiungere una o più regole di risposta alla politica.	La configurazione delle regole di risposta è indipendente dalle politiche. Vedere "Configurazione di regole di risposta" a pagina 1491. Vedere "Aggiunta di una regola di risposta automatica a una politica" a pagina 455.

Aggiunta di una regola a una politica

Nella schermata **Gestisci > Politiche > Elenco politiche > Configura politica - Aggiungi regola** è possibile aggiungere una o più regole a una politica.

È possibile aggiungere due tipi di regole a una politica: rilevamento e gruppo. Se due o più regole in una politica sono dello stesso tipo, il sistema le collega con OR. Se due o più regole in una politica sono di tipo differente, il sistema le collega con AND.

Vedere ["Esecuzione del rilevamento di politiche"](#) a pagina 402.

Nota: Le eccezioni sono aggiunte separatamente dalle regole. Vedere ["Aggiunta di un'eccezione a una politica"](#) a pagina 434.

Per aggiungere una o più regole a una politica

- 1 Scegliere il tipo di regola (rilevamento o gruppo) da aggiungere alla politica.

Per aggiungere una regola di rilevamento, selezionare la scheda **Rilevamento** e fare clic su **Aggiungi regola**.

Per aggiungere una regola di gruppo (identità), selezionare la scheda **Gruppi** e fare clic su **Aggiungi regola**.

Vedere ["Condizioni di corrispondenza di politiche"](#) a pagina 392.
- 2 Selezionare la regola di rilevamento o di gruppo da implementare dall'elenco delle regole.

Vedere [Tabella 19-2](#) a pagina 425.
- 3 Selezionare il componente necessario, se richiesto.

Se la regola di politica richiede un **profilo di dati**, un **identificatore di dati** o un **gruppo di utenti**, selezionarlo dall'elenco.
- 4 Fare clic su **Avanti** per configurare la regola di politica.

Vedere ["Configurazione di regole di politica"](#) a pagina 427.

Tabella 19-2 Aggiunta di regole di politica

Regola	Prerequisito	Descrizione
Condizioni di corrispondenza Contenuto		
Contenuto corrispondente a espressione regolare		Vedere "Introduzione alla corrispondenza con espressioni regolari" a pagina 787.
Contenuto corrispondente a profilo dati esatti	Profilo dati esatti	Vedere "Informazioni sul profilo dati esatti e sull'indice" a pagina 478. Vedere "Scelta di un profilo dati esatti" a pagina 417.
Contenuto corrispondente a parola chiave		Vedere "Introduzione alla corrispondenza con parole chiave" a pagina 771.
Contenuto corrispondente a firma documento	Profilo documento indicizzato	Vedere "Introduzione a Indexed Document Matching (IDM)" a pagina 569. Vedere "Scelta di un profilo documento indicizzato" a pagina 419.
Contenuto corrispondente a identificatore dati	Identificatore dati	Vedere "Introduzione agli identificatori di dati" a pagina 681. Vedere "Selezione di una copertura dell'identificatore di dati" a pagina 703.
Classificazione corrispondenze contenuto	ICT	Vedere "Panoramica dei passaggi per associare Information Centric Tagging a Data Loss Prevention" a pagina 232. Vedere "Configurazione della condizione Classificazione corrispondenze contenuto" a pagina 799.
Rileva con profilo Vector Machine Learning	Profilo VML	Vedere "Introduzione a Vector Machine Learning (VML)" a pagina 629. Vedere "Configurazione dei profili VML e delle condizioni delle politiche" a pagina 633.
Condizioni di corrispondenza Contesto		
Attributi contestuali (solo applicazioni cloud e dispositivo di rilevamento API)	Servizio di rilevamento cloud o dispositivo di rilevamento API	Vedere "Introduzione a attributi contestuali per le applicazioni cloud" a pagina 861.
Condizioni di corrispondenza Proprietà file		
Corrispondenza allegato messaggio o tipo file		Vedere "Informazioni sulla corrispondenza con tipi di file" a pagina 808.

Regola	Prerequisito	Descrizione
Corrispondenza allegato messaggio o dimensioni file		Vedere "Informazioni sulla corrispondenza di dimensione di file" a pagina 810.
Corrispondenza allegato messaggio o nome file		Vedere "Informazioni sulla corrispondenza del nome del file" a pagina 811.
Firma tipi di file personalizzati	Regola attivata Script personalizzato	Vedere "Informazioni sull'identificazione di tipi di file personalizzati" a pagina 809. Vedere "Attivazione della condizione Firma tipi di file personalizzati nella console della politica" a pagina 817.
Condizioni di corrispondenza Protocollo ed Endpoint		
Monitoraggio protocollo	Protocolli personalizzati (se esistenti)	Vedere "Introduzione al monitoraggio di protocolli per la rete" a pagina 821.
Monitoraggio endpoint		Vedere "Informazioni sul monitoraggio del protocollo endpoint" a pagina 824.
Classe o ID dispositivo endpoint	Dispositivi personalizzati	Vedere "Informazioni sul rilevamento di dispositivi endpoint" a pagina 826.
Posizione endpoint		Vedere "Informazioni sul rilevamento della posizione dell'endpoint" a pagina 826.
Riconoscimento moduli		
Esegui rilevamento utilizzando il profilo Riconoscimento moduli	Profilo di riconoscimento moduli	Vedere "Informazioni sul rilevamento Riconoscimento moduli" a pagina 662. Vedere "Configurazione della regola di rilevamento di riconoscimento moduli" a pagina 666.
Condizioni di corrispondenza Gruppi (identità)		
Mittente/utente corrisponde a criterio Destinatario corrispondente a criterio		Vedere "Introduzione alla corrispondenza con identità descritte" a pagina 835.
Mittente/utente basato su gruppo di server di directory Destinatario basato su gruppo di server di directory	Gruppo utenti	Vedere "Introduzione a Directory Group Matching (DGM) sincronizzato" a pagina 846. Vedere "Configurazione di gruppi di utenti" a pagina 847.

Regola	Prerequisito	Descrizione
Mittente/utente basato su una directory di:	Profilo dati esatti	Vedere "Introduzione a Directory Group Matching (DGM) con profilo" a pagina 855.
Destinatario basato su una directory di:		Vedere "Configurazione di profili dati esatti per DGM" a pagina 856.

Configurazione di regole di politica

Nella schermata **Gestisci > Politiche > Elenco politiche > Configura politica - Modifica regola**, configurare una regola di politica con una o più condizioni di corrispondenza. La configurazione di ogni condizione della regola dipende dal tipo della stessa.

Vedere [Tabella 19-4](#) a pagina 428.

Tabella 19-3 Configurazione di regole di politica

Passaggio	Azione	Descrizione
Passaggio 1	Aggiungere una regola a una politica o modificare una regola.	Vedere "Aggiunta di una regola a una politica" a pagina 424. Per modificare una regola esistente, selezionare la regola nell'interfaccia del generatore di politiche nella schermata Configura politica - Modifica regola .
Passaggio 2	Denominare la regola o modificare un nome.	Nella sezione Generale della regola, immettere un nome nel campo Nome regola o modificare il nome di una regola esistente.
Passaggio 3	Impostare la gravità della regola.	Nella sezione Gravità della regola, selezionare o modificare un livello di gravità "predefinito". Oltre alla gravità predefinita, è possibile aggiungere molteplici livelli di gravità a una regola. Vedere "Definizione di gravità della regola" a pagina 430.
Passaggio 4	Configurare la condizione di corrispondenza.	Nella sezione Condizioni della regola, configurare uno o più condizioni di corrispondenza per la regola. La configurazione di una condizione dipende dal tipo della stessa. Vedere Tabella 19-4 a pagina 428.
Passaggio 5	Configurare il conteggio delle corrispondenze (se richiesto).	Se la regola lo richiede, configurare come conteggiare le corrispondenze. Vedere "Configurazione del conteggio delle corrispondenze" a pagina 431.
Passaggio 6	Selezionare i componenti in cui cercare la corrispondenza (se disponibile).	Se la regola è basata sul contenuto, selezionare una o più regole di contenuto per la ricerca della corrispondenza. Vedere "Selezione dei componenti per la corrispondenza" a pagina 433.

Passaggio	Azione	Descrizione
Passaggio 7	Aggiungere e configurare una o più condizioni di corrispondenza supplementari (facoltativo).	<p>Per definire una regola composta, aggiungere un'altra condizione di corrispondenza dall'elenco Confronta anche.</p> <p>Configurare la condizione supplementare secondo il tipo della stessa (passaggio 4).</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p> <p>Nota: Tutte le condizioni in una singola regola devono essere vere per generare un incidente. Vedere "Esecuzione del rilevamento di politiche" a pagina 402.</p>
Passaggio 8	Salvare la configurazione della politica.	<p>Al termine della configurazione della regola, fare clic su OK.</p> <p>Viene visualizzata di nuovo la schermata Configura politica in cui è possibile salvare la politica.</p> <p>Vedere "Gestione e aggiunta di politiche" a pagina 444.</p>

[Tabella 19-4](#) elenca ogni condizione di corrispondenza disponibile e fornisce collegamenti agli argomenti per la configurazione di ogni condizione.

Tabella 19-4 Configurazione delle condizioni di corrispondenza delle politiche

Regola	Descrizione
Condizioni di corrispondenza Contenuto	
Contenuto corrispondente a espressione regolare	Vedere "Configurazione della condizione Contenuto corrispondente a espressione regolare" a pagina 789.
Il contenuto corrisponde ai dati esatti da un profilo dati esatti	Vedere "Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti" a pagina 503.
Contenuto corrispondente a parola chiave	Vedere "Configurazione della condizione Contenuto corrispondente a parola chiave" a pagina 779.
Contenuto corrispondente a firma documento	Vedere "Configurazione della condizione di politica Contenuto corrispondente a firma documento" a pagina 605.
Contenuto corrispondente a identificatore dati	Vedere "Configurazione della condizione Contenuto corrispondente a identificatore dati" a pagina 700.
Rileva utilizzando il profilo Vector Machine Learning	Vedere "Configurazione della condizione Rileva utilizzando il profilo Vector Machine Learning" a pagina 645.
Classificazione corrispondenze contenuto	Vedere "Configurazione della condizione Classificazione corrispondenze contenuto" a pagina 799.

Regola	Descrizione
Esegui rilevamento utilizzando il profilo Riconoscimento moduli	Vedere "Configurazione della regola di rilevamento di riconoscimento moduli" a pagina 666.
C	
Contesto	
Attributi contestuali (solo applicazioni cloud e dispositivo di rilevamento API)	Vedere "Introduzione a attributi contestuali per le applicazioni cloud" a pagina 861.
Condizioni di corrispondenza Proprietà file	
Corrispondenza allegato messaggio o tipo file	Vedere "Configurazione della condizione Corrispondenza allegato messaggio o tipo file." a pagina 812.
Corrispondenza allegato messaggio o dimensioni file	Vedere "Configurazione della condizione Corrispondenza allegato messaggio o dimensioni file" a pagina 813.
Corrispondenza allegato messaggio o nome file	Vedere "Configurazione della condizione Corrispondenza allegato messaggio o nome file" a pagina 815.
Firma tipi di file personalizzati	Vedere "Configurazione della condizione Firma tipi di file personalizzati" a pagina 817.
Condizioni di corrispondenza Protocollo	
Monitoraggio della rete	Vedere "Configurazione della condizione Monitoraggio protocollo per il rilevamento nella rete" a pagina 822.
Monitoraggio endpoint	Vedere "Configurazione della condizione di monitoraggio dell'endpoint" a pagina 827.
Classe o ID dispositivo endpoint	Vedere "Configurazione della condizione Classe o ID dispositivo endpoint" a pagina 830.
Posizione endpoint	Vedere "Configurazione della condizione Posizione endpoint" a pagina 829.
Condizioni di corrispondenza Gruppi	
Mittente/utente corrisponde a criterio	Vedere "Configurazione della condizione Mittente/utente corrisponde a criterio" a pagina 837.
Destinatario corrispondente a criterio	Vedere "Configurazione della condizione Destinatario corrispondente a criterio" a pagina 840.
Mittente/utente basato su gruppo di server di directory	Vedere "Configurazione della condizione Mittente/utente basato su gruppo di server di directory" a pagina 851.

Regola	Descrizione
Mittente/utente basato su una directory di un profilo dati esatti	Vedere "Configurazione del Mittente/Utente in base a una condizione della Profiled Directory" a pagina 858.
Destinatario basato su gruppo di server di directory	Vedere "Configurazione della condizione Destinatario basato su gruppo di server di directory" a pagina 852.
Destinatario basato su una directory di un profilo dati esatti	Vedere "Configurazione del destinatario in base a una condizione Profiled Directory" a pagina 859.

Definizione di gravità della regola

Il sistema assegna un livello di gravità a una violazione di una regola della politica. L'impostazione predefinita è "Alta". È possibile configurare l'impostazione predefinita e aggiungere uno o più livelli aggiuntivi di gravità.

Vedere ["Gravità delle politiche"](#) a pagina 379.

La gravità della regola della politica funziona con la condizione della regola di risposta **Gravità**. Se si imposta il livello di gravità predefinito della regola della politica su "Alto" e si definiscono livelli aggiuntivi di gravità, il sistema non assegna la gravità aggiuntiva all'incidente sulla base del conteggio di corrispondenze. Pertanto se si ha una regola di risposta impostata su un livello di gravità conteggio corrispondenze inferiore alla gravità "Alta" predefinita, la regola di risposta non viene eseguita.

Vedere ["Configurazione della condizione di risposta Gravità"](#) a pagina 1506.

Per definire la gravità di una regola di politica

- 1 Configurare una regola di politica.

Vedere ["Configurazione di regole di politica"](#) a pagina 427.

- 2 Selezionare il livello **Predefinito** nell'elenco **Gravità**.

Il livello di gravità predefinito è il livello base segnalato dal sistema. Il sistema applica il livello di gravità predefinito a tutte le corrispondenze con la regola, a meno che livelli di gravità aggiuntivi sovrascrivano l'impostazione predefinita.

- 3 Fare clic su **Aggiungi gravità** per definire livelli di gravità aggiuntivi per la regola.

Se si aggiunge un livello di gravità, questo è basato sul numero di corrispondenze.

- 4 Selezionare il livello di gravità desiderato, scegliere l'intervallo di numero di corrispondenze e immettere il numero di corrispondenze.

Ad esempio, è possibile impostare una gravità Media con l'intervallo X che attiva una corrispondenza dopo che sono state rilevate 100 corrispondenze.

- 5 Se si aggiunge un livello di gravità aggiuntivo, è possibile selezionarlo come gravità predefinita.
- 6 Per rimuovere un livello di gravità definito, fare clic sull'icona **X** accanto alla definizione di gravità.

Configurazione del conteggio delle corrispondenze

Alcune condizioni consentono di specificare il modo in cui conteggiare le corrispondenze. L'impostazione predefinita è Conta tutte le corrispondenze. È possibile configurare il numero minimo di corrispondenze necessario per generare un incidente. Oppure, è possibile conteggiare tutte le corrispondenze come un incidente. Se una condizione supporta il conteggio delle corrispondenze, è possibile configurare questa impostazione per le regole e le eccezioni delle politiche.

Vedere [Tabella 19-6](#) a pagina 433.

Tabella 19-5 Configurazione del conteggio delle corrispondenze

Parametro	Tipo di condizione	Descrizione incidente
Verificare esistenza	Semplice	Questa configurazione segnala un numero di corrispondenze pari a 1 se vi sono una o più corrispondenze; non conteggia le corrispondenze multiple. Ad esempio, 10 corrispondenze sono un incidente.
	Composta	Questa configurazione segnala un numero di corrispondenze pari a 1 se vi sono una o più corrispondenze e TUTTE le condizioni nella regola o nell'eccezione sono impostate per verificare l'esistenza.

Parametro	Tipo di condizione	Descrizione incidente
Conta tutte le corrispondenze	Semplice	Questa configurazione segnala il numero esatto di corrispondenze rilevate dalla condizione. Ad esempio, 10 corrispondenze vengono conteggiate come 10 incidenti.
	Composta	<p>Questa configurazione segnala un numero di corrispondenze pari alla somma delle corrispondenze con la condizione nella regola o nell'eccezione. Il valore predefinito è un incidente per ogni corrispondenza con la condizione e viene applicato se qualsiasi condizione nella regola o nell'eccezione è impostata per conteggiare tutte le corrispondenze.</p> <p>Ad esempio, se una regola ha due condizioni, una impostata per conteggiare tutte le corrispondenze e che rileva quattro corrispondenze, e l'altra impostata per verificare l'esistenza e che rileva sei corrispondenze, il numero di corrispondenze segnalate è 10. Se una terza condizione nella regola rileva una corrispondenza, il conteggio delle corrispondenze è 11.</p>
	Segnala solo gli incidenti che presentano almeno _ corrispondenze	<p>È possibile cambiare l'impostazione predefinita, ovvero un incidente per corrispondenza, specificando il numero minimo di corrispondenze necessario per segnalare un incidente.</p> <p>Ad esempio, in una regola con due condizioni, se se ne configura una per conteggiare tutte le corrispondenze e si specifica cinque come numero minimo di corrispondenze per ogni condizione, la somma di 10 corrispondenze segnalata dalla due condizioni genera due incidenti. È necessario essere coerenti e selezionare questa opzione per ogni condizione nella regola o nell'eccezione per ottenere questo comportamento.</p> <p>Nota: L'impostazione Conta tutte le corrispondenze viene applicata a ogni componente dei messaggi in cui cercare le corrispondenze. Ad esempio, si consideri una politica dove si specifica un numero di corrispondenze pari a 3 e si configura una regola di parola chiave che cerca la corrispondenza in tutti e quattro i componenti dei messaggi (impostazione predefinita per questa condizione). Se si riceve un messaggio con due istanze della parola chiave nel corpo e un'istanza della parola chiave nella busta, il sistema non segnala una corrispondenza. Tuttavia, se tre istanze della parola chiave sono contenute in un allegato (o in qualsiasi altro singolo componente del messaggio), il sistema segnalerebbe una corrispondenza.</p>
Conta tutte le corrispondenze univoche	Conta solo le corrispondenze univoche	<p>Il conteggio delle corrispondenze univoche è una nuova funzionalità di Symantec Data Loss Prevention versione 11.6 ed è disponibile solo per gli identificatori di dati.</p> <p>Vedere "Informazioni sul conteggio delle corrispondenze univoche" a pagina 697.</p>

Tabella 19-6 Condizioni che supportano il conteggio delle corrispondenze

Condizione	Descrizione
Contenuto corrispondente a espressione regolare	Vedere "Introduzione alla corrispondenza con espressioni regolari" a pagina 787. Vedere "Configurazione della condizione Contenuto corrispondente a espressione regolare" a pagina 789.
Contenuto corrispondente a parola chiave	Vedere "Introduzione alla corrispondenza con parole chiave" a pagina 771. Vedere "Configurazione della condizione Contenuto corrispondente a parola chiave" a pagina 779.
Contenuto corrispondente a firma documento (IDM)	Vedere "Configurazione della condizione di politica Contenuto corrispondente a firma documento" a pagina 605.
Contenuto corrispondente a identificatore dati	Vedere "Introduzione agli identificatori di dati" a pagina 681. Vedere "Configurazione della condizione Contenuto corrispondente a identificatore dati" a pagina 700. Vedere "Configurazione del conteggio delle corrispondenze univoche" a pagina 724.
Destinatario corrispondente a criterio	Vedere "Introduzione alla corrispondenza con identità descritte" a pagina 835. Vedere "Configurazione della condizione Destinatario corrispondente a criterio" a pagina 840.

Selezione dei componenti per la corrispondenza

La disponibilità di uno o più componenti del messaggio per la corrispondenza dipende dal tipo di condizione di regola o eccezione implementato.

Vedere ["Messaggi di rilevamento e componenti di messaggio"](#) a pagina 398.

Tabella 19-7 Corrispondenza con componenti

Componente	Descrizione
Busta	<p>Se la condizione supporta la corrispondenza con il componente Busta, selezionarlo per cercare la corrispondenza con i metadati del messaggio. La busta contiene l'intestazione, le informazioni sul trasporto e l'oggetto se il messaggio è un'e-mail SMTP.</p> <p>Se la condizione non supporta la corrispondenza con il componente Busta, questa opzione è disattivata.</p> <p>Se la condizione prevede la corrispondenza con l'intero messaggio, il componente Busta è selezionato e non può essere deselezionato, mentre gli altri componenti non possono essere selezionati.</p>

Componente	Descrizione
Oggetto	<p>Determinate condizioni di rilevamento prevedono la corrispondenza con il componente Oggetto per alcuni tipi di messaggi.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p> <p>Per le condizioni di rilevamento che supportano la corrispondenza con i componenti oggetto, è possibile cercare la corrispondenza con il componente Oggetto per i seguenti tipi di messaggi:</p> <ul style="list-style-type: none">■ Messaggi (e-mail) SMTP di Network Monitor o Network Prevent for Email.■ Messaggi NNTP di Network Monitor. <p>Per cercare la corrispondenza con il componente Oggetto, è necessario selezionare il componente Oggetto e deselezionare il componente Busta per la regola di politica. Se si selezionano entrambi i componenti, il sistema cerca la corrispondenza con l'oggetto due volte perché l'oggetto del messaggio è incluso nella busta come parte dell'intestazione.</p>
Corpo	<p>Se la condizione prevede la corrispondenza con il componente del messaggio Corpo, selezionarla per cercare la corrispondenza con il testo o il contenuto del messaggio.</p>
Allegati	<p>Se la condizione prevede la corrispondenza con il componente del messaggio Allegati, selezionarla per rilevare il contenuto nei file inviati da, scaricati con o allegati al messaggio.</p>

Aggiunta di un'eccezione a una politica

Nella schermata **Gestisci > Politiche > Elenco politiche > Configura politica – Aggiungi eccezione** è possibile aggiungere una o più condizioni di eccezione a una politica. Le eccezioni delle politiche sono eseguite prima delle regole delle politiche. In caso di corrispondenza con un'eccezione, l'intero messaggio viene ignorato.

Vedere "[Condizioni di eccezione](#)" a pagina 400.

Nota: È possibile creare eccezioni per tutte le condizioni delle politiche, ad eccezione della condizione EDM **Il contenuto corrisponde ai dati esatti da**. Inoltre, Network Prevent for Web non supporta le eccezioni DGM sincronizzate.

Per aggiungere un'eccezione a una politica**1** Aggiungere un'eccezione a una politica.

Per aggiungere un'eccezione delle regole di rilevamento, selezionare la scheda **Rilevamento** e fare clic su **Aggiungi eccezione**.

Per aggiungere un'eccezione delle regole di gruppi, selezionare la scheda **Gruppi** e fare clic su **Aggiungi eccezione**.

2 Selezionare l'eccezione di politica da implementare.

Nella schermata **Aggiungi eccezione di rilevamento** sono elencate tutte le eccezioni di rilevamento disponibili che è possibile aggiungere a una politica.

La schermata **Aggiungi eccezione di gruppo** elenca tutte le eccezioni di gruppo disponibili che è possibile aggiungere a una politica.

Vedere [Tabella 19-8](#) a pagina 435.

3 Se necessario, scegliere il profilo, l'identificatore di dati o il gruppo di utenti.**4** Fare clic su **Avanti** per configurare l'eccezione.

Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.

Tabella 19-8 Selezione di un'eccezione di politica

Eccezione	Prerequisito	Descrizione
Contenuto		
Contenuto corrispondente a espressione regolare		Vedere "Introduzione alla corrispondenza con espressioni regolari" a pagina 787.
Contenuto corrispondente a parola chiave		Vedere "Introduzione alla corrispondenza con parole chiave" a pagina 771.
Contenuto corrispondente a firma documento	Profilo documento indicizzato	Vedere "Scelta di un profilo documento indicizzato" a pagina 419.
Contenuto corrispondente a identificatore dati	Identificatore dati	Vedere "Introduzione agli identificatori di dati" a pagina 681. Vedere "Selezione di una copertura dell'identificatore di dati" a pagina 703.
Rileva utilizzando il profilo Vector Machine Learning	Profilo VML	Vedere "Configurazione delle eccezioni alla politica VML" a pagina 646. Vedere "Configurazione dei profili VML e delle condizioni delle politiche" a pagina 633.

Contesto

Eccezione	Prerequisito	Descrizione
Attributi contestuali (solo applicazioni cloud e dispositivo di rilevamento API)	Servizio di rilevamento cloud o dispositivo di rilevamento API	Vedere "Introduzione a attributi contestuali per le applicazioni cloud" a pagina 861.
Proprietà file		
Corrispondenza allegato messaggio o tipo file		Vedere "Informazioni sulla corrispondenza con tipi di file" a pagina 808.
Corrispondenza allegato messaggio o dimensioni file		Vedere "Informazioni sulla corrispondenza di dimensione di file" a pagina 810.
Corrispondenza allegato messaggio o nome file		Vedere "Informazioni sulla corrispondenza del nome del file" a pagina 811.
Firma tipi di file personalizzati	Condizione attivata Script personalizzato aggiunto	Vedere "Informazioni sull'identificazione di tipi di file personalizzati" a pagina 809.
Protocollo e endpoint		
Protocollo di rete		Vedere "Introduzione al monitoraggio di protocolli per la rete" a pagina 821.
Protocollo, destinazione, applicazione endpoint		Vedere "Informazioni sul monitoraggio del protocollo endpoint" a pagina 824.
Classe o ID dispositivo endpoint		Vedere "Informazioni sul rilevamento di dispositivi endpoint" a pagina 826.
Posizione endpoint		Vedere "Informazioni sul rilevamento della posizione dell'endpoint" a pagina 826.
Riconoscimento moduli		
Esegui rilevamento utilizzando il profilo Riconoscimento moduli	Profilo riconoscimento moduli	Vedere "Informazioni sul rilevamento Riconoscimento moduli" a pagina 662. Vedere "Configurazione della regola di eccezione Riconoscimento moduli" a pagina 667.
Identità gruppo		

Eccezione	Prerequisito	Descrizione
Mittente/utente corrisponde a criterio Destinatario corrispondente a criterio		Vedere "Introduzione alla corrispondenza con identità descritte" a pagina 835.
Mittente/utente basato su gruppo di server di directory Destinatario basato su gruppo di server di directory	Gruppo utenti	Vedere "Introduzione a Directory Group Matching (DGM) sincronizzato" a pagina 846. Vedere "Configurazione di gruppi di utenti" a pagina 847. Nota: Network Prevent for Web non supporta questo tipo di eccezione, ma utilizza DGM con profilo.
Mittente/utente basato su una directory di: Destinatario basato su una directory di:	Profilo dati esatti	Vedere "Introduzione a Directory Group Matching (DGM) con profilo" a pagina 855. Vedere "Configurazione di profili dati esatti per DGM" a pagina 856.

Configurazione delle eccezioni di politica

Nella schermata **Gestisci > Politiche > Elenco politiche > Configura politica - Modifica eccezione**, configurare una o più condizioni per un'eccezione di politica.

Vedere [Tabella 19-10](#) a pagina 438.

In caso di corrispondenza con una condizione di eccezione, il sistema elimina il componente corrispondente dal sistema. Questo componente non è più disponibile per la valutazione.

Vedere ["Condizioni di eccezione"](#) a pagina 400.

Tabella 19-9 Configurazione di eccezioni di politica

Passaggio	Azione	Descrizione
Passaggio 1	Aggiungere una nuova eccezione di politica o modificarne una esistente.	Vedere "Aggiunta di un'eccezione a una politica" a pagina 434. Selezionare un'eccezione di politica per modificarla.
Passaggio 2	Assegnare un nome all'eccezione o modificare un nome o una descrizione esistente.	Nella sezione Generale , immettere un nome univoco per l'eccezione o modificare il nome di un'eccezione esistente. Nota: Il nome deve avere una lunghezza massima di 60 caratteri.

Passaggio	Azione	Descrizione
Passaggio 3	Selezionare i componenti ai quali si desidera applicare l'eccezione (se disponibile).	<p>Se l'eccezione è basata su contenuto, è possibile cercare la corrispondenza nell'intero messaggio o nei singoli componenti del messaggio.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p> <p>Selezionare una delle opzioni di Applica eccezione a :</p> <ul style="list-style-type: none"> ■ Intero messaggio Questa opzione applica l'eccezione all'intero messaggio. ■ Solo componenti con corrispondenza Questa opzione applica l'eccezione a ogni componente del messaggio selezionato in Cerca corrispondenza con nella sezione Condizioni dell'eccezione.
Passaggio 4	Configurare la condizione per l'eccezione.	<p>Nella sezione Condizioni della schermata Configura politica - Modifica eccezione, definire la condizione per l'eccezione. La configurazione di una condizione dipende dal tipo di eccezione.</p> <p>Vedere Tabella 19-10 a pagina 438.</p>
Passaggio 5	Aggiungere una o più condizioni supplementari all'eccezione (facoltativo).	<p>È possibile aggiungere condizioni fino a che l'eccezione è strutturata come desiderato.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p> <p>Per aggiungere un'altra condizione a un'eccezione, selezionare la condizione dall'elenco Confronta anche.</p> <p>Fare clic su Aggiungi e configurare la condizione.</p>
Passaggio 6	Salvare e gestire la politica.	<p>Fare clic su OK per completare il processo di definizione dell'eccezione.</p> <p>Fare clic su Salva per salvare la politica.</p> <p>Vedere "Gestione e aggiunta di politiche" a pagina 444.</p>

[Tabella 19-10](#) elenca le condizioni di eccezione che è possibile configurare, con collegamenti a informazioni dettagliate sulla configurazione.

Tabella 19-10 Condizioni per eccezioni di politica disponibili per la configurazione

Eccezione	Descrizione
Contenuto	
Contenuto corrispondente a espressione regolare	Vedere "Configurazione della condizione Contenuto corrispondente a espressione regolare" a pagina 789.

Eccezione	Descrizione
Contenuto corrispondente a parola chiave	Vedere "Configurazione della condizione Contenuto corrispondente a parola chiave" a pagina 779.
Contenuto corrispondente a firma documento	Vedere "Configurazione della condizione di politica Contenuto corrispondente a firma documento" a pagina 605.
Contenuto corrispondente a identificatore dati	Vedere "Configurazione della condizione Contenuto corrispondente a identificatore dati" a pagina 700.
Rileva utilizzando il profilo Vector Machine Learning	Vedere "Configurazione delle eccezioni alla politica VML" a pagina 646.
Contesto	
Attributi contestuali (solo applicazioni cloud e dispositivo di rilevamento API)	Vedere "Introduzione a attributi contestuali per le applicazioni cloud" a pagina 861.
Proprietà file	
Corrispondenza allegato messaggio o tipo file	Vedere "Configurazione della condizione Corrispondenza allegato messaggio o tipo file." a pagina 812.
Corrispondenza allegato messaggio o dimensioni file	Vedere "Configurazione della condizione Corrispondenza allegato messaggio o dimensioni file" a pagina 813.
Corrispondenza allegato messaggio o nome file	Vedere "Configurazione della condizione Corrispondenza allegato messaggio o nome file" a pagina 815.
Firma tipi di file personalizzati	Vedere "Configurazione della condizione Firma tipi di file personalizzati" a pagina 817.
Protocollo e endpoint	
Protocollo di rete	Vedere "Configurazione della condizione Monitoraggio protocollo per il rilevamento nella rete" a pagina 822.
Protocollo o Destinazione endpoint	Vedere "Configurazione della condizione di monitoraggio dell'endpoint" a pagina 827.
Classe o ID dispositivo endpoint	Vedere "Configurazione della condizione Classe o ID dispositivo endpoint" a pagina 830.
Posizione endpoint	Vedere "Configurazione della condizione Posizione endpoint" a pagina 829.
Riconoscimento moduli	
Esegui rilevamento utilizzando il profilo Riconoscimento moduli	Vedere "Configurazione della regola di eccezione Riconoscimento moduli" a pagina 667.

Eccezione	Descrizione
Identità gruppo	
Mittente/utente corrisponde a criterio	Vedere "Configurazione della condizione Mittente/utente corrisponde a criterio" a pagina 837.
Destinatario corrispondente a criterio	Vedere "Configurazione della condizione Destinatario corrispondente a criterio" a pagina 840.
Mittente/utente basato su gruppo di server di directory	Vedere "Configurazione della condizione Mittente/utente basato su gruppo di server di directory" a pagina 851.
Destinatario basato su gruppo di server di directory	Vedere "Configurazione della condizione Destinatario basato su gruppo di server di directory" a pagina 852.
Mittente/utente basato su una directory di un profilo EDM	Vedere "Configurazione del Mittente/Utente in base a una condizione della Profiled Directory" a pagina 858.
Destinatario basato su una directory di un profilo EDM	Vedere "Configurazione del destinatario in base a una condizione Profiled Directory" a pagina 859.

Configurazione delle condizioni di corrispondenza composte

È possibile creare condizioni di corrispondenza composte per le regole e le eccezioni di politica.

Vedere ["Configurazione delle condizioni di corrispondenza composte"](#) a pagina 440.

Il motore di rilevamento collega le condizioni composte con un AND. Tutte le condizioni nella regola o nell'eccezione devono essere soddisfatte per attivare o escludere un incidente.

Vedere ["Esecuzione del rilevamento di politiche"](#) a pagina 402.

Non esiste un limite al numero di condizioni di corrispondenza che è possibile includere in una regola o un'eccezione. Tuttavia le varie condizioni che si dichiarano in una singola regola o eccezione devono essere associate logicamente. Non confondere le regole o le eccezioni composte con più regole o eccezioni in una politica.

Vedere ["Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza."](#) a pagina 469.

Tabella 19-11 Configurazione di una regola o eccezione di politica composta

Passaggio	Azione	Descrizione
Passaggio 1	Modificare o configurare una regola o un'eccezione di politica esistente.	È possibile aggiungere una o più condizioni di corrispondenza supplementari a una regola di politica nella schermata Configura politica - Modifica regola . È possibile aggiungere una o più condizioni di corrispondenza supplementari a una regola o un'eccezione nella schermata Configura politica - Modifica regola o Configura politica - Modifica eccezione .
Passaggio 2	Selezionare una condizione di corrispondenza aggiuntiva.	Selezionare la condizione di corrispondenza aggiuntiva dall'elenco Confronta anche . Questo elenco è visualizzato nella parte inferiore della sezione Condizioni per una regola o un'eccezione esistente.
Passaggio 3	Esaminare le condizioni disponibili.	Il sistema elenca tutte le condizioni supplementari disponibili che è possibile aggiungere una regola o un'eccezione di politica. Vedere "Aggiunta di una regola a una politica" a pagina 424. Vedere "Aggiunta di un'eccezione a una politica" a pagina 434.
Passaggio 4	Aggiungere la condizione supplementare.	Fare clic su Aggiungi per aggiungere la condizione di corrispondenza supplementare alla regola o all'eccezione di politica. Dopo l'aggiunta è possibile comprimere ed espandere ciascuna condizione in una regola o un'eccezione.
Passaggio 5	Configurare la condizione aggiuntiva.	Vedere "Configurazione di regole di politica" a pagina 427. Vedere "Configurazione delle eccezioni di politica" a pagina 437.
Passaggio 6	Selezionare lo stesso componente o un componente qualsiasi per la corrispondenza.	Se la condizione supporta la corrispondenza di componenti, specificare dove devono corrispondere i dati per generare o escludere un incidente. Stesso componente - I dati corrispondenti devono esistere nello stesso componente delle altre condizioni che supportano anche la corrispondenza di componenti per attivare una corrispondenza. Qualsiasi componente - I dati corrispondenti possono esistere in qualsiasi componente selezionato. Vedere "Informazioni sulla corrispondenza con diversi componenti" a pagina 696.
Passaggio 6	Ripetere questo processo per aggiungere altre condizioni di corrispondenza alla regola o all'eccezione.	È possibile aggiungere a una regola o un'eccezione tutte le condizioni necessarie. Tutte le condizioni in una singola regola o eccezione devono corrispondere per attivare un incidente o per attivare l'eccezione.

Passaggio	Azione	Descrizione
Passaggio 7	Salvare la politica.	Fare clic su OK per chiudere la schermata di configurazione della regola o dell'eccezione. Fare clic su Salva per salvare la configurazione della politica.

Limiti di immissione caratteri per la configurazione di politiche

Quando si configura una politica, tenere presenti i seguenti limiti di immissione caratteri per i componenti di configurazione della politica.

Tabella 19-12 Limiti di immissione caratteri per la configurazione di politiche

Elemento di configurazione	Limiti di immissione caratteri
Nome di un componente della politica, che include: <ul style="list-style-type: none">■ Politica■ Regola■ Eccezione■ Gruppo■ Condizione	60 caratteri Nota: Per importare una politica come modello, il nome della politica deve essere inferiore a 60 caratteri. In caso contrario il nome non appare nell'elenco Modelli importati .
Descrizione del componente della politica.	255 caratteri
Nome del profilo dati, che include: <ul style="list-style-type: none">■ Dati esatti■ Documento indicizzato■ Vector Machine Learning■ Riconoscimento moduli	255 caratteri
Limiti del criterio Identificatore dati	100 caratteri per riga Vedere "Utilizzo della lingua dei criteri degli identificatori dati" a pagina 751.

Amministrazione delle politiche

Il capitolo contiene i seguenti argomenti:

- Gestione e aggiunta di politiche
- Gestione e aggiunta di gruppi di politiche
- Creazione e modifica di gruppi di politiche
- Importazione politiche
- Esportazione delle politiche
- Clonazione delle politiche
- Importazione di modelli di politica
- Esportazione del rilevamento di politiche come modello
- Aggiunta di una regola di risposta automatica a una politica
- Eliminazione di politiche e gruppi di politiche
- Visualizzazione e stampa dei dettagli della politica
- Download dei dettagli delle politiche
- Risoluzione dei problemi delle politiche
- Aggiornamento dei profili EDM e IDM alla versione più recente
- Aggiornamento delle politiche dopo l'upgrade alla versione più recente

Gestione e aggiunta di politiche

La schermata **Gestisci > Politiche > Elenco politiche** consente di aggiungere e modificare politiche. Le politiche vengono implementate per rilevare le perdite di dati e generare report sulle stesse.

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

[Tabella 20-1](#) elenca e descrive le azioni che è possibile intraprendere nella schermata **Elenco politiche**.

Tabella 20-1 Azioni nella schermata Elenco politiche

Azione	Descrizione
Aggiungere una politica	Fare clic su Nuovo per creare una nuova politica. Vedere "Aggiunta di una nuova politica o di un modello di politica" a pagina 421.
Modificare una politica	Fare clic sul nome della politica o sull'icona di modifica per modificare una politica esistente. Vedere "Configurazione di politiche" a pagina 422.
Attivare una politica	Selezionare la politica o le politiche che si desidera attivare, quindi fare clic su Attiva nella barra degli strumenti dell'elenco di politiche.
Disattivare una politica	Selezionare la politica o le politiche che si desidera disattivare, quindi fare clic su Sospendi nella barra degli strumenti dell'elenco di politiche. Nota: Per impostazione predefinita, tutte le politiche del pacchetto di soluzioni vengono attivate all'installazione del pacchetto di soluzioni.
Ordinare le politiche	Fare clic su qualsiasi intestazione di colonna per ordinare l'elenco delle politiche.
Filtrare le politiche	È possibile filtrare l'elenco di politiche per Stato , Nome , Descrizione o Gruppo di politiche . Per filtrare l'elenco di politiche, fare clic su Filtro nella barra degli strumenti dell'elenco di politiche, quindi selezionare o immettere i criteri di filtro nella colonna o nelle colonne appropriate. Per rimuovere i filtri dall'elenco di politiche, fare clic su Cancella nella barra degli strumenti dell'elenco di politiche.

Azione	Descrizione
Rimuovere una politica	<p>Selezionare la politica o le politiche che si desidera rimuovere, quindi fare clic su Elimina nella barra degli strumenti dell'elenco di politiche.</p> <p>È anche possibile fare clic sulla X rossa in fondo alla riga della politica per eliminare una singola politica.</p> <p>Nota: Non è possibile rimuovere una politica con incidenti attivi.</p> <p>Vedere "Eliminazione di politiche e gruppi di politiche" a pagina 456.</p>
Importare ed esportare politiche	<p>È possibile importare ed esportare politiche usando i pulsanti Importa ed Esporta nella barra degli strumenti dell'elenco di politiche.</p> <p>Vedere "Importazione politiche" a pagina 449.</p> <p>Vedere "Esportazione delle politiche" a pagina 451.</p>
Esportare e importare modelli di politiche	<p>È possibile esportare e importare modelli di politiche da riutilizzare per la creazione di nuove politiche.</p> <p>Vedere "Importazione di modelli di politica" a pagina 453.</p> <p>Vedere "Esportazione del rilevamento di politiche come modello" a pagina 454.</p>
Scaricare i dettagli di una politica	<p>Fare clic su Scarica dettagli nella barra degli strumenti dell'elenco di politiche per scaricare i dettagli per le politiche selezionate in Elenco politiche. Symantec Data Loss Prevention esporta i dettagli della politica come file HTML in un file zip. Aprire l'archivio per visualizzare e stampare i dettagli delle politiche.</p> <p>Vedere "Download dei dettagli delle politiche" a pagina 457.</p>
Visualizzare e stampare i dettagli di una politica	<p>Per visualizzare i dettagli di una singola politica, fare clic sull'icona della stampante alla fine della riga della politica. Per stampare i dettagli della politica, utilizzare la funzionalità di stampa del browser Web in uso.</p> <p>Vedere "Visualizzazione e stampa dei dettagli della politica" a pagina 456.</p>
Clonare una politica	<p>Selezionare la politica o le politiche che si desidera clonare, quindi fare clic su Clona nella barra degli strumenti dell'elenco di politiche.</p> <p>Vedere "Clonazione delle politiche" a pagina 452.</p>
Assegnazione di politiche a un gruppo di politiche	<p>È possibile assegnare una o più politiche a un gruppo di politiche dalla pagina di elenco delle politiche.</p> <p>Selezionare la politica o le politiche che si desidera assegnare al gruppo di politiche, quindi fare clic su Assegna gruppo nella barra degli strumenti dell'elenco di politiche. Selezionare il gruppo di politiche nell'elenco a discesa.</p> <p>Vedere "Gruppi di politiche" a pagina 377.</p>

Tabella 20-2 elenca e descrive i campi di visualizzazione nella schermata **Elenco politiche**.

Tabella 20-2 Campi di visualizzazione della schermata Elenco politiche

Colonna	Descrizione
Stato	<p>La colonna di stato visualizza uno di tre stati per la politica:</p> <ul style="list-style-type: none"> ■ Politica configurata erroneamente: L'icona della politica è un simbolo di attenzione giallo. Vedere "Componenti della politica" a pagina 375. ■ Politica attiva: L'icona della politica è verde. Una politica attiva può rilevare incidenti. ■ Politica sospesa L'icona della politica è rossa. Una politica sospesa viene distribuita ma non rileva incidenti.
Nome	<p>Visualizza e ordina le politiche per nome.</p> <p>Vedere "Informazioni sulle politiche di Data Loss Prevention" a pagina 373.</p>
Descrizione	<p>Visualizza la descrizione della politica.</p> <p>Vedere "Modelli di politica" a pagina 376.</p>
Gruppo di politiche	<p>Visualizza e ordina le politiche in base al gruppo a cui vengono distribuite.</p> <p>Vedere "Gruppi di politiche" a pagina 377.</p>
Ultima modifica	<p>Visualizza e ordina per data dell'ultima modifica della politica.</p> <p>Vedere "Privilegi di creazione politiche" a pagina 380.</p>

Gestione e aggiunta di gruppi di politiche

La schermata **Sistema > Server e rilevatori > Gruppi di politiche** elenca i gruppi di politiche configurati nel sistema.

Nella schermata **Gruppi di politiche** è possibile gestire i gruppi di politiche esistenti e aggiungerne di nuovi.

Tabella 20-3 Azioni della schermata Gruppi di politiche

Azione	Descrizione
Aggiungere un gruppo di politiche	<p>Fare clic su Aggiungi per definire un nuovo gruppo di politiche.</p> <p>Vedere "Gruppi di politiche" a pagina 377.</p>
Modificare un gruppo di politiche	<p>Per modificare un gruppo di politiche esistente, fare clic sul nome del gruppo.</p> <p>Vedere "Creazione e modifica di gruppi di politiche" a pagina 447.</p>

Azione	Descrizione
Eliminare un gruppo di politiche	<p>Selezionare il gruppo di politiche, quindi fare clic su Elimina.</p> <p>Nota: Se si elimina un gruppo di politiche, si eliminano anche le politiche assegnate a quel gruppo.</p> <p>Vedere "Eliminazione di politiche e gruppi di politiche" a pagina 456.</p>
Trovare un gruppo di politiche	<p>È possibile cercare un gruppo di politiche applicando/immettendo un termine di ricerca nella barra Ricerca. È possibile filtrare i risultati per Nome, Descrizione o Server selezionando il filtro e facendo clic su Applica filtro.</p>
Visualizzare le politiche in un gruppo	<p>Per visualizzare le politiche distribuite a un gruppo di politiche esistente, accedere alla schermata Sistema > Server e rilevatori > Gruppi di politiche > Configura gruppo di politiche.</p> <p>Vedere "Creazione e modifica di gruppi di politiche" a pagina 447.</p>

Tabella 20-4 Campi di visualizzazione della schermata Gruppi di politiche

Colonna	Descrizione
Nome	Il nome del gruppo di politiche.
Descrizione	La descrizione del gruppo di politiche.
Server e rilevatori disponibili	<p>Il server di rilevamento o rilevatore di cloud a cui il gruppo di politiche è distribuito.</p> <p>Vedere "Distribuzione di politiche" a pagina 378.</p>
Ultima modifica	La data dell'ultima modifica del gruppo di politiche.

Creazione e modifica di gruppi di politiche

Nella schermata **Sistema > Server e rilevatori > Gruppi di politiche** è possibile configurare un nuovo gruppo di politiche o modificarne uno esistente.

Vedere "[Gruppi di politiche](#)" a pagina 377.

Per configurare un gruppo di politiche

- 1 Aggiungere un nuovo gruppo di politiche o modificarne uno esistente.
Vedere ["Gestione e aggiunta di gruppi di politiche"](#) a pagina 446.
- 2 Immettere il **nome** del gruppo di politiche o modificare un nome esistente.
Utilizzare un nome informativo. Gli autori di politiche e gli amministratori di Enforce Server si basano sul nome del gruppo di politiche per associare il gruppo di politiche a politiche, ruoli e target.
Il nome non deve includere più di 256 caratteri.
- 3 Immettere una **descrizione** del gruppo di politiche o modificare la descrizione di un gruppo di politiche esistente.
- 4 Selezionare uno o più **server e rilevatori** a cui assegnare il gruppo di politiche.
Il sistema visualizza una casella di controllo per ogni server di rilevamento attualmente configurato e registrato con Enforce Server.
 - Selezionare l'opzione **Tutti i server o rilevatori** per assegnare il gruppo di politiche a tutti i server di rilevamento e rilevatori di cloud nel sistema. Se non si seleziona questa casella di controllo, è possibile assegnare il gruppo di politiche a singoli server. L'opzione **Tutti i Discover Server** non è configurabile in quanto il sistema assegna automaticamente tutti i gruppi di politiche a tutti i server Network Discover. Questa funzionalità consente di assegnare gruppi di politiche a singoli target di Discover. Vedere ["Configurazione dei campi obbligatori per i target di Network Discover"](#) a pagina 1832.
 - Deselezionare l'opzione **Tutti i server o rilevatori** per assegnare il gruppo di politiche a singoli server di rilevamento.
Il sistema visualizza una casella di controllo per ogni server configurato e registrato con Enforce Server.
Selezionare ogni singolo server di rilevamento per assegnare il gruppo di politiche.
- 5 Fare clic su **Salva** per salvare la configurazione del gruppo di politiche.

Nota: La sezione **Politiche nel gruppo** della schermata **Gruppo di politiche** elenca tutte le politiche nel gruppo di politiche. Non è possibile modificare queste voci. Quando si crea un nuovo gruppo di politiche, questa sezione è vuota. Dopo la distribuzione di una o più politiche a un gruppo di politiche (durante la configurazione della politica), la sezione **Politiche nel gruppo** visualizza ogni politica nel gruppo di politiche.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Distribuzione di politiche"](#) a pagina 378.

Importazione politiche

È possibile esportare le politiche da un Enforce Server e importarle in un altro Enforce Server. Questa caratteristica semplifica lo spostamento di politiche da un ambiente all'altro. Ad esempio, è possibile esportare le politiche dall'ambiente di test e importarle nell'ambiente di produzione.

Informazioni sull'importazione di politiche

Per importare le politiche, è necessario disporre del privilegio **Importa politiche**. Per attivare questo privilegio, è inoltre necessario disporre dei privilegi **Amministrazione server**, **Crea politiche**, **Crea regole di risposta** e **Tutti i gruppi di politiche**.

Vedere ["Ruoli di configurazione"](#) a pagina 114.

Quando si importa una politica, si osservino i punti seguenti:

- La politica viene importata nello stesso stato in cui è stata esportata. Ad esempio, se una politica era attiva al momento dell'esportazione, è attiva quando la si importa. L'unica eccezione a questo comportamento riguarda le politiche preesistenti sul sistema su cui si sta importando la politica ("sistema target"). Se la politica esistente è attiva, lo è anche la politica importata, indipendentemente dallo stato del sistema di esportazione.
- Le politiche importate sovrascrivono le politiche esistenti con lo stesso nome. È possibile modificare il nome della politica esportata nel file XML se si desidera importarla senza sovrascrivere la politica esistente.
- Se il gruppo di politiche a cui apparteneva la politica esportata esiste sul sistema target, la politica viene aggiunta a tale gruppo o sovrascrive una politica con lo stesso nome nel gruppo. Se il gruppo di politiche non esiste sul sistema target, viene creato al momento dell'importazione. Se la politica esiste sul sistema target, ma appartiene a un gruppo di politiche diverso, la politica importata viene assegnata a un nuovo gruppo di politiche creato sul sistema target e non sovrascrive la politica esistente.
- Quando si importa una politica, è possibile scegliere se importare o meno le regole di risposta se tali regole sono in conflitto con le regole di risposta esistenti sul sistema target.
- Nella pagina **Anteprima importazione politica** vengono visualizzati gli avvisi relativi a eventuali elementi della politica che verranno creati o sovrascritti quando si importa la politica.
- È possibile importare solo una politica alla volta.

Per importare una politica

- 1 Accedere a **Gestisci > Politiche > Elenco politiche**.
- 2 Fare clic su **Importa**.

Viene visualizzata la pagina **Importa politica**.

3 Fare clic su **Sfoglia** per selezionare il file di politica esportato che si desidera importare.

4 Fare clic su **Importa politica**.

Viene visualizzata la pagina **Anteprima importazione politica**. In questa pagina vengono visualizzati gli avvisi relativi a eventuali elementi della politica che possono venire sovrascritti al momento dell'importazione. Se la politica che si sta importando include regole di risposta tra gli elementi che possono venire sovrascritti, è possibile escludere tali regole dall'importazione in questa pagina.

5 Fare clic su **Procedi con l'importazione**.

La politica viene importata. Se la politica contiene riferimenti irrisolti, viene visualizzata la pagina **Controllo riferimenti politica**.

È possibile risolvere eventuali riferimenti della politica irrisolti in questa pagina.

Vedere ["Informazioni sui riferimenti della politica"](#) a pagina 450.

Informazioni sui riferimenti della politica

Le politiche sono esportate in formato XML. I file della politica XML contengono metadati della politica, riferimenti ai profili di dati, regole di risposta, identificatori di dati e regole ed eccezioni di rilevamento e gruppo. I file non contengono i profili dati effettivi, le connessioni di directory, le credenziali o i plug-in di FlexResponse. È necessario fornire tali elementi sul sistema su cui si sta importando la politica.

Quando si importa una politica, Symantec Data Loss Prevention avvisa l'utente in caso di eventuali riferimenti irrisolti nella pagina **Controllo riferimenti politica**. La pagina **Controllo riferimenti politica** viene visualizzata al termine del processo di importazione delle politiche. Per visualizzare questa pagina, è inoltre possibile fare clic sull'icona dei riferimenti irrisolti nelle pagine **Elenco politiche** e **Modifica politica**.

Per risolvere i riferimenti della politica, fare clic sull'icona per la modifica (a forma di matita) nella pagina **Controllo riferimenti politica**. Symantec Data Loss Prevention visualizza la pagina di modifica appropriata per ciascun riferimento irrisolto. [Tabella 20-5](#) fornisce informazioni sulla risoluzione dei riferimenti della politica.

Tabella 20-5 Risoluzione dei riferimenti della politica

Riferimento politica irrisolto	Risoluzione
Gruppo di politiche in cui non è specificato alcun server di rilevamento:	Selezionare i server di rilevamento per il gruppo di politiche.
Connessione a directory con credenziali mancanti:	Fornire le credenziali per la connessione della directory.
Profilo EDM con indice e file origine mancanti:	Specificare il file origine dati corretto.

Riferimento politica irrisolto	Risoluzione
Profilo IDM con nome di file e percorso di importazione mancanti:	Specificare l'origine dati corretta.
Profilo IDM remoto con credenziali mancanti:	Fornire le credenziali per il profilo IDM remoto.
Profilo VML con profilo sottoposto a training e dati correlati mancanti:	Fornire il profilo sottoposto a training e i dati correlati, eseguire il training e accettare il profilo VML.
Profilo di riconoscimento moduli con archivio ZIP della galleria mancante:	Fornire l'archivio ZIP della galleria.
Regola di risposta di quarantena endpoint con credenziali salvate mancanti:	Fornire le credenziali per la regola di risposta di quarantena endpoint.
Regola di risposta con un plug-in di FlexResponse server mancante:	Distribuire il file JAR di FlexResponse server sul sistema target. Vedere " Distribuzione di un plug-in di FlexResponse server " a pagina 1888.

Esportazione delle politiche

È possibile esportare i dati della politica in un file XML per condividere facilmente le politiche tra Enforce Server.

Informazioni sull'esportazione della politica

Le politiche sono esportate in formato XML. I file della politica XML contengono metadati della politica, riferimenti ai profili di dati, regole di risposta, identificatori di dati e regole ed eccezioni di rilevamento e gruppo. I file non contengono i profili dati effettivi, le connessioni di directory, le credenziali o i plug-in di FlexResponse. È necessario copiare tali elementi sul sistema in cui si sta importando la politica.

È possibile esportare le politiche singolarmente o in una volta sola. Per esportare le politiche, è necessario disporre del privilegio **Crea politiche**.

Vedere "[Ruoli di configurazione](#)" a pagina 114.

Le politiche esportate includono i seguenti elementi:

- Nome, descrizione e gruppo della politica
- Regole della politica, tra cui Riconoscimento moduli, definizioni VML, EDM e IDM
- Dispositivi e posizioni endpoint

- Criteri destinatario e mittente
- Regole di risposta
- Identificatori di dati
- Protocolli personalizzati

Le politiche esportate non includono i seguenti elementi:

- Credenziali
- Riconoscimento moduli, indici VML, EDM o IDM
- Riconoscimento moduli, origini dati IDM o EDM
- File di esercitazione VML
- Plug-in FlexResponse

Per esportare le politiche

- 1 Accedere a **Gestisci > Politiche > Elenco politiche**.
- 2 Eseguire una delle seguenti operazioni:
 - Per esportare una singola politica, fare clic sull'icona di esportazione per tale politica.
 - Per esportare più politiche in un archivio ZIP, selezionare le politiche da esportare, quindi fare clic su **Esporta**.
- 3 Symantec Data Loss Prevention esporta la politica o le politiche tramite le seguenti convenzioni di denominazione:
 - Per le singole politiche, la convenzione di denominazione è
ENFORCEHOSTNAME-POLICYNAME-DATE-TIME.XML.
 - Per l'esportazione di massa della politica, la convenzione di denominazione è
ENFORCEHOSTNAME-policies-DATE-TIME.ZIP.

Clonazione delle politiche

È possibile clonare le politiche dalla pagina Elenco politiche.

Le politiche clonate sono copie esatte della politica originale. Comprendono i seguenti elementi:

- Nome, descrizione e gruppo della politica modificata.
 Le politiche clonate vengono visualizzate in Elenco politiche come **Copia N di nome politica originale**.
- Regole della politica, tra cui Riconoscimento moduli, definizioni VML, EDM e IDM
- Dispositivi e posizioni endpoint

- Criteri destinatario e mittente
- Regole di risposta
- Identificatori di dati
- Protocolli personalizzati

Nota: Per clonare le politiche è necessario disporre dei privilegi di creazione di politiche.

Per informazioni sull'importazione e l'esportazione delle politiche e dei modelli di politica, vedere questi argomenti:

Vedere ["Esportazione delle politiche"](#) a pagina 451.

Vedere ["Importazione politiche"](#) a pagina 449.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Vedere ["Importazione di modelli di politica"](#) a pagina 453.

Importazione di modelli di politica

È possibile importare uno o più modelli di politica in Enforce Server. Per importare modelli di politica, è necessario avere privilegi di sistema per le politiche.

Vedere ["Importazione ed esportazione dei modelli politica"](#) a pagina 383.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Per importare uno o più modelli di politica in Enforce Server

- 1 Inserire uno o più modelli di politica di file XML nella directory `\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\templates` sull'host di Enforce Server.

È possibile importare più modelli di politica posizionandoli tutte nella directory dei modelli.

- 2 Assicurarsi che l'utente di sistema "Protect" abbia accesso alla directory e ai file.
- 3 Accedere alla console di amministrazione di Enforce Server con privilegi di creazione di politiche.
- 4 Accedere a **Gestisci > Politiche > Elenco politiche** e fare clic su **Aggiungi politica**.
- 5 Scegliere l'opzione **Aggiungere una politica da un modello** e fare clic su **Avanti**.

- 6 Scorrere verso il basso l'elenco di modelli fino alla sezione **Modelli importati**.

Una voce dovrebbe essere visualizzata per ogni file XML presente nella directory dei modelli.

- 7 Selezionare il modello di politica importato e fare clic su **Avanti** per configurarlo.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Esportazione del rilevamento di politiche come modello

È possibile esportare le regole e le eccezioni di rilevamento delle politiche in un modello (file XML). Non è possibile esportare le regole di risposta delle politiche. È possibile esportare solo un modello di politica alla volta.

Vedere ["Importazione ed esportazione dei modelli politica"](#) a pagina 383.

Per esportare una politica come modello

- 1 Accedere alla console di amministrazione di Enforce Server con i privilegi dell'amministratore.
- 2 Accedere alla schermata **Gestisci > Politiche > Elenco politiche > Configura politica** per la politica che si desidera esportare.
- 3 Nella parte inferiore della schermata **Configura politica** fare clic sul collegamento **Esporta questa politica come modello**.
- 4 Salvare la politica nella destinazione locale o di rete desiderata.

Ad esempio, il sistema esporta una politica denominata **Webmail** nel file modello della politica `Webmail.xml` che è possibile salvare sull'unità locale.

Vedere ["Importazione di modelli di politica"](#) a pagina 453.

Per informazioni sull'importazione, l'esportazione e la clonazione delle politiche, vedere questi argomenti:

Vedere ["Esportazione delle politiche"](#) a pagina 451.

Vedere ["Importazione politiche"](#) a pagina 449.

Vedere ["Clonazione delle politiche"](#) a pagina 452.

Aggiunta di una regola di risposta automatica a una politica

È possibile aggiungere una o più regole di risposta automatica a una politica, in modo che quando la politica viene violata venga attivata un'azione.

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Nota: Le regole di risposta smart sono eseguite manualmente e non sono distribuite con le politiche.

Per aggiungere una regola di risposta automatica a una politica

- 1 Accedere alla console di amministrazione di Enforce Server con privilegi di creazione di politiche.

Vedere ["Privilegi di creazione politiche"](#) a pagina 380.

- 2 Passare alla schermata **Gestisci > Politiche > Elenco politiche > Configura politica** per la politica alla quale si desidera aggiungere una regola di risposta.
- 3 Selezionare la regola di risposta che si desidera aggiungere tra quelle disponibili nel menu a discesa.

Le politiche e le regole di risposta sono configurate separatamente. Per aggiungere una regola di risposta a una politica, è necessario in primo luogo definire e salvare in modo indipendente la regola di risposta.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

- 4 Fare clic su **Aggiungi regola di risposta** per aggiungere la regola di risposta alla politica.
- 5 Ripetere il processo per aggiungere altre regole di risposta alla politica.
- 6 **Salvare** la politica una volta completata l'aggiunta di regole di risposta.
- 7 Verificare che lo stato della politica sia verde dopo l'aggiunta della regola di risposta.

Vedere ["Gestione e aggiunta di politiche"](#) a pagina 444.

Nota: Se lo stato della politica mostra un segno giallo di attenzione, la politica non è configurata correttamente. Il sistema non supporta determinati abbinamenti di regole di rilevamento e azioni delle regole di risposta automatiche. Vedere [Tabella 76-2](#) a pagina 2037.

Eliminazione di politiche e gruppi di politiche

Prima di eliminare una politica o un gruppo di politiche da Enforce Server, leggere le linee guida esposte di seguito.

Tabella 20-6 Linee guida per l'eliminazione di politiche e gruppi di politiche

Azione	Descrizione	Linea guida
Eliminare una politica	Se si tenta di eliminare una politica a cui sono associati degli incidenti, il sistema impedisce l'eliminazione della politica.	<p>Se si desidera eliminare una politica, è necessario rimuovere dapprima tutti gli incidenti associati a quella politica da Enforce Server.</p> <p>Vedere "Gestione e aggiunta di politiche" a pagina 444.</p> <p>Un'alternativa è creare un gruppo di politiche non distribuito (non assegnato ad alcun server di rilevamento). Questo metodo è utile per conservare gli incidenti e le politiche precedenti per scopi di revisione senza mantenere tali politiche in un gruppo di politiche distribuito.</p> <p>Vedere "Importazione ed esportazione dei modelli politica" a pagina 383.</p>
Eliminare un gruppo di politiche	Se si tenta di eliminare un gruppo di politiche che contiene una o più politiche, il sistema visualizza un messaggio di errore. Inoltre, il gruppo di politiche non viene eliminato.	<p>Prima di eliminare un gruppo di politiche, rimuovere tutte le politiche da quel gruppo eliminandole o assegnandole a differenti gruppi di politiche.</p> <p>Vedere "Gestione e aggiunta di gruppi di politiche" a pagina 446.</p> <p>Se si desidera rimuovere un gruppo di politiche, creare un gruppo di politiche di manutenzione e spostare le politiche da rimuovere nel gruppo di manutenzione.</p> <p>Vedere "Creazione e modifica di gruppi di politiche" a pagina 447.</p>

Vedere ["Informazioni sulle politiche di Data Loss Prevention"](#) a pagina 373.

Vedere ["Gruppi di politiche"](#) a pagina 377.

Visualizzazione e stampa dei dettagli della politica

È possibile visualizzare e stampare i dettagli di una singola politica dalla schermata **Elenco politiche**.

Per visualizzare e stampare le politiche desiderate, è necessario disporre dei privilegi **Crea politiche**.

Vedere ["Privilegi di creazione politiche"](#) a pagina 380.

Vedere ["Visualizzazione, stampa e download dei dettagli della politica"](#) a pagina 385.

Per visualizzare e stampare i dettagli delle politiche

- 1 Accedere a **Gestisci > Politiche > Elenco politiche** e fare clic sull'icona della stampante alla fine della riga della politica.
Viene visualizzata la schermata **Istantanea politica**.
- 2 È possibile visualizzare le informazioni generiche relative alla politica, le regole di rilevamento e le regole di risposta nella schermata **Istantanea politica**.
- 3 Per stampare i dettagli della politica, utilizzare il comando **Stampa** dalla schermata **Istantanea politica** del browser Web in uso.

Download dei dettagli delle politiche

È possibile scaricare un archivio ZIP contenente dettagli delle politiche in **Elenco politiche**. L'archivio ZIP contiene documenti HTML con i dettagli di ogni politica selezionata nell'Elenco politiche, nonché un file indice per semplificare la ricerca dei dettagli della politica desiderati. I nomi dei file derivano dall'ID della politica, come `123.html`. Il file indice si chiama `downloaded_policies_DATA.html` e contiene il nome della politica, la descrizione, lo stato, il gruppo della politica e la data dell'ultima modifica di tutte le politiche selezionate, nonché collegamenti ai dettagli della politica.

Per scaricare le politiche desiderate, è necessario disporre dei privilegi **Crea politiche**.

Vedere ["Privilegi di creazione politiche"](#) a pagina 380.

Vedere ["Visualizzazione, stampa e download dei dettagli della politica"](#) a pagina 385.

Per scaricare i dettagli della politica

- 1 Andare a **Gestisci > Politiche > Elenco politiche**, selezionare le politiche desiderate, quindi fare clic su **Scarica dettagli**.
- 2 Nella finestra di dialogo **Apri file**, fare clic su **Salva file**, quindi su **OK**.
- 3 Per visualizzare i dettagli di una politica, estrarre i file dalla cartella zip e aprire il file che si desidera visualizzare. Utilizzare il file indice per cercare nelle politiche scaricate mediante il nome della politica, la descrizione, lo stato, il gruppo della politica o la data di ultima modifica.
Viene visualizzata la schermata **Istantanea politica**.
- 4 Per stampare i dettagli della politica, utilizzare il comando **Stampa** dalla schermata **Istantanea politica** del browser Web in uso.

Risoluzione dei problemi delle politiche

La [Tabella 20-7](#) elenca i file di registro da consultare per la risoluzione dei problemi delle politiche.

Tabella 20-7 File di registro per la risoluzione dei problemi delle politiche

File di registro	Descrizione
SymantecDLPDetectionServer.log	Registra quando le politiche e i profili sono inviati da Enforce Server ai server di rilevamento e ai server endpoint. Visualizza gli errori JRE. Vedere "File di registro di debug" a pagina 339.
detection_operational.log detection_operational_trace.log	Registra il caricamento delle politiche e l'esecuzione del rilevamento. Vedere "File di registro operativi" a pagina 336.
FileReader.log	Registra quando un file indice viene caricato in memoria. Per EDM, vedere la riga "Profilo database caricato". Per IDM, vedere la riga "Profilo documento caricato". Vedere "File di registro di debug" a pagina 339.
Indexer.log	Registra le operazioni del processo di indicizzazione per generare gli indici EDM e IDM. Vedere "File di registro di debug" a pagina 339.

Vedere ["Informazioni sui file di registro"](#) a pagina 335.

Vedere ["Schermata per la raccolta e la configurazione di registri"](#) a pagina 345.

Vedere ["Configurazione del comportamento di registrazione di un server"](#) a pagina 345.

Vedere ["Raccolta dei registri e dei file di configurazione del server"](#) a pagina 351.

Vedere ["File di log per la risoluzione dei problemi del training VML e del rilevamento di politiche"](#) a pagina 652.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.

Aggiornamento dei profili EDM e IDM alla versione più recente

Symantec Data Loss Prevention 14.0 fornisce diversi aggiornamenti significativi alle tecnologie EDM (Exact Data Matching) e IDM (Indexed Document Matching).

Per utilizzare queste nuove funzionalità su un sistema aggiornato, è necessario reindicizzare le origini di dati e documenti. Prima di distribuire un indice per la produzione, è necessario testare il profilo e le politiche aggiornati in base a esso per garantire che rilevino la perdita di dati come previsto sul sistema aggiornato.

La [Tabella 20-8](#) elenca i requisiti di reindicizzazione per l'aggiornamento dei profili EDM e IDM alla versione 14.0 e fornisce i collegamenti per ulteriori informazioni.

Tabella 20-8 Requisiti di reindicizzazione per i profili di dati EDM e IDM

Tecnologia e funzionalità	Azioni obbligatorie	Ulteriori informazioni
Exact Data Matching (EDM) <ul style="list-style-type: none"> Corrispondenza multitoken Intervallo di prossimità proporzionale 	Se si dispone di profili di dati esatti esistenti che supportano le politiche EDM e si desidera utilizzare nuove funzionalità EDM, prima di aggiornare i server di rilevamento, è necessario: <ul style="list-style-type: none"> reindicizzare tutte le origini dati strutturate con un indicizzatore EDM compatibile con la versione 14.0 e caricare ciascun indice in un profilo di dati esatti generato da 14.0. 	Vedere "Aggiornamento degli indici EDM alla versione più recente" a pagina 527. Inoltre fare riferimento al capitolo "Aggiornamento degli indici EDM alla versione più recente" nel <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> e alla Guida in linea.
Indexed Document Matching (IDM) <ul style="list-style-type: none"> IDM con corrispondenza esatta sull'endpoint (IDM agente) 	Se si dispone di profili di documenti indicizzati esistenti che supportano le politiche IDM e si desidera utilizzare l'IDM dell'agente, dopo l'upgrade a 14.0, è necessario: <ul style="list-style-type: none"> disattivare il rilevamento in due fasi su Endpoint Server e reindicizzare tutte le origini dati di documenti in modo che l'indice endpoint venga generato e distribuito a Endpoint Server per il download da DLP Agent. 	In alternativa fare riferimento all'argomento relativo all'utilizzo dell'IDM dell'agente dopo l'upgrade alla versione 14.0 nel <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> e nella Guida in linea.

Aggiornamento delle politiche dopo l'upgrade alla versione più recente

Diversi modelli di politiche sono stati aggiornati a Symantec Data Loss Prevention 15.1. Quando si esegue l'upgrade alla versione 15.1, il sistema aggiorna i modelli di politiche definiti dal sistema. Le politiche create in base a un modello di politica aggiornato non vengono modificate in modo che le configurazioni definite non vengano sovrascritte. Se si sono create politiche in base a uno o più modelli di politica aggiornati, è necessario aggiornare le politiche in modo che siano correnti.

I modelli della politica Regolamento generale per la protezione dei dati (GDPR) sono stati aggiornati per includere diversi nuovi identificatori di dati europei. Anche gli elenchi di parole chiave sono stati aggiornati.

I modelli di politica che utilizzano i criteri di identificatore dati per rilevare i Social Security Number sono stati aggiornati in modo da usare l'identificatore dati Social Security Number (SSN) statunitense randomizzato in Symantec Data Loss Prevention 12.5, che rileva i Social Security Number tradizionali e randomizzati. Symantec consiglia di aggiornare le politiche SSN per utilizzare l'identificatore dati Social Security Number (SSN) statunitense randomizzato, se non è già stato aggiornato.

Vedere ["Aggiornamento delle politiche per l'utilizzo dell'identificatore dati Social Security Number \(SSN\) statunitense randomizzato"](#) a pagina 747.

La [Tabella 20-9](#) elenca i modelli di politica aggiornati per questa versione di Symantec Data Loss Prevention.

Tabella 20-9 Modelli di politica aggiornati in Data Loss Prevention 12.5

Modello aggiornato	Componenti aggiornati	Descrizione politica
Regolamenti generali per la protezione dei dati (attività bancarie e finanza)	Identificatori di dati Elenchi di parole chiave	Questa politica protegge le informazioni personali identificabili relative ad attività bancarie e finanza. Vedere "Regolamento generale per la protezione dei dati (attività bancarie e finanza)" a pagina 1342.
Regolamento generale per la protezione dei dati (identità digitale)	Identificatori di dati Elenchi di parole chiave	Questa politica protegge le informazioni personali identificabili relative all'identità digitale. Vedere "Regolamento generale per la protezione dei dati (identità digitale)" a pagina 1364.
Regolamento generale per la protezione dei dati (identificazione governativa)	Identificatori di dati Elenchi di parole chiave	Questa politica protegge le informazioni personali identificabili relative all'identificazione governativa. Vedere "Regolamento generale per la protezione dei dati (identificazione governativa)" a pagina 1365.
Regolamento generale per la protezione dei dati (sanità e assicurazioni)	Identificatori di dati Elenchi di parole chiave	Questa politica protegge le informazioni personali identificabili relative a sanità e assicurazioni. Vedere "Regolamento generale per la protezione dei dati (sanità e assicurazioni)" a pagina 1389.
Regolamento generale per la protezione dei dati (profilo personale)	Identificatori di dati Elenchi di parole chiave	Questa politica protegge le informazioni personali identificabili relative al profilo personale. Vedere "Regolamento generale per la protezione dei dati (profilo personale)" a pagina 1401.

Modello aggiornato	Componenti aggiornati	Descrizione politica
Regolamento generale per la protezione dei dati (viaggi)	Identificatori di dati Elenchi di parole chiave	Questa politica protegge le informazioni personali identificabili relative ai viaggi. Vedere "Regolamento generale per la protezione dei dati (viaggi)" a pagina 1404.

Best practice per la creazione di politiche

Il capitolo contiene i seguenti argomenti:

- Best practice per la creazione di politiche
- Sviluppo di una strategia di politiche che supporti gli obiettivi di protezione dei dati
- Utilizzo iniziale di un numero limitato di politiche
- Utilizzo dei modelli di politica modificati in base alle esigenze
- Utilizzare lo stato di corrispondenza appropriato per gli obiettivi di prevenzione della perdita di dati.
- Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze
- Iniziare con soglie di corrispondenza elevate per ridurre i falsi positivi
- Utilizzo di un numero limitato di eccezioni per restringere l'ambito di rilevamento
- Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza.
- Creazione di politiche per limitare l'effetto potenziale del rilevamento in due fasi
- Utilizzo dei gruppi di politiche per gestire il ciclo di vita delle politiche
- Best practice specifiche del rilevamento

Best practice per la creazione di politiche

Questa sezione fornisce best practice generali per la creazione di politiche per Symantec Data Loss Prevention. Questa sezione presuppone che il lettore abbia una familiarità generale con

la creazione di politiche, e in particolare con la configurazione, il testing e la distribuzione di politiche, regole di rilevamento, condizioni di corrispondenza ed eccezioni alle politiche.

Vedere ["Informazioni sulle politiche di Data Loss Prevention"](#) a pagina 373.

Vedere ["Rilevamento della perdita di dati"](#) a pagina 387.

Le best practice non hanno il fine di fornire istruzioni precise per la risoluzione dei problemi. Lo scopo di questa sezione è quello di fornire best practice che, se osservate, contribuiranno a ridurre l'esigenza di risoluzione dei problemi e supporto per le politiche.

Tabella 21-1 Riassunto delle best practice per la creazione di politiche

Best practice	Descrizione
Sviluppare una strategia di politiche che supporti gli obiettivi di protezione dei dati.	Vedere "Sviluppo di una strategia di politiche che supporti gli obiettivi di protezione dei dati" a pagina 464.
Utilizzare inizialmente un numero limitato di politiche.	Vedere "Utilizzo iniziale di un numero limitato di politiche" a pagina 464.
Utilizzare i modelli di politica ma modificarli in base alle esigenze.	Vedere "Utilizzo dei modelli di politica modificati in base alle esigenze" a pagina 465.
Utilizzare i gruppi di politiche per gestire il ciclo di vita delle politiche.	Vedere "Utilizzo dei gruppi di politiche per gestire il ciclo di vita delle politiche" a pagina 471.
Utilizzare lo stato di corrispondenza appropriato per gli obiettivi di prevenzione della perdita di dati.	Vedere "Utilizzare lo stato di corrispondenza appropriato per gli obiettivi di prevenzione della perdita di dati." a pagina 465.
Provare e adattare le politiche per migliorare l'accuratezza delle corrispondenze.	Vedere "Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze" a pagina 466.
Iniziare con soglie di corrispondenza elevate per ridurre i falsi positivi.	Vedere "Iniziare con soglie di corrispondenza elevate per ridurre i falsi positivi" a pagina 468.
Utilizzare un numero limitato di eccezioni per restringere l'ambito di rilevamento.	Vedere "Utilizzo di un numero limitato di eccezioni per restringere l'ambito di rilevamento" a pagina 468.
Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza.	Vedere "Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza." a pagina 469.
Creare politiche per limitare l'effetto potenziale del rilevamento in due fasi.	Vedere "Creazione di politiche per limitare l'effetto potenziale del rilevamento in due fasi" a pagina 469.
Osservare le best practice specifiche per il rilevamento.	Vedere "Best practice specifiche del rilevamento" a pagina 471.

Sviluppo di una strategia di politiche che supporti gli obiettivi di protezione dei dati

Lo scopo del rilevamento è di ottenere risultati accurati in base a corrispondenze vere con le politiche. Le politiche create devono rilevare in modo accurato i dati che si desidera proteggere con falsi positivi minimi. Mediante l'uso di politiche ben definite che implementano il tipo appropriato di combinazioni di regole, condizioni ed eccezioni, è possibile ottenere risultati di rilevamento accurati e impedire la perdita dei dati più critici dell'azienda.

È possibile sviluppare una strategia di politiche di prevenzione contro le perdite di dati mediante due approcci:

- In base alle informazioni: identificando i dati riservati e creando politiche per prevenirne la perdita.
- In base alle normative: esaminando normative governative e industriali e creando politiche per la conformità con le stesse.

Tabella 21-2 descrive più dettagliatamente questi due approcci.

Tabella 21-2 Approcci per il rilevamento di politiche

Approccio	Descrizione
In base alle informazioni	Questo approccio prevede inizialmente l'identificazione di specifici elementi di dati e combinazioni di dati che si intende proteggere. Esempi di tali dati possono includere campi con profilo definito da un database, un elenco di parole chiave, un set di utenti o una combinazione di questi elementi. In seguito, si raggruppano elementi di dati simili e si creano politiche per identificarli e proteggerli. Questo approccio è più efficace quando si ha un accesso limitato ai dati o nessun problema particolare con una determinata normativa.
In base alle normative	Questo approccio prevede inizialmente l'utilizzo di un modello di politica basato sulle normative alle quali è necessario conformarsi. Esempi di tali modelli possono essere HIPAA o FACTA. Cominciare inoltre con l'utilizzare un set di dati di grandi dimensioni (come i dati relativi ad impiegati o clienti). Utilizzare i requisiti di alto livello stipulati dalle normative come base per questo approccio. Stabilire quindi quali documenti ed elementi di dati riservati nell'azienda soddisfano questi requisiti. Tali elementi di dati diventano le condizioni per le eccezioni e le regole di rilevamento nelle politiche.

Utilizzo iniziale di un numero limitato di politiche

Le regole di rilevamento delle politiche implementate si basano sugli obiettivi di sicurezza delle informazioni dell'organizzazione. Le azioni intraprese in risposta alle violazioni delle politiche si basano sui requisiti di conformità dell'organizzazione. In generale è necessario iniziare gradualmente con il rilevamento delle politiche. Attivare uno o due modelli di politica o alcune semplici condizioni, ad esempio la corrispondenza di parole chiave. Esaminare gli incidenti

rilevati da ciascuna politica. Ottimizzare i risultati prima di implementare le regole di risposta per intraprendere un'azione.

Generalmente è meglio disporre di un numero ridotto di politiche configurate per realizzare gli obiettivi di prevenzione della perdita di dati specifici invece di molte politiche che tentano di soddisfare tutti i requisiti di sicurezza. Se si dispone di troppe politiche, le prestazioni del sistema possono risentirne e possono generarsi troppi falsi positivi.

Vedere ["Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze"](#) a pagina 466.

Utilizzo dei modelli di politica modificati in base alle esigenze

I modelli di politica rappresentano un ottimo punto di partenza per la creazione di politiche. Symantec Data Loss Prevention fornisce 65 modelli di politica predefiniti che contengono regole di rilevamento e condizioni per molti tipi diversi di casi di utilizzo, compresi la conformità normativa, la protezione dei dati, l'applicazione delle norme di sicurezza e gli scenari di utilizzo accettabili.

È necessario utilizzare i modelli di politica forniti dal sistema come punto di partenza per le politiche. In questo modo si risparmia tempo e si evitano errori e lacune di informazioni nelle politiche in quanto i metodi di rilevamento sono predefiniti. Tuttavia nella maggior parte delle situazioni si consiglia di modificare il modello di politica e personalizzarlo in base all'ambiente specifico. Non è consigliato distribuire un modello di politica predefinito senza configurarlo per l'ambiente.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Utilizzare lo stato di corrispondenza appropriato per gli obiettivi di prevenzione della perdita di dati.

Per impedire la perdita di dati, è necessario rilevare accuratamente tutti i tipi di dati riservati ogni volta che i dati vengono memorizzati, copiati o trasmessi. Per raggiungere gli obiettivi per la sicurezza dei dati, è necessario implementare i metodi di rilevamento adatti al tipo di dati che si desidera proteggere. Il consiglio è di stabilire i metodi di rilevamento più idonei all'azienda e di ottimizzare le politiche in base ai risultati della prova di rilevazione.

La [Tabella 21-3](#) descrive i casi di utilizzo principali per ogni tipo di condizione di corrispondenza delle politiche fornito da Data Loss Prevention.

Tabella 21-3 Confronto delle condizioni di corrispondenza

Tipo di dati che si desidera proteggere	Condizione	Corrispondenza
Informazioni che consentono l'identificazione dell'utente (PII), quali i numeri di codice fiscale, di carta di credito e di patente	EDM	Dati esatti specificati nel profilo
	Identificatori di dati	Criteri di dati descritti e convalidati
Documenti riservati, come Microsoft Word, PowerPoint, PDF e così via.	IDM	Contenuti esatti del file Contenuti parziali del file (derivati)
	VML	Contenuti simile del file
File riservati e immagini, ad esempio disegni CAD	IDM	File esatto
	Proprietà file	Contesto del file (tipo, nome, dimensione)
Parole e frasi, quali "Riservato" o "Privato"	Parole chiave	Parole esatte, frasi, prossimità
Caratteri, stringhe, testo	Espressioni regolari	Testo descritto
Comunicazioni di endpoint e della rete	Protocollo ed endpoint	Protocolli, destinazioni, monitoraggio
Determinati dall'identità di utente, mittente, destinatario	DGM sincronizzato	Identità esatta dal server LDAP
	DGM con profilo	Identità esatta con profilo
	Mittente/utente, destinatario	Criteri di identità descritti
Descrizione di un documento, come l'autore, il titolo, la data, ecc.	Condizioni basate sul contenuto	Metadati sul tipo di file

Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze

Quando si creano politiche di rilevamento, ci sono due problemi comuni da evitare. Se si crea una politica troppo generica o troppo ampia, questa genera incidenti anche quando non si verifica nessuna reale corrispondenza (falso positivo). D'altra parte, se una politica ha regole troppo specifiche o restrittive riguardo ai dati da rilevare, la politica potrebbe non rilevare alcune delle corrispondenze che si intende cogliere (falsi negativi). [Tabella 21-4](#) descrive più dettagliatamente questi problemi comuni.

Per ridurre i falsi positivi e negativi, è necessario ottimizzare le politiche. Il modo migliore di ottimizzare il rilevamento è di identificare un singolo, specifico caso d'uso che è una priorità, come la protezione del codice sorgente di un particolare prodotto. Inoltre è possibile creare

una singola politica, a partire da zero o in base a un modello, a seconda della strategia DLP adottata, che contenga una o due regole di rilevamento e provare la politica per vedere quanti (quantità) e che tipo (qualità) di incidenti genera tale politica. Sulla base di questi risultati iniziali, è possibile modificare le regole di rilevamento ove necessario. Se la politica genera più falsi positivi di quanto si desidera, occorre rendere le regole di rilevamento più specifiche regolando le condizioni di corrispondenza esistenti, aggiungendo ulteriori condizioni di corrispondenza e creando eccezioni alla politica. Se la politica non individua alcuni incidenti, rendere le condizioni di rilevamento meno specifiche.

Man mano che le politiche si evolvono, è importante verificarle continuamente e ottimizzarle per assicurarne l'accuratezza costante.

Vedere ["Best practice specifiche del rilevamento"](#) a pagina 471.

Tabella 21-4 Problemi di rilevamento comuni da evitare

Problema	Causa	Descrizione
Falsi positivi	Regole di politica troppo generiche o ampie	<p>I falsi positivi determinano alti costi in termini di tempo e risorse necessari per individuare e risolvere incidenti apparenti che non sono incidenti effettivi. Poiché molte organizzazioni non hanno le risorse per gestire i falsi positivi in eccesso, è importante che le politiche definiscano delle regole contestuali per migliorare l'accuratezza.</p> <p>Ad esempio, una policy è studiata per proteggere i nomi dei clienti e genera un incidente per qualunque elemento contenente un nome e un cognome. Poiché la maggior parte dei messaggi contengono un nome, spesso insieme al cognome, questa politica è troppo vasta e generica. Sebbene possa trovare tutte le occorrenze dei nomi di clienti inviati fuori della rete, questa politica restituirà troppi falsi positivi individuando messaggi e-mail che non divulgano informazioni protette. Nomi e cognomi richiedono una comprensione molto più ampia del contesto per determinare se si tratta di dati confidenziali</p>
Falsi negativi	Le regole di politica troppo rigorose o restrittive	<p>I falsi negativi nascondono le falle della sicurezza ed espongono al rischio di perdite di dati, perdite finanziarie, problemi legali e danni alla reputazione di un'organizzazione. I falsi negativi sono particolarmente pericolosi perché non si è consapevoli di aver perso dati sensibili.</p> <p>Ad esempio, una politica che contiene una corrispondenza sulla parola "confidenziale" ma contiene anche una condizione che esclude tutti i documenti di Microsoft Word sarebbe troppo restrittiva e in grado di generare falsi negativi perché probabilmente potrebbe non individuare molti incidenti effettivi contenuti in tali documenti</p>

Vedere ["Iniziare con soglie di corrispondenza elevate per ridurre i falsi positivi"](#) a pagina 468.

Vedere ["Utilizzo di un numero limitato di eccezioni per restringere l'ambito di rilevamento"](#) a pagina 468.

Vedere ["Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza."](#) a pagina 469.

Iniziare con soglie di corrispondenza elevate per ridurre i falsi positivi

Per le regole di rilevamento basate sul contenuto, un'impostazione di configurazione consente di "contare tutte le corrispondenze" ma di segnalare un incidente solo dopo il raggiungimento di un numero di corrispondenze limite. In genere si consiglia di iniziare con soglie di corrispondenze elevate per le politiche di rilevamento basate sul contenuto. Man mano che si ottimizzano le politiche sarà possibile ridurre le soglie di corrispondenze per risultati più precisi.

Vedere ["Configurazione del conteggio delle corrispondenze"](#) a pagina 431.

Utilizzo di un numero limitato di eccezioni per restringere l'ambito di rilevamento

È possibile implementare condizioni di eccezione per qualsiasi regola di rilevamento, salvo le regole EDM. L'utilizzo limitato delle condizioni di eccezione può contribuire a ridurre i falsi positivi restringendo l'ambito di rilevamento delle politiche. Tuttavia, se è necessario usare diverse eccezioni in una singola politica per ottenere i risultati di rilevamento desiderati, riconsiderare la progettazione della politica. Assicurarsi che la politica sia definita correttamente e utilizzi le condizioni di corrispondenza appropriate.

Attenzione: troppe eccezioni composte in una politica possono causare problemi di prestazioni a livello di sistema. È necessario evitare il più possibile l'utilizzo di eccezioni composte.

È importante comprendere come funzionano le condizioni di eccezione in modo che sia possibile utilizzarle correttamente. Le condizioni di eccezione impediscono ai messaggi di generare incidenti. Le condizioni di eccezione vengono verificate prima dal server di rilevamento, prima delle condizioni di corrispondenza. Se la condizione di eccezione corrisponde, il sistema scarta immediatamente l'intero messaggio o il componente del messaggio che ha soddisfatto l'eccezione. Le eccezioni a livello di corrispondenza non sono supportate. Dopo che il messaggio o il componente del messaggio è stato scartato in base a un'eccezione, i dati non sono più disponibili per la valutazione della politica.

Vedere ["Condizioni di eccezione"](#) a pagina 400.

Vedere ["Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza."](#) a pagina 469.

Utilizzare condizioni composte per migliorare l'accuratezza della corrispondenza.

Le condizioni composte consentono di migliorare l'accuratezza della corrispondenza delle politiche utilizzate. Si supponga di essere interessati ai documenti di Microsoft Word inviati dall'organizzazione. Inizialmente, si aggiunge una politica che usa una condizione tipo di allegato per rilevare tutti i file Word. Si scopre rapidamente che troppi messaggi contengono allegati Word che non divulgano informazioni protette. Quando si esaminano gli incidenti in modo più approfondito, si realizza di essere interessati più ai file Word che contengono la parola RISERVATO. In questo caso, è possibile convertire la condizione tipo di allegato in una regola composta aggiungendo una regola di parola chiave per la parola RISERVATO. Una tale configurazione consentirebbe di ottenere risultati di rilevamento più accurati.

Vedere ["Condizioni composte"](#) a pagina 401.

Creazione di politiche per limitare l'effetto potenziale del rilevamento in due fasi

Le condizioni EDM (Exact Data Matching) e DGM (Directory Group Matching) con profilo richiedono il rilevamento in due fasi. Per queste condizioni, DLP Agent deve inviare i dati a Endpoint Server per la valutazione. Se attivata, l'IDM (Indexed Document Matching) utilizza il rilevamento in due fasi.

Vedere ["Rilevamento in due fasi per DLP Agent."](#) a pagina 403.

Sull'endpoint DLP Agent esegue prima le regole che richiedono meno elaborazione. Se si sta distribuendo all'endpoint una politica che richiede il rilevamento in due fasi, è possibile creare la politica in modo tale da limitare l'effetto potenziale del rilevamento in due fasi.

La [Tabella 21-5](#) fornisce alcune considerazioni per la creazione di politiche per limitare l'effetto potenziale del rilevamento in due fasi.

Vedere ["Messaggi di rilevamento e componenti di messaggio"](#) a pagina 398.

Tabella 21-5 Configurazioni delle politiche per le regole di rilevamento in due fasi

Condizione di corrispondenza in due fasi	Configurazione politica
Exact Data Matching (EDM)	<p>Per le politiche EDM si consideri l'inclusione delle regole di identificatore dati connesse alle regole EDM dalla condizione OR. Ad esempio, per una politica che utilizza una condizione EDM per la corrispondenza di codici fiscali è possibile aggiungere una seconda regola che usa la condizione di identificatore dati numero di previdenza sociale. L'identificatore dati non richiede il rilevamento in due fasi e viene valutato localmente da DLP Agent. Se DLP Agent non è connesso a Endpoint Server quando riceve i dati, può continuare a cercare la corrispondenza dei criteri di numero di previdenza sociale in base alla condizione di identificatore dati.</p> <p>Vedere "Combinazione tra identificatori dati e regole EDM per limitare l'impatto del rilevamento in due fasi" a pagina 567.</p> <p>Per le configurazioni di politica di esempio, ciascuno dei modelli di politica che fornisce le condizioni EDM fornisce anche le condizioni di identificatore dati corrispondenti.</p> <p>Vedere "Scelta di un profilo dati esatti" a pagina 417.</p>
Indexed Document Matching (IDM)	<p>Per le politiche IDM che corrispondono ai contenuti di file si consideri la possibilità di utilizzare le regole VML connesse alle regole IDM dalla condizione OR. Le regole VML non richiedono il rilevamento in due fasi e vengono eseguite localmente da DLP Agent. Se non è necessario cercare la corrispondenza esatta dei contenuti di file, si consiglia di utilizzare il VML invece dell'IDM.</p> <p>Vedere "Utilizzare lo stato di corrispondenza appropriato per gli obiettivi di prevenzione della perdita di dati." a pagina 465.</p> <p>Se è necessario cercare solo la corrispondenza di file, non di contenuti di file, si consideri la possibilità di usare le regole composte delle proprietà dei file invece dell'IDM. Le regole delle proprietà dei file non richiedono il rilevamento in due fasi.</p> <p>Vedere "Utilizzo delle regole proprietà file composte per proteggere i file di progettazione e multimediali" a pagina 819.</p>
Directory Group Matching (DGM)	<p>Per la condizione di destinatario DGM sincronizzata si consideri la possibilità di includere una condizione Destinatario corrispondente a criterio connessa alla condizione DGM tramite la condizione OR. La condizione di criterio non richiede il rilevamento in due fasi e viene valutata localmente da DLP Agent.</p> <p>Vedere "Informazioni sul rilevamento in due fasi per DGM sincronizzata" a pagina 847.</p>

Utilizzo dei gruppi di politiche per gestire il ciclo di vita delle politiche

Utilizzare i gruppi di politiche per testare le politiche prima di usarle in produzione. Creare un gruppo di politiche di test a cui l'utente è l'unico ad avere accesso. Quindi creare le politiche e aggiungerle al gruppo di politiche di test. Esaminare gli incidenti acquisiti dalle politiche di test. Dopo avere ottimizzato le politiche e confermato che acquisiscono gli incidenti previsti, è possibile rinominare il gruppo di politiche e concedervi l'accesso ai ruoli appropriati. È inoltre possibile utilizzare i gruppi di politiche per gestire le politiche precedenti, nonché le politiche che si desidera importare o esportare.

Vedere ["Gruppi di politiche"](#) a pagina 377.

Vedere ["Eliminazione di politiche e gruppi di politiche"](#) a pagina 456.

Best practice specifiche del rilevamento

Oltre a queste considerazioni generali sulla creazione di politiche è necessario essere consapevoli di e tenere a mente le considerazioni sull'ottimizzazione delle politiche specifiche di ciascun tipo di condizione di corrispondenza.

La [Tabella 21-6](#) elenca le considerazioni specifiche del rilevamento, con collegamenti agli argomenti per ulteriori informazioni.

Tabella 21-6 Best practice per metodi di rilevamento specifici

Metodo di rilevamento	Descrizione
EDM	Vedere "Best practice per l'utilizzo dell'EDM" a pagina 557.
IDM	Vedere "Best practice per l'utilizzo di IDM" a pagina 607.
VML	Vedere "Procedure ottimali per l'utilizzo di VML" a pagina 653.
Identificatori dati	Vedere "Best practice per l'utilizzo degli identificatori dati" a pagina 765.
Parole chiave	Vedere "Best practice per l'utilizzo della corrispondenza di parole chiave" a pagina 784.
Espressioni regolari	Vedere "Best practice per l'utilizzo della corrispondenza di espressioni regolari" a pagina 791.
Rilevamento in lingua non inglese	Vedere "Best practice per il rilevamento di contenuti non in inglese" a pagina 803.
Proprietà file	Vedere "Best practice per l'utilizzo di corrispondenza delle proprietà file" a pagina 818.
Protocolli di rete	Vedere "Best practice per l'utilizzo della corrispondenza di protocolli di rete" a pagina 823.

Metodo di rilevamento	Descrizione
Eventi endpoint	Vedere "Best practice per l'utilizzo del rilevamento endpoint" a pagina 833.
Identità descritte	Vedere "Best practice per l'utilizzo della corrispondenza di identità descritte" a pagina 843.
DGM sincronizzata	Vedere "Best practice per l'utilizzo di condizioni DGM sincronizzate" a pagina 853.
DGM con profilo	Vedere "Procedure ottimali per l'utilizzo di DGM con profilo" a pagina 859.
Rilevamento metadati	Vedere "Best practice per l'utilizzo del rilevamento di metadati" a pagina 905.

Rilevamento del contenuto mediante Exact Data Matching (EDM)

Il capitolo contiene i seguenti argomenti:

- [Introduzione all'Exact Data Matching \(EDM\)](#)
- [Configurazione di profili dati esatti](#)
- [Configurazione dei criteri EDM](#)
- [Utilizzo della corrispondenza multitoken](#)
- [Aggiornamento degli indici EDM alla versione più recente](#)
- [Requisiti di memoria per EDM](#)
- [Indicizzazione EDM remota](#)
- [Best practice per l'utilizzo dell'EDM](#)

Introduzione all'Exact Data Matching (EDM)

Exact Data Matching (EDM) è progettato per proteggere i contenuti più sensibili. È possibile utilizzare EDM per rilevare dati tabulari, strutturati, incluse le informazioni che consentono l'identificazione dell'utente (PII). EDM è progettato per trovare i record che fanno parte di un'origine dati indicizzata nelle destinazioni strutturate o non strutturate. Alcuni esempi sono codici fiscali, numeri di conti bancari e numeri di carta di credito. È anche possibile rilevare record riservati di clienti e dipendenti, voci di listini, parti di una distinta, nonché altri dati riservati archiviati in un'origine dati strutturata, ad esempio un database, un server di directory o un file di dati strutturato, a esempio un CSV o un foglio di calcolo.

Per implementare politiche EDM, identificare e preparare i dati che si desidera proteggere. È possibile creare un **Profilo dati esatti** e indicizzare l'origine dati strutturata mediante la console di amministrazione di Enforce Server o da remoto mediante l'Indicizzatore EDM remoto. Durante il processo di indicizzazione, il sistema esegue il fingerprinting dei dati accedendo al ed estraendo il contenuto basato su testo, normalizzandolo e proteggendolo mediante un hash non reversibile. È possibile pianificare l'indicizzazione su base regolare dopo aver estratto dati correnti dall'origine dati, al fine di garantire che l'indice EDM rifletta i dati correnti.

Una volta specificati i dati nel profilo, configurare la condizione **Corrispondenze contenuto dati esatti** per cercare la corrispondenza di singole parti di dati indicizzati. Per una maggiore precisione è possibile configurare la condizione in modo da cercare la corrispondenza di combinazioni di campi di dati da uno specifico record. La condizione della politica EDM cerca la corrispondenza dei dati provenienti dalla stessa riga o record di dati. Ad esempio, è possibile configurare la condizione della politica EDM per cercare qualsiasi combinazione di tre elementi tra nome, cognome, SSN, numero di account o numero di telefono presenti insieme in un messaggio e corrispondenti a un record del database clienti.

Una volta che la politica viene distribuita a uno o più server di rilevamento, servizi di rilevamento cloud o dispositivi, il sistema può rilevare i campi dati (o record) inseriti nel profilo in formato strutturato o non strutturato. Ad esempio, è possibile distribuire la politica EDM su un server Network Discover ed eseguire la scansione di archivi di dati alla ricerca di dati riservati corrispondenti a record di dati nell'indice. In alternativa, è possibile distribuire la politica EDM su un server Network Prevent for Email per rilevare record in comunicazioni e-mail e allegati, ad esempio file di Microsoft Word. Se l'allegato è un foglio elettronico, come ad esempio un file Microsoft Excel, la politica EDM può rilevare anche la presenza di record privati.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Informazioni sull'utilizzo di EDM per proteggere i contenuti

Per capire come funziona EDM, considerare il seguente esempio. La società gestisce un database dei dipendenti che contiene i seguenti campi colonna:

- Nome
- Cognome
- Numero di previdenza sociale
- Data assunzione
- Stipendio

In un formato di dati strutturati quale un database, ogni riga rappresenta un record e ogni record contiene valori per ciascun campo dati colonna. In questo esempio, ogni riga nel database contiene informazioni per un dipendente ed è possibile usare EDM per proteggere ciascun record. Ad esempio, una riga del file origine dati contiene il seguente record delimitato da pipe ("|"):

First Name | Last Name | SSN | Date of hire | Salary

Bob | Smith | 123-45-6789 | 05/26/99 | \$42500

Si definisce un Profilo dati esatti e si indicizza il file origine dati. Quando si configura il profilo, si mappano le colonne campo dati a criteri definiti dal sistema e si procede alla convalida dei dati. Quindi si configura la condizione della politica EDM che fa riferimento al Profilo dati esatti. In questo esempio la condizione determina una corrispondenza se un messaggio contiene tutti e cinque i campi di dati.

Il server di rilevamento segnala una corrispondenza se individua quanto segue in qualsiasi messaggio in entrata:

Bob Smith 123-45-6789 05/26/99 \$42500

Tuttavia un messaggio che contiene quanto segue non determina una corrispondenza, perché tale record non è incluso nell'indice:

Betty Smith 000-00-0000 05/26/99 \$42500

Se la condizione è stata limitata alla sola corrispondenza dei campi Last Name, SSN e Salary, il messaggio che segue attiva una corrispondenza perché soddisfa i criteri:

Robert, Smith, 123-45-6789, 05/29/99, \$42500

Infine il contenuto del messaggio seguente non determina una corrispondenza perché il valore di SSN non è presente nel profilo:

Bob, Smith, 415-789-0000, 05/26/99, \$42500

Vedere ["Configurazione di profili dati esatti"](#) a pagina 484.

Funzionalità della politica EDM

La corrispondenza della politica EDM include la ricerca di contenuto indicizzato in un determinato messaggio o file e la generazione di un incidente se viene rilevata una corrispondenza all'interno dell'intervallo di prossimità definito. L'intervallo di prossimità può essere cambiato modificando l'impostazione avanzata del server

`EDM.SimpleTextProximityRadius.`

Le funzionalità di corrispondenza della politica di EDM includono le seguenti:

- È possibile selezionare qualsiasi numero di colonne per la corrispondenza da un'origine dati definita.
- È possibile definire combinazioni escluse in modo che le corrispondenze rilevate con tali combinazioni non vengano segnalate.
- Quando il sistema crea l'indice, fornisce la convalida del criterio per numeri della previdenza sociale, numeri di carta di credito, numeri telefonici e codici postali di Stati Uniti e Canada, indirizzi e-mail e IP, numeri, percentuali e campi con altri valori.

- C'è un dizionario di parole non significative modificabile e utilizzabile per impedire la corrispondenza di parole non significative con token singolo e per impedire che articoli e preposizioni siano considerati come possibile corrispondenza di campo. Le parole non significative sono parole comuni, ad esempio articoli e preposizioni. Le parole non significative non vengono indicizzate.
- Il sistema fornisce l'evidenziazione delle corrispondenze nella schermata istantanea incidente: i token delle righe corrispondenti sono evidenziati.
- È possibile utilizzare una clausola WHERE nella regola EDM: le corrispondenze che non soddisfano la clausola WHERE verranno ignorate. Ad esempio, è possibile utilizzare una clausola WHERE per la corrispondenza solo con i record in cui il paese del cliente è Stati Uniti.
- È possibile usare l'eccezione Proprietario dati per ignorare il rilevamento in base all'indirizzo e-mail o al dominio del mittente o del destinatario. L'eccezione Proprietario dati consente di autorizzare o applicare tag a un campo specifico nel Profilo dati esatti come proprietario dei dati. Al momento dell'esecuzione, se il mittente o il destinatario dei dati viene autorizzato come proprietario dei dati, la condizione non avvia una corrispondenza e i dati sono inviati o ricevuti dal proprietario.
- È possibile usare la corrispondenza gruppo directory (DGM, Directory Group Matching) con profili per la corrispondenza con mittenti o destinatari di dati in base a indirizzo e-mail o nome utente di Windows.
- Intervallo di corrispondenza per prossimità proporzionale al numero di corrispondenze richieste impostate nella condizione della politica.
- Supporto completo dell'indicizzazione e corrispondenza di celle a token singolo e multitoken. Una cella multitoken è una cella indicizzata che contiene due o più parole. Poiché un singolo carattere CJK (Cinese, Giapponese, Coreano) viene considerato come un token, due o più caratteri CJK vengono considerati come un multitoken.

Vedere ["Modelli di politica EDM"](#) a pagina 476.

Modelli di politica EDM

Symantec Data Loss Prevention fornisce vari modelli di politica che includono EDM. Se si utilizza uno di questi modelli, il sistema consente di convalidare il Profilo dati esatti rispetto al modello durante la configurazione del profilo.

- Relazione Caldicott
Vedere ["Modello della politica Relazione Caldicott"](#) a pagina 1319.
- Protezione dei dati dei clienti
Vedere ["Modello di politica Protezione dei dati dei clienti"](#) a pagina 1325.
- Data Protection Act (legge sulla protezione dei dati) del 1988

Vedere ["Modello della politica Data Protection Act 1998 \(legge sulla protezione dei dati del 1998\)"](#) a pagina 1327.

- Protezione dei dati dei dipendenti
Vedere ["Modello di politica Protezione dei dati dei dipendenti"](#) a pagina 1333.
- Direttive UE sulla protezione dei dati
Vedere ["Modello della politica Direttive UE sulla protezione dei dati"](#) a pagina 1329.
- Export Administration Regulations (EAR, normativa sulla gestione delle esportazioni)
Vedere ["Modello di politica Export Administration Regulations \(EAR\)"](#) a pagina 1335.
- FACTA 2003 (regole Red Flag)
- Regolamento generale per la protezione dei dati (GDPR) - Attività bancarie e finanza
Vedere ["Regolamento generale per la protezione dei dati \(attività bancarie e finanza\)"](#) a pagina 1342.
- Regolamento generale per la protezione dei dati (GDPR) - Identità digitale
Vedere ["Regolamento generale per la protezione dei dati \(attività bancarie e finanza\)"](#) a pagina 1342.
- Regolamento generale per la protezione dei dati (GDPR) - Identificazione governativa
Vedere ["Regolamento generale per la protezione dei dati \(identificazione governativa\)"](#) a pagina 1365.
- Regolamento generale per la protezione dei dati (GDPR) - Sanità e assicurazioni
Vedere ["Regolamento generale per la protezione dei dati \(sanità e assicurazioni\)"](#) a pagina 1389.
- Regolamento generale per la protezione dei dati (GDPR) - Profilo personale
Vedere ["Regolamento generale per la protezione dei dati \(profilo personale\)"](#) a pagina 1401.
- Regolamento generale per la protezione dei dati (GDPR) - Viaggi
Vedere ["Regolamento generale per la protezione dei dati \(viaggi\)"](#) a pagina 1404.
- Gramm-Leach-Bliley
Vedere ["Modello di politica Gramm-Leach-Bliley"](#) a pagina 1414.
- HIPAA e HITECH (incluso PHI)
Vedere ["Modello di politica HIPAA e HITECH \(incluso PHI\)"](#) a pagina 1416.
- Human Rights Act (legge sui diritti umani) del 1998
Vedere ["Modello di politica Human Rights Act \(legge sui diritti umani\) del 1998"](#) a pagina 1421.
- International Traffic in Arms Regulations (ITAR, normativa sul traffico internazionale di armi)
Vedere ["Modello di politica International Traffic in Arms Regulations \(ITAR\)"](#) a pagina 1422.
- Payment Card Industry Data Security Standard

Vedere ["Modello della politica Payment Card Industry \(PCI\) Data Security Standard"](#) a pagina 1437.

- PIPEDA
Vedere ["Modello di politica PIPEDA"](#) a pagina 1439.
- Informazioni sui prezzi
Vedere ["Modello di politica Informazioni sui prezzi"](#) a pagina 1441.
- Curriculum
Vedere ["Modello della politica Curriculum"](#) a pagina 1444.
- Privacy dei dati relativi allo stato
Vedere ["Modello della politica Normativa sull'imparzialità della trasparenza SEC"](#) a pagina 1447.

Vedere ["Creazione e modifica di profili dati esatti"](#) a pagina 492.

Vedere ["Sfruttamento dei modelli di politica EDM quando possibile"](#) a pagina 562.

Informazioni sul profilo dati esatti e sull'indice

Il **Profilo dati esatti** è la configurazione definita dall'utente creata prima dell'indicizzazione per indicizzare l'origine dati. L'indice è un insieme di file sicuri che contengono hash dei valori di dati esatti di ogni campo nell'origine dati, oltre a informazioni su quei valori di dati. L'indice non contiene i valori di dati.

L'indice generato consiste di 19 file `DataSource.rdx` binari, ciascuno con spazio integrabile nella RAM sui server di rilevamento. Per impostazione predefinita, Symantec Data Loss Prevention memorizza i file di indice in `C:\ProgramData\Symantec\Data Loss Prevention\Server Platform Common\15.1\Protect\index` (su Windows) o in `/var/Symantec/DataLossPrevention/Server Platform Common/15.1/Protect/index` (su Linux) sull'Enforce Server.

Symantec Data Loss Prevention distribuisce automaticamente gli indici EDM (file `*.rdx`) nella directory `indice` su tutti i server di rilevamento. Quando una politica attiva che fa riferimento a un profilo EDM è distribuita a un server di rilevamento, quest'ultimo carica l'indice EDM corrispondente nella RAM. Se un nuovo server di rilevamento viene aggiunto dopo che un indice è stato creato, i file `*.rdx` nella cartella `indice` sull'Enforce Server vengono distribuiti nella cartella `indice` sul nuovo server di rilevamento. Non è possibile distribuire manualmente i file di indice ai server di rilevamento.

Durante il rilevamento, il sistema converte il contenuto estratto in valori di dati con hash utilizzando lo stesso algoritmo che impiega per gli indici. Confronta quindi i valori di dati del contenuto input con quelli nei file di indice appropriati, identificando le corrispondenze.

Vedere ["Creazione e modifica di profili dati esatti"](#) a pagina 492.

Vedere ["Requisiti di memoria per EDM"](#) a pagina 532.

Informazioni sul file origine dati esatti

Il file origine dati è un file tabulare che contiene, in un formato delimitato standard (virgola, punto e virgola, barra verticale o tabulazione), i dati che sono stati estratti da un database, un foglio di calcolo o un'altra origine dati strutturata e puliti per il profiling. Caricare il file origine dati in Enforce Server quando si definisce il **profilo di dati esatti**. Ad esempio, è possibile convertire un foglio di calcolo Excel in un formato con valori separati da virgole (CSV) e il file *.csv risultante può essere utilizzato come origine dati per il profilo EDM.

Vedere ["Informazioni sulla pulizia del file origine dati esatti"](#) a pagina 480.

Vedere ["Creazione del file origine dati esatti per EDM"](#) a pagina 486.

È possibile usare il preindicizzatore SQL per indicizzare direttamente l'origine dati. Tuttavia questo approccio presenta alcune limitazioni perché nella maggior parte dei casi i dati devono venire puliti prima di essere indicizzati.

Vedere ["Indicizzazione EDM remota"](#) a pagina 539.

Il file origine dati deve contenere almeno un campo di colonna univoco. Un campo di colonna univoco è una colonna che contiene prevalentemente valori univoci. È possibile avere valori duplicati, ma non in numero superiore a quello impostato in `term_commonority_threshold`. Il valore predefinito per questa impostazione è 10. Tra gli esempi di campi di colonna univoci figurano il codice fiscale, il numero di patente di guida e il numero di carta di credito.

Vedere ["Best practice per l'utilizzo dell'EDM"](#) a pagina 557.

Il numero massimo di colonne per un file di origine dati singola è 32. Se il file origine dati ha più di 32 colonne, la console di amministrazione di Enforce Server restituisce un messaggio di errore nella schermata del profilo e il file origine dati non viene indicizzato. Il numero massimo di righe è 4.294.967.294 e il numero totale di celle in un singolo file origine dati non deve eccedere 6 miliardi di celle. Se il file origine dati è più grande, dividerlo in più file e indicizzare ciascun file separatamente.

La [Tabella 22-1](#) riepiloga le limitazioni delle dimensioni per i file origine dati EDM.

Nota: Il formato per il file origine dati deve essere un formato basato su testo con contenuti delimitati da virgole, punti e virgola, barre verticali o tabulazioni. In generale è necessario evitare di utilizzare un formato di foglio di calcolo per il file origine dati (ad esempio, XLS o XLSX) perché tali programmi utilizzano notazioni scientifiche per eseguire il rendering dei numeri.

Tabella 22-1 Limitazioni delle dimensioni del file origine dati EDM

File origine dati	Limite	Descrizione
Colonne	32	Il file origine dati non può avere più di 32 colonne. In caso contrario il sistema non lo indicizza.

File origine dati	Limite	Descrizione
Celle	6 miliardi	Il file origine dati non può avere più di 6 miliardi di celle di dati. In caso contrario il sistema non lo indicizza.
Righe	4.294.967.294	Il numero massimo di righe supportato è 4.294.967.294.

Informazioni sulla pulizia del file origine dati esatti

Una volta creato il file origine dati, è necessario preparare i dati per l'indicizzazione eseguendo una pulizia. L'operazione di pulizia è essenziale per garantire che le politiche EDM siano il più possibile accurate. È possibile utilizzare strumenti quali Stream Editor (sed) e AWK per la pulizia del file origine dati. Melissa Data offre strumenti ottimali per la normalizzazione dei dati nell'origine dati, ad esempio gli indirizzi.

La [Tabella 22-2](#) fornisce il flusso di lavoro per la pulizia del file origine dati ai fini dell'indicizzazione.

Tabella 22-2 Flusso di lavoro per la pulizia del file origine dati

Passaggio	Azione	Descrizione
1	Preparare il file origine dati per l'indicizzazione.	Vedere "Preparazione del file origine dati esatti per l'indicizzazione" a pagina 488.
2	Verificare che l'origine dati abbia almeno una colonna di dati univoci.	Vedere "Verifica della presenza di almeno una colonna di dati univoci nell'origine dati" a pagina 558.
3	Rimuovere i record incompleti e duplicati. Non riempire le celle vuote con dati simulati.	Vedere "Eliminazione di colonne vuote e righe duplicate dal file origine dati" a pagina 559.
4	Rimuovere i caratteri non adatti.	Vedere "Rimozione di tipi di carattere ambigui dal file origine dati" a pagina 560.
5	Verificare che il file origine dati sia sotto la soglia di errore. La Soglia di errore è la percentuale massima di righe che possono contenere errori prima dell'arresto dell'indicizzazione.	Vedere "Preparazione del file origine dati esatti per l'indicizzazione" a pagina 488.

Informazioni sull'utilizzo di campi di sistema per la convalida di origini dati

Le intestazioni di colonne nell'origine dati sono utili come riferimento visivo. Tuttavia, non indicano a Symantec Data Loss Prevention che tipo di dati le colonne contengono. A questo proposito, si utilizza la sezione **Mapping campi** del **profilo dati esatti** per specificare i mapping

tra i campi nell'origine dati. È anche possibile utilizzare i mapping dei campi per specificare i campi che il sistema riconosce nei modelli di politica forniti dal sistema. La sezione **Mapping campi** include anche opzioni avanzate per specificare campi personalizzati e convalidare i dati in quei campi.

Vedere ["Mapping dei campi del profilo dati esatti"](#) a pagina 496.

Considerare il seguente esempio di utilizzo dei mapping dei campi. Una società vuole proteggere i dati dei suoi dipendenti, inclusi i numeri di codice fiscale. Si crea quindi una politica di Data Loss Prevention basata sul modello Protezione dei dati dei dipendenti. La politica richiede un indice di dati esatti con campi per i numeri di codice fiscale e altri dati dei dipendenti. Si prepara l'origine dati e si crea il **profilo dati esatti**. Per convalidare i dati nel campo del numero di codice fiscale, si esegue il mapping di questo campo di colonna nell'indice al criterio di campo di sistema "Numero di codice fiscale". Il sistema convalida quindi tutti i dati in quel campo utilizzando la convalida Numero di codice fiscale per assicurare che ogni elemento sia un numero di codice fiscale.

L'utilizzo di criteri di campo definiti dal sistema per convalidare i dati è essenziale per l'accuratezza delle politiche EDM. Se non si ha un criterio di campo definito dal sistema che corrisponde a uno o più campi di dati nell'indice, è possibile definire campi personalizzati e scegliere la convalida appropriata per convalidare i dati.

Vedere ["Mappaggio delle colonne origine dati ai campi di sistema per utilizzare la convalida"](#) a pagina 561.

Informazioni sulla pianificazione degli indici

Dopo l'indicizzazione di un'estrazione esatta dell'origine dati, lo schema corrispondente non può essere modificato perché il file indice *.rdx è binario. Se l'origine dati cambia o cambia il numero di colonne o il mapping dei dati del file origine dati esatti, è necessario creare un nuovo indice EDM e aggiornare le politiche che fanno riferimento ai dati che sono cambiati. In questo caso è possibile pianificare l'indicizzazione in modo da mantenere l'indice in sincronia con l'origine dati.

Il caso di utilizzo tipico è il seguente. Si estraggono i dati da un database in un file e si effettua la pulizia per creare il file origine dati. Mediante la console di amministrazione di Enforce Server si definisce un Profilo dati esatti e si indicizza il file origine dati. Il sistema genera i file indice *.rdx e li distribuisce a uno o più server di rilevamento. Tuttavia, se si sa che i dati cambiano frequentemente, è necessario generare un nuovo file origine dati ogni settimana o mese per incorporare le modifiche apportate al database. In questo caso, è possibile usare la pianificazione indice per automatizzare l'indicizzazione del file origine dati, in modo da non dover tornare alla console di amministrazione di Enforce Server per reindicizzare l'origine dati aggiornata. L'unica attività necessaria è quella di posizionare un file origine dati aggiornato e ottimizzato in Enforce Server per l'indicizzazione pianificata.

Nota: È necessario reindicizzare dopo l'upgrade a Symantec Data Loss Prevention 15.1.

Vedere ["Configurazione di profili dati esatti"](#) a pagina 484.

Vedere ["Pianificazione dell'indicizzazione di profili dati esatti"](#) a pagina 499.

Vedere ["Utilizzo dell'indicizzazione pianificata per automatizzare gli aggiornamenti del profilo"](#) a pagina 564.

Informazioni sulla condizione Il contenuto corrisponde ai dati esatti da

La condizione **Il contenuto corrisponde ai dati esatti da un profilo dati esatti** è il componente di rilevamento utilizzato per implementare le condizioni delle politiche EDM. Quando si definisce questa condizione, selezionare il profilo EDM sui cui si basa la condizione. Selezionare inoltre le colonne da utilizzare nella condizione, nonché eventuali limitazioni della clausola WHERE.

Nota: non è possibile utilizzare la condizione **Il contenuto corrisponde ai dati esatti da un profilo dati esatti** come eccezione di politica. Symantec Data Loss Prevention non supporta l'utilizzo della condizione EDM come eccezione di politica.

Vedere ["Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti"](#) a pagina 503.

Informazioni sull'eccezione Proprietario dati

Sebbene EDM non supporti l'uso esplicito delle eccezioni di corrispondenza nelle politiche, esso supporta le eccezioni di corrispondenza basate su criteri. Questa funzionalità di EDM è nota come **Eccezione Proprietario dati**. L'eccezione Proprietario dati consente di autorizzare o applicare tag a un campo specifico nel Profilo dati esatti come proprietario dei dati. Al momento dell'esecuzione, se il mittente o il destinatario dei dati viene autorizzato come proprietario dei dati, la condizione non avvia una corrispondenza e i dati sono inviati o ricevuti dal proprietario.

L'eccezione del Proprietario dati viene implementata includendo il campo di indirizzo e-mail o il campo di dominio nel **Profilo dati esatti**. Nella condizione della politica EDM, specificare il campo come mittente o proprietario dei dati del destinatario. Un proprietario di dati autorizzato, identificato tramite l'indirizzo di posta elettronica o l'indirizzo di dominio, può inviare informazioni riservate senza causare una corrispondenza EDM o un incidente. Ciò significa che il mittente può inviare qualsiasi informazione contenuta nella riga in cui è specificato il suo indirizzo e-mail o il dominio. È possibile specificare singoli destinatari autorizzati del proprietario o tutti i destinatari nell'elenco in modo da autorizzarli a ricevere i dati senza causare una corrispondenza.

Come autore della politica, l'eccezione Proprietario dati offre la flessibilità di consentire ai proprietari di dati di utilizzare i loro dati legittimamente. Ad esempio, se viene attivata l'eccezione Proprietario dati, un dipendente può inviare un'e-mail contenente i propri dati riservati (ad esempio un codice fiscale) senza causare una corrispondenza o un incidente. Analogamente, se l'eccezione Proprietario dati è configurata per un destinatario, il sistema non genera una corrispondenza EDM o un incidente se il proprietario dei dati riceve le proprie informazioni, ad esempio quando qualcuno al di fuori dell'azienda invia un'e-mail al proprietario dei dati contenente il numero di conto del proprietario dei dati stesso.

Vedere ["Informazioni sull'upgrade delle distribuzioni EDM"](#) a pagina 484.

Vedere ["Creazione del file origine dati esatti per l'eccezione Proprietario dati"](#) a pagina 487.

Vedere ["Configurazione dell'eccezione Proprietario dati per le condizioni della politica EDM"](#) a pagina 505.

Informazioni su Directory Group Matching (DGM) con profilo

Directory Group Matching (DGM) con profilo è un'implementazione specializzata di EDM utilizzata per rilevare l'identità esatta di un utente, mittente o destinatario di un messaggio il cui profilo è stato definito da un server di directory o da un database.

DGM con profilo si basa sulla tecnologia EDM per individuare identità indicizzate dal database o dal server di directory mediante un Profilo dati esatti. Ad esempio, è possibile usare DGM con profilo per identificare l'attività dell'utente in rete o per analizzare i contenuti associati a determinati utenti, mittenti o destinatari. Oppure, è possibile escludere dall'analisi determinati indirizzi e-mail. O ancora potrebbe risultare utile impedire a determinati utenti l'invio di informazioni riservate tramite e-mail.

Per implementare DGM con profilo, il file origine dati esatti deve contenere uno o più dei seguenti campi:

- Indirizzo e-mail
- Indirizzo IP
- Nome utente Windows
- Nome IM

Se si include il campo dell'indirizzo e-mail nel profilo DGM, il campo appare nell'elenco a discesa **Directory EDM** nella schermata dell'istantanea incidente della console di Enforce Server, il che semplifica la riparazione.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Vedere ["Inclusione di un campo per l'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo"](#) a pagina 567.

Vedere ["Utilizzo della DGM con profilo per il rilevamento di identità di Network Prevent for Web"](#) a pagina 567.

Informazioni sul rilevamento in due fasi per l'EDM sull'endpoint

L'indice EDM è basato sul server. Se si distribuisce una politica contenente una condizione EDM a DLP Agent sull'endpoint, il sistema utilizza il rilevamento in due fasi per valutare i dati per la corrispondenza. La condizione di rilevamento EDM non viene valutata localmente dal DLP Agent. DLP Agent invia invece i dati a Endpoint Server per la valutazione in base all'indice. Se l'endpoint non è in linea, il messaggio non può essere inviato fintantoché il server è disponibile, il che può influenzare le prestazioni dell'endpoint. Inoltre, il rilevamento in due fasi non è in grado di bloccare, crittografare o notificare. Symantec non consiglia il rilevamento in due fasi.

Vedere ["Rilevamento in due fasi per DLP Agent."](#) a pagina 403.

Per verificare se il rilevamento in due fasi è in uso, vedere il registro c:

```
\ProgramData\Symantec\Data Loss Prevention\Detection  
Server\15.1\logs\debug\FileReader.log
```

 su Endpoint Server per determinare se sono caricati indici EDM. Cercare la riga che conferma che il profilo del database è stato caricato.

Vedere ["Risoluzione dei problemi delle politiche"](#) a pagina 458.

Informazioni sull'upgrade delle distribuzioni EDM

Per sfruttare gli ultimi miglioramenti EDM, è necessario aggiornare i server a Symantec Data Loss Prevention 15.1 e reindicizzare le origini dati EDM con l'indicizzatore EDM 15.1. La reindicizzazione deve essere eseguita dopo l'upgrade di tutti i server. In tal caso, i server di rilevamento precedenti possono continuare a lavorare con gli indici precedenti mentre si esegue l'upgrade.

Vedere ["Informazioni sull'eccezione Proprietario dati"](#) a pagina 482.

Vedere ["Aggiornamento degli indici EDM alla versione più recente"](#) a pagina 527.

Vedere ["Requisiti di memoria per EDM"](#) a pagina 532.

Vedere ["Codici di errore per indice EDM obsoleto"](#) a pagina 531.

Configurazione di profili dati esatti

Per implementare EDM, creare il **profilo dati esatti**, indicizzare l'origine dati e definire una o più condizioni di corrispondenza contenuto con i dati esatti per la corrispondenza esatta con dati con profilo.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Tabella 22-3 Implementazione di Exact Data Matching

Passaggio	Azione	Descrizione
1	Creare il file origine dati.	<p>Esportare l'origine dati dal database (o altro archivio dati) a un file di testo tabulare con campi delimitati.</p> <p>Se si desidera escludere i proprietari di dati dalla corrispondenza, è necessario includere specifici elementi di dati nel file origine dati.</p> <p>Vedere "Informazioni sul file origine dati esatti" a pagina 479.</p> <p>Se si desidera cercare la corrispondenza con identità per Directory Group Matching (DGM) con profilo, è necessario includere specifici elementi di dati nei file origine dati.</p> <p>Vedere "Creazione del file origine dati esatti per EDM" a pagina 486.</p> <p>Vedere "Creazione del file origine dati esatti per DGM con profilo" a pagina 487.</p>
2	Preparare il file origine dati per l'indicizzazione.	<p>Ripulire il file di origine dati.</p> <p>Vedere "Preparazione del file origine dati esatti per l'indicizzazione" a pagina 488.</p>
3	Caricare il file origine dati in Enforce Server.	<p>È possibile copiare o caricare il file origine dati in Enforce Server, o accedervi a distanza.</p> <p>Vedere "Caricamento di file origine dati esatti in Enforce Server" a pagina 490.</p>
4	Creare un profilo dati esatti.	<p>Un profilo dati esatti è richiesto di implementare le politiche EDM. Il profilo dati esatti specifica l'origine dati, i tipi di campo dati e la pianificazione dell'indicizzazione.</p> <p>Vedere "Creazione e modifica di profili dati esatti" a pagina 492.</p>
5	Mappare e convalidare i campi dati.	<p>Mappare i campi dell'origine dati ai tipi di dati personalizzati o del sistema che il sistema convalida. Ad esempio, un campo dati relativo al numero di previdenza sociale deve avere nove cifre.</p> <p>Vedere "Informazioni sull'utilizzo di campi di sistema per la convalida di origini dati" a pagina 480.</p> <p>Vedere "Mapping dei campi del profilo dati esatti" a pagina 496.</p>
6	Indicizzare l'origine dati o pianificare l'indicizzazione.	<p>Pianificare l'indicizzazione in modo da mantenere l'indice in sincronia con l'origine dati. Vedere "Informazioni sulla pianificazione degli indici" a pagina 481.</p> <p>Vedere "Pianificazione dell'indicizzazione di profili dati esatti" a pagina 499.</p>

Passaggio	Azione	Descrizione
7	Configurare e ottimizzare una o più condizioni della politica Corrispondenze contenuto dati esatti	Vedere "Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti" a pagina 503.

Creazione del file origine dati esatti per EDM

Il primo passaggio nel processo di indicizzazione EDM è di creare l'origine dati. Un'origine dati è un file in formato tabulare che contiene dati in un formato delimitato standard, in cui i dati sono delimitati da virgole, punti e virgola, barre verticali o tabulazioni.

Se si prevede di utilizzare un modello di politica, esaminarlo prima di creare il file origine dati per determinare quali campi di dati la politica utilizza. Per le origini dati relativamente piccole, includere nell'origine dati il maggior numero possibile di campi consigliati. Da notare tuttavia che più campi si includono, maggiore sarà la quantità di memoria utilizzata dall'indice risultante. Questa considerazione è importante se si dispone di una grande origine dati. Quando si crea il profilo dati, è possibile confermare la corrispondenza tra i campi dell'origine dati e i campi consigliati per il modello.

Vedere [Tabella 22-4](#) a pagina 486.

Tabella 22-4 Creazione del file origine dati esatti

Passaggio	Descrizione
1	<p>Esportare i dati che si desidera proteggere da una database o altro formato di dati tabulare, come un foglio Excel, in un file flat. Il file origine dati creato deve essere un file di testo tabulare che contiene righe di dati dell'origine originale. Ogni riga dell'origine originale è inclusa come riga nel file origine dati. Delimitare le colonne utilizzando un carattere di tabulazione, una virgola o una barra verticale. La barra verticale è il delimitatore preferito. Non utilizzare la virgola se i campi dell'origine dati contengono numeri.</p> <p>Vedere "Informazioni sul file origine dati esatti" a pagina 479.</p> <p>È necessario mantenere tutti i dati strutturati esportati dalla tabella del database di origine o dal formato di tipo tabella in un file origine dati. Non è possibile suddividere l'origine dati in più file.</p> <p>Il file di origine dati non può includere più di 32 colonne, 4.294.967.294 miliardi di righe o 6 miliardi celle. Se si prevede di caricare il file origine dati in Enforce Server, la capacità del browser limita la dimensione dell'origine dati a 2 GB. Per le dimensioni di file superiore a questa dimensione è possibile copiare il file nell'Enforce Server utilizzando FTP/S, SCP, SFTP, NFS o CIFS.</p>

Passaggio	Descrizione
2	<p>Includere i campi di dati richiesti per specifiche implementazioni EDM:</p> <ul style="list-style-type: none"> ■ Dati univoci Per tutte le implementazioni EDM, assicurarsi che l'origine dati contenga almeno una colonna di dati univoci. Vedere "Verifica della presenza di almeno una colonna di dati univoci nell'origine dati" a pagina 558. ■ Eccezione Proprietario dati Assicurarsi che l'origine dati contenga il campo dell'indirizzo e-mail o quello del dominio, se si intendono utilizzare le eccezioni Proprietario dati. Vedere "Creazione del file origine dati esatti per l'eccezione Proprietario dati" a pagina 487. ■ Directory Group Matching Assicurarsi che l'origine dati includa uno o più campi di identificazione mittente/destinatario. Vedere "Creazione del file origine dati esatti per DGM con profilo" a pagina 487.
3	<p>Preparare il file origine dati per l'indicizzazione.</p> <p>Vedere "Preparazione del file origine dati esatti per l'indicizzazione" a pagina 488.</p>

Creazione del file origine dati esatti per l'eccezione Proprietario dati

Per implementare l'eccezione Proprietario dati ed escludere i proprietari dei dati dal rilevamento, è necessario includere esplicitamente l'indirizzo e-mail o l'indirizzo del dominio di ciascun utente nel Profilo dati esatti. Ogni dominio previsto (ad esempio **symantec.com**) deve essere aggiunto esplicitamente al profilo dati esatti. Il sistema non rileva automaticamente le corrispondenze nei sottodomini (ad esempio, **support.symantec.com**). Ogni sottodominio previsto deve essere aggiunto esplicitamente al profilo dati esatti.

Per implementare la funzionalità dell'eccezione Proprietario dati è necessario includere uno o entrambi i seguenti campi nel file origine dati:

- Indirizzo e-mail, come john_smith@symantec.com
- Indirizzo di dominio, ad esempio symantec.com

Vedere ["Informazioni sull'eccezione Proprietario dati"](#) a pagina 482.

Vedere ["Configurazione dell'eccezione Proprietario dati per le condizioni della politica EDM"](#) a pagina 505.

Creazione del file origine dati esatti per DGM con profilo

DGM con profilo si basa sulla tecnologia Exact Data Matching (EDM) per rilevare identità in modo preciso. Gli attributi relativi alle identità possono includere indirizzo IP, indirizzo e-mail, nome utente, unità operativa, reparto, responsabile, titolo o stato lavorativo. Altri attributi possono essere il consenso del dipendente ad essere monitorato o l'autorizzazione del

dipendente ad accedere a informazioni riservate. Per implementare DGM con profilo, è necessario includere almeno un campo dati obbligatorio nell'origine dati.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

[Tabella 22-5](#) elenca i campi obbligatori per DGM con profilo. Il file origine dati deve contenere almeno uno di questi campi.

Tabella 22-5 Campi origine dati per DGM con profilo

Campo	Descrizione
Indirizzo e-mail	Se si utilizza un campo della colonna degli indirizzi e-mail del file origine dati, l'indirizzo e-mail è visualizzato nell'elenco a discesa Directory EDM della schermata dell'istantanea incidente.
Indirizzo IP	Ad esempio: 172.24.56.33
Nome utente Windows	Se si utilizza un nome utente Windows nell'origine dati, i dati devono essere nel formato domain\user, ad esempio ACME\john_smith.
Nome AOL IM	Nome schermata IM
Nome Skype	Ad esempio: myscreename123
Nome Microsoft Office Communicator	

Preparazione del file origine dati esatti per l'indicizzazione

Dopo aver creato il file origine dati esatti, è necessario prepararlo in modo da poter indicizzare in modo efficace i dati che si desidera proteggere.

Quando si esegue l'indicizzazione di un profilo dati esatti, Enforce Server tiene traccia delle celle vuote e di tutti i dati non trovati che vengono conteggiati come errori. Ad esempio, un errore può essere un nome che compare in una colonna per numeri di telefono. Gli errori possono costituire una determinata percentuale dei dati nel profilo (per impostazione predefinita, il cinque per cento). Se questa soglia di errore predefinita viene superata, Symantec Data Loss Prevention arresta l'indicizzazione. Visualizza quindi un errore per indicare che i dati possono essere destrutturati o danneggiati.

Per preparare l'origine dati esatti per l'indicizzazione EDM

- 1 Assicurarsi che il file origine dati esatti sia formattato nel modo seguente:
 - Se l'origine dati ha più di 200.000 righe, verificare che abbia almeno due colonne di dati. Una delle colonne deve contenere valori univoci. Ad esempio, numeri di carta di credito, numeri di patente di guida o numeri di conto (anziché nome e cognome, che sono valori generici).

Vedere ["Verifica della presenza di almeno una colonna di dati univoci nell'origine dati"](#) a pagina 558.

- Verificare di aver delimitato l'origine dati utilizzando barre verticali (|) o tabulazioni. Se il file origine dati usa le virgole come delimitatori, rimuovere quelle non utilizzate come delimitatori.
 Vedere ["Mancato utilizzo del delimitatore virgola se l'origine dati ha campi numerici"](#) a pagina 561.
- Verificare che i valori di dati non siano racchiusi tra virgolette.
- Rimuovere i valori di dati con un unico carattere o abbreviati dall'origine dati. Ad esempio, rimuovere il nome della colonna e tutti i valori per una colonna in cui i valori possibili sono S e N.
- Facoltativamente, rimuovere tutte le colonne che contengono valori numerici con meno di cinque cifre, in quanto possono provocare falsi positivi in fase di produzione.
 Vedere ["Rimozione di tipi di carattere ambigui dal file origine dati"](#) a pagina 560.
- Verificare che i numeri, come le carte di credito o i codici fiscali, siano delimitati internamente da trattini, spazi o che non abbiano alcun delimitatore. Assicurarsi di non utilizzare un delimitatore quale una virgola come delimitatore interno in tali numeri. Ad esempio: 123-45-6789, 123 45 6789 o 123456789 sono validi, ma non 123,45,6789.
 Vedere ["Mancato utilizzo del delimitatore virgola se l'origine dati ha campi numerici"](#) a pagina 561.
- Eliminare i record duplicati, che possono causare incidenti duplicati.
 Vedere ["Eliminazione di colonne vuote e righe duplicate dal file origine dati"](#) a pagina 559.
- Non indicizzare valori comuni. EDM funziona al meglio con valori univoci. È importante riflettere sui dati che si desidera indicizzare (e quindi proteggere). Questi dati sono veramente importanti? Se il valore è molto comune, non è utile come valore EDM. Ad esempio, si supponga di voler cercare "stati USA". Poiché ci sono solo 50 stati, se il profilo dati esatti ha 300.000 righe, il risultato conterrà molti duplicati di valori comuni. Symantec Data Loss Prevention indicizza tutti i valori nel profilo dati esatti, indipendentemente dall'uso o meno dei dati in una politica. È buona pratica usare i valori che sono meno comuni e preferibilmente univoci per ottenere i migliori risultati con EDM.
 Vedere ["Verifica della presenza di almeno una colonna di dati univoci nell'origine dati"](#) a pagina 558.

- 2 Dopo aver preparato il file origine dati esatti, procedere con il passaggio seguente del processo EDM: caricare il file origine dati esatti su Enforce Server per il profiling dei dati che si desidera proteggere.

Vedere ["Caricamento di file origine dati esatti in Enforce Server"](#) a pagina 490.

Caricamento di file origine dati esatti in Enforce Server

Dopo la preparazione del file origine dati per l'indicizzazione, caricarlo in Enforce Server di modo che l'origine dati possa essere indicizzata.

Vedere ["Creazione e modifica di profili dati esatti"](#) a pagina 492.

Di seguito sono riportate le opzioni mediante le quali rendere disponibile il file origine dati a Enforce Server. Consultare l'amministratore del database per determinare il migliore metodo per le proprie esigenze.

Tabella 22-6 Caricamento del file origine dati su Enforce Server per l'indicizzazione

Opzioni di caricamento	Caso di utilizzo	Descrizione
Carica origine dati sul server ora	Il file di origine dati è inferiore a 50 MB	<p>Se si ha un file origine dati di piccole dimensioni (fino a 50 MB), caricarlo su Enforce Server utilizzando la console di amministrazione di Enforce Server (interfaccia Web). Quando si crea il profilo dati esatti, è possibile specificare il percorso del file o selezionare la directory e caricare il file origine dati.</p> <p>Nota: A causa dei limiti di capacità del browser, è possibile caricare file di non più di 2 GB. Tuttavia, il caricamento di qualsiasi file oltre i 50 MB non è consigliato poiché per i file di dimensione maggiore potrebbe richiedere molto tempo. Se il file origine dati è superiore a 50 MB, considerare la possibilità di copiare il file origine dati nella directory <code>datafiles</code> utilizzando l'opzione seguente.</p>
Usa origine dati nell'host manager come riferimento	Il file di origine dati è superiore a 50 MB	<p>Se si ha un file origine dati di grandi dimensioni (oltre 50 MB), copiarlo nella directory <code>datafiles</code> sull'host in cui Enforce è installato.</p> <ul style="list-style-type: none">■ In Windows questa directory si trova in <code>\Programmi\Symantec\Data Loss Protection\Enforce Server\15.1\Protect\datafiles</code>.■ In Linux questa directory si trova in <code>/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/datafiles</code>. <p>Questa opzione è utile in quanto rende il file di dati disponibile mediante un elenco a discesa durante la configurazione del Profilo dati esatti. Se il file è di grandi dimensioni, usare una soluzione di terze parti (come Secure FTP) per trasferire il file origine dati a Enforce Server.</p> <p>Nota: Assicurarsi che l'utente Enforce (in genere denominato "protect") disponga delle autorizzazioni di modifica (in Windows) o lettura/scrittura (in Linux) per tutti i file nella directory <code>datafiles</code>.</p>

Opzioni di caricamento	Caso di utilizzo	Descrizione
Usa questo nome file	Il file di origine dati non è ancora stato creato	<p>Si desidera creare un profilo EDM prima di aver creato il file di origine dati. In questo caso è possibile creare un modello di profilo e specificare il nome del file origine dati che si intende creare. Questa opzione consente di definire le politiche EDM utilizzando il modello di profilo EDM prima di indicizzare l'origine dati. Le politiche non sono attive fino all'indicizzazione dell'origine dati. Quando è stato creato il file di origine dati, posizionarlo nella directory <code>\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\datafiles</code> e indicizzare immediatamente l'origine dati al salvataggio o pianificare l'indicizzazione.</p> <p>Vedere "Creazione e modifica di profili dati esatti" a pagina 492.</p>
Usa questo nome file e Carica indice generato esternamente	L'origine dati deve essere indicizzata a distanza e copiata in Enforce Server	<p>In alcuni ambienti, può non essere sicuro o fattibile copiare o caricare il file origine dati in Enforce Server. In tal caso, è possibile indicizzare l'origine dati a distanza utilizzando l'indicizzatore EDM remoto.</p> <p>Vedere "Indicizzazione EDM remota" a pagina 539.</p> <p>Questa utilità consente di indicizzare un'origine dati esatti su un computer che non sia l'host di Enforce Server. Questa funzionalità è utile quando non si desidera copiare il file origine dati nello stesso computer di Enforce Server. Ad esempio, considerare una situazione in cui il reparto di origine vuole evitare il rischio di copiare i dati in un host all'esterno del reparto. In questo caso, è possibile utilizzare l'indicizzatore EDM remoto.</p> <p>Creare dapprima un modello di profilo EDM in cui si scelgono le opzioni Usa questo nome file e Numero di colonne. È necessario specificare il nome del file origine dati e il numero di colonne che contiene.</p> <p>Vedere "Creazione del modello di un profilo EDM per l'indicizzazione remota" a pagina 543.</p> <p>Utilizzare quindi l'indicizzatore EDM remoto per indicizzare a distanza l'origine dati e copiare i file di indice nell'host di Enforce Server e caricare l'indice generato esternamente. L'opzione Carica indice generato esternamente è disponibile solo dopo aver definito e salvato il profilo. Gli indici remoti sono caricati dalla directory <code>\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\index</code> sull'host di Enforce Server.</p> <p>Vedere "Copia e caricamento di file di indice remoti su Enforce Server" a pagina 549.</p>

Creazione e modifica di profili dati esatti

La schermata **Gestisci > Profili dati > Dati esatti > Aggiungi profilo dati esatti** è la home page per la gestione e l'aggiunta di profili dati esatti. È necessario un profilo dati esatti per implementare un'istanza della regola di rilevamento Contenuto corrispondente a dati esatti. Un profilo dati esatti specifica l'origine dati, i parametri di indicizzazione e la pianificazione dell'indicizzazione. Dopo aver creato il profilo EDM, indicizzare l'origine dati e configurare uno o più condizioni contenuto corrispondente ai dati esatti che possono essere aggiunte a regole per utilizzare il profilo e rilevare corrispondenze esatte di contenuto.

Vedere ["Configurazione di profili dati esatti"](#) a pagina 484.

Nota: Se si utilizza Remote EDM Indexer per generare il profilo dati esatti, fare riferimento al seguente argomento.

Per creare o modificare un profilo dati esatti

- 1 Assicurarsi di aver creato il file origine dati.
Vedere ["Creazione del file origine dati esatti per EDM"](#) a pagina 486.
- 2 Assicurarsi di aver preparato il file origine dati per l'indicizzazione.
Vedere ["Preparazione del file origine dati esatti per l'indicizzazione"](#) a pagina 488.
- 3 Assicurarsi che l'origine dati contenga il campo dell'indirizzo e-mail o quello del dominio, se si intendono utilizzare le eccezioni Proprietario dati.
Vedere ["Informazioni sull'eccezione Proprietario dati"](#) a pagina 482.
- 4 Nella console di amministrazione di Enforce Server accedere a **Gestisci > Profili dati > Dati esatti**.
- 5 Fare clic su **Aggiungi profilo dati esatti**.
- 6 Immettere un **Nome** descrittivo univoco per il profilo (limitazione di 256 caratteri).
Per comodità, scegliere un nome che descriva il contenuto e il tipo di indice (ad esempio, EDM dati dipendente).
Se si modifica un profilo dati esatti esistente è possibile cambiare il nome del profilo.
- 7 Selezionare una delle seguenti opzioni **Origine dati** per rendere disponibile il file origine dati a Enforce Server:
 - **Carica origine dati sul server ora**
Se si sta creando un nuovo profilo, fare clic su **Sfoglia** e selezionare il file origine dati, o immettere il percorso completo al file origine dati.
Se si sta modificando un profilo esistente, selezionare **Carica ora**.
Vedere ["Caricamento di file origine dati esatti in Enforce Server"](#) a pagina 490.

- **Usa origine dati nell'host manager come riferimento**

Se il file origine dati è stato copiato nella directory `datafiles` su Enforce Server, compare nell'elenco a discesa per la selezione.

Vedere ["Caricamento di file origine dati esatti in Enforce Server"](#) a pagina 490.

- **Usa questo nome file**

Selezionare questa opzione se il file origine dati non è stato ancora creato ma si desidera configurare le politiche EDM utilizzando di un profilo EDM segnaposto. Immettere il nome del file origine dati che si intende creare, compreso il **Numero di colonne** che avrà. Quando si crea l'origine dati, è necessario copiarla nella directory `datafiles`.

Vedere ["Caricamento di file origine dati esatti in Enforce Server"](#) a pagina 490.

Nota: Utilizzare questa opzione con prudenza. Ricordarsi di creare il file origine dati e di copiarlo nella directory `datafiles`. Assegnare al file origine dati il nome esatto immesso qui e includere il numero esatto di colonne specificato.

- **Carica indice generato esternamente**

Selezionare questa opzione se è stato creato un indice su un computer remoto utilizzando Remote EDM Indexer. Questa opzione è disponibile solo dopo aver definito e salvato il profilo. I profili sono caricati dalla directory `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\index` sull'host di Enforce Server.

Vedere ["Caricamento di file origine dati esatti in Enforce Server"](#) a pagina 490.

8 Se la prima riga dell'origine dati contiene **Nomi di colonna** selezionare , **Leggi prima riga come nomi di colonna**.

9 Specificare la **Soglia di errore**, ossia la percentuale massima di righe che possono contenere errori prima dell'arresto dell'indicizzazione.

Un errore dell'origine dati è una cella vuota, una cella con il tipo di dati errato o celle extra nell'origine dati. Ad esempio, un nome in una colonna per numeri di telefono è un errore. Se gli errori superano una determinata percentuale dell'origine dati complessiva (per impostazione predefinita, 5%), il sistema interrompe l'indicizzazione e visualizza un messaggio di errore di indicizzazione. L'indice non viene creato se l'origine dati ha più record non validi di quanto consentito dal valore della soglia di errore. Sebbene sia possibile cambiare il valore di soglia, una percentuale di errori più che minima nell'origine dati può indicare che l'origine dati è danneggiata, in un formato sbagliato o illeggibile. Se è presente una percentuale significativa di errori (10% o più), interrompere l'indicizzazione e ripulire l'origine dati.

Vedere ["Preparazione del file origine dati esatti per l'indicizzazione"](#) a pagina 488.

- 10 Selezionare il **Carattere separatore colonne** (delimitatore) usato per separare i valori nel file origine dati. I delimitatori che è possibile usare sono tabulazioni, virgole o barre verticali.
- 11 Selezionare uno dei seguenti valori di codifica per il contenuto da analizzare, che deve coincidere con la codifica dell'origine dati:
 - **ISO-8859-1 (Latin-1)** (valore predefinito)
La codifica a 8 bit standard per le lingue dell'Europa occidentale che utilizzano l'alfabeto latino.
 - **UTF-8**
Utilizzare questa codifica per tutte le lingue che usano lo standard Unicode 4.0 (tutti i caratteri a byte singolo e doppio), incluse le lingue asiatiche orientali.
 - **UTF-16**
Utilizzare questa codifica per tutte le lingue che usano lo standard Unicode 4.0 (tutti i caratteri a byte singolo e doppio), incluse le lingue asiatiche orientali.

Nota: Assicurarsi di selezionare la codifica corretta. Il sistema non impedisce di creare un profilo EDM utilizzando la codifica sbagliata. Il sistema genera un errore solo al momento del runtime quando la politica EDM tenta di generare una corrispondenza con i dati in entrata. Per assicurarsi di selezionare la codifica corretta, dopo aver fatto clic su **Avanti**, verificare che i nomi di colonna appaiano correttamente. Se i nomi di colonna non sembrano corretti, è stata scelta la codifica sbagliata.

- 12 Fare clic su **Avanti** per passare alla seconda schermata **Aggiungi profilo dati esatti**.
- 13 La sezione **Mapping campi** visualizza le colonne nell'origine dati e il campo a cui è mappata ogni colonna nel profilo dati esatti. Il mapping dei campi nei profili dati esatti esistenti è fisso e, pertanto, non modificabile.

Vedere ["Informazioni sull'utilizzo di campi di sistema per la convalida di origini dati"](#) a pagina 480.

Vedere ["Mapping dei campi del profilo dati esatti"](#) a pagina 496.

Confermare che i nomi di colonna nell'origine dati siano rappresentati esattamente nella colonna **Campo Origine dati**. Se è stata selezionata l'opzione **Nomi di colonna**, la colonna Campo Origine dati elenca i nomi nella prima riga dell'origine dati. Se l'opzione Nomi di colonna non è stata selezionata, la colonna elenca Col 1, Col 2 e così via.

- 14 Nella colonna **Campo di sistema**, selezionare un campo dall'elenco a discesa per ogni campo dell'origine dati. Questo passaggio è necessario se si utilizza un modello di politica o se si desidera verificare la presenza di errori nell'origine dati.

Ad esempio, per un campo di origine dati chiamato NUMERO_CODICE_FISCALE, selezionare **Numero di codice fiscale** dall'elenco a discesa corrispondente. I valori negli elenchi a discesa **Campo di sistema** comprendono tutti i campi suggeriti per tutti i modelli di politica.

- 15 Facoltativamente, specificare e assegnare un nome agli eventuali campi personalizzati (cioè i campi che non sono precompilati negli elenchi a discesa **Campo di sistema**). A questo scopo, eseguire queste operazioni nel seguente ordine:

- Fare clic su **Visualizzazione avanzata** a destra dell'intestazione Mapping campi. Questa schermata visualizza due colonne aggiuntive (**Nome personalizzato** e **Tipo**).
- Per aggiungere un nome di campo di sistema personalizzato, accedere all'elenco a discesa Campo di sistema appropriato. Selezionare **Personalizzato** e digitare il nome nel campo di testo Nome personalizzato corrispondente.
- Per specificare un tipo di criterio (a fini di verifica degli errori), andare all'elenco a discesa Tipo appropriato e selezionare il criterio desiderato. Per visualizzare le descrizioni di tutti i tipi di criterio disponibili, fare clic su **Descrizione** in alto nella colonna.

- 16 Controllare il mapping dei campi rispetto ai campi suggeriti per il modello di politica che si intende utilizzare. A questo scopo, accedere all'elenco a discesa **Verificare il mapping sulla base del modello di politica**, selezionare un modello e fare clic su **Controlla ora** a destra.

Il sistema visualizza un elenco di tutti i campi del modello che non sono stati mappati. A questo punto è possibile tornare indietro e mappare questi campi. In alternativa, è possibile espandere l'origine dati per includere tutti i campi previsti possibili e quindi ricreare il profilo dati esatti. Symantec raccomanda di includere tutti i campi informativi previsti possibili.

- 17 Nella sezione **Indicizzazione** della schermata, selezionare una delle opzioni seguenti:

- **Invia processo di indicizzazione al salvataggio**
Selezionare questa opzione per iniziare a indicizzare l'origine dati quando si salva il profilo dati esatti.
- **Invia processo di indicizzazione secondo pianificazione**
Selezionare questa opzione per indicizzare l'origine dati secondo una pianificazione specifica. Fare una selezione dall'elenco a discesa **Pianifica** e specificare i giorni, le date e le ore secondo necessità.
Vedere ["Informazioni sulla pianificazione degli indici"](#) a pagina 481.

Vedere ["Pianificazione dell'indicizzazione di profili dati esatti"](#) a pagina 499.

18 Fare clic su **Fine**.

Quando Symantec Data Loss Prevention termina l'indicizzazione, elimina l'origine dati originale da Enforce Server. Dopo aver indicizzato un'origine dati, non è possibile cambiarne lo schema. Se si cambia il mapping delle colonne per un'origine dati dopo l'indicizzazione, è necessario creare un nuovo profilo dati esatti.

Al termine del processo di indicizzazione è possibile creare nuove condizioni di contenuto corrispondente a dati esatti che possono essere aggiunti a una regola che fa riferimento al Profilo dati esatti creato.

Vedere ["Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti"](#) a pagina 503.

Mapping dei campi del profilo dati esatti

Dopo aver aggiunto e configurato il file origine dati e le impostazioni, nella schermata **Gestisci > Profili dati > Dati esatti > Aggiungi profilo dati esatti** è possibile eseguire il mapping dei campi dal file origine dati al profilo dati esatti configurato.

Per attivare il controllo errori su un campo in un'origine dati o per usare l'indice con un modello di politica che utilizza un campo di sistema, è necessario eseguire il mapping del campo nell'origine dati al campo di sistema. Nella sezione Mapping campi è possibile eseguire il mapping delle colonne nell'origine dati originale ai campi di sistema nel profilo dati esatti.

Tabella 22-7 Opzioni di mapping dei campi

Campo	Descrizione
Campo Origine dati	<p>Se è stata selezionata l'opzione Nomi di colonna nella schermata Aggiungi profilo dati esatti, questa colonna elenca i valori trovati nella prima riga dell'origine dati. Se questa opzione non è stata selezionata, questa colonna elenca le colonne per nomi generici (come Col 1, Col 2 e così via).</p> <p>Nota: Se si implementa l'eccezione Proprietario dati, è necessario mappare uno o entrambi i campi indirizzo e-mail e dominio.</p> <p>Vedere "Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti" a pagina 503.</p>
Campo di sistema	<p>Selezionare il campo di sistema per ogni colonna.</p> <p>Non è possibile eseguire il mapping di un valore di campo di sistema (eccetto Nessuna selezione) a più di una colonna.</p> <p>Alcuni campi di sistema hanno criteri di sistema associati (come un codice fiscale) mentre altri non ne hanno (come il cognome).</p> <p>Vedere "Utilizzo delle convalide dei criteri fornite dal sistema per i profili EDM" a pagina 498.</p>

Campo	Descrizione
Verificare il mapping sulla base del modello di politica	<p>Selezionare un modello di politica a partire dall'elenco a discesa per verificare il mapping dei campi e fare clic su Controlla ora.</p> <p>Tutti i modelli di politica che EDM implementa sono visualizzati nel menu a discesa, inclusi quelli importati.</p> <p>Vedere "Scelta di un profilo dati esatti" a pagina 417.</p> <p>Se si prevede di utilizzare più di un modello di politica, selezionarne uno e verificarlo, quindi selezionarne un altro e verificarlo e così di seguito.</p> <p>Se vi sono dei campi nel modello di politica per i quali non esistono dati nell'origine dati, viene visualizzato un messaggio che elenca i campi mancanti. È possibile salvare comunque il profilo o usare un profilo dati esatti differente.</p>
Visualizzazione avanzata	<p>Se si desidera personalizzare lo schema per il profilo dati esatti, fare clic su Visualizzazione avanzata per visualizzare le opzioni avanzate per il mapping dei campi.</p> <p>Tabella 22-8 elenca e descrive le colonne supplementari che è possibile specificare nella schermata Visualizzazione avanzata.</p>
Indicizzazione	<p>Selezionare una delle opzioni di indicizzazione.</p> <p>Vedere "Pianificazione dell'indicizzazione di profili dati esatti" a pagina 499.</p>
Fine	Fare clic su Fine al termine della configurazione del profilo dati esatti.

Nella schermata **Visualizzazione avanzata** è possibile eseguire il mapping dei campi di sistema e dell'origine dati ai criteri di sistema. I criteri di sistema eseguono il mapping della struttura specificata ai dati nel profilo dati esatti, consentono un controllo errori efficace e forniscono suggerimenti per l'indicizzatore.

Tabella 22-8 Opzioni di Visualizzazione avanzata

Campo	Descrizione
Nome personalizzato	Se si seleziona Nome personalizzato per un campo di sistema, immettere un nome univoco per quel campo e selezionare un valore per Tipo. Il nome deve avere una lunghezza massima di 60 caratteri.
Tipo	<p>Se per un campo di sistema si seleziona un valore che non è Personalizzato, per alcuni tipi di dati viene automaticamente selezionato un valore per Tipo. Ad esempio, se si seleziona Data di nascita per il campo di sistema, Data viene selezionato automaticamente come tipo. È possibile accettare o modificare questa selezione automatica.</p> <p>Per alcuni tipi di dati non viene selezionato automaticamente un valore per Tipo. Ad esempio, se per il campo di sistema si seleziona Numero di conto, nessun valore viene selezionato per Tipo. È possibile specificare il tipo di dati di determinati numeri di conto.</p> <p>Vedere "Utilizzo delle convalide dei criteri fornite dal sistema per i profili EDM" a pagina 498.</p>

Campo	Descrizione
Descrizione	Fare clic sul collegamento (descrizione) accanto all'intestazione della colonna Tipo per visualizzare una finestra contenente i tipi di dati di sistema disponibili. Vedere "Utilizzo delle convalide dei criteri fornite dal sistema per i profili EDM" a pagina 498.
Visualizzazione semplice	Fare clic su Visualizzazione semplice per ritornare alla visualizzazione semplice (con le colonne Tipo e Nome personalizzato nascoste).

Vedere ["Creazione e modifica di profili dati esatti"](#) a pagina 492.

Utilizzo delle convalide dei criteri fornite dal sistema per i profili EDM

La [Tabella 22-9](#) elenca e descrive le convalide dei dati fornite dal sistema per i profili EDM.

Tabella 22-9 Convalide dei dati fornite dal sistema per i profili EDM

Tipo	Descrizione
Numero di carta di credito	Il criterio Carta di credito si basa sulla conoscenza di varie carte di credito internazionali, sui relativi prefissi registrati e sul numero di cifre nei numeri di conto. Sono convalidati i tipi di criteri di carta di credito seguenti: Mastercard, Visa, America Express, Diners Club, Discover, Ernoute e JCB. Gli spazi opzionali nelle aree designate all'interno dei numeri di carta di credito sono riconosciuti. Si tenga presente che solo gli spazi nelle posizioni generalmente accettate (ad esempio, dopo ogni quarta cifra in MC/Visa) sono riconosciuti. La posizione possibile degli spazi varia a seconda del tipo di carta di credito. I numeri di carta di credito vengono convalidati con l'algoritmo di checksum. Se un numero è simile a quello di una carta di credito (ovvero ha un numero di cifre e un prefisso corretti), ma non supera l'algoritmo di checksum, non è considerato un numero di carta di credito, ma soltanto un numero.
E-mail	L'e-mail è una sequenza di caratteri di questo tipo: <code>string@string.tld</code> , dove la stringa può contenere lettere, cifre, caratteri di sottolineatura, trattini e punti e "tld" è uno dei domini generici DNS di livello superiore approvati oppure due lettere qualsiasi (per i domini di paese).
Indirizzo IP	L'indirizzo IP è una raccolta di 4 sequenze di 1-3 cifre separate da punti.
Numero	Il numero è intero o a virgola mobile, senza altri caratteri oppure racchiuso tra parentesi tonde ().
Percentuale	Una percentuale è un numero seguito immediatamente dal simbolo di percentuale ("%"). Non è consentito alcuno spazio tra il numero e il segno di percentuale.

Tipo	Descrizione
Telefono	<p>Sono riconosciuti solo i numeri di telefono degli Stati Uniti e del Canada. I numeri di telefono devono iniziare con qualsiasi cifra tranne 1, a eccezione dei numeri che includono il prefisso internazionale.</p> <p>Un numero di telefono può avere uno dei seguenti formati:</p> <ul style="list-style-type: none">■ 7 cifre (senza spazi o trattini)■ Come sopra, preceduto da 3 cifre o da 3 cifre tra parentesi tonde, seguite da spazi o trattini■ 3 cifre, seguite da spazi o trattini opzionali, seguiti da 4 cifre■ Come sopra, preceduto dal numero 1, seguito da spazi o trattini <p>Tutti questi casi possono essere seguiti facoltativamente da un numero di estensione, preceduti da spazi o trattini. L'interno può essere composto da 2-5 cifre precedute, senza distinzione tra maiuscole e minuscole, da "x", "ex", "ext", "exten", "extens", "extensions" e facoltativamente seguite da un punto o da spazi.</p> <p>Nota: il sistema non riconosce il criterio XXX-XXX-XXXX come formato di numero di telefono valido perché questo formato viene spesso utilizzato in altre forme di identificazione. Se l'origine dati contiene una colonna di numeri di telefono in tale formato, selezionare Nessuna selezione per evitare confusione tra numeri di telefono e altri dati.</p>
CAP	<p>Sono riconosciuti solo i CAP degli Stati Uniti e del Canada. Il CAP statunitense è composto da una sequenza di 5 cifre, seguite facoltativamente da un trattino e da altre 4 cifre. Il CAP canadese è una sequenza come K2B 8C8, ovvero "lettera-cifra-lettera-spazio-cifra-lettera-cifra", con uno o più spazi intermedi opzionali.</p>
Numero di codice fiscale	<p>Sono riconosciuti solo i Social Security Number statunitensi. Questi numeri sono composti da 3 cifre, seguite eventualmente da spazi o trattini, da altre 2 cifre, da altri spazi o trattini opzionali e infine da 4 cifre.</p>

Pianificazione dell'indicizzazione di profili dati esatti

Quando si configura un profilo dati esatti, è possibile definire una pianificazione per l'indicizzazione dell'origine dati (**Invia processo di indicizzazione secondo pianificazione**).

Vedere ["Informazioni sulla pianificazione degli indici"](#) a pagina 481.

Prima di configurare una pianificazione, considerare quanto segue:

- Se le origini dati vengono aggiornate (ad esempio, meno di una volta al mese), non è necessario creare una pianificazione. Indicizzare i dati ogni volta che si aggiorna l'origine dati.
- Pianificare l'indicizzazione per gli orari di uso minimo del sistema. L'indicizzazione ha effetto sulle prestazioni in tutto il sistema Symantec Data Loss Prevention e quella delle origini dati di grandi dimensioni può richiedere tempo.

- Indicizzare un'origine dati non appena si aggiunge o si modifica il profilo dati esatti corrispondente e ripetere l'indicizzazione dell'origine dati ogni volta che viene aggiornata. Ad esempio, si consideri uno scenario che prevede l'aggiornamento dell'origine dati ogni mercoledì alle 2.00. In questo caso è necessario pianificare l'indicizzazione ogni mercoledì alle 3.00. Non eseguire l'indicizzazione delle origini dati giornalmente in quanto può degradare le prestazioni.
- Se è necessario aggiornare gli indici frequentemente (ad esempio ogni giorno), Symantec consiglia di utilizzare l'indicizzatore EDM remoto.
- Controllare i risultati e modificare la pianificazione di indicizzazione di conseguenza. Se le prestazioni sono soddisfacenti e si desiderano aggiornamenti più tempestivi, programmare aggiornamenti e indicizzazioni dei dati più frequenti.

La sezione Indicizzazione consente di indicizzare il profilo dati esatti non appena viene salvato (consigliato) o secondo una pianificazione regolare nel modo seguente:

Tabella 22-10 Pianificazione dell'indicizzazione dei profili dati esatti

Parametro	Descrizione
Invia processo di indicizzazione al salvataggio	Selezionare questa opzione per indicizzare il profilo dati esatti quando si fa clic su Salva.
Invia processo di indicizzazione secondo pianificazione	Selezionare questa opzione per pianificare l'operazione di indicizzazione. Il valore predefinito è Nessuna pianificazione regolare . Se si intende eseguire l'indicizzazione secondo una pianificazione, selezionare un periodo di pianificazione desiderato, come descritto.
Una volta	<p>Il - Immettere la data per l'indicizzazione del profilo documento nel formato MM/GG/AA. È anche possibile fare clic sul widget data e selezionare una data.</p> <p>Alle - Selezionare l'ora di inizio dell'indicizzazione.</p>
Ogni giorno	<p>Alle - Selezionare l'ora di inizio dell'indicizzazione.</p> <p>Fino a - Selezionare questa casella di controllo per specificare la data di arresto dell'indicizzazione nel formato MM/GG/AA. È anche possibile fare clic sul widget data e selezionare una data.</p>
Ogni settimana	<p>Giorno della settimana - Selezionare i giorni in cui indicizzare il profilo documento.</p> <p>Alle - Selezionare l'ora di inizio dell'indicizzazione.</p> <p>Fino a - Selezionare questa casella di controllo per specificare la data di arresto dell'indicizzazione nel formato MM/GG/AA. È anche possibile fare clic sul widget data e selezionare una data.</p>

Parametro	Descrizione
Ogni mese	<p>Giorno - Immettere il numero del giorno di ogni mese in cui eseguire l'indicizzazione. Il valore deve essere tra 1 e 28.</p> <p>Alle - Selezionare l'ora di inizio dell'indicizzazione.</p> <p>Fino a - Selezionare questa casella di controllo per specificare la data di arresto dell'indicizzazione nel formato MM/GG/AA. È anche possibile fare clic sul widget data e selezionare una data.</p>

Vedere ["Mapping dei campi del profilo dati esatti"](#) a pagina 496.

Vedere ["Creazione e modifica di profili dati esatti"](#) a pagina 492.

Gestione e aggiunta di profili dati esatti

È possibile gestire e creare **Profili dati esatti** per EDM nella schermata **Gestisci > Profili dati > Dati esatti**. Dopo aver creato un profilo, la schermata **Dati esatti** elenca tutti i profili di dati esatti configurati nel sistema.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Tabella 22-11 Azioni della schermata Dati esatti

Azione	Descrizione
Aggiunta del profilo EDM	<p>Fare clic su Aggiungi profilo dati esatti per definire un nuovo profilo dati esatto.</p> <p>Vedere "Configurazione di profili dati esatti" a pagina 484.</p>
Modifica del profilo EDM	<p>Per modificare un Profilo dati esatti, fare clic sul nome del profilo o sull'icona della matita all'estrema destra della riga del profilo.</p> <p>Vedere "Creazione e modifica di profili dati esatti" a pagina 492.</p>
Rimozione del profilo EDM	<p>Fare clic sull'icona rossa X all'estrema destra della riga del profilo per eliminare il profilo dati esatti dal sistema. Una finestra di dialogo conferma l'eliminazione.</p> <p>Nota: Non è possibile modificare o rimuovere un profilo se un altro utente lo sta modificando o se esiste una politica che dipende da quel profilo.</p>
Download del profilo EDM	<p>Fare clic su Scarica profilo per scaricare e salvare il profilo dati esatti.</p> <p>Questo passaggio è utile per archiviare e condividere i profili contenuti negli ambienti. Il file è in formato binario *.edm.</p>
Aggiornamento dello stato del profilo EDM	<p>Fare clic sull'icona di aggiornamento a forma di freccia in alto a destra nella schermata Dati esatti per recuperare lo stato aggiornato del processo di indicizzazione.</p> <p>Durante il processo di indicizzazione, il sistema visualizza il messaggio "Avvio indicizzazione in corso.". Il sistema non aggiorna automaticamente la schermata al termine del processo di indicizzazione.</p>

Tabella 22-12 Dettagli della schermata Dati esatti

Colonna	Descrizione
Profilo dati esatti	Il nome del profilo dati esatti.
Ultima versione attiva	La versione del profilo dati esatti e il nome del server di rilevamento che esegue il profilo.
Stato	<p>Lo stato attuale del profilo dati esatti che può essere uno dei seguenti:</p> <ul style="list-style-type: none"> ■ Prossima indicizzazione pianificata (se non vi sono indicizzazioni in corso) ■ Invio di un indice a un server di rilevamento ■ Indicizzazione ■ Distribuzione ai server <p>Inoltre, lo stato attuale del processo di indicizzazione per ogni server di rilevamento che può essere uno dei seguenti:</p> <ul style="list-style-type: none"> ■ Completato, inclusa una data di completamento ■ Completamento indicizzazione in sospeso (in attesa che Enforce Server termini l'indicizzazione del file origine dati esatti) ■ Replica dell'indicizzazione ■ Creazione dell'indice (internamente) ■ Creazione delle cache
Messaggi di errore	<p>La schermata Dati esatti consente di visualizzare qualsiasi messaggio di errore in rosso.</p> <p>Ad esempio, se il profilo dati esatti è danneggiato o non esiste, il sistema visualizza un messaggio di errore.</p>

Configurazione dei criteri EDM

Questa sezione descrive come configurare le condizioni della politica EDM.

Vedere ["Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti"](#) a pagina 503.

Vedere ["Configurazione dell'eccezione Proprietario dati per le condizioni della politica EDM"](#) a pagina 505.

Vedere ["Configurazione della condizione di politica di mittente/utente basato su una directory con profilo"](#) a pagina 506.

Vedere ["Configurazione del destinatario in base a una condizione della politica Profiled Directory"](#) a pagina 507.

Vedere ["Configurazione di impostazioni avanzate per i criteri EDM"](#) a pagina 509.

Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti

Dopo aver definito il profilo dati esatti e indicizzato l'origine dati, si configurano una o più condizioni Contenuto corrispondente a profilo dati esatti nelle regole di politiche.

Vedere ["Informazioni sulla condizione Il contenuto corrisponde ai dati esatti da"](#) a pagina 482.

Tabella 22-13 Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti

Passaggi	Azione	Descrizione
1	Configurare una regola di rilevamento EDM.	<p>Creare una nuova regola di rilevamento EDM in una politica o modificarne una esistente.</p> <p>Vedere "Configurazione di politiche" a pagina 422.</p> <p>Vedere "Configurazione di regole di politica" a pagina 427.</p>
Corrispondenza righe di dati quando tutti i campi corrispondono		
2	Selezionare i campi per la corrispondenza.	<p>La prima cosa da fare quando si configura la condizione EDM è selezionare ogni campo di dati che deve corrispondere alla condizione. È possibile selezionare o deselezionare tutti i campi con seleziona tutto o deseleziona tutto. Il sistema visualizza tutti i campi o le colonne inclusi nell'indice. Non è necessario selezionare tutti i campi, ma almeno 2 o 3, uno dei quali deve essere univoco, come il codice fiscale, il numero di carta di credito e così via.</p> <p>Vedere "Best practice per l'utilizzo dell'EDM" a pagina 557.</p>
3	Scegliere il numero di campi selezionati per la corrispondenza.	<p>Scegliere il numero dei campi selezionati per la corrispondenza dal menu a discesa. Questo numero rappresenta il numero di campi tra quelli selezionati che devono essere presenti in un messaggio per generare una corrispondenza. Il numero di campi selezionati per la corrispondenza deve essere almeno uguale a quello dei campi di dati selezionati. Ad esempio, se si scelgono 2 dei campi selezionati nel menu, è necessario aver selezionato almeno due campi presenti in un messaggio per il rilevamento.</p> <p>Vedere "Verifica della presenza di almeno una colonna di dati univoci nell'origine dati" a pagina 558.</p>

Passaggi	Azione	Descrizione
4	Selezionare la clausola WHERE per immettere specifici valori di campo per la corrispondenza (facoltativo).	<p>L'opzione della clausola WHERE cerca la corrispondenza con il valore di campo specificato. Per specificare un valore della clausola WHERE, selezionare un campo di dati esatti dal menu e immettere un valore per quel campo nella casella di testo adiacente. Se si immettono più valori, separarli con virgole.</p> <p>Vedere "Utilizzare una clausola WHERE per individuare i record che soddisfano criteri specifici" a pagina 566.</p> <p>Ad esempio, considerare un profilo dati esatti per "impiegati" con un campo "Stato" contenente abbreviazioni degli stati. In questo esempio, per implementare la clausola WHERE, si seleziona WHERE, si sceglie "Stato" dall'elenco a discesa e si immette CA,NV nella casella di testo. Con questa clausola WHERE, il server di rilevamento troverà delle corrispondenze solo con i messaggi che contengono CA o NV, ovvero il valore del campo Stato.</p> <p>Nota: Per WHERE, non è possibile specificare uno dei campi selezionati per la corrispondenza.</p>

Ignora righe di dati quando alcuni campi corrispondono

5	Ignorare i proprietari di dati (facoltativo).	<p>La selezione di questa opzione implementa l'eccezione Proprietario dati.</p> <p>Vedere "Configurazione dell'eccezione Proprietario dati per le condizioni della politica EDM" a pagina 505.</p>
6	Escludere combinazioni di campi di dati (facoltativo).	<p>È possibile utilizzare Combinazioni escluse per specificare combinazioni di valori di dati da escludere dal rilevamento. Se i dati compaiono nei gruppi o nelle coppie esclusi, non viene generata una corrispondenza. Le combinazioni escluse sono disponibili solo quando si cerca la corrispondenza in 2 o 3 campi. Per attivare questa opzione, è necessario selezionare 2 o 3 campi per la corrispondenza dal menu _ dei campi selezionati nella parte superiore della configurazione della condizione.</p> <p>Vedere "Sfruttamento delle tuple di eccezione per evitare i falsi positivi" a pagina 566.</p> <p>Per implementare le combinazioni escluse, selezionare un'opzione da ogni colonna Campo n. visualizzata. Fare quindi clic sull'icona con la freccia a destra per aggiungere la combinazione di campi all'elenco Combinazioni escluse. Per rimuovere un campo dall'elenco, selezionarlo e fare clic sull'icona con la freccia a sinistra.</p> <p>Nota: Tenere premuto il tasto Ctrl per selezionare più di un campo nella colonna di destra.</p>

Parametri supplementari per la condizione di corrispondenza

Passaggi	Azione	Descrizione
7	Selezionare un numero minimo di incidenti.	<p>Immettere o modificare il numero minimo di corrispondenze necessarie perché la condizione segnali un incidente.</p> <p>Ad esempio, si consideri uno scenario in cui si specifica 1 dei campi selezionati per un campo relativo al codice fiscale e un numero minimo di incidenti pari a 5. In questo caso, il motore deve rilevare almeno cinque codici fiscali corrispondenti in un singolo messaggio per generare un incidente.</p> <p>Vedere "Esempi di varianti di totale corrispondenze" a pagina 523.</p>
8	Selezionare i componenti in cui cercare la corrispondenza.	<p>Selezionare una o più componenti dei messaggi in cui cercare la corrispondenza:</p> <ul style="list-style-type: none"> ■ Busta - L'intestazione del messaggio. ■ Oggetto - (non disponibile per EDM). ■ Corpo - Il contenuto del messaggio. ■ Allegati - Il contenuto di qualsiasi file allegato al messaggio o trasportato dallo stesso. <p>Vedere "Selezione dei componenti per la corrispondenza" a pagina 433.</p>
9	Selezionare una o più condizioni per le quali cercare una corrispondenza.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere perché la regola generi un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile dall'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>
10	Provare una politica e risolvere i problemi relativi.	<p>Vedere "Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze" a pagina 466.</p> <p>Vedere "Risoluzione dei problemi delle politiche" a pagina 458.</p>

Configurazione dell'eccezione Proprietario dati per le condizioni della politica EDM

Per escludere i proprietari di dati dal rilevamento, è necessario includere nel Profilo dati esatti un indirizzo e-mail o un campo di indirizzo di dominio (ad esempio `symantec.com`). Una volta che l'eccezione Proprietario dati (DOE) è attivata, se il mittente o il destinatario di dati riservati è il proprietario dei dati (per indirizzo e-mail o di dominio), il server di rilevamento consente che i dati siano inviati o ricevuti senza generare un incidente.

Per configurare l'eccezione DOE per una condizione di politica EDM

- 1 Quando si configura la condizione Il contenuto corrisponde ai dati esatti, selezionare l'opzione **Ignora proprietari dei dati**.
- 2 Selezionare una delle opzioni seguenti:

- **Il mittente corrisponde** : selezionare questa opzione per escludere il mittente dei dati dal rilevamento.
- **Qualsiasi destinatario o Tutti i destinatari** : selezionare una di queste opzioni per escludere dal rilevamento qualsiasi destinatario o tutti i destinatari.

Nota: Quando si configura l'eccezione DOE per la condizione EDM, non è possibile selezionare un valore per Ignora mittente/destinatario uguale a quello dei campi corrispondenti.

Vedere ["Informazioni sull'eccezione Proprietario dati"](#) a pagina 482.

Configurazione della condizione di politica di mittente/utente basato su una directory con profilo

La regola di rilevamento **Mittente/utente basato su una directory di** consente di creare le regole di rilevamento basate sull'identità del mittente o (per gli incidenti endpoint) sull'identità dell'utente. Questa condizione richiede un profilo di dati esatti.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Dopo avere selezionato il profilo di dati esatti, quando si configura la regola, la directory selezionata e gli identificatori del mittente vengono visualizzati nella parte superiore della pagina.

La [Tabella 22-14](#) descrive i parametri per la configurazione della condizione **Mittente/utente basato su una directory di un profilo EDM**.

Tabella 22-14 Configurazione della condizione Mittente/utente basato su una directory di un profilo EDM

Parametro	Descrizione
Dove	<p>Selezionare questa opzione in modo che il sistema cerchi la corrispondenza con i valori dei campi specificati. Specificare i valori selezionando un campo dall'elenco a discesa e digitando i valori per il campo nella casella di testo adiacente. Se si immettono più valori, separarli con virgole.</p> <p>Ad esempio, per un profilo di un gruppo di directory Dipendenti che include un campo Reparto, selezionare Dove, selezionare Reparto dall'elenco a discesa e immettere Marketing, Vendite nella casella di testo. Se la condizione viene implementata come regola, in questo esempio viene trovata una corrispondenza solo se il mittente o l'utente lavora nel reparto Marketing o Vendite (a condizione che l'altro contenuto immesso soddisfi tutti i criteri di rilevamento). Se la condizione viene implementata come eccezione, in questo esempio il sistema esclude dalla corrispondenza i messaggi di un mittente o un utente che lavora nel reparto Marketing o Vendite.</p>

Parametro	Descrizione
È uno qualsiasi dei seguenti valori	Immettere o modificare le informazioni per cui si desidera cercare la corrispondenza. Ad esempio, se si desidera cercare la corrispondenza con qualsiasi mittente nel reparto Vendite, selezionare Reparto dall'elenco a discesa, quindi immettere Vendite in questo campo (si presupponga che i dati includono una colonna Reparto). Utilizzare un elenco separato da virgole se si desidera specificare più valori.

Configurazione del destinatario in base a una condizione della politica Profiled Directory

La condizione **Destinatario basato su una directory di** consente di creare metodi di rilevamento basati sull'identità del destinatario. Questo metodo richiede un profilo dati esatti.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Dopo avere selezionato il profilo dati esatti, quando si configura la regola, la directory selezionata e i o gli identificatori del destinatario appaiono in alto nella pagina.

[Tabella 22-15](#) descrive i parametri per la configurazione della condizione **Destinatario basato su una directory di un profilo EDM**.

Tabella 22-15 Configurazione della condizione Destinatario basato su una directory di un profilo EDM

Parametro	Descrizione
Dove	<p>Selezionare questa opzione in modo che il sistema cerchi la corrispondenza con i valori dei campi specificati. Specificare i valori selezionando un campo dall'elenco a discesa e digitando i valori per il campo nella casella di testo adiacente. Se si immettono più valori, separarli con i virgole.</p> <p>Ad esempio per un profilo di gruppo directory Dipendenti che include un campo Reparto è possibile selezionare Dove, selezionare Reparto dall'elenco a discesa e digitare Marketing, Vendite nella casella di testo. Per una regola di rilevamento, questo esempio fa sì che il sistema rilevi un incidente solo se almeno un destinatario lavora nel reparto Marketing o Vendite (sempre che il contenuto di input soddisfi tutti gli altri criteri di rilevamento). Per un'eccezione, questo esempio impedisce al sistema di rilevare l'incidente se almeno un destinatario lavora nel reparto Marketing o Vendite.</p>
È uno qualsiasi dei seguenti valori	Immettere o modificare i dati per la corrispondenza. Ad esempio, per rilevare la corrispondenza con qualsiasi destinatario nel reparto Vendite, selezionare Reparto nell'elenco a discesa, quindi digitare Vendite in questo campo (supponendo che i dati includano una colonna Reparto). Se si desidera specificare più di un valore utilizzare un elenco separato da virgole.

Informazioni sulla configurazione dell'elaborazione del linguaggio naturale per cinese, giapponese e coreano per le politiche EDM.

Introduzione alla corrispondenza token EDM

I server di rilevamento Symantec Data Loss Prevention supportano l'elaborazione della lingua naturale per cinese, giapponese e coreano (CJK) in politiche che utilizzano il rilevamento Exact Data Matching (EDM). Quando l'elaborazione della lingua naturale per le lingue CJK è attivata, il server di rilevamento convalida i token CJK prima della segnalazione di una corrispondenza, che migliora l'accuratezza della corrispondenza.

Esempi di corrispondenze token EDM per lingue CJK

[Tabella 22-16](#) fornisce gli esempi di corrispondenza token EDM per cinese, giapponese e coreano. Tutti gli esempi presuppongono che la parola chiave sia configurata per corrispondere unicamente a tutte le parole.

Se la verifica token è attivata, le dimensioni del messaggio devono essere sufficienti per il riconoscimento della lingua da parte dello strumento di verifica del token. Ad esempio: il messaggio "東京都市部の人口" è troppo breve perché il processo di verifica del token possa riconoscere la lingua del messaggio. Il seguente messaggio è di dimensione sufficiente per l'elaborazione di verifica del token:

今朝のニュースによると東京都市部の人口は増加傾向にあるとのことでした。全国的な人口減少の傾向の中、東京への一極集中を表しています。

Tabella 22-16 Esempi di corrispondenze token EDM per CJK

Lingua	Parola chiave	Corrispondenze sul server con convalida token attivata	Corrispondenze sul server con convalida token disattivata
Cinese	通信	数字无线通信	数字无线通信 交通信息 网站
Giapponese	京都市	京都府京都市左京区	京都府京都市左京区 東京都市部の人口
Coreano	정부	정부의 방침	정부의 방침 의정부 경전철

Attivazione e utilizzo della token CJK per EDM

Per utilizzare la verifica token per il cinese, il giapponese e il coreano (CJK) è necessario attivarla su ogni server di rilevamento impostando l'impostazione di server avanzata **EDM.TokenVerifierEnabled** su `true`. Inoltre deve esservi un testo di dimensioni sufficienti affinché il sistema riconosca la lingua.

Tabella 22-17 elenca e descrive il parametro del server di rilevamento che consente di attivare la verifica dei token per le lingue CJK.

Tabella 22-17 Parametro di verifica dei token EDM

Impostazione	Impostazione predefinita	Descrizione
EDM.TokenVerifierEnabled	false	Per impostazione predefinita è disattivato (false). Se è attivato (true), il server convalida i token per le parole chiave in cinese, giapponese e coreano.

Vedere ["Per attivare la verifica dei token per le parole chiave CJK"](#) a pagina 782. descrive come attivare e utilizzare la verifica del token per le parole chiave CJK.

Per attivare la verifica dei token EDM per CJK

- 1 Accedere a Enforce Server come utente amministrativo.
- 2 Accedere alla schermata **Sistema > Server e rilevatori > Panoramica > Dettagli server/rilevatore - Impostazioni avanzate** per il server di rilevamento che si desidera configurare.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.
- 3 Individuare il parametro **EDM.TokenVerifierEnabled**.
- 4 Modificare il valore **false** (impostazione predefinita) e impostarlo su **true**.

Se si imposta il parametro del server su **EDM.TokenVerifierEnabled true**, viene attivata la convalida dei token per il rilevamento dei token CJK.
- 5 **Salvare** la configurazione del server di rilevamento.
- 6 **Riciclare** il server di rilevamento.

Configurazione di impostazioni avanzate per i criteri EDM

EDM dispone di varie impostazioni avanzate, disponibili nella schermata **Sistema > Server e rilevatori > Panoramica > Dettagli server/rilevatore - Impostazioni avanzate** del server di rilevamento selezionato. Prestare attenzione quando si modificano queste impostazioni su un server. Prima di modificare le impostazioni di questa schermata contattare il Supporto di Symantec Data Loss Prevention. Le modifiche a tali impostazioni diventano attive solo dopo il riavvio del server.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Tabella 22-18 Impostazioni avanzate di indicizzazione e rilevamento EDM

Parametro EDM	Impostazione predefinita	Descrizione
EDM.MatchCountVariant	3	<p>Questa impostazione specifica come vengono conteggiate le corrispondenze.</p> <ul style="list-style-type: none"> ■ 1 - Conta il numero dei set di token con i quali è stata rilevata una corrispondenza, indipendentemente dall'uso dello stesso token in più corrispondenze. ■ 2 - Conta il numero di set di token unici. ■ 3 - Conta il numero dei superset unici di set di token. (impostazione predefinita) <p>Vedere "Esempi di varianti di totale corrispondenze" a pagina 523.</p>
EDM.MaximumNumberOfMatchesToReturn	100	<p>Definisce un limite superiore per il numero di corrispondenze restituite da ciascuna ricerca indice RAM. Per gli indici a più file il limite è applicato in modo indipendente a ciascuna ricerca di sottoindice prima della combinazione dei risultati della ricerca. Di conseguenza il numero di corrispondenze effettive può superare questo limite per gli indici a più file.</p>
EDM.RunProximityLogic	true	<p>Se true (impostazione predefinita), questa impostazione esegue il controllo di prossimità del token. La prossimità del testo in formato libero è definita dall'impostazione <code>EDM.SimpleTextProximityRadius</code>. La prossimità del testo tabulare è definita dall'appartenenza alla stessa riga di tabella.</p> <p>Nota: La disattivazione della prossimità non è consigliata, in quanto può influire negativamente sulle prestazioni del sistema.</p>

Parametro EDM	Impostazione predefinita	Descrizione
EDM.SimpleTextProximityRadius	35	<p>Fornisce l'intervallo base per il controllo di prossimità di un token con corrispondenza. Questo valore viene moltiplicato per il numero di corrispondenze necessarie a uguagliare l'intervallo completo del controllo di prossimità.</p> <p>Per mantenere la stessa "densità di corrispondenze richiesta", il controllo di prossimità funziona come una finestra mobile in una pagina di testo. D è definito come fattore di proporzionalità per la finestra ed è impostato nella condizione della politica scegliendo il numero di campi sul quale basare la corrispondenza per la condizione EDM. N è il valore SimpleTextProximityRadius. Se il primo token si trova entro $N \times D$ parole dall'ultimo token, vari token si troveranno nell'intervallo di prossimità. L'intervallo di verifica di prossimità è direttamente proporzionale al numero delle corrispondenze in base a un fattore D.</p> <p>Vedere "Esempio di corrispondenza di prossimità" a pagina 525.</p> <p>Nota: L'incremento del valore del raggio a un valore superiore a quello predefinito può avere un effetto negativo sulle prestazioni del sistema ed è sconsigliato.</p>
EDM.TokenVerifierEnabled	false	<p>Per impostazione predefinita è disattivato (false).</p> <p>Se è attivato (true), il server convalida i token per le parole chiave in cinese, giapponese e coreano.</p>
Lexer.IncludePunctuationInWords	true	<p>Se true, durante il rilevamento i caratteri di punteggiatura sono considerati come parte di un token.</p> <p>Se false, durante il rilevamento la punteggiatura all'interno di un token o di un multitoken è considerata come spazi.</p> <p>Vedere "Multi-token con punteggiatura" a pagina 516.</p> <p>Nota: Questa impostazione si applica al rilevamento di contenuto, non al contenuto indicizzato.</p>

Parametro EDM	Impostazione predefinita	Descrizione
Lexer.MaximumNumberOfTokens	12000	<p>Numero massimo dei token estratti da ogni componente messaggio per il rilevamento. Applicabile a tutte le tecnologie di rilevamento nelle quali l'applicazione di token è obbligatoria (EDM, DGM con profilo e criteri di sistema supportati da tali tecnologie). L'incremento del valore predefinito può determinare l'esaurimento della memoria e il riavvio del server di rilevamento.</p> <p>Nota: In Data Loss Prevention versione 12.5 e successive il valore predefinito è stato modificato da 30.000 a 12.000. In precedenza venivano inviati al rilevamento tutti i token fino al limite massimo, incluse le parole non significative e le parole a lettera singola. Nelle versioni 12.5 e successive i token inviati al rilevamento non includono le parole non significative e le parole a lettera singola. Il numero di token significativi inviati al rilevamento è circa lo stesso delle versioni precedenti.</p>
Lexer.Validate	true	<p>Se true, esegue la convalida specifica per criterio sistema durante l'indicizzazione. L'impostazione di questa opzione su false è sconsigliata.</p> <p>Vedere "Utilizzo delle convalide dei criteri fornite dal sistema per i profili EDM" a pagina 498.</p>
MessageChain.NumChains	Varia	<p>Questo numero varia a seconda del tipo di server di rilevazione. Può essere 4 o 8. Numero di messaggi in parallelo che verranno elaborati dal filereader. L'impostazione di questo numero su un valore superiore a 8 (con le altre impostazioni predefinite) è sconsigliata. Un'impostazione più alta non incrementa sostanzialmente le prestazioni e comporta un rischio molto maggiore di esaurimento della memoria. L'impostazione su un valore inferiore a 8 (talvolta su 1) risulta utile per l'elaborazione di file di grandi dimensioni, ma può rallentare considerevolmente le prestazioni del sistema.</p>

Nota: I token massimi per multitoken e parole non significative vengono calcolati e valutati rispettivamente durante l'indicizzazione. Le impostazioni Lexer.MaxTokensPerMultiToken e Lexer.Stopword Languages Advanced Server non sono più necessarie. La lingua delle parole non significative su Enforce è specificata nel file `indexer.properties` in `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\Indexer.properties`. In inglese, la proprietà è `stopword_languages = en`.

Utilizzo della corrispondenza multitoken

La corrispondenza della politica EDM è basata sui token presenti nell'indice. Per le lingue basate sull'alfabeto latino, un token è una parola o una serie di caratteri alfanumerici delimitati da spazi. Per cinese, giapponese e coreano, un token è determinato da altri metodi. I token sono normalizzati per consentire di ignorare la formattazione e il caso. Al momento del runtime, il server esegue una ricerca full-text di un messaggio in arrivo, controllando ogni parola rispetto all'indice e rilevando eventuali corrispondenze. L'algoritmo della corrispondenza confronta ogni parola nel messaggio con il contenuto di ogni token dell'indice.

Una cella multitoken è una cella dell'indice che contiene più parole separate da spazi, punteggiatura all'inizio o alla fine o caratteri latini, cinesi, giapponesi o coreani. Le parti subtoken di una cella multitoken rispondono alle stesse regole delle celle del token singolo: vengono normalizzate secondo il loro formato nel quale è possibile applicare la normalizzazione. I dati di un messaggio in entrata devono corrispondere esattamente a una cella multitoken, inclusi spazi, punteggiatura e parole non significative (in base alle impostazioni predefinite).

Ad esempio, una cella indicizzata che contiene la stringa "Banca d'America" è un multitoken che include 3 parti subtoken. Durante il rilevamento, il messaggio in arrivo "banca d'america" (normalizzato) corrisponde alla cella multitoken mentre "banca america" no.

La corrispondenza multitoken è attivata per impostazione predefinita. Le celle multitoken richiedono più elaborazione di calcolo rispetto a quelle a token singolo. Se l'indice comprende celle multitoken, è necessario verificare che vi sia memoria sufficiente per indicizzare, caricare ed elaborare il profilo EDM.

Vedere ["Caratteristiche delle celle multitoken"](#) a pagina 513.

Vedere ["Requisiti di memoria per EDM"](#) a pagina 532.

Caratteristiche delle celle multitoken

[Tabella 22-19](#) elenca e descrive le caratteristiche della corrispondenza del multitoken.

Vedere ["Utilizzo della corrispondenza multitoken"](#) a pagina 513.

Tabella 22-19 Caratteristiche dei multitoken

Caratteristiche	Descrizione
Il numero di token in una singola cella è limitato a 200 token.	Il numero di caratteri non è limitato. Nel caso di un token CJK, ogni carattere viene considerato come un token singolo e il numero di caratteri CJK è limitato a 200 caratteri.
Viene considerato lo spazio vuoto in celle multitoken con caratteri latini, mentre più spazi vuoti vengono normalizzati a 1.	Vedere "Multitoken con spazi" a pagina 514.

Caratteristiche	Descrizione
La punteggiatura immediatamente prima e dopo un token o un subtoken viene sempre ignorata.	Vedere "Multi-token con punteggiatura" a pagina 516. Vedere "Ulteriori esempi per celle multitoken con punteggiatura" a pagina 517.
È possibile configurare come la punteggiatura viene considerata all'interno di un token o di un multitoken durante il rilevamento. L'impostazione predefinita ("true") funziona nella maggior parte dei casi. Se invece è impostata su "false", la punteggiatura verrà considerata come spazio vuoto.	<code>Lexer.IncludePunctuationInWords = true</code> Vedere "Configurazione di impostazioni avanzate per i criteri EDM" a pagina 509.
Per il controllo dell'intervallo di prossimità, le parti subtoken di un multitoken vengono considerate come token singoli.	Vedere "Esempio di corrispondenza di prossimità" a pagina 525.
Il sistema non considera le parole non significative durante la corrispondenza di multitoken. In altri termini, le parole non significative non vengono escluse.	Vedere "Multitoken con parole non significative" a pagina 515.
Le celle multitoken richiedono più elaborazione di calcolo rispetto a quelle a token singolo e richiedono memoria supplementare per indicizzare, caricare ed elaborare.	Vedere "Requisiti di memoria per EDM" a pagina 532.

Multitoken con spazi

La [Tabella 22-20](#) mostra gli esempi di multitoken con spazi.

Tabella 22-20 Esempi di cella multitoken con spazi

Descrizione	Contenuto indicizzato	Contenuto rilevato	Spiegazione
La cella contiene uno spazio	Bank of America	Bank of America	La cella con spazi è multitoken. Il multitoken deve corrispondere esattamente.
Le celle contengono più spazi	Bank of America	Bank of America	Più spazi sono normalizzati in uno.
Le celle contengono uno spazio tra i caratteri CKJ	尙儼 尙儼	尙儼 尙儼 尙儼 尙儼	Gli spazi vuoti tra caratteri CKJ vengono ignorati.
Le celle contengono uno spazio tra i caratteri latini e CJK	EDM 尙儼	EDM 尙儼 EDM 尙儼	Gli spazi vuoti tra caratteri latini e CJK vengono ignorati.

Multitoken con parole non significative

Le parole non significative sono parole comuni, ad esempio articoli e preposizioni. Quando si creano token singoli, il processo di indicizzazione EDM ignora le parole rilevate nell'elenco di parole non significative EDM (`\Program Data\Symantec\Data Loss Prevention\Enforce Server\15.1\config\stopwords`), nonché le singole lettere. Tuttavia, quando si creano multitoken, le parole non significative e le singole lettere non vengono ignorate. Fanno invece parte del multitoken.

La [Tabella 22-21](#) mostra le corrispondenze multitoken con parole non significative, singole lettere e singole cifre.

Tabella 22-21 La cella contiene parole non significative, singole lettere o singole cifre

Descrizione	Contenuto cella	Corrispondenza	Spiegazione
La cella contiene una parola non significativa.	tirare altri palloni	tirare altri palloni	La parola comune ("altri") viene esclusa durante l'indicizzazione ma non quando fa parte di un multitoken.
La cella contiene una singola lettera.	tirare i palloni	tirare i palloni	La singola lettera ("i") viene esclusa, ma non quando fa parte di un multitoken.
La cella contiene una singola cifra.	tirare 2 palloni	tirare 2 palloni	Diversamente dalle parole con una singola lettera che sono parole non significative, le singole cifre non vengono mai ignorate.

Multitoken con caratteri in lingue miste

La [Tabella 22-22](#) mostra esempi di multitoken con caratteri latini e CJK misti.

Tabella 22-22 Esempi di cella multitoken con caratteri latini e CJK

Descrizione	Contenuto cella	Corrispondenza	Spiegazione
La cella contiene caratteri latini e CJK senza spazi.	ABC 𐄂𐄃 𐄂𐄃ABC	ABC 𐄂𐄃 𐄂𐄃ABC Corrisponde anche a: ABC 𐄂𐄃 𐄂𐄃 ABC EDM ignora lo spazio vuoto tra i caratteri latini e il token CJK.	La cella con caratteri latini e CJK misti è multitoken. Gli spazi vuoti tra caratteri latini e CJK vengono ignorati.
La cella contiene caratteri latini e CJK con uno o più spazi.	ABC 𐄂𐄃 𐄂𐄃 ABC	ABC 𐄂𐄃 𐄂𐄃 ABC Corrisponde anche a: ABC 𐄂𐄃 𐄂𐄃ABC	Gli spazi multipli vengono ignorati.
La cella contiene caratteri latini o CJK con numeri.	𐄂𐄃 𐄂𐄃 𐄂𐄃 𐄂𐄃 𐄂𐄃 147(𐄂𐄃 𐄂𐄃 51-1)	𐄂𐄃 𐄂𐄃 𐄂𐄃 𐄂𐄃 𐄂𐄃 147(𐄂𐄃 𐄂𐄃 51-1)	La cella contiene un singolo token.

Multi-token con punteggiatura

La punteggiatura viene sempre ignorata se si trova all'inizio o alla fine di un token o multi-token. L'obbligatorietà o meno della punteggiatura in un token o multi-token per la corrispondenza dipende dall'impostazione server avanzata `Lexer.IncludePunctuationInWords`, che per impostazione predefinita è **true** (attivata).

Vedere ["Caratteri di punteggiatura multitoken"](#) a pagina 522.

Nota: Per praticità il parametro `Lexer.IncludePunctuationInWords` verrà citato con l'acronimo a tre lettere "WIP" nella presente sezione.

L'impostazione WIP opera al momento del rilevamento per modificare la modalità di segnalazione delle corrispondenze. Per la maggior parte delle politiche EDM non è necessario cambiare l'impostazione WIP. Per casi limitati, quali numeri di conto o indirizzi, può risultare necessario impostare `IncludePunctuationInWords` su **false** a seconda dei requisiti di rilevamento.

Vedere ["Caratteri di punteggiatura multitoken"](#) a pagina 522.

La [Tabella 22-23](#) elenca e spiega come funziona la corrispondenza multitoken con la punteggiatura.

Tabella 22-23 Tabella di punteggiatura multi-token

Contenuto indicizzato	Contenuto rilevato	Impostazione WIP	Corrispondenza	Spiegazione
a.b	a.b	TRUE	Sì	Il contenuto indicizzato e il contenuto rilevato sono esattamente identici.
		FALSE	No	Il contenuto rilevato è considerato come "a b" e quindi non è una corrispondenza.
a.b	a b	TRUE	No	Il contenuto indicizzato e il contenuto rilevato sono differenti.
		FALSE	No	Il contenuto indicizzato e il contenuto rilevato sono differenti.
a b	a.b	TRUE	No	Il contenuto indicizzato e il contenuto rilevato sono differenti.
		FALSE	Sì	Il contenuto rilevato è considerato come "a b" e quindi è una corrispondenza.
a b	a b	TRUE	Sì	Il contenuto indicizzato e il contenuto rilevato sono esattamente identici.
		FALSE	Sì	Il contenuto indicizzato e il contenuto rilevato sono esattamente identici.

Ulteriori esempi per celle multitoken con punteggiatura

[Tabella 22-24](#) elenca e descrive alcuni esempi aggiuntivi per celle multitoken con punteggiatura. In questi esempi, è importante che durante l'indicizzazione, se un token include segni di punteggiatura tra i caratteri, la punteggiatura venga sempre mantenuta. Ciò significa che EDM non può individuare la cella interessata se l'impostazione WIP è FALSE, cioè se i dati indicizzati contengono celle con token con punteggiatura interna, l'impostazione WIP deve essere TRUE.

Tabella 22-24 Ulteriori casi di utilizzo per celle multitoken con punteggiatura

Descrizione	Contenuto indicizzato	Contenuto rilevato	Spiegazione
La cella contiene un indirizzo fisico con punteggiatura.	346 Guerrero St., Apt. #2	346 Guerrero St., Apt. #2 346 Guerrero St Apt 2	Il contenuto indicizzato è una cella multitoken. Entrambe corrispondono poiché la punteggiatura è stata inserita all'inizio o alla fine delle parti del subtoken, quindi viene ignorata.
La cella contiene punteggiatura interna senza spazio prima o dopo.	O'NEAL ST.	O'NEAL ST	Il contenuto indicizzato è una cella multitoken. La punteggiatura interna è inclusa (supponendo che WIP sia TRUE) e quella all'inizio o alla fine viene ignorata (supponendo che vi sia uno spazio di delimitazione dopo la punteggiatura).
La cella contiene caratteri asiatici (CJK) con punteggiatura interna indicizzata.	尙儗## 尙儗	尙儗##尙儗 (se WIP è TRUE)	Il contenuto indicizzato è una cella token singola. Durante il rilevamento, i caratteri asiatici (CJK) con punteggiatura interna vengono interessati dall'impostazione WIP. Quindi, in questo caso 尙儗##尙儗 corrisponde solo se l'impostazione WIP è TRUE. Se l'impostazione WIP è FALSE, 尙儗##尙儗 viene considerato un multitoken perché la punteggiatura interna viene considerata come spazio. Quindi, non può essere trovato alcun contenuto corrispondente.

Descrizione	Contenuto indicizzato	Contenuto rilevato	Spiegazione
La cella contiene caratteri asiatici (CJK) senza punteggiatura interna indicizzata.	尙儻 尙儻	尙儻 尙儻 尙儻##尙儻 (se WIP è FALSE)	Il contenuto indicizzato è una cella multitoken. Le corrispondenze dei contenuti individuate come indicizzate. Se l'impostazione WIP è FALSE, il contenuto individuato corrisponde a 尙儻##尙儻 perché la punteggiatura interna viene ignorata.
La cella contiene sia caratteri latini che asiatici con punteggiatura che li separa.	EDM##尙儻	EDM 尙儻	Il contenuto indicizzato è una cella multitoken. Una cella con caratteri latini e asiatici alternati è sempre un multitoken e la punteggiatura interna viene sempre considerata come un singolo spazio bianco indipendentemente dall'impostazione WIP.
La cella contiene sia caratteri latini che asiatici con punteggiatura interna.	DLP##EDM 尙儻##尙儻	DLP##EDM##尙儻##尙儻 (se WIP è true) DLP##EDM 尙儻##尙儻 (se WIP è true)	Il contenuto indicizzato è una cella multitoken. Durante il rilevamento, la punteggiatura tra i caratteri latini e asiatici viene considerata come un singolo spazio mentre la punteggiatura all'inizio e alla fine viene ignorata. Se l'impostazione WIP è TRUE, la punteggiatura interna ai caratteri latini e asiatici viene mantenuta. Se l'impostazione WIP è FALSE, non è possibile far corrispondere nessun contenuto perché la punteggiatura interna viene ignorata.

Descrizione	Contenuto indicizzato	Contenuto rilevato	Spiegazione
La cella contiene sia caratteri latini che asiatici con punteggiatura interna.	DLP EDM 衛像 衛像	DLP EDM 衛像 衛像 DLP#EDM 衛像#衛像 (se WIP è false) DLP#EDM##衛像#衛像 (se WIP è false)	Il contenuto indicizzato è una cella multitoken. Durante il rilevamento, la punteggiatura tra i caratteri latini e asiatici viene considerata come un singolo spazio mentre la punteggiatura all'inizio e alla fine viene ignorata. Quindi, esegue la corrispondenza come indicizzato. Se l'impostazione WIP è FALSE, viene cercata la corrispondenza con DLP;EDM##衛像#衛像 perché la punteggiatura interna viene ignorata.

Alcuni casi particolari di utilizzo per formati di dati riconosciuti dal sistema

EDM fornisce la convalida per e il riconoscimento dei seguenti formati speciali di dati:

- Numero di carta di credito
- Indirizzo e-mail
- Indirizzo IP
- Numero
- Percentuale
- Numero di telefono (Stati Uniti, Canada)
- Codice postale (Stati Uniti, Canada)
- Numero di previdenza sociale (Stati Uniti SSN)

Vedere ["Utilizzo delle convalide dei criteri fornite dal sistema per i profili EDM"](#) a pagina 498.

Nota: È riconosciuta come best practice convalidare sempre l'indice rispetto ai formati riconosciuti dal sistema quando l'origine dati include uno o più campi della colonna. altro. Vedere ["Mappaggio delle colonne origine dati ai campi di sistema per utilizzare la convalida"](#) a pagina 561.

La regola generale per i formati riconosciuti dal sistema è che l'impostazione WIP non viene applicata durante il rilevamento. Le regole per quel formato particolare invece si applicano. In altri termini, se il formato è riconosciuto durante il rilevamento, l'impostazione WIP non viene controllata. Ciò è sempre valido se il formato è una stringa di serie di caratteri come un indirizzo e-mail e se la cella contiene un numero conforme a uno dei numeri dei formati riconosciuti (quali CCN o SSN).

Inoltre, anche se il formato è un numero generico come il codice conto che non è conforme a uno dei numeri dei formati riconosciuti, l'impostazione WIP potrebbe non essere applicata. Per assicurare la corrispondenza precisa di numeri generici non conformi a uno dei formati riconosciuti dal sistema, non è necessario includere la punteggiatura in queste celle numero. Se i contenuti della cella sono conformi a uno dei formati riconosciuti dal sistema, le regole della punteggiatura per quel formato vengono applicate mentre le impostazioni WIP no.

Vedere ["Mancato utilizzo del delimitatore virgola se l'origine dati ha campi numerici"](#) a pagina 561.

Vedere [Tabella 22-25](#) a pagina 521. elenca e descrive gli esempi per rilevare i formati di dati riconosciuti dal sistema.

Attenzione: Questo elenco non è esauriente. Viene fornito solo a scopo informativo per garantire che l'utente disponga delle giuste informazioni relative alla corrispondenza dei dati dei formati riconosciuti dal sistema e che questi sono prioritari mentre le impostazioni WIP vengono ignorate. Prima di distribuire le politiche EDM nella fase di produzione, è necessario verificare l'accuratezza del rilevamento e regolare l'indice di conseguenza per assicurarsi che i dati indicizzati corrispondano come previsto durante il rilevamento.

Tabella 22-25 Alcuni casi particolari di utilizzo per formati di dati riconosciuti dal sistema

Descrizione	Contenuto indicizzato	Contenuto rilevato	Spiegazione
La cella contiene un indirizzo e-mail.	person@example.com	person@example.com	Un indirizzo e-mail viene indicizzato e individuato come token singolo indipendentemente dall'impostazione WIP. Deve corrispondere esattamente all'indicizzazione. Se dovesse essere necessario impostare le WIP su FALSE, "person example com" non corrisponderebbe né come multitoken né come token singolo indicizzato.

Descrizione	Contenuto indicizzato	Contenuto rilevato	Spiegazione
Le celle contengono un codice conto di 10 cifre.	#####	##### (###) ### #### (###) ### ####	L'impostazione WIP viene ignorata poiché il numero è conforme al formato del numero di telefono e le sue regole sono prioritarie.
	## ##### ##	## ##### ##	Deve corrispondere esattamente. Il formato ### ##### ## non corrisponde anche se WIP è impostato su FALSE.
	### ##### ###	### ##### ###	Deve corrispondere esattamente. Il formato ### ##### ### non corrisponde anche se WIP è impostato su FALSE.

Caratteri di punteggiatura multitoken

Nell'EDM una cella multitoken è qualsiasi cella indicizzata che contiene caratteri di punteggiatura (nonché spazi o parole latine alternative e caratteri CJK).

Vedere [Tabella 22-26](#) a pagina 522.

[Utilizzo della corrispondenza multitoken](#) elenca i simboli che vengono identificati e trattati come punteggiatura durante l'indicizzazione EDM.

Tabella 22-26 Caratteri trattati come punteggiatura per l'indicizzazione

Nome segno di punteggiatura	Rappresentazione con carattere
Apostrofo	'
Tilde	~
Punto esclamativo	!
E commerciale	&
Trattino	-
Virgoletta singola	'
Virgoletta doppia	"
Punto	.

Nome segno di punteggiatura	Rappresentazione con carattere
Punto interrogativo	?
Chiocciola	@
Segno di dollaro	\$
Segno di percentuale	%
Asterisco	*
Accento circonflesso	^
Parentesi tonda aperta	(
Parentesi tonda chiusa)
Parentesi quadra aperta	[
Parentesi quadra chiusa]
Parentesi graffa aperta	{
Parentesi graffa chiusa	}
Barra	/
Barra rovesciata	\
Segno del cancelletto	#
Segno di uguale	=
Segno più	+

Esempi di varianti di totale corrispondenze

Il valore predefinito dell'impostazione Advanced Server **EDM.MatchCountVariant** elimina le corrispondenze che sono composte dallo stesso set di token di qualche altra corrispondenza. Raramente è necessario modificare il valore predefinito. Tuttavia, se necessario, è possibile configurare come le corrispondenze EDM vengono contate con questo parametro.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

La [Tabella 22-27](#) fornisce alcuni esempi di conteggio delle corrispondenze. In tutti gli esempi si presuppone che la politica sia impostata per cercare la corrispondenza con tre campi di colonna su quattro e che l'indice del profilo contenga i contenuti di cella seguenti:

Mario | Rossi | 123-45-6789 | 1111-1111-1111-1111

Mario | Rossi | 123-45-6789 | 2222-2222-2222-2222

Mario | Rossi | 123-45-6789 | 3333-3333-3333-3333

Tabella 22-27 Esempi di varianti di totale corrispondenze

Contenuto messaggio in entrata	Variante totale corrispondenze	Numero di corrispondenze	Spiegazione
Mario Rossi 123-45-6789	1	3	Record corrispondenti nel profilo: nome, cognome e numero di previdenza sociale.
	2	1	Numero di set di token univoci corrispondenti.
	3	1	Numero di superset univoci di set di token.
Mario Rossi 123-45-6789 1111-1111-1111-1111	1	3	Se EDM.HighlightAllMatchesInProximity=false, l'EDM cerca la corrispondenza dei token all'estrema sinistra per ciascuna riga di dati del profilo. Il set di token per ciascuna riga è il seguente: Riga n. 1: Mario Rossi 123-45-6789
Mario Rossi 123-45-6789	2	1: se EDM.HighlightAllMatchesInProximity=false (impostazione predefinita) 2: se EDM.HighlightAllMatchesInProximity=true	Riga n. 2: Mario Rossi 123-45-6789 Riga n. 3: Mario Rossi 123-45-6789
	3	1	Se EDM.HighlightAllMatchesInProximity=true, l'EDM cerca la corrispondenza di tutti i token nell'intervallo di prossimità. Il set di token per ciascuna riga è il seguente: Riga n. 1: Mario Rossi 123-45-6789 1111-1111-1111-1111 Mario Rossi 123-45-6789 Riga n. 2: Mario Rossi 123-45-6789 Mario Rossi 123-45-6789 Riga n. 3: Mario Rossi 123-45-6789 Mario Rossi 123-45-6789

Contenuto messaggio in entrata	Variante totale cognome	Numero di corrispondenze	Spiegazione
1111-1111-1111-1111 Mario Rossi 123-45-6789	1	3	Se
	2	2	EDM.HighlightAllMatchesInProximity=false, l'EDM cerca la corrispondenza dei token all'estrema sinistra per ciascuna riga di dati del profilo. Il set di token per ciascuna riga è il seguente:
	3	2: se EDM.HighlightAllMatchesInProximity=false (impostazione predefinita) 1: se EDM.HighlightAllMatchesInProximity=true	Riga n. 1: 1111-1111-1111-1111 Mario Rossi Riga n. 2: Mario Rossi 123-45-6789 Riga n. 3: Mario Rossi 123-45-6789 Se EDM.HighlightAllMatchesInProximity=true, l'EDM cerca la corrispondenza di tutti i token nell'intervallo di prossimità. Il set di token per ciascuna riga è il seguente: Riga n. 1: 1111-1111-1111-1111 Mario Rossi 123-45-6789 Riga n. 2: Mario Rossi 123-45-6789 Riga n. 3: Mario Rossi 123-45-6789

Esempio di corrispondenza di prossimità

L'EDM protegge i dati riservati correlando informazioni identificabili in modo unico, ad esempio il numero di previdenza sociale, con dati che non sono univoci, ad esempio il cognome. Nella correlazione dei dati è importante assicurarsi che i termini siano correlati. Nelle lingue naturali è più probabile che, quando due parole compaiono vicino, vengano utilizzate nello stesso contesto e siano pertanto correlate.

Se si parte dal presupposto che la prossimità delle parole indica una correlazione, l'EDM impiega un raggio o un intervallo di corrispondenza di prossimità per limitare la quantità di contenuto libero che il sistema esaminerà durante la ricerca di corrispondenze. La corrispondenza di prossimità EDM ha lo scopo di ridurre i falsi positivi garantendo che i termini corrispondenti siano vicini.

L'intervallo di prossimità è proporzionale alla definizione della politica. L'intervallo di prossimità è determinato dal raggio di prossimità moltiplicato per il numero di corrispondenze richieste dalla condizione di politica EDM. Il raggio è impostato dal parametro delle impostazioni avanzate del server EDM.SimpleTextProximityRadius. Il valore predefinito è 35. Inoltre la corrispondenza di prossimità si applica sia al testo libero sia ai dati tabulari. Tra i due non

esiste alcuna distinzione in fase di runtime. Pertanto i dati tabulari vengono trattati allo stesso modo del testo libero e il controllo di prossimità eseguito va oltre l'ambito della lunghezza del contenuto delle righe.

Ad esempio si presupponga che il raggio predefinito sia 35 e che la politica corrisponda a 3 campi di colonna su 4. In questo caso l'intervallo di prossimità è 105 token (3×35). Se la politica corrisponde a 2 campi su 3, l'intervallo di prossimità è 70 token (35×2).

Avvertimento: Anche se è possibile ridurre il valore del raggio di prossimità, Symantec non consiglia l'aumento del valore oltre l'impostazione predefinita (35). In caso contrario possono sorgere problemi prestazionali. Vedere ["Configurazione di impostazioni avanzate per i criteri EDM"](#) a pagina 509.

La [Tabella 22-28](#) mostra un esempio di corrispondenza di prossimità in base all'impostazione predefinita del raggio di prossimità. In questo esempio, il contenuto rilevato restituisce una corrispondenza univoca di un set di token, come descritto di seguito:

- L'intervallo di prossimità è 105 token (35×3).
- L'intervallo di prossimità inizia con la corrispondenza all'estrema sinistra ("Rossi") e termina all'estremità destra ("123-45-6789").
- Il numero totale di token tra "Rossi" e il numero di previdenza sociale (entrambi compresi) è 105 token.
- Le parole non significative "altro" e "un" vengono considerate per scopi di prossimità.
- "Bank of America" è un multitoken. Ogni parte del subtoken di un multitoken è considerata un singolo token per scopi di prossimità.

Tabella 22-28 Esempio di prossimità

Dati indicizzati	Politica	Prossimità	Contenuto rilevato
Cognome Datore di lavoro Numero di previdenza sociale Rossi Bank of America 123-45-6789	Corrispondenza 3 di 3	Raggio = 35 token (impostazione predefinita)	Zenderit inceptos Mario Rossi lorem ipsum pharetra convallis leo suscipit ipsum sodales rhoncus, vitae dui nisi volutpat augue maecenas in, luctus id risus magna arcu maecenas leo quisque. Rutrum convallis tortor urna morbi elementum hac curabitur morbi, nunc dictum primis elit senectus faucibus convallis surfrent. Aptentnour gravida adipiscing iaculis himenaeos, himenaeos a porta etiam viverra. Class torquent uni other tristique cubilia in Bank of America . Dictumst lorem eget ipsum. Hendrerit inceptos other sagittis quisque. Leo mollis per nisl per felis, nullam cras mattis augue turpis integer pharetra convallis suscipit hendrerit? Lubilia en mictumst horem eget ipsum. Inceptos urna sagittis quisque dictum odio hendrerit convallis suscipit ipsum wrdsrf 123-45-6789 .

Aggiornamento degli indici EDM alla versione più recente

Quando si eseguire l'upgrade a Symantec Data Loss Prevention 15.1 da una versione precedente, è necessario aggiornare ciascun profilo **Dati esatti** reindicizzando l'origine dati mediane l'indicizzatore EDM 15.1. È necessario verificare la quantità di memoria necessaria per l'indicizzazione dell'origine dati e il caricamento e l'elaborazione dell'indice in fase di runtime sul server di rilevamento.

Vedere ["Informazioni sull'upgrade delle distribuzioni EDM"](#) a pagina 484.

Vedere ["Requisiti di memoria per EDM"](#) a pagina 532.

Se non si reindicizza il file origine dati, il sistema restituisce messaggi di errore indicanti che il profilo **Dati esatti** è obsoleto. È necessario reindicizzare il profilo **Dati esatti** e ricalcolare i requisiti di memoria.

Vedere ["Codici di errore per indice EDM obsoleto"](#) a pagina 531.

Per EDM esistono due scenari principali di upgrade a 15.1:

- Si utilizza Remote EDM Indexer per creare remotamente indici conformi alla versione 15.1 e copiarli in Enforce Server.
Vedere ["Processo di aggiornamento con Remote EDM Indexer"](#) a pagina 528.
- Si dispone già di un file origine dati aggiornato e ottimizzato, da copiare in Enforce Server 15.1 aggiornato per l'indicizzazione.

Vedere ["Processo di aggiornamento con Enforce Server"](#) a pagina 530.

Processo di aggiornamento con Remote EDM Indexer

Utilizzare la seguente procedura per l'aggiornamento delle distribuzioni EDM a Symantec Data Loss Prevention 15.1. In questa procedura si presuppone che sia possibile indicizzare in remoto l'origine dati e copiare il file di indice su Enforce Server.

Vedere ["Indicizzazione EDM remota"](#) a pagina 539.

Se l'indicizzazione remota non è possibile, l'altra opzione per l'upgrade è copiare il file origine dati su Enforce Server 15.1.

Vedere ["Processo di aggiornamento con Enforce Server"](#) a pagina 530.

Tabella 22-29 Processo di aggiornamento con Remote EDM Indexer

Passaggio	Azione	Descrizione
1	Eseguire l'upgrade di Enforce Server a 15.1.	<p>Consultare il <i>Manuale di upgrade di Symantec Data Loss Prevention</i> all'indirizzo http://www.symantec.com/docs/DOC9258 per informazioni dettagliate.</p> <p>Non aggiornare ora i server di rilevamento EDM.</p> <p>Enforce Server 15.1 può continuare a ricevere incidenti dai server di rilevamento non 15.1 durante il processo di upgrade. Le politiche e altri dati non possono venire distribuiti ai server di rilevamento non 15.1 (comunicazione unidirezionale solo tra Enforce Server 15.1 e server di rilevamento non 15.1).</p>
2	Creare un modello di profilo EDM remoto compatibile con 15.1.	<p>Utilizzando la console di amministrazione di Enforce Server 15.1, creare un nuovo modello di profilo EDM per l'indicizzazione EDM remota.</p> <p>Vedere "Creazione del modello di un profilo EDM per l'indicizzazione remota" a pagina 543.</p> <p>Scaricare il modello di profilo *.edm e copiarlo sul sistema host dell'origine dati remoto.</p> <p>Vedere "Download e copia del file di profilo EDM in un sistema remoto" a pagina 546.</p>
3	Installare Remote EDM Indexer 15.1 sull'host dell'origine dati remoto.	<p>Installare Remote EDM Indexer di Symantec Data Loss Prevention 15.1 sull'host dell'origine dati remoto in modo che sia possibile indicizzare l'origine dati.</p> <p>Vedere "Indicizzazione EDM remota" a pagina 539.</p>

Passaggio	Azione	Descrizione
4	Calcolare la memoria necessaria per indicizzare l'origine dati e regolare l'impostazione di memoria dell'indicizzatore.	<p>Calcolare la memoria necessaria per l'indicizzazione prima di tentare di indicizzare l'origine dati. A Remote EDM Indexer viene allocata memoria sufficiente per indicizzare la maggior parte delle origini dati. Se si dispone di un indice molto grande, è possibile che sia necessario assegnare altra memoria.</p> <p>Vedere "Requisiti di memoria per EDM" a pagina 532.</p>
5	Indicizzare l'origine dati con Remote EDM Indexer 15.1.	<p>Da questo processo risultano più file *.rdx compatibili con 15.1, che è possibile caricare in un sistema Enforce Server 15.1.</p> <p>Se si dispone di un file origine dati preparato, eseguire Remote EDM Indexer e indicizzarlo.</p> <p>Vedere "Esempi di indicizzazione remota mediante il file origine dati" a pagina 547.</p> <p>Se l'origine dati è un database Oracle e i dati sono puliti, utilizzare SQL Preindexer per collegare in cascata i dati a Remote EDM Indexer.</p> <p>Vedere "Esempi di indicizzazione remota con SQL Preindexer" a pagina 548.</p>
6	Calcolare la memoria necessaria per caricare ed elaborare l'indice e regolare l'impostazione della memoria del server di rilevazione per ciascun host del server di rilevazione EDM.	<p>Occorre calcolare quanta RAM richiede il server di rilevazione per caricare ed elaborare l'indice in fase di runtime. Questi calcoli sono necessari per ciascun indice EDM che si desidera distribuire.</p> <p>Vedere "Requisiti di memoria per EDM" a pagina 532.</p>
7	Aggiornare il profilo EDM caricando l'indice 15.1.	<p>Copiare i file *.pdx e *.rdx dall'host remoto sul file system dell'host di Enforce Server 15.1.</p> <p>Caricare l'indice nel profilo EDM creato nel passaggio 2.</p> <p>Vedere "Copia e caricamento di file di indice remoti su Enforce Server" a pagina 549.</p>
8	Aggiornare uno o più server di rilevamento EDM a 15.1.	<p>Dopo avere creato i profili EDM compatibili con 15.1 e avere eseguito l'upgrade a Enforce Server, è possibile aggiornare i server di rilevamento.</p> <p>Consultare il <i>Manuale di upgrade di Symantec Data Loss Prevention</i> all'indirizzo http://www.symantec.com/docs/DOC9258 per informazioni dettagliate.</p> <p>Assicurarsi di avere calcolato e verificato i requisiti di memoria per il caricamento e l'elaborazione degli indici multitoken sul server di rilevamento.</p> <p>Vedere "Requisiti di memoria per EDM" a pagina 532.</p>

Passaggio	Azione	Descrizione
9	Testare e verificare l'indice aggiornato.	Per testare il sistema e l'indice aggiornati, è possibile creare una nuova politica che faccia riferimento all'indice aggiornato.
10	Rimuovere gli indici EDM obsoleti.	Dopo avere verificato il nuovo indice EDM e la nuova politica, è possibile ritirare la politica e l'indice EDM precedenti. Nota: Gli indici creati per le versioni precedenti a 14.0 non funzionano con la versione 14.5 e successive.

Processo di aggiornamento con Enforce Server

Utilizzare la procedura di aggiornamento dell'indice descritta di seguito se l'indicizzazione remota non è possibile e si dispone di un file origine dati corrente che si può copiare su Enforce Server.

Tabella 22-30 Processo di aggiornamento con Enforce Server

Passaggio	Azione	Descrizione
1	Eseguire l'upgrade di Enforce Server a 15.1.	Consultare il <i>Manuale di upgrade di Symantec Data Loss Prevention</i> all'indirizzo http://www.symantec.com/docs/DOC9258 per informazioni dettagliate. Non eseguire ora l'upgrade dei server di rilevamento EDM. Enforce Server 15.1 può continuare a ricevere incidenti dai server di rilevamento non 15.1 durante il processo di upgrade. Le politiche e altri dati non possono venire distribuiti ai server di rilevamento non 15.1 (comunicazione unidirezionale solo tra Enforce Server 15.1 e server di rilevamento non 15.1).
2	Creare, preparare e copiare il file origine dati sull'host di Enforce Server 15.1.	Copiare il file di origine dati nella directory <code>opt/Symantec/DataLoss Prevention/Enforce Server/15.1/Protect/datafiles</code> (Linux) o <code>C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\datafiles</code> (in Windows) nel file system dell'host di Enforce Server 15.1 sottoposto a upgrade. Vedere " Creazione del file origine dati esatti per EDM " a pagina 486. Vedere " Preparazione del file origine dati esatti per l'indicizzazione " a pagina 488. Vedere " Caricamento di file origine dati esatti in Enforce Server " a pagina 490.
3	Calcolare la memoria necessaria per indicizzare l'origine dati e aggiornare l'impostazione della memoria dell'indicizzatore.	Calcolare la memoria necessaria per l'indicizzazione prima di tentare di indicizzare l'origine dati. Vedere " Requisiti di memoria per EDM " a pagina 532.

Passaggio	Azione	Descrizione
4	Creare un nuovo profilo EDM conforme a 15.1 e indicizzare il file origine dati.	<p>Creare un nuovo profilo EDM utilizzando la console di amministrazione di Enforce Server 15.1.</p> <p>Scegliere l'opzione Usa origine dati nell'host manager come riferimento per caricare il file origine dati (si presupponga che lo si sia copiato nella directory /datafiles).</p> <p>Indicizzare il file origine dati al momento del salvataggio del profilo.</p> <p>Vedere "Creazione e modifica di profili dati esatti" a pagina 492.</p>
5	Calcolare la memoria necessaria per caricare ed elaborare l'indice in fase di runtime. Regolare le impostazioni della memoria per ciascun host del server di rilevamento EDM.	<p>È necessario calcolare la quantità di RAM richiesta dal server di rilevamento per caricare ed elaborare l'indice in fase di runtime. Questi calcoli sono necessari per ogni indice EDM che si desidera distribuire. Le regolazioni della memoria sono cumulative.</p> <p>Vedere "Requisiti di memoria per EDM" a pagina 532.</p>
6	Eseguire l'upgrade a 15.1 del server di rilevamento EDM.	<p>Dopo avere creato il profilo EDM conforme a 15.1, è possibile aggiornare i server di rilevamento.</p> <p>Consultare il <i>Manuale di upgrade di Symantec Data Loss Prevention</i> all'indirizzo http://www.symantec.com/docs/DOC9258 per informazioni dettagliate.</p> <p>Assicurarsi di avere calcolato e verificato i requisiti di memoria per il caricamento e l'elaborazione degli indici multitoken sul server di rilevamento.</p> <p>Vedere "Requisiti di memoria per EDM" a pagina 532.</p>
7	Testare e verificare l'indice aggiornato.	<p>Per testare il sistema e l'indice aggiornati, è possibile creare una nuova politica che faccia riferimento all'indice aggiornato.</p>
8	Rimuovere gli indici EDM obsoleti.	<p>Dopo avere verificato il nuovo indice EDM e la nuova politica, è possibile ritirare la politica e l'indice EDM precedenti.</p> <p>Nota: Gli indici creati per le versioni precedenti a 14.0 non funzionano con la versione 14.5 e successive.</p> <p>Vedere "Indicizzazione EDM remota" a pagina 539.</p>

Codici di errore per indice EDM obsoleto

Symantec Data Loss Prevention versione 15.1 ha fornito vari aggiornamenti per EDM. È necessario reindicizzare l'origine dati per ogni profilo **Dati esatti** utilizzando l'indicizzatore EDM 15.1.

Se l'indice EDM non è compatibile con la versione corrente, il sistema restituisce codici di errore. Questi codici di errore sono elencati in [Tabella 22-31](#).

Tabella 22-31 Messaggi di errore per Profili dati esatti non conformi

Tipo di messaggio di errore	Codice errore	Messaggio di errore
Evento errore Enforce Server	2928	Uno o più profili EDM sono obsoleti e devono essere reindicizzati. Vedere "Aggiornamento degli indici EDM alla versione più recente" a pagina 527. Vedere "Requisiti di memoria per EDM" a pagina 532.
Dettagli evento errore Enforce Server	2928	Verificare la pagina Gestisci > Profili dati > Dati esatti . I seguenti profili DM sono obsoleti: Profilo X, Profilo XY e così via.
Errore di evento di sistema	2928	Uno o più profili EDM sono obsoleti e devono essere reindicizzati.
Errore Profilo dati esatti	N/D	Il profilo non è aggiornato e deve essere reindicizzato.

Requisiti di memoria per EDM

L'utilizzo di EDM per le distribuzioni di Symantec Data Loss Prevention ha effetto sui requisiti di memoria hardware per le distribuzioni di Symantec Data Loss Prevention. In particolare, EDM ha effetto sulla memoria necessaria per indicizzare i dati e sulla memoria necessaria per caricare l'indice nel server di rilevamento.

Una volta definiti i requisiti di memoria specifici di EDM, è possibile valutare come tali requisiti influiscano sui requisiti di sistema generali della distribuzione di Data Loss Prevention. Per informazioni dettagliate sui requisiti generali e sul potenziale effetto della distribuzione di EDM, consultare la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*.

Informazioni sui requisiti di memoria per EDM

I requisiti di memoria per EDM sono correlati a molti fattori, tra cui:

- Numero degli indici che si sta costruendo
- Dimensione totale degli indici
- Numero di celle in ogni indice
- Numero di catene di messaggi

Queste limitazioni di dimensioni si applicano agli indici EDM:

- Il numero massimo di righe supportato è 4.294.967.294.

- Il numero massimo di celle supportato è 6 miliardi.

Tabella 22-32 offre una panoramica dei passaggi a cui attenersi per determinare e impostare i requisiti di memoria per EDM.

Tabella 22-32 Flusso di lavoro per determinare i requisiti di memoria per indici EDM

Passaggio	Azione	Per ulteriori informazioni
1	Determinare la memoria necessaria per indicizzare l'origine dati.	Vedere "Panoramica della memoria di configurazione e di indicizzazione dell'origine dati" a pagina 533.
2	Aumentare la memoria dell'indicizzatore sulla base dei calcoli.	Vedere "Determinazione dei requisiti per indicizzatori locali e remoti" a pagina 534.
3	Determinare la memoria necessaria per caricare l'indice sul server di rilevazione.	Vedere "Requisiti di memoria del server di rilevazione" a pagina 535.
4	Aumentare la memoria del server di rilevazione in base ai calcoli.	Vedere "Aumento della memoria del server di rilevamento (lettore del file)" a pagina 538.
5	Ripetere la procedura per ogni indice di EDM che si desidera distribuire.	

Panoramica della memoria di configurazione e di indicizzazione dell'origine dati

Tabella 22-33 fornisce i passaggi per determinare la quantità di memoria necessaria per indicizzare l'origine dati.

Tabella 22-33 Requisiti di memoria dell'indicizzazione dell'origine dati

Passaggio	Azione	Dettagli
1	Stimare i requisiti di memoria dell'indicizzatore.	Vedere "Determinazione dei requisiti per indicizzatori locali e remoti" a pagina 534.
2	Aumentare la memoria dell'indicizzatore.	Quindi, aumentare la memoria allocata all'indicizzatore. La procedura per aumentare la memoria dell'indicizzatore cambia se si sta utilizzando l'indicizzatore EDM locale nell'Enforce Server o l'indicizzatore EDM remoto.

Passaggio	Azione	Dettagli
3	Riavviare il servizio Symantec DLP Manager.	È necessario riavviare questo servizio dopo aver modificato l'allocazione della memoria.
4	Indicizzare l'origine dati.	Infine, indicizzare l'origine dati. È necessario eseguire questo passaggio prima di calcolare i requisiti di memoria rimanente. Vedere "Configurazione di profili dati esatti" a pagina 484.

Determinazione dei requisiti per indicizzatori locali e remoti

Questo argomento fornisce una panoramica dei requisiti di memoria per l'indicizzatore EDM locale in Symantec Data Loss Prevention Enforce Server e per l'indicizzatore EDM remoto.

Con le impostazioni predefinite, entrambi gli indicizzatori EDM possono indicizzare qualsiasi origine dati con un massimo di 500 milioni di celle. Per qualsiasi origine dati con oltre 500 milioni di celle, sono necessari 3 byte per cella per indicizzare l'origine dati.

È possibile programmare l'indicizzazione per più indici in sequenza (in momenti diversi) o in parallelo (nello stesso momento). Nell'indicizzazione in sequenza, è necessario assegnare la memoria per ospitare l'indicizzazione dell'indice maggiore. Nell'indicizzazione in parallelo, è necessario assegnare la memoria per ospitare l'indicizzazione di tutti gli indici in corso di creazione in quel momento.

Indicizzazione seriale

Se si creano gli indici in sequenza (due sono creati in parallelo), i requisiti di memoria per l'indice maggiore sono:

2 miliardi di celle – 0,5 miliardi predefiniti x 3 byte = 4,5 GB arrotondati in 5 GB di memoria aggiuntiva.

Questo requisito di memoria include 2 GB (2048 MB) di memoria predefinita per Enforce Server e 5 GB di memoria di sistema aggiuntiva.

[Tabella 22-34](#) fornisce esempi su come le dimensioni dell'origine dati influiscono sui requisiti di memoria dell'indicizzatore per gli indici seriali.

Tabella 22-34 Esempi per indicizzazione seriale requisiti di memoria indicizzatore

Dimensioni origine dati	Requisito memoria indicizzatore	Descrizione
100 milioni di celle	2048 MB (predefinito)	Nessuna RAM aggiuntiva necessaria per l'indicizzatore.
500 milioni di celle	2048 MB (predefinito)	Nessuna RAM aggiuntiva necessaria per l'indicizzatore.

Dimensioni origine dati	Requisito memoria indicizzatore	Descrizione
1 miliardo di celle	4 GB	Se si dispone di una singola origine dati con 1 miliardo di celle (ad esempio, 10 colonne per 100 milioni di righe), è necessario disporre di memoria di sistema aggiuntiva per 0.5 miliardi di celle (1 miliardo di celle – 0,5 milioni predefiniti) 0.5 milioni x 3 byte, o 1.5 GB di RAM (arrotondato a 2 GB) per indicizzare l'origine dati. Questo importo viene aggiunto all'utilità di servizio RAM dell'indicizzatore di default.
2 miliardi di celle	7 GB	Se si dispone di una singola origine dati con 2 miliardi di celle (ad esempio, 10 colonne per 200 milioni di righe), è necessario disporre di memoria aggiuntiva per 1,5 miliardi di celle (2 miliardi di celle – 0,5 milioni predefiniti) 1,5 milioni x 3 byte, o 4,5 GB di RAM (arrotondato a 5 GB) per indicizzare l'origine dati.

Indicizzazione parallela

Se vengono indicizzati questi quattro file in [Tabella 22-34](#) simultaneamente (in parallelo), è in corso l'indicizzazione di oltre 500 milioni di celle. Quindi, la memoria aggiuntiva (3,6 miliardi di celle – 0,5 miliardi di celle forniti per impostazione predefinita) richiesta è la seguente:

3,1 miliardi di celle x 3 byte = 9,3 GB arrotondati a 10 GB di memoria aggiuntiva.

Come spiegato in dettaglio in seguito, impostare `wrapper.java.maxmemory` su 12 GB. Questo requisito di memoria include 2048 MB di memoria predefinita per Enforce Server e 9 GB di memoria di sistema aggiuntiva dal calcolo della memoria aggiuntiva di cui sopra.

Nota: Per gli indici di lingua CJK o gli indici in maniera predominante a più token, tali formule dovrebbero utilizzare un moltiplicatore di 4 byte invece che 3. In entrambi i casi, un'origine dati da 350 milioni di celle è supportata per impostazione predefinita.

Requisiti di memoria del server di rilevazione

Il server di rilevamento non dovrebbe utilizzare più del 60% della memoria del computer. Ad esempio, se il server di rilevazione necessita di 6 GB di memoria per l'esecuzione, assicurarsi di disporre di 10 GB su tale server.

Configurazione predefinita per un server di rilevamento

La configurazione predefinita per un server di rilevamento prevede 4 GB e 8 catene di messaggi. Consultare le seguenti formule e [Tabella 22-35](#) per determinare come calcolare gli effettivi requisiti di memoria. Inoltre, per determinare i requisiti di memoria effettivi è possibile utilizzare il foglio di calcolo fornito nel centro di supporto Symantec

<http://www.symantec.com/docs/DOC8255.html>. Vedere "Utilizzo del foglio di elettronico dei requisiti di memoria EDM" a pagina 539.

Per caricare l'indice, il server di rilevamento necessita di 13 byte per cella per la memoria di sistema più 1 GB di memoria heap Java per ciascuna catena di messaggi nel server di rilevamento. I seguenti esempi mostrano gli scenari per un cliente con tre indici, tutti con la stessa pianificazione.

Per i requisiti di memoria heap Java, la formula è:

Requisito di memoria heap Java = il numero di catene di messaggi * 1 GB.

Per i requisiti di memoria di sistema, la formula generale è:

Requisito di memoria di sistema = numero di celle * 13 byte.

Impostazioni di memoria Server di rilevamento

La proprietà Impostazioni server avanzate per il numero di catene di messaggi è:

```
MessageChain.NumChains.
```

Le impostazioni di memoria heap Java per un server di rilevamento si effettuano nella console di amministrazione del server di rilevamento alla pagina **Dettagli server - Impostazioni server avanzate**, tramite `BoxMonitor.FileReaderMemory.` proprietà. Il formato è `-Xrs -Xms1200M -Xmx4G`. Non è necessario cambiare l'impostazione della memoria di sistema, ma occorre assicurarsi che il server di rilevamento abbia memoria disponibile sufficiente.

Nota: Quando si aggiorna questa impostazione, modificare solo il valore `-Xmx` in questa proprietà. Ad esempio, modificare solo "4G." in un nuovo valore e lasciare uguali tutti gli altri valori.

Gli esempi in [Tabella 22-35](#) mostrano le impostazioni per cinque diverse situazioni.

Tabella 22-35 Impostazioni di memoria heap Java del server di rilevamento EDM ed esempi di memoria di sistema aggiuntiva

Esempio	Calcolo	Impostazione Boxmonitor.FileReaderMemory	Memoria di sistema aggiuntiva necessaria
Esempio 1: singolo indice di piccole dimensioni con 2 milioni di celle da caricare	<p>Requisito di memoria heap di Java:</p> $1 * 1 \text{ GB} = 2 \text{ GB}$ <p>La memoria di sistema è:</p> $2 \text{ milioni} * 13 \text{ byte} = 25 \text{ MB}$	-Xmx6G	25 MB
<p>Esempio 2:</p> <p>3 indici durante l'esecuzione di 24 catene di messaggi:</p> <ul style="list-style-type: none"> ■ Indice 1: 100 milioni di celle ■ Indice 2: 1 miliardo di celle ■ Indice 3: 2 miliardi di celle 	<p>Il requisito di memoria heap Java è:</p> $24 * 1 \text{ GB} = 24 \text{ GB}$ <p>Il requisito di memoria di sistema è:</p> <p>Per l'indice da 100 milioni di celle: $100 \text{ milioni} * 13 \text{ byte} = 1,2 \text{ GB}$</p> <p>Per l'indice da 1 miliardo di celle:</p> $1 \text{ miliardo} * 13 \text{ byte} = 12 \text{ GB}$ <p>Per l'indice da 2 miliardi di celle:</p> $2 \text{ miliardi} * 13 \text{ byte} = 24 \text{ GB}$ <p>Il requisito di memoria di sistema totale è:</p> $1,2 \text{ GB} * 12 = 12 \text{ GB} + 24 \text{ GB} = 36 \text{ GB}$	-Xmx28G	37.2 GB

Esempio	Calcolo	Impostazione Boxmonitor.FileReaderMemory	Memoria di sistema aggiuntiva necessaria
Esempio 3: un singolo indice con 5 miliardi di celle e 24 catene di messaggi	<p>Il requisito di memoria heap Java è:</p> $24 * 1 \text{ GB} = 24 \text{ GB}$ <p>Il requisito di memoria di sistema è:</p> $5 \text{ miliardi} * 13 \text{ byte} = 60,5 \text{ GB}$	-Xmx28G	60.5 GB
Esempio 4: un singolo indice con 1,6 miliardi di celle e 24 catene di messaggi	<p>Il requisito di memoria heap Java è:</p> $24 * 1 \text{ GB} = 24 \text{ GB}$ <p>Il requisito di memoria di sistema è:</p> $1,6 \text{ miliardi} * 13 \text{ byte} = 19,3 \text{ GB}$	-Xmx28G	19.3 GB
Esempio 5: un singolo indice con 500 milioni di celle e 8 catene di messaggi	<p>Il requisito di memoria heap Java è:</p> $8 * 1 \text{ GB} = 8 \text{ GB}$ <p>Il requisito di memoria di sistema è:</p> $500 \text{ milioni} * 13 \text{ byte} = 6,1 \text{ GB}$	-Xmx12G	6,1 GB

Aumento della memoria del server di rilevamento (lettore del file)

Questo argomento fornisce le istruzioni per aumentare allocazione della memoria del lettore del file per un server di rilevamento. Per eseguire queste istruzioni è necessario aver calcolato la disponibilità necessaria.

Per aumentare la memoria dell'elaborazione dell'Enforce Server

- 1 Nella console di amministrazione di Enforce Server, accedere alla schermata **Dettagli server - Impostazioni server avanzate** del server di rilevamento in cui l'indice EDM è distribuito o deve essere distribuito.
- 2 Individuare l'impostazione seguente: `BoxMonitor.FileReaderMemory`.

- 3 Cambiare il valore **-Xmx4G** nella seguente stringa secondo i calcoli effettuati.
-Xrs -Xms1200M **-Xmx4G** -XX:PermSize=128M -XX:MaxPermSize=256M
Ad esempio: -Xrs -Xms1200M **-Xmx11G** -XX:PermSize=128M -XX:MaxPermSize=256M
- 4 Salvare la configurazione e riavviare il server di rilevamento.

Utilizzo del foglio di elettronico dei requisiti di memoria EDM

Il foglio elettronico dei requisiti di memoria EDM consente di determinare la quantità di memoria di sistema aggiuntiva necessaria sul server di rilevamento per eseguire gli indici. È disponibile come foglio elettronico Excel nel centro di supporto Symantec all'indirizzo:

https://support.symantec.com/en_US/article.DOC8255.html

Figura 22-1 mostra un esempio del foglio elettronico con quattro catene di messaggi e tre indici.

Figura 22-1 Foglio elettronico dei requisiti di memoria EDM

	A	B	C	
1	# of cells in Index 1	# of cells in Index 2	# of cells in Index 3	# of
2	10,000,000	120,000,000	50,000,000	
10	Required RAM		2 GB	

Per calcolare la memoria di sistema aggiuntiva necessari per eseguire gli indici, immettere le seguenti informazioni:

1. Ottenere il numero di celle in ogni indice (è possibile specificare fino a 10 indici).
2. Immettere tale numero in **numero di celle in indice**.

Quando si modifica un valore, il foglio elettronico aggiorna il campo della **RAM necessaria**.

Il valore del campo **RAM necessaria** è la quantità di memoria di sistema aggiuntiva richiesta per eseguire gli indici specificati.

Indicizzazione EDM remota

Un indice EDM mappa i dati che si desidera proteggere al profilo di dati esatti. Il tipico flusso di lavoro EDM per creare l'indice EDM comporta il caricamento del file origine dati su Enforce Server, la creazione del profilo di dati esatti e l'indicizzazione dell'origine dati. Invece di caricare il file origine dati su Enforce Server per l'indicizzazione, è possibile indicizzare l'origine dati in locale e in modo sicuro con Remote EDM Indexer.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Ad esempio, se la copia del file origine dati riservato su Enforce Server presenta un potenziale problema di sicurezza o logistica, è possibile utilizzare Remote EDM Indexer per creare l'indice crittografico direttamente sull'host origine dati prima di spostare l'indice su Enforce Server. Se si esegue l'upgrade alla versione più recente di Symantec Data Loss Prevention, è possibile utilizzare Remote EDM Indexer per aggiornare gli indici EDM esistenti.

Vedere ["Informazioni su Remote EDM Indexer"](#) a pagina 540.

Vedere ["Informazioni su SQL Preindexer"](#) a pagina 540.

Remote EDM Indexer è uno strumento stand-alone che consente di indicizzare il file origine dati direttamente sull'host origine dati.

Vedere ["Requisiti di sistema per l'indicizzazione EDM remota"](#) a pagina 541.

Informazioni su Remote EDM Indexer

L'utilità Remote EDM Indexer converte un file origine dati in un indice EDM. È simile all'indicizzatore EDM locale utilizzato da Enforce Server. Tuttavia Remote EDM Indexer è progettato per l'utilizzo su un computer che non fa parte della configurazione del server Symantec Data Loss Prevention.

L'utilizzo di Remote EDM Indexer per indicizzare un'origine dati su un computer remoto presenta i vantaggi seguenti rispetto all'indicizzatore EDM su Enforce Server:

- Consente al proprietario dei dati, e non all'amministratore di Symantec Data Loss Prevention, di indicizzare i dati.
- Sposta il carico del sistema necessario per l'indicizzazione su un altro computer. La CPU e la RAM su Enforce Server sono riservate per altre attività.

Vedere ["Informazioni su SQL Preindexer"](#) a pagina 540.

Vedere ["Flusso di lavoro per l'indicizzazione EDM remota"](#) a pagina 541.

Informazioni su SQL Preindexer

L'utilità SQL Preindexer può essere utilizzata con Remote EDM Indexer per eseguire query SQL su database Oracle e inoltrare i dati risultati a Remote EDM Indexer per l'indicizzazione.

Vedere ["Requisiti di sistema per l'indicizzazione EDM remota"](#) a pagina 541.

L'utilità SQL Preindexer è installata nella directory `C:\Programmi\Symantec\Data Loss Prevention\Server Platform Common\Indexer\15.1\Protect\bin` durante l'installazione di Remote EDM Indexer. L'utilità SQL Preindexer genera direttamente un indice da un database Oracle SQL. SQL Preindexer elabora la query del database e la passa all'input standard dell'utilità Remote EDM Indexer.

Per utilizzare SQL Preindexer l'origine dati deve essere relativamente ottimizzata, poiché i dati dei risultati delle query vengono inoltrati direttamente a Remote EDM Indexer.

Vedere ["Informazioni su Remote EDM Indexer"](#) a pagina 540.

Requisiti di sistema per l'indicizzazione EDM remota

Remote EDM Indexer funziona nelle versioni dei sistemi operativi Windows e Linux supportate per i server Symantec Data Loss Prevention. Per ulteriori informazioni sul supporto dei sistemi operativi, consultare la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*.

SQL Preindexer supporta i database Oracle e richiede un'origine dati con dati in buono stato.

Vedere ["Informazioni su SQL Preindexer"](#) a pagina 540.

I requisiti di RAM per l'utilizzo di Remote EDM Indexer variano a seconda delle dimensioni dell'origine dati indicizzata e del numero di colonne multitoken presenti nell'origine dati.

Vedere ["Requisiti di memoria per EDM"](#) a pagina 532.

Flusso di lavoro per l'indicizzazione EDM remota

In questa sezione vengono illustrati i passaggi per indicizzare un file di dati su un computer remoto e utilizzare quindi l'indice in Symantec Data Loss Prevention.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Tabella 22-36 Passaggi per l'utilizzo di Remote EDM Indexer

Passaggio	Azione	Descrizione
Passaggio 1	Installare Remote EDM Indexer su un computer che non fa parte del sistema Symantec Data Loss Prevention.	Vedere "Informazioni sull'installazione e l'esecuzione delle utilità Remote EDM Indexer e SQL Preindexer" a pagina 542.
Passaggio 2	Creare un profilo di dati esatti in Enforce Server da utilizzare con Remote EDM Indexer.	In Enforce Server generare un modello di profilo EDM utilizzando l'estensione del nome di file *.edm e specificando il numero esatto di colonne da indicizzare. Vedere "Creazione del modello di un profilo EDM per l'indicizzazione remota" a pagina 543.
Passaggio 3	Copiare il file del profilo di dati esatti sul computer su cui risiede Remote EDM Indexer.	Scaricare il modello di profilo da Enforce Server e copiarlo sul computer host dell'origine dati remoto. Vedere "Download e copia del file di profilo EDM in un sistema remoto" a pagina 546.

Passaggio	Azione	Descrizione
Passaggio 4	Eseguire Remote EDM Indexer e creare i file di indice.	<p>Se si dispone di un file origine dati pulito, utilizzare <code>RemoteEDMIndexer</code> con le opzioni <code>-data</code>, <code>-profile</code> e <code>-result</code>.</p> <p>Se l'origine dati è un database Oracle, utilizzare <code>SqlPreindexer</code> e <code>RemoteEDMIndexer</code> per indicizzare l'origine dati direttamente con le credenziali <code>-alias</code> (host del database Oracle), <code>-username</code> e <code>-password</code>, e <code>-query_string</code> o <code>-query_path</code>.</p> <p>Vedere "Generazione remota di file indice" a pagina 546.</p>
Passaggio 5	Copiare i file di indice dal computer remoto su Enforce Server.	<p>Copiare i file <code>*.pdx</code> e <code>*.rdx</code> risultanti dal computer remoto sull'host di Enforce Server nel percorso <code>C:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\index</code>.</p> <p>Vedere "Copia e caricamento di file di indice remoti su Enforce Server" a pagina 549.</p>
Passaggio 6	Caricare i file di indice su Enforce Server.	<p>Aggiornare il profilo EDM caricando l'indice generato esternamente.</p> <p>Inviare il profilo per l'indicizzazione.</p> <p>Vedere "Copia e caricamento di file di indice remoti su Enforce Server" a pagina 549.</p>
Passaggio 7	Risolvere eventuali problemi che si verificano durante il processo di indicizzazione.	<p>Verificare che l'indicizzazione venga completata.</p> <p>Cercare <code>Code 2926</code> negli eventi di sistema ("Profilo dati esatti creato" e "Origine dati salvata").</p> <p>I file <code>ExternalDataSource.<nome>.rdx</code> e <code>*.pdx</code> vengono rimossi dalla directory dell'indice e sostituiti dal file <code>DataSource.<ID profilo>.<versione>.rdxver</code>.</p> <p>Vedere "Risoluzione dei problemi dell'indicizzazione remota" a pagina 554.</p>
Passaggio 8	Creare una politica con la condizione EDM.	<p>Per definire la condizione EDM, è necessario consultare i dati della colonna.</p> <p>Vedere "Configurazione della condizione di politica Contenuto corrispondente a profilo dati esatti" a pagina 503.</p>

Informazioni sull'installazione e l'esecuzione delle utilità Remote EDM Indexer e SQL Preindexer

Remote EDM Indexer viene installato con lo stesso programma di installazione usato dagli altri componenti di Symantec Data Loss Prevention. SQL Preindexer viene installato automaticamente quando si installa Remote EDM Indexer. Entrambe le utilità sono eseguite dalla riga di comando e sono archiviate in

`opt/Symantec/DataLossPrevention/Indexer/15.1/Protect/bin`.

Vedere ["Generazione remota di file indice"](#) a pagina 546.

Per installare Remote EDM Indexer, copiare il file `ProtectInstaller.exe` (Windows) o il file `ProtectInstaller.sh` (Linux) nel computer remoto in cui si trovano i file da indicizzare.

Quando si esegue il programma di installazione scegliere solo "Indexer" e nessun altro componente. Il programma di installazione Linux per Remote EDM Indexer si esegue dalla console dei comandi.

Sia Remote EDM Indexer che SQL Preindexer sono eseguibili dalla riga di comando. In un sistema Linux impostare gli utenti sull'utente "protect" prima di eseguire SQL Preindexer. (Il programma di installazione crea l'utente "protect".)

Vedere ["Generazione remota di file indice"](#) a pagina 546.

Nota: Per le installazioni di Data Loss Prevention a due e tre livelli, evitare di installare Remote EDM Indexer nello stesso sistema che include un server di rilevamento. Per ulteriori informazioni, consultare il *Manuale di installazione di Symantec Data Loss Prevention*.

Creazione del modello di un profilo EDM per l'indicizzazione remota

Remote EDM Indexer utilizza un profilo di dati esatti quando viene eseguito per assicurarsi che i dati siano formattati correttamente. È necessario creare il profilo di dati esatti prima di utilizzare Remote EDM Indexer. Il profilo è un modello che descrive le colonne utilizzate per organizzare i dati. Il profilo non deve contenere alcun dato. Dopo avere creato il profilo, copiarlo sul computer che esegue Remote EDM Indexer.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Per creare un profilo EDM per l'indicizzazione remota

- 1 Nella console di amministrazione di Enforce Server accedere alla schermata **Gestisci > Profili dati > Dati esatti**.
- 2 Fare clic su **Aggiungi profilo dati esatti**.
- 3 Nel campo **Nome** immettere un nome per il profilo.

- 4 Nel campo **Origine dati** selezionare **Usa questo nome file** e immettere il nome del file di indice da creare con l'estensione * .edm.

È necessario selezionare questa opzione perché per ora si sta solo creando il modello di profilo. Successivamente si indicizzerà il profilo con l'origine dati mediante Remote EDM Indexer. Immettere il nome di file dell'origine dati che si intende creare per l'indicizzazione EDM remota. Assicurarsi di assegnare al file origine dati il nome esatto immesso qui.

Vedere ["Caricamento di file origine dati esatti in Enforce Server"](#) a pagina 490.

Dopo avere copiato di nuovo su Enforce Server l'indice remoto generato, utilizzare l'opzione **Carica indice generato esternamente** per caricare l'indice remoto nel modello di profilo.

Vedere ["Copia e caricamento di file di indice remoti su Enforce Server"](#) a pagina 549.

- 5 Nella casella di testo **Numero di colonne** specificare il numero di colonne nell'origine dati da indicizzare.

Ai fini dell'indicizzazione EDM remota è necessario specificare il **numero di colonne** esatto che l'indice deve avere. Assicurarsi di includere il numero di colonne esatto specificato qui nel file origine dati.

Vedere ["Caricamento di file origine dati esatti in Enforce Server"](#) a pagina 490.

- 6 Se la prima riga dell'origine dati contiene i nomi delle colonne, selezionare l'opzione **Leggi prima riga come nomi di colonna**.

- 7 Nella casella di testo **Soglia di errore** immettere la percentuale massima di righe che possono contenere errori.

Se, durante l'indicizzazione dell'origine dati, il numero di righe con errori supera la percentuale specificata qui, l'indicizzazione non riesce.

- 8 Nel campo **Carattere separatore colonne** selezionare il tipo di carattere utilizzato nell'origine dati per separare le colonne di dati.

- 9 Nel campo **Codifica file** selezionare la codifica dei caratteri utilizzata nell'origine dati.

Se si utilizzano caratteri latini, selezionare l'opzione ISO-8859-1. Per le lingue asiatiche orientali utilizzare le opzioni UTF-8 o UTF-16.

- 10 Fare clic su **Avanti** per mappare le intestazioni di colonna dell'origine dati al profilo.

- 11 Nella sezione **Mapping campi** mappare **Campo Origine dati** a **Campo di sistema** per ogni colonna selezionando il nome della colonna dall'elenco a discesa **Campo di sistema**.

Campo Origine dati elenca il numero di colonne specificato nella schermata precedente. **Campo di sistema** contiene un elenco di intestazioni di colonna standard. Se una delle intestazioni di colonna nell'origine dati corrisponde alle scelte disponibili nell'elenco **Campo di sistema**, mappare ciascuna intestazione di conseguenza. Assicurarsi di cercare la corrispondenza tra la selezione nella colonna **Campo di sistema** e la colonna numerata corrispondente in **Campo Origine dati**.

Ad esempio, per un'origine dati nel cui profilo si sono specificate tre colonne, la configurazione del mapping può essere:

Campo Origine dati	Campo di sistema
Colonna 1	Nome
Colonna 2	Cognome
Colonna 3	Numero di codice fiscale

- 12 Se **Campo Origine dati** non viene mappato a un valore di intestazione nelle opzioni disponibili nella colonna **Campo di sistema**, fare clic sul collegamento **Visualizzazione avanzata**.

In **Visualizzazione avanzata**, il sistema visualizza una colonna **Nome personalizzato** accanto alla colonna **Campo di sistema**.

Immettere il nome di colonna corretto nella casella di testo che corrisponde alla colonna appropriata nell'origine dati.

Facoltativamente è possibile specificare il tipo di dati per il **nome personalizzato** immesso. A questo scopo selezionare il tipo di dati dall'elenco a discesa **Tipo**. Questi tipi di dati sono definiti dal sistema. Fare clic sul collegamento della **descrizione** accanto al nome **Tipo** per i dettagli di ciascun tipo di dati definito dal sistema.

- 13 Se si intende utilizzare il profilo di dati esatti per implementare un modello di politica che contiene una o più regole EDM, è possibile convalidare i mapping del profilo per il modello. A questo scopo selezionare il modello dall'elenco a discesa **Verificare il mapping sulla base del modello di politica** e fare clic su **Controlla ora**. Il sistema indica eventuali campi non mappati richiesti dal modello.
- 14 Non selezionare alcuna opzione di **Indicizzazione** disponibile in questa schermata perché si intende eseguire l'indicizzazione in remoto.
- 15 Fare clic su **Fine** per completare il processo di creazione del profilo.

Download e copia del file di profilo EDM in un sistema remoto

Scaricare e copiare il profilo EDM nel sistema remoto

- 1 Configurare un profilo dati esatti.
Vedere ["Creazione del modello di un profilo EDM per l'indicizzazione remota"](#) a pagina 543.
- 2 Scaricare il profilo EDM selezionando il collegamento **scarica profilo** nella schermata **Gestisci > Profili dati > Dati esatti**.
Il sistema richiede di salvare il profilo EDM come file. L'estensione del file è *.edm.
- 3 Salvare il file.
Se il computer host origine dati nel quale si desidera eseguire Remote EDM Indexer è disponibile nella stessa subnet dell'Enforce Server è possibile andare a tale computer e selezionarlo come destinazione. In caso contrario copiare manualmente il profilo nel sistema remoto.
- 4 Utilizzare il profilo per indicizzare l'origine dati mediante Remote EDM Indexer.
Vedere ["Generazione remota di file indice"](#) a pagina 546.

Generazione remota di file indice

L'utilità della riga di comando Remote EDM Indexer consente di generare un indice EDM da importare in Enforce Server. È possibile usare Remote EDM Indexer per indicizzare il file origine dati che è stato generato e ottimizzato. Oppure è possibile inviare l'output da SQL Preindexer all'input standard di Remote EDM Indexer. SQL Preindexer richiede un'origine dati database di Oracle e dati ottimizzati.

Al completamento del processo di indicizzazione, Remote EDM Indexer genera vari file nella directory dei risultati specificata. Tali file sono denominati come il file di dati indicizzato: uno ha l'estensione .pdx e l'altro l'estensione .rdx. Il sistema genera 12 file .rdx denominati

ExternalDataSource.<DataSourceName>.rdx.0 -

ExternalDataSource.<DataSourceName>.rdx.11.

Tabella 22-37 Opzioni per la generazione di indici EDM remoti

Caso di utilizzo	Descrizione	Osservazioni
Remote EDM Indexer con file origine dati.	Specificare il file origine dati, il profilo EDM e la directory di output.	Utilizzare con un file origine dati ottimizzato; utilizzare per l'aggiornamento a DLP 15.1. Vedere "Esempi di indicizzazione remota mediante il file origine dati" a pagina 547.

Caso di utilizzo	Descrizione	Osservazioni
Remote EDM Indexer con SQL Preindexer	Query nel database e invio dell'output a Remote EDM Indexer.	Richiede un database Oracle e dati ottimizzati. Vedere "Esempi di indicizzazione remota con SQL Preindexer" a pagina 548.

Esempi di indicizzazione remota mediante il file origine dati

Per utilizzare Remote EDM Indexer per indicizzare un file di origine dati flat generato e ottimizzato, specificare il nome e il percorso del file origine dati locale (`-data`), il nome e il percorso dei file del profilo EDM locale (`-profile`) e la directory di output dei file indice generati (`-result`).

La sintassi per l'utilizzo di Remote EDM Indexer per generare un indice da un file di origine dati tabulare generato e ottimizzato è la seguente:

```
RemoteEDMIndexer -data=<local data source filename and path>  
-profile=<local *.edm profile file name and path>  
-result=<local output directory for *.rdx and *pdx index files>
```

Ad esempio:

```
RemoteEDMIndexer -data=C:\EDMIndexDirectory\CustomerData.dat  
-profile=C:\EDMIndexDirectory\RemoteEDMProfile.edm  
-result=C:\EDMIndexDirectory\
```

Questo comando genera un indice EDM utilizzando il file di origine dati locale tabulare `CustomerData.dat` e il file locale `RemoteEDMProfile.edm` generato e copiato da Enforce Server all'host remoto, dove `\EDMIndexDirectory` è la directory per il posizionamento dei file indice generati.

Quando la generazione degli indici riesce, l'utilità visualizza il messaggio "Successfully created index" (Indice creato correttamente) come ultima riga di output.

Inoltre, i seguenti file di indice vengono creati e posizionati nella directory `-result`:

- `ExternalDataSource.CustomerData.pdx`
- `ExternalDataSource.CustomerData.rdx`

Dodici file denominati `ExternalDataSource.<DataSourceName>.rdx.0` - `ExternalDataSource.<DataSourceName>.rdx.11` vengono generati in ogni caso. Copiare questi file in Enforce Server e aggiornare il profilo EDM utilizzando l'indice remoto.

Vedere ["Opzioni di comando di Remote EDM Indexer"](#) a pagina 552.

Esempi di indicizzazione remota con SQL Preindexer

Se l'origine dati è un database Oracle con dati ottimizzati, è possibile indicizzare direttamente l'origine dati con SQL Preindexer mediante Remote EDM Indexer.

La sintassi è la seguente:

```
SqlPreindexer -alias=<oracle connect string: //host:port/SID>  
-username=<DB user> -password=<DB password> -query=<sql to run> |  
RemoteEDMIndexer -profile=<*.edm profile file name and path>  
-result=<output directory for index files>
```

Ad esempio:

```
SqlPreindexer -alias=@//myhost:1521/orcl -username=scott -password=tiger  
-query="SELECT name, salary FROM employee" |  
RemoteEDMIndexer -profile=C:\ExportEDMProfile.edm -result=C:\EDMIndexDirectory\
```

Con questo comando, l'utilità SQL Preindexer si collega al database Oracle ed esegue la query SQL per recuperare nomi e dati di retribuzione dalla tabella dei dipendenti. SQL Preindexer restituisce il risultato della query a stdout (la console comandi). La query SQL deve essere racchiusa tra virgolette singole. Il comando Remote EDM Indexer esegue l'utilità e legge i risultati della query dalla console stdin. Remote EDM Indexer indicizza i dati utilizzando il profilo `ExportEDMProfile.edm` come specificato dal nome file e dal percorso file locale del profilo.

Quando la generazione degli indici riesce, l'utilità visualizza il messaggio "Successfully created index" (Indice creato correttamente) come ultima riga di output.

Inoltre l'utilità posiziona i seguenti file di indice generati nella directory `-result EDMIndexDirectory`:

- `ExternalDataSource.CustomerData.pdx`
- `ExternalDataSource.CustomerData.rdx`

Ecco un altro esempio dell'utilizzo dei comandi SQL Preindexer e Remote EDM Indexer:

```
SqlPreindexer -alias=@//localhost:1521/CUST -username=cust_user -password=cust_pword  
-query="SELECT account_id, amount_owed, available_credit FROM customer_account" -verbose |  
RemoteEDMIndexer -profile=C:\EDMIndexDirectory\CustomerData.edm  
-result=C:\EDMIndexDirectory\ -verbose
```

Qui il comando SQL Preindexer esegue una query nella tabella `CUST.customer_account` del database per ottenere i record `account_id`, `amount_owed` e `available_credit`. Il risultato viene inoltrato a Remote EDM Indexer, che genera i file di indice sulla base del profilo `CustomerData.edm`. L'opzione `-verbose` è utilizzata per la risoluzione dei problemi.

Come alternativa alla stringa SQL `-query` è possibile utilizzare l'opzione `-query_path` e specificare il percorso e il nome file della query SQL (*.sql). Se non si specifica una query o un percorso la query viene effettuata sull'intero database.

```
SqlPreindexer -alias=@//localhost:1521/cust -username=cust_user -password=cust_pwr  
-query_path=C:\EDMIndexDirectory\QueryCust.sql -verbose |  
RemoteEDMIndexer -profile=C:\EDMIndexDirectory\CustomerData.edm  
-result=C:\EDMIndexDirectory\ -verbose
```

Vedere ["Opzioni di comando di SQL Preindexer"](#) a pagina 550.

Copia e caricamento di file di indice remoti su Enforce Server

I file riportati di seguito vengono creati nella directory `-result` quando si indicizza un'origine dati in remoto:

- ExternalDataSource.<DataSourceName>.pdx
- ExternalDataSource.<NomeOrigineDati>.rdx.0 -
ExternalDataSource.<NomeOrigineDati>.rdx.11

Dopo avere creato i file di indice su un computer remoto, è necessario copiarli su Enforce Server, caricarli nel profilo EDM remoto creato in precedenza e indicizzarli.

Vedere ["Creazione del modello di un profilo EDM per l'indicizzazione remota"](#) a pagina 543.

Per copiare e caricare i file su Enforce Server

- 1 Selezionare la directory in cui sono stati generati i file di indice. (Questa directory è quella specificata nell'opzione `-result`.)
- 2 Copiare tutti i file di indice con le estensioni `.pdx` e `.rdx` nella directory di indice su Enforce Server. Questa directory si trova in `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\Index (Windows)` o `/var/Symantec/DataLossPrevention/Enforce Server/15.1/index (Linux)`.
- 3 Dalla console di amministrazione di Enforce Server accedere alla schermata **Gestisci > Politiche > Dati esatti**.

In questa schermata sono elencati tutti i profili di dati esatti del sistema.
- 4 Fare clic sul nome del profilo di dati esatti utilizzato con Remote EDM Indexer.
- 5 Per caricare i nuovi file di indice, accedere alla sezione Origine dati del profilo di dati esatti e selezionare **Carica indice generato esternamente**.

6 Nella sezione Indicizzazione selezionare **Invia processo di indicizzazione al salvataggio**.

In alternativa all'indicizzazione immediata al salvataggio considerare la possibilità di pianificare un processo sul computer remoto per eseguire regolarmente Remote EDM Indexer. Il processo deve inoltre copiare i file generati nella directory di indice su Enforce Server. È quindi possibile pianificare il caricamento dei file di indice aggiornati su Enforce Server dal profilo. A questo scopo selezionare **Carica indice generato esternamente e Invia processo di indicizzazione secondo pianificazione** e configurare una pianificazione di indicizzazione.

Vedere ["Utilizzo dell'indicizzazione pianificata per automatizzare gli aggiornamenti del profilo"](#) a pagina 564.

7 Fare clic su **Salva**.

Opzioni di comando di SQL Preindexer

Al momento dell'installazione, l'utilità SQL Preindexer è disponibile in

`C:\Programmi\Symantec\Data Loss Prevention\Indexer\15.1\Protect\bin` (Windows)
`e /Symantec/DataLossPrevention/Indexer/15.1/Protect/bin` (Linux).

SQL Preindexer fornisce un'interfaccia della riga di comando. La sintassi per l'esecuzione dell'utilità è la seguente:

```
SqlPreindexer -alias=<@//oracle_host:port/SID> -username=<DB_user> [options]
```

Si tenga presente quanto segue sugli argomenti:

- SQL Preindexer richiede gli argomenti `-alias` e `-username`.
- Se si omette l'opzione `-password`, all'utente viene richiesto di immetterla.
- Se si utilizza l'opzione `-query`, la stringa della query SQL deve essere racchiusa tra virgolette.
- Se si omette l'opzione `-query`, l'utilità indicizza l'intero database.
- Per eseguire una query con caratteri jolly, utilizzare l'opzione `-query_path`. SQL Preindexer non supporta l'utilizzo di caratteri jolly dalla riga di comando con l'opzione `-query`. Ad esempio, "select * from CUST_DATA" non funziona con `-query`. È necessario eseguire una query in ciascun campo di colonna: "select cust_ID, cust_Name, cust_SSN from CUST_DATE". La query "select * from CUST_DATA" funziona con il comando `-query_path`.

Vedere ["Esempi di indicizzazione remota con SQL Preindexer"](#) a pagina 548.

La [Tabella 22-38](#) elenca le opzioni di comando per SQL Preindexer.

Tabella 22-38 Opzioni di comando di SQL Preindexer

Opzione	Riepilogo	Descrizione
-alias	Stringa di connessione del database Oracle Obbligatoria	Specifica l'alias del database utilizzato per la connessione al database nel formato seguente: <i>@//oracle_db_host:port/SID</i> Ad esempio: -alias=@//myhost:1521/ORCL -alias=@//localhost:1521/CUST
-driver	Classe di driver Oracle JDBC	Specifica la classe del driver JDBC, ad esempio: <i>driver.oracle.jdbc.DriverOracle.</i>
-encoding	Codifica dei caratteri (iso-8859-1)	Specifica la codifica dei caratteri dei dati da indicizzare. L'impostazione predefinita è iso-8859-1. I dati con caratteri non inglesi devono utilizzare UTF-8 o UTF-16.
-password	Password del database Oracle	Specifica la password per il database. Se questa opzione non è specificata, la password viene letta da stdin.
-query	Query SQL	Questa opzione specifica la query SQL da eseguire. L'istruzione deve essere racchiusa tra virgolette. Se si omette l'opzione -query, l'utilità indicizza l'intero database.
-query_path	Script SQL	Specifica il nome del file e il percorso locale che contiene una query SQL da eseguire. Deve essere un percorso completo. Questa opzione può essere utilizzata in alternativa all'opzione -query quando la query è un'istruzione SQL lunga.
-separator	Separatore di colonna di output (tabulazione)	Specifica se il separatore di colonna di output è una virgola, una barra verticale o una tabulazione. Il separatore predefinito è una tabulazione. Per specificare un separatore virgola o barra verticale, racchiudere il carattere del separatore tra virgolette: " , " o " ".
-subprotocol	Thin driver Oracle	Specifica il sottoprotocollo della stringa di connessione JDBC (ad esempio, oracle:thin).
-username	Utente del database Oracle Obbligatoria	Specifica il nome dell'utente del database.

Opzione	Riepilogo	Descrizione
-verbose	Stampa l'output dettagliato per il debug.	Visualizza un riepilogo statistico dell'operazione completata. Vedere "Risoluzione dei problemi per gli errori di preindicizzazione" a pagina 553.

Opzioni di comando di Remote EDM Indexer

Al momento dell'installazione, l'utilità Remote EDM Indexer è disponibile in
\\Programmi\\Symantec\\Data Loss Prevention\\Indexer\\15.1\\Protect\\bin (Windows) e
opt/Symantec/DataLossPrevention/Indexer/15.1/Protect/bin (Linux).

In un sistema Linux impostare gli utenti sull'utente "SymantecDLP" prima di eseguire Remote EDM Indexer. (Il programma di installazione crea l'utente "SymantecDLP".)

Remote EDM Indexer fornisce un'interfaccia della riga di comando. La sintassi per l'esecuzione dell'utilità è la seguente:

```
RemoteEDMIndexer -profile=<file *.edm> -result=<out_dir> [options]
```

Si tenga presente quanto segue sulla sintassi:

- Remote EDM Indexer richiede le istruzioni `-profile` e `-result`.
- Se si utilizza un file origine dati flat, è necessario specificare il nome del file e il percorso locale con l'opzione `-data`.
- L'opzione `-data` viene omessa quando si utilizza SQL Preindexer per collegare a catena i dati a Remote EDM Indexer.

Vedere ["Esempi di indicizzazione remota mediante il file origine dati"](#) a pagina 547.

La [Tabella 22-39](#) descrive le opzioni di comando per Remote EDM Indexer.

Tabella 22-39 Opzioni di comando di Remote EDM Indexer

Opzione	Riepilogo	Descrizione
-data	Origine dati da indicizzare (stdin) Obbligatoria se si utilizza un file di testo tabulare	Specifica l'origine dati da indicizzare. Se questa opzione non è specificata, l'utilità legge i dati da stdin. Obbligatoria se si utilizza il file origine dati e non SQL Preindexer.
-encoding	Codifica dei caratteri dei dati da indicizzare (ISO-8859-1)	Specifica la codifica caratteri dei dati da indicizzare. L'impostazione predefinita è ISO-8859-1. Utilizzare UTF-8 o UTF-16 se i dati contengono caratteri non inglesi.

Opzione	Riepilogo	Descrizione
<code>-ignore_date</code>	Ignora la data di scadenza del profilo EDM	Sovrascrive la data di scadenza del profilo dati esatti se il profilo è scaduto. Per impostazione predefinita, un profilo dati esatti scade dopo 30 giorni.
<code>-profile</code>	File contenente il profilo EDM Obbligatorio	Specifica il profilo dati esatti da utilizzare. Questo profilo è quello che viene selezionato facendo clic sul "collegamento di download" nello schermo Dati esatti della console di gestione di Enforce Server
<code>-result</code>	Directory nella quale inserire gli indici risultanti Obbligatorio	Specifica la directory in cui sono generati i file indice.
<code>-verbose</code>	Mostra output dettagliato	Visualizza un riepilogo statistico dell'operazione di indicizzazione quando l'indice è completo. Vedere "Risoluzione dei problemi per gli errori di preindicizzazione" a pagina 553.

Risoluzione dei problemi per gli errori di preindicizzazione

Se si riceve un errore indicante che SQL Preindexer non è stato in grado di eseguire la query o non è riuscito a preparare l'indicizzazione, verificare che la stringa `-query` sia racchiusa tra virgolette. È possibile provare la stringa `-query` eseguendo solo il comando SQL Preindexer. Se il comando è corretto i dati estratti dal database vengono visualizzati nella console come `stdout`.

È possibile che si riscontrino errori quando si indicizzano volumi di dati considerevoli. Spesso l'insieme di dati contiene un record dei dati incompleto, non coerente o inesatto. Spesso le righe di dati che contengono più colonne del previsto o dati colonna errati non vengono indicizzate correttamente e non sono riconosciute.

SQL Preindexer può essere configurato per fornire un riepilogo di informazioni sull'operazione di indicizzazione una volta che questa viene completata. A tal fine specificare l'opzione `verbose` quando si esegue SQL Preindexer.

Per vedere le righe di dati che Remote EDM Indexer non ha indicizzato, adattare la configurazione nel file `Indexer.properties` utilizzando la seguente procedura.

Per registrare le righe di dati che non sono state indicizzate

- 1 Individuare il file `Indexer.properties` in `\Programmi\Symantec\Data Loss Prevention\Indexer\15.1\Protect\config\Indexer.properties` (Windows) o `/Symantec/DataLossPrevention/Indexer/15.1/Protect/config/Indexer.properties` (Linux).
- 2 Aprire il file in un editor di testo.
- 3 Individuare la proprietà `create_error_file` e cambiare l'impostazione da "false" a "true".
- 4 Salvare e chiudere il file `Indexer.properties`.

Remote EDM Indexer registra gli errori in un file con lo stesso nome del file di dati sottoposto a indicizzazione e con il suffisso `.err`.

Le righe di dati elencate nel file di errori non sono crittografate. Proteggere il file di errori per evitare rischi per la sicurezza derivanti dalla divulgazione di dati.

Vedere ["Informazioni su SQL Preindexer"](#) a pagina 540.

Risoluzione dei problemi dell'indicizzazione remota

Remote EDM Indexer indica in un messaggio se l'operazione di indicizzazione è riuscita. Se Remote EDM Indexer crea l'indice, la console visualizza il messaggio "Successfully created index" (Indice creato correttamente) come ultima riga di output. Inoltre vengono creati file `*.pdx` e `*.rdx` nella directory `-result`.

Il risultato dipende dalla soglia di errore specificata nel profilo EDM. Se la percentuale di errore è inferiore alla soglia, l'operazione viene completata correttamente. Informazioni dettagliate sull'operazione di indicizzazione sono disponibili con l'opzione `-verbose`.

Vedere ["Opzioni di comando di Remote EDM Indexer"](#) a pagina 552.

Se la generazione dell'indice non riesce, tentare con questi suggerimenti di risoluzione dei problemi:

Tabella 22-40 Suggerimenti per la risoluzione dei problemi di Remote Indexer

Errore	Sintomo	Descrizione
File indici non generati	Utilizzare l'opzione <code>-verbose</code> nel comando per mostrare il messaggio di errore.	L'opzione verbose in Remote EDM Indexer offre un riepilogo statistico di informazioni sull'operazione di indicizzazione dopo il completamento. Le informazioni includono il numero di errori e la posizione in cui si sono verificati.

Errore	Sintomo	Descrizione
"Impossibile creare l'indice" "Impossibile calcolare l'indice" "Impossibile generare l'indice"	Verificare i nomi del percorso e del file.	Verificare di aver incluso il percorso completo e il nome file esatto per i file <code>-data</code> e <code>-profile (*.edm)</code> . I percorsi devono essere locali nell'host.
"La destinazione non è una directory"	Il percorso della directory non è corretto.	Verificare di aver immesso correttamente il percorso completo della directory di destinazione per l'argomento <code>-result</code> obbligatorio.
File <code>*.idx</code> invece di un file <code>*.rdx</code>	Non è stato utilizzato l'argomento <code>-data</code>	L'opzione <code>-data</code> è obbligatoria se si utilizza un file origine dati e non SQL Preindexer. In altri termini l'argomento <code>-data</code> può essere ignorato solo quando si utilizza SQL Preindexer. Se si esegue Remote EDM Indexer senza l'opzione <code>-data</code> e nessuna query SQL Preindexer, si ottiene un file <code>*.idx</code> e un file <code>*.rdx</code> non utilizzabili per l'indice EDM. Eseguire di nuovo l'indice utilizzando l'opzione <code>-data</code> o un'opzione <code>-query</code> o <code>-query-path</code> di SQL Preindexer.

Inoltre è possibile che si riscontrino errori quando si indicizzano volumi di dati considerevoli. Spesso l'insieme di dati contiene un record dei dati incompleto, non coerente o formattato in modo errato. Spesso le righe di dati che contengono più colonne del previsto o tipi di dati errati non vengono indicizzate correttamente e non sono riconosciute durante l'indicizzazione. Le righe di dati con errori non possono essere indicizzate fino a quando non si correggono gli errori e non si ripete l'esecuzione di Remote EDM Indexer. Symantec dispone di due metodi per ottenere informazioni sui possibili errori e sul completamento dell'operazione di indicizzazione.

Per vedere le righe di dati che Remote EDM Indexer non ha indicizzato, modificare il file `Indexer.properties`.

Per modificare il file `Indexer.properties` e visualizzare gli errori di indicizzazione remota

- 1 Individuare il file `Indexer.properties` in `\Programmi\Symantec\Data Loss Prevention\Indexer\15.1\Protect\config\Indexer.properties` (Windows) o `/opt/Symantec/DataLossPrevention/Indexer/15.1/Protect/config/Indexer.properties` (Linux).
- 2 Aprire il file in un editor di testo per modificarlo.

- 3 Individuare il parametro `create_error_file` e cambiare l'impostazione da "false" a "true".
- 4 Salvare e chiudere il file `Indexer.properties`.

Remote EDM Indexer registra gli errori in un file con lo stesso nome del file di dati sottoposto a indicizzazione e con l'estensione `.err`. Questo file di errori è creato nella directory dei registri.

Le righe di dati elencate nel file di errori non sono crittografate. Crittografare il file di errori per evitare rischi per la sicurezza derivanti dalla divulgazione di dati.

Installazione di Remote EDM Indexer

L'indicizzatore IDM remoto viene installato su uno o più sistemi dove sono memorizzati i file riservati che si desidera indicizzare.

È possibile installare l'indicizzatore EDM remoto su tutte le piattaforme Windows e Linux supportate. Per ulteriori dettagli, consultare la *Guida ai requisiti di sistema di Symantec Data Loss Prevention*.

Installazione di Remote EDM Indexer

- 1 Copiare i file `Indexers.msi` (Windows) o `SymantecDLPIndexers.zip` (Linux) nel sistema remoto.
- 2 Eseguire l'applicazione `Indexers.msi` (Windows) o `SymantecDLPIndexers.zip` (Linux). Per ulteriori informazioni sull'installazione, vedere la *Guida all'installazione di Symantec Data Loss Prevention* per la piattaforma in uso.

Vedere [Tabella 22-41](#) a pagina 556.

- 3 Selezionare l'opzione Indicizzatore e deselezionare le altre opzioni.

Nota: L'Indicizzatore include sia l'Indicizzatore IDM remoto e l'Indicizzatore EDM remoto.

- 4 Verificare l'installazione dell'indicizzatore EDM remoto.

Tabella 22-41 Edizioni dell'indicizzatore EDM remoto

Piattaforma	Edizione	Percorso file	Eseguibile
Linux	CLI	/opt/Symantec/DataLossPrevention/Indexers/15.1/Protect/bin/	RemoteEDMIndexer
Windows	CLI	\Symantec\Data Loss Prevention/Indexers\15.1\Protect\bin\	RemoteEDMIndexer.exe

Best practice per l'utilizzo dell'EDM

L'EDM è la forma di rilevamento più accurata, nonché la più complessa da configurare e mantenere. Per assicurarsi che le politiche EDM siano le più accurate possibile, considerare le raccomandazioni riportate in questa sezione quando si implementano i profili e le politiche EDM.

Nella tabella seguente viene fornito un riepilogo della considerazioni sulle politiche EDM esaminate in questo capitolo, con collegamenti a singoli argomenti per ulteriori informazioni.

Tabella 22-42 Riepilogo delle best practice EDM

Best practice	Descrizione
Assicurarsi che il file origine dati contenga almeno una colonna di dati univoci.	Vedere "Verifica della presenza di almeno una colonna di dati univoci nell'origine dati" a pagina 558.
Eliminare le righe duplicate e le colonne vuote prima di eseguire l'indicizzazione.	Vedere "Eliminazione di colonne vuote e righe duplicate dal file origine dati" a pagina 559.
Per ridurre i falsi positivi, evitare i singoli caratteri, le virgolette, le abbreviazioni, i campi numerici con meno di 5 cifre e le date.	Vedere "Rimozione di tipi di carattere ambigui dal file origine dati" a pagina 560.
Esaminare l'indicizzazione multitoken e pulire in base alle esigenze.	Vedere "Funzionamento della corrispondenza di celle multitoken" a pagina 560.
Utilizzare la barra verticale () per delimitare le colonne nell'origine dati.	Vedere "Mancato utilizzo del delimitatore virgola se l'origine dati ha campi numerici" a pagina 561.
Esaminare un file origine dati pulito di esempio.	Vedere "Assicurarsi che l'origine dati sia pronta per l'indicizzazione" a pagina 562.
Mappare la colonna origine dati ai campi di sistema per sfruttare la convalida durante l'indicizzazione.	Vedere "Mappaggio delle colonne origine dati ai campi di sistema per utilizzare la convalida" a pagina 561.
Quando possibile, sfruttare i modelli di politica EDM.	Vedere "Sfruttamento dei modelli di politica EDM quando possibile" a pagina 562.
Includere le intestazioni di colonna come prima riga del file origine dati.	Vedere "Inclusione delle intestazioni di colonna come prima riga del file origine dati" a pagina 563.
Verificare gli avvisi di sistema per ottimizzare i profili di dati esatti.	Vedere "Verifica degli avvisi di sistema per ottimizzare la precisione del profilo" a pagina 563.
Utilizzare parole non significative per escludere le parole comuni dalla corrispondenza.	Vedere "Utilizzo di parole non significative per escludere le parole comuni dal rilevamento" a pagina 563.
Automatizzare gli aggiornamenti del profilo con l'indicizzazione pianificata.	Vedere "Utilizzo dell'indicizzazione pianificata per automatizzare gli aggiornamenti del profilo" a pagina 564.

Best practice	Descrizione
Cercare la corrispondenza con due o tre colonne in una regola EDM.	Vedere "Corrispondenza con 3 colonne in una condizione EDM per aumentare la precisione di rilevamento" a pagina 565.
Sfruttare le tuple di eccezione per evitare falsi positivi.	Vedere "Sfruttamento delle tuple di eccezione per evitare i falsi positivi" a pagina 566.
Utilizzare una clausola where per individuare i record che soddisfano criteri specifici.	Vedere "Utilizzare una clausola WHERE per individuare i record che soddisfano criteri specifici" a pagina 566.
Utilizzare il campo Corrispondenze minime per ottimizzare le regole EDM.	Vedere "Utilizzo del campo Corrispondenze minime per ottimizzare le regole EDM" a pagina 566.
Considerare la possibilità di utilizzare gli identificatori dati in combinazione con le regole EDM.	Vedere "Combinazione tra identificatori dati e regole EDM per limitare l'impatto del rilevamento in due fasi" a pagina 567.
Includere un campo per l'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo.	Vedere "Inclusione di un campo per l'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo" a pagina 567.
Utilizzo della DGM con profilo per il rilevamento di identità di Network Prevent for Web	Vedere "Utilizzo della DGM con profilo per il rilevamento di identità di Network Prevent for Web" a pagina 567.

Verifica della presenza di almeno una colonna di dati univoci nell'origine dati

L'EDM consente di rilevare le combinazioni di campi di dati globalmente univoci. L'indice EDM deve includere almeno una colonna di dati che contenga un valore univoco per ciascun record nella riga. Diversamente dalla provincia, dal CAP o dai nomi, i dati della colonna, ad esempio il numero di conto, il numero di codice fiscale e il numero di carta di credito sono inerentemente univoci. Se non si include almeno una colonna di dati univoci nell'indice, il profilo EDM non rileva in modo preciso i dati che si desidera proteggere.

Un campo di colonna univoco è una colonna che contiene prevalentemente valori univoci. È possibile avere valori duplicati, ma non in numero superiore a quello impostato in `term_commonority_threshold`. Il valore predefinito per questa impostazione è 10.

La [Tabella 22-43](#) descrive i vari tipi di dati univoci da includere negli indici EDM, nonché i campi che non sono univoci. È possibile includere campi non univoci negli indici EDM a condizione che si disponga di almeno un campo di colonna univoco.

Tabella 22-43 Esempi di dati univoci per le politiche EDM

Dati univoci per EDM	Dati non univoci
<p>Solitamente i campi di dati riportati di seguito sono univoci:</p> <ul style="list-style-type: none"> ■ Numero di conto ■ Numero di carta di credito ■ Numero di telefono ■ Indirizzo e-mail ■ Numero di codice fiscale ■ Codice di identificazione del contribuente ■ Numero di patente di guida ■ Numero dipendente ■ Numero di previdenza sociale 	<p>I campi di dati riportati di seguito non sono univoci:</p> <ul style="list-style-type: none"> ■ Nome ■ Cognome ■ Città ■ Provincia ■ CAP ■ Password ■ Numero PIN

Eliminazione di colonne vuote e righe duplicate dal file origine dati

Il file origine dati deve essere ottimizzato per quanto possibile prima della creazione dell'indice EDM. In caso contrario il profilo risultante potrebbe creare falsi positivi.

Quando si crea il file origine dati, evitare di includere celle o colonne vuote. Le colonne o i campi vuoti vengono conteggiati come errori quando si genera il profilo EDM. Un errore dell'origine dati è una cella vuota o una cella con il tipo di dati errato (ad esempio un nome che compare in una colonna dei numeri di telefono). La Soglia di errore è la percentuale massima di righe che possono contenere errori prima dell'arresto dell'indicizzazione. Se gli errori superano la soglia percentuale di errori per il profilo (impostazione predefinita 5%), il sistema interrompe l'indicizzazione e visualizza un messaggio di errore dell'indicizzazione.

La best practice consiste nel rimuovere le colonne e le celle vuote dal file origine dati, anziché nell'incrementare la soglia di errore. Tenere presente che se sono presenti molte celle vuote, per creare il profilo può essere necessario impostare una soglia di errori pari al 100%. Se si specifica 100% come valore soglia di errori, il sistema indicizza l'origine dati senza verificare la possibile presenza di errori.

Inoltre evitare di riempire le celle o i campi vuoti con dati fittizi per soddisfare il requisito della soglia di errori. L'aggiunta di dati fittizi o "null" all'origine dati riduce l'accuratezza del profilo EDM ed è vivamente sconsigliata. Il contenuto che si desidera monitorare deve essere legittimo e non nullo.

Vedere ["Informazioni sulla pulizia del file origine dati esatti"](#) a pagina 480.

Vedere ["Preparazione del file origine dati esatti per l'indicizzazione"](#) a pagina 488.

Vedere ["Assicurarsi che l'origine dati sia pronta per l'indicizzazione"](#) a pagina 562.

Rimozione di tipi di carattere ambigui dal file origine dati

Non è possibile utilizzare spazi estranei, segni di punteggiatura e campi compilati in modo incoerente nel file origine dati. È possibile usare strumenti quali Stream Editor (sed) e AWK per rimuovere questi elementi dai file origine dati prima di indicizzarli.

Tabella 22-44 Caratteri da evitare nel file origine dati

Caratteri da evitare	Spiegazione
Singoli caratteri	Eliminare i campi con singoli caratteri dal file origine dati, in quanto è più probabile che generino falsi positivi perché un singolo carattere appare frequentemente nelle comunicazioni normali.
Abbreviazioni	Eliminare i campi con abbreviazioni dal file origine dati per lo stesso motivo per cui è necessario eliminare i campi con singoli caratteri.
Virgolette	Non racchiudere i campi di testo tra virgolette.
Numeri piccoli	L'indicizzazione di campi numerici che contengono meno di 5 cifre non è consigliata perché è probabile che generi molti falsi positivi.
Date	Anche i campi della data non sono consigliati. Le date vengono trattate come una stringa. Quindi, se si indicizza una data, ad esempio 6/12/2007, la stringa deve corrispondere esattamente. L'indicizzatore trova solo 6/12/2007 e non altri formati di data, ad esempio 6 dicembre 2007, 6-12-2007 o 6 dic 2007. Deve essere una corrispondenza esatta.

Funzionamento della corrispondenza di celle multitoken

Una regola EDM esegue una ricerca full-text nel messaggio Controlla ogni parola (a eccezione di quelle che sono escluse con le colonne scelte per la corrispondenza nella politica) per verificare se è una potenziale corrispondenza. L'algoritmo di corrispondenza confronta ogni singola parola nel messaggio con i contenuti di ciascun token nel profilo di dati.

Se una cella nel profilo di dati contiene più parole separate da spazi, punteggiatura o caratteri alternativi in lingua latina e cinese, giapponese e coreano (CJK), la cella è una cella multitoken. Le parti subtoken di una cella multitoken rispondono alle stesse regole delle celle a token singolo: vengono normalizzate secondo il loro criterio nel quale è possibile applicare la normalizzazione.

Se una cella contiene un multitoken, quest'ultimo deve corrispondere esattamente. Ad esempio, un campo di colonna con il valore "Mario Rossi" è una cella multitoken (si presupponga che sia attivata la corrispondenza multitoken). In fase di runtime il processore cerca la corrispondenza della stringa esatta "Mario Rossi", compreso lo spazio (più spazi vengono normalizzati in uno). Il sistema non trova una corrispondenza per "Mario" e "Rossi" se vengono rilevati come singoli token.

Inoltre le celle multitoken richiedono un livello di elaborazione di calcolo superiore rispetto alle celle a token singolo. Se l'indice include celle multitoken, è necessario verificare che vi sia una quantità di memoria sufficiente per indicizzare, caricare ed elaborare il profilo EDM.

Se la corrispondenza multitoken è attivata, eventuali segni di punteggiatura accanto a uno spazio vengono ignorati. Di conseguenza la punteggiatura prima di e dopo uno spazio viene ignorata.

Infine non cambiare l'impostazione WIP da "true" a "false" a meno che questo non sia il risultato desiderato. Impostare WIP su false solo quando è necessario ampliare i criteri di corrispondenza, ad esempio i numeri di conto per cui la formattazione può cambiare nei vari messaggi. Verificare i risultati del rilevamento per assicurarsi di ottenere le corrispondenze previste.

Vedere ["Requisiti di memoria per EDM"](#) a pagina 532.

Mancato utilizzo del delimitatore virgola se l'origine dati ha campi numerici

Dei tre tipi di delimitatore di colonna che è possibile scegliere per separare i campi nel file origine dati (barra verticale, tabulazione, punto e virgola o virgola), è consigliata la barra verticale, il punto e virgola o la tabulazione (impostazione predefinita). Il delimitatore virgola è ambiguo e non deve essere utilizzato, in particolare se uno o più campi nell'origine dati contengono numeri. Se si utilizza un file origine dati delimitato da virgole, assicurarsi che non vi siano virgole nel set di dati oltre a quelle utilizzate come delimitatori di colonna.

Nota: Sebbene il sistema tratti anche il segno del cancelletto, il segno uguale, il segno più, il punto e virgola e i due punti come separatori, non utilizzarli perché, come nel caso della virgola, il loro significato è ambiguo.

Mappaggio delle colonne origine dati ai campi di sistema per utilizzare la convalida

Quando si crea il Profilo dati esatti, è possibile convalidare la corrispondenza tra i campi dell'origine dati e i criteri definiti dal sistema per il campo. Se ad esempio si mappa un campo sul criterio di sistema carta di credito, il sistema convaliderà i dati se corrispondono al criterio previsto per la carta di credito. In caso contrario, il sistema creerà un errore per ogni record che contiene un numero di carta di credito non valido. Il mapping dei campi origine dati dell'indice su criteri campo definiti dal sistema contribuisce a garantire che i campi dell'indice soddisfino i criteri del tipo di dati.

Se non è presente un campo di sistema corrispondente da mappare a una colonna dell'origine dati, può essere utile creare un campo personalizzato per mappare i dati colonna dell'origine

dati. È possibile usare il campo descrizione per annotare sia i campi di sistema che i campi personalizzati.

Vedere ["Mapping dei campi del profilo dati esatti"](#) a pagina 496.

Vedere ["Creazione e modifica di profili dati esatti"](#) a pagina 492.

Assicurarsi che l'origine dati sia pronta per l'indicizzazione

Il seguente elenco riassume un'origine dati ottimizzata pronta per l'indicizzazione:

- Contiene almeno un campo colonna unico.
- Non è un'origine dati a colonna singola; ha due o più colonne.
- Le celle e le righe vuote e le colonne in bianco vengono rimosse.
- I record incompleti e duplicati vengono rimossi.
- Il numero delle celle danneggiate è inferiore al tasso di errore predefinito (5%) per l'indicizzazione.
- I dati simulati non vengono utilizzati per compilare le celle o le righe in bianco.
- I caratteri non adatti e ambigui vengono rimossi.
- I multitoken sono conformi ai requisiti di spazio e memoria.
- I campi della colonna vengono convalidati rispetto modelli definiti dal sistema disponibili.
- I mapping vengono convalidati secondo i modelli della politica, dove applicabile.

Vedere ["Verifica della presenza di almeno una colonna di dati univoci nell'origine dati"](#) a pagina 558.

Vedere ["Eliminazione di colonne vuote e righe duplicate dal file origine dati"](#) a pagina 559.

Vedere ["Rimozione di tipi di carattere ambigui dal file origine dati"](#) a pagina 560.

Vedere ["Funzionamento della corrispondenza di celle multitoken"](#) a pagina 560.

Vedere ["Mappaggio delle colonne origine dati ai campi di sistema per utilizzare la convalida"](#) a pagina 561.

Sfruttamento dei modelli di politica EDM quando possibile

Symantec Data Loss Prevention fornisce diversi modelli di politica che implementano le regole EDM. Si consiglia di utilizzare i modelli di politica tutte le volte possibili quando si implementa l'EDM. Se si utilizza un modello di politica per l'EDM, è necessario convalidare l'indice in base al modello quando si configura il profilo di dati esatti.

Vedere ["Modelli di politica EDM"](#) a pagina 476.

Vedere ["Creazione e modifica di profili dati esatti"](#) a pagina 492.

Inclusione delle intestazioni di colonna come prima riga del file origine dati

Quando si estraggono i dati di origine nel file origine dati, è necessario includere le intestazioni di colonna come prima riga nel file origine dati. L'inclusione delle intestazioni di colonna consente di identificare più facilmente i dati da utilizzare nelle politiche.

I nomi delle colonne riflettono i mapping delle colonne creati quando è stato aggiunto il profilo di dati esatti. Se una colonna non è mappata, si chiama Col **X**, dove **X** è il numero della colonna (a partire da 1) nel profilo di dati originali.

Se è necessario utilizzare il profilo di dati esatti per la DGM, il file deve disporre di una colonna con un'intestazione **e-mail** o la DGM non viene visualizzata nell'elenco a discesa **Directory EDM** (nella pagina di risoluzione).

Verifica degli avvisi di sistema per ottimizzare la precisione del profilo

È necessario esaminare sempre gli avvisi di sistema dopo avere creato il profilo di dati esatti. Gli avvisi di sistema forniscono informazioni molto specifiche sui problemi riscontrati quando si crea il profilo, ad esempio un numero di previdenza sociale in un campo di indirizzo, che incideranno sulla precisione.

Utilizzo di parole non significative per escludere le parole comuni dal rilevamento

Durante l'indicizzazione, le parole trovate nei file di parole non significative vengono ignorate. Le parole non significative sono parole comuni escluse dalla corrispondenza. Ad esempio, il file di parole non significative contiene parole comuni, quali articoli, preposizioni e così via. Per regolare il file di parole non significative, aggiungere o rimuovere parole nel file. Si consiglia di eseguire il backup dell'originale prima di modificarlo.

I file di parole non significative sono situati nella directory seguente, dove è installato il server di rilevazione che esegue l'indice: `\Program Data\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\stopwords`. Per impostazione predefinita, il sistema utilizza il file `stopwords_en.txt`, che è la versione in lingua inglese. Anche i file di parole non significative in altre lingue sono situati nella stessa directory. È possibile modificare il file della lingua delle parole non significative predefinito aggiornando la proprietà `stopword_languages` = en nel file `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\Indexer.properties` in Enforce Server.

Utilizzo dell'indicizzazione pianificata per automatizzare gli aggiornamenti del profilo

Quando si configura un **profilo di dati esatti**, è possibile definire una pianificazione per l'indicizzazione del file origine dati. La pianificazione dell'indice aiuta a decidere quando indicizzare il file origine dati. Ad esempio, invece di indicizzare l'origine dati contemporaneamente alla definizione del profilo, è possibile pianificare l'indicizzazione per una data successiva. In alternativa, se è necessario reindicizzare regolarmente l'origine dati, è possibile pianificare l'indicizzazione in modo che avvenga regolarmente.

Prima di configurare una pianificazione dell'indice, considerare quanto segue:

- Se si aggiornano le origini dati occasionalmente (ad esempio, meno di una volta al mese), generalmente non è necessario creare una pianificazione. Indicizzare i dati ogni volta che si aggiorna l'origine dati.
- Pianificare l'indicizzazione per gli orari di uso minimo del sistema. L'indicizzazione ha effetto sulle prestazioni in tutto il sistema Symantec Data Loss Prevention e quella delle origini dati di grandi dimensioni può richiedere tempo.
- Indicizzare un'origine dati non appena si aggiunge o si modifica il profilo di dati esatti corrispondente e indicizzarla di nuovo ogni volta che la si aggiorna. Ad esempio si consideri uno scenario in cui ogni mercoledì alle 14:00 si genera un file origine dati aggiornato. In questo caso è possibile pianificare l'indicizzazione ogni mercoledì alle 15:00 e avere tempo sufficiente per pulire il file origine dati e copiarlo su Enforce Server.
- Non indicizzare le origini dati giornalmente in quanto le prestazioni possono risentirne.
- Controllare i risultati e modificare la pianificazione di indicizzazione di conseguenza. Se le prestazioni sono soddisfacenti e si desiderano aggiornamenti più tempestivi, programmare aggiornamenti e indicizzazioni dei dati più frequenti.

Considerare la possibilità di utilizzare l'indicizzazione pianificata con l'indicizzazione EDM remota per mantenere aggiornato un profilo EDM. Ad esempio è possibile pianificare un cron job sul computer remoto per eseguire regolarmente Remote EDM Indexer. Il processo può inoltre copiare i file di indice generati nella directory di indice su Enforce Server. È quindi possibile configurare Enforce Server in modo da caricare l'indice generato esternamente e inviarlo per l'indicizzazione in base alla pianificazione.

Vedere ["Informazioni sulla pianificazione degli indici"](#) a pagina 481.

Vedere ["Pianificazione dell'indicizzazione di profili dati esatti"](#) a pagina 499.

Vedere ["Copia e caricamento di file di indice remoti su Enforce Server"](#) a pagina 549.

Corrispondenza con 3 colonne in una condizione EDM per aumentare la precisione di rilevamento

In un formato di dati strutturati come un database, ogni riga rappresenta un record e ogni record contiene valori correlati per ciascun campo di dati delle colonne. Quindi, affinché una condizione di regola di politica EDM corrisponda, tutti i dati devono provenire dalla stessa riga o dallo stesso record di dati. Quando si definisce una regola EDM, è necessario selezionare i campi necessari per la corrispondenza. Sebbene non vi sia un limite al numero di colonne che è possibile selezionare per la corrispondenza in una riga (fino al numero totale di colonne nell'indice, ovvero 32 al massimo), si consiglia di cercare la corrispondenza con almeno 2 o 3 colonne, una delle quali deve essere univoca. Generalmente si preferisce la corrispondenza con 3 campi. Tuttavia, se una delle colonne contiene un valore univoco, ad esempio il numero di previdenza sociale o il numero di una carta di credito, è possibile utilizzare 2 colonne.

Considerare l'esempio riportato di seguito. Creare una condizione di politica EDM basata su un **profilo di dati esatti** che contiene le 5 colonne seguenti di dati indicizzati:

- Nome
- Cognome
- Numero di previdenza sociale
- Numero di telefono
- Indirizzo e-mail

Se si selezionano tutte le 5 colonne da includere nella politica, considerare i risultati possibili in base al numero di campi necessari per ciascuna corrispondenza.

Se si sceglie "1 dei campi selezionati" per la corrispondenza, la politica genera senza dubbio un numero elevato di falsi positivi perché il record non è abbastanza unico. (Anche se la condizione corrisponde solo al campo del numero di previdenza sociale, possono esservi ancora falsi positivi perché esistono altri tipi di numeri a 9 cifre in grado di attivare una corrispondenza.)

Se si scelgono "2 dei campi selezionati" per la corrispondenza, la politica continua a restituire falsi positivi perché vi sono combinazioni di dati potenzialmente inutili: nome + cognome, numero di telefono + indirizzo e-mail o nome + numero di telefono.

Se si sceglie di cercare la corrispondenza con 4 o tutti i 5 campi di colonna, non è possibile escludere determinate combinazioni di campi di dati perché l'opzione non è disponibile per le corrispondenze con 2 o 3 campi.

Vedere ["Sfruttamento delle tuple di eccezione per evitare i falsi positivi"](#) a pagina 566.

In questo esempio, per assicurarsi di generare la corrispondenza più accurata, si consiglia di scegliere "3 dei campi selezionati per la corrispondenza". In questo modo è possibile ridurre il numero di falsi positivi e utilizzare una o più eccezioni per escludere le combinazioni che non costituiscono un problema, ad esempio nome + cognome + numero di telefono.

Qualunque sia il numero di campi che si sceglie per la corrispondenza, assicurarsi di includere la colonna con i dati più univoci e di cercare la corrispondenza con almeno 2 campi di colonna.

Sfruttamento delle tuple di eccezione per evitare i falsi positivi

La condizione di politica EDM consente di definire le tuple di eccezione per escludere combinazioni di dati. È necessario selezionare 2 o 3 colonne per la corrispondenza per sfruttare le tuple di eccezione.

L'EDM consente il rilevamento in base a qualsiasi combinazione di colonne in una determinata riga di dati (ovvero N di M campi di un dato record). Può venire attivato in caso di "tuple" o set di tipi di dati specificati. Ad esempio, una combinazione dei campi del nome e del numero di previdenza sociale può essere accettabile, mentre una combinazione dei campi del cognome e del numero di previdenza sociale può non esserlo. L'EDM prevede inoltre regole più complesse, ad esempio la ricerca di N di M campi, ma esclude le tuple specificate. Ad esempio, questo tipo di definizione di regola è necessario per identificare gli incidenti in violazione delle leggi sulla privacy dei dati statali, ad esempio California SB 1386, che richiede una combinazione di nome e cognome con qualsiasi dato seguente: numero di previdenza sociale, numero di conto bancario o numero di patente di guida.

Mentre le tuple di eccezione possono contribuire a ridurre i falsi positivi, l'utilizzo di diverse tuple di eccezione può indicare la presenza di errori sull'indice. In questo caso considerare la possibilità di rieseguire l'indicizzazione in modo da non dovere utilizzare così tante combinazioni escluse per raggiungere le corrispondenze desiderate.

Utilizzare una clausola WHERE per individuare i record che soddisfano criteri specifici

Un altro parametro di configurazione della condizione della politica EDM è l'opzione della clausola "Where". Questa opzione definisce una corrispondenza con il valore esatto specificato per il campo selezionato. È possibile fornire più valori separandoli con virgole. L'utilizzo di una clausola WHERE per rilevare record che soddisfano criteri specifici migliora l'accuratezza delle politiche EDM.

Ad esempio per trovare solo corrispondenze profilo dati esatti per "Employees" con un campo "State" contenente determinati stati, è possibile configurare una corrispondenza in cui "State" corrisponda a "CA,NV". Con questa regola il motore di rilevamento cerca la corrispondenza con un messaggio che contiene CA o NV.

Utilizzo del campo Corrispondenze minime per ottimizzare le regole EDM

Il campo Corrispondenze minime è utile per ottimizzare la sensibilità di una regola EDM. Ad esempio, il nome e il cognome di un dipendente in un'e-mail in uscita possono essere accettabili.

Tuttavia il nome e il cognome di 100 dipendenti è una violazione grave. Un altro esempio può essere rappresentato da una politica relativa al cognome e al numero di codice fiscale. La politica potrebbe consentire a un dipendente di inviare informazioni a un medico. Tuttavia l'invio di due cognomi e due numeri di codice fiscale è sospetto.

Combinazione tra identificatori dati e regole EDM per limitare l'impatto del rilevamento in due fasi

Quando si implementano le politiche EDM, è consigliabile combinare le regole identificatore dati (DI) con la condizione EDM per formare politiche composte. Per riferimento, tenere presente che tutti modelli di politica forniti dal sistema che implementano regole EDM implementano anche regole le regole identificatore dati nella stessa politica.

Sia gli identificatori dati sia le politiche EDM hanno lo scopo di proteggere le informazioni che consentono l'identificazione dell'utente (PII). Se si includono identificatori dati nelle regole EDM le politiche risultano più robuste e facilmente riutilizzabili nei server di rilevamento perché a differenza delle regole EDM gli identificatori dati vengono eseguiti sugli endpoint e non richiedono il rilevamento in due fasi. Quindi, se un endpoint è fuori dalla rete, le regole dell'identificatore dati possono proteggere i dati PII, ad esempio il numero SSN.

Le regole dell'identificatore dati sono inoltre utili nelle politiche EDM quando si raccolgono e si preparano i dati riservati per l'indicizzazione EDM. Ad esempio, una politica può contenere l'identificatore dati SSN degli Stati Uniti e una regola EDM per un numero SSN non ancora indicizzato o sconosciuto.

Inclusione di un campo per l'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo

È necessario includere i campi appropriati nel profilo di dati esatti per implementare la DGM con profilo.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Se si include il campo dell'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo e lo si mappa alla convalida di dati e-mail, l'indirizzo e-mail viene visualizzato nell'elenco a discesa **Directory EDM** (nella pagina di risoluzione).

Utilizzo della DGM con profilo per il rilevamento di identità di Network Prevent for Web

Se si desidera implementare la DGM per Network Prevent for Web, utilizzare una delle condizioni DGM con profilo per implementare la corrispondenza di identità. Ad esempio è possibile usare la corrispondenza di identità per bloccare tutto il traffico Web per un utente specifico. Per Network Prevent for Web non è possibile utilizzare le condizioni DGM sincronizzate per questo caso di utilizzo.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Vedere ["Configurazione del Mittente/Utente in base a una condizione della Profiled Directory"](#) a pagina 858.

Rilevamento del contenuto mediante Indexed Document Matching (IDM)

Il capitolo contiene i seguenti argomenti:

- [Introduzione a Indexed Document Matching \(IDM\)](#)
- [Configurazione di profili IDM e condizioni delle politiche](#)
- [Best practice per l'utilizzo di IDM](#)
- [Indicizzazione EDM remota](#)

Introduzione a Indexed Document Matching (IDM)

Indexed Document Matching (IDM) consente di proteggere le informazioni riservate contenute come dati non strutturati in documenti e file. Ad esempio, è possibile utilizzare IDM per rilevare dati di report finanziari contenuti in documenti di Microsoft Office, informazioni su fusioni e acquisizioni in file PDF e codice sorgente in file di testo. È anche possibile usare IDM per rilevare file binari, come immagini JPEG, progetti CAD e file multimediali. Inoltre, IDM consente di rilevare contenuto derivato come testo copiato da un documento di origine in un altro file.

Vedere ["Metodi di corrispondenza supportati da IDM"](#) a pagina 570.

Vedere ["Informazioni sul profilo documenti indicizzati"](#) a pagina 572.

Informazioni sull'utilizzo dell'IDM

Per utilizzare l'IDM, raccogliere i documenti e i file che si desidera proteggere e indicizzarli con Enforce Server. Durante il processo di indicizzazione, il sistema utilizza un algoritmo per

creare l'impronta di ciascun file o contenuto di file. Creare quindi una politica che contenga una o più condizioni IDM che fanno riferimento all'indice. A questo punto il sistema controlla i file in base all'indice alla ricerca di corrispondenze.

Ad esempio considerare un'origine di documento raccolta che includa diversi documenti di Microsoft Office riservati (Word, Excel, PowerPoint) e file immagine (JPEG, BMP). Creare un **profilo di documento indicizzato** e indicizzare i documenti e i file. Configurare quindi la condizione di politica **Contenuto corrispondente a firma documento** con un'impostazione **Esposizione minima documento** pari al 50%. L'indice e la politica IDM vengono distribuiti a un server di rilevamento.

In fase di produzione il server di rilevamento controlla i file in entrata in base all'indice alla ricerca di corrispondenze. Se un file basato su testo in entrata da cui il sistema estrae il contenuto contiene almeno il 50% del contenuto indicizzato di uno dei documenti di origine, il sistema registra una corrispondenza. E se un file immagine in entrata ha la stessa firma binaria di uno dei file che è stato indicizzato, il sistema registra una corrispondenza. Il server e l'agente cercano automaticamente la corrispondenza esatta del file con file binari (non estraibili) anche se la condizione di politica è configurata per la corrispondenza parziale.

Nota: l'agente Mac è fondamentalmente uguale all'agente Windows, ma non supporta il rilevamento in due fasi. Sui due agenti sono supportati canali diversi. Vedere ["Panoramica delle tecnologie di rilevamento dell'agente Mac e delle funzionalità di creazione di politiche"](#) a pagina 2041.

Vedere ["Tipi di rilevamento IDM"](#) a pagina 571.

Vedere ["Informazioni sul profilo documenti indicizzati"](#) a pagina 572.

Metodi di corrispondenza supportati da IDM

IDM supporta tre forme di corrispondenza: file esatto, contenuto file esatto e contenuto file parziale. I server di rilevamento supportano tutte e tre le forme di corrispondenza. DLP Agent supporta le corrispondenze file esatto e contenuto file parziale localmente sull'endpoint.

[Tabella 23-1](#) riassume le forme di corrispondenza in base alle piattaforme supportate da IDM.

Tabella 23-1 Metodi di corrispondenza per IDM

Tipo di corrispondenza	Descrizione	Piattaforma
Contenuto file parziale	Corrispondenza di singoli passaggi dei contenuti estratti e normalizzati del file. Vedere "Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali" a pagina 579.	Server di rilevamento DLP Agent

Tipo di corrispondenza	Descrizione	Piattaforma
File esatto	La corrispondenza è basata sulla firma binaria del file. Vedere "Utilizzo di IDM per rilevare file esatti" a pagina 578.	Server di rilevamento DLP Agent
Contenuto file esatto	La corrispondenza è una corrispondenza esatta del contenuto estratto e normalizzato del file. Vedere "Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali" a pagina 579.	Server di rilevamento Nota: Symantec consiglia di usare la corrispondenza contenuto file parziale anziché la corrispondenza contenuto file esatto.

Tipi di rilevamento IDM

Vi sono tre tipi di rilevamento IDM: agente, server e in due fasi. Il tipo scelto si basa sui requisiti di Data Loss Prevention.

La [Tabella 23-2](#) riassume i tre tipi di rilevamento IDM.

Tabella 23-2 Tipi di rilevamento IDM

Tipo	Descrizione	Dettagli
IDM agente	DLP Agent supporta la corrispondenza parziale di contenuti oltre alla corrispondenza esatta di file in locale sull'endpoint.	Vedere "Rilevamento Agent IDM" a pagina 571.
IDM server	Il server di rilevamento cerca la corrispondenza esatta di file, la corrispondenza esatta di contenuti di file e la corrispondenza parziale di contenuti di file.	Vedere "Rilevamento IDM su server" a pagina 572.
IDM in due fasi	DLP Agent invia i dati al server di rilevamento per la valutazione della politica.	Vedere "Rilevamento IDM in due fasi" a pagina 572.

Rilevamento Agent IDM

Con il rilevamento Agent IDM, DLP Agent valuta i documenti localmente in tempo reale per corrispondenze con contenuti parziali e corrispondenze file esatte. Agente IDM consente di utilizzare le regole di risposta di blocco, notifica e annullamento utente sull'endpoint con le politiche IDM. Symantec Data Loss Prevention supporta anche il rilevamento su canali basati sul flusso, quali la stampa o le operazioni Copia/Incolla dagli Appunti.

Vedere ["Metodi di corrispondenza supportati da IDM"](#) a pagina 570.

Agent IDM è attivato per impostazione predefinita per le nuove installazioni di Endpoint Server. Agent IDM per macOS è attivato per impostazione predefinita per gli endpoint server appena installati, ma è disattivato se si esegue l'upgrade. Per tutti gli upgrade, se si desidera utilizzare

Agent IDM è necessario attivarlo e reindicizzare i profili IDM in modo che l'indice endpoint venga generato e reso disponibile per il download da parte dei DLP Agent.

Rilevamento IDM su server

Con il rilevamento IDM su server, l'indice IDM viene distribuito a uno o più server di rilevamento e l'intero processo di rilevamento si verifica sui server. È possibile utilizzare l'IDM su server per cercare la corrispondenza esatta di file e contenuti di file. Per la corrispondenza di contenuti di file è possibile scegliere di cercare la corrispondenza esatta o parziale (dal 10% al 90%) dei contenuti dei file secondo la condizione **Esposizione minima documento** impostata per l'IDM.

Vedere ["Metodi di corrispondenza supportati da IDM"](#) a pagina 570.

Rilevamento IDM in due fasi

Il metodo di rilevamento in due fasi richiede la comunicazione e il trasferimento di dati tra DLP Agent e Endpoint Server per il rilevamento degli incidenti. È consigliabile solo se si dispone di indici molto grandi e gli agenti non hanno spazio sufficiente per supportare i profili. Il metodo di rilevamento in due fasi presenta maggior latenza rispetto al rilevamento locale e richiede molta più larghezza di banda di rete. Di conseguenza, non supporta le regole di risposta inline per i blocchi o le notifiche pop-up.

Con il rilevamento IDM in due fasi, DLP Agent invia i dati a Endpoint Server per la corrispondenza con l'indice del server. Se il rilevamento in due fasi è attivato per IDM, il server supporta tutte le modalità di corrispondenza, compresi file esatto, contenuti file esatti e contenuti file parziali.

Nota: Il rilevamento in due fasi non è supportato negli agenti eseguiti in endpoint macOS.

Se si usa il rilevamento in due fasi per IDM sull'endpoint Windows, tenere presenti le implicazioni per le prestazioni del rilevamento in due fasi.

Vedere ["Rilevamento in due fasi per DLP Agent."](#) a pagina 403.

Informazioni sul profilo documenti indicizzati

Profili documenti indicizzati è la configurazione definita dall'utente per creare e generare indici IDM. Un **Profilo documenti indicizzati** viene definito mediante la console di amministrazione di Enforce Server. Quindi si fa riferimento al profilo in una o più regole o eccezioni di politica IDM. Il profilo è riutilizzabile da una politica all'altra: è possibile creare un solo profilo di documento e far riferimento al profilo in più politiche. Quando si crea il **Profilo documenti indicizzati**, è possibile scegliere se indicizzare l'origine del documento immediatamente al momento del salvataggio del profilo o in un momento successivo

pianificabile. Tuttavia, è necessario indicizzare l'origine documento per poter rilevare le violazioni della politica.

Vedere ["Creazione e modifica di profili di documento indicizzati"](#) a pagina 588.

Ad esempio, si consideri uno scenario in cui si desidera creare un indice IDM per rilevare quando vengono trovate le versioni esatte di determinati documenti o quando vengono visualizzati passaggi o sezioni dei documenti. Quando si definisce il **Profilo documenti indicizzati**, è possibile caricare i documenti in Enforce Server oppure indicizzarli mediante Indicizzatore IDM remoto. È anche possibile utilizzare filtri per nome file e dimensione file nel profilo del documento per includere o ignorare determinati file durante l'indicizzazione.

Informazioni sull'origine dati del documento

L'origine dati del documento è la raccolta di documenti che si desidera indicizzare e rilevare mediante IDM. L'algoritmo di indicizzazione usa una quantità fissa di memoria per documento e pertanto è limitato dal numero dei documenti anziché dalle loro dimensioni complessive. Con un profilo che utilizza 2 GB una volta caricato in memoria, è possibile indicizzare circa 1.000.000 di documenti. Il numero esatto di documenti consentito dal sistema dipende dal numero di documenti con testo che può essere estratto.

Vedere ["Preparazione di un'origine dati di documento per l'indicizzazione"](#) a pagina 583.

Per i set di documenti più piccoli (fino a 50 MB) è possibile caricare i file di origine in Enforce Server mediante un file ZIP. Per i set di documenti più grandi (fino a 2 GB), è possibile copiare i file di origine nel file system host in cui è installato Enforce Server, come file singoli o in un file ZIP. È possibile usare FTP/S per trasferire i file a Enforce Server. In alternativa, è possibile usare Indicizzatore IDM remoto per l'indicizzazione remota dei documenti.

Vedere ["Informazioni sull'indicizzazione remota dei documenti"](#) a pagina 574.

L'origine dati del documento può contenere qualsiasi tipo di file e qualsiasi combinazione di file. Se il sistema è in grado di estrarre il contenuto del file, IDM individua i contenuti del file, esattamente o parzialmente a seconda della piattaforma e della configurazione della politica. Se il sistema non è in grado di estrarre il contenuto del file, IDM individua il file esatto.

Vedere ["Metodi di corrispondenza supportati da IDM"](#) a pagina 570.

Informazioni sul processo di indicizzazione

L'indicizzatore IDM è un processo separato che viene installato con ed eseguito su Enforce Server. La corrispondenza parziale è disattivata per impostazione predefinita sull'agente e attivata per impostazione predefinita sul server di rilevamento. Vedere ["Configurazione della corrispondenza parziale del contenuto endpoint"](#) a pagina 590.

Il numero di documenti che è possibile indicizzare è aumentato fino a 1.000.000 sul server e fino a 30.000 sull'agente. Questi valori sono basati sui limiti predefiniti iniziali di 2 MB/60 GB.

È possibile modificare il limite di 60 MB nella pagina Configura corrispondenza parziale. Sebbene sia possibile riconfigurare il limite di 2 GB mediante la modifica della dimensione di `com.vontu.profiles.documents.maxIndexSize` in `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\indexer.properties`, Symantec consiglia di contattare il supporto Symantec prima di riconfigurare i file delle proprietà.

Durante l'indicizzazione, il sistema archivia l'origine del documento modificando `\Programmi\Symantec\Data Loss Prevention\Server Platform Common\15.1\Protect\documentprofiles` (in Windows) o `/var/Symantec/DataLossPrevention/Server Platform Common/15.1/documentprofiles` (in Linux). Dopo l'indicizzazione, per motivi di sicurezza, il sistema elimina i file di origine dei documenti che sono stati caricati su Enforce Server.

Il processo di indicizzazione restituisce quattro indici separati: uno per i server di rilevamento (indice server) e tre per i DLP Agent (indici endpoint). Tutti gli indici vengono generati indipendentemente dal fatto che si disponga o meno della licenza per Endpoint Prevent o Endpoint Discover. In Enforce Server, il sistema archivia gli indici in `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\index` (in Windows) o `/var/Symantec/DataLossPrevention/Enforce Server/15.1/index` (in Linux).

Vedere ["Informazioni sui file di indice del server e i file di indice dell'agente"](#) a pagina 575.

Per la maggior parte delle distribuzioni IDM non è necessario configurare l'indicizzatore. Se necessario è possibile configurare le impostazioni chiave per l'indicizzatore con il file `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\Indexer.properties`.

Nota: Symantec consiglia di contattare il supporto Symantec per informazioni se si decide di modificare un file di proprietà. La modifica errata delle proprietà può causare problemi seri con il funzionamento di Symantec Data Loss Prevention.

Informazioni sull'indicizzazione remota dei documenti

L'indicizzazione IDM può essere eseguita su Enforce Server o remotamente mediante l'Indicizzatore ID remoto.

Vedere ["Creazione e modifica di profili di documento indicizzati"](#) a pagina 588.

Mediante il protocollo CIFS è possibile indicizzare remotamente documenti archiviati su una o più condivisioni file in un ambiente di rete Microsoft Windows. Si fornisce il percorso Universal Naming Convention (UNC) a una risorsa cartella di rete condivisa, quindi si indicizzano i documenti archiviati in tale cartella o nelle sottocartelle, a seconda del livello di autorizzazione concesso.

Vedere ["Utilizzo dell'opzione di condivisione SMB remota per indicizzare le condivisioni di file"](#) a pagina 595.

WebDAV fornisce estensioni al protocollo HTTP 1.1 che consentono la modifica e la gestione collaborativa dei file archiviati su server Web remoti. È possibile indicizzare a distanza tali documenti rendendoli disponibili a Enforce Server mediante WebDAV. Ad esempio è possibile utilizzare l'opzione SMB remota con un indirizzo UNC e un client WebDAV per indicizzare documenti Microsoft SharePoint o OpenText Livelink.

Vedere ["Utilizzo dell'opzione di condivisione SMB remota per indicizzare i documenti SharePoint"](#) a pagina 596.

Nota: Per indicizzare i documenti su un server SharePoint mediante l'opzione Usa condivisione SMB remota, è necessario distribuire Enforce Server su un sistema operativo host Windows Server. Data Loss Prevention dipende dai servizi Windows NTLM per il montaggio di un server WebDAV.

Informazioni sui file di indice del server e i file di indice dell'agente

Quando si crea un **Profilo documento indicizzato** e si indicizza un'origine dati documento, il sistema genera quattro file di indice, uno per il server e tre per l'endpoint. Gli indici vengono generati indipendentemente dal fatto che si disponga di una licenza per un server di rilevamento o per il DLP Agent.

Vedere ["Informazioni sulla distribuzione e sulla registrazione degli indici"](#) a pagina 576.

L'indice server è un file binario denominato `DocSource.rdx`. L'indice server supporta la corrispondenza file esatto, contenuto file esatto e contenuto file parziale. Se l'origine dati del documento è molto grande, l'indice server può estendersi su più file `*.rdx`.

L'indice endpoint è costituito da un file binario protetto, `EndpointDocSource.rdx` o `LegacyEndpointDocSource.rdx`, per compatibilità con le versioni precedenti 14.0 e 12.5 degli agenti. L'indice endpoint supporta le corrispondenze file esatto e contenuto file parziale. `EncryptedDocSource.rdx` è destinato alla corrispondenza parziale endpoint.

Vedere ["Metodi di corrispondenza supportati da IDM"](#) a pagina 570.

Per creare le voci di indice per la corrispondenza file esatto e contenuto file esatto il sistema usa l'algoritmo di elaborazione messaggi MD5. Questo algoritmo è una funzione di hashing unidirezionale che prende come input un messaggio di lunghezza arbitraria e produce come output un'elaborazione messaggio o "fingerprint" a 128 bit dell'input. Se l'input del messaggio è un documento di testo dal quale il sistema può estrarre contenuto, quale un file Microsoft Word, il sistema estrae tutto il contenuto del file, lo normalizza rimuovendo gli spazi, la punteggiatura e la formattazione e crea un hash di crittografia. Se invece l'input del messaggio è un file dal quale il sistema non è in grado di estrarre i contenuti, quale un file immagine, un file di piccole dimensioni o un tipo di file non supportato, il sistema crea un hash crittografico basato sulla firma binaria del file stesso.

Nota: Per migliorare l'accuratezza su diverse versioni di Enforce Server e DLP Agent, sull'agente è supportato solo il MDF con corrispondenza binaria, sia che il file contenga o meno del testo.

Vedere ["Utilizzo di IDM per rilevare file esatti"](#) a pagina 578.

Vedere ["Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali"](#) a pagina 579.

Inoltre per i formati di file dai quali il sistema è in grado di estrarre il contenuto, l'indicizzatore crea hash per singole sezioni di contenuto o passaggi di testo. Tali hash vengono utilizzati per la corrispondenza parziale per indici sia del server che dell'agente. Il sistema usa un metodo di selezione per archiviare le sezioni hash di contenuto parziale in modo che non tutto il testo estraibile venga indicizzato. La funzione di hashing garantisce che l'indice del server non includa contenuto reale del documento. [Tabella 23-3](#) riassume i tipi di corrispondenze supportati dagli indici endpoint e server.

Tabella 23-3 Tipi di corrispondenze supportati dal gli indici endpoint e server

Input del messaggio	Output	Corrispondenze	Incluso nel file indice
File di testo dal quale il sistema può estrarre contenuto	Singolo hash crittografico derivato da tutto il contenuto del file estratto e normalizzato	Contenuto file esatto	DocSource.rdx LegacyEndpointDocSource.rdx
	Uno o più hash in sequenza basati su passaggi distinti di contenuto estratto e normalizzato mediante un metodo di selezione	Contenuto parziale del file (10% - 90%)	DocSource.rdx EndpointDocSource.rdx EncryptedDocSource.rdx
File binario, file personalizzato, piccolo file, file encapsulated Solo agente: file di testo dal quale il sistema può estrarre contenuto	Hash crittografico singolo basato sulla firma binaria del file.	File binario esatto	DocSource.rdx EndpointDocSource.rdx LegacyEndpointDocSource.rdx

Informazioni sulla distribuzione e sulla registrazione degli indici

Enforce Server è responsabile della distribuzione degli indici endpoint e del server IDM ai server di rilevazione e agli Endpoint Server. Non è possibile distribuire manualmente gli indici.

Il sistema distribuisce l'indice del server a ogni server di rilevazione designato nella cartella `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\index` (su Windows) o `/var/Symantec/DataLossPrevention/Enforce Server/15.1/index` (su Linux). In fase di runtime il server di rilevamento carica l'indice del server nella RAM quando una politica IDM attiva che fa riferimento all'indice viene distribuita al server di rilevamento.

Il sistema distribuisce l'indice endpoint (`EndpointDocSource.rdx` o `LegacyEndpointDocSource.rdx`) a ogni Endpoint Server designato. Quando DLP Agent si connette a Endpoint Server, scarica l'indice endpoint. Se l'IDM dell'agente è attivata, DLP Agent carica l'indice endpoint nella memoria quando l'indice è richiesto da una politica locale attiva.

Vedere ["Stima dell'utilizzo di memoria dell'endpoint per Agent IDM"](#) a pagina 605.

Non è possibile distribuire manualmente i file di indice endpoint o del server mediante la copia dei file `*.rdx` da Enforce Server su un server di rilevazione. Il server di rilevazione non monitora la cartella di destinazione dell'indice alla ricerca di nuovi file di indice. Enforce Server deve avvertire il server di rilevazione quando viene distribuito un indice. Se un server di rilevazione non è in linea durante il processo di distribuzione dell'indice, Enforce Server si arresta nel tentativo di distribuire l'indice. Quando il server di rilevazione torna in linea, Enforce Server distribuisce l'indice al server di rilevazione. Lo stesso vale per i DLP Agent. Non è possibile copiare manualmente l'indice endpoint all'host endpoint e fare in modo che DLP Agent riconosca l'indice.

La [Tabella 23-4](#) riepiloga come gli indici IDM vengono distribuiti ed elenca i file di registro da controllare per risolvere i problemi relativi alla distribuzione degli indici.

Tabella 23-4 Distribuzione e registrazione degli indici IDM

Piattaforma	File di indice	Distribuzione	Registrato
Server	<code>DocSource.rdx</code>	<p>Inviato automaticamente da Enforce Server a ciascun server di rilevazione designato dopo la generazione dell'indice.</p> <p>Caricato dal server di rilevazione nella RAM in fase di runtime.</p>	<p><code>detection_operational.log</code></p> <p>Utilizzarlo per determinare se il profilo dell'indice è stato distribuito al server di rilevazione.</p> <p><code>FileReader.log</code></p> <p>Utilizzarlo per determinare se il profilo dell'indice è caricato nella memoria.</p>

Piattaforma	File di indice	Distribuzione	Registrato
Agente	EndpointDocSource.rdx o LegacyEndpointDocSource.rdx	Entrambi i file vengono inviati da Enforce Server a ciascun Endpoint Server designato. L'agente seleziona il file appropriato in base alla versione dell'agente. LegacyEndpointDocSource.rdx è per la retrocompatibilità con gli agenti 14.0 e 12.5. Scaricato da DLP Agent in base all'intervallo di connessione dell'agente. Caricato nella RAM in fase di runtime quando una politica attiva locale richiede l'indice.	endpoint_server_operational.log Utilizzarlo per determinare se il profilo dell'indice è stato distribuito a Endpoint Server. Estrarre i registri dell'agente per determinare se il profilo dell'indice è caricato nella memoria.

Utilizzo di IDM per rilevare file esatti

Il sistema esegue automaticamente la corrispondenza esatta di file su tutti i file binari. Inoltre, se il formato di file è basato su testo ma il sistema non è in grado di estrarre il contenuto dal file, il sistema esegue la corrispondenza esatta di file. Questo comportamento è vero anche se si seleziona una percentuale di **Esposizione minima documento** per la condizione IDM che è inferiore al valore **Esatto**. DLP Agent esegue la corrispondenza esatta su tutti i file, sia binari che con testo estraibile.

Vedere ["Informazioni sui file di indice del server e i file di indice dell'agente"](#) a pagina 575.

Ad esempio, una regola IDM con un'esposizione minima del documento del 50% cerca automaticamente una corrispondenza esatta con un file binario in quanto l'impostazione **Esposizione minima documento** riguarda solo i file da cui il sistema non può estrarre il contenuto. Inoltre, il sistema esegue la corrispondenza esatta per i file che contengono una piccola quantità di testo, come pure i file che sono stati incapsulati durante l'indicizzazione, anche se basati su testo.

Per ottimizzare la corrispondenza esatta di tipi di file nel rilevamento IDM endpoint, il sistema controlla la dimensione in byte del file prima di calcolare l'hash di runtime per il raffronto in base all'indice. Se la dimensione in byte non corrisponde alla dimensione del file indicizzato, non c'è la necessità di calcolare l'hash del file esatto. Il sistema non considera il formato di file quando crea l'impronta digitale del file esatto.

[Tabella 23-5](#) riepiloga il comportamento della corrispondenza esatta di tipi di file.

Tabella 23-5 Requisiti per l'uso di IDM per il rilevamento di file

Formato di file	Esempio	Descrizione
Formato di file da cui il sistema non può estrarre il contenuto	Formato di documento proprietario o non supportato	Se il sistema non può estrarre il contenuto dal formato di file, è possibile usare IDM per rilevare quel file specifico utilizzando la corrispondenza binaria esatta. Vedere "Non comprimere i file nell'origine documento" a pagina 608.
File binario	File GIF, MPG, AVI, progetti CAD, JPEG, file audio/video	È possibile usare IDM per rilevare tipi di file binari da cui non è possibile estrarre contenuto, come immagini, file grafica, JPEG e così via. Il rilevamento di file binari non è supportato su canali basati sul flusso.
File contenente una piccola quantità di testo	File CAD e diagrammi Visio	Un file contenente una piccola quantità di testo viene trattato come file binario anche se il contenuto è basato su testo e può essere estratto. Vedere "Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali" a pagina 579.
File incapsulato	Qualsiasi file che viene incapsulato durante l'indicizzazione (anche se è basato su testo e il contenuto può essere estratto); ad esempio, file di Microsoft Word in un file ZIP.	Se un file origine dati di un documento è incapsulato in un file di archivio, il contenuto del file secondario non può essere estratto ed è possibile creare l'impronta soltanto della firma binaria del file. Ciò non vale per gli archivi documenti che sono indici. Vedere "Informazioni sull'origine dati del documento" a pagina 573.

Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali

Il caso di utilizzo principale per l'IDM è il rilevamento di contenuti di file (distinti dai file binari, ad esempio file audio o video). Sul server e sull'endpoint è possibile utilizzare l'IDM per cercare la corrispondenza dei file esatta o parziale (dal 10% al 90%). Inoltre sul server è possibile cercare la corrispondenza dei contenuti di file esatta. Symantec consiglia di utilizzare la corrispondenza dei contenuti parziale perché è molto più affidabile di quella esatta. I contenuti di file includono contenuto basato su testo di qualsiasi tipo di documento da cui il sistema può estrarre i contenuti, ad esempio documenti di Microsoft Office (Word, Excel, PowerPoint), PDF e molti altri.

Vedere ["Formati supportati per l'estrazione di contenuto"](#) a pagina 893.

Una corrispondenza dei contenuti di file esatta significa che il contenuto estratto normalizzato del file corrisponde esattamente al contenuto di un file che è stato indicizzato. Con la corrispondenza parziale sull'endpoint, l'utilizzo di una soglia pari al 90% genera corrispondenze

di contenuto dal 90% al 100%. Queste corrispondenze sono meno rigorose delle corrispondenze di contenuti esatte precedenti e in certi casi possono corrispondere anche se vi sono alcune differenze minori tra il file sottoposto a scansione e il file indicizzato.

Il sistema non considera il formato o la dimensione del file quando crea l'hash di crittografia per l'indice o quando cerca una corrispondenza dei contenuti di file esatta in base all'indice. Un documento potrebbe contenere molto più contenuto, ma il sistema rileva solo i contenuti di file che sono indicizzati come parte del **profilo del documento indicizzato**. Ad esempio si consideri una situazione in cui si indicizza un documento di una pagina e che tale documento sia incluso come parte di un documento di 100 pagine. Il documento di 100 pagine è considerato una corrispondenza esatta perché il contenuto corrisponde esattamente al documento di una pagina.

Vedere ["Informazioni sui file di indice del server e i file di indice dell'agente"](#) a pagina 575.

Per i file basati su testo da cui è possibile estrarre i contenuti, oltre a creare l'impronta MD5 per la corrispondenza di contenuti di file esatta, il sistema utilizza un algoritmo hash progressivo per registrare sezioni o passaggi di contenuto distinti. In questo caso il sistema utilizza un metodo di selezione per condividere le sezioni di contenuti con hash. Non tutto il testo è contrassegnato da hash nell'indice. L'indice non contiene contenuto del documento effettivo.

La [Tabella 23-6](#) elenca i requisiti per cercare la corrispondenza dei contenuti di file con l'IDM.

Tabella 23-6 Requisiti per l'utilizzo dell'IDM per rilevare il contenuto

Requisito	Descrizione
Formati di file da cui è possibile estrarre i contenuti	<p>Il sistema deve essere in grado di estrarre il formato di file ed estrarre il contenuto del file. Data Loss Prevention supporta l'estrazione di contenuto per oltre 100 tipi di file.</p> <p>Vedere "Formati supportati per l'estrazione di contenuto" a pagina 893.</p>
File non incapsulato	<p>Per cercare la corrispondenza di contenuti di file, il file origine non può venire incapsulato in un file di archivio quando il file origine viene indicizzato. Se un file nell'origine del documento viene incapsulato in un file di archivio, il sistema non indicizza i contenuti del file incapsulato. I file incapsulati vengono considerati solo per le corrispondenze esatte, ad esempio i file immagine e altri formati di file non supportati.</p> <p>Vedere "Non comprimere i file nell'origine documento" a pagina 608.</p> <p>Nota: l'eccezione è rappresentata dal file ZIP principale che contiene l'origine dati del documento per i metodi di caricamento che utilizzano un file di archivio. Vedere "Creazione e modifica di profili di documento indicizzati" a pagina 588.</p>

Requisito	Descrizione
Quantità minima di testo	<p>Per la corrispondenza dei contenuti di file esatta, il file origine deve contenere almeno 50 caratteri di testo normalizzato prima che il contenuto estratto venga indicizzato. La normalizzazione comporta la rimozione della punteggiatura e degli spazi bianchi. Pertanto un carattere normalizzato è un numero o una lettera. Questa dimensione è impostata dal parametro <code>min_normalized_size=50</code> nel file <code>\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\Indexer.properties</code>. Se il file contiene meno di 50 caratteri normalizzati, il sistema cerca una corrispondenza esatta del file in base al file binario.</p> <p>Nota: Symantec consiglia di rivolgersi al supporto Symantec per assistenza nella modifica di un'impostazione avanzata o un file di proprietà. L'aggiornamento errato di un file di proprietà può avere conseguenze impreviste.</p> <p>Per la corrispondenza di contenuti di file parziale devono esservi almeno 300 caratteri normalizzati. Tuttavia la lunghezza esatta varia a seconda dei contenuti di file e della codifica.</p> <p>Vedere "Mancata indicizzazione di documenti vuoti" a pagina 609.</p>
Quantità massima di testo	<p>La dimensione massima predefinita del documento che può essere elaborato per l'estrazione di contenuti in fase di runtime è 30.000.000 di byte. Se il documento misura oltre 30.000.000 di byte, è necessario aumentare la dimensione massima predefinita nelle impostazioni avanzate del server. Contattare il supporto Symantec per assistenza nella modifica delle impostazioni avanzate del server per evitare conseguenze impreviste.</p>

Informazioni sull'utilizzo della condizione Contenuto corrispondente a firma documento

Utilizzare la condizione IDM **Il contenuto corrisponde alla firma del documento** di per implementare le regole e le eccezioni di rilevamento IDM nelle politiche.

Vedere ["Configurazione della condizione di politica Contenuto corrispondente a firma documento"](#) a pagina 605.

Quando si configura questa condizione, specificare l'indice IDM da utilizzare e come la condizione deve corrispondere all'indice con l'impostazione **Esposizione minima documento**. È possibile selezionare **Esatto** o un valore parziale compreso tra il 10% e il 90%. Ad esempio, se si seleziona **70%** per **Esposizione minima documento**, viene trovata una corrispondenza solo se viene rilevato il 70% o più dei contenuti di file con hash.

Vedere ["Utilizzo di regole IDM parallele per ottimizzare le soglie di corrispondenze"](#) a pagina 614.

Se un file non è basato sul testo, il contenuto non è estraibile, è molto piccolo o è incapsulato in un file di archivio, viene trovata una corrispondenza esatta del file in base alla firma binaria. Questa forma di corrispondenza viene cercata automaticamente dal sistema, indipendentemente dall'opzione di configurazione scelta per l'impostazione **Esposizione minima documento**. Questa impostazione viene applicata solo alla corrispondenza parziale dei contenuti di file.

Vedere ["Utilizzo di IDM per rilevare file esatti"](#) a pagina 578.

La [Tabella 23-7](#) descrive la corrispondenza supportata dalla condizione di politica **Il contenuto corrisponde alla firma del documento di**.

Tabella 23-7 Impostazioni di esposizione minima del documento per la condizione IDM

Impostazione di configurazione	Contenuti di file	Corrisponde	Esempio
Corrispondenza esatta file	Contenuti di file Vedere "Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali" a pagina 579.	Tutti i contenuti di file estratti e normalizzati, se il file è basato sul testo e da cui il contenuto non può essere estratto	Microsoft Word
Corrispondenza esatta contenuto	L'endpoint cerca una corrispondenza binaria con tutti i file.		Microsoft Word, JPG, MP3
Corrispondenza parziale contenuto	Contenuti di file Vedere "Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali" a pagina 579.	Passaggi distinti di testo	Microsoft Word

Informazioni sull'aggiunta del contenuto file parziale a una lista bianca

Spesso i documenti riservati contengono testo boilerplate standard che non richiede protezione, ad esempio pagine introduttive, intestazioni e piè di pagina. Le informazioni contenute nelle intestazioni e nei piè di pagina dei documenti possono dare origine a falsi positivi. Inoltre i testi boilerplate, quali linguaggio standard e contenuti corporativi non privati che vengono ripetuti nei documenti riservati, possono causare falsi positivi.

Vedere ["Creazione di una lista bianca di contenuto di file da escludere dalla corrispondenza parziale"](#) a pagina 585.

La rimozione di contenuto boilerplate non riservato o di contenuto di intestazioni/piè di pagina prima dell'indicizzazione non è in genere fattibile, specie con un set di dati documento molto grande. In questo caso è possibile configurare il sistema per escludere (inserire in una lista bianca) il testo non riservato. È possibile fare ciò aggiungendo il testo da ignorare al file lista bianca. Durante l'indicizzazione, tutto il contenuto della lista bianca rilevato nei file di origine viene ignorato. In fase di runtime il contenuto non causa falsi positivi perché è stato escluso.

Vedere ["Utilizzare la lista bianca per escludere il contenuto non sensibile dalla corrispondenza parziale"](#) a pagina 611.

Nota: Le liste bianche sono valide solo per le corrispondenze con contenuto file parziale, e non per le corrispondenze con contenuto file esatto. Il file lista bianca non viene verificato in fase di runtime quando il sistema elabora gli hash di crittografia per la corrispondenza con contenuto file esatto.

Configurazione di profili IDM e condizioni delle politiche

[Tabella 23-8](#) fornisce il flusso di lavoro per creare profili IDM e configurare politiche IDM. Completare i passaggi per assicurarsi che le regole IDM siano implementate correttamente e siano il più possibile accurate ed efficienti.

Tabella 23-8 Implementazione IDM

Passaggio	Azione	Descrizione
1	Identificare il contenuto che si desidera proteggere e raccogliere i documenti che contengono questo contenuto.	Vedere "Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali" a pagina 579. Vedere "Utilizzo di IDM per rilevare file esatti" a pagina 578.
2	Preparare i documenti per l'indicizzazione.	Vedere "Preparazione di un'origine dati di documento per l'indicizzazione" a pagina 583.
3	Intestazioni, piè di pagina e testo standard lista bianca.	Vedere "Creazione di una lista bianca di contenuto di file da escludere dalla corrispondenza parziale" a pagina 585.
4	Creare un profilo di documento indicizzato e specificare la fonte del documento.	Vedere "Creazione e modifica di profili di documento indicizzati" a pagina 588.
5	Configurare tutti i filtri delle fonti di documenti.	Vedere "Filtraggio di documenti per nome di file" a pagina 599.
6	Programmare l'indicizzazione ove necessario.	Vedere "Pianificazione dell'indicizzazione di profili documento" a pagina 602.
7	Configurare una o più condizioni o eccezioni della politica IDM.	Vedere "Configurazione della condizione di politica Contenuto corrispondente a firma documento" a pagina 605.
8	Testare e risolvere i problemi di implementazione IDM.	Vedere "Risoluzione dei problemi delle politiche" a pagina 458.

Preparazione di un'origine dati di documento per l'indicizzazione

È necessario raccogliere e preparare i documenti che si desidera indicizzare. Ognuno di questi documenti è un'origine dati di documento.

Vedere ["Informazioni sull'origine dati del documento"](#) a pagina 573.

Un'origine dati di documento è un file ZIP che contiene i documenti da indicizzare. Può anche essere un file archiviato in una condivisione di file su un computer locale o remoto. Un file ZIP di origine dati di documento può contenere qualsiasi tipo di file e qualsiasi combinazione di file. Se si ha una condivisione di file che già contiene i documenti da proteggere, è possibile fare riferimento a questa condivisione nel profilo di documento.

Tabella 23-9 Preparazione dell'origine dati di documento per l'indicizzazione

Passaggio	Azione	Descrizione
1	Raccogliere tutti i documenti da proteggere.	Raccogliere tutti i documenti da indicizzare e spostarli in una cartella. Vedere "Informazioni sull'origine dati del documento" a pagina 573.
2	Decomprimere tutti i file da indicizzare.	I file da indicizzare non devono essere incapsulati e nemmeno compressi. Verificare la raccolta di documenti per assicurarsi che nessuno dei file sia incapsulato in un file di archivio, come ZIP, TAR o RAR. Se un file è incorporato in un file di archivio, estrarre il file di origine dal file di archivio e rimuovere quest'ultimo. Vedere "Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali" a pagina 579.
3	Separare i documenti se si hanno più di 1.000.000 di file da indicizzare.	Per proteggere una grande quantità di contenuto e un gran numero di file, creare raccolte distinte per ogni set di documenti con più di 1.000.000 di file, con tutti i file non incapsulati e non compressi. Ad esempio, se si hanno 1.500.000 documenti da indicizzare, inserirli in più cartelle: 750.000 file in una cartella e gli altri 750.000 in un'altra cartella. Oppure, è possibile cambiare il valore di <code>com.vontu.profiles.documents.maxIndexSize</code> in <code>Indexer.properties</code> per consentire set di dati più grandi. La regola generale è 2 GB/1 milione di documenti. Vedere "Creazione di profili separati per indicizzare origini di documenti di grandi dimensioni" a pagina 613.
4	Decidere come rendere disponibili i file di origine dei documenti a Enforce Server.	Il processo di indicizzazione è un processo distinto che viene eseguito su Enforce Server. Per indicizzare l'origine dei documenti è necessario rendere i file accessibili a Enforce Server. Sono disponibili diverse opzioni. Stabilire qual è la più appropriata e procedere di conseguenza. Vedere "Caricamento di un archivio di documenti in Enforce Server" a pagina 591. Vedere "Riferimento a un archivio documenti in Enforce Server" a pagina 592. Vedere "Utilizzo del percorso locale sul Enforce Server" a pagina 594. Vedere "Utilizzo dell'opzione di condivisione SMB remota per indicizzare le condivisioni di file" a pagina 595.

Passaggio	Azione	Descrizione
5	Configurare il profilo di documento.	<p>Il passaggio seguente consiste nel configurare il profilo di documento, oppure, se si desidera escludere del contenuto specifico dal rilevamento, nell'includerlo in una lista bianca.</p> <p>Vedere "Creazione e modifica di profili di documento indicizzati" a pagina 588.</p> <p>Vedere "Creazione di una lista bianca di contenuto di file da escludere dalla corrispondenza parziale" a pagina 585.</p>

Creazione di una lista bianca di contenuto di file da escludere dalla corrispondenza parziale

È possibile utilizzare una lista bianca per escludere contenuto non importante o non critico, come testo boilerplate e intestazioni e piè di pagina di documenti, dall'indice IDM. Una lista bianca di tale contenuto consente di ridurre il numero di falsi positivi.

Vedere ["Informazioni sull'aggiunta del contenuto file parziale a una lista bianca"](#) a pagina 582.

Vedere ["Utilizzare la lista bianca per escludere il contenuto non sensibile dalla corrispondenza parziale"](#) a pagina 611.

Per escludere contenuto dalla corrispondenza, copiare il contenuto che si desidera escludere in un file di testo e salvare il file come `Whitelisted.txt`. Per impostazione predefinita, il file deve contenere almeno 300 caratteri senza spazi vuoti perché ne venga creata l'impronta. Quando si indicizza l'origine del documento, Enforce Server o l'Indicizzatore IDM remoto cerca il file `Whitelisted.txt`.

Vedere ["Utilizzare la lista bianca per escludere il contenuto non sensibile dalla corrispondenza parziale"](#) a pagina 611.

[Tabella 23-10](#) descrive il processo di esclusione di contenuto di documenti utilizzando una lista bianca.

Tabella 23-10 Creazione di una lista bianca di contenuto non riservato

Passaggio	Azione	Descrizione
1	Copiare il contenuto che si desidera escludere dalla corrispondenza in un file di testo.	<p>Copiare solo contenuto non critico, ad esempio testo boilerplate e intestazioni e piè di pagina di documenti, nel file di testo. Per impostazione predefinita, il contenuto corrispondente al file da indicizzare deve contenere almeno 300 caratteri. Questa impostazione predefinita si applica anche al file <code>Whitelisted.txt</code>. È possibile modificare questa impostazione predefinita per il testo nella lista bianca.</p> <p>Vedere "Modifica delle proprietà predefinite dell'indicizzatore" a pagina 603.</p>

Passaggio	Azione	Descrizione
2	Salvare il file di testo come <code>Whitelisted.txt</code> .	Il file <code>Whitelisted.txt</code> è il file di origine con il contenuto che si desidera escludere dalla corrispondenza.
3	Salvare il file nella directory <code>whitelisted</code> sul file system dell'host di Enforce Server.	Salvare il file in <code>\Program Files\Symantec\Data Loss Prevention\Server Platform Common\15.1\Protect\documentprofiles\whitelisted</code> (su Windows) o in <code>/var/Symantec/DataLossPrevention/Server Platform Common/15.1/documentprofiles/whitelisted</code> (su Linux).
4	Configurare il profilo di documento indicizzato e generare l'indice.	Quando si indicizza l'origine dati del documento, Enforce Server o l'Indicizzatore IDM remoto cerca il file <code>Whitelisted.txt</code> . Se il file esiste, Enforce Server lo copia in <code>Whitelisted.x.txt</code> , dove <code>x</code> è un numero di identificazione univoco corrispondente al profilo di documento indicizzato . Per le indicizzazioni future del profilo, viene utilizzato il file <code>Whitelisted.x.txt</code> specifico del profilo e non il file <code>Whitelisted.txt</code> generico. Vedere "Creazione e modifica di profili di documento indicizzati" a pagina 588.

Gestione e aggiunta di profili documenti indicizzati

La schermata **Gestisci > Profili dati > Documenti indicizzati** elenca tutti i **Profili documenti indicizzati** configurati nel sistema. Da questa schermata è possibile gestire i profili esistenti e aggiungerne nuovi.

Tabella 23-11 Azioni della schermata Documenti indicizzati

Azione	Descrizione
Aggiunta del profilo IDM	Fare clic su Aggiungi profilo documento per creare un nuovo profilo di documento indicizzato. Vedere "Configurazione di profili IDM e condizioni delle politiche" a pagina 583.
Modifica del profilo IDM	Fare clic sul nome del profilo del documento o sull'icona della matita all'estrema destra della riga del profilo per modificare un profilo documento esistente. Vedere "Creazione e modifica di profili di documento indicizzati" a pagina 588.
Rimozione del profilo IDM	Fare clic sull'icona rossa X all'estrema destra della riga del profilo documento per eliminare il profilo dal sistema. Una finestra di dialogo conferma l'eliminazione. Nota: Non è possibile modificare o rimuovere un profilo se un altro utente lo sta modificando o se esiste una politica che dipende da quel profilo.

Azione	Descrizione
Aggiornamento dello stato del profilo IDM	Fare clic sull'icona di aggiornamento a forma di freccia in alto a destra nella schermata Documenti indicizzati per recuperare lo stato aggiornato del processo di indicizzazione. Durante il processo di indicizzazione, il sistema visualizza il messaggio "Avvio indicizzazione in corso.". Il sistema non aggiorna automaticamente la schermata al termine del processo di indicizzazione.

Tabella 23-12 Dettagli della schermata Documenti indicizzati

Colonna	Descrizione
Profilo documento	Il nome del profilo documento indicizzato.
Server di rilevamento	Il nome del server di rilevamento che indicizza il profilo documento e la versione del profilo documento. Fare clic sull'icona a forma di triangolo accanto al nome del profilo documento per visualizzare tali informazioni che vengono visualizzate sotto il nome del profilo documento.
Posizione	La posizione dei file su Enforce Server per il quale il sistema ha creato il profilo e l'indicizzazione.
Documenti	Il numero dei documenti che il sistema ha indicizzato per il profilo documento.
Stato	Lo stato attuale del processo di indicizzazione del documento che può essere uno dei seguenti: <ul style="list-style-type: none"> ■ Prossima indicizzazione pianificata (se non vi sono indicizzazioni in corso) ■ Invio di un indice a un server di rilevamento ■ Indicizzazione ■ Distribuzione a un server di rilevamento Inoltre, sotto lo stato del processo di indicizzazione, il sistema visualizza lo stato di ogni server di rilevamento che può essere uno dei seguenti: <ul style="list-style-type: none"> ■ Completato, inclusa una data di completamento ■ Completamento indicizzazione in sospeso (in attesa che Enforce Server termini l'indicizzazione di un file) ■ Replica dell'indicizzazione ■ Creazione dell'indice (internamente)
Messaggi di errore	La schermata Documento indicizzato visualizza anche tutti i messaggi di errore in rosso (ad esempio, se il profilo documento è danneggiato o non esiste).

Vedere ["Profili dati"](#) a pagina 381.

Vedere ["Pianificazione dell'indicizzazione di profili documento"](#) a pagina 602.

Vedere ["Configurazione della condizione di politica Contenuto corrispondente a firma documento"](#) a pagina 605.

Creazione e modifica di profili di documento indicizzati

È possibile definire e configurare un **profilo di documento indicizzato** nella schermata **Gestisci > Profili dati > Documenti indicizzati > Configura profilo documento**. Il profilo di documento specifica l'origine dati del documento, i parametri di indicizzazione e la pianificazione dell'indicizzazione. È necessario definire un profilo di documento per implementare il rilevamento IDM.

Vedere ["Informazioni sul profilo documenti indicizzati"](#) a pagina 572.

[Tabella 23-13](#) descrive i passaggi per creare e modificare profili IDM.

Tabella 23-13 Configurazione di un profilo di documento

Passaggio	Azione	Descrizione
1	Accedere alla schermata Gestisci > Profili dati > Documenti indicizzati .	È necessario essere connessi alla console di amministrazione di Enforce Server come amministratore o autore di politiche. Vedere "Privilegi di creazione politiche" a pagina 380.
2	Fare clic su Aggiungi profilo documento .	Selezionare un profilo di documento indicizzato esistente per modificarlo. Vedere "Gestione e aggiunta di profili documenti indicizzati" a pagina 586.
3	Immettere un nome per il profilo di documento.	Scegliere un nome che descriva il contenuto e il tipo di indice (ad esempio, "IDM documenti di ricerca"). Il nome non deve includere più di 255 caratteri. Vedere "Limiti di immissione caratteri per la configurazione di politiche" a pagina 442.

Passaggio	Azione	Descrizione
4	Selezionare l' origine del documento per l'indicizzazione.	<p>Selezionare una delle cinque opzioni per l'indicizzazione dell'origine dati del documento, a seconda della dimensione dell'origine dati e del metodo di compressione della stessa.</p> <p>Vedere "Informazioni sull'origine dati del documento" a pagina 573.</p> <p>Opzioni per rendere l'origine dati disponibile a Enforce Server.</p> <ul style="list-style-type: none"> Carica archivio documenti sul server Per utilizzare questo metodo, scegliere Sfoglia e selezionare un file ZIP contenente i documenti da indicizzare. La dimensione massima del file ZIP è 50 MB. Vedere "Caricamento di un archivio di documenti in Enforce Server" a pagina 591. Archivio di riferimento su Enforce Server Usare questo metodo se il file ZIP è stato copiato nell'host del file system in cui Enforce Server è installato. La dimensione massima del file ZIP è 2 GB. Questo file ZIP è disponibile per la selezione nel campo a discesa. Vedere "Riferimento a un archivio documenti in Enforce Server" a pagina 592. Usa percorso locale su Enforce Server Questo metodo consente di indicizzare singoli file che sono locali su Enforce Server. Con questo metodo i file da indicizzare non possono essere archiviati in un file ZIP. Vedere "Utilizzo del percorso locale sul Enforce Server" a pagina 594. Usa condivisione SMB remota Vedere "Informazioni sull'indicizzazione remota dei documenti" a pagina 574. Importa da un profilo IDM creato in remoto L'Indicizzatore IDM remoto è uno strumento autonomo che consente di indicizzare documenti e file riservati localmente sui sistemi in cui sono stati archiviati. Per ulteriori informazioni, vedere Indicizzazione IDM remota Vedere "Informazioni sull'Indicizzatore IDM remoto" a pagina 615.. Vedere "Utilizzo dell'opzione di condivisione SMB remota per indicizzare i documenti SharePoint" a pagina 596.

Passaggio	Azione	Descrizione
5	Opzionalmente, è possibile configurare i filtri .	<p>È possibile specificare i filtri di nome file e di dimensione di file nel profilo di documento. I filtri indicano al sistema quali file includere o ignorare durante l'indicizzazione.</p> <p>Vedere "Escludere documenti dall'indicizzazione per ridurre i falsi positivi." a pagina 611.</p> <p>Immettere i file da includere nel campo Filtri di inclusione nome file o quelli da escludere nel campo Filtri di esclusione nome file.</p> <p>Vedere "Filtraggio di documenti per nome di file" a pagina 599.</p> <p>Selezionare le dimensioni di file da ignorare con l'opzione Ignora file di dimensioni inferiori a o Ignora file di dimensioni superiori a.</p> <p>Vedere "Filtraggio di documenti per dimensioni file" a pagina 601.</p>
6	Selezionare una delle opzioni di indicizzazione .	<p>Come parte del processo di creazione di un profilo di documento, è possibile configurare una pianificazione per l'indicizzazione dell'origine del documento.</p> <p>Non è necessario selezionare un'opzione di indicizzazione per creare un profilo a cui è possibile fare riferimento in una politica, ma è necessario selezionarlo per generare l'indice e rilevare le corrispondenze utilizzando una politica IDM.</p> <ul style="list-style-type: none"> ■ Selezionare Invia processo di indicizzazione al salvataggio per indicizzare l'origine del documento quando si salva il profilo di documento. ■ Selezionare Invia processo di indicizzazione secondo pianificazione per visualizzare le opzioni di pianificazione in modo da poter pianificare l'indicizzazione in un secondo momento. <p>Vedere "Pianificazione dell'indicizzazione di profili documento" a pagina 602.</p>
7	Fare clic su Salva .	È necessario salvare il profilo di documento.

Configurazione della corrispondenza parziale del contenuto endpoint

È possibile attivare o disattivare la corrispondenza parziale del contenuto endpoint per profili IDM nella console di amministrazione Enforce Server su **Gestisci > Profili dati > Documenti indicizzati > Configura corrispondenza parziale endpoint**. In questa pagina viene visualizzata un'istantanea in tempo reale di tutti i profili distribuiti con la dimensione corrente stimata. Quando si fa clic su **Salva**, i profili selezionati dispongono di una corrispondenza parziale.

[Tabella 23-14](#) descrive i passaggi per la configurazione di una corrispondenza parziale con il contenuto sull'endpoint.

Tabella 23-14 Configurazione di corrispondenza parziale del contenuto endpoint

Passaggio	Azione	Descrizione
1	Passare alla schermata Gestisci > Profili dati > Documenti indicizzati> .	
2	Fare clic su Configura corrispondenza parziale .	Nella pagina Configura corrispondenza contenuto parziale viene visualizzata un'istantanea di tutti i profili distribuiti nel momento in cui si accede alla pagina, insieme alla relativa dimensione corrente stimata. Nota: La pagina Configura corrispondenza contenuto parziale non è accessibile durante l'indicizzazione di qualsiasi profilo IDM.
3	Fare clic sulla casella di controllo in Corrispondenza parziale endpoint per tutti i profili che si desidera attivare per la corrispondenza parziale.	Nota: Se un profilo avvia la reindicizzazione mentre ci si trova su questa pagina e le dimensioni dei profili cambiano in maniera significativa e se anche il profilo è selezionato per la corrispondenza parziale, l'elenco dei profili selezionati potrebbe essere interessato dalla modifica.
4	Fare clic su Salva .	Nota: La somma di tutti i profili distribuiti sull'endpoint non può superare il valore Dimensioni profilo totali endpoint (MB) , impostato per impostazione predefinita su 60 MB. Per modificare questo valore, immettere un diverso valore nella casella Dimensioni profilo totali endpoint (MB) . Dopo aver fatto clic su Salva , i profili selezionati dispongono di una corrispondenza parziale attivata. Fare clic su Aggiorna per assicurarsi di avere eseguito gli ultimi passaggi dell'operazione di indicizzazione.

Caricamento di un archivio di documenti in Enforce Server

L'opzione **Carica archivio documenti sul server** consente di caricare un file ZIP con una dimensione massima di 50 MB su Enforce Server e di indicizzarne i contenuti. Per l'utilizzo di questo metodo di indicizzazione, l'origine documento deve soddisfare i requisiti descritti nella tabella [Tabella 23-15](#)

[Per caricare l'archivio documenti in Enforce Server](#) descrive l'utilizzo del metodo di indicizzazione **Carica archivio documenti sul server**.

Per caricare l'archivio documenti in Enforce Server

- 1 Passare alla schermata **Gestisci > Profili dati > Documenti indicizzati > Configura profilo documento**.
- 2 Selezionare l'opzione **Carica archivio documenti sul server**.
Fare clic su **Sfoggia** e selezionare il file ZIP. Il file ZIP può trovarsi in qualsiasi punto della rete di Enforce Server.
Facoltativamente, è possibile digitare il percorso completo e il nome file se il file ZIP è locale rispetto a Enforce Server, ad esempio: `c:\Documents\Research.zip`.
- 3 Specificare uno o più filtri per nomi file o dimensioni file (facoltativo).
Vedere ["Filtraggio di documenti per nome di file"](#) a pagina 599.
- 4 Selezionare una delle opzioni di indicizzazione (facoltativo).
Vedere ["Pianificazione dell'indicizzazione di profili documento"](#) a pagina 602.
- 5 Fare clic su **Salva**.

Tabella 23-15 Requisiti per l'uso dell'opzione Carica archivio documenti sul server

Requisito	Descrizione
Solo file ZIP	L'archivio documenti deve essere un file ZIP; nessun altro formato di incapsulamento è supportato per questa opzione.
Fino a 50 MB	Non è possibile usare questa opzione se il file ZIP dell'archivio documenti ha dimensioni superiori a 50 MB, perché il caricamento dei file che superano tale limite di dimensioni può richiedere troppo tempo e rallentare le prestazioni di Enforce Server. Se il file ZIP dell'archivio documenti ha dimensioni superiori a 50 MB, utilizzare invece il metodo Archivio di riferimento su Enforce Server .
Solo nomi file UTF-8	<p>Il processo di indicizzazione IDM non riesce (e restituisce un "Errore imprevisto") se l'archivio documenti (file ZIP) contiene nomi file non ASCII in codifiche diverse da UTF-8.</p> <p>Se il file ZIP contiene file con nomi non ASCII, utilizzare invece una delle opzioni seguenti per rendere disponibili i file a Enforce Server per l'indicizzazione:</p> <ul style="list-style-type: none"> ■ Usare l'Indicizzatore IDM remoto. ■ Usa percorso locale su Enforce Server ■ Usa condivisione SMB remota

Riferimento a un archivio documenti in Enforce Server

L'opzione **Archivio di riferimento su Enforce Server** consente di creare un indice IDM sulla base di un file ZIP locale di Enforce Server. Utilizzare questa opzione per indicizzare i documenti di origine archiviati in un file ZIP di dimensioni superiori a 50 MB.

Vedere ["Informazioni sull'origine dati del documento"](#) a pagina 573.

Nota: Se il file ZIP ha dimensioni inferiori a 50 MB è invece possibile utilizzare l'opzione **Carica archivio documenti sul server**. Vedere ["Caricamento di un archivio di documenti in Enforce Server"](#) a pagina 591.

Per utilizzare l'opzione **Archivio di riferimento su Enforce Server** copiare il file ZIP nella cartella `\Programmi\Symantec\Data Loss Prevention\Enforce Server\Protect\documentprofiles` sull'host del file system di Enforce Server. Una volta copiato il file ZIP in Enforce Server, è possibile selezionare l'origine documento dal menu a discesa nella schermata **Aggiungi profilo documento**. Vedere ["Creazione e modifica di profili di documento indicizzati"](#) a pagina 588.

Il paragrafo [Per definire un riferimento all'archivio documenti su Enforce Server](#) descrive la procedura per l'utilizzo dell'opzione **Archivio di riferimento su Enforce Server**.

Per definire un riferimento all'archivio documenti su Enforce Server

- 1 Copiare il file ZIP in Enforce Server.
 - In Windows, copiare il file ZIP nella directory `\Programmi\Symantec\Data Loss Prevention\Server Platform Common\15.1\Protect\documentprofiles`
 - In Linux, copiare il file ZIP nella directory `/var/Symantec/DataLossPrevention/Server Platform Common/15.1/documentprofiles`

Vedere [Tabella 23-16](#) a pagina 594.

Nota: Il sistema elimina il file origine dati del documento dopo il completamento del processo di indicizzazione.

- 2 Accedere alla console di amministrazione di Enforce Server.
- 3 Passare alla schermata **Gestisci > Profili dati > Documenti indicizzati > Configura profilo documento**.
- 4 Selezionare il file nel menu a discesa **Archivio di riferimento su Enforce Server**.

Nota: Se un altro **profilo documento indicizzato** fa attualmente riferimento a un'origine documento, questa non compare nell'elenco.

- 5 Specificare uno o più filtri per nomi file o dimensioni file (facoltativo).
Vedere ["Filtraggio di documenti per nome di file"](#) a pagina 599.

- 6 Selezionare una delle opzioni di indicizzazione (facoltativo).
Vedere ["Pianificazione dell'indicizzazione di profili documento"](#) a pagina 602.
- 7 Fare clic su **Salva** per salvare il profilo documento.

Tabella 23-16 Requisiti per utilizzare l'opzione Archivio di riferimento su Enforce Server

Requisito	Descrizione
Solo file ZIP	<p>L'archivio documenti deve essere un file ZIP; nessun altro formato di incapsulamento è supportato per questa opzione.</p> <p>Il file ZIP può avere dimensioni massime pari a 2 GB. Considerare la possibilità di utilizzare una soluzione di terzi (quale Secure FTP) per copiare in modo protetto il file ZIP nel server Enforce Server.</p> <p>Vedere "Informazioni sull'origine dati del documento" a pagina 573.</p>
file secondario non archiviato	<p>Verificare che i file secondari siano adeguati e non incapsulati in un archivio (salvo l'archivio profilo di livello superiore).</p> <p>Vedere "Non comprimere i file nell'origine documento" a pagina 608.</p> <p>Vedere "Mancata indicizzazione di documenti vuoti" a pagina 609.</p>
Solo nomi file UTF-8	<p>Non utilizzare questo metodo se uno dei nomi dei file che si stanno indicizzando contiene caratteri non ASCII.</p> <p>Utilizzare invece una delle seguenti opzioni:</p> <ul style="list-style-type: none"> ■ Usare l'Indicizzatore IDM remoto. ■ Usa percorso locale su Enforce Server Vedere "Utilizzo del percorso locale sul Enforce Server" a pagina 594. ■ Usa condivisione SMB remota Vedere "Utilizzo dell'opzione di condivisione SMB remota per indicizzare le condivisioni di file" a pagina 595.

Utilizzo del percorso locale sul Enforce Server

Il metodo **Usa percorso locale su Enforce Server** consente di indicizzare singoli file locali in Enforce Server. Con questo metodo i file da indicizzare non possono essere archiviati in un file ZIP. Il sistema elimina i documenti dopo il completamento del processo di indicizzazione.

Vedere ["Creazione e modifica di profili di documento indicizzati"](#) a pagina 588.

Per utilizzare il metodo **Usa percorso locale su Enforce Server** per rendere disponibile l'origine documento a Enforce Server per l'indicizzazione, si immette il percorso locale alla directory contenente i documenti da indicizzare. Se ad esempio i file sono stati copiati nel file system nella directory `C:\Documents`, si immetterà **C:\Documents** nel campo dell'opzione

Usa percorso locale su Enforce Server. È necessario specificare il percorso esatto, non un percorso relativo. Non includere i nomi file nel percorso.

Nota: Se i file indicizzati includono un file di dimensioni superiori a 2 GB, il sistema indicizza tutti i file eccetto il file da 2 GB. Ciò è valido solo per l'opzione **Usa percorso locale su Enforce Server**. Non è valido per l'opzione **Archivio di riferimento su Enforce Server**.

Utilizzo dell'opzione di condivisione SMB remota per indicizzare le condivisioni di file

Il metodo **Usa condivisione SMB remota** consente di indicizzare i documenti in remoto con il protocollo Common Internet File System (CIFS). Per utilizzare questo metodo per rendere l'origine del documento disponibile a Enforce Server, immettere il percorso UNC (Universal Naming Convention) per la condivisione SMB (Server Message Block) che contiene i documenti da indicizzare.

Vedere ["Informazioni sull'indicizzazione remota dei documenti"](#) a pagina 574.

Vedere ["Per indicizzare i documenti remoti sulle condivisioni di file con CIFS"](#) a pagina 595. fornisce i passaggi per utilizzare CIFS per indicizzare i documenti remoti.

Nota: Symantec Data Loss Prevention non elimina i documenti dopo l'indicizzazione quando si utilizza l'opzione **Usa condivisione SMB remota**.

Per indicizzare i documenti remoti sulle condivisioni di file con CIFS

- 1 Accedere alla console di amministrazione di Enforce Server.
- 2 Accedere alla schermata **Gestisci > Profili dati > Documenti indicizzati > Configura profilo documento**.
- 3 Selezionare l'opzione **Usa condivisione SMB remota**.
- 4 In **Percorso UNC** immettere il percorso per la condivisione SMB che contiene i documenti da indicizzare.

Un percorso UNC è composto da un nome del server, un nome della condivisione e un percorso di file opzionale, ad esempio: \\server\condivisione\percorso_file.

- 5 Immettere un nome utente e una password validi per la condivisione, quindi immettere di nuovo la password. L'utente specificato deve avere l'accesso generale all'unità condivisa e disporre delle autorizzazioni di lettura per i file costitutivi.

Facoltativamente è possibile selezionare l'opzione **Usa credenziali salvate**. In questo caso le credenziali sono disponibili dal menu a discesa.

Vedere ["Informazioni sull'archivio credenziali"](#) a pagina 167.

- 6 Completare la configurazione del **profilo di documento indicizzato**.

Vedere ["Creazione e modifica di profili di documento indicizzati"](#) a pagina 588.

Utilizzo dell'opzione di condivisione SMB remota per indicizzare i documenti SharePoint

Per indicizzare in remoto i file su SharePoint, esporre la condivisione di file remota con WebDAV. Dopo avere attivato WebDAV per SharePoint, utilizzare l'opzione **Usa condivisione SMB remota** e immettere il percorso UNC per indicizzare i documenti remoti. Symantec Data Loss Prevention supporta l'indicizzazione IDM remota utilizzando le istanze di WebDAV per SharePoint 2007 e SharePoint 2010.

Vedere ["Informazioni sull'indicizzazione remota dei documenti"](#) a pagina 574.

Nota: per indicizzare i documenti su un server SharePoint con l'opzione di condivisione SMB remota, è necessario distribuire Enforce Server su un host con sistema operativo Windows Server supportato. Data Loss Prevention dipende dai servizi Windows NTLM per montare un server WebDAV.

La [Tabella 23-17](#) illustra la procedura per l'indicizzazione remota dei documenti SharePoint con WebDAV.

Tabella 23-17 Indicizzazione dei documenti SharePoint

Passo	Operazione	Descrizione
1	Attivare WebDAV per SharePoint.	Vedere "Attivazione di WebDAV per Microsoft IIS" a pagina 598.
2	Avviare il servizio WebClient.	Dal computer su cui è installato Enforce Server, avviare il servizio WebClient utilizzando la console dei servizi. Se questo servizio è "disattivato", farvi clic sopra con il pulsante destro del mouse e selezionare Proprietà . Attivare il servizio, impostarlo su Manuale , quindi avviarlo . Nota: Per attivare questo servizio, è necessario disporre dei privilegi amministrativi.

Passo	Operazione	Descrizione
3	Accedere all'istanza di SharePoint.	Dal computer su cui è installato Enforce Server, accedere a SharePoint utilizzando il browser e il formato di indirizzo seguente: http://<server_name>:port Ad esempio: http://protect-x64:80
4	Accedere a SharePoint come utente autorizzato.	Non è necessario disporre dei privilegi amministrativi di SharePoint.
5	Individuare i documenti da sottoporre a scansione.	In SharePoint selezionare i documenti di cui si desidera eseguire la scansione. Spesso i documenti SharePoint vengono archiviati nella schermata Home page > Documenti condivisi . È possibile archiviare i documenti in una posizione diversa.
6	Individuare il percorso UNC per i documenti.	In SharePoint, per i documenti che si desidera sottoporre a scansione, selezionare l'opzione Raccolta > Apri con Esplora risorse . Esplora risorse di Windows apre una finestra e visualizza i documenti. Nel campo Indirizzo cercare il percorso per i documenti. Questo indirizzo è il percorso UNC che è necessario per eseguire la scansione dei documenti in remoto. Ad esempio: \\protect-x64\Documenti condivisi. Copiare questo percorso negli Appunti o in un file di testo.
7	Creare l'indice IDM.	Vedere "Creazione e modifica di profili di documento indicizzati" a pagina 588.
8	Configurare l'origine di indicizzazione remota di SharePoint.	Per configurare l'origine di indicizzazione remota: <ul style="list-style-type: none"> ■ Per il campo Origine documento selezionare l'opzione Usa condivisione SMB remota. ■ In Percorso UNC incollare (o immettere) l'indirizzo copiato nel passaggio precedente. Ad esempio: \\protect-x64\Documenti condivisi. ■ In Credenziali utente immettere il nome utente e la password di SharePoint. In alternativa selezionare questi dati dall'elenco a discesa Credenziali salvate. ■ Selezionare l'opzione Invia processo di indicizzazione al salvataggio e fare clic su Salva.
9	Verificare che l'operazione sia riuscita.	Nella schermata Gestisci > Profili dati > Documenti indicizzati si dovrebbe vedere che l'indice è stato creato. Verificare lo "stato" e il numero di documenti indicizzati. Se l'indice è stato creato, è ora possibile utilizzarlo per creare le politiche IDM. Vedere "Risoluzione dei problemi di indicizzazione dei documenti SharePoint" a pagina 598.

Attivazione di WebDAV per Microsoft IIS

Esistono vari metodi per attivare WebDAV per IIS. Di seguito è descritto un approccio per Windows Server 2008 R2. Questo approccio viene fornito esclusivamente a titolo esemplificativo. L'approccio e l'ambiente possono differire.

Le distribuzioni di Microsoft IIS che ospitano le istanze di SharePoint possono essere attivate per accettare le connessioni di WebDAV dei client Web.

Vedere ["Utilizzo dell'opzione di condivisione SMB remota per indicizzare i documenti SharePoint"](#) a pagina 596.

Per attivare WebDAV per SharePoint

- 1 Accedere al sistema di SharePoint in cui si desidera attivare WebDAV.
- 2 Aprire la console di Gestione IIS (Internet Information Services).
- 3 Selezionare il nome del server nell'albero IIS.
- 4 Espandere l'albero, fare clic sulla cartella **Siti Web** ed espanderla.
- 5 Selezionare l'istanza di SharePoint dall'elenco.
- 6 Fare clic con il pulsante destro del mouse sull'istanza di SharePoint e selezionare **Nuovo > Directory virtuale**.
- 7 Viene visualizzata la Creazione guidata Directory virtuale. Fare clic su **Avanti**.
- 8 Immettere un nome nel campo **Alias** (ad esempio "WebDAV") e fare clic su **Avanti**.
- 9 Immettere un percorso di directory nel campo **Directory contenuto sito Web**. Può essere qualsiasi percorso di directory a condizione che esista. Fare clic su **Avanti**.
- 10 Selezionare **Accesso in lettura** e fare clic su **Avanti**.
- 11 Fare clic su **Fine**.
- 12 Fare clic con il pulsante destro del mouse sulla directory virtuale creata e selezionare **Proprietà**.
- 13 Nella scheda **Directory virtuale** selezionare l'opzione "Reindirizzamento a un URL" e fare clic su **Crea**. Il nome dell'alias viene inserito nel campo **Nome applicazione**.
- 14 Immettere l'URL del sito di SharePoint nel campo "Reindirizza a" e fare clic su **OK**. WebDAV è ora attivato per questa istanza di SharePoint.

Risoluzione dei problemi di indicizzazione dei documenti SharePoint

Se non è possibile connettere il computer Enforce Server al computer SharePoint Server dopo l'attivazione di WebDAV, verificare di aver avviato il servizio WebClient nel computer Enforce Server. È necessario avviare questo servizio e verificare la connessione WebDAV prima di configurare l'indicizzazione IDM.

Vedere ["Utilizzo dell'opzione di condivisione SMB remota per indicizzare i documenti SharePoint"](#) a pagina 596.

Se si prevede di reindicizzare periodicamente i documenti SharePoint man mano che vengono aggiornati, può risultare utile mappare la risorsa di rete remota sul computer locale in cui è installato Enforce Server. È possibile utilizzare il comando "net use" di MS-DOS per mappare SharePoint mediante il percorso UNC. Ad esempio:

- `net use`
Questo comando senza parametri recupera e visualizza un elenco di connessioni di rete.
- `net use s: \\sharepoint_server\Shared Documents`
Questo comando assegna (mappa) il server SharePoint sull'unità "S" locale.
- `net use * \\sharepoint_server\Shared Documents`
Questo comando assegna (mappa) il server SharePoint sulla lettera di unità disponibile successiva.
- `net use s: /delete`
Questo comando rimuove il mapping di rete sull'unità specificata.

Filtraggio di documenti per nome di file

Quando si configura un profilo documenti indicizzati, è possibile utilizzare dei filtri per includere o escludere dall'indicizzazione documenti nell'origine dati. Sono presenti due tipi di filtri di nomi di file: filtri di inclusione nome file e filtri di esclusione nome file. Se si sceglie di utilizzare i filtri di nome di file Symantec consiglia di selezionare filtri di inclusione o esclusione, ma non entrambi.

Vedere ["Escludere documenti dall'indicizzazione per ridurre i falsi positivi."](#) a pagina 611.

[Tabella 23-18](#) descrive le differenze tra filtri di inclusione e di esclusione per nomi di file.

Tabella 23-18 Filtri di nome file distinti

Filtro	Descrizione
Filtri di inclusione nome file	<p>Se il campo Filtri di inclusione nome file è vuoto, la corrispondenza viene eseguita per tutti i documenti nel profilo documenti. Qualsiasi inserimento all'interno del campo Filtri di inclusione nome file viene trattato come un filtro di inclusione. In questo caso il documento viene indicizzato solo se corrisponde al filtro specificato.</p> <p>Ad esempio, se si immette *.docx nel campo Filtri di inclusione nome file, il sistema indicizza solo i file *.docx nell'origine documenti.</p>

Filtro	Descrizione
Filtri di esclusione nome file	<p>Il campo Filtri di esclusione consente di specificare i documenti da escludere nel processo di corrispondenza.</p> <p>Se si lascia vuoto il campo Filtri di esclusione, il sistema ricerca la corrispondenza in tutti i documenti nel file ZIP o nella condivisione file. Se si immette un qualsiasi valore nel campo, il sistema sottopone a scansione solo i documenti non corrispondenti al filtro.</p>

Il sistema tratta le barre dritte (/) e rovesciate (\) come equivalenti. Il sistema ignora all'inizio gli spazi vuoti all'inizio o alla fine del criterio. Il filtraggio del nome file non supporta i caratteri escape, pertanto non è possibile cercare una corrispondenza per punti interrogativi, virgole o asterischi.

[Tabella 23-19](#) descrive la sintassi accettata dalla funzionalità **Filtri di nome file**. La sintassi per i filtri di inclusione ed esclusione è la stessa.

Tabella 23-19 Sintassi di filtraggio dei nomi di file

Operatore	Descrizione
Asterisco (*)	Rappresenta qualsiasi numero di caratteri.
Punto interrogativo (?)	Rappresenta un singolo carattere.
Virgola (,) e nuova linea	Corrisponde a un OR logico.

[Tabella 23-20](#) fornisce filtri e descrizioni campione di comportamento, se vengono immessi nel campo **Filtri di inclusione nome file** :

Tabella 23-20 Esempi di filtro del nome di file

Stringa di filtro	Descrizione
<code>*.txt, *.docx</code>	Il sistema indicizza solo i file .txt e .docx nel file zip o nella condivisione file, ignorando tutto il resto.
<code>?????.docx</code>	Il sistema indicizza i file con estensione .docx e file con i nomi di cinque caratteri, come <code>hello.docx</code> e <code>stats.docx</code> , ma non <code>good.docx</code> o <code>marketing.docx</code> .
<code>*/documentation/*, */specs/*</code>	Il sistema indicizza solo i file in due sottodirectory sotto alla directory principale, una chiamata "documentation" e l'altra "specs".

Stringa di filtro	Descrizione
<p>Esempio caratteri jolly e sottodirectory:</p> <pre>*\scan_dir\1*.txt</pre>	<p>L'indicizzazione IDM non riesce o ignora l'impostazione del filtro se la stringa del filtro di inclusione/esclusione del nome del file inizia con un carattere jolly, ad esempio: 1*.txt. La soluzione alternativa consiste nel configurare il filtro di inclusione/esclusione con la stringa del filtro come indicato in questo esempio, cioè *\scan_dir\1*.txt.</p> <p>Ad esempio, il filtro 1*.txt non funziona per un percorso di file \\dlp.symantec.com\scan_dir\lincoln-LyceumAddress.txt. Tuttavia, se il filtro è configurato come *\scan_dir\1*.txt, l'indicizzatore riconosce il filtro e indicizza il file.</p>

Filtraggio di documenti per dimensioni file

I filtri consentono di specificare i documenti da includere o escludere dall'indicizzazione. I tipi di filtri sono i filtri di inclusione nome file, i filtri di esclusione nome file e i filtri dimensioni file. I filtri di dimensioni file consentono escludere file dal processo di corrispondenza in base alla loro dimensione. Tutti i file che corrispondono ai filtri di dimensioni file vengono ignorati.

Vedere ["Filtraggio di documenti per nome di file"](#) a pagina 599.

Nei campi **Filtri dimensioni**, specificare tutte le restrizioni relative alle dimensioni file che il sistema dovrà indicizzare. In generale è consigliabile usare solo un tipo di filtro dimensioni file.

Vedere ["Escludere documenti dall'indicizzazione per ridurre i falsi positivi."](#) a pagina 611.

La [Tabella 23-21](#) descrive le opzioni del filtro dimensioni file.

Tabella 23-21 Opzioni di configurazione del filtro dimensioni file

Filtro	Descrizione
Ignora file di dimensioni inferiori a	<p>Per escludere i file più piccoli di determinate dimensioni:</p> <ul style="list-style-type: none"> ■ Immettere un numero nel campo Ignora file di dimensioni inferiori a. ■ Selezionare l'unità di misura Byte, KB (kilobyte) o MB (megabyte) dall'elenco a discesa. <p>Ad esempio, per impedire l'indicizzazione di file di dimensioni inferiori a un kilobyte (), immettere 11 nel campo e selezionare KB nell'elenco a discesa corrispondente.</p>

Filtro	Descrizione
Ignora file di dimensioni superiori a	<p>Per escludere i file più grandi di determinate dimensioni:</p> <ul style="list-style-type: none"> ■ Immettere un numero nel campo Ignora file di dimensioni superiori a. ■ Selezionare quindi l'unità di misura appropriata (byte, KB o MB) dall'elenco a discesa. <p>Ad esempio, per impedire l'indicizzazione di file di dimensioni superiori a due megabyte (KB), immettere 22 nel campo e selezionare MB nell'elenco a discesa corrispondente.</p>

Pianificazione dell'indicizzazione di profili documento

Quando si configura un profilo documento, selezionare **Invia processo di indicizzazione al salvataggio** per indicizzare il profilo documento non appena viene salvato. In alternativa, è possibile configurare una pianificazione per l'indicizzazione del documento di origine.

Per pianificare l'indicizzazione del documento, selezionare **Invia processo di indicizzazione secondo pianificazione** e selezionare una pianificazione dall'elenco a discesa come descritto in [Tabella 23-22](#).

Nota: Enforce Server può indicizzare un solo profilo documento alla volta. Se un processo d'indicizzazione è pianificato per cominciare mentre un altro è in esecuzione, il nuovo processo non inizia fino a che il primo non viene completato.

Tabella 23-22 Opzioni per la pianificazione dell'indicizzazione di profili documento

Parametro	Descrizione
Una volta	<p>Il - Immettere la data per l'indicizzazione del profilo documento nel formato MM/GG/AA. È anche possibile fare clic sul widget data e selezionare una data.</p> <p>Alle - Selezionare l'ora di inizio dell'indicizzazione.</p>
Ogni giorno	<p>Alle - Selezionare l'ora di inizio dell'indicizzazione.</p> <p>Fino a - Selezionare questa casella di controllo per specificare la data di arresto dell'indicizzazione nel formato MM/GG/AA. È anche possibile fare clic sul widget data e selezionare una data.</p>
Ogni settimana	<p>Giorno della settimana - Selezionare i giorni in cui indicizzare il profilo documento.</p> <p>Alle - Selezionare l'ora di inizio dell'indicizzazione.</p> <p>Fino a - Selezionare questa casella di controllo per specificare la data di arresto dell'indicizzazione nel formato MM/GG/AA. È anche possibile fare clic sul widget data e selezionare una data.</p>

Parametro	Descrizione
Ogni mese	<p>Giorno - Immettere il numero del giorno di ogni mese in cui eseguire l'indicizzazione. Il valore deve essere tra 1 e 28.</p> <p>Alle - Selezionare l'ora di inizio dell'indicizzazione.</p> <p>Fino a - Selezionare questa casella di controllo per specificare la data di arresto dell'indicizzazione nel formato MM/GG/AA. È anche possibile fare clic sul widget data e selezionare una data.</p>

Modifica delle proprietà predefinite dell'indicizzatore

L'indice del server contiene l'impronta MD5 di ogni file che è stato indicizzato: contenuto binario non elaborato o contenuto estratto esatto se il contenuto del file può essere estratto e hash di passaggi distinti di contenuto.

Vedere ["Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali"](#) a pagina 579.

La dimensione dei passaggi dipende dall'impostazione `low_threshold_k` nel file delle proprietà dell'indicizzatore (`\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\indexer.properties`). Generalmente non è necessario modificare le impostazioni predefinite. Quando si abbassa il minimo predefinito, Enforce Server crea hash a partire da sezioni più piccole dei documenti indicizzati.

Le impostazioni predefinite si applicano anche al file `Whitelisted.txt`. Se la quantità di contenuto necessaria per la lista bianca è inferiore alla quantità minima richiesta per la corrispondenza parziale, è possibile regolare l'impostazione minima predefinita.

Per modificare il minimo predefinito per il testo nella lista bianca

- 1 Sull'host di Symantec Data Loss Prevention, accedere alla directory `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` in Windows o `/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config` in Linux.
- 2 Utilizzare un editor di testo per aprire il file `Indexer.properties`
- 3 Individuare il parametro `low_threshold_k`:
`low_threshold_k=50`

- 4 Modificare la parte numerica del valore del parametro per riflettere il numero minimo desiderato di caratteri consentiti in `Whitelisted.txt`.

Ad esempio, per modificare il minimo e impostarlo su 30 caratteri, modificare il valore in modo che abbia l'aspetto seguente:

```
low_threshold_k=30
```

Il valore di questo parametro deve corrispondere con il valore `min_normalized_size`. L'impostazione predefinita per `min_normalized_size` è 50.

- 5 Salvare il file.

Per ulteriori informazioni sulla configurazione e sulla personalizzazione dell'IDM, vedere l'articolo "Understanding IDM configuration and customization" all'indirizzo <http://www.support.symantec.com/doc/TECH234899> nel centro di supporto Symantec.

Attivazione dell'IDM dell'agente

Attivare l'IDM con corrispondenza esatta e parziale sull'endpoint Windows impostando il parametro di configurazione avanzata dell'agente `Detection.TWO_TIER_IDM_ENABLED.str` su **OFF**. Dopo avere disattivato il rilevamento in due fasi, DLP Agent cerca la corrispondenza esatta e parziale di file e di contenuti di file, presupponendo che si sia generato l'indice endpoint.

Nota: la distribuzione in due fasi non è supportata sull'agente Mac.

Vedere "[Creazione e modifica di profili di documento indicizzati](#)" a pagina 588.

Per le nuove installazioni, l'IDM con corrispondenza esatta e parziale sull'endpoint è l'impostazione predefinita per la configurazione dell'agente endpoint predefinita (`TWO_TIER_IDM_ENABLED = OFF`). Non è necessario attivarla.

Per i sistemi aggiornati, l'IDM con corrispondenza esatta e parziale sull'endpoint è disattivata (`TWO_TIER_IDM_ENABLED = ON`), quindi non vi è alcuna modifica di funzionalità per le politiche IDM esistenti distribuite all'endpoint. Se si desidera utilizzare l'IDM con corrispondenza esatta sull'endpoint dopo l'upgrade, è necessario disattivare il rilevamento in due fasi e reindicizzare l'origine dati di ogni documento.

Vedere "[Per attivare o disattivare il rilevamento in due fasi](#)" a pagina 604.

Per attivare o disattivare il rilevamento in due fasi

- 1 Accedere alla console di amministrazione di Enforce Server.
- 2 Selezionare **Sistema > Agenti > Configurazione agente**.
- 3 Selezionare la configurazione dell'agente applicabile.
- 4 Selezionare la scheda **Impostazioni agente avanzate**.

- 5 Individuare il parametro `Detection.TWO_TIER_IDM_ENABLED.str.`
- 6 Modificare il valore e impostarlo su "ON" oppure "OFF" (senza distinzione tra maiuscole e minuscole) a seconda dei requisiti.
Vedere [Tabella 23-23](#) a pagina 605.
- 7 Fare clic su **Salva** nella parte superiore della pagina per salvare le modifiche.
- 8 Applicare la configurazione dell'agente al gruppo o ai gruppi di agenti.
Vedere ["Applicazione di configurazioni agente a un gruppo di agenti"](#) a pagina 2179.

Tabella 23-23 Impostazioni avanzate dell'agente per l'IDM con corrispondenza esatta sull'endpoint

Parametro Impostazioni agente avanzate	Valore	Impostazione predefinita	Motore di rilevamento	Tipo di corrispondenza
<code>Detection.TWO_TIER_IDM_ENABLED.str</code>	OFF	Nuova installazione 14.6 o upgrade del sistema da 12.5.	DLP Agent	File esatto Contenuti di file parziali
	ON	Upgrade del sistema da 12.0.x	Endpoint Server	File esatto Contenuti di file esatti Contenuti di file parziali

Stima dell'utilizzo di memoria dell'endpoint per Agent IDM

DLP 14.6 utilizza circa il 20% di memoria in meno rispetto a DLP 14.0 per la corrispondenza parziale con i profili di documento IDM. Per la corrispondenza parziale DLP richiede circa 2 KB di RAM per file, ovvero circa 60 MB per 30.000 file per l'agente. Per la sola corrispondenza esatta, DLP richiede circa 40 byte per file.

Vedere ["Informazioni sui file di indice del server e i file di indice dell'agente"](#) a pagina 575.

Configurazione della condizione di politica Contenuto corrispondente a firma documento

La condizione **Il contenuto corrisponde alla firma del documento di** corrisponde al contenuto del documento non strutturato basato sul profilo di documenti indicizzati. La condizione **Il contenuto corrisponde alla firma del documento di** è disponibile per le regole e le eccezioni di rilevamento.

Vedere ["Informazioni sull'utilizzo della condizione Contenuto corrispondente a firma documento"](#) a pagina 581.

Per configurare la condizione Contenuto corrispondente a firma documento

- 1 Aggiungere una condizione IDM a una regola o eccezione di politica o modificarne una esistente.
Vedere ["Configurazione di politiche"](#) a pagina 422.
Vedere ["Configurazione di regole di politica"](#) a pagina 427.
Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.
- 2 Configurare i parametri della condizione IDM.
Vedere [Tabella 23-24](#) a pagina 606.
- 3 Salvare la configurazione della politica.

Tabella 23-24 Parametri della condizione Contenuto corrispondente a firma documento

Azione	Descrizione
Impostare l'esposizione minima del documento.	<p>Selezionare un'opzione dall'elenco a discesa.</p> <p>Scegliere Esatto per cercare la corrispondenza esatta dei contenuti del documento.</p> <p>Scegliere una percentuale compresa tra il 10% e il 90% per cercare la corrispondenza parziale dei contenuti del documento.</p>
Configurare il conteggio delle corrispondenze.	<p>Selezionare il metodo di conteggio delle corrispondenze:</p> <ul style="list-style-type: none"> ■ Verificare esistenza Segnala un numero di corrispondenze pari a 1 se esistono una o più condizioni corrispondenti. ■ Conta tutte le corrispondenze Segnala il numero esatto di corrispondenze. <p>Vedere "Configurazione del conteggio delle corrispondenze" a pagina 431.</p>
Selezionare i componenti per la corrispondenza.	<p>Selezionare uno dei componenti del messaggio disponibili per la corrispondenza:</p> <ul style="list-style-type: none"> ■ Corpo - Contenuto del messaggio. ■ Allegati - Qualsiasi file allegato al messaggio o inoltrato dallo stesso. <p>Vedere "Selezione dei componenti per la corrispondenza" a pagina 433.</p>
Configurare condizioni aggiuntive per Confronta anche.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere soddisfatte per attivare o escludere una corrispondenza.</p> <p>È possibile aggiungere qualsiasi condizione disponibile dal menu a discesa.</p>

Azione	Descrizione
Testare e ottimizzare la politica.	Vedere "Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze" a pagina 466. Vedere "Utilizzo di regole IDM parallele per ottimizzare le soglie di corrispondenze" a pagina 614. Vedere "Risoluzione dei problemi delle politiche" a pagina 458.

Best practice per l'utilizzo di IDM

Indexed Document Matching (IDM) protegge il contenuto e le immagini dei documenti. IDM si basa su un indice di documenti con impronta per definire corrispondenze di contenuto basate sul testo parziali e derivative. Inoltre è possibile usare IDM per definire la corrispondenza esatta dei documenti in base all'impronta binaria, inclusi non solo i documenti di testo ma anche i documenti grafici e multimediali.

Grazie alla vasta gamma di corrispondenze supportate da IDM, è consigliabile tenere in considerazione le best practice di questa sezione per implementare le politiche IDM che consentono di definire la corrispondenza esatta con i dati che si desidera proteggere.

[Tabella 23-25](#) riassume le considerazioni IDM discusse in questa sezione, con collegamenti ai singoli argomenti per ciascuna considerazione.

Tabella 23-25 Best practice per la politica IDM

Considerazioni	Descrizione
Reindicizzare i profili IDM dopo l'aggiornamento.	Vedere "Reindicizzazione dei profili IDM dopo un upgrade importante" a pagina 608.
Non comprimere i documenti dei quali si desidera acquisire l'impronta del contenuto.	Vedere "Non comprimere i file nell'origine documento" a pagina 608.
Preferire la corrispondenza parziale alla corrispondenza esatta per DLP Agent.	Vedere "Preferenza della corrispondenza parziale alla corrispondenza esatta con DLP Agent" a pagina 609.
Non indicizzare i documenti di testo senza contenuto.	Vedere "Mancata indicizzazione di documenti vuoti" a pagina 609.
Tenere presenti le limitazioni della corrispondenza esatta.	Vedere "Informazioni sulle limitazioni della corrispondenza esatta" a pagina 610.
Utilizzare la lista bianca per escludere contenuti file parziali dalla corrispondenza e per ridurre i falsi positivi.	Vedere "Utilizzare la lista bianca per escludere il contenuto non sensibile dalla corrispondenza parziale" a pagina 611.

Considerazioni	Descrizione
Escludere i documenti non critici dall'indicizzazione per ridurre i falsi positivi.	Vedere "Escludere documenti dall'indicizzazione per ridurre i falsi positivi." a pagina 611.
Cambiare la dimensione massima dell'indice per indicizzare più di 1.000.000 di documenti.	Vedere "Creazione di profili separati per indicizzare origini di documenti di grandi dimensioni" a pagina 613.
Utilizzare l'indicizzazione remota per gli insiemi di documenti grandi.	Vedere "Indicizzazione EDM remota" a pagina 615.
Utilizzare l'indicizzazione pianificata per automatizzare gli aggiornamenti di profilo.	Vedere "Utilizzo dell'indicizzazione pianificata per tenere aggiornati i profili" a pagina 613.
Utilizzare più regole IDM in parallelo per definire e adattare soglie di corrispondenza.	Vedere "Utilizzo di regole IDM parallele per ottimizzare le soglie di corrispondenze" a pagina 614.

Reindicizzazione dei profili IDM dopo un upgrade importante

È necessario aggiornare tutti i profili IDM. A questo scopo reindicizzare ogni origine dati associata dopo un upgrade importante di Symantec Data Loss Prevention.

Se si è eseguito l'aggiornamento a Symantec Data Loss Prevention 15.1 e si desidera utilizzare l'IDM con corrispondenza parziale sull'endpoint per le politiche IDM esistenti, è necessario reindicizzare l'origine dati per ciascun profilo di documento indicizzato in modo che ogni indice endpoint venga generato e distribuito ai DLP Agent.

Se si è eseguito l'upgrade a Data Loss Prevention 15.1 e non si utilizza Agent IDM, non è necessario reindicizzare le origini dati, ma è consigliato farlo.

Vedere ["Attivazione dell'IDM dell'agente"](#) a pagina 604.

Non comprimere i file nell'origine documento

Per i formati di file il cui contenuto può essere estratto, il processo di indicizzazione del server apre il documento, estrae il contenuto di testo e contrassegna i dati nel complesso e nelle varie parti (sezioni). Tuttavia, il processo di indicizzazione non può ispezionare in modo ricorsivo gli archivi documenti inclusi nel set di documenti. Se un documento di cui si desidera indicizzare i contenuti file è compresso in un file di archiviazione (ad esempio un file ZIP, RAR, o TAR) nell'origine dati del documento, il sistema non è in grado di estrarre i contenuti dal file e indicizzare i contenuti stessi. In tal caso il sistema registra solo un hash crittografico della firma del file binario. Il file incorporato viene considerato solo per le corrispondenze esatte di file, ad esempio per i file immagine e altri formati di file non supportati.

Questo comportamento è specifico per il processo di indicizzazione in fase di realizzazione. In fase di runtime il server di rilevamento ispeziona in modo ricorsivo gli archivi di documenti

ed estrae il testo o i file contenuti in tali archivi. Tuttavia per valutare tale contenuto l'indice IDM deve essere stato in grado di indicizzare tutti i file di contenuto.

La best practice consiste nell'evitare di includere in un archivio documenti (file compresso) qualsiasi file del quale si desidera indicizzare il contenuto. L'unica eccezione è il file ZIP dell'archivio documenti che si carica o copia in Enforce Server e contiene l'intero set di documenti. Tutti i file inclusi nel file contenitore devono essere non compressi. Se l'archivio documenti caricato in Enforce Server per l'indicizzazione contiene uno o più file archivio incorporati (ad esempio un file ZIP), il sistema esegue una corrispondenza binaria esatta con tutti i file contenuti nel file archivio incorporato

Vedere ["Creazione e modifica di profili di documento indicizzati"](#) a pagina 588.

Mancata indicizzazione di documenti vuoti

È necessario prestare attenzione ai documenti che si indicizzano. In particolare evitare di indicizzare documenti vuoti.

Ad esempio, l'indicizzazione di un file PPTX che comprende solo fotografie o altro contenuto grafico, ma nessun contenuto di testo corrisponde esattamente ad altri file PPTX vuoti e genera falsi positivi. In questo caso, anche se un file PPTX non contiene alcun testo immesso dall'utente, contiene segnaposti di intestazioni e piè di pagina che il sistema estrae come contenuto di file. Poiché il testo estratto e normalizzato contiene più di 50 caratteri diversi dallo spazio, il sistema tratta il file come non binario e crea un hash crittografico di tutti i contenuti del file. Di conseguenza tutti gli altri file PPTX vuoti generano corrispondenze esatte dei contenuti di file perché il MD5 risultante del contenuto estratto è lo stesso.

Nota: questo comportamento non è stato osservato con i file XLSX. In altre parole i falsi positivi non vengono creati se i file vuoti sono diversi.

Vedere ["Utilizzo dell'IDM per rilevare i contenuti di file esatti e parziali"](#) a pagina 579.

Preferenza della corrispondenza parziale alla corrispondenza esatta con DLP Agent

Se si stanno distribuendo politiche IDM all'endpoint, si consiglia l'IDM con corrispondenza parziale. Il vantaggio principale dell'IDM con corrispondenza parziale sull'endpoint è che la corrispondenza è veloce perché viene cercata localmente dall'agente invece che in remoto dal server. Inoltre l'IDM con corrispondenza parziale consente di utilizzare le regole di risposta direttamente sull'endpoint.

Vedere ["Tipi di rilevamento IDM"](#) a pagina 571.

Informazioni sulle limitazioni della corrispondenza esatta

Secondo la corrispondenza esatta, i dati in entrata devono corrispondere all'impronta MD5 di una firma di un file binario o di una corrispondenza esatta di contenuti di file estratti e normalizzati. .

Vedere ["Metodi di corrispondenza supportati da IDM"](#) a pagina 570.

Quando si implementa l'IDM con corrispondenza esatta sul server, si consideri quanto riportato di seguito:

- Le liste bianche sono valide solo per la corrispondenza di contenuti di file parziale.
- Per i file binari e i file basati su testo inseriti nel motore di rilevazione per la corrispondenza di file esatta, ai fini dell'ottimizzazione il sistema verifica la dimensione in byte del file prima di calcolare MD5 runtime per il confronto con l'indice. Se le dimensioni in byte del file non corrispondono, non viene eseguito alcun confronto degli hash di crittografia.
- Per il tipo di file non viene mai verificata la corrispondenza di file o di contenuti di file esatta.
- Alcuni formati di file cambiano la dimensione in byte di un file se questo viene aperto nell'applicazione nativa e quindi salvato senza modifiche. Ne risulta che il file non corrisponde esattamente. Ad esempio, se si apre un file, quale un'immagine JPEG, con Visualizzatore immagini e fax per Windows e si salva il file senza apportare modifiche, la dimensione binaria del file risulta comunque alterata. Il risultato è una mancata corrispondenza esatta.
- Per alcune applicazioni, l'operazione di stampa di Windows può modificare i dati del file in modo che i contenuti estratti non corrispondano esattamente. Tra i tipi di file noti interessati da questa operazione figurano i documenti di Microsoft Office.

La [Tabella 1](#) elenca alcune limitazioni note della corrispondenza di contenuto esatta. Questa lista non è esauriente. Possono esservi altri formati di file che cambiano al momento del nuovo salvataggio.

Tabella 1 Limitazioni della corrispondenza di contenuti di file esatta

Tipo di file	Applicazione	Risultato al nuovo salvataggio
dwg	AutoCAD 2012	Non corrisponde
jpeg	Visualizzatore immagini e fax per Windows	Non corrisponde
doc	Microsoft Office Word 2007	Non corrisponde
xls	Microsoft Excel 2007	Non corrisponde
ppt	Microsoft Presentation 2007	Non corrisponde
pdf	Adobe Acrobat 9 Pro	Non corrisponde

Tipo di file	Applicazione	Risultato al nuovo salvataggio
docx	Microsoft Office Word 2007	Corrisponde
xlsx	Microsoft Excel 2007	Corrisponde
pptx	Microsoft Presentation 2007	Corrisponde

Utilizzare la lista bianca per escludere il contenuto non sensibile dalla corrispondenza parziale

Mediante la lista bianca è possibile escludere dalla corrispondenza parti del contenuto dei file. Utilizzare la lista bianca per escludere dalla corrispondenza intestazioni, piè di pagina e boilerplate, riducendo così i falsi positivi. Le informazioni contenute nelle intestazioni e nei piè di pagina dei documenti possono dare origine a falsi positivi. Inoltre i testi boilerplate, quali paragrafi standard e contenuti corporativi non privati che vengono ripetuti spesso nei documenti riservati, possono causare falsi positivi.

Per risultati ottimali sarebbe utile rimuovere le intestazioni e i piè di pagina dai documenti prima di indicizzarli. Tuttavia ciò può non risultare fattibile, specie se si ha un grande insieme di documenti. Come best practice, è consigliabile aggiungere a una lista bianca il contenuto di intestazioni, più di pagina e boilerplate in modo da escludere tali contenuti quando viene generato l'indice del server. Grazie alle liste bianche è in genere possibile ridurre l'impostazione **Esposizione minima documento** nella politica senza riscontrare un aumento dei falsi positivi, perché una quantità maggiore del contenuto indicizzato corrisponderà a dati riservati, anziché a testo comune e ripetute.

Nota: Le liste bianche non sono valide per le corrispondenze di tipo File esatto o Contenuto file esatto.

Vedere ["Informazioni sull'aggiunta del contenuto file parziale a una lista bianca"](#) a pagina 582.

Vedere ["Creazione di una lista bianca di contenuto di file da escludere dalla corrispondenza parziale"](#) a pagina 585.

Escludere documenti dall'indicizzazione per ridurre i falsi positivi.

Quando si configura un profilo documenti indicizzati, è possibile utilizzare filtri per includere o escludere dall'indicizzazione documenti presenti nell'origine dati. Sono disponibili due tipi di filtri: nome file e dimensione file.

Vedere ["Creazione e modifica di profili di documento indicizzati"](#) a pagina 588.

I filtri consentono di escludere dall'indicizzazione i documenti non critici e di garantire che l'indice protegga solo i file e i contenuti riservati. I filtri contribuiscono a ridurre i falsi positivi e le dimensioni dell'indice IDM.

Vedere ["Mancata indicizzazione di documenti vuoti"](#) a pagina 609.

La best practice consiste nell'utilizzare un filtro di esclusione o di inclusione per ciascuno tipo di filtro, ma non entrambi. Ad esempio, potrebbe non essere necessario indicizzare tutti i file inclusi in un archivio documenti o resi disponibili al sistema mediante condivisione file. In tal caso, è possibile enumerare i file da includere (filtro di inclusione) o elencare i tipi di file da escludere (filtro di esclusione) dall'indicizzazione, ma non utilizzare entrambe le soluzioni. È anche possibile utilizzare i filtri dimensione file per impostare una soglia di inclusione o esclusione dall'indice.

Vedere ["Filtraggio di documenti per nome di file"](#) a pagina 599.

Vedere ["Filtraggio di documenti per dimensioni file"](#) a pagina 601.

Distinzione delle eccezioni IDM dalla lista bianca e dal filtro

La lista bianca consente di escludere i contenuti di file parziali dalla corrispondenza. Il filtro consente di escludere documenti specifici dal processo di indicizzazione. Le eccezioni IDM, d'altra parte, consentono di escludere i file indicizzati dalla corrispondenza esatta in fase di runtime.

Utilizzare la condizione IDM come eccezione di politica per escludere i file dal rilevamento. Per essere escluso dalla corrispondenza, un file in entrata deve essere una corrispondenza esatta con un file nell'indice IDM. Non è possibile utilizzare le eccezioni IDM per escludere il contenuto dalla corrispondenza. Per escludere il contenuto, è necessario includerlo nella lista bianca.

Nota: la lista bianca non è disponibile per la corrispondenza esatta di file o contenuti di file. È solo disponibile per la corrispondenza parziale di contenuto.

Tabella 23-27 Distinzione tra lista bianca, filtri ed eccezioni

Configurazione IDM	Utilizzo
Eccezione	Esclusione del file esatto dalla corrispondenza Ad esempio, il modello di politica CAN-SPAM Act utilizza un'eccezione IDM.
Lista bianca	Esclusione dei contenuti di file dalla corrispondenza Vedere "Utilizzare la lista bianca per escludere il contenuto non sensibile dalla corrispondenza parziale" a pagina 611.

Configurazione IDM	Utilizzo
Filtro	Inclusione o esclusione dei file dall'indicizzazione Vedere "Escludere documenti dall'indicizzazione per ridurre i falsi positivi." a pagina 611.

Creazione di profili separati per indicizzare origini di documenti di grandi dimensioni

Il rilevamento IDM si basa su un profilo di documento indicizzato. La dimensione massima di un singolo profilo IDM nella RAM è 2 GB. Questo limite di dimensione massimo si basa sul numero complessivo di documenti indicizzati. A seconda della dimensione dei file origine effettivi e della dimensione di testo estratto, ciò si traduce in circa 1.000.000 di file. È possibile modificare la dimensione massima di 2 GB di un indice di un singolo profilo IDM nel file `indexer.properties` con `com.vontu.profiles.documents.maxIndexSize`.

Vedere ["Informazioni sull'origine dati del documento"](#) a pagina 573.

Se è necessario indicizzare oltre 1.000.000 di file, si consiglia di organizzare i documenti in file ZIP o directory di condivisione separati. È necessario creare un profilo di documento indicizzato distinto per ogni singolo set di documenti. Quindi è possibile definire regole separate che facciano riferimento a ciascun indice e aggiungere le regole a una o più politiche.

Utilizzo di WebDAV o CIFS per indicizzare le origini dati di documenti remoti

Per insiemi di documenti più piccoli (fino a 50 MB) è possibile caricare i file in Enforce Server. Per gli insiemi di documenti più grandi, considerare l'utilizzo di FTP Secure per caricare i file in Enforce Server.

In alternativa, è possibile indicizzare remotamente i documenti archiviati in una condivisione di file che supporta il protocollo CIFS o su un server Web che supporta il protocollo WebDAV, quale Microsoft SharePoint o OpenText Livelink

Vedere ["Informazioni sull'indicizzazione remota dei documenti"](#) a pagina 574.

Utilizzo dell'indicizzazione pianificata per tenere aggiornati i profili

È possibile usare la pianificazione indici per tenere aggiornati i profili IDM. L'indice iniziale esegue la scansione di tutti i documenti da indicizzare. Qualsiasi indice successivo esegue la scansione delle sole differenze. È necessario programmare l'indicizzazione fuori dagli orari di esercizio normali per ridurre i potenziali effetti sulle prestazioni del sistema.

Vedere ["Pianificazione dell'indicizzazione di profili documento"](#) a pagina 602.

Prima di configurare un'indicizzazione pianificata, tenere presenti i seguenti consigli:

- Se le origini documento vengono aggiornate solo occasionalmente (ad esempio meno di una volta al mese), non è necessario creare una pianificazione. Indicizzare il documento ogni volta che lo si aggiorna.
- Pianificare l'indicizzazione negli orari di utilizzo minimo del sistema. L'indicizzazione ha effetto sulle prestazioni dell'intero sistema Symantec Data Loss Prevention e l'indicizzazione di documenti grandi può richiedere tempo.
- Indicizzare un documento subito dopo la modifica del profilo di documento corrispondente e ripeterne l'indicizzazione ogni volta che lo si aggiorna. Ad esempio, considerare una situazione per cui ogni mercoledì alle 2.00 si aggiorna un documento. In tal caso la programmazione del processo di indicizzazione ogni mercoledì alle 3.00 è ottimale. La pianificazione quotidiana dell'indicizzazione di documenti non è consigliata perché è troppo frequente e può compromettere le prestazioni del server.
- Controllare i risultati e modificare la pianificazione dell'indicizzazione di conseguenza. Se le prestazioni sono soddisfacenti e si desiderano aggiornamenti più tempestivi, programmare aggiornamenti e indicizzazioni più frequenti.
- Symantec Data Loss Prevention esegue l'indicizzazione incrementale. Quando una condivisione o una directory già sottoposta a indicizzazione in precedenza viene indicizzata di nuovo, vengono indicizzati solo i file che sono stati modificati o aggiunti. Tutti i file che non sono più nell'archivio vengono eliminati durante questa indicizzazione. Così un'operazione di reindicizzazione può essere eseguita in tempi molto più rapidi rispetto all'operazione di indicizzazione iniziale.

Utilizzo di regole IDM parallele per ottimizzare le soglie di corrispondenze

Le politiche IDM sono utilizzate in primo luogo per rilevare contenuto di documenti non strutturato sulla base di un requisito percentuale di corrispondenza denominato Esposizione minima documento. Questo valore è un parametro configurabile che specifica la percentuale minima di contenuto nel messaggio che deve corrispondere all'indice IDM per produrre una corrispondenza. L'impostazione predefinita della politica IDM è "Esatta": ciò significa che per i documenti di testo l'intero contenuto del messaggio deve corrispondere all'impronta per creare un incidente. Un'impostazione di Esposizione minima documento pari al 10% significa che, in media, una pagina di un documento di 10 deve corrispondere all'indice IDM per creare un incidente.

Un documento può includere una quantità molto maggiore di contenuto, ma Symantec Data Loss Prevention protegge solo il contenuto indicizzato come parte di un profilo di documento. Si consideri ad esempio una situazione in cui si indicizza un documento di una pagina e tale documento di una pagina viene incluso come parte di un documento di 100 pagine. Il documento di 100 pagine è considerato una corrispondenza esatta perché il suo contenuto corrisponde esattamente al documento di una pagina. Inoltre, il documento nel quale si rileva la corrispondenza non deve essere dello stesso tipo o formato di file del documento indicizzato.

Ad esempio, se si indicizza un documento Word come parte di un profilo di documento e il suo contenuto viene incollato nel corpo di un e-mail o utilizzato per creare un PDF, il motore di rilevamento lo considera come una corrispondenza.

Una valore empirico per l'impostazione di Esposizione minima documento è 60%. In genere i valori di Esposizione minima documento inferiori al 50% creano molti falsi positivi. I valori a partire dal 60% dovrebbero fornire dati sufficienti per determinare se è opportuno passare a una percentuale di corrispondenza più alta o più bassa senza creare un numero eccessivo di falsi positivi.

Come alternativa, considerare un approccio a livelli per la definizione di impostazioni di Esposizione minima documento. Ad esempio, è possibile creare più regole IDM, ciascuna con una soglia percentuale diversa, quale 80% per i documenti con un'alta percentuale di corrispondenza, 50% per i documenti con una percentuale di corrispondenza media e 10% per i documenti con una percentuale di corrispondenza bassa. Mediante questo approccio è più facile escludere i falsi positivi e stabilire un'impostazione accurata di Esposizione minima documento per ogni indice IDM distribuito come componente delle politiche.

Indicizzazione EDM remota

Questa sezione fornisce istruzioni e contenuti di riferimento per l'utilizzo dell'Indicizzatore IDM remoto.

Informazioni sull'Indicizzatore IDM remoto

L'indicizzatore IDM remoto è uno strumento autonomo. Esso consente di indicizzare documenti e file riservati localmente sui sistemi in cui sono stati archiviati. Grazie all'indicizzatore IDM remoto non è più necessario dovere raccogliere e copiare tutti i file sull'host di Enforce Server per l'indicizzazione.

L'Indicizzatore IDM remoto genera un file di preindice (*.prdx) crittografato e protetto tramite password. Caricare il file di preindice sull'host di Enforce Server per la creazione e la distribuzione dell'indice finale.

L'Indicizzatore IDM remoto è supportato su piattaforme Windows e Linux. Lo strumento è configurato mediante un'interfaccia riga di comando (CLI) o un file di proprietà. In Windows è possibile utilizzare l'interfaccia utente grafica (GUI) dello strumento per configurarlo.

È possibile integrare lo strumento con sistemi esterni per pianificare l'indicizzazione. Inoltre, è possibile indicizzare in maniera incrementale un'origine dati specificando un file *.prdx esistente quando viene eseguito lo strumento.

Tabella 23-28 Funzionalità dell'Indicizzatore IDM remoto

Funzionalità	Descrizione
Installazione classica	Installatori DLP per Windows e Linux
Diverse opzioni di configurazione	File di proprietà (predefinito) Interfaccia della riga di comando (CLI) GUI interfaccia utente grafica (Windows)
File di preindice protetto	Protezione con password Contenuti di dati crittografati
Indicizzazione incrementale	Possibilità di caricare un preindice esistente e di eseguire la scansione solo di file nuovi o aggiornati.
Indicizzazione pianificata	Utilità di pianificazione Windows Cron job di Linux Per ulteriori informazioni consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> .
Caricamento protetto su Enforce	UI per il caricamento del preindice in Enforce Server L'utente deve fornire una password per completare il processo di indicizzazione.

Indicizzazione dell'origine dati del documento mediante l'edizione GUI (solo Windows)

Per configurare l'edizione UI dell'Indicizzatore IDM remoto, immettere i parametri nei campi obbligatori. È anche possibile fornire parametri aggiuntivi, come un file lista bianca per i filtri.

Una volta che l'indicizzazione si è completata correttamente, viene generato il file di preindice (*.prdx). Spostare questo file su Enforce Server per completare il processo di indicizzazione.

[Figura 23-1](#) mostra l'edizione GUI dell'Indicizzatore IDM remoto.

[Tabella 23-29](#) fornisce istruzioni per la configurazione dell'edizione GUI dell'Indicizzatore IDM remoto.

Figura 23-1 Edizione GUI dell'Indicizzatore IDM remoto

The screenshot displays the 'Indicizzatore IDM remoto' (Remote IDM Indexer) GUI. The window title is 'Indicizzatore IDM remoto'. The menu bar contains 'File', 'Modifica', and 'Guida'. The main header area shows a 'V' icon and the text 'Data Loss Prevention'. Below this is a yellow banner with the text 'Crea indice' (Create Index).

The configuration is organized into several sections:

- Parametri obbligatori** (Mandatory Parameters):
 - 'URI di origine' (Source URI) with a text input field and an 'Apri...' (Open...) button.
 - 'File di output' (Output file) with a text input field and an 'Apri...' (Open...) button.
- Filtri** (Filters):
 - 'Filtro di inclusione nome file' (File name inclusion filter) with a large text input field.
 - 'Filtro di esclusione nome file' (File name exclusion filter) with a large text input field.
 - 'Ignora file di dimensioni inferiori a' (Ignore files smaller than) with a text input field and a dropdown menu set to 'B'.
 - 'Ignora file di dimensioni superiori a' (Ignore files larger than) with a text input field and a dropdown menu set to 'B'.
 - 'Conserva sempre i file' (Always keep files) with an unchecked checkbox.
- File in lista bianca** (Whitelist):
 - A text input field and an 'Apri...' (Open...) button.
- Avanzamento** (Progress):
 - 'Fase corrente: Non avviato' (Current phase: Not started).
 - 'Avanzamento:' (Progress:).
 - 'File corrente:' (Current file:).
 - A progress bar.

At the bottom of the window are three buttons: 'Esegui' (Run), 'Pianifica...' (Schedule...), and 'Annulla' (Cancel).

Tabella 23-29 Configurazione dell'Indicizzatore IDM remoto mediante l'edizione GUI

Passaggio	Parametri	Descrizione
1	Immettere il percorso URI di origine .	<p>L'URI di origine è il percorso file locale (cartella directory) in cui vengono archiviati i file da indicizzare. Può anche essere un percorso di file system condiviso accessibile dall'host.</p> <p>I file da indicizzare non dovrebbero essere incapsulati.</p> <p>Se l'origine dati del documento richiede credenziali, fornirle nella sezione Credenziali URI.</p>
2	Immettere il nome del File di output .	<p>Specificare il nome e il percorso del file di preindice generato dallo strumento.</p> <p>Includere l'estensione del file *.prdx quando si specifica il nome del file di output.</p>
3	È anche possibile immettere il percorso di File in lista bianca .	<p>Specificare il percorso file sul file <code>whitelist.txt</code>.</p> <p>Il testo nel file lista bianca viene ignorato durante il rilevamento per la corrispondenza parziale basata su server.</p> <p>Per ulteriori informazioni sulla lista bianca consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i>.</p>
4	È anche possibile immettere uno o più Filtri di nome file .	<p>Immettere uno o più nomi di file da includere per l'indicizzazione o da escludere per l'indicizzazione.</p> <p>Il Filtro di inclusione nome file include i file denominati per l'indicizzazione.</p> <p>Il Filtro di esclusione nome file esclude i file denominati dall'indicizzazione.</p> <p>Il formato dei filtri di inclusione ed esclusione accetta valori sia separati da virgola sia separati da nuova riga.</p> <p>Se si utilizza un filtro, utilizzare un tipo ma non entrambi. Ad esempio, se si sceglie di utilizzare un filtro di inclusione nome file, non fornire un filtro di esclusione nome file.</p> <p>Per ulteriori informazioni sulla lista bianca consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i>.</p>
5	È anche possibile immettere un Filtro dimensioni file .	<p>Se si seleziona Ignora file di dimensioni inferiori a i file di dimensione inferiore a quella dimensione specificata non vengono indicizzati.</p> <p>Se si seleziona Ignora file di dimensioni superiori a i file di dimensione inferiore a quella specificata non vengono indicizzati.</p> <p>Per dettagli consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i>.</p>

Passaggio	Parametri	Descrizione
6	Se desiderato, fare clic su Conserva sempre i file .	Fare clic su Conserva sempre i file . <ul style="list-style-type: none"> ■ Quando si desidera aggiungere più origini dati in modo incrementale per lo stesso file di preindice. ■ Se si dispone di una cartella il cui contenuto viene spostato e si desidera mantenere il contenuto precedente nel file di preindice.
7	Fare clic su Esegui per indicizzare immediatamente l'origine dati.	Fare clic su Esegui per avviare il processo di indicizzazione. In alternativa, è possibile fare clic su Pianifica per pianificare l'indicizzazione. Lo strumento apre l' utilità di pianificazione di Windows . Vedere " Pianificazione dell'indicizzazione remota con l'app Indicizzatore IDM remoto per Windows " a pagina 623.
8	Immettere la Password per il file di preindice.	Per motivi di sicurezza è necessario fornire una password per il file di preindice. La password deve soddisfare uno dei seguenti requisiti: <ul style="list-style-type: none"> ■ Password ASCII: almeno 10 caratteri, tra cui almeno una lettera maiuscola, una lettera minuscola e un numero. ■ Password non ASCII: almeno 10 caratteri, tra cui almeno un numero. Il file di preindice è crittografato con la password fornita. La password che si inserisce qui è necessaria per caricare il preindice in Enforce Server per l'indicizzazione.
9	Verificare l'avanzamento dell'indicizzazione.	Quando si fa clic su Esegui , la barra di stato mostra la percentuale di completamento della scansione. Inoltre la sezione Avanzamento dell'interfaccia fornisce le seguenti informazioni: Fase corrente : gli stati sono In esecuzione , Completato o Errore . Avanzamento : il numero totale di file indicizzati. File corrente : il nome del file che viene indicizzato.

Vedere "[Indicizzazione dell'origine dati del documento tramite file di proprietà](#)" a pagina 619.

Indicizzazione dell'origine dati del documento tramite file di proprietà

È possibile passare i parametri all'Indicizzatore IDM remoto tramite il file delle proprietà.

Il percorso del file delle proprietà è \Symantec\Data Loss

Prevention\Indexer\15.1\Protect\config\remote_idm.properties (Windows) o
/opt/Symantec/DataLoss

Prevention/Indexer/15.1/Protect/config/remote_idm.properties (Linux).

Per indicizzare l'origine dati utilizzando il file delle proprietà, modificare il file e fornire i parametri. Quindi eseguire l'Indicizzatore IDM remoto senza alcun argomento della riga di comando. In questo caso, i parametri vengono letti dal file `remote_idm.properties`. Ad esempio, utilizzando il seguente comando senza alcun argomento viene eseguito lo strumento per la lettura degli argomenti dal file delle proprietà:

```
Symantec\Data Loss Prevention\Indexer\15.1\Protect\bin\RemoteIDMIndexer
```

Attenzione: Se si esegue lo strumento dalla riga di comando con argomenti, tali argomenti sovrascrivono i parametri nel file delle proprietà.

Tabella 23-30 elenca e descrive i parametri necessari per l'esecuzione dell'Indicizzatore IDM remoto dalla riga di comando.

Nota: Fare riferimento al *Manuale dell'amministratore di Symantec Data Loss Prevention* per dettagli sulla preparazione dell'origine dati del documento per l'indicizzazione.

Tabella 23-30 Parametri del file di proprietà richiesti

Parametro del file di configurazione	Descrizione
param.uri=	<p>Questo parametro è il percorso del file locale (cartella directory) o la directory condivisa in cui i file da indicizzare vengono memorizzati.</p> <p>Se si desidera indicizzare i file da una condivisione, è necessario caricare tale condivisione sul sistema che contiene l'indicizzatore. È inoltre necessario specificare il percorso del file di tale condivisione nel campo param.uri dello strumento Indicizzatore IDM remoto.</p> <p>I file non dovrebbero essere incapsulati.</p>
param.out=	<p>Questo parametro è il nome e il percorso del file di preindice generato dallo strumento.</p>

Tabella 23-31 elenca e descrive i parametri opzionali per l'esecuzione dell'Indicizzatore IDM remoto dalla riga di comando.

Nota: Fare riferimento al *Manuale dell'amministratore Symantec Data Loss Prevention* per dettagli sull'utilizzo della lista bianca e sull'utilizzo di filtri di dimensioni file e tipo di file.

Tabella 23-31 Parametri del file di proprietà facoltativi

Parametro del file di proprietà	Descrizione
param.whitelist=	Questo parametro è il percorso file completo (compreso il nome) del file <code>whitelist.txt</code> . Il file della lista bianca deve essere locale nell'Indicizzatore IDM remoto. Il testo nel file lista bianca viene ignorato durante il rilevamento in caso di corrispondenza parziale con i contenuti del file.
param.include_filter=	Questo parametro è il tipo di file da includere per l'indicizzazione. Separare più voci di tipo di file con una virgola.
param.exclude_filter=	Questo parametro è il tipo di file da escludere per l'indicizzazione. I valori multipli sono separati da virgola.
param.min_filesize_bytes=	Questo parametro è il filtro di dimensione file minimo. I file inferiori alla dimensione specificata non sono indicizzati.
param.max_filesize_bytes=	Questo parametro è il filtro di dimensione file massimo. I file superiori alla dimensione specificata non sono indicizzati.

Vedere ["Indicizzazione dell'origine dati del documento tramite CLI"](#) a pagina 621.

Indicizzazione dell'origine dati del documento tramite CLI

L'interfaccia della riga di comando (CLI) consente di configurare ed eseguire l'Indicizzatore IDM remoto dalla riga di comando.

È possibile passare i parametri allo strumento direttamente dalla riga di comando o tramite un file delle proprietà. Le opzioni della riga di comando sovrascrivono i parametri del file delle proprietà.

Questo esempio passa argomenti tramite la riga di comando. In questo caso il file delle proprietà viene ignorato.

```
Symantec\Data Loss Prevention\Indexer\15.1\Protect\bin>RemoteIDMIndexer
-uri=\\10.66.195.173\remoteIDM\files -out=C:\temp\myRemoteIDMPreIndex.prdx
```

Attenzione: Se si esegue lo strumento dalla riga di comando con argomenti, tali argomenti sovrascrivono i parametri nel file delle proprietà.

[Tabella 23-32](#) elenca e descrive i parametri necessari per l'esecuzione dell'Indicizzatore IDM remoto dalla riga di comando.

Nota: Fare riferimento al *Manuale dell'amministratore di Symantec Data Loss Prevention* per dettagli sulla preparazione dell'origine dati del documento per l'indicizzazione.

Tabella 23-32 Parametri CLI richiesti

Parametro della riga di comando	Descrizione
-uri	Questo parametro è il percorso del file locale (cartella directory) o la directory condivisa in cui i file da indicizzare vengono memorizzati. I file da indicizzare non dovrebbero essere incapsulati.
-out	Questo parametro è il nome e il percorso del file di preindice generato dallo strumento.

[Tabella 23-33](#) elenca e descrive i parametri opzionali per l'esecuzione dell'Indicizzatore IDM remoto dalla riga di comando.

Nota: Fare riferimento al *Manuale dell'amministratore Symantec Data Loss Prevention* per dettagli sull'utilizzo della lista bianca e sull'utilizzo di filtri di dimensioni file e tipo di file.

Tabella 23-33 Parametri CLI facoltativi

Parametro della riga di comando	Descrizione
-whitelist	Questo parametro è il percorso file completo del file <code>whitelist.txt</code> . Il file della lista bianca deve essere locale nell'Indicizzatore IDM remoto. Il testo nel file lista bianca viene ignorato durante il rilevamento.
-include_filter	Questo parametro rappresenta uno o più tipi di file da includere per l'indicizzazione. Separare più voci con una virgola.
-exclude_filter	Questo parametro rappresenta uno o più tipi di file da escludere per l'indicizzazione. Separare più voci con una virgola.
-min_filesize_bytes	Questo parametro è il filtro di dimensione file minimo. I file inferiori alla dimensione specificata non sono indicizzati.

Parametro della riga di comando	Descrizione
<code>-max_filesize_bytes</code>	Questo parametro è il filtro di dimensione file massimo. I file superiori alla dimensione specificata non vengono indicizzati.

Pianificazione dell'indicizzazione remota con l'app Indicizzatore IDM remoto per Windows

Se si sta utilizzando la versione GUI di Windows dell'Indicizzatore IDM remoto, è possibile pianificare o modificare un'attività direttamente dallo strumento. Il seguente screenshot illustra il processo.

Vedere ["Per pianificare l'indicizzazione mediante la versione GUI di Windows"](#) a pagina 623.

Vedere ["Per modificare un'attività pianificata esistente mediante la GUI di Windows"](#) a pagina 625.

Per pianificare l'indicizzazione mediante la versione GUI di Windows

- 1 Fare clic su **Pianifica** per aprire la finestra di dialogo. Vedere ["Pianificazione dell'indicizzazione remota con l'app Indicizzatore IDM remoto per Windows"](#) a pagina 623.
- 2 Fare clic su **Crea** per creare una nuova attività pianificata. In alternativa, se si dispone già di un'attività creata, fare clic su **Modifica**.

Viene richiesto di fornire un file di password con codifica UTF8 in testo non crittografato per il processo pianificato. L'accesso a questo file deve essere limitato all'utente appropriato, come utente Proteggi.

Fare clic su **Crea** e fornire le credenziali per l'host Windows.

- 3 Immettere il nome utente e la password per l'host Windows in cui è installata l'utilità di pianificazione attività.

Quando si immettono le appropriate credenziali (solitamente sono richieste privilegi di amministratore), l'Indicizzatore IDM remoto crea una nuova attività nell'utilità di pianificazione di Windows. Lo strumento visualizza una finestra di dialogo che indica che l'attività è stata creata correttamente e fornisce il nome dell'attività. Vedere [Figura 23-3](#) a pagina 624.
- 4 Fare clic su **OK** per chiudere la finestra di dialogo.

Dopo aver completato questa operazione con Windows viene visualizzata l'interfaccia.

- 5 Selezionare la cartella **SymantecDLP** nella libreria utilità di pianificazione.
Sul lato destro è presente un'attività creata denominata "Indicizzatore IDM remoto <time-stamp>". Vedere [Figura 23-4](#) a pagina 625.
- 6 Fare doppio clic sull'attività creata.
Questa azione visualizza la finestra di dialogo di proprietà Utilità di pianificazione di Windows per questa attività. Mediante questa finestra di dialogo è possibile pianificare l'esecuzione dell'Indicizzatore IDM remoto. Fare riferimento alla guida relativa all'utilità di pianificazione per dettagli sull'utilizzo dell'utilità di pianificazione di Windows.

Figura 23-2 Pianificazione dell'indicizzazione della finestra di dialogo

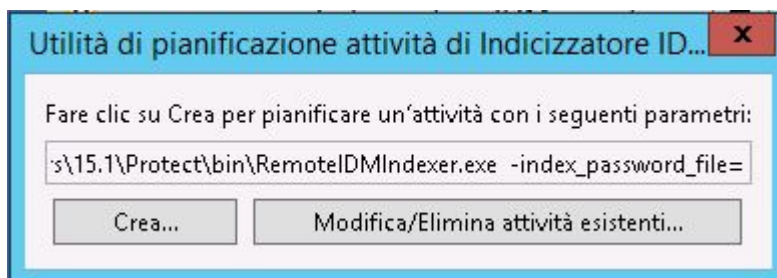


Figura 23-3 Finestra di dialogo attività pianificata correttamente

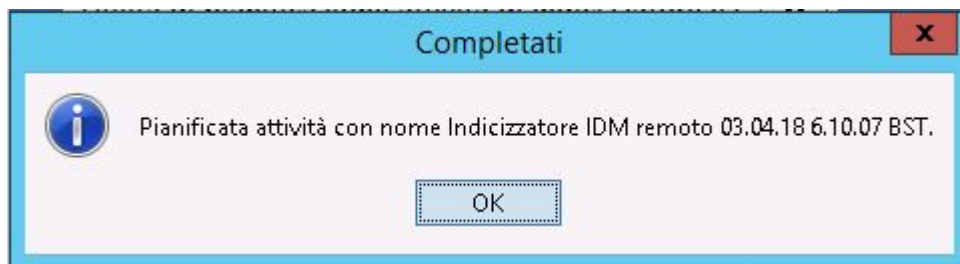
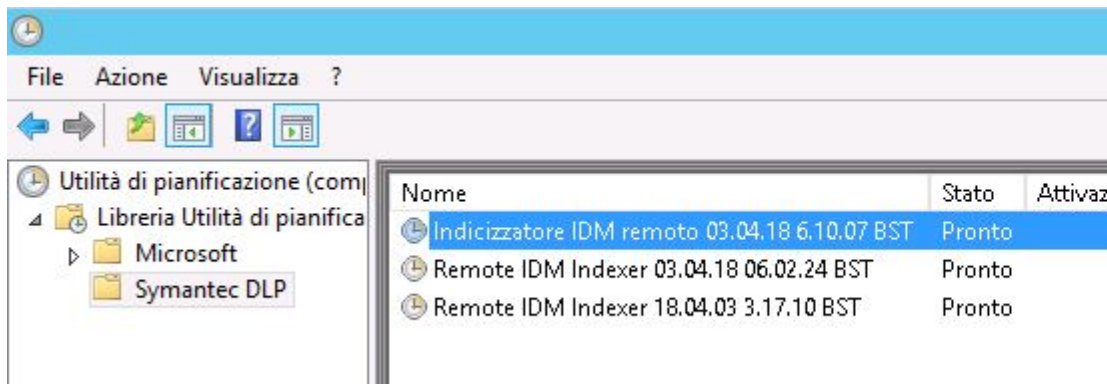


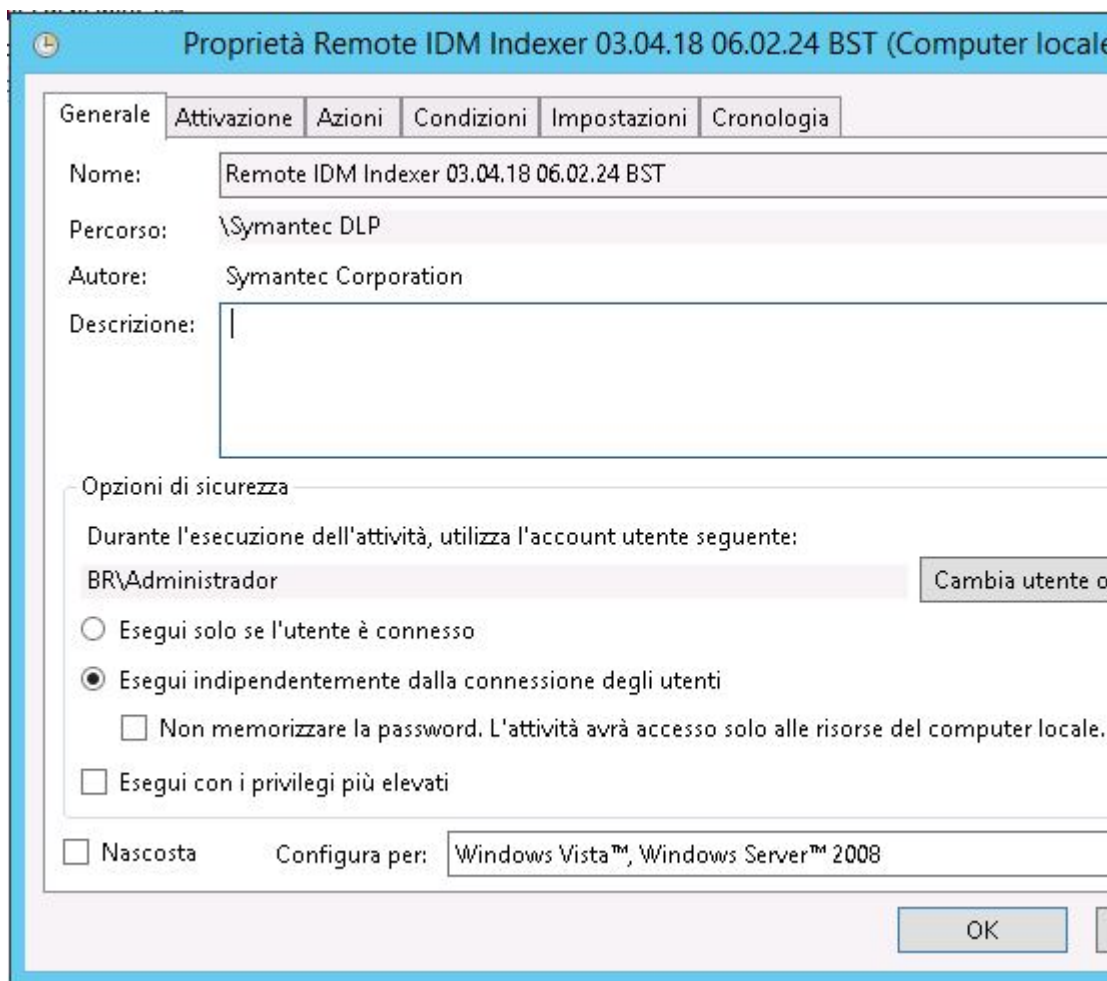
Figura 23-4 Attività pianificata Symantec DLP



Per modificare un'attività pianificata esistente mediante la GUI di Windows

- 1 Fare clic su **Pianifica** per aprire la finestra di dialogo. Vedere [Figura 23-2](#) a pagina 624.
- 2 Fare clic sul pulsante **Modifica/Elimina attività esistenti** per aprire l' **Utilità di pianificazione Windows**. Qui è possibile modificare o eliminare un'attività pianificata esistente.

Figura 23-5 Configurazione delle proprietà dell'utilità di pianificazione Windows



Vedere ["Indicizzazione incrementale"](#) a pagina 626.

Indicizzazione incrementale

È possibile indicizzare in maniera incrementale un'origine dati remota specificando un file di preindice esistente (*.prdx) nell'argomento della riga di comando quando viene eseguito lo strumento.

Nella versione GUI dello strumento è possibile sfogliare e selezionare un file *.prdx esistente per il percorso **File di output**.

Il processo di indicizzazione aggiunge file indicizzati recenti e contenuti file alle voci di preindice esistenti.

Lo strumento confronta la data di ultima modifica del file. Se il file è stato modificato dopo il file con preindice, lo strumento aggiorna il preindice con le modifiche apportate al file. Se la data in cui è stato modificato il file è la stessa, il preindice non viene aggiornato. Se si modificano i filtri relativi a dimensioni, esclusione o inclusione nel file di preindice esistente, tali filtri sono applicati a qualsiasi file indicizzato in precedenza. Ad esempio, per un'origine dati remota con file `.docx` e file `.pptx`, se il primo processo di indicizzazione remoto non presenta filtri, tutti i file vengono indicizzati. Se si aggiunge un filtro di esclusione per file `.docx` (`-exclude_filter=*.docx`) e viene eseguito nuovamente il processo di indicizzazione, i file `.docx` sono rimossi dall'indice e restano solo i file `.pptx`.

Conserva sempre i file

Se si desidera aggiungere in modo incrementale più origini dati allo stesso file di preindice, è possibile selezionare **Conserva sempre i file** nella versione GUI dell'indicizzatore IDM remoto per Windows oppure utilizzare `keep_all_files=true` nella riga di comando per Windows e Linux. Mantiene i file che sono nel preindice precedente, ma non nell'origine dati corrente. Consente inoltre di aggiungere in modo incrementale più origini dati allo stesso file di preindice. Si può utilizzare `keep_all_files` se si dispone di una cartella con un contenuto spostato e si desidera mantenere il contenuto precedente nel file di preindice.

L'indicizzatore incrementale IDM precedente e l'indicizzatore reso disponibile dalla console di amministrazione di Enforce Server sostituiscono il vecchio indice intero con uno nuovo. Ad esempio, quando un set di documenti A viene indicizzato e poi il set di documenti B viene indicizzato in modo incrementale per lo stesso profilo, l'indice del set A viene eliminato e sostituito con l'indice del set B.

Registrazione e risoluzione dei problemi

I messaggi di stato relativi all'indicizzazione dell'IDM remoto vengono registrati nel file `Indexer.log`.

Il percorso del file di registro è `C:\ProgramData\Symantec\Data Loss Prevention\Indexer\15.1\logs` (Windows) o `/var/log/Symantec/DataLossPrevention/Indexer/15.1/` (Linux).

Il registro presenta messaggi di errore che indicano se è stato negato l'accesso ai file o se l'indicizzazione dei file non è riuscita.

Vedere ["Copia del file di preindice sull'host di Enforce Server"](#) a pagina 628.

Copia del file di preindice sull'host di Enforce Server

Dopo avere generato il file di preindice è necessario copiarlo sull'host di Enforce Server in modo che possa essere caricato per il profiling e la distribuzione.

Copiare il file *.prdx nella seguente directory sull'host dell'Enforce Server:

C:\ProgramData\Symantec\Data Loss Prevention\Server Platform
Common\15.1\documentprofiles.

È possibile utilizzare FTP o FTP/S per copiare il file *.prdx sul file system dell'host di Enforce Server.

Nota: Assicurarsi che l'utente di Enforce che legge e carica il file .prdx abbia l'autorizzazione per consentire la copia e il caricamento del file.

Vedere ["Caricamento del file di indice remoto in Enforce Server"](#) a pagina 628.

Caricamento del file di indice remoto in Enforce Server

La console di amministrazione di Enforce Server fornisce un'interfaccia utente per il caricamento di preindici IDM remoti su Enforce Server.

L'amministratore o l'autore della politica di Data Loss Prevention deve specificare la password di preindice che è stata immessa quando il file di preindice è stato creato inizialmente.

Il sistema usa il preindice per generare l'indice finale che è distribuito ai server di rilevamento e agli agenti (se IDM agente è attivato).

Nota: Se non si è copiato il file di preindice nella directory corretta sull'host di Enforce Server (C:\Programmi\Symantec\Data Loss Prevention\Server Platform Common\15.1\documentprofiles), il file non viene visualizzato nel campo a discesa per la selezione.

Figura 23-6 Caricamento dell'indice remoto in Enforce

☐ Importa da un profilo IDM creato in remoto

Seleziona profilo IDM remoto Nessuna selezione ▼

Password per decrittografare profilo IDM remoto

Immettere di nuovo la password

Rilevamento del contenuto mediante Vector Machine Learning (VML)

Il capitolo contiene i seguenti argomenti:

- [Introduzione a Vector Machine Learning \(VML\)](#)
- [Configurazione dei profili VML e delle condizioni delle politiche](#)
- [Procedure ottimali per l'utilizzo di VML](#)

Introduzione a Vector Machine Learning (VML)

Vector Machine Learning (VML) esegue analisi statistiche per proteggere i dati non strutturati. L'analisi determina se il contenuto è simile al contenuto di esempio utilizzato per l'apprendimento.

Con VML non è necessario individuare e contrassegnare tutti i dati che si desidera proteggere. Inoltre non è necessario descriverli e rischiare potenziali imprecisioni. Con VML, si prepara il sistema all'apprendimento del tipo di contenuto che si desidera proteggere in base ai documenti di esempio forniti.

Il rilevamento con VML è basato su un profilo VML. Si crea un profilo VML caricando una quantità rappresentativa di contenuto da una categoria specifica di dati. Il sistema esegue la scansione del contenuto, estrae le caratteristiche e crea un modello statistico basato sulla frequenza delle parole chiave nei documenti di esempio. Al runtime il sistema applica il modello per analizzare e individuare il contenuto con caratteristiche che sono statisticamente simili al profilo.

VML semplifica il rilevamento di contenuto non strutturato basato su testo offrendo il potenziale per un'elevata precisione. La chiave per l'implementazione di VML è il contenuto di esempio

utilizzato per preparare il sistema. È necessario selezionare documenti che sono molto rappresentativi del tipo di contenuto che si desidera proteggere. Ed è necessario selezionare buoni esempi del contenuto da ignorare che sono strettamente correlati al contenuto che si desidera proteggere.

Vedere ["Configurazione dei profili VML e delle condizioni delle politiche"](#) a pagina 633.

Informazioni sul profilo Vector Machine Learning

Il profilo Vector Machine Learning è il profilo dati da definire per implementare le politiche VML.

Ad esempio, è possibile creare un profilo VML per proteggere il codice sorgente. Eseguire il training del sistema utilizzando documenti positivi di esempio (codice privato che si desidera proteggere). Eseguire il training del sistema utilizzando documenti negativi di esempio (codice open source che non è necessario proteggere). Una politica VML fa riferimento al profilo VML per analizzare i dati dei messaggi e riconoscere il contenuto simile alle funzionalità positive. Il profilo VML può essere adattato e aggiornato facilmente aggiungendo o rimuovendo documenti nei set di training.

Vedere ["Profili dati"](#) a pagina 381.

Vedere ["Creazione di nuovi profili VML"](#) a pagina 635.

Informazioni sul contenuto sottoposto a training

La raccolta dei documenti per il training è il passaggio più importante nel processo Vector Machine Learning. L'accuratezza di Vector Machine Learning è direttamente proporzionale a quella del contenuto di esempio utilizzato per il training.

Vedere ["Configurazione dei profili VML e delle condizioni delle politiche"](#) a pagina 633.

Un profilo VML è basato su una categoria di contenuto che rappresenta un caso specifico di uso professionale. Una categoria di contenuto include due set di training: positivo e negativo.

Il set di training positivo è il contenuto che si desidera proteggere. A una categorizzazione più specifica corrispondono risultati più accurati. Ad esempio "Customer Purchase Orders" è migliore di "Financial Documents" perché è più specifica.

Il set di training negativo è il contenuto che si desidera ignorare, ma è comunque correlato al set di training positivo. Se ad esempio il set di training positivo è "Weekly Sales Reports", il set di training negativo potrebbe contenere "Sales Press Releases."

È consigliabile raccogliere una quantità uguale di contenuto positivo e negativo, costituito principalmente da testo. Non è necessario raccogliere tutto il contenuto che si desidera proteggere. Tuttavia, è necessario assemblare set di training abbastanza grandi da offrire statistiche affidabili.

Il numero consigliato di documenti per set di training è 250. Il numero minimo di documenti per set di training è 50.

[Tabella 24-1](#) riassume i requisiti base del contenuto da raccogliere per il training del profilo VML.

Tabella 24-1 Requisiti per il set di training VML

Categoria di contenuto	Tipo di dati	Set di training	Quantità	Contenuto	Dimensione
Caso singolo e specifico di utilizzo aziendale	Basato su testo (in maggioranza)	Positivo	Consigliato: 250 documenti Minimo: 50 documenti	Contenuto che si desidera proteggere.	30 MB per caricamento
		Negativo	Approssimativamente la stessa quantità della categoria positiva.	Contenuto che non si desidera proteggere ma è associato a livello di argomento alla categoria positiva.	Nessun limite di dimensione per categoria.

Informazioni sui livelli percentuali di precisione di base da training

Durante il processo di training del profilo VML, il sistema estrae il contenuto del documento di esempio e lo converte in testo non elaborato. Il sistema seleziona le funzionalità (o parole chiave) con un algoritmo proprietario e genera il profilo VML. Nell'ambito del processo di formazione, il sistema calcola e segnala i livelli di precisione di base per i falsi positivi e i falsi negativi. I livelli percentuali di precisione di base da training indicano la qualità dei set di training positivo e negativo.

Mentre l'obiettivo è quello di raggiungere il 100% della precisione (incidenza dei falsi negativi di base pari allo 0%), ottenere questo livello di qualità per entrambi i set di training solitamente non è possibile. In generale è necessario rifiutare un profilo di training se l'incidenza dei falsi positivi o dei falsi negativi di base è superiore al 5%. Un'incidenza percentuale dei falsi negativi di base relativamente alta indica che il set di training non è categorizzato correttamente. In questo caso è necessario aggiungere documenti a un set di training sottorappresentato, rimuovere documenti da un set di training sovrarappresentato o eseguire entrambe le operazioni.

Vedere ["Gestione dei documenti dei set di training"](#) a pagina 641.

[Tabella 24-2](#) descrive il significato dei livelli percentuali di precisione di base da training relativamente ai set di training positivo e negativo per un profilo VML dato.

Tabella 24-2 Livelli di precisione di base da training

Livello di precisione	Descrizione
Incidenza di falsi positivi di base (%)	Percentuale del contenuto nel set di training negativo statisticamente simile al contenuto positivo.
Incidenza di falsi negativi di base (%)	Percentuale del contenuto nel set di training positivo statisticamente simile al contenuto negativo.

Informazioni sulla soglia di similarità e sul punteggio di somiglianza

Ogni profilo VML ha una **Soglia di similarità** che può essere impostata su un valore compreso tra 0 e 10. Questa impostazione consente di apportare una regolazione delle informazioni imperfette con un set di training per ottenere la migliore precisione possibile. Durante il rilevamento, un messaggio deve disporre di un punteggio di somiglianza superiore alla soglia di similarità affinché venga generato un incidente. La Soglia di similarità è impostata a livello di profilo, non all'interno di una politica. È impostata in questo modo perché esiste un'impostazione Soglia di similarità ideale specifica del set di training con cui è possibile ottenere i livelli di precisione migliori (in termini sia di falsi positivi sia di falsi negativi).

Quando una politica VML rileva un incidente, il sistema visualizza il **punteggio di somiglianza** nella sezione di evidenziazione delle corrispondenze di **Istantanea incidente** nella console di amministrazione di Enforce Server. Il punteggio di somiglianza indica la somiglianza del contenuto rilevato con il profilo VML. Più alto è il punteggio, più il messaggio è statisticamente simile ai documenti di esempio positivi nel profilo VML.

Considerare un esempio in cui una soglia di similarità è impostata su 4 e viene rilevato un messaggio con un punteggio di somiglianza di 5. In questo caso il sistema segnala la corrispondenza come un incidente e visualizza il punteggio di somiglianza durante l'evidenziazione delle corrispondenze. Tuttavia, se viene rilevato un messaggio con un punteggio di somiglianza pari a 3, il sistema non segnala alcuna corrispondenza (e alcun incidente) perché il punteggio di somiglianza è inferiore alla soglia di similarità.

[Tabella 24-3](#) descrive i valori della soglia di similarità e del punteggio di somiglianza.

Tabella 24-3 Dettagli della soglia di similarità e del punteggio di somiglianza

Similarità/Somiglianza	Descrizione
Soglia di similarità	<p>La soglia di similarità è un parametro configurabile tra 0 e 10, specifico di ciascun profilo VML. L'impostazione predefinita è 10, che richiede la corrispondenza più simile tra le funzionalità del profilo VML e il contenuto del messaggio rilevato. In quanto tale è probabile che questa impostazione generi un numero inferiore di incidenti. L'impostazione 0 restituisce il maggior numero di corrispondenze, molte delle quali probabilmente sono falsi positivi.</p> <p>Vedere "Regolazione della soglia di similarità" a pagina 647.</p>

Similarità/Somiglianza	Descrizione
Punteggio di somiglianza	Il punteggio di somiglianza è una statistica di runtime a sola lettura compresa tra 0 e 10, segnalata dal sistema in base ai risultati di rilevamento di una politica VML. Per segnalare un incidente, il punteggio di somiglianza deve essere superiore alla soglia di similarità. Altrimenti la politica VML non segnala una corrispondenza.

Informazioni sull'utilizzo di profili VML non accettati nelle politiche

Il sistema consente di creare una politica basata su un profilo VML che non è mai stato accettato. Tuttavia il profilo VML non è attivo e non è distribuito a una politica di riferimento finché il profilo non viene accettato una prima volta.

Vedere ["Training dei profili VML"](#) a pagina 638.

Se è presente una politica VML che fa riferimento a un profilo VML mai accettato, il risultato della configurazione dipende dal tipo di server di rilevamento. [Tabella 24-4](#) descrive il comportamento:

Tabella 24-4 Riferimenti a profili VML mai accettati

Server di rilevamento	Descrizione
Discover Server	La scansione Discover non inizia finché non sono state caricate tutte le dipendenze della politica. Una scansione Discover basata su una politica VML non si avvia fino a quando il profilo VML al quale fa riferimento la politica non viene accettato. In questo caso il sistema visualizza un messaggio nell'interfaccia di scansione Discover che indica che la scansione è in attesa del caricamento della dipendenza.
Server di rete e Endpoint Server	<p>Per una regola semplice o una regola composta in cui le condizioni sono di tipo AND, l'intera regola non riesce perché la condizione VML non può essere soddisfatta. Se questa è l'unica regola della politica, la politica non funzionerà.</p> <p>Per una politica in cui sono presenti molte regole concatenate con OR, solo la regola VML non riesce, mentre le altre regole della politica vengono valutate.</p> <p>Vedere "Esecuzione del rilevamento di politiche" a pagina 402.</p>

Configurazione dei profili VML e delle condizioni delle politiche

Vector Machine Learning (VML) esegue analisi statistiche per proteggere i dati non strutturati. Inoltre determina se il contenuto è simile a un set di documenti di esempio utilizzato per il training.

Vedere ["Introduzione a Vector Machine Learning \(VML\)"](#) a pagina 629.

La seguente tabella descrive il processo di implementazione di VML.

Tabella 24-5 Implementazione di VML

Passaggio	Azione	Descrizione
Passaggio 1	Raccogliere i documenti di esempio per il training del sistema.	Raccogliere un numero rappresentativo di documenti di esempio con il contenuto positivo che si desidera proteggere e il contenuto negativo che si desidera ignorare. Vedere "Informazioni sul contenuto sottoposto a training" a pagina 630.
Passaggio 2	Creare un nuovo profilo VML.	Definire un nuovo profilo VML basato sulla categoria commerciale specifica dei dati da cui sono stati elaborati i set di training positivi e negativi. Vedere "Creazione di nuovi profili VML" a pagina 635.
Passaggio 3	Caricare i documenti di esempio.	Caricare i set di training positivi e negativi di esempio separatamente in Enforce Server. Vedere "Caricamento dei documenti di esempio per il training" a pagina 636.
Passaggio 4	Sottoporre a training il profilo VML.	Eseguire il training del sistema affinché apprenda il tipo di contenuto che si desidera proteggere e generare il profilo VML. Vedere "Training dei profili VML" a pagina 638.
Passaggio 5	Accettare o rifiutare il profilo ottenuto.	Accettare il profilo ottenuto per distribuirlo. Oppure, rifiutare il profilo, aggiornare uno o entrambi i set di training (aggiungendo o rimuovendo documenti di esempio) e riavviare il processo di training. Vedere "Informazioni sui livelli percentuali di precisione di base da training" a pagina 631. Vedere "Gestione di profili VML" a pagina 642.
Passaggio 6	Creare una politica VML e una regola di rilevamento di prova.	Creare una politica VML che faccia riferimento al profilo VML. Vedere "Configurazione della condizione Rileva utilizzando il profilo Vector Machine Learning" a pagina 645. Verificare ed esaminare gli incidenti in base al punteggio somiglianza. Vedere "Informazioni sulla soglia di similarità e sul punteggio di somiglianza" a pagina 632.
Passaggio 7	Mettere a punto il profilo VML.	Regolare l'impostazione Soglia di similarità come necessario per ottimizzare i risultati del rilevamento. Vedere "Regolazione della soglia di similarità" a pagina 647.

Passaggio	Azione	Descrizione
Passaggio 8	Seguire le best practice VML.	Vedere "Procedure ottimali per l'utilizzo di VML" a pagina 653.

Creazione di nuovi profili VML

Un profilo VML contiene il modello generato dai contenuti del set di training. Dopo avere definito un profilo VML, utilizzarlo per creare una o più politiche VML.

Vedere ["Configurazione dei profili VML e delle condizioni delle politiche"](#) a pagina 633.

Nota: è necessario disporre dei privilegi di amministratore per creare i profili VML.

Per creare un nuovo profilo VML

- 1 Fare clic su **Nuovo profilo** nella schermata **Gestisci > Profili dati > Vector Machine Learning** (se non lo si è già fatto).
- 2 Immettere un **nome** per il profilo VML nella finestra di dialogo **Crea nuovo profilo**.
Utilizzare un nome logico per il profilo VML che corrisponde alla categoria di dati che si desidera proteggere.
Vedere ["Informazioni sul contenuto sottoposto a training"](#) a pagina 630.
- 3 Facoltativamente immettere una **descrizione** per il profilo VML.
Si consiglia di includere una descrizione che identifichi lo scopo del profilo VML.
- 4 Fare clic su **Crea** per creare il nuovo profilo VML.
In alternativa fare clic su **Annulla** per annullare l'operazione.
- 5 Fare clic su **Gestisci profilo** per caricare i documenti di esempio.
Vedere ["Caricamento dei documenti di esempio per il training"](#) a pagina 636.

Utilizzo delle schede Profilo corrente e Area di lavoro temporanea

Per ogni profilo VML singolo sono disponibili due versioni: Corrente e Temporaneo. Il profilo corrente è la versione runtime; il profilo temporaneo è la versione della fase di realizzazione. Quando si sviluppa un profilo VML, si crea un Profilo corrente che è stato sottoposto a training, accettato ed eventualmente distribuito a una o più politiche. Si crea inoltre un Profilo temporaneo che si modifica e mette a punto attivamente.

La console di amministrazione di Enforce Server mostra le diverse versioni del profilo VML in schede separate:

- **Profilo corrente**

Questa versione è l'istanza attiva del profilo VML. Questa versione è stata sottoposta a training e accettata ed è disponibile per la distribuzione a una o più politiche.

- **Area di lavoro temporanea**

Questa versione è una versione modificabile del profilo VML. Questa versione non è stata sottoposta a training o accettata e non può essere assegnata a una politica.

Inizialmente, quando si crea un nuovo profilo VML, il sistema visualizza solo la scheda **Profilo corrente** con un set di training vuoto. Dopo aver inizialmente sottoposto a training e accettato il profilo, la tabella **Set con training** della scheda **Profilo corrente** viene compilata con dettagli relativi al set di training. Le informazioni che sono visualizzate in questa tabella e scheda sono di sola lettura.

Per modificare un profilo VML

- ◆ Fare clic su **Gestisci profilo** all'estremità destra della scheda **Profilo corrente**.

Il sistema visualizza la versione modificabile del profilo nella scheda **Area di lavoro temporanea**. È ora possibile procedere al training e alla gestione del profilo.

Vedere ["Training dei profili VML"](#) a pagina 638.

La scheda **Area di lavoro temporanea** rimane nell'interfaccia utente finché non si prepara ed accetta una nuova versione del profilo VML. In altri termini l'unico modo per chiudere la scheda **Area di lavoro temporanea** consiste nel preparare e accettare il profilo, anche se di fatto non sono state apportate modifiche al profilo stesso.

Quando si accetta una nuova versione del profilo VML, il sistema sovrascrive il Profilo corrente precedente con la versione appena accettata. Non è possibile tornare a un Profilo corrente accettato in precedenza. Tuttavia è possibile tornare alle versioni precedenti del set di training di un Profilo temporaneo.

Vedere ["Gestione dei documenti dei set di training"](#) a pagina 641.

Caricamento dei documenti di esempio per il training

Il set di training include i documenti di esempio positivi e negativi con i quali si desidera eseguire il training del sistema. I documenti positivi e negativi vanno caricati separatamente.

Nota: È possibile caricare singoli documenti. Tuttavia, si consiglia di caricare un archivio di documenti (ZIP, RAR, TAR) contenente il numero consigliato (250) o minimo (50) di documenti di esempio. La dimensione massima di caricamento è 30 MB. È possibile partizionare i documenti tra gli archivi se si dispone di più di 30 MB di dati da caricare. Vedere ["Informazioni sul contenuto sottoposto a training"](#) a pagina 630.

Per caricare il set di training

- 1 Se l'operazione non è ancora stata eseguita, fare clic su **Gestisci profilo** nella scheda **Profilo corrente**.

Questa azione attiva il profilo VML per la modifica nella scheda **Area di lavoro temporanea**.

Vedere ["Utilizzo delle schede Profilo corrente e Area di lavoro temporanea"](#) a pagina 635.

- 2 Fare clic su **Aggiorna contenuti** (se questa operazione non è stata ancora eseguita).
Viene visualizzata la finestra di dialogo **Aggiorna contenuti**.
- 3 Selezionare la categoria di contenuto:
 - Scegliere **Positivo: considera contenuti simili a questi** per caricare un archivio di documenti positivi.
 - Scegliere **Negativo: ignora contenuti simili a questi** per caricare un archivio di documenti negativi.

- 4 Fare clic su **Sfoglia** per selezionare l'archivio di documenti da caricare.

- 5 Accedere al file system in cui sono stati salvati i documenti di esempio.

- 6 Scegliere il file da caricare e fare clic su **Apri**.

- 7 Scegliere la categoria corrispondente al contenuto: Positivo o Negativo.

In caso di errori di caricamento (ad esempio se si seleziona Negativo ma si carica un archivio di documenti positivi) il profilo risultante non sarà accurato.

- 8 Fare clic su **Invia** per caricare l'archivio di documenti in Enforce Server.

Il sistema visualizza un messaggio che indica se il file è stato caricato correttamente. Se il caricamento riesce, l'archivio di documenti appare nella tabella **Nuovi documenti**. La tabella visualizza il tipo di documento, il nome, la dimensione, la data di caricamento e l'utente che ha eseguito il caricamento. Se il caricamento non riesce, vedere il messaggio di errore e ritentare. Fare clic sull'icona X nella colonna **Rimuovi** per eliminare un documento o un archivio documenti caricato dal set di training.

- 9 Fare clic su **Aggiorna contenuti** per ripetere il processo per l'altro set di training.

Il profilo non è completo e non può essere sottoposto a training finché non si carica il numero minimo di documenti di esempio positivi e negativi.

Vedere [Tabella 24-1](#) a pagina 631.

- 10 Una volta caricati correttamente entrambi i set di training si è pronti per il training del profilo VML.

Vedere ["Training dei profili VML"](#) a pagina 638.

Training dei profili VML

Durante il processo di training del profilo, il sistema esegue la scansione del contenuto di training, estrae le funzionalità chiave e genera un modello statistico. Se il processo di training viene completato correttamente, il sistema richiede di accettare o rifiutare il profilo di training. Se si accettano i risultati del training, quella versione del profilo VML diventa il profilo corrente. Il profilo corrente è attivo e disponibile per l'uso in una o più politiche.

Vedere ["Configurazione dei profili VML e delle condizioni delle politiche"](#) a pagina 633.

Tabella 24-6 Training del profilo VML

Passaggio	Azione	Descrizione
Passaggio 1	Attivare la modalità di training.	<p>Selezionare il profilo VML per il training nella schermata Gestisci > Profili dati > Vector Machine Learning. Oppure, creare un nuovo profilo VML.</p> <p>Vedere "Creazione di nuovi profili VML" a pagina 635.</p> <p>Fare clic su Gestisci profilo all'estrema destra della scheda Profilo corrente. Il sistema visualizza il profilo per il training nella scheda Area di lavoro temporanea.</p> <p>Vedere "Utilizzo delle schede Profilo corrente e Area di lavoro temporanea" a pagina 635.</p>
Passaggio 2	Caricare il contenuto di training.	<p>Acquisire familiarità con i requisiti e le raccomandazioni relativi ai set di training.</p> <p>Vedere "Informazioni sul contenuto sottoposto a training" a pagina 630.</p> <p>Caricare i set di training positivi e negativi in archivi di documenti distinti in Enforce Server.</p> <p>Vedere "Caricamento dei documenti di esempio per il training" a pagina 636.</p>
Passaggio 3	Regolare l'allocazione di memoria (solo se necessario).	<p>Il valore predefinito è "Alta" che generalmente assicura il miglior livello di precisione per i set di training. In genere, non è necessario modificare questa impostazione. In alcuni casi, è tuttavia possibile che si voglia scegliere l'impostazione "Media" o "Bassa" (ad esempio, quando si distribuisce il profilo all'endpoint).</p> <p>Vedere "Regolazione dell'assegnazione di memoria" a pagina 640.</p> <p>Nota: Se si modifica l'impostazione della memoria, è necessario farlo prima di eseguire il training del profilo per avere risultati di training accurati. Se il training del profilo è già stato eseguito, è necessario ripeterlo dopo aver regolato l'allocazione di memoria.</p>

Passaggio	Azione	Descrizione
Passaggio 4	Avviare il processo di training.	<p>Fare clic su Inizia training per iniziare il processo di training del profilo.</p> <p>Durante il processo di training, il sistema:</p> <ul style="list-style-type: none"> ■ Estrae le funzionalità chiave dal contenuto. ■ Crea il modello. ■ Calcola la precisione predittiva in base ai livelli medi di falsi positivi e falsi negativi per l'intero set di training. ■ Genera il profilo VML.
Passaggio 5	Verificare il completamento del training.	<p>Al termine del processo di training, il sistema indica se il profilo di training è stato creato correttamente.</p> <p>Se il processo di training non è riuscito, il sistema visualizza un errore. Esaminare i file di registro di debug e riavviare il processo di training.</p> <p>Vedere "File di registro di debug" a pagina 339.</p> <p>Se il processo di training è stato completato correttamente, il sistema visualizza le seguenti informazioni per il nuovo profilo :</p> <ul style="list-style-type: none"> ■ Documenti di esempio sottoposti a training Il numero di documenti di esempio in ogni set di training che il sistema ha utilizzato per il training e per i quali ha creato un profilo. ■ Livello di precisione da training La qualità del set di training espressa con livelli percentuali di falsi negativi e falsi positivi di base. Vedere "Informazioni sui livelli percentuali di precisione di base da training" a pagina 631. ■ Memoria <ul style="list-style-type: none"> ■ La quantità minima di memoria necessaria per caricare il profilo per il rilevamento nella fase di runtime. <p>Nota: Se il profilo è stato accettato in precedenza, il sistema visualizza le statistiche del profilo corrente per un raffronto.</p>

Passaggio	Azione	Descrizione
Passaggio 6	Accettare o rifiutare il profilo di training.	<p>Se il processo di training viene completato correttamente, il sistema richiede di accettare o rifiutare il profilo di training. La decisione deve essere basata sulle percentuali espresse in Livello di precisione da training.</p> <p>Vedere "Informazioni sui livelli percentuali di precisione di base da training" a pagina 631.</p> <p>Per accettare o rifiutare il profilo di training:</p> <ul style="list-style-type: none"> ■ Fare clic su Accetta per salvare i risultati del training come profilo corrente. Dopo l'accettazione del profilo di training, il profilo è visualizzato nella scheda Profilo corrente e la scheda Area di lavoro temporanea viene rimossa. ■ Fare clic su Rifiuta per non accettare i risultati del training. Il profilo rimane nella scheda Area di lavoro temporanea per un'eventuale modifica. È possibile regolare uno o entrambi i set di training aggiungendo o rimuovendo documenti e ripetendo il training del profilo. Vedere "Gestione dei documenti dei set di training" a pagina 641. <p>Nota: Un profilo VML sottoposto a training non è attivo fino a che non viene accettato. Il sistema consente di creare una politica basata su un profilo VML che non è stato sottoposto a training o accettato. Tuttavia il profilo VML non è distribuito a quella politica di riferimento finché il profilo non viene accettato. Vedere "Informazioni sull'utilizzo di profili VML non accettati nelle politiche" a pagina 633.</p>
Passaggio 7	Testare e ottimizzare il profilo.	<p>Dopo il training e l'accettazione del profilo VML, è possibile utilizzarlo per definire regole di politica e ottimizzarlo.</p> <p>Vedere "Configurazione della condizione Rileva utilizzando il profilo Vector Machine Learning" a pagina 645.</p> <p>Vedere "Informazioni sulla soglia di similarità e sul punteggio di somiglianza" a pagina 632.</p> <p>Nota: Consultare la <i>Guida alle best practice di Symantec Data Loss Prevention Vector Machine Learning</i>, disponibile nel centro di supporto Symantec (http://www.symantec.com/docs/DOC8733).</p>

Regolazione dell'assegnazione di memoria

L'impostazione **Allocazione memoria** determina la quantità di memoria necessaria per caricare il profilo VML in fase di runtime per il rilevamento della politica. Quando si assegna più memoria al training, il profilo VML diventa più grande. Vengono modellate più caratteristiche. Per impostazione predefinita, questo valore è impostato su Alta. Normalmente non è necessario regolare questo valore. Le risorse sono però limitate sull'endpoint. Se si intende distribuire il profilo VML all'endpoint, utilizzare un'impostazione di memoria più bassa per ridurre la dimensione del profilo.

Per regolare l'allocazione di memoria

- 1 Fare clic su **Regola** accanto all'impostazione **Allocazione memoria**.

Questa impostazione è disponibile nella scheda **Area di lavoro temporanea**. Se non è disponibile, fare clic su **Gestisci profilo** nella scheda **Profilo corrente**.

Vedere ["Utilizzo delle schede Profilo corrente e Area di lavoro temporanea"](#) a pagina 635.

- 2 Selezionare il livello di allocazione di memoria desiderato.

Sono disponibili le opzioni riportate di seguito:

- **Alta**

Richiede una quantità di memoria runtime superiore. Solitamente comporta una precisione di rilevamento maggiore (impostazione predefinita).

- **Media**

- **Bassa**

Richiede una quantità di memoria runtime inferiore, il che può comportare una precisione di rilevamento minore.

- 3 Fare clic su **Salva** per salvare l'impostazione.

La visualizzazione di **Impostazione memoria** deve riflettere la regolazione apportata.

- 4 Fare clic su **Inizia training** per iniziare il processo di training.

È necessario regolare l'allocazione di memoria prima di eseguire il training del profilo VML. Se si è già eseguito il training del profilo, rieseguire il training dopo avere regolato questa impostazione.

Vedere ["Training dei profili VML"](#) a pagina 638.

- 5 Verificare la quantità di memoria necessaria per eseguire il profilo VML.

Dopo avere eseguito il training del profilo VML, il sistema visualizza il valore **Memoria richiesta (KB)**. Questo valore rappresenta la quantità minima di memoria necessaria per caricare il profilo nella fase di runtime.

Vedere ["Gestione di profili VML"](#) a pagina 642.

Gestione dei documenti dei set di training

Quando si esegue il training e l'ottimizzazione di un profilo VML, può essere necessario regolare uno o entrambi i set di training. Ad esempio, se si rifiuta un profilo di training, è necessario aggiungere o rimuovere documenti di esempio per migliorare i livelli di accuratezza del training.

Vedere ["Informazioni sui livelli percentuali di precisione di base da training"](#) a pagina 631.

Per aggiungere documenti a un set di training

- 1 Fare clic su **Gestisci profilo** per il profilo che si desidera modificare.
Il profilo modificabile appare nella scheda **Area di lavoro temporanea**.
- 2 Fare clic su **Aggiorna contenuti**.
Vedere ["Caricamento dei documenti di esempio per il training"](#) a pagina 636.

Per rimuovere documenti da un set di training

- 1 Fare clic su **Gestisci profilo** per il profilo che si desidera modificare.
Il profilo modificabile appare nella scheda **Area di lavoro temporanea**.
- 2 Fare clic sulla X rossa nella colonna **Contrassegna rimosso** per il documento di training che si desidera rimuovere.
Il documento rimosso appare nella tabella **Documenti rimossi**. Ripetere questa procedura in base alle esigenze per rimuovere tutti i documenti non desiderati dal set di training.
- 3 Fare clic su **Inizia training** per ripetere il training del profilo.
È necessario ripetere il training e accettare il profilo aggiornato per completare il processo di rimozione dei documenti. Se non si accetta il nuovo profilo, il o i documenti che si tenta di rimuovere continuano a far parte del profilo.
Vedere ["Training dei profili VML"](#) a pagina 638.

Per ripristinare i documenti rimossi

- 1 Fare clic sull'icona di ripristino nella colonna **Ripristina** per un documento rimosso.
Il documento viene nuovamente aggiunto al set di training.
- 2 Fare clic su **Inizia training** per ripetere il training del profilo.
È necessario ripetere il training del profilo e accettarlo di nuovo anche se è stata ripristinata la configurazione originale.

Gestione di profili VML

Nella schermata **Gestisci > Profili dati > Vector Machine Learning** è possibile gestire i profili VML esistenti e crearne altri.

Vedere ["Configurazione dei profili VML e delle condizioni delle politiche"](#) a pagina 633.

Nota: È necessario disporre di privilegi di amministratore per Enforce Server per gestire e creare profili VML.

Tabella 1 Creazione e gestione di profili VML

Azione	Descrizione
Creare nuovi profili.	Fare clic su Nuovo profilo per creare un nuovo profilo VML. Vedere " Creazione di nuovi profili VML " a pagina 635.
Visualizzare e ordinare i profili.	Il sistema elenca tutti i profili VML esistenti e il relativo stato nella schermata Vector Machine Learning . Fare clic sull'intestazione della colonna per ordinare i profili VML per nome o stato.
Gestire ed eseguire il training dei profili.	Selezionare un profilo VML dall'elenco per visualizzarlo e gestirlo. La scheda Profilo corrente visualizza il profilo attivo. Vedere " Utilizzo delle schede Profilo corrente e Area di lavoro temporanea " a pagina 635. Fare clic su Gestisci profilo per modificare il profilo. Il profilo modificabile appare nella scheda Area di lavoro temporanea . In questa scheda è possibile: <ul style="list-style-type: none"> ■ Caricare documenti del set di training. Vedere "Caricamento dei documenti di esempio per il training" a pagina 636. ■ Eseguire il training del profilo. Vedere "Training dei profili VML" a pagina 638. ■ Aggiungere e rimuovere documenti dai set di training. Vedere "Gestione dei documenti dei set di training" a pagina 641.
Monitorare i profili.	Il sistema elenca e descrive lo stato di tutti i profili VML. <ul style="list-style-type: none"> ■ Memoria richiesta (KB) La quantità minima di memoria richiesta per caricare il profilo nella memoria per il rilevamento. Vedere "Regolazione dell'assegnazione di memoria" a pagina 640. ■ Stato Lo stato corrente del profilo. Vedere Tabella 24-8 a pagina 644. ■ Stato distribuzione Lo stato cronologico del profilo. Vedere Tabella 24-9 a pagina 644.
Rimuovere i profili.	Fare clic sull'icona X all'estrema destra per eliminare un profilo esistente. Se si elimina un profilo, il sistema rimuove i metadati del profilo e il set di training da Enforce Server.

Il campo **Stato** visualizza lo stato corrente di ogni profilo VML.

Tabella 24-8 Valori di stato per i profili VML

Valore di stato	Descrizione
Accettato il <data>	La data in cui il profilo di training è stato accettato.
Gestione	Il profilo corrente è attivato per la modifica.
Vuoto	Il profilo viene creato, ma il contenuto non è caricato.
In attesa dell'accettazione	Il profilo è pronto per essere accettato.
Annullamento training	Il sistema sta annullando il training.
Training annullato	Il processo di training è stato annullato.
Non riuscito	Il processo di training non è riuscito.
Training <tempo>	Il training è in corso (per il tempo indicato).

Il campo **Stato distribuzione** indica se il profilo VML è stato accettato o meno.

Tabella 24-9 Valori di Stato distribuzione per i profili VML

Valore di stato	Descrizione
Mai accettato	Il profilo VML non è mai stato accettato. Vedere " Informazioni sull'utilizzo di profili VML non accettati nelle politiche " a pagina 633.
Accettato il <data>	Il profilo VML è stato accettato alla data indicata.

Modifica dei nomi e delle descrizioni per i profili VML

Se necessario, è possibile modificare il nome di un profilo VML o modificarne la descrizione. Quando si è pronti a distribuire un profilo VML a una o più politiche, assegnare al profilo un nome autodescrittivo in modo che gli autori della politica possano riconoscerlo facilmente.

Nota: non è necessario rieseguire il training di un profilo se si modifica il nome o la descrizione.

Per modificare il nome o la descrizione del profilo VML

- 1 Selezionare il profilo VML nella schermata **Gestisci > Profili dati > Vector Machine Learning**.
Vedere "[Gestione di profili VML](#)" a pagina 642.
- 2 Fare clic sul collegamento **Modifica** accanto al nome del profilo VML.

- 3 Modificare il nome e la descrizione del profilo nella finestra di dialogo **Cambia nome e descrizione** visualizzata.
- 4 Fare clic su **OK** per salvare le modifiche apportate al nome o alla descrizione del profilo VML.
- 5 Verificare le modifiche nella schermata iniziale per il profilo VML.

Configurazione della condizione Rileva utilizzando il profilo Vector Machine Learning

Dopo aver preparato e accettato il profilo VML, configurare una politica VML utilizzando la condizione **Rileva utilizzando il profilo Vector Machine Learning**. Questa condizione fa riferimento al profilo VML per individuare contenuti simili a quelli di esempio utilizzati per il training.

Vedere ["Configurazione dei profili VML e delle condizioni delle politiche"](#) a pagina 633.

Tabella 24-10 Configurazione di una regola della politica VML

Passaggio	Azione	Descrizione
Passaggio 1	Creare e sottoporre a training il profilo VML.	Vedere "Creazione di nuovi profili VML" a pagina 635. Vedere "Training dei profili VML" a pagina 638. Vedere "Informazioni sull'utilizzo di profili VML non accettati nelle politiche" a pagina 633.
Passaggio 2	Configurare una politica nuova o esistente.	Vedere "Configurazione di politiche" a pagina 422.
Passaggio 3	Aggiungere la regola VML alla politica.	Nella schermata Configura politica : <ul style="list-style-type: none"> ■ Selezionare Aggiungi regola. ■ Selezionare la regola Rileva utilizzando il profilo Vector Machine Learning dall'elenco delle regola del contenuto. ■ Selezionare il profilo VML che si desidera utilizzare dal menu a discesa. ■ Fare clic su Avanti.
Passaggio 4	Configurare la regola di rilevamento VML.	Assegnare un nome alla regola e configurarne la gravità. Vedere "Configurazione di regole di politica" a pagina 427.

Passaggio	Azione	Descrizione
Passaggio 5	Selezionare i componenti in cui cercare la corrispondenza.	<p>Selezionare uno o entrambi i componenti dei messaggi in cui cercare la corrispondenza :</p> <ul style="list-style-type: none"> ■ Corpo, ovvero il contenuto del messaggio ■ Allegati, ovvero tutti i file trasportati dal messaggio <p>Nota: Sull'endpoint il Symantec DLP Agent cerca la corrispondenza nell'intero messaggio, non nei suoi singoli componenti.</p> <p>Vedere "Selezione dei componenti per la corrispondenza" a pagina 433.</p>
Passaggio 6	Configurare condizioni aggiuntive (facoltativo).	<p>Facoltativamente, è possibile creare una regola di rilevamento composta aggiungendo condizioni alla regola.</p> <p>Per aggiungere ulteriori condizioni, selezionare quella desiderata dal menu a discesa e fare clic su Aggiungi.</p> <p>Nota: Tutte le condizioni devono essere vere perché la regola generi un incidente.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>
Passaggio 7	Salvare la configurazione della politica.	Fare clic su OK e quindi fare clic su Salva per salvare la politica.

Configurazione delle eccezioni alla politica VML

In determinate situazioni può risultare utile implementare un'eccezione alla politica VML per ignorare determinati contenuti.

Vedere "[Configurazione dei profili VML e delle condizioni delle politiche](#)" a pagina 633.

Tabella 24-11 Configurazione di un'eccezione alla politica VML

Passaggio	Azione	Descrizione
Passaggio 1	Creare e sottoporre a training il profilo VML.	<p>Vedere "Creazione di nuovi profili VML" a pagina 635.</p> <p>Vedere "Training dei profili VML" a pagina 638.</p>
Passaggio 2	Configurare una politica nuova o esistente.	Vedere " Configurazione di politiche " a pagina 422.

Passaggio	Azione	Descrizione
Passaggio 3	Aggiungere un'eccezione VML alla politica.	<p>Nella schermata Configura politica :</p> <ul style="list-style-type: none"> ■ Selezionare Aggiungi eccezione. ■ Selezionare l'eccezione Rileva utilizzando il profilo Vector Machine Learning dall'elenco delle eccezioni del contenuto. ■ Selezionare il profilo VML che si desidera utilizzare dal menu a discesa. ■ Fare clic su Avanti.
Passaggio 4	Configurare l'eccezione della politica.	<p>Assegnare un nome all'eccezione.</p> <p>Selezionare i componenti ai quali si desidera applicare l'eccezione:</p> <ul style="list-style-type: none"> ■ Intero messaggio Selezionare questa opzione per confrontare l'eccezione con l'intero messaggio. Se un'eccezione viene rilevata in qualsiasi punto del messaggio, l'eccezione viene attivata e non vengono ricercate le corrispondenze. ■ Solo componenti con corrispondenza Selezionare questa opzione per cercare una corrispondenza per l'eccezione uguale a quella della regola. Ad esempio se la regola definisce la corrispondenza in base a Corpo (il corpo del messaggio) e l'eccezione si trova in un allegato, l'eccezione non viene attivata.
Passaggio 5	Configurare la condizione.	<p>In genere è possibile accettare le impostazioni delle condizioni predefinite per le eccezioni della politica.</p> <p>Vedere "Configurazione delle eccezioni di politica" a pagina 437.</p>
Passaggio 6	Salvare la configurazione della politica.	Fare clic su OK e quindi fare clic su Salva per salvare la politica.

Regolazione della soglia di similarità

Regolare l'impostazione Soglia di similarità per ottimizzare il profilo VML. La soglia di similarità determina come il contenuto rilevato simile deve essere un profilo VML per generare un incidente.

Vedere ["Informazioni sulla soglia di similarità e sul punteggio di somiglianza"](#) a pagina 632.

Nota: non è necessario rieseguire il training del profilo VML dopo avere regolato la soglia di similarità a meno che non si modifichi un set di training basato sui risultati del test.

Per regolare il valore corrente della soglia di similarità

- 1 Fare clic su **Modifica** accanto all'etichetta **Soglia di similarità** per il profilo VML che si desidera ottimizzare.

Questa azione apre la finestra di dialogo **Soglia di similarità**.

- 2 Trascinare l'indicatore sull'impostazione **Valore corrente** desiderata.

Impostare la soglia di similarità su un valore decimale compreso tra 0 e 10. Il valore predefinito è 10, che genera un numero inferiore di incidenti. Un'impostazione pari a 0 genera più incidenti.

- 3 Fare clic su **Salva** per salvare l'impostazione Soglia di similarità.

- 4 Testare il profilo VML utilizzando una politica VML.

Confrontare i punteggi di somiglianza in varie corrispondenze. Un messaggio rilevato deve avere un punteggio di somiglianza superiore alla soglia di similarità per generare un incidente. Apportare ulteriori modifiche all'impostazione Soglia di similarità in base alle esigenze per ottimizzare il profilo VML.

Vedere "[Configurazione della condizione Rileva utilizzando il profilo Vector Machine Learning](#)" a pagina 645.

Test e ottimizzazione dei profili VML

Per ottimizzare un profilo VML, testarlo con la soglia di similarità impostata su 0. Dopo avere determinato l'intervallo possibile dei punteggi di somiglianza per i falsi positivi, impostare la soglia di similarità in modo che sia maggiore del punteggio di somiglianza più alto segnalato dai falsi positivi. Questo processo è noto come test negativo.

Per un set di training valido è definito un intervallo in cui la soglia di similarità è impostata in modo da raggiungere i migliori livelli di precisione. Un set di training non valido restituisce risultati di precisione scarsi indipendentemente dalla soglia di similarità. Una soglia di similarità impostata su un valore troppo alto o troppo basso può restituire un numero elevato di falsi positivi o falsi negativi.

Per determinare l'impostazione corretta della soglia di similarità, si consiglia di eseguire un test negativo come descritto nei passaggi riportati di seguito.

Tabella 24-12 Passaggi per l'ottimizzazione dei profili VML

Passaggio	Azione	Descrizione
Passaggio 1	Eseguire il training del profilo VML.	Seguire i suggerimenti riportati nel presente manuale per definire la categoria e caricare i documenti del set di training. Regolare l'allocazione della memoria prima di eseguire il training del profilo. Consultare il <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i> per informazioni sull'esecuzione delle attività interessate.

Passaggio	Azione	Descrizione
Passaggio 2	Impostare la soglia di similarità su 0.	La soglia di similarità predefinita è 10. Con questo valore il sistema non genera alcun incidente. L'impostazione 0 genera il maggior numero di incidenti, molti dei quali sono probabilmente falsi positivi. Lo scopo dell'impostazione di questo valore su 0 è quello di visualizzare l'intero intervallo di corrispondenze potenziali. Serve inoltre a ottimizzare il profilo in modo che sia maggiore del punteggio di falso positivo più alto.
Passaggio 3	Creare una politica VML.	Creare una politica che faccia riferimento al profilo VML che si desidera ottimizzare. Il profilo deve essere accettato per potere essere distribuito a una politica.
Passaggio 4	Testare la politica.	Testare la politica VML utilizzando un insieme di dati di prova. Ad esempio è possibile usare il file <code>DLP_Wikipedia_sample.zip</code> come riferimento per il test delle politiche VML. Creare un meccanismo per rilevare gli incidenti. Il meccanismo può essere un target di scansione Discover di una cartella di file locale in cui inserire i dati del test. Oppure può essere una scansione di DLP Agent di un'operazione di copia e incolla.
Passaggio 5	Esaminare gli incidenti.	Esaminare eventuali corrispondenze nella schermata Istantanea incidente. Verificare un punteggio di somiglianza relativamente basso per ciascuna corrispondenza. Un punteggio di somiglianza relativamente basso indica un falso positivo. Se uno o più documenti del test generano una corrispondenza con un punteggio di somiglianza relativamente alto, significa che si è verificato un problema di qualità relativo al set di training. In questo caso è necessario esaminare il contenuto e, se appropriato, aggiungere i documenti al set di training positivo. È quindi necessario rieseguire il training e ottimizzare di nuovo il profilo. Vedere "File di log per la risoluzione dei problemi del training VML e del rilevamento di politiche" a pagina 652.
Passaggio 6	Regolare la soglia di similarità.	Esaminare gli incidenti per determinare il punteggio di somiglianza più alto tra i falsi positivi rilevati in base a cui si è testato il profilo. Quindi è possibile regolare la soglia di similarità in modo che il profilo sia maggiore del punteggio di somiglianza più alto per i falsi positivi. Ad esempio, se il falso positivo più alto ha un punteggio di somiglianza pari a 4.5, impostare la soglia di similarità su 4.6. Questa impostazione filtra i falsi positivi conosciuti dalla segnalazione come incidenti.

Proprietà per la configurazione del training

Il VML include diversi file di proprietà per la configurazione del training e della registrazione VML. La tabella seguente elenca e descrive le proprietà di configurazione VML pertinenti.

Tabella 24-13 File di proprietà per il VML

File di proprietà in \Protect\config\	Descrizione
MLDTraining.properties	File di proprietà principale per la configurazione delle impostazioni di training VML. Vedere Tabella 24-14 a pagina 650.
Manager.properties	File di proprietà per Enforce Server; contiene 1 impostazione VML. Vedere Tabella 24-15 a pagina 652.
MLDTrainingLogging.properties	File di proprietà per la configurazione della registrazione VML. Vedere "File di log per la risoluzione dei problemi del training VML e del rilevamento di politiche" a pagina 652.

La tabella seguente elenca e descrive i parametri di training VML disponibili per la configurazione nel file di proprietà `MLDTraining.properties`.

Tabella 24-14 Parametri di configurazione pertinenti per il training VML

Parametro	Descrizione
minimum_documents_per_category	Specifica il numero minimo di documenti necessari per ogni set di training (positivo e negativo). L'impostazione predefinita è 50. La riduzione di questo numero a meno di 50 non è consigliato o supportato. Vedere "Scelte consigliate per la definizione del set di training" a pagina 656.
mld_num_folds	Specifica il numero di fold da utilizzare per il processo di valutazione k-fold. La porta predefinita è 10. Se si diminuisce questo valore, si riduce il tempo che il sistema richiede per eseguire il training del contenuto perché viene valutato un numero inferiore di fold. Questa accelerazione potrebbe avvenire a discapito della visibilità della qualità del profilo. Non è necessario modificare questo valore, a meno che non si disponga di un numero elevato di documenti di esempio (e in questo caso i set di training sono molto grandi). Oppure qualora si sappia con certezza che il set di training è categorizzato correttamente. Vedere "Scelte consigliate per accettare o rifiutare un profilo" a pagina 659.

Parametro	Descrizione
<code>minimum_features_to_keep</code>	<p>Specifica il numero minimo di funzionalità da conservare per il profilo. L'impostazione predefinita è 1000.</p> <p>Se si diminuisce questo valore, si riduce la dimensione del profilo. Tuttavia la regolazione dell'impostazione non è consigliata. Utilizzare invece l'impostazione di allocazione della memoria per ottimizzare la dimensione del profilo.</p> <p>Vedere "Linee guida per il dimensionamento del profilo" a pagina 658.</p>
<code>significance_threshold</code>	<p>Specifica il numero minimo di volte che una parola deve presentarsi prima che sia considerata una funzionalità. La porta predefinita è 2.</p> <p>Se si aumenta questo valore (a 3 o 4, ad esempio), si può ridurre la dimensione del profilo perché un numero inferiore di parole si qualifica come funzionalità. In generale non è necessario regolare questa impostazione a meno che la definizione di un'allocazione della memoria bassa non produca un profilo sufficientemente piccolo per i requisiti di distribuzione.</p> <p>Vedere "Linee guida per il dimensionamento del profilo" a pagina 658.</p>
<code>stopword_file</code>	<p>Specifica il file di parole non significative predefinito <code>\config\machinelearningconfig\stopwords.txt</code>.</p> <p>Le parole non significative sono parole comuni, ad esempio articoli e preposizioni. Durante il training, il sistema ignora (ovvero non considera per l'estrazione di funzionalità) qualsiasi parola contenuta nel file di parole non significative.</p> <p>Se si aggiungono parole da ignorare, è necessario utilizzare solo lettere minuscole perché l'estrazione di funzionalità VML normalizza il contenuto con lettere minuscole per la valutazione.</p>
<code>logging_config_file</code>	<p>Specifica il file di configurazione per la registrazione VML standard.</p> <p>Vedere "File di log per la risoluzione dei problemi del training VML e del rilevamento di politiche" a pagina 652.</p>

Parametro	Descrizione
<code>native_logging_config_file</code>	<p>Specifica il file di configurazione per la registrazione VML nativa.</p> <p>Vedere "File di log per la risoluzione dei problemi del training VML e del rilevamento di politiche" a pagina 652.</p>

Il seguente parametro è disponibile per la configurazione nel file di proprietà `MLDTraining.properties`.

Tabella 24-15 Parametro di configurazione per i profili VML

Parametro	Descrizione
<code>DEFAULT_SIMILARITY_THRESHOLD</code>	<p>Stabilisce il valore predefinito per la soglia di similarità, ovvero 10. La modifica di questo valore incide solo sul valore predefinito. È possibile regolare il valore con la console di amministrazione di Enforce Server.</p> <p>Vedere "Test e ottimizzazione dei profili VML" a pagina 648.</p>

File di log per la risoluzione dei problemi del training VML e del rilevamento di politiche

Il sistema fornisce file di registro di debug per la risoluzione dei problemi del processo di training VML e il rilevamento di politiche. La tabella seguente elenca e descrive i file di registro di debug.

Vedere ["Risoluzione dei problemi delle politiche"](#) a pagina 458.

Tabella 24-16 File di registro di debug per VML

File di registro	Descrizione
<code>machinelearning_training.log</code>	<p>Registra l'accuratezza dai valori percentuali del training per ciascun ciclo del processo di valutazione per ciascuna fase del training del profilo VML.</p> <p>Esamina la qualità di ciascun set di training a livello granulare, per fold.</p> <p>Vedere "Scelte consigliate per accettare o rifiutare un profilo" a pagina 659.</p>

File di registro	Descrizione
machinelearning_native_filereader.log	<p>Registra la "distanza" espressa come numero positivo o negativo e la "fiducia", una percentuale di similarità, per ciascun messaggio valutato da una politica VML.</p> <p>Esamina tutti i messaggi o documenti valutati dalle politiche VML, incluse le corrispondenze positive con le percentuali di similarità al di sotto della soglia di similarità o i messaggi che il sistema ha categorizzato come negativi (valore di "distanza" negativo).</p> <p>Vedere "Test e ottimizzazione dei profili VML" a pagina 648.</p>
machinelearning_training_native_manager.log	<p>Registra il numero totale di funzionalità modellate e il numero di funzionalità conservate per generare il profilo per ciascuna fase di training.</p> <p>Il numero totale di funzionalità modellate rispetto al numero di funzionalità conservate per il profilo dipende dall'impostazione di allocazione della memoria:</p> <ul style="list-style-type: none"> ■ Se è "Alta" il sistema conserva l'80% delle funzionalità. ■ Se è "Media" il sistema conserva il 50% delle funzionalità. ■ Se è "Bassa" il sistema conserva il 30% delle funzionalità. <p>Vedere "Linee guida per il dimensionamento del profilo" a pagina 658.</p>

Procedure ottimali per l'utilizzo di VML

Questa sezione fornisce le best practice per implementare le politiche VML, incluse le best practice per il testing e la regolazione delle politiche VML.

È inoltre possibile scaricare documenti del set di training VML di esempio dal centro di supporto Symantec all'indirizzo <http://www.symantec.com/docs/DOC8733>. Questi documenti sono forniti in conformità alla licenza Creative Commons (<http://creativecommons.org/licenses/by-sa/3.0/>).

Tabella 24-17 fornisce un riepilogo delle best practice VML illustrate nella presente sezione. Contiene collegamenti ai singoli argomenti per consigli più dettagliati.

Tabella 24-17 Riepilogo delle best practice VML

Area funzionale	Best practice
Usi consigliati per VML	Utilizzare VML per proteggere contenuto non strutturato basato su testo. Non utilizzare VML per proteggere grafica, dati binari, o informazioni che consentono l'identificazione dell'utente (PII). Vedere "Quando utilizzare VML" a pagina 654.
Categoria di contenuto	Definire il profilo VML in base a una singola categoria di contenuti che si desidera proteggere. La categoria di contenuto deve essere derivata da un caso specifico di utilizzo aziendale. Le categorie con definizione più specifica definire sono migliori di quelle con definizione più generica. Vedere "Scelte consigliate per la definizione del set di training" a pagina 656.
Set di training positivo	Archiviare e caricare il numero consigliato di documenti di esempio (250) per il set di training positivo o quantomeno il numero minimo (50). Vedere "Linee guida per le dimensioni del set di training" a pagina 657.
Set di training negativo	Archiviare e caricare i documenti di esempio per il set di training negativo. Il set di training negativo contiene nel migliore dei casi un numero di documenti correttamente categorizzati simile a quello del set di training positivo. Aggiungere inoltre alcuni documenti con contenuto generico o neutrale al set di training negativo. Vedere "Linee guida per le dimensioni del set di training" a pagina 657.
Dimensionamento profilo	Può essere utile regolare l'assegnazione di memoria sul valore minimo. Test interni hanno dimostrato che riducendo l'assegnazione di memoria al minimo l'accuratezza può risultare migliorata. Vedere "Linee guida per il dimensionamento del profilo" a pagina 658.
Qualità del set di training	Rifiutare il risultato del training e riorganizzare i documenti di esempio se uno dei valori base di accuratezza del training è superiore al 5%. Vedere "Scelte consigliate per accettare o rifiutare un profilo" a pagina 659.
Regolazione del profilo	Eseguire il test negativo per regolare il profilo VML con un insieme di dati testabili. Vedere "Test e ottimizzazione dei profili VML" a pagina 648.
Distribuzione profilo	Rimuovere i profili accettati non utilizzati dalle politiche per ridurre il carico del server di rilevamento. Adattare il valore Soglia di similarità prima di distribuire un profilo alla produzione su tutti gli endpoint, per evitare il sovraccarico della rete. Vedere "Consigli per la distribuzione di profili" a pagina 661.

Quando utilizzare VML

Lo scopo di VML è di proteggere il contenuto non strutturato che è soprattutto basato su testo. VML è appropriato per la protezione di contenuto riservato altamente distribuito che non è possibile o pratico contrassegnare con impronta digitale. VML è inoltre utile nel proteggere

contenuto sensibile che non è possibile descrivere adeguatamente e per raggiungere un'elevata accuratezza della corrispondenza.

La tabella seguente riassume i casi d'uso consigliati per VML.

Tabella 24-18 Usi consigliati per VML

Utilizzare VML quando	Descrizione
Non è possibile o pratico contrassegnare con impronta digitale tutti i dati che si desidera proteggere.	<p>Spesso la raccolta di tutto il contenuto che si desidera proteggere per acquisirne l'impronta è un'attività impossibile. Questa situazione si ha per molte forme di dati non strutturati: materiale marketing, documenti finanziari, dati di pazienti, formule di prodotti, codice sorgente e così via.</p> <p>VML è appropriato per questa situazione poiché non è necessario raccogliere tutto il contenuto che si desidera proteggere. È sufficiente raccogliere un numero ridotto di documenti di esempio.</p>
Non è possibile descrivere adeguatamente i dati che si desidera proteggere.	<p>Spesso descrivere i dati che si desidera proteggere è difficile senza sacrificare una certa accuratezza. Questa situazione può verificarsi quando si hanno lunghe liste di parole chiave difficili da generare, adattare e mantenere.</p> <p>VML risulta utile in queste situazioni perché modella automaticamente le funzionalità (parole chiave) che si desidera proteggere. Consente di gestire e aggiornare il contenuto di origine.</p>
Una politica restituisce falsi positivi frequenti.	<p>A volte una determinata categoria di informazioni è un'origine costante di falsi positivi. Ad esempio, un report sulle vendite settimanali può produrre spesso falsi positivi per una politica Identificatore dati che cerca numeri di previdenza sociale.</p> <p>VML può rivelarsi utile in questa situazione perché è possibile eseguire il training in base al contenuto che causa i falsi positivi e creare un'eccezione della politica affinché ignori quelle funzionalità.</p> <p>Nota: I contenuti con falsi positivi devono appartenere a una categoria ben definita affinché VML sia una soluzione efficace per questo caso d'uso. Vedere "Scelte consigliate per la definizione del set di training" a pagina 656.</p>

Quando non utilizzare il VML

Il VML non è progettato per proteggere dati strutturati, ad esempio informazioni che consentono l'identificazione dell'utente, o contenuto binario, come documenti che contengono file di grafica o di immagine.

Nella tabella riportata di seguito sono riepilogati gli utilizzi non consigliati del VML.

Tabella 24-19 Utilizzi non consigliati per il VML

Non utilizzare il VML per	Spiegazione
Proteggere informazioni che consentono l'identificazione dell'utente	L'EDM (Exact Data Matching) e gli identificatori dati rappresentano l'opzione migliore per proteggere i tipi comuni di informazioni che consentono l'identificazione dell'utente.
Proteggere i file binari e le immagini	L'IDM (Indexed Document Matching) è l'opzione migliore per proteggere il contenuto che è prevalentemente binario, ad esempio file di immagine o file CAD.

Scelte consigliate per la definizione del set di training

Una categoria VML è il caso di utilizzo aziendale specifico da cui si derivano i documenti di esempio per il training del profilo VML. Più specifica è la categoria, migliori sono i risultati di rilevamento. Ad esempio, la categoria "Documenti finanziari" non è consigliata perché è troppo ampia. Una classificazione migliore della categoria è "Previsioni vendite" o "Guadagni trimestrali" perché ciascuna categoria fa riferimento a un caso di utilizzo aziendale specifico.

Una categoria VML comprende il contenuto di due set di training: positivo e negativo. Il set di training positivo include contenuto da proteggere, mentre il set di training negativo comprende contenuto che si desidera ignorare. È necessario derivare entrambi i set di training positivo e negativo dalla stessa categoria di contenuto in modo che tutti i documenti siano correlati da un punto di vista tematico.

Utilizzare esclusivamente contenuto generico per il set di training negativo, per quanto possibile, non è consigliato. Benché il contenuto generico produca buoni livelli di precisione di training in fase di realizzazione, non è possibile rilevare il contenuto che si desidera proteggere durante il runtime con precisione sufficiente.

Nota: sebbene un set di training negativo esclusivamente generico non sia consigliato, il seeding del set di training negativo con alcuni documenti con contenuto neutro ha qualche valore. Vedere ["Linee guida per le dimensioni del set di training"](#) a pagina 657.

Nella tabella seguente sono illustrati alcuni esempi di categorie e set di training positivi e negativi possibili che comprendono tali categorie.

Tabella 24-20 Esempi di categorie e set di training

Categoria	Set di training positivo	Set di training negativo
Codice sorgente del prodotto	Codice sorgente del prodotto personalizzato	Codice sorgente di progetti Open Source
Formule di prodotti	Formule di prodotti personalizzati	Informazioni sui prodotti non personalizzati

Categoria	Set di training positivo	Set di training negativo
Guadagni trimestrali	Guadagni precedenti, stime di vendite, documenti contabili	Dettagli dei conti annuali pubblicati
Piani di marketing	Piani di marketing	Materiale di marketing pubblicato e testi pubblicitari
Cartelle cliniche	Cartelle cliniche dei pazienti	Documenti sanitari
Vendite dei clienti	Comportamento di acquisto dei clienti	Dati dei consumatori accessibili al pubblico
Fusioni e acquisizioni	Documenti legali riservati, documenti di fusioni e acquisizioni	Materiali accessibili al pubblico, comunicati stampa
Metodi di fabbricazione	Metodi di fabbricazione e ricerca personalizzati	Standard di settore

Linee guida per le dimensioni del set di training

L'accuratezza di VML è direttamente proporzionale a quella del contenuto di esempio utilizzato per il training. Per usare VML non è necessario individuare tutti i dati che si desidera proteggere, né è necessario descriverli. Piuttosto, i documenti di esempio devono rappresentare con precisione il tipo di contenuto che si desidera proteggere e rappresentare il contenuto che si desidera ignorare. Questo contenuto deve essere correlato al contenuto positivo dal punto di vista tematico.

Un maggior numero di documenti di esempio raccolti per il training genera profili VML più precisi. Una categoria di contenuto ben definita contiene 500 documenti di esempio: 250 positivi e 250 negativi. Il numero minimo di documenti per set di training è 50.

Idealmente, è necessario raccogliere un numero simile di documenti negativi e positivi per il training. È necessario distribuire nel set di training negativo documenti generici o di contenuto neutro. Il file archivio `DLP_Wikipedia_sample.zip` allegato a questa guida nel centro di supporto Symantec viene fornito a tale scopo.

Ad esempio, il set di training positivo contiene 250 documenti di esempio e il set di training negativo contiene 150 documenti. È possibile aggiungere da 100 a 200 documenti generici al set di training negativo dal file archivio `DLP_Wikipedia_sample.zip`. Il testing interno ha dimostrato che l'aggiunta di contenuto generico per complementare un insieme di training altrimenti ben definito di training può migliorare l'accuratezza di VML.

Se non è possibile raccogliere abbastanza documenti positivi per soddisfare il requisito minimo, è possibile caricare più volte il set di training di dimensioni insufficienti. Ad esempio, considerare un caso in cui si dispone della categoria di contenuti "Previsioni vendite". Per tale categoria sono stati raccolti 25 fogli elettronici positivi e 50 documenti negativi. In questo caso, è possibile

caricare il set di training positivo due volte per raggiungere la soglia minima di documenti e uguagliare il numero di documenti negativi. Tenere presente che questa tecnica va utilizzata solo per scopi di sviluppo e testing. Per il training dei profili di produzione è necessario utilizzare un numero di documenti non inferiore al minimo per entrambi i set di training.

Tabella 24-21 elenca il numero di documenti ottimale, consigliato e minimo da includere in ciascun set di training.

Nota: Ai fini delle presenti linee guida per il set di training, si presuppongono dimensioni medie dei documenti pari a 3 KB. Se si dispone di documenti più grandi, un numero inferiore può essere sufficiente.

Tabella 24-21 Linee guida per le dimensioni dei set di training

Set di training	Minimo	Consigliato
Documenti di esempio positivi	50	250
Documenti di esempio negativi	50	250
Numero totale di documenti per la categoria	100	500

Scelte consigliate per il caricamento di documenti per il training

Anche se è possibile caricare singoli documenti su Enforce Server per il training, si consiglia di caricare un archivio di documenti (ZIP, RAR, TAR) contenente i documenti di esempio per ciascun set di training. La dimensione massima di caricamento è 30 MB. Non esiste alcuna limite di dimensione per il set di training.

Per raccogliere i documenti per il training, si consiglia di creare un'area di gestione temporanea. Ad esempio considerare una categoria denominata "Report di vendita". In questo caso creare una cartella denominata `\VML\area_gestione_temporanea\report_vendita` che rappresenta la categoria. In questa cartella creare due sottocartelle: una per il set di training positivo e l'altra per il set di training negativo (ad esempio, `\VML\area_gestione_temporanea\report_vendita\positivo`). Quando si è pronti a eseguire il training del profilo, comprimere la sottocartella positiva e la sottocartella negativa in archivi di documenti distinti. È possibile partizionare il set di training tra gli archivi se si dispone di più di 30 MB di dati da caricare per un set di training. Non incorporare un archivio dentro un altro.

Linee guida per il dimensionamento del profilo

Prima di eseguire il training di un profilo VML è possibile regolare la quantità di memoria assegnata al profilo. La quantità di memoria assegnata determina la quantità di caratteristiche dei modelli di sistema, che a sua volta ha effetto sulle dimensioni del profilo. Maggiore è

l'impostazione di allocazione di memoria, più approfondita è l'estrazione di funzionalità e la definizione del modello e più grandi sono le dimensioni del profilo. In genere, per il rilevamento di politiche basate su server l'impostazione di allocazione di memoria consigliata è Alta, che è anche l'impostazione predefinita.

Nell'endpoint, il profilo VML viene assegnato al computer host e caricato in memoria da DLP Agent. (A differenza di EDM e IDM, VML non si basa sul rilevamento in due fasi per le politiche endpoint.) Poiché la memoria sull'endpoint è limitata, è consigliabile assegnare memoria Bassa o Media per le politiche di endpoint. Prove interne hanno mostrato che riducendo l'assegnazione di memoria non si riduce l'accuratezza del profilo, che anzi può risultare migliorata in determinate situazioni.

Tabella 24-22 Consigli per l'allocazione di memoria

Allocazione memoria	Descrizione
Alta	Impostazione predefinita, in genere appropriata per il rilevamento basato su server.
Media	Utilizzare questa impostazione per ridurre le dimensioni del profilo.
Bassa	Utilizzare questa impostazione per il rilevamento di endpoint.

Scelte consigliate per accettare o rifiutare un profilo

Quando si esegue il training di un profilo VML in base al contenuto di categoria, il sistema seleziona le funzionalità, crea il modello e calcola i livelli di precisione di base per i falsi positivi e i falsi negativi. I livelli di precisione di base vengono calcolati con un processo standard, generalmente accettato, denominato valutazione k-fold. I livelli di precisione di base rappresentano un primo indicatore della qualità dei set di training della categoria.

Per illustrare come funziona il processo di valutazione k-fold, si presupponga di disporre di una categoria con 500 documenti di esempio totali: 250 positivi e 250 negativi. Durante l'esecuzione del training, il sistema divide il set di training in 10 fold. Ciascun fold è un sottoinsieme distinto del set di training complessivo e contiene documenti di esempio positivi e negativi. Il sistema utilizza nove fold per generare un profilo VML e un fold per testare il profilo. Qualsiasi fold può diventare il fold di test per la prima serie di valutazione. Per la serie successiva, il fold successivo nella coda diventa il fold di test. Questo processo viene ripetuto per tutti i 10 fold. Il sistema esegue un training finale detto cross-fold, calcola la media dei risultati di tutti i fold e genera il modello finale.

Al termine del processo di training, il sistema visualizza i livelli di precisione medi e chiede all'utente di accettare o rifiutare il profilo di training. Il livello di precisione dei falsi positivi è la percentuale dei documenti di test negativi classificati erroneamente come positivi. Il livello di precisione dei falsi negativi è la percentuale dei documenti di test positivi classificati erroneamente come negativi. Come regola generale è necessario rifiutare il profilo di training se uno dei due livelli è superiore al 5%.

Nota: è possibile utilizzare il file di registro `machinelearning_training.log` per valutare i livelli di precisione del training per fold.

Vedere ["File di log per la risoluzione dei problemi del training VML e del rilevamento di politiche"](#) a pagina 652.

Linee guida per l'accettazione o il rifiuto dei risultati del training

Decidere se accettare o rifiutare un profilo di training basato sulle percentuali di falsi positivi e falsi negativi che il sistema visualizza alla fine del processo di training.

Vedere ["Informazioni sulla soglia di similarità e sul punteggio di somiglianza"](#) a pagina 632.

Per comprendere meglio come il sistema calcola i livelli di precisione del set di training del profilo Machine Learning, si consideri l'esempio riportato di seguito.

Si dispone di un set di training che include 1.000 documenti, 500 positivi e 500 negativi. Quando si esegue il training del profilo, il sistema prende il 90% dei documenti, ne estrae le funzionalità e crea un modello. Prende il restante 10% dei documenti e ne valuta le funzionalità in base al modello in termini di similarità. Quindi produce livelli di precisione per falsi positivi e falsi negativi. Questo processo è noto come "fold". Per ogni set di training, il sistema valuta dieci fold. Ogni volta confronta un 10% diverso dei documenti in base al 90%. Al termine del ciclo, il sistema esegue una valutazione incrociata di tutti i dieci fold. Quindi genera un livello percentuale di precisione medio per le categorie positive e negative.

Sempre in questo esempio si presupponga che il risultato del processo di training generi un'incidenza di falsi positivi di base pari a circa 1,2% e un'incidenza di falsi negativi di base uguale a circa 1%. In media l'1,2% dei documenti negativi nel set di training è categorizzato erroneamente come positivo e l'1% dei documenti nel set di training è categorizzato erroneamente come negativo. Mentre l'obiettivo è 0% per entrambe le incidenze, in generale un'incidenza percentuale inferiore al 5% per ciascuna categoria è accettabile.

Le percentuali restituite alla fine del processo di training sono medie dei 10 fold. Piuttosto che affidarsi alla regola generale del 5%, è preferibile esaminare i risultati dell'incidenza percentuale per ciascun fold. Per controllare le percentuali, esaminare il file di registro

`\ProgramData\Symantec\Data Loss Prevention\Enforce`

`Server\15.1\Protect\logs\debug\mld0.log (Windows) o`

`/var/log/Symantec/DataLossPrevention/Detection Server/15.1/debug/mld0.log`

(Linux). Come illustrato sotto, le singole incidenze di fold restituiscono una lettura per ciascuno dei dieci fold su cui si basa la decisione di accettare o rifiutare il profilo.

Tabella 24-23 Processo di valutazione della precisione del set di training

Valutazione fold	Livelli di precisione delle categorie per fold e medie cross-fold	
Fold 0	Incidenza di falsi positivi 2,013422727584839	Incidenza di falsi negativi 0,0

Valutazione fold	Livelli di precisione delle categorie per fold e medie cross-fold	
Fold 1	Incidenza di falsi positivi 1,3513513803482056	Incidenza di falsi negativi 1,7857142686843872
Fold 2	Incidenza di falsi positivi 1,3513513803482056	Incidenza di falsi negativi 0,8928571343421936
Fold 3	Incidenza di falsi positivi 1,3513513803482056	Incidenza di falsi negativi 1,7857142686843872
Fold 4	Incidenza di falsi positivi 1,3513513803482056	Incidenza di falsi negativi 0,8928571343421936
Fold 5	Incidenza di falsi positivi 1,3513513803482056	Incidenza di falsi negativi 2,6785714626312256
Fold 6	Incidenza di falsi positivi 0,0	Incidenza di falsi negativi 0,0
Fold 7	Incidenza di falsi positivi 0,6756756901741028	Incidenza di falsi negativi 0,0
Fold 8	Incidenza di falsi positivi 1,3513513803482056	Incidenza di falsi negativi 0,8928571343421936
Fold 9	Incidenza di falsi positivi 1,3513513803482056	Incidenza di falsi negativi 1,8018018007278442
Cross-fold	Incidenza di falsi positivi media 1,214855808019638	Incidenza di falsi negativi media 1,0730373203754424

Consigli per la distribuzione di profili

I profili VML accettati vengono trasferiti a ogni server di rilevamento e DLP Agent Symantec, anche se tali profili non sono richiesti dalle politiche attive sul server o sull'endpoint. I server di rilevamento caricano tutti i profili VML in memoria indipendentemente dal fatto che in tali server siano distribuite politiche VML associate. I DLP Agent caricano solo i profili VML richiesti da una politica attiva. Per ottimizzare le prestazioni del server, è consigliabile non distribuire (accettare) profili VML non necessari e rimuovere eventuali profili VML accettati (distribuiti) non richiesti dalle politiche attive.

Inoltre, quando si modifica la soglia di similarità il sistema risincronizza l'intero profilo con i server di rilevamento e i DLP Agent. Se si dispone di un profilo VML di grandi dimensioni e sono presenti possibili limitazioni di larghezza di banda (ad esempio la distribuzione a molti endpoint), ciò può causare una congestione della rete. In tal caso è consigliabile provare e mettere a punto il profilo su alcuni endpoint prima di distribuirlo in produzione a tutti gli endpoint della rete.

Rilevamento del contenuto mediante Riconoscimento moduli - Riconoscimento di immagini riservate

Il capitolo contiene i seguenti argomenti:

- [Informazioni sul rilevamento Riconoscimento moduli](#)
- [Configurazione del rilevamento Riconoscimento moduli](#)
- [Gestione dei profili di Riconoscimento moduli](#)
- [Impostazioni di server avanzate per il riconoscimento moduli](#)
- [Visualizzazione di un incidente di Riconoscimento moduli](#)

Informazioni sul rilevamento Riconoscimento moduli

Il Riconoscimento moduli fornisce la possibilità di rilevare i moduli che contengono informazioni sensibili, come moduli fiscali, sanitari, assicurativi e così via.

Il Riconoscimento moduli rileva immagini di modulo in diversi formati immagine, compresi i seguenti:

- PDF (solo versione 1.2 e successive)
- PDF che usano il formato AcroForms

- XFA (è supportata solo l'immagine stampata, o l'immagine visualizzata se si stampa il modulo. Le copie elettroniche, come i moduli compilabili, non sono supportate. Inoltre, l'estrazione del testo da XFA non è supportata)
- JPEG (.jpg, .jpeg)
- PNG
- TIFF (pagina singola o multipla, .tif o .tiff)
- Bitmap (.bmp, .dib)

Il Riconoscimento moduli è disponibile per Network Monitor, Network Prevent for Email, Network Prevent for Web e Network Discover. Il Riconoscimento moduli non è disponibile per Endpoint Discover, Endpoint Prevent o i rilevatori di cloud.

Vedere ["Configurazione del rilevamento Riconoscimento moduli"](#) a pagina 664.

Come funziona il riconoscimento dei moduli

Symantec Data Loss Prevention analizza le caratteristiche dei moduli vuoti e archivia i risultati come caratteristiche principali nel profilo Riconoscimento moduli. Tale processo viene definito indicizzazione. Durante la rilevazione, il server di rilevazione confronta le immagini nel traffico di rete o archiviate in archivi dati con i moduli indicizzati. La misura in cui il modulo rilevato corrisponde alle caratteristiche principali del modulo vuoto indicizzato viene chiamata "allineamento". Per impostazione predefinita, la corrispondenza si verifica quando l'85% delle caratteristiche principali corrisponde o si allinea al modulo.

Il confronto tra l'immagine rilevata e il modulo vuoto indicizzato consente inoltre a Symantec Data Loss Prevention di determinare in che misura il modulo è stato compilato. La soglia di riempimento è rappresentata da un intervallo compreso tra 1 e 10, dove 1 rappresenta il modulo compilato al minimo e 10 è il modulo interamente compilato. La soglia di riempimento consente di specificare quando Symantec Data Loss Prevention crea un incidente. Una soglia bassa crea più incidenti rilevando moduli compilati parzialmente, moduli compilabili elettronicamente contenenti almeno un'opzione compilata o moduli non completati. Una soglia alta crea meno incidenti, ma non rileva tutte le possibili perdite di dati. Una soglia di riempimento di 0 rileva tutti i moduli corrispondenti, inclusi i moduli vuoti. Per impostazione predefinita, la soglia di riempimento per un profilo Riconoscimento moduli è 1. È possibile specificare un altro valore quando si crea un profilo. È anche possibile regolare questo valore per un profilo esistente per ottimizzare i risultati di rilevazione.

Vedere ["Configurazione del rilevamento Riconoscimento moduli"](#) a pagina 664.

Vedere ["Gestione dei profili di Riconoscimento moduli"](#) a pagina 668.

Configurazione del rilevamento Riconoscimento moduli

Per configurare il Riconoscimento moduli, raccogliere un set vuoto di moduli che si desidera proteggere e aggiungerli a un archivio ZIP di file PDF a pagina singola. Questo archivio ZIP è chiamato **Archivio galleria**. Caricare quindi l'archivio galleria in un profilo Riconoscimento moduli in Enforce Server per l'indicizzazione. Enforce Server indicizza i moduli e spinge l'indice fuori dai server di rilevazione. Specificare inoltre la Soglia di riempimento per il profilo: la soglia di riempimento specifica la quantità di compilazione del modulo che attiva la creazione di un incidente.

[Tabella 25-1](#) fornisce un flusso di lavoro ad alto livello per la configurazione del rilevamento di Riconoscimento moduli:

Tabella 25-1 Flusso di lavoro Riconoscimento moduli

Passaggio	Azione	Ulteriori informazioni
1	Raccogliere e preparare copie vuote dei moduli che si desidera proteggere.	Vedere "Preparazione di un archivio della galleria Riconoscimento moduli" a pagina 664.
2	Configurare un profilo Riconoscimento moduli. Specificare l'archivio della galleria con i moduli che si desidera rilevare e una soglia di riempimento per la creazione di incidenti.	Vedere "Configurazione del profilo Riconoscimento moduli" a pagina 666.
3	Configurare una politica con una regola di rilevamento o di eccezione di riconoscimento moduli mediante il profilo Riconoscimento moduli.	Vedere "Configurazione della regola di rilevamento di riconoscimento moduli" a pagina 666. Vedere "Configurazione della regola di eccezione Riconoscimento moduli" a pagina 667.

Preparazione di un archivio della galleria Riconoscimento moduli

L'archivio della galleria Riconoscimento moduli è un archivio ZIP che contiene copie PDF a pagina singola dei moduli vuoti che si desidera proteggere. L'archivio della galleria consente di creare un profilo Riconoscimento moduli.

Symantec consiglia di indicizzare non più di 500 immagini in totale in tutti i profili Riconoscimento moduli. Per migliorare le prestazioni, Symantec consiglia di creare meno profili contenenti più moduli, anziché più profili contenenti meno moduli.

Per i migliori risultati, assicurarsi che le immagini di moduli nell'archivio della galleria rispettino le seguenti linee guida:

- I file PDF che contengono le immagini dei moduli devono avere una risoluzione di almeno 200 DPI.
- I moduli con campi compilabili elettronicamente devono essere nel formato AcroForm. Altri formati di modulo interattivo non sono supportati per il rilevamento.
- Ogni modulo deve avere una quantità sufficiente di testo e di contenuto grafico. I moduli con poco contenuto possono causare un numero superiore di corrispondenze false.
- Ogni modulo deve contenere contenuto univoco. I moduli che condividono contenuto molto simile sono più difficili da abbinare e possono causare corrispondenze false. Ad esempio, i moduli di imposta del 2014 e 2015 condividono molte funzionalità che sarebbe difficile rilevare se si trovassero nello stesso profilo.
- Ogni modulo deve presentare contenuto distribuito in tutta la pagina. I moduli con contenuto raggruppato e aree vuote sono più difficili da abbinare.
- Ogni modulo deve presentare uno sfondo bianco o di colore chiaro. Gli sfondi neri o scuri non sono supportati.

Per preparare un archivio della galleria di riconoscimento moduli

- 1 Raccogliere copie vuote dei moduli che si desidera rilevare.
- 2 Salvare tutte le copie in bianco dei moduli come file PDF. Considerare le seguenti linee guida nella preparazione dei file PDF:
 - La galleria deve contenere solo file PDF. Symantec Data Loss Prevention ignora tutte le altre cartelle e i file nell'archivio ZIP.
 - Se un modulo presenta due o più pagine, separarle in file a pagina singola, quindi convertirle in formato PDF.
Ad esempio, se il modulo è un file unico di Microsoft Word da tre pagine intitolato `YourForm.docx`, separare il file in tre file singoli da una pagina l'uno, quindi convertirli in PDF:
 - `YourForm_1of3.PDF`
 - `YourForm_2of3.PDF`
 - `YourForm_3of3.PDF`
 - Se il modulo contiene campi compilabili elettronicamente, utilizzare uno strumento di modifica PDF per il processo di conversione che mantenga la formattazione AcroForms, ad esempio Adobe Acrobat.
 - Se il modulo include diverse pagine di boilerplate non compilabile, aggiungere solo le pagine compilabili all'archivio della galleria.
- 3 Aggiungere tutti i file PDF a un archivio ZIP.

Configurazione del profilo Riconoscimento moduli

Configurare un profilo Riconoscimento moduli caricando un archivio galleria e specificando una Soglia di riempimento.

Vedere "[Preparazione di un archivio della galleria Riconoscimento moduli](#)" a pagina 664.

Per configurare e indicizzare un profilo Riconoscimento moduli

- 1 Passare a **Gestisci > Profili dati > Riconoscimento moduli** per visualizzare la schermata **Profili di riconoscimento moduli**.
- 2 Fare clic su **Aggiungi profilo** per visualizzare **Configura profilo di riconoscimento moduli**.
- 3 Immettere un nome per il profilo nel campo **Nome**.

Nota: Il nome immesso viene utilizzato durante la configurazione di politiche e viene visualizzato nell'istantanea incidente per gli incidenti Riconoscimento moduli.

- 4 (Facoltativo) Immettere una descrizione per il profilo nel campo **Descrizione**.
- 5 Immettere un valore nel campo **Soglia di riempimento**.

La soglia di riempimento è compresa tra 1 e 10, dove 1 rappresenta un modulo completato in maniera minima e 10 un modulo completato totalmente. È inoltre possibile immettere 0 per rilevare moduli vuoti.

Nota: Per i moduli compilati elettronicamente, immettendo 1 come soglia di riempimento vengono rilevati gli oggetti compilati elettronicamente in un modulo. Ad esempio, impostando la soglia su 1 viene rilevata una singola casella di controllo selezionata. Per contro, impostando la soglia su 1 potrebbe non venire rilevata una casella di controllo simile compilata a penna.

- 6 Caricare l'archivio della galleria facendo clic su **Sfoglia** e selezionando il file ZIP dell'archivio della galleria.
- 7 Fare clic su **Salva** per avviare l'indicizzazione del profilo.

Quando la galleria completa l'indicizzazione, è possibile utilizzarlo per configurare una regola Riconoscimento moduli in una politica.

Vedere "[Configurazione della regola di rilevamento di riconoscimento moduli](#)" a pagina 666.

Configurazione della regola di rilevamento di riconoscimento moduli

Configurare la regola di rilevamento specificando un profilo Riconoscimento moduli.

Vedere ["Configurazione del profilo Riconoscimento moduli"](#) a pagina 666.

I moduli indicizzati nel profilo vengono confrontati rispetto ai moduli rilevati per determinare se corrispondono. La regola di riconoscimento moduli cerca corrispondenze solo negli allegati.

Per configurare la regola di rilevamento di riconoscimento moduli

- 1 Andare a **Gestisci politiche > Elenco politiche**, fare clic su **Nuovo** e creare una nuova politica vuota o una politica da un modello.

Vedere ["Aggiunta di una nuova politica o di un modello di politica"](#) a pagina 421.

- 2 Fare clic su **Aggiungi regola** nella scheda **Rilevamento** per visualizzare **Configura politica - Aggiungi regola**.
- 3 Selezionare **Esegui rilevamento utilizzando il profilo Riconoscimento moduli** nella sezione **Riconoscimento moduli** e selezionare il profilo Riconoscimento moduli che contiene i moduli da proteggere.
- 4 Fare clic su **Avanti** per visualizzare la pagina **Configura politica - Modifica regola**.
- 5 Immettere un nome per la regola nel campo **Nome regola**.
- 6 Scegliere la gravità della regola.
Vedere ["Gravità delle politiche"](#) a pagina 379.
- 7 Selezionare le condizioni per la regola di rilevamento Riconoscimento moduli.
È possibile utilizzare il campo **Confronta anche** per configurare le condizioni di corrispondenza composta. Vedere ["Condizioni composte"](#) a pagina 401.
- 8 Fare clic su **OK** per aggiungere la regola di rilevamento.
- 9 Fare clic su **Salva** per applicare la regola di rilevamento alla politica.
La nuova politica viene visualizzata nell' **Elenco politiche**.

Configurazione della regola di eccezione Riconoscimento moduli

Configurare la regola di eccezione specificando un profilo Riconoscimento moduli.

Vedere ["Configurazione del profilo Riconoscimento moduli"](#) a pagina 666.

Per configurare la regola di eccezione Riconoscimento moduli

- 1 Andare a **Gestisci politiche > Elenco politiche**, fare clic su **Nuovo** e creare una nuova politica vuota o una politica da un modello.
Vedere ["Aggiunta di una nuova politica o di un modello di politica"](#) a pagina 421.
- 2 Fare clic su **Aggiungi eccezione** nella scheda **Rilevamento** per visualizzare **Configura politica - Aggiungi eccezione**.

- 3

Selezionare **Esegui rilevamento utilizzando il profilo Riconoscimento moduli** nella sezione **Riconoscimento moduli** e selezionare il profilo **Riconoscimento moduli** che contiene i moduli da proteggere.
- 4

Fare clic su **Avanti** per visualizzare la pagina **Configura politica - Modifica eccezione**.
- 5

Immettere un nome per l'eccezione nel campo **Nome eccezione**.
- 6

Selezionare le condizioni per la regola di rilevamento Riconoscimento moduli.
È possibile utilizzare il campo **Confronta anche** per configurare le condizioni di corrispondenza composta. Vedere "[Condizioni composte](#)" a pagina 401.
- 7

Fare clic su **OK** per aggiungere la regola di eccezione.
- 8

Fare clic su **Salva** per applicare la regola di rilevamento alla politica.

La nuova politica viene visualizzata nell' **Elenco politiche**.

Gestione dei profili di Riconoscimento moduli

La schermata **Profili di riconoscimento moduli** (**Gestisci > Profili dati > Riconoscimento moduli**) fornisce una vista riepilogativa di tutti i profili di Riconoscimento moduli. È possibile utilizzare questa schermata per confermare che un profilo è stato indicizzato correttamente, visualizzare lo stato dell'indicizzazione e così via.

Tabella 25-2 Dettagli dei profili di Riconoscimento moduli

Elemento	Descrizione
Aggiungi profilo	Fare clic su Aggiungi profilo per configurare un nuovo profilo di riconoscimento moduli. Vedere " Configurazione del profilo Riconoscimento moduli " a pagina 666.
Mostra voci	Selezionare un valore da Mostra voci per specificare il numero di profili che è possibile visualizzare su questa pagina.
Spostamento sulle pagine	È possibile utilizzare i seguenti pulsanti per cambiare la visualizzazione dei profili: <ul style="list-style-type: none">Fare clic su Ultimo per visualizzare i profili con le date più recenti in ordine ascendente.Fare clic su un numero per accedere a tale specifico numero di pagina.Fare clic su Avanti per visualizzare la pagina successiva.Fare clic su Precedente per visualizzare la pagina precedente.

Elemento	Descrizione
Nome profilo	<p>Fare clic sul Nome profilo per visualizzare o modificare il profilo.</p> <p>Nota: È possibile ordinare i dati di una colonna in ordine ascendente (A-Z/1-3) facendo clic sulla freccia su o in ordine discendente (Z-A/3-1) facendo clic sulla freccia giù.</p>
Descrizione	<p>La descrizione del profilo. È possibile modificare la descrizione facendo clic sul nome del profilo o sull'icona della matita nella colonna Azioni.</p>
Stato	<p>Ogni profilo mostra uno dei seguenti stati:</p> <ul style="list-style-type: none"> ■ Galleria mancante o non valida indica che l'indicizzazione per il profilo non è riuscita. La galleria non si è caricata perché l'archivio ZIP non è valido. ■ Indicizzazione non avviata indica che l'indicizzazione per il profilo non è iniziata. La galleria caricata non è stata elaborata. ■ Indicizzazione in corso indica che è in corso l'indicizzazione della galleria caricata. ■ Profilo indicizzato indica che l'indicizzazione per questo profilo è completa e l'indice creato con successo. ■ Galleria non valida indica che l'indicizzazione per il profilo non è riuscita. La galleria caricata non ha avviato l'indicizzazione perché non è valida. ■ L'indice non contiene immagini indica che l'indicizzazione per il profilo non è riuscita. La galleria caricata non ha eseguito l'indicizzazione perché non contiene file compatibili. ■ Indicizzazione non riuscita indica che l'indicizzazione per questo profilo non è riuscita. La galleria caricata non è stata indicizzata. ■ Durante il processo di indicizzazione sono stati rilevati file inutilizzabili indica che l'indicizzazione per il profilo è stata completata con errori. Alcuni degli archivi nella galleria caricata non possono essere indicizzati.
Galleria	<p>Il nome dell'archivio della galleria.</p> <p>Non è possibile modificare il nome della galleria. È possibile caricare una nuova galleria o una galleria esistente che è stata rinominata facendo clic sul nome di profilo o sull'icona della matita nella colonna Azioni.</p>
Numero di moduli utilizzabili	<p>Il numero totale delle immagini di moduli nella galleria che sono state indicizzate senza errori e possono essere utilizzare in una politica.</p>
Data indicizzata	<p>La data in cui il profilo è stato indicizzato.</p>
Versione indice	<p>Il numero di versione dell'indice.</p>

Elemento	Descrizione
Soglia di riempimento	Il valore della soglia di riempimento fornito quando è stato configurato il profilo Riconoscimento moduli. È possibile modificare questo valore facendo clic sul nome del profilo o sull'icona della matita nella colonna Azioni .
Azioni	Fare clic sulla matita per modificare i dettagli del profilo. Fare clic sulla X rossa per eliminare un profilo. Se si elimina un profilo, il sistema rimuove i metadati del profilo e la galleria da Enforce Server.

Impostazioni di server avanzate per il riconoscimento moduli

In alcuni casi, per determinare quali impostazioni predefinite del server di riconoscimento moduli sono più adatte per le proprie esigenze, potrebbe essere necessario effettuare dei test e operazioni di ottimizzazione. È possibile modificare queste impostazioni alla pagina **Sistema > Server e rilevatori > Panoramica > Dettagli server/rilevatore - Impostazioni avanzate**. Symantec consiglia di contattare il supporto tecnico di Symantec prima di modificare delle impostazioni avanzate del server.

Sono disponibili nove impostazioni avanzate relative al riconoscimento moduli:

- ContentExtraction.ImageExtractorEnabled
- ContentExtraction.MaxNumImagesToExtract
- FormRecognition.ALIGNMENT_COEFFICIENT
- FormRecognition.CANONICAL_FORM_WIDTH
- FormRecognition.MAXIMUM_FORM_WIDTH
- FormRecognition.MINIMUM_FORM_ASPECT_RATIO
- FormRecognition.MINIMUM_FORM_WIDTH
- FormRecognition.OPENCV_THREADPOOL_SIZE
- FormRecognition.PRECLASSIFIER_ACTION

È possibile visualizzare i dettagli su queste impostazioni qui:

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Visualizzazione di un incidente di Riconoscimento moduli

È possibile visualizzare e riparare gli incidenti di Riconoscimento moduli come si farebbe con qualsiasi incidente di Symantec Data Loss Prevention. Vedere ["Informazioni sulla riparazione degli incidenti"](#) a pagina 1570.

Oltre alle informazioni di istantanea incidente consuete, gli incidenti di Riconoscimento moduli includono i seguenti elementi:

- Aree evidenziate in giallo sul modulo, che indicano gli elementi del modulo allineati e i campi elettronici compilati.
- Aree evidenziate in arancione sul modulo, che corrispondono alle aree discutibili.
- Un **Punteggio somiglianza** che indica la somiglianza degli elementi di modulo. Più alto è il punteggio, più i contenuti del campo sono statisticamente simili ai campi del modulo.

Rilevamento del contenuto mediante OCR - Riconoscimento di immagini riservate

Il capitolo contiene i seguenti argomenti:

- [Informazioni sul rilevamento dei contenuti con il riconoscimento OCR delle immagini riservate](#)
- [Requisiti di sistema del Server OCR](#)
- [Utilizzo del foglio di calcolo per la stima del dimensionamento per i server OCR](#)
- [Configurazione dei server OCR](#)
- [Installazione di una licenza di riconoscimento OCR delle immagini riservate](#)
- [Creazione di una configurazione OCR](#)
- [Utilizzo del motore OCR](#)
- [Ulteriori informazioni su lingue e dizionari](#)
- [Visualizzazione di incidenti OCR nei report](#)

Informazioni sul rilevamento dei contenuti con il riconoscimento OCR delle immagini riservate

Il riconoscimento OCR delle immagini riservate offre la possibilità di estrarre il testo dalle immagini (documenti acquisiti, schermate, immagini e così via) e dai PDF, consentendo di applicare regole di rilevamento testuale nuove o esistenti a questo contenuto.

Nota: L'estrazione di immagini dai file Microsoft Office non è supportata.

Il testo estratto entra quindi nella catena di rilevamento ed è elaborato allo stesso modo del testo estratto normalmente. Le istantanee incidenti per il testo OCR sono simili a quelle per testo estratto normalmente: viene visualizzata la porzione di testo, con le parole rilevate in evidenza. Gli incidenti OCR hanno indicatori visivi per indicare che il testo deriva da OCR e un'anteprima dell'immagine originale.

È possibile configurare OCR per utilizzare diverse lingue. Per migliorare i risultati del riconoscimento, è inoltre possibile scegliere un dizionario specializzato (ad esempio legale, finanziario o medico) per consentire un controllo ortografico supplementare. È inoltre possibile configurare un dizionario personalizzato relativo a nomi propri o altri termini specifici dell'azienda.

Benché l'estrazione di contenuti OCR possa integrarsi con i server di rilevamento sia Windows che Linux, Symantec supporta l'installazione del server OCR solo sui server Windows. L'estrazione del contenuto OCR non è supportata negli agenti Windows, negli agenti macOS, nei servizi cloud di Data Loss Prevention o nei dispositivi di Data Loss Prevention (sia virtuali che fisici). Per informazioni sulle versioni supportate dei server Windows, vedere la *Guida ai requisiti di sistema di Symantec Data Loss Prevention* all'indirizzo

<http://www.symantec.com/docs/DOC10602>

Nota: Il riconoscimento OCR delle immagini riservate di Symantec Data Loss Prevention è stato introdotto nella versione 15.0, ma la versione del server OCR non è legata a nessuna versione di Symantec Data Loss Prevention e può essere aggiornata indipendente.

Vedere "[Installazione di una licenza di riconoscimento OCR delle immagini riservate](#)" a pagina 676.

Tipi di rilevamento supportati per l'estrazione OCR

I seguenti tipi di rilevamento sono supportati per l'estrazione OCR:

- Network Monitor
- Network Prevent for Email

- Network Prevent for Web
- Network Discover

Tipi di file supportati per l'estrazione OCR

Le immagini nei seguenti tipi di file sono estratte e inviate a OCR:

- JPEG (.jpg, .jpeg)
- PNG
- TIFF (pagina singola o multipla, .tif o .tiff)
- Bitmap (.bmp)
- Immagini estratte da file PDF, come le pagine di un documento acquisito.

Requisiti di sistema del Server OCR

Il Server OCR presenta requisiti specifici a livello di hardware, sistema operativo e impostazioni server, diversi dai server di rilevamento e Data Loss Prevention Enforce Server. È possibile trovare le informazioni più recenti su questi requisiti nel centro di supporto Symantec all'indirizzo

<http://www.symantec.com/docs/doc10612.html>

Vedere "Utilizzo del foglio di calcolo per la stima del dimensionamento per i server OCR" a pagina 674.

Utilizzo del foglio di calcolo per la stima del dimensionamento per i server OCR

Il foglio di calcolo per la stima del dimensionamento per i server OCR consente di fare una stima del numero di server OCR necessari per ciascun server di rilevamento nella distribuzione corrente. Il foglio di calcolo e le istruzioni relative al suo utilizzo sono disponibili nel centro di supporto Symantec all'indirizzo

<http://www.symantec.com/docs/doc10612.html>

Vedere "Configurazione dei server OCR" a pagina 674.

Configurazione dei server OCR

L'estrazione dei contenuti OCR richiede anche l'installazione di un server OCR. Configurare il server OCR (micro servizio) dalla console di amministrazione di Enforce Server. Symantec consiglia di installare il server OCR su hardware dedicato, a causa dei suoi elevati requisiti di

elaborazione. È inoltre richiesto un certificato per la comunicazione tra il client OCR su Enforce Server e il server OCR.

Il server OCR è un server indipendente, separato da ogni server di rilevamento di Data Loss Prevention. È possibile configurare il server di rilevamento per comunicare con un indirizzo OCR (indirizzo IP o nome host). Tale indirizzo può essere un singolo server OCR o un singolo bilanciamento del carico davanti a diversi server OCR. È possibile utilizzare un bilanciamento del carico esterno o un'altra tecnologia, come Bilanciamento carico di rete di Windows.

Nota: un server di rilevamento può essere configurato solo con un singolo indirizzo del server OCR: l'indirizzo IP o il nome host di un singolo server OCR o l'indirizzo IP virtuale di un bilanciamento del carico (o di una coppia di bilanciamenti del carico) che è il front-end di più server OCR. Se si desidera configurare un server di rilevamento per comunicare con un pool di server OCR, il server di rilevamento è limitato a supportare la configurazione di singolo indirizzo del server OCR. Più server OCR devono avere come front-end un bilanciamento del carico che fornisce un indirizzo singolo.

Nel caso di un singolo server OCR, questo può essere installato su un computer separato o sullo stesso computer del server di rilevamento (opzione non consigliata). Le informazioni di configurazione sono incluse nella richiesta, quindi i server OCR possono soddisfare le richieste da diversi server di rilevamento con diverse configurazioni.

Ad esempio, è possibile configurare un server di rilevamento per rilevare l'inglese con la massima precisione OCR possibile. Quindi, è possibile configurare un altro server di rilevamento per rilevare il giapponese con la massima velocità possibile. In questo caso, lo stesso server OCR può gestire entrambi i tipi di richiesta. Symantec consiglia di installare il server OCR in un computer diverso dal server di rilevamento. Tuttavia, Symantec supporta la compresenza del server OCR con un server di rilevamento.

Installare un server OCR utilizzando la procedura guidata del programma di installazione del server OCR di Symantec DLP.

Per installare un server OCR

- 1 Aprire il **programma di installazione del server OCR**.
- 2 Fare doppio clic su **OCSServerInstaller64**.
- 3 Fare clic su **Avanti**.
- 4 Selezionare la **directory di destinazione** desiderata. Fare clic su **Avanti**. Viene eseguito il programma di installazione.
- 5 Fare clic su **Fine** al termine dell'installazione.

Ora il servizio OCR è in esecuzione e pronto a ricevere le richieste OCR.

Vedere ["Creazione di una configurazione OCR"](#) a pagina 676.

Installazione di una licenza di riconoscimento OCR delle immagini riservate

Quando si acquista Symantec Data Loss Prevention per la prima volta, si passa a una versione successiva, o si acquistano moduli supplementari del prodotto, è necessario installare uno o più file di licenza di Symantec Data Loss Prevention. I nomi dei file di licenza hanno formato `name.slf`.

Vedere Vedere ["Installazione di un nuovo file di licenza"](#) a pagina 237. per ulteriori informazioni sull'aggiunta di una licenza a Symantec Data Loss Prevention.

Vedere ["Requisiti di sistema del Server OCR"](#) a pagina 674.

Creazione di una configurazione OCR

Aggiunta di un profilo OCR

- 1 Accedere a **Sistema > Impostazioni > Configurazione del motore OCR**.
- 2 Fare clic su **Aggiungi configurazione del motore OCR**.

Configurazione del motore OCR

- 1 Immettere il **Nome** del profilo.
- 2 Immettere una **Descrizione** facoltativa del profilo.
- 3 Immettere il **Nome host del server OCR** relativo al server a cui vanno inviate le richieste OCR. Può essere un singolo bilanciamento del carico o un singolo server OCR.
- 4 Immettere il numero della **Porta** a cui vanno inviate le richieste. La porta predefinita è 8555.
- 5 Immettere il valore **Timeout motore OCR (secondi)**. Questa impostazione definisce il tempo prima del timeout di una richiesta OCR. Il timeout predefinito è 30.

Il timeout indica quanto tempo la richiesta può rimanere all'interno del server OCR e non comprende il tempo di transito o altri ritardi.

Il timeout deve essere definito con altre impostazioni di timeout del contenuto in Impostazioni avanzate. Come per le altre attività di estrazione dei contenuti, se si raggiunge il timeout, il componente OCR viene ignorato e il contenuto estratto in precedenza procede verso il rilevamento.

- 6 Immettere un valore per **Precisione o velocità**. Per impostazione predefinita, il server OCR imposta dinamicamente il valore per ogni documento. Il pre-classificatore di riconoscimento di immagini riservate sul server di rilevamento ispeziona ogni immagine e determina se è adatta per l'estrazione del contenuto OCR (e il riconoscimento moduli). Quindi determina quali valori predefiniti sono più adatti. Se si deseleziona questa casella, è possibile selezionare dei valori predefiniti da utilizzare per tutte le immagini. È possibile scegliere tra **Preciso**, **Bilanciato** e **Veloce**. Questa strategia può essere adatta per le scansioni di rilevamento, dove la precisione è più importante del tempo.
- 7 Nella sezione **Lingue supportate**, selezionare le lingue candidate per OCR.

È possibile selezionare una o più lingue e il server OCR ne sceglierà una dal pool da utilizzare per l'immagine. Symantec suppone che i documenti siano soprattutto in una lingua (ad esempio, tutto in francese o tutto in inglese, piuttosto che un insieme di inglese e francese). Il numero delle lingue deve essere il più piccolo possibile. Più lingue si selezionano, più lenta è la velocità di elaborazione.

Anche se non si seleziona una lingua, è comunque possibile ottenere del testo accurato in quella lingua. Ad esempio, è possibile selezionare l'inglese e il tedesco e inviare al server OCR un'immagine mista inglese-francese. Il server potrebbe scegliere l'inglese e restituire comunque del testo in francese. La selezione della lingua determina il dizionario di controllo ortografico da utilizzare. Determina inoltre il pool di caratteri tra i quali scegliere se l'immagine è poco chiara.
- 8 Nella sezione **Lingue e dizionari > Dizionari specializzati**, attivare il controllo ortografico supplementare per diversi settori (legale, finanziario, medico) in diverse lingue.
- 9 Nella sezione **Lingue e dizionari > Dizionario personalizzato**, specificare il nome del file di dizionario personalizzato per migliorare la precisione del riconoscimento. Ad esempio, se determinati nomi propri creano difficoltà per il server OCR, è possibile inserirli in questo dizionario personalizzato.

L'utilizzo dei dizionari e del controllo ortografico migliora i risultati del riconoscimento per le scansioni e le immagini di bassa qualità (come i fax). Se i caratteri sono chiari e nitidi, il motore li legge più facilmente e i dizionari sono meno utili.
- 10 Il dizionario personalizzato è un file di testo, con una voce per riga. Questo file di testo deve trovarsi nella directory del dizionario di ogni server, in
c:\Symantec\DLPOCR\Protect\bin.

Assegnazione di un profilo a un server di rilevamento

- 1 Accedere a **Sistema > Server e rilevatori > Panoramica**.
- 2 Selezionare un monitor.
- 3 Nella pagina **Dettagli server/rilevatore**, fare clic su **Configura**.

4 Nella pagina **Configura server**, fare clic su **Motore OCR**. In **Configurazione del motore OCR** selezionare la configurazione che si desidera utilizzare per il server.

5 Fare clic su **Salva**.

Vedere ["Utilizzo del motore OCR"](#) a pagina 678.

Utilizzo del motore OCR

È possibile consultare tutte le proprie configurazioni OCR e aggiungere una configurazione del motore OCR nella pagina **Configurazione del motore OCR**. In questa pagina è possibile:

- Fare clic su **Aggiungi configurazione del motore OCR** per aggiungere una nuova configurazione.
- Fare clic sul nome della configurazione o sull'icona della matita per modificare una configurazione esistente.
- Fare clic sulla **X** rossa per eliminare una configurazione.

Vedere ["Informazioni sul rilevamento dei contenuti con il riconoscimento OCR delle immagini riservate"](#) a pagina 673.

Vedere ["Visualizzazione di incidenti OCR nei report"](#) a pagina 680.

Ulteriori informazioni su lingue e dizionari

Anziché scegliere da un insieme di lingue, il server OCR suppone che nell'immagine possano essere presenti tutte le lingue selezionate. È una strategia valida quando si utilizzano documenti in più lingue, ma non si consiglia di selezionare più di quattro lingue, poiché può incidere negativamente sia sulla velocità che sulla precisione.

Dizionari specializzati disponibili per l'estrazione del contenuto OCR

I seguenti dizionari specializzati sono disponibili per l'estrazione del contenuto OCR:

- Dizionario legale olandese
- Dizionario medico olandese
- Dizionario finanziario inglese
- Dizionario legale inglese
- Dizionario medico inglese
- Dizionario legale francese
- Dizionario medico francese

- Dizionario legale tedesco
- Dizionario medico tedesco

Lingue supportate per l'estrazione OCR

Le seguenti lingue sono supportate per l'estrazione OCR:

- Arabo
- Cinese (semplificato)
- Cinese (tradizionale)
- Ceco
- Danese
- Olandese
- Inglese
- Finlandese
- Francese
- Tedesco
- Greco
- Ungherese
- Italiano
- Giapponese
- Coreano
- Norvegese
- Polacco
- Portoghese
- Portoghese (Brasile)
- Romani
- Russo
- Spagnolo
- Svedese
- Turco

Altre lingue possono essere rilevate se utilizzano uno dei set di caratteri supportati.

Visualizzazione di incidenti OCR nei report

Gli incidenti OCR sono contrassegnati e il testo rilevato è evidenziato in giallo nei report di incidente. Le anteprime della pagina sono incluse nell'incidente. Facendo clic su sull'anteprima è possibile visualizzare una versione più grande dell'immagine. Questa immagine contiene il testo estratto che viola la politica di Symantec Data Loss Prevention.

Rilevamento del contenuto mediante identificatori di dati

Il capitolo contiene i seguenti argomenti:

- [Introduzione agli identificatori di dati](#)
- [Configurazione delle condizioni della politica dell'identificatore dati](#)
- [Modifica degli identificatori dati di sistema](#)
- [Creazione di identificatori dati personalizzati](#)
- [Best practice per l'utilizzo degli identificatori dati](#)

Introduzione agli identificatori di dati

Symantec Data Loss Prevention fornisce degli identificatori di dati per rilevare specifiche istanze del contenuto descritto. Gli identificatori di dati consentono di implementare rapidamente e facilmente un metodo preciso di corrispondenza di dati in forma breve.

Gli identificatori di dati sono algoritmi che combinano la corrispondenza dei criteri con le convalide dei dati per rilevare il contenuto. I criteri sono simili alle espressioni regolari ma più efficaci in quanto ottimizzati per trovare corrispondenze precise con i dati. Le convalide sono controlli di accuratezza che delineano l'ambito del rilevamento e assicurano la conformità.

Ad esempio, l'identificatore di dati di sistema "Numero carta di credito" del sistema rileva i numeri che corrispondono a uno specifico criterio. Il criterio corrispondente viene convalidato mediante un algoritmo, ovvero il "controllo di Luhn". In questo caso la convalida viene eseguita sulle prime 15 cifre del numero che valuta per uguagliare la sedicesima cifra.

Symantec Data Loss Prevention fornisce identificatori di dati preconfigurati che è possibile utilizzare per rilevare dati riservati comunemente usati, quali numeri di carte di credito, previdenza sociale e patente di guida. La maggior parte degli identificatori di dati include tre coperture, ovvero ampia, media e limitata, in modo da poter affinare i risultati del rilevamento. Gli identificatori di dati offrono un ampio supporto per il rilevamento di contenuto internazionale.

Se un identificatore di dati definito dal sistema non soddisfa le esigenze, è possibile modificarlo. È anche possibile definire identificatori di dati personalizzati per rilevare tutto il contenuto che è possibile descrivere.

Vedere ["Identificatori di dati definiti dal sistema"](#) a pagina 682.

Vedere ["Selezione di una copertura dell'identificatore di dati"](#) a pagina 703.

Identificatori di dati definiti dal sistema

Symantec Data Loss Prevention fornisce parecchi identificatori di dati definiti dal sistema per consentire il rilevamento e la convalida di dati riservati basati su criteri.

Tabella 27-1 Identificatori di dati di sistema

Categoria	Descrizione
Identità personale	<p>Rilevano vari tipi di numeri di identificazione per le regioni di Africa, Asia Pacifico, Europa, America del Nord e America del Sud.</p> <p>Vedere Tabella 27-2 a pagina 683.</p> <p>Vedere Tabella 27-3 a pagina 683.</p> <p>Vedere Tabella 27-4 a pagina 684.</p> <p>Vedere Tabella 27-5 a pagina 690.</p> <p>Vedere Tabella 27-6 a pagina 691.</p>
Finanza	<p>Rilevano numeri di identificazione finanziari, come numeri di carta di credito e numeri di routing ABA.</p> <p>Vedere Tabella 27-7 a pagina 692.</p>
Sanità	<p>Rilevano codici di medicinali degli Stati Uniti e internazionali, nonché informazioni riservate basate su criteri relative al settore sanitario.</p> <p>Vedere Tabella 27-8 a pagina 692.</p>
Informatica	<p>Rilevano indirizzi IP.</p> <p>Vedere "Identificatori dati informatica" a pagina 693.</p>
Parole chiave internazionali	<p>Parole chiave internazionali per gli identificatori di dati PII.</p> <p>Vedere "Parole chiave internazionali per gli identificatori dati PII" a pagina 693.</p>

Identificatori dati dell'identità personale

Symantec Data Loss Prevention fornisce vari identificatori dati per rilevare le informazioni che consentono l'identificazione dell'utente per le regioni di Africa, Asia Pacifico, Europa, America del Nord e America del Sud.

La [Tabella 27-2](#) elenca gli identificatori dati definiti dal sistema per la regione del Medio Oriente e dell'Africa.

Tabella 27-2 Identità personale Africa

Identificatore dati	Descrizione
Numero di identificazione personale sudafricano	Vedere " Numero di identificazione personale sudafricano " a pagina 1235.

La [Tabella 27-3](#) elenca gli identificatori dati definiti dal sistema per la regione dell'Asia Pacifico.

Tabella 27-3 Identità personale Asia Pacifico

Identificatore dati	Descrizione
Australian Business Number (partita IVA australiana)	Vedere " Copertura ampia Australian Business Number " a pagina 923.
Codice azienda australiano (ACN)	Vedere " Codice azienda australiano (ACN) " a pagina 925.
Numero di passaporto australiano	Vedere " Numero di passaporto australiano " a pagina 930.
Tax File Number (codice fiscale) australiano	Vedere " Tax File Number (codice fiscale) australiano " a pagina 932.
Numero di passaporto cinese	Vedere " Numero di passaporto cinese " a pagina 977.
ID Hong Kong	Vedere " ID Hong Kong " a pagina 1076.
Numero tessera Aadhaar indiana	Vedere " Numero tessera Aadhaar indiana " a pagina 1098.
Codice di identificazione fiscale indiano (PAN)	Vedere " Codice di identificazione fiscale indiano (PAN) " a pagina 1100.
Numero di carta di identità indonesiana (KTP)	Vedere " Numero di carta di identità indonesiana (KTP) " a pagina 1102.
Numero di identificazione personale israeliano	Vedere " Numero di identificazione personale israeliano " a pagina 1124.
Numero di patente di guida giapponese	Vedere " Numero di patente di guida giapponese " a pagina 1133.
Numero di passaporto giapponese	Vedere " Numero di passaporto giapponese " a pagina 1135.

Identificatore dati	Descrizione
Numero di identificazione giapponese (Juki Net)	Vedere "Numero di identificazione giapponese (Juki Net)" a pagina 1137.\
Numero di identificazione personale giapponese - Aziendale	Vedere "Numero di identificazione personale giapponese - Aziendale" a pagina 1139.
Numero di identificazione personale giapponese - Personale	Vedere "Numero di identificazione personale giapponese - Personale" a pagina 1141.
Numero di passaporto coreano	Vedere "Numero di passaporto coreano" a pagina 1143.
Numero di registrazione anagrafica coreano per stranieri	Vedere "Numero di registrazione anagrafica coreano per stranieri." a pagina 1145.
Numero di registrazione anagrafica coreano per coreani	Vedere "Numero di registrazione anagrafica coreano per coreani" a pagina 1148.
Numero di carta di identità malese (MyKad)	Vedere "Numero di carta di identità malese (MyKad)" a pagina 1164.
Codice di assistenza sanitaria della Nuova Zelanda (NHI)	Vedere "Codice di assistenza sanitaria della Nuova Zelanda (NHI)" a pagina 1191.
Documento di identità cinese	Vedere "Documento di identità cinese" a pagina 1196.
NRIC Singapore	Vedere "Identificatore di dati NRIC Singapore" a pagina 1229.
ID Taiwan	Vedere "ID ROC Taiwan" a pagina 1271.
Numero di identificazione personale thailandese	Vedere "Numero di identificazione personale thailandese" a pagina 1273.
Numero di identificazione personale degli Emirati Arabi Uniti	Vedere "Numero di identificazione personale degli Emirati Arabi Uniti" a pagina 1300.

La [Tabella 27-4](#) elenca gli identificatori dati definiti dal sistema per la regione europea.

Tabella 27-4 Identità personale Europa

Identificatore dati	Descrizione
Numero di passaporto austriaco	Vedere "Numero di passaporto austriaco" a pagina 933.
Numero di identificazione fiscale austriaco	Vedere "Numero di identificazione fiscale austriaco" a pagina 935.
Numero di partita IVA austriaco	Vedere "Numero di partita IVA austriaco" a pagina 936.

Identificatore dati	Descrizione
Numero di previdenza sociale austriaco	Vedere " Numero di previdenza sociale austriaco " a pagina 939.
Numero di identificazione nazionale belga	Vedere " Numero di identificazione nazionale belga " a pagina 942.
Numero di patente di guida belga	Vedere " Numero di patente di guida belga " a pagina 945.
Numero di passaporto belga	Vedere " Numero di passaporto belga " a pagina 947.
Numero di identificazione fiscale belga	Vedere " Numero di identificazione fiscale belga " a pagina 948.
Numero di partita IVA belga	Vedere " Numero di partita IVA belga " a pagina 951.
Numero di cittadinanza univoco bulgaro (EGN)	Vedere " Numero di cittadinanza univoco bulgaro (EGN) " a pagina 967.
Burgerservicenummer	Vedere " Burgerservicenummer " a pagina 970.
Codice Fiscale	Vedere " Codice Fiscale " a pagina 979.
Numero di identificazione personale ceco	Vedere " Numero di identificazione personale ceco " a pagina 1004.
Numero di identificazione personale danese	Vedere " Numero di identificazione personale danese " a pagina 1007.
Numero di identificazione fiscale danese	Vedere " Numero di identificazione fiscale danese " a pagina 1009.
Numero di partita IVA danese	Vedere " Numero di partita IVA danese " a pagina 1012.
Numero di patente di guida finlandese	Vedere " Numero di patente di guida finlandese " a pagina 1029.
Numero di previdenza sociale europea della Finlandia	Vedere " Numero di previdenza sociale europea della Finlandia " a pagina 1032.
Numero di passaporto finlandese	Vedere " Numero di passaporto finlandese " a pagina 1034.
Numero di identificazione fiscale finlandese	Vedere " Numero di identificazione fiscale finlandese " a pagina 1035.
Numero di partita IVA finlandese	Vedere " Numero di partita IVA finlandese " a pagina 1038.
Codice identificativo personale finlandese	Vedere " Codice identificativo personale finlandese " a pagina 1040.

Identificatore dati	Descrizione
Numero di patente di guida francese	Vedere "Numero di patente di guida francese" a pagina 1042.
Numero di previdenza sociale francese	Vedere "Numero di previdenza sociale francese" a pagina 1044.
Numero di identificazione fiscale francese	Vedere "Numero di identificazione fiscale francese" a pagina 1045.
Numero di partita IVA francese	Vedere "Numero di partita IVA francese" a pagina 1047.
Codice INSEE francese	Vedere "Codice INSEE francese" a pagina 1049.
Numero di passaporto francese	Vedere "Numero di passaporto francese" a pagina 1051.
Numero di previdenza sociale francese	Vedere "Numero di previdenza sociale francese" a pagina 1052.
Numero di passaporto tedesco	Vedere "Numero di passaporto tedesco" a pagina 1054.
Numero di identificazione personale tedesco	Vedere "Numero di identificazione personale tedesco" a pagina 1056.
Numero di patente di guida tedesca	Vedere "Numero di patente di guida tedesca" a pagina 1059.
Numero di identificazione fiscale tedesco	Vedere "Numero di identificazione fiscale tedesco" a pagina 1060.
Numero di partita IVA tedesca	Vedere "Numero di partita IVA tedesca" a pagina 1063.
Codice fiscale della Grecia (AMKA)	Vedere "Codice fiscale della Grecia (AMKA)" a pagina 1065.
Codice fiscale greco (AFM)	Vedere "Codice fiscale greco (AFM)" a pagina 1067.
Numero di previdenza sociale ungherese (TAJ)	Vedere "Numero di previdenza sociale ungherese" a pagina 1078.
Numero di identificazione fiscale (TIN) ungherese	Vedere "Numero di identificazione fiscale ungherese" a pagina 1080.
Numero di partita IVA ungherese	Vedere "Numero di partita IVA ungherese" a pagina 1082.
Numero di passaporto irlandese	Vedere "Numero di passaporto irlandese" a pagina 1113.
Numero di identificazione fiscale irlandese	Vedere "Numero di identificazione fiscale irlandese" a pagina 1114.
Numero di partita IVA irlandese	Vedere "Numero di partita IVA irlandese" a pagina 1118.
Numero personale di servizio pubblico irlandese (PPS)	Vedere "Numero personale di servizio pubblico irlandese" a pagina 1121.

Identificatore dati	Descrizione
Numero di patente di guida italiana	Vedere "Numero di patente di guida italiana" a pagina 1126.
Numero di previdenza sociale italiano	Vedere "Numero di previdenza sociale italiano" a pagina 1127.
Numero di passaporto italiano	Vedere "Numero di passaporto italiano" a pagina 1129.
Numero di partita IVA italiano	Vedere "Numero di partita IVA italiano" a pagina 1131.
Numero di identificazione personale lettone	Vedere "Numero di identificazione personale lettone" a pagina 1151.
Numero di identificazione lussemburghese	Vedere "Numero di identificazione lussemburghese (RNPP)" a pagina 1153.
Numero di passaporto lussemburghese	Vedere "Numero di passaporto lussemburghese" a pagina 1155.
Numero di identificazione fiscale lussemburghese	Vedere "Numero di identificazione fiscale lussemburghese" a pagina 1157.
Numero di partita IVA lussemburghese	Vedere "Numero di partita IVA lussemburghese" a pagina 1161.
Numero di patente di guida dei Paesi Bassi	Vedere "Numero di patente di guida dei Paesi Bassi" a pagina 1183.
Numero di passaporto dei Paesi Bassi	Vedere "Numero di passaporto dei Paesi Bassi" a pagina 1184.
Numero di identificazione fiscale dei Paesi Bassi	Vedere "Numero di identificazione fiscale dei Paesi Bassi" a pagina 1185.
Numero di partita IVA dei Paesi Bassi	Vedere "Numero di partita IVA dei Paesi Bassi" a pagina 1189.
Numero di identificazione personale norvegese	Vedere "Numero di identificazione personale norvegese" a pagina 1193.
Numero di carta di identità polacca	Vedere "Numero di carta di identità polacca" a pagina 1197.
Codice statistico polacco (REGON)	Vedere "Codice statistico polacco (REGON)" a pagina 1199.
Codice fiscale polacco (PESEL)	Vedere "Codice fiscale polacco (PESEL)" a pagina 1201.
Numero di identificazione fiscale polacco (NIP)	Vedere "Numero di identificazione fiscale polacco (NIP)" a pagina 1203.

Identificatore dati	Descrizione
Numero di patente di guida portoghese	Vedere "Numero di patente di guida portoghese" a pagina 1206.
Numero di identificazione nazionale portoghese	Vedere "Numero di identificazione nazionale portoghese" a pagina 1208.
Numero di passaporto portoghese	Vedere "Numero di passaporto portoghese" a pagina 1211.
Numero di identificazione fiscale portoghese	Vedere "Numero di identificazione fiscale portoghese" a pagina 1212.
Numero di partita IVA portoghese	Vedere "Numero di partita IVA portoghese" a pagina 1215.
Numero di identificazione nazionale rumeno	Vedere "Numero di identificazione nazionale rumeno" a pagina 1221.
Numero di identificazione personale rumeno (CNP)	Vedere "Numero di identificazione personale rumeno (CNP)" a pagina 1223.
Numero di passaporto russo interno	Vedere "Numero di passaporto russo interno" a pagina 1225.
Numero di identificazione fiscale russo (INN)	Vedere "Numero di identificazione fiscale russo (INN)" a pagina 1227.
Numero di identificazione nazionale slovacco	Vedere "Numero di identificazione nazionale slovacco" a pagina 1230.
Numero identificativo cittadini della Slovenia	Vedere "Numero identificativo cittadini della Slovenia" a pagina 1233.
Numero di patente di guida spagnola	Vedere "Numero di patente di guida spagnola" a pagina 1238.
Numero di partita IVA spagnolo	Vedere "Numero di partita IVA spagnolo" a pagina 1240.
Numero di conto cliente spagnolo	Vedere "Numero di conto cliente spagnolo" a pagina 1243.
Numero di DNI spagnolo	Vedere "Numero di DNI spagnolo" a pagina 1245.
Numero di passaporto spagnolo	Vedere "Numero di passaporto spagnolo" a pagina 1247.
Numero di previdenza sociale spagnolo	Vedere "Numero di previdenza sociale spagnolo " a pagina 1249.
Codice fiscale spagnolo (CIF)	Vedere "Codice fiscale spagnolo (CIF)" a pagina 1251.
Numero di patente di guida svedese	Vedere "Numero di patente di guida svedese" a pagina 1254.

Identificatore dati	Descrizione
Numero di identificazione fiscale svedese	Vedere "Numero di identificazione fiscale svedese" a pagina 1256.
Numero di partita IVA svedese	Vedere "Numero di partita IVA svedese" a pagina 1258.
Numero di passaporto svedese	Vedere "Numero di passaporto svedese" a pagina 1260.
Numero di identificazione personale svedese	Vedere "Numero di identificazione personale svedese" a pagina 1262.
Numero AHV svizzero	Vedere "Numero AHV svizzero" a pagina 1267.
Numero di previdenza sociale svizzero (AHV)	Vedere "Numero di previdenza sociale svizzero (AHV)" a pagina 1269.
Numero di identificazione turco	Vedere "Numero di identificazione turco" a pagina 1275.
Coordinate bancarie di un numero di conto britannico	Vedere "Coordinate bancarie di un numero di conto britannico" a pagina 1277.
Numero patente di guida britannica	Vedere "Numero di patente di guida britannica" a pagina 1279.
Numero di tessera elettorale britannico	Vedere "Numero di tessera elettorale britannico" a pagina 1282.
Numero di passaporto britannico	Vedere "Numero di passaporto britannico" a pagina 1287.
Numero NHS (National Health Service) britannico	Vedere "Numero NHS (National Health Service) del Regno Unito" a pagina 1282.
Numero di previdenza sociale britannico	Vedere "Numero di previdenza sociale britannico" a pagina 1285.
Codice fiscale britannico	Vedere "Codice fiscale britannico" a pagina 1289.
Numero di partita IVA britannico (VAT)	Vedere "Numero di partita IVA britannico (VAT)" a pagina 1291.
Carta di identità ucraina	Vedere "Carta di identità ucraina" a pagina 1296.
Passaporto ucraino (interno)	Vedere "Passaporto ucraino (interno)" a pagina 1294.
Passaporto ucraino (internazionale)	Vedere "Passaporto ucraino (internazionale)" a pagina 1298.

La [Tabella 27-5](#) elenca gli identificatori dati definiti dal sistema per la regione nordamericana.

Tabella 27-5 Identità personale America del Nord

Identificatore dati	Descrizione
Social Insurance Number (numero di previdenza sociale) canadese	Vedere " Social Insurance Number (numero di previdenza sociale) canadese " a pagina 971.
Numero patente di guida - Stato della California	Vedere " Numero patente di guida - Stato della California " a pagina 1015.
Numero patente di guida - Stato dell'Illinois	Vedere " Numero patente di guida - Stato dell'Illinois " a pagina 1018.
Numero patente di guida - Stato del New Jersey	Vedere " Numero patente di guida - Stato del New Jersey " a pagina 1020.
Numero patente di guida - Stato di New York	Vedere " Numero patente di guida - Stato di New York " a pagina 1021.
Numero di patente di guida - Stati della Florida, del Michigan e del Minnesota	Vedere " Numero di patente di guida - Stati della Florida, del Michigan e del Minnesota " a pagina 1016.
Numero di patente di guida - Stato di Washington	Vedere " Numero di patente di guida - Stato di Washington " a pagina 1023.
Numero di patente di guida - Stato del Wisconsin	Vedere " Numero di patente di guida - Stato del Wisconsin " a pagina 1025.
Numero di registrazione e identificazione personale messicano	Vedere " Numero di registrazione e identificazione personale messicano " a pagina 1169.
Numero di identificazione fiscale messicano	Vedere " Numero di identificazione fiscale messicano " a pagina 1171.
Codice di identificazione personale messicano (CURP)	Vedere " Codice di identificazione personale messicano (CURP) " a pagina 1174.
Numero di conto bancario esteso messicano (CLABE)	Vedere " Numero di conto bancario esteso messicano (CLABE) " a pagina 1176.
Social Security Number (SSN) statunitense randomizzato	Vedere " Social Security Number (SSN) statunitense randomizzato " a pagina 1218.
US Individual Tax Identification Number (ITIN - codice di ID fiscale statunitense)	Vedere " Codice fiscale britannico " a pagina 1289.
Numero di passaporto statunitense	Vedere " Numero di passaporto statunitense " a pagina 1305.

Identificatore dati	Descrizione
Social Security Number (SSN) statunitense randomizzato	Vedere "Social Security Number (SSN) statunitense" a pagina 1307. Nota: Questo identificatore dati è sostituito dall'identificatore dati Social Security Number (SSN) statunitense randomizzato
Codici di avviamento postale Zip+4 statunitensi	Vedere "Codici di avviamento postale Zip+4 statunitensi" a pagina 1310.

La [Tabella 27-6](#) elenca gli identificatori definiti dal sistema per la regione sudamericana.

Tabella 27-6 Identità personale America del Sud

Identificatore dati	Descrizione
Numero di identificazione fiscale argentino	Vedere "Numero di identificazione fiscale argentino" a pagina 920.
Numero di conto bancario brasiliano	Vedere "Numero di conto bancario brasiliano" a pagina 953.
Numero di tessera elettorale brasiliana	Vedere "Numero di tessera elettorale brasiliana" a pagina 955.
Numero del Registro Nazionale delle Persone Giuridiche brasiliano	Vedere "Numero del Registro Nazionale delle Persone Giuridiche brasiliano" a pagina 959.
Codice fiscale per persone fisiche brasiliano (CPF)	Vedere "Codice fiscale per persone fisiche brasiliano (CPF)" a pagina 962.
Numero di identificazione nazionale cileno	Vedere "Numero di identificazione nazionale cileno" a pagina 975.
Indirizzi colombiani	Vedere "Indirizzi colombiani" a pagina 980.
Numero di cellulare colombiano	Vedere "Numero di cellulare colombiano" a pagina 983.
Numero di identificazione personale colombiano	Vedere "Numero di identificazione personale colombiano" a pagina 986.
Tax Identification Number (codice fiscale) colombiano	Vedere "Tax Identification Number (codice fiscale) colombiano" a pagina 988.
Numero di identificazione nazionale venezuelano	Vedere "Numero di identificazione nazionale venezuelano" a pagina 1312.

Identificatori di dati finanziari

Tabella 27-7 elenca gli identificatori dati definiti dal sistema per il rilevamento di numeri di identificazione finanziari, come numeri di carta di credito e numeri di routing ABA.

Tabella 27-7 Identificatori di dati finanziari

Identificatore dati	Descrizione
Numero di routing ABA	Vedere "Numero di routing ABA" a pagina 918.
Numero carta di credito	Vedere "Numero carta di credito" a pagina 993.
Dati banda magnetica carta di credito	Vedere "Dati banda magnetica per carte di credito" a pagina 990.
Numero CUSIP	Vedere "Numero CUSIP" a pagina 1002.
IBAN paesi centrali	Vedere "IBAN paesi centrali" a pagina 1084.
IBAN paesi orientali	Vedere "IBAN paesi orientali" a pagina 1088.
IBAN paesi occidentali	Vedere "IBAN paesi occidentali" a pagina 1094.
Codice ISIN (International Securities Identification Number)	Vedere "Codice ISIN (International Securities Identification Number)" a pagina 1106.
Codice SWIFT	Vedere "Codice SWIFT" a pagina 1265.

Identificatori dati sanitari

La **Tabella 27-8** elenca gli identificatori dati definiti dal sistema per il rilevamento dei codici di medicinali degli Stati Uniti e internazionali e di informazioni su fornitori e consumatori in ambito sanitario.

Tabella 27-8 Sanità

Identificatore dati	Descrizione
Numero Medicare australiano	Vedere "Numero Medicare australiano" a pagina 927.
Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica	Vedere "Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica" a pagina 964.
Numero DEA (Drug Enforcement Agency)	Vedere "Numero DEA (Drug Enforcement Agency)" a pagina 1027.
Healthcare Common Procedure Coding System (codice CPT HCPCS).	Vedere "Healthcare Common Procedure Coding System (codice CPT HCPCS)." a pagina 1069.

Identificatore dati	Descrizione
Numero di assicurazione sanitaria	Vedere " Numero di assicurazione sanitaria " a pagina 1072.
Identificatore beneficiario di assistenza sanitaria	Vedere " Identificatore beneficiario di assistenza sanitaria " a pagina 1167.
National Drug Code (NDC, codici identificativi dei medicinali)	Vedere " National Drug Code (NDC, codici identificativi dei farmaci) " a pagina 1178.
Numero NPI	Vedere " Numero NPI " a pagina 1181.

Identificatori dati informatica

Vedere [Tabella 27-9](#) a pagina 693. elenca gli identificatori dati definiti dal sistema per rilevare i criteri informatici, ad esempio gli indirizzi IPv4 e IPv6 e i numeri di identificazione dei dispositivi mobili.

Tabella 27-9 Informatica

Identificatore dati	Descrizione
Numero IMEI	Vedere " Numero IMEI " a pagina 1104.
Indirizzo IP	Vedere " Indirizzo IP " a pagina 1108.
Indirizzo IPv6	Vedere " Indirizzo IPv6 " a pagina 1110.

Parole chiave internazionali per gli identificatori dati PII

Symantec Data Loss Prevention consente di modificare gli identificatori dati del sistema e di personalizzare le parole chiave di input per individuare una vasta gamma di contenuti internazionali.

Vedere "[Estensione e personalizzazione di identificatori di dati](#)" a pagina 693.

Vedere "[Utilizzo di parole chiave personalizzate per gli identificatori di dati del sistema](#)" a pagina 804.

Estensione e personalizzazione di identificatori di dati

È possibile personalizzare gli identificatori di dati a seconda delle proprie esigenze. È possibile estendere gli identificatori di dati definiti dal sistema modificandoli, nonché creare nuovi identificatori di dati per corrispondenze di dati personalizzate.

Il caso di utilizzo più comune per la modifica di un identificatore di dati definito dal sistema è modificare l'input di dati per una convalida che accetta l'input di dati. Ad esempio, se l'identificatore di dati implementa la convalida "Trova parole chiave", è possibile aggiungere

o rimuovere valori dall'elenco di parole chiave. Un altro caso di utilizzo può comportare l'aggiunta o la rimozione di convalide dall'identificatore di dati, oppure la modifica di uno o più criteri definiti dall'identificatore di dati.

Vedere ["Clonazione di un identificatore dati di sistema prima della sua modifica "](#) a pagina 726.

Per creare un identificatore di dati personalizzato, implementare uno o più criteri di rilevamento, selezionare una o più convalide, fornire l'input di dati se la convalida lo richiede e scegliere un normalizzatore di dati.

Vedere ["Configurazione degli identificatori dati personalizzati"](#) a pagina 751.

Gli autori di politiche possono riutilizzare gli identificatori di dati modificati e personalizzati in una o più politiche.

Informazioni sulla configurazione dell'identificatore dati

È possibile configurare tre tipi di identificatori dati:

- Istanza - definito a livello di politica
Vedere ["Configurazione delle condizioni della politica dell'identificatore dati"](#) a pagina 697.
- Modificato - configurato a livello di sistema
Vedere ["Modifica degli identificatori dati di sistema"](#) a pagina 725.
- Personalizzato - creato a livello di sistema
Vedere ["Creazione di identificatori dati personalizzati"](#) a pagina 748.

Il tipo di identificatore dati implementato dipende dai requisiti aziendali. Per la maggior parte dei casi di utilizzo la configurazione di un'istanza della politica che usa un identificatore dati non modificato e definito dal sistema è sufficiente per individuare accuratamente la perdita di dati. Se necessario, è possibile estendere un identificatore dati definito dal sistema modificandolo oppure è possibile implementare uno o più identificatori dati personalizzati per individuare dati univoci.

La configurazione dell'identificatore dati eseguita a livello di istanza della politica è specifica per la politica. Le modifiche apportate agli identificatori dati a livello di sistema si applicano a tutti gli identificatori dati derivati dall'identificatore dati modificato.

Informazioni sulle coperture degli identificatori di dati

Gli identificatori di dati di sistema sono implementati per copertura. La copertura definisce l'ambito di rilevamento per quell'identificatore di dati. Ogni identificatore di dati implementa almeno una copertura di rilevamento. L'opzione più ampia disponibile per l'identificatore di dati è probabile che generi la maggior parte di falsi positivi; l'opzione più limitata produce il minimo di falsi positivi. Generalmente le convalide e spesso i criteri differiscono da una copertura all'altra.

Vedere ["Utilizzo delle coperture identificatore dati"](#) a pagina 702.

Ad esempio, l'identificatore di dati Numero patente di guida - Stato della California fornisce le coperture ampia e media, con la copertura media che utilizza una convalida con parola chiave.

Nota: Non tutti gli identificatori di dati di sistema forniscono ogni copertura di rilevamento. Consultare l'elenco completo di identificatori di dati e coperture per determinare quali sono disponibili.

Vedere ["Selezione di una copertura dell'identificatore di dati"](#) a pagina 703.

Informazioni sulle convalide facoltative per identificatori di dati

Le convalide facoltative consentono di affinare l'ambito del rilevamento per un identificatore di dati. Quando si configura un'istanza dell'identificatore di dati, è possibile selezionare tra cinque convalide facoltative.

Vedere ["Utilizzo delle convalide opzionali"](#) a pagina 719.

Il tipo di caratteri accettati per ogni convalida facoltativa dipende dall'identificatore di dati.

Vedere ["Caratteri accettabili per le convalide opzionali"](#) a pagina 721.

Nota: Le convalide facoltative si applicano solo all'istanza della politica che si sta configurando e non a tutto il sistema.

Informazioni sui criteri dell'identificatore dati

Gli identificatori dati implementano criteri per definire la corrispondenza tra i dati. La sintassi del criterio dell'identificatore dati è simile al linguaggio delle espressioni regolari, ma con maggiori limitazioni. Ad esempio, la sintassi del criterio dell'identificatore dati non supporta alcune caratteristiche delle espressioni regolari, quali il raggruppamento, le espressioni lookbehind e lookahead e molti caratteri speciali (in particolare il punto "."). Inoltre, il sistema consente solo l'uso dei caratteri ASCII per i criteri dell'identificatore dati.

Vedere ["Utilizzo della lingua dei criteri degli identificatori dati"](#) a pagina 751.

Quando si modifica un identificatore dati di sistema, il sistema rende disponibile il criterio per la visualizzazione e la modifica. I criteri dell'identificatore dati sono stati adattati e ottimizzati per una corrispondenza del contenuto precisa.

Vedere ["Selezione di una copertura dell'identificatore di dati"](#) a pagina 703.

Inoltre è possibile creare un identificatore dati personalizzato. In tal caso è necessario implementare almeno un criterio. Il miglior metodo per apprendere a creare i criteri consiste nell'esaminare i criteri dell'identificatore dati definiti dal sistema.

Vedere ["Creazione di criteri di identificatore di dati per la corrispondenza con i dati"](#) a pagina 755.

Il linguaggio dei criteri dell'identificatore dati è un sottoinsieme del linguaggio delle espressioni regolari.

Vedere ["Specifica lingua criterio identificatore dati"](#) a pagina 752.

Informazioni sulle convalide criterio

Le convalide criterio sono controlli di convalida applicati ai dati che corrispondono a un criterio identificatore dati. Le convalide contribuiscono ad affinare l'ambito del rilevamento e a ridurre i falsi positivi. Molte convalide consentono l'immissione di dati. Ad esempio la convalida Parola chiave consente di immettere un elenco di parole chiave.

Vedere ["Utilizzo delle convalide criterio"](#) a pagina 755.

Quando si modifica un identificatore dati, è possibile modificare i valori di input per qualsiasi convalida che accetta dati.

Vedere ["Modifica dell'input di convalida dei criteri"](#) a pagina 727.

Quando si modifica un identificatore dati, è possibile aggiungere e rimuovere le convalide criterio. Quando si creano identificatori dati personalizzati, è possibile configurare una o più convalide. Il sistema consente inoltre di creare una convalida script personalizzata per definire controlli di convalida propri.

Vedere ["Selezione di convalide dei criteri"](#) a pagina 763.

Informazioni sui normalizzatori di dati

Un normalizzatore di dati riconcilia i dati rilevati dal criterio dell'identificatore dati con il formato previsto dal normalizzatore. Non è possibile modificare il normalizzatore di un identificatore dati definito dal sistema. Quando si crea un identificatore dati personalizzato, si seleziona un normalizzatore di dati.

Vedere ["Caratteri accettabili per le convalide opzionali"](#) a pagina 721.

Vedere ["Selezione di un normalizzatore di dati"](#) a pagina 764.

Informazioni sulla corrispondenza con diversi componenti

Gli identificatori di dati supportano la corrispondenza con i componenti. Ciò significa che è possibile configurare gli identificatori di dati per la corrispondenza con uno o più componenti di messaggi. Tuttavia, se l'identificatore di dati implementa una convalida (facoltativa o obbligatoria), come Trova parole chiave, i dati convalidati e i dati corrispondenti devono esistere nello stesso componente per generare o escludere un incidente.

Vedere ["Messaggi di rilevamento e componenti di messaggio"](#) a pagina 398.

Ad esempio, si consideri uno scenario in cui si implementa l'identificatore di dati Social Security Number (SSN) statunitense randomizzato. Questo identificatore di dati esegue il rilevamento

in base a vari criteri di 9 cifre e usa una convalida con parole chiave per restringere l'ambito del rilevamento (la parola chiave e le frasi nell'elenco sono "social security number, ssn"). Se il motore di rilevamento riceve un messaggio con il criterio numerico 123-45-6789 e la parola chiave "social security number" ed entrambi gli elementi di dati sono contenuti nel componente allegato del messaggio, il motore di rilevamento segnala una corrispondenza. Tuttavia, se l'allegato contiene il numero ma il corpo contiene la convalida con parola chiave, il motore di rilevamento non segnala una corrispondenza.

Vedere ["Configurazione della condizione Contenuto corrispondente a identificatore dati"](#) a pagina 700.

Informazioni sul conteggio delle corrispondenze univoche

Gli identificatori dati, le parole chiave e le espressioni regolari supportano il conteggio delle corrispondenze univoche. Questa funzionalità consente di contare solo quelle corrispondenze di criteri che sono univoche.

Il conteggio delle corrispondenze univoche è utile quando è necessario rilevare solo i criteri unici e non tutti i criteri corrispondenti. Ad esempio è possibile utilizzare il conteggio delle corrispondenze univoche per attivare un incidente se un documento contiene 10 o più codici fiscali unici. In questo caso, se un documento contiene 10 istanze dello stesso codice fiscale, la politica non attiva un incidente.

Vedere ["Utilizzo del totale corrispondenze univoche"](#) a pagina 723.

Vedere ["Configurazione del conteggio delle corrispondenze univoche"](#) a pagina 724.

Configurazione delle condizioni della politica dell'identificatore dati

La [Tabella 27-10](#) elenca e descrive le opzioni di configurazione per le condizioni dell'identificatore dati.

Vedere ["Introduzione agli identificatori di dati"](#) a pagina 681.

Vedere ["Configurazione della condizione Contenuto corrispondente a identificatore dati"](#) a pagina 700.

Tabella 27-10 Configurazione dell'identificatore dati dell'istanza della politica

Selezionabile a livello di politica	Non configurabile
<ul style="list-style-type: none"> ■ Copertura È possibile implementare tutta la copertura supportata dall'identificatore dati a livello dell'istanza. ■ Convalide opzionali È possibile selezionare una o più convalide opzionali a livello di istanza. 	<ul style="list-style-type: none"> ■ Modelli Non è possibile modificare i modelli di corrispondenza a livello di istanza. ■ Convalide obbligatorie Non è possibile modificare, aggiungere o rimuovere le convalide richieste a livello di istanza.

Flusso di lavoro per la configurazione delle politiche dell'identificatore dati

La [Tabella 27-11](#) descrive il flusso di lavoro per l'implementazione degli identificatori dati definiti dal sistema.

Tabella 27-11 Flusso di lavoro per l'implementazione degli identificatori dati

Passaggio	Azione	Descrizione
1	Scegliere il tipo di identificatore dati che si desidera implementare.	Vedere "Introduzione agli identificatori di dati" a pagina 681.
2	Scegliere la copertura dell'identificatore dati.	Vedere "Informazioni sulle coperture degli identificatori di dati" a pagina 694.
3	Configurare l'identificatore dati.	Vedere "Configurazione della condizione Contenuto corrispondente a identificatore dati" a pagina 700.
4	Collaudare e adattare la politica dell'identificatore dati.	Vedere "Best practice per l'utilizzo degli identificatori dati" a pagina 765.

Gestione e aggiunta degli identificatori dati

Nella schermata **Gestisci > Politiche > Identificatore dati** sono elencati tutti gli identificatori dati, compresi quelli definiti dal sistema e personalizzati. In questa schermata è possibile gestire e modificare gli identificatori dati esistenti e aggiungerne di nuovi.

Vedere ["Introduzione agli identificatori di dati"](#) a pagina 681.

Tabella 27-12 Gestione degli identificatori dati

Azione	Descrizione
Modificare un identificatore dati.	<p>Selezionare l'identificatore dati dall'elenco per modificarlo.</p> <p>Vedere "Selezione di una copertura dell'identificatore di dati" a pagina 703.</p> <p>Vedere "Estensione e personalizzazione di identificatori di dati" a pagina 693.</p> <p>Vedere "Modifica degli identificatori dati" a pagina 699.</p>
Definire un identificatore dati personalizzato.	<p>Fare clic su Aggiungi identificatore dati per creare un identificatore dati personalizzato.</p> <p>Vedere "Configurazione degli identificatori dati personalizzati" a pagina 751.</p> <p>Vedere "Flusso di lavoro per la creazione di identificatori di dati personalizzati" a pagina 749.</p>
Ordinare e visualizzare gli identificatori dati.	<p>L'elenco viene disposto in ordine alfabetico per Nome.</p> <p>È inoltre possibile ordinare per Categoria.</p> <p>Un'icona a forma di matita a sinistra indica che l'identificatore dati è stato modificato rispetto allo stato originale o è personalizzato.</p>
Rimuovere un identificatore dati.	<p>Fare clic sull'icona X a destra per eliminare un identificatore dati.</p> <p>Il sistema non consente di eliminare gli identificatori dati del sistema. È possibile eliminare solo gli identificatori dati personalizzati.</p>

Modifica degli identificatori dati

È possibile modificare gli identificatori dati definiti dal sistema, inclusi i criteri, le convalide e gli input delle convalide. Le modifiche vengono propagate a tutte le politiche che dichiarano l'identificatore dati. Non è possibile rinominare un identificatore dati di sistema. Considerare la possibilità di creare manualmente una copia clonata prima di modificare un identificatore dati di sistema.

Vedere ["Estensione e personalizzazione di identificatori di dati"](#) a pagina 693.

Nota: Il sistema non esporta gli identificatori dati in un modello di politica. Il sistema esporta un riferimento all'identificatore dati di sistema. Il sistema di destinazione in cui viene importato il modello di politica fornisce l'identificatore dati effettivo. Se si modifica un identificatore dati definito dal sistema, le modifiche non vengono esportate nel modello.

Tabella 27-13 Flusso di lavoro per la modifica degli identificatori dati

Passaggio	Azione	Descrizione
1	Clonare l'identificatore dei dati di sistema che si desidera modificare.	Clonare l'identificatore dati di sistema prima di modificarlo. Vedere "Clonazione di un identificatore dati di sistema prima della sua modifica" a pagina 726. Vedere "Clonare gli identificatori di dati definiti dal sistema prima della modifica per mantenere lo stato originale" a pagina 767.
2	Modificare l'identificatore dati clonato.	Se si modifica un identificatore dati di sistema, fare clic sul segno più per visualizzare la copertura e modificare l'identificatore dati. Vedere "Selezione di una copertura dell'identificatore di dati" a pagina 703.
3	Modificare uno o più Modelli .	È possibile modificare qualsiasi modello fornito dall'identificatore dati. Vedere "Creazione di criteri di identificatore di dati per la corrispondenza con i dati" a pagina 755.
4	Modificare l'immissione dei dati per qualsiasi convalida che accetta l'input.	Vedere "Modifica dell'input di convalida dei criteri" a pagina 727. Vedere "Elenco delle convalide criterio che accettano dati di input" a pagina 727.
5	Facoltativamente, è possibile aggiungere o rimuovere convalide in base alle esigenze.	Vedere "Selezione di convalide dei criteri" a pagina 763.
6	Salvare l'identificatore dati.	Fare clic su Salva per salvare le modifiche. Una volta salvato l'identificatore dati, l'icona nella schermata Identificatore dati indica che è modificata rispetto al suo stato originale o è personalizzata. Vedere "Gestione e aggiunta degli identificatori dati" a pagina 698. Nota: Fare clic su Annulla per non salvare l'identificatore dati.
7	Implementare l'identificatore dati in una regola o in un'eccezione della politica.	Vedere "Configurazione della condizione Contenuto corrispondente a identificatore dati" a pagina 700.

Configurazione della condizione Contenuto corrispondente a identificatore dati

È possibile configurare la condizione Contenuto corrispondente a identificatore dati nelle eccezioni e nelle regole di rilevamento delle politiche.

Vedere ["Introduzione agli identificatori di dati"](#) a pagina 681.

Tabella 27-14 Configurazione della condizione Contenuto corrispondente a identificatore dati

Passaggio	Azione	Descrizione
1	Aggiungere una regola o un'eccezione dell'identificatore di dati a una politica, o configurarne una esistente.	<p>Selezionare la condizione Contenuto corrispondente a identificatore dati nella schermata Aggiungi regola di rilevamento o Aggiungi eccezione.</p> <p>Vedere "Aggiunta di una regola a una politica" a pagina 424.</p> <p>Vedere "Aggiunta di un'eccezione a una politica" a pagina 434.</p>
2	Scegliere un identificatore di dati.	<p>Scegliere un identificatore di dati dall'elenco e fare clic su Avanti.</p> <p>Vedere "Identificatori di dati definiti dal sistema" a pagina 682.</p>
3	Selezionare una copertura di rilevamento.	<p>Utilizzare l'opzione Copertura per restringere l'ambito del rilevamento.</p> <p>Vedere "Informazioni sulle coperture degli identificatori di dati" a pagina 694.</p> <p>Ampia è l'impostazione predefinita e rileva il set di corrispondenze più ampio. Le coperture media e limitata, se disponibili, controllano criteri supplementari e rilevano meno corrispondenze.</p> <p>Vedere "Selezione di una copertura dell'identificatore di dati" a pagina 703.</p>
4	Selezionare e configurare una o più convalide opzionali .	<p>Le convalide opzionali limitano i criteri di corrispondenza e riducono i falsi positivi.</p> <p>Vedere "Informazioni sulle convalide facoltative per identificatori di dati" a pagina 695.</p>
5	Configurare Conteggio corrispondenze .	<p>Selezionare il metodo di conteggio delle corrispondenze:</p> <ul style="list-style-type: none"> ■ Verificare esistenza Non conteggia le corrispondenze multiple; restituisce un numero di corrispondenze pari a 1 per una o più corrispondenze. ■ Conta tutte le corrispondenze Conteggia ogni corrispondenza; specificare il numero minimo di corrispondenze per segnalare un incidente. Vedere "Configurazione del conteggio delle corrispondenze" a pagina 431. ■ Conta tutte le corrispondenze univoche È l'impostazione predefinita per la versione 11.6 e versioni successive. Vedere "Informazioni sul conteggio delle corrispondenze univoche" a pagina 697. Vedere "Configurazione del conteggio delle corrispondenze univoche" a pagina 724.

Passaggio	Azione	Descrizione
6	Configurare i componenti del messaggio su Cerca corrispondenza con .	<p>Selezionare uno o più componenti del messaggio in cui cercare la corrispondenza.</p> <p>Sull'endpoint, il motore di rilevamento cerca la corrispondenza nell'intero messaggio, non nei singoli componenti.</p> <p>Vedere "Selezione dei componenti per la corrispondenza" a pagina 433.</p> <p>Se l'identificatore di dati usa convalide di parole chiave obbligatorie o opzionali, la parola chiave deve essere presente nello stesso componente del contenuto dell'identificatore di dati corrispondente.</p> <p>Vedere "Informazioni sulla corrispondenza con diversi componenti" a pagina 696.</p>
7	Configurare le condizioni supplementari su Confronta anche .	<p>Facoltativamente, è possibile aggiungere una o più condizioni supplementari tra quelle disponibili nell'elenco di condizioni Confronta anche.</p> <p>Tutte le condizioni in una regola o eccezione composta devono essere vere per generare o escludere un incidente.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Utilizzo delle coperture identificatore dati

Ogni identificatore dati di sistema fornisce una o più coperture di rilevamento. Quando si configura un'istanza di identificatore dati di sistema o quando si modifica un identificatore dati di sistema, è possibile selezionare la copertura da implementare. Non tutte le opzioni di copertura sono disponibili per tutti gli identificatori dati.

Vedere ["Informazioni sulle coperture degli identificatori di dati"](#) a pagina 694.

Tabella 27-15 Coperture regola disponibili per gli identificatori dati di sistema

Copertura	Descrizione
Ampia	La copertura ampia definisce uno o più criteri per restituire il numero massimo di corrispondenze. In generale questa copertura produce una quantità più elevata di falsi positivi rispetto alle coperture media e limitata.
Media	La copertura media può ridurre i criteri di rilevamento e/o aggiungere una o più convalide di dati per limitare il numero delle corrispondenze.
Limitata	La copertura limitata offre i criteri più restrittivi e la convalida più rigorosa per fornire le corrispondenze più accurate. In generale questa opzione richiede la presenza di una parola chiave o di un'altra restrizione di convalida per attivare una corrispondenza.

Selezione di una copertura dell'identificatore di dati

Non è possibile modificare il normalizzatore che un identificatore di dati del sistema implementa. Queste informazioni sono utili quando si implementano uno o più convalide facoltative.

Vedere ["Caratteri accettabili per le convalide opzionali"](#) a pagina 721.

Tabella 27-16 Coperture e normalizzatori dell'identificatore di dati del sistema

Identificatore dati	Coperture	Normalizzatore
Numero di routing ABA Vedere "Numero di routing ABA" a pagina 918.	Ampia Media Limitata	Cifre
Numero di identificazione fiscale argentino Vedere "Numero di identificazione fiscale argentino" a pagina 920.	Ampia Media Limitata	Cifre
Australian Business Number (partita IVA australiana) Vedere "Copertura ampia Australian Business Number" a pagina 923.	Ampia Media Limitata	Cifre
Codice azienda australiano (ACN) Vedere "Codice azienda australiano (ACN)" a pagina 925.	Ampia Media Limitata	Cifre
Numero Medicare australiano Vedere "Numero Medicare australiano" a pagina 927.	Ampia Media Limitata	Cifre
Numero di passaporto australiano Vedere "Numero di passaporto australiano" a pagina 930.	Ampia Limitata	Minuscolo
Tax File Number (codice fiscale) australiano Vedere "Tax File Number (codice fiscale) australiano" a pagina 932.	Ampia Media Limitata	Cifre
Numero di passaporto austriaco Vedere "Numero di passaporto austriaco" a pagina 933.	Ampia Limitata	Cifre e lettere

Identificatore dati	Coperture	Normalizzatore
Numero di identificazione fiscale austriaco Vedere "Numero di identificazione fiscale austriaco" a pagina 935.	Ampia Limitata	Cifre
Numero di partita IVA austriaco Vedere "Numero di partita IVA austriaco" a pagina 936.	Ampia Media Limitata	Cifre e lettere
Numero di previdenza sociale austriaco Vedere "Numero di previdenza sociale austriaco" a pagina 939.	Ampia Media Limitata	Cifre
Numero di identificazione nazionale belga Vedere "Numero di identificazione nazionale belga" a pagina 942.	Ampia Media Limitata	Cifre
Numero di patente di guida belga Vedere "Numero di patente di guida belga" a pagina 945.	Ampia Limitata	Cifre
Numero di passaporto belga Vedere "Numero di passaporto belga" a pagina 947.	Ampia Limitata	Cifre e lettere
Numero di identificazione fiscale belga Vedere "Numero di identificazione fiscale belga" a pagina 948.	Ampia Limitata	Cifre
Numero di partita IVA belga Vedere "Numero di partita IVA belga" a pagina 951.	Ampia Media Limitata	Cifre e lettere
Numero di conto bancario brasiliano Vedere "Numero di conto bancario brasiliano" a pagina 953.	Ampia Media Limitata	Cifre
Numero di tessera elettorale brasiliana Vedere "Numero di tessera elettorale brasiliana" a pagina 955.	Ampia Media Limitata	Cifre

Identificatore dati	Coperture	Normalizzatore
<p>Numero del Registro Nazionale delle Persone Giuridiche brasiliano</p> <p>Vedere "Numero del Registro Nazionale delle Persone Giuridiche brasiliano" a pagina 959.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Cifre
<p>Codice fiscale per persone fisiche brasiliano (CPF)</p> <p>Vedere "Codice fiscale per persone fisiche brasiliano (CPF)" a pagina 962.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Cifre
<p>Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica</p> <p>Vedere "Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica" a pagina 964.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Cifre
<p>Numero di cittadinanza univoco bulgaro (EGN)</p> <p>Vedere "Numero di cittadinanza univoco bulgaro (EGN)" a pagina 967.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Cifre
<p>Burgerservicenummer</p> <p>Vedere "Burgerservicenummer" a pagina 970.</p>	<p>Ampia</p> <p>Limitata</p>	Cifre
<p>Social Insurance Number (numero di previdenza sociale) canadese</p> <p>Vedere "Social Insurance Number (numero di previdenza sociale) canadese" a pagina 971.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Cifre
<p>Numero di identificazione nazionale cileno</p> <p>Vedere "Numero di identificazione nazionale cileno" a pagina 975.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Cifre e lettere
<p>Numero di passaporto cinese</p> <p>Vedere "Numero di passaporto cinese" a pagina 977.</p>	<p>Ampia</p> <p>Limitata</p>	Cifre e lettere
<p>Codice Fiscale</p> <p>Vedere "Codice Fiscale" a pagina 979.</p>	<p>Ampia</p> <p>Limitata</p>	Cifre e lettere
<p>Indirizzi colombiani</p> <p>Vedere "Indirizzi colombiani" a pagina 980.</p>	<p>Ampia</p> <p>Limitata</p>	Minuscolo
<p>Numero di cellulare colombiano</p> <p>Vedere "Numero di cellulare colombiano" a pagina 983.</p>	<p>Ampia</p> <p>Limitata</p>	Cifre

Identificatore dati	Coperture	Normalizzatore
Numero di identificazione personale colombiano Vedere "Numero di identificazione personale colombiano" a pagina 986.	Ampia Limitata	Cifre
Tax Identification Number (codice fiscale) colombiano Vedere "Tax Identification Number (codice fiscale) colombiano" a pagina 988.	Ampia Limitata	Cifre
Dati banda magnetica per carte di credito Vedere "Dati banda magnetica per carte di credito" a pagina 990.	Media	Cifre
Numero carta di credito Vedere "Numero carta di credito" a pagina 993.	Ampia Media Limitata	Cifre
Numero CUSIP Vedere "Numero CUSIP" a pagina 1002.	Ampia Media Limitata	Minuscolo
Numero di identificazione personale ceco Vedere "Numero di identificazione personale ceco" a pagina 1004.	Ampia Media Limitata	Cifre
Numero di identificazione personale danese Vedere "Numero di identificazione personale danese" a pagina 1007.	Ampia Media Limitata	Cifre e lettere
Numero di identificazione fiscale danese Vedere "Numero di identificazione fiscale danese" a pagina 1009.	Ampia Media Limitata	Cifre
Numero di partita IVA danese Vedere "Numero di partita IVA danese" a pagina 1012.	Ampia Media Limitata	Cifre e lettere
Numero patente di guida - Stato della California Vedere "Numero patente di guida - Stato della California " a pagina 1015.	Ampia Media	Minuscolo

Identificatore dati	Coperture	Normalizzatore
<p>Numero patente di guida - Stati della Florida, del Michigan e del Minnesota</p> <p>Vedere "Numero di patente di guida - Stati della Florida, del Michigan e del Minnesota" a pagina 1016.</p>	<p>Ampia</p> <p>Media</p>	Minuscolo
<p>Numero patente di guida - Stato dell'Illinois</p> <p>Vedere "Numero patente di guida - Stato dell'Illinois" a pagina 1018.</p>	<p>Ampia</p> <p>Media</p>	Minuscolo
<p>Numero patente di guida - Stato del New Jersey</p> <p>Vedere "Numero patente di guida - Stato del New Jersey" a pagina 1020.</p>	<p>Ampia</p> <p>Media</p>	Minuscolo
<p>Numero patente di guida - Stato di New York</p> <p>Vedere "Numero patente di guida - Stato di New York" a pagina 1021.</p>	<p>Ampia</p> <p>Media</p>	Minuscolo
<p>Numero patente di guida - Stato di Washington</p> <p>Vedere "Numero di patente di guida - Stato di Washington" a pagina 1023.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Minuscolo
<p>Numero patente di guida - Stato del Wisconsin</p> <p>Vedere "Numero di patente di guida - Stato del Wisconsin" a pagina 1025.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Cifre e lettere
<p>Numero DEA</p> <p>Vedere "Numero DEA (Drug Enforcement Agency)" a pagina 1027.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Minuscolo
<p>Numero di patente di guida finlandese</p> <p>Vedere "Numero di patente di guida finlandese" a pagina 1029.</p>	<p>Ampia</p> <p>Media</p> <p>Limitata</p>	Cifre e lettere
<p>Numero di previdenza sociale europea della Finlandia</p> <p>Vedere "Numero di previdenza sociale europea della Finlandia" a pagina 1032.</p>	<p>Ampia</p> <p>Limitata</p>	Cifre
<p>Numero di passaporto finlandese</p> <p>Vedere "Numero di passaporto finlandese" a pagina 1034.</p>	<p>Ampia</p> <p>Limitata</p>	Cifre e lettere

Identificatore dati	Coperture	Normalizzatore
Numero di identificazione fiscale finlandese Vedere "Numero di identificazione fiscale finlandese" a pagina 1035.	Ampia Media Limitata	Non intervenire
Numero di partita IVA finlandese Vedere "Numero di partita IVA finlandese" a pagina 1038.	Ampia Media Limitata	Cifre e lettere
Codice identificativo personale finlandese Vedere "Codice identificativo personale finlandese" a pagina 1040.	Ampia Media Limitata	Minuscolo
Numero di patente di guida francese Vedere "Numero di patente di guida francese" a pagina 1042.	Ampia Limitata	Cifre
Numero di previdenza sociale francese Vedere "Numero di previdenza sociale francese" a pagina 1044.	Ampia Limitata	Cifre
Numero di identificazione fiscale francese Vedere "Numero di identificazione fiscale francese" a pagina 1045.	Ampia Limitata	Cifre
Numero di partita IVA francese Vedere "Numero di partita IVA francese" a pagina 1047.	Ampia Media Limitata	Cifre e lettere
Codice INSEE francese Vedere "Codice INSEE francese" a pagina 1049.	Ampia Limitata	Cifre
Numero di passaporto francese Vedere "Numero di passaporto francese" a pagina 1051.	Ampia Limitata	Cifre e lettere
Numero di previdenza sociale francese Vedere "Numero di previdenza sociale francese" a pagina 1052.	Ampia Media Limitata	Cifre e lettere
Numero di passaporto tedesco Vedere "Numero di passaporto tedesco" a pagina 1054.	Ampia Media Limitata	Minuscolo

Identificatore dati	Coperture	Normalizzatore
Numero di identificazione personale tedesco Vedere "Numero di identificazione personale tedesco" a pagina 1056.	Ampia Media Limitata	Minuscolo
Numero di patente di guida tedesca Vedere "Numero di patente di guida tedesca" a pagina 1059.	Ampia Limitata	Cifre e lettere
Numero di identificazione fiscale tedesco Vedere "Numero di identificazione fiscale tedesco" a pagina 1060.	Ampia Media Limitata	Cifre
Numero di partita IVA tedesca Vedere "Numero di partita IVA tedesca" a pagina 1063.	Ampia Media Limitata	Cifre e lettere
Codice fiscale della Grecia (AMKA) Vedere "Codice fiscale della Grecia (AMKA)" a pagina 1065.	Ampia Media Limitata	Cifre
Codice fiscale greco (AFM) Vedere "Codice fiscale greco (AFM)" a pagina 1067.	Ampia Media Limitata	Cifre
Healthcare Common Procedure Coding System (codice CPT HCPCS). Vedere "Healthcare Common Procedure Coding System (codice CPT HCPCS)." a pagina 1069.	Media Limitata	Cifre e lettere
Numero di assicurazione sanitaria Vedere "Numero di assicurazione sanitaria" a pagina 1072.	Ampia Media Limitata	Cifre e lettere
ID Hong Kong Vedere "ID Hong Kong" a pagina 1076.	Ampia Limitata	Minuscolo
Numero di previdenza sociale ungherese Vedere "Numero di previdenza sociale ungherese" a pagina 1078.	Ampia Media Limitata	Cifre

Identificatore dati	Coperture	Normalizzatore
Codice fiscale (TIN) ungherese Vedere "Numero di identificazione fiscale ungherese" a pagina 1080.	Ampia Media Limitata	Cifre
Numero di partita IVA ungherese Vedere "Numero di partita IVA ungherese" a pagina 1082.	Ampia Media Limitata	Minuscolo
IBAN paesi centrali Vedere "IBAN paesi centrali" a pagina 1084.	Ampia Limitata	Non intervenire
IBAN paesi orientali Vedere "IBAN paesi orientali" a pagina 1088.	Ampia Limitata	Non intervenire
IBAN paesi occidentali Vedere "IBAN paesi occidentali" a pagina 1094.	Ampia Limitata	Non intervenire
Numero tessera Aadhaar indiana Vedere "Numero tessera Aadhaar indiana" a pagina 1098.	Ampia Media Limitata	Cifre
Codice di identificazione fiscale indiano (PAN) Vedere "Codice di identificazione fiscale indiano (PAN)" a pagina 1100.	Ampia Limitata	Cifre e lettere
Numero di carta di identità indonesiana (KTP) Vedere "Numero di carta di identità indonesiana (KTP)" a pagina 1102.	Ampia Media Limitata	Cifre
Numero IMEI Vedere "Numero IMEI" a pagina 1104.	Ampia Media Limitata	Cifre
Codice ISIN (International Securities Identification Number) Vedere "Codice ISIN (International Securities Identification Number)" a pagina 1106.	Ampia Media Limitata	Minuscolo

Identificatore dati	Coperture	Normalizzatore
Indirizzo IP Vedere "Indirizzo IP" a pagina 1108.	Ampia Media Limitata	Non intervenire
Indirizzo IPv6 Vedere "Indirizzo IPv6" a pagina 1110.	Ampia Media Limitata	Non intervenire
Numero di passaporto irlandese Vedere "Numero di passaporto irlandese" a pagina 1113.	Ampia Limitata	Cifre e lettere
Numero di identificazione fiscale irlandese Vedere "Numero di identificazione fiscale irlandese" a pagina 1114.	Ampia Media Limitata	Cifre e lettere
Numero di partita IVA irlandese Vedere "Numero di partita IVA irlandese" a pagina 1118.	Ampia Media Limitata	Cifre e lettere
Numero personale di servizio pubblico irlandese (PPS) Vedere "Numero personale di servizio pubblico irlandese" a pagina 1121.	Ampia Media Limitata	Minuscolo
Numero di identificazione personale israeliano Vedere "Numero di identificazione personale israeliano" a pagina 1124.	Ampia Media Limitata	Cifre
Numero di patente di guida italiana Vedere "Numero di patente di guida italiana" a pagina 1126.	Ampia Limitata	Cifre e lettere
Numero di previdenza sociale italiano Vedere "Numero di previdenza sociale italiano" a pagina 1127.	Ampia Limitata	Cifre e lettere
Numero di passaporto italiano Vedere "Numero di passaporto italiano" a pagina 1129.	Ampia Limitata	Cifre e lettere
Numero di partita IVA italiano Vedere "Numero di partita IVA italiano" a pagina 1131.	Ampia Media Limitata	Cifre e lettere

Identificatore dati	Coperture	Normalizzatore
Numero di patente di guida giapponese Vedere "Numero di patente di guida giapponese" a pagina 1133.	Ampia Media Limitata	Cifre
Numero di passaporto giapponese Vedere "Numero di passaporto giapponese" a pagina 1135.	Ampia Limitata	Cifre e lettere
Numero di identificazione giapponese (Juki Net) Vedere "Numero di identificazione giapponese (Juki Net)" a pagina 1137.	Ampia Media Limitata	Cifre
Numero di identificazione personale giapponese - Aziendale Vedere "Numero di identificazione personale giapponese - Aziendale" a pagina 1139.	Ampia Limitata	Cifre
Numero di identificazione personale giapponese - Personale Vedere "Numero di identificazione personale giapponese - Personale" a pagina 1141.	Ampia Media Limitata	Cifre
Numero di passaporto coreano Vedere "Numero di passaporto coreano" a pagina 1143.	Ampia Limitata	Cifre e lettere
Numero di registrazione anagrafica coreano per stranieri Vedere "Numero di registrazione anagrafica coreano per stranieri." a pagina 1145.	Ampia Media Limitata	Cifre
Numero di registrazione anagrafica coreano per coreani Vedere "Numero di registrazione anagrafica coreano per coreani" a pagina 1148.	Ampia Media Limitata	Cifre
Numero di identificazione personale lettone Vedere "Numero di identificazione personale lettone" a pagina 1151.	Ampia Media Limitata	Cifre
Numero di identificazione lussemburghese (RNPP) Vedere "Numero di identificazione lussemburghese (RNPP)" a pagina 1153.	Ampia Media Limitata	Cifre

Identificatore dati	Coperture	Normalizzatore
Numero di passaporto lussemburghese Vedere " Numero di passaporto lussemburghese " a pagina 1155.	Ampia Limitata	Cifre e lettere
Numero di identificazione fiscale lussemburghese Vedere " Numero di identificazione fiscale lussemburghese " a pagina 1157.	Ampia Media Limitata	Cifre
Numero di partita IVA lussemburghese Vedere " Numero di partita IVA lussemburghese " a pagina 1161.	Ampia Media Limitata	Cifre e lettere
Numero di carta di identità malese (MyKad) Vedere " Numero di carta di identità malese (MyKad) " a pagina 1164.	Ampia Media Limitata	Cifre
Identificatore beneficiario di assistenza sanitaria Vedere " Identificatore beneficiario di assistenza sanitaria " a pagina 1167.	Ampia Media Limitata	Cifre e lettere
Numero di registrazione e identificazione personale messicano Vedere " Numero di registrazione e identificazione personale messicano " a pagina 1169.	Ampia Media Limitata	Cifre e lettere
Numero di identificazione fiscale messicano Vedere " Numero di identificazione fiscale messicano " a pagina 1171.	Ampia Media Limitata	Cifre e lettere
Codice di identificazione personale messicano (CURP) Vedere " Codice di identificazione personale messicano (CURP) " a pagina 1174.	Ampia Media Limitata	Minuscolo
Numero di conto bancario esteso messicano (CLABE) Vedere " Numero di conto bancario esteso messicano (CLABE) " a pagina 1176.	Ampia Media Limitata	Cifre
National Drug Code (NDC, codici identificativi dei medicinali) Vedere " National Drug Code (NDC, codici identificativi dei farmaci) " a pagina 1178.	Ampia Media Limitata	Non intervenire

Identificatore dati	Coperture	Normalizzatore
Numero NPI Vedere "Numero NPI" a pagina 1181.	Ampia Media Limitata	Cifre
Numero di patente di guida dei Paesi Bassi Vedere "Numero di patente di guida dei Paesi Bassi" a pagina 1183.	Ampia Limitata	Cifre
Numero di passaporto dei Paesi Bassi Vedere "Numero di passaporto dei Paesi Bassi" a pagina 1184.	Ampia Limitata	Cifre e lettere
Numero di identificazione fiscale dei Paesi Bassi Vedere "Numero di identificazione fiscale dei Paesi Bassi" a pagina 1185.	Ampia Media Limitata	Cifre
Numero di partita IVA dei Paesi Bassi Vedere "Numero di partita IVA dei Paesi Bassi" a pagina 1189.	Ampia Media Limitata	Cifre e lettere
Codice di assistenza sanitaria della Nuova Zelanda (NHI) Vedere "Codice di assistenza sanitaria della Nuova Zelanda (NHI)" a pagina 1191.	Ampia Media Limitata	Minuscolo
Numero di identificazione personale norvegese Vedere "Numero di identificazione personale norvegese" a pagina 1193.	Ampia Media Limitata	Cifre
Documento di identità cinese Vedere "Documento di identità cinese" a pagina 1196.	Ampia Limitata	Minuscolo
Numero di carta di identità polacca Vedere "Numero di carta di identità polacca" a pagina 1197.	Ampia Media Limitata	Cifre e lettere
Codice statistico polacco (REGON) Vedere "Codice statistico polacco (REGON)" a pagina 1199.	Ampia Media Limitata	Cifre

Identificatore dati	Coperture	Normalizzatore
Codice fiscale polacco (PESEL) Vedere "Codice fiscale polacco (PESEL)" a pagina 1201.	Ampia Media Limitata	Cifre
Numero di identificazione fiscale polacco (NIP) Vedere "Numero di identificazione fiscale polacco (NIP)" a pagina 1203.	Ampia Media Limitata	Cifre
Numero di patente di guida portoghese Vedere "Numero di patente di guida portoghese" a pagina 1206.	Ampia Limitata	Cifre e lettere
Numero di identificazione nazionale portoghese Vedere "Numero di identificazione nazionale portoghese" a pagina 1208.	Ampia Media Limitata	Cifre e lettere
Numero di passaporto portoghese Vedere "Numero di passaporto portoghese" a pagina 1211.	Ampia Limitata	Cifre e lettere
Numero di identificazione fiscale portoghese Vedere "Numero di identificazione fiscale portoghese" a pagina 1212.	Ampia Media Limitata	Cifre
Numero di partita IVA portoghese Vedere "Numero di partita IVA portoghese" a pagina 1215.	Ampia Media Limitata	Cifre e lettere
Social Security Number (SSN) statunitense randomizzato Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218.	Media Limitata	Cifre
Numero di identificazione nazionale rumeno Vedere "Numero di identificazione nazionale rumeno" a pagina 1221.	Ampia Media Limitata	Cifre
Numero di identificazione personale rumeno (CNP) Vedere "Numero di identificazione personale rumeno (CNP)" a pagina 1223.	Ampia Media Limitata	Cifre

Identificatore dati	Coperture	Normalizzatore
Numero di passaporto russo interno Vedere "Numero di passaporto russo interno" a pagina 1225.	Ampia Limitata	Cifre
Numero di identificazione fiscale russo (INN) Vedere "Numero di identificazione fiscale russo (INN)" a pagina 1227.	Ampia Media Limitata	Cifre
NRIC Singapore Vedere "Identificatore di dati NRIC Singapore" a pagina 1229.	Ampia	Minuscolo
Numero di identificazione nazionale slovacco Vedere "Numero di identificazione nazionale slovacco" a pagina 1230.	Ampia Media Limitata	Cifre e lettere
Numero identificativo cittadini della Slovenia Vedere "Numero identificativo cittadini della Slovenia" a pagina 1233.	Ampia Media Limitata	Cifre
Numero di identificazione personale sudafricano Vedere "Numero di identificazione personale sudafricano" a pagina 1235.	Ampia Media Limitata	Cifre
Numero di patente di guida spagnola Vedere "Numero di patente di guida spagnola" a pagina 1238.	Ampia Limitata	Cifre e lettere
Numero di partita IVA spagnolo Vedere "Numero di partita IVA spagnolo" a pagina 1240.	Ampia Media Limitata	Cifre e lettere
Numero di conto cliente spagnolo Vedere "Numero di conto cliente spagnolo" a pagina 1243.	Ampia Media Limitata	Cifre
Numero di DNI spagnolo Vedere "Numero di DNI spagnolo" a pagina 1245.	Ampia Limitata	Cifre e lettere
Numero di previdenza sociale spagnolo Vedere "Numero di previdenza sociale spagnolo" a pagina 1249.	Ampia Media Limitata	Cifre

Identificatore dati	Coperture	Normalizzatore
Codice fiscale spagnolo (CIF) Vedere "Codice fiscale spagnolo (CIF)" a pagina 1251.	Ampia Media Limitata	Cifre e lettere
Numero di patente di guida svedese Vedere "Numero di patente di guida svedese" a pagina 1254.	Ampia Media Limitata	Cifre
Numero di identificazione fiscale svedese Vedere "Numero di identificazione fiscale svedese" a pagina 1256.	Ampia Media Limitata	Cifre
Numero di partita IVA svedese Vedere "Numero di partita IVA svedese" a pagina 1258.	Ampia Media Limitata	Cifre e lettere
Numero di passaporto svedese Vedere "Numero di passaporto svedese" a pagina 1260.	Ampia Limitata	Cifre e lettere
Numero di identificazione personale svedese Vedere "Numero di identificazione personale svedese" a pagina 1262.	Ampia Media Limitata	Cifre
Codice SWIFT Vedere "Codice SWIFT " a pagina 1265.	Ampia Limitata	Swift
Numero AHV svizzero Vedere "Numero AHV svizzero" a pagina 1267.	Ampia Limitata	Cifre
Numero di previdenza sociale svizzero (AHV) Vedere "Numero di previdenza sociale svizzero (AHV)" a pagina 1269.	Ampia Media Limitata	Cifre
ID ROC di Taiwan Vedere "ID ROC Taiwan" a pagina 1271.	Ampia Limitata	Non intervenire
Numero di identificazione personale thailandese Vedere "Numero di identificazione personale thailandese" a pagina 1273.	Ampia Media Limitata	Cifre

Identificatore dati	Coperture	Normalizzatore
Numero di identificazione turco Vedere "Numero di identificazione turco" a pagina 1275.	Ampia Media Limitata	Cifre
Coordinate bancarie di un numero di conto britannico Vedere "Coordinate bancarie di un numero di conto britannico" a pagina 1277.	Ampia Media Limitata	Cifre
Numero patente di guida britannica Vedere "Numero di patente di guida britannica" a pagina 1279.	Ampia Media Limitata	Cifre e lettere
Numero di tessera elettorale britannico Vedere "Numero di tessera elettorale britannico" a pagina 1282.	Limitata	Minuscolo
Numero NHS (National Health Service) britannico Vedere "Numero NHS (National Health Service) del Regno Unito" a pagina 1282.	Media Limitata	Cifre
Numero di previdenza sociale britannico Vedere "Numero di previdenza sociale britannico" a pagina 1285.	Ampia Media Limitata	Minuscolo
Numero di passaporto britannico Vedere "Numero di passaporto britannico" a pagina 1287.	Ampia Media Limitata	Non intervenire
Codice fiscale britannico Vedere "Codice fiscale britannico" a pagina 1289.	Ampia Media Limitata	Non intervenire
Numero di partita IVA britannico (VAT) Vedere "Numero di partita IVA britannico (VAT)" a pagina 1291.	Ampia Media Limitata	Cifre e lettere
Carta di identità ucraina Vedere "Carta di identità ucraina" a pagina 1296.	Ampia Media Limitata	Cifre

Identificatore dati	Coperture	Normalizzatore
Passaporto ucraino (interno) Vedere "Passaporto ucraino (interno)" a pagina 1294.	Ampia Limitata	Cifre
Passaporto ucraino (internazionale) Vedere "Passaporto ucraino (internazionale)" a pagina 1298.	Ampia Limitata	Cifre e lettere
Numero di identificazione personale degli Emirati Arabi Uniti Vedere "Numero di identificazione personale degli Emirati Arabi Uniti" a pagina 1300.	Ampia Media Limitata	Cifre
US Individual Tax Identification Number (ITIN) (codice fiscale statunitense) Vedere "US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)" a pagina 1302.	Ampia Media Limitata	Cifre
Numero di passaporto statunitense Vedere "Numero di passaporto statunitense" a pagina 1305.	Ampia Limitata	Cifre
Social Security Number (SSN) statunitense randomizzato Vedere "Social Security Number (SSN) statunitense" a pagina 1307.	Ampia Media Limitata	Cifre
Codici di avviamento postale Zip+4 statunitensi Vedere "Codici di avviamento postale Zip+4 statunitensi" a pagina 1310.	Ampia Media Limitata	Cifre e lettere
Numero di identificazione nazionale venezuelano Vedere "Numero di identificazione nazionale venezuelano" a pagina 1312.	Ampia Media Limitata	Cifre e lettere

Utilizzo delle convalide opzionali

La [Tabella 27-17](#) elenca le convalide opzionali che gli autori di politiche possono configurare per gli identificatori dati del sistema.

Vedere ["Informazioni sulle convalide facoltative per identificatori di dati"](#) a pagina 695.

Tabella 27-17 Convalide opzionali disponibili per le istanze di politica

Convalida opzionale	Descrizione
Richiedi caratteri iniziali	<p>Cerca la corrispondenza con i caratteri all'inizio dei dati corrispondenti.</p> <p>Ad esempio, per l'identificatore dati della patente di guida della California è possibile richiedere che il carattere iniziale sia la lettera "C". In questo caso il motore trova la corrispondenza con il numero di patente C6457291.</p> <p>Vedere "Caratteri accettabili per le convalide opzionali" a pagina 721.</p>
Richiedi caratteri finali	<p>Cerca la corrispondenza con i caratteri alla fine dei dati corrispondenti.</p> <p>Vedere "Caratteri accettabili per le convalide opzionali" a pagina 721.</p>
Escludi caratteri iniziali	<p>Esclude dalla corrispondenza i caratteri all'inizio dei dati corrispondenti.</p> <p>Vedere "Caratteri accettabili per le convalide opzionali" a pagina 721.</p>
Escludi caratteri finali	<p>Esclude dalla corrispondenza i caratteri alla fine dei dati corrispondenti.</p> <p>Vedere "Caratteri accettabili per le convalide opzionali" a pagina 721.</p>
Trova parole chiave	<p>Cerca la corrispondenza di una o più parole chiave o frasi chiave oltre ai dati corrispondenti. Può verificare la prossimità dei criteri corrispondenti con un elenco di parole chiave.</p> <p>È inoltre possibile analizzare le parole chiave per la distinzione maiuscole/minuscole. Viene quindi eseguita una verifica della prossimità dei criteri degli identificatori dati soddisfatti rispetto a un elenco di parole chiave. Viene generato un incidente quando tutti i criteri dell'identificatore dati nella regola corrispondono. Le parole chiave acquisite sono evidenziate negli incidenti. La prossimità, la distinzione tra maiuscole e minuscole e l'evidenziazione della convalida sono disattivate per impostazione predefinita e per funzionare devono essere attivate.</p> <p>Per segnalare una corrispondenza, la parola chiave deve essere rilevata nello stesso componente del messaggio del contenuto dell'identificatore dati</p> <p>Vedere "Informazioni sulla corrispondenza con diversi componenti" a pagina 696.</p> <p>Questa convalida opzionale accetta qualsiasi carattere (numeri, lettere, altro).</p> <p>Vedere "Caratteri accettabili per le convalide opzionali" a pagina 721.</p> <p>Vedere "Elenco delle convalide criterio che accettano dati di input" a pagina 727.</p>

Configurazione delle convalide opzionali

Implementare le convalide opzionali per affinare l'ambito di un identificatore dati definito nell'istanza di una politica. Gli identificatori dati del sistema e personalizzati supportano la configurazione delle convalide opzionali.

Vedere ["Informazioni sulle convalide facoltative per identificatori di dati"](#) a pagina 695.

Il tipo di input consentito da una convalida opzionale (numeri, lettere, caratteri) dipende dall'identificatore dati. Se si immettono caratteri di input non accettabili e si tenta di salvare la configurazione, il sistema segnala un errore.

Ad esempio, l'identificatore dati Social Security Number (SSN) statunitense accetta solo numeri. Se si configura la convalida opzionale "Richiedi caratteri finali" e si fornisce un input sotto forma di lettere, si riceve l'errore seguente quando si tenta di salvare la configurazione: **Input per convalida "Richiedi caratteri finali" non corretto: L'elenco contiene caratteri non numerici.**

Vedere [Tabella 27-18](#) a pagina 722.

Per configurare una convalida opzionale

- 1 Fare clic sul segno più accanto all'etichetta **Convalide opzionali** per l'istanza dell'identificatore dati che si sta configurando.
Vedere ["Configurazione della condizione Contenuto corrispondente a identificatore dati"](#) a pagina 700.
- 2 Selezionare una o più convalide opzionali.
Vedere ["Informazioni sulle convalide facoltative per identificatori di dati"](#) a pagina 695.
- 3 Fornire l'input previsto per ciascuna convalida opzionale selezionata.
Ogni valore può avere una lunghezza qualsiasi. Utilizzare virgole per separare più valori.
- 4 Fare clic su **Salva** per salvare la configurazione.
Se il sistema visualizza un messaggio di errore, assicurarsi di avere immesso il tipo corretto di input di caratteri previsto.
Vedere [Tabella 27-18](#) a pagina 722.

Caratteri accettabili per le convalide opzionali

Ogni convalida opzionale richiede di immettere alcuni valori di dati. È necessario immettere il tipo appropriato di dati in base all'identificatore dati. La [Tabella 27-18](#) elenca il tipo di dati accettabili per ciascuna coppia identificatore dati/convalida opzionale.

Vedere ["Informazioni sulle convalide facoltative per identificatori di dati"](#) a pagina 695.

Nota: la convalida opzionale **Trova parole chiave** accetta qualsiasi carattere come valore per tutti gli identificatori dati.

Il tipo di dati previsto dalla convalida opzionale dipende dall'identificatore dati. La maggior parte delle coppie identificatore dati/convalida opzionale accetta solo numeri. Alcune accettano valori alfanumerici e altre accettano qualsiasi carattere. Se si immette un carattere inaccettabile e si tenta di salvare la politica, il sistema segnala un errore.

Vedere ["Configurazione delle convalide opzionali"](#) a pagina 720.

Tabella 27-18 Caratteri accettabili per le convalide opzionali

Identificatore dati	Richiedi caratteri finali	Escludi caratteri finali	Richiedi caratteri iniziali	Escludi caratteri iniziali
Social Security Number (SSN) statunitense randomizzato	Solo numeri			
Social Insurance Number (numero di previdenza sociale) canadese	Solo numeri			
US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)	Solo numeri			
Numero patente di guida - Stato della California	Solo numeri		Qualsiasi carattere (normalizzato in minuscolo)	
Numero patente di guida - Stato dell'Illinois	Solo numeri		Qualsiasi carattere (normalizzato in minuscolo)	
Numero patente di guida - Stato del New Jersey	Solo numeri		Qualsiasi carattere (normalizzato in minuscolo)	
Numero patente di guida - Stato di New York	Solo numeri			
Numero di patente di guida - Stati della Florida, del Michigan e del Minnesota	Solo numeri		Qualsiasi carattere (normalizzato in minuscolo)	
Numero di carta di credito	Solo numeri			
Numero di routing ABA	Solo numeri			
Numero CUSIP	Solo numeri			
Codice SWIFT	Alfanumerico (numeri o lettere)			
Dati banda magnetica carta di credito	Solo numeri			
IBAN paesi occidentali	Alfanumerico (numeri o lettere)			
IBAN paesi centrali	Alfanumerico (numeri o lettere)			
IBAN paesi orientali	Alfanumerico (numeri o lettere)			
National Drug Code (NDC, codici identificativi dei medicinali)	Solo numeri			

Identificatore dati	Richiedi caratteri finali	Escludi caratteri finali	Richiedi caratteri iniziali	Escludi caratteri iniziali
Numero Medicare australiano	Solo numeri			
Indirizzo IP	Qualsiasi carattere			
Codice Fiscale	Solo numeri			
Numero di DNI spagnolo	Solo numeri			
Burgerservicenummer	Solo numeri			
Numero di patente di guida britannica	Alfanumerico (normalizzato in minuscolo)			
Codice fiscale britannico	Solo numeri			
Numero di passaporto britannico	Solo numeri			
Numero di previdenza sociale britannico	Alfanumerico (normalizzato in minuscolo)			
Numero NHS (National Health Service) britannico	Solo numeri			
Numero di tessera elettorale britannico	Solo numeri		Qualsiasi carattere (normalizzato in minuscolo)	
Codice INSEE francese	Solo numeri			
Numero AHV svizzero	Solo numeri			
Tax File Number (codice fiscale) australiano	Solo numeri			
Documento di identità cinese	Solo numeri			
ID Hong Kong	Solo numeri			
NRIC Singapore	Solo numeri			
ID Taiwan	Solo numeri			

Utilizzo del totale corrispondenze univoche

Quando si definisce una nuova regola dell'identificatore dati, una nuova regola per le parole chiave o una nuova regola per le espressioni regolari, il metodo predefinito per il conteggio delle corrispondenze è **Conta tutte le corrispondenze univoche**.

La seguente tabella descrive le caratteristiche di conteggio delle corrispondenze univoche.

Tabella 27-19 Caratteristiche di conteggio delle corrispondenze univoche

Caratteristica di conteggio delle corrispondenze univoche	Descrizione
La prima corrispondenza è univoca	Una corrispondenza univoca è la prima corrispondenza trovata in un componente del messaggio. Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.
Match count updated for each unique match (Conteggio corrispondenze aggiornato per ogni corrispondenza univoca)	Il conteggio delle corrispondenze viene incrementato di 1 per ogni corrispondenza del criterio univoca.
Solo le corrispondenze univoche sono evidenziate	Le corrispondenze duplicate non vengono conteggiate né evidenziate nella schermata Istantanea incidente Vedere "Risoluzione di incidenti" a pagina 1573.
L'univocità non si estende ai componenti del messaggio	Se ad esempio lo stesso SSN appare sia nel corpo del messaggio che in un allegato, vengono generate due corrispondenze e non una sola. Ciò dipende dal fatto che ogni istanza viene individuata in un componente distinto del messaggio.
Regola composta con condizioni di identificatore dati e prossimità parole chiave	In una regola composta che combina una condizione dell'identificatore dati con una condizione parola chiave che specifica la logica della prossimità delle parole chiave, la corrispondenza segnalata è la prima corrispondenza trovata

Configurazione del conteggio delle corrispondenze univoche

Conta tutte le corrispondenze univoche è la selezione predefinita per i nuovi identificatori dati creati. Se non lo si è fatto prima, dopo avere aggiornato Data Loss Prevention, è possibile che sia necessario configurare manualmente le regole degli identificatori dati preesistenti per l'utilizzo del conteggio delle corrispondenze univoche.

Vedere ["Informazioni sul conteggio delle corrispondenze univoche"](#) a pagina 697.

Per configurare il conteggio delle corrispondenze univoche

- 1 Selezionare la politica che contiene le regole degli identificatori dati se si desidera eseguire l'upgrade nella schermata **Gestisci > Politiche > Elenco politiche**.
- 2 Selezionare la regola dell'identificatore dati nella schermata **Configura politica**.
- 3 Selezionare l'opzione di conteggio delle corrispondenze **Conta tutte le corrispondenze univoche**.
- 4 Fare clic su **OK** per applicare la modifica di configurazione del conteggio delle corrispondenze univoche.

5 Fare clic su **Salva** per salvare la modifica della politica.

6 Testare il conteggio delle corrispondenze univoche.

Creare un incidente con più istanze di un criterio di identificatore dati, ad esempio diverse istanze dello stesso codice fiscale nello stesso componente del messaggio (ad esempio, in un allegato di e-mail).

In **Istantanea incidente** verificare che vengano evidenziate e contate solo le corrispondenze univoche.

Modifica degli identificatori dati di sistema

Il sistema consente di modificare gli identificatori dati definiti dal sistema, ma non di eliminarli. Tutte le modifiche apportate alla configurazione di un identificatore dati definito dal sistema entrano in vigore nell'intero sistema. Ciò significa che le modifiche si applicano a tutte le politiche che dichiarano l'identificatore dati attivamente o in un secondo momento.

Una volta che è stato modificato, non è possibile riportare automaticamente un identificatore dati alla configurazione originale. Prima di modificare un identificatore dati di sistema, considerare la possibilità di clonarlo.

Lo stesso vale per gli identificatori dati personalizzati che sono stati creati. Tutte le modifiche apportate a un identificatore dati hanno effetto nell'intero sistema. Ciò significa che le modifiche si applicano a tutte le politiche che dichiarano l'identificatore dati modificato.

Il sistema non include gli identificatori dati modificati nelle politiche esportate come modelli. Prima della modifica di un identificatore dati di sistema, esportare tutte le politiche che lo dichiarano.

Vedere ["Modifica degli identificatori dati"](#) a pagina 699.

Vedere ["Modifica dell'input di convalida dei criteri"](#) a pagina 727.

Nota: Il sistema non esporta gli identificatori dati modificati e personalizzati in un modello di politica. Il sistema esporta un riferimento all'identificatore dati di sistema. Il sistema di destinazione in cui viene importato il modello di politica fornisce l'identificatore dati vero e proprio. Vedere ["Clonare gli identificatori di dati definiti dal sistema prima della modifica per mantenere lo stato originale"](#) a pagina 767.

Vedere ["Modifica degli identificatori dati"](#) a pagina 699.

Tabella 27-20 Opzioni di modifica dell'identificatore dati di sistema

Modificabile a livello di sistema	Non configurabile
<ul style="list-style-type: none"> ■ Criteri È possibile modificare uno o più criteri identificatore dati a livello di sistema. ■ Convalide attive È possibile aggiungere o rimuovere le convalide richieste a livello di sistema. ■ Immissione dati È possibile modificare l'input di una convalida attiva per un identificatore dati di sistema. 	<ul style="list-style-type: none"> ■ Nome, Descrizione e Categoria Non è possibile modificare il nome, la descrizione o la categoria di un identificatore dati di sistema. ■ Copertura Non è possibile definire una nuova copertura di rilevamento per un identificatore dati di sistema; è solo possibile modificare una copertura esistente. ■ Convalide opzionali Non è possibile definire convalide opzionali a livello di sistema. È possibile configurare convalide opzionali solo a livello di politica. ■ Normalizzatore di dati Non è possibile modificare il tipo di normalizzatore di dati implementato da un identificatore dati di sistema. ■ Eliminazione Non è possibile eliminare un identificatore dati di sistema.

Clonazione di un identificatore dati di sistema prima della sua modifica

Enforce Server non fornisce un meccanismo automatizzato per la clonazione di un identificatore dati di sistema.

Vedere ["Estensione e personalizzazione di identificatori di dati"](#) a pagina 693.

Prima di modificare un identificatore dati di sistema, considerare la possibilità di clonarlo manualmente in modo poter tornare alla configurazione originale, se necessario. Come minimo è consigliabile esportare una politica come modello prima di modificare qualsiasi Identificatore dati di sistema dichiarato dal tale politica.

Per clonare manualmente un identificatore dati di sistema

- 1 Esaminare la configurazione originale dell'identificatore dati che si desidera modificare.
- 2 Creare un identificatore dati personalizzato.
Vedere ["Flusso di lavoro per la creazione di identificatori di dati personalizzati"](#) a pagina 749.
- 3 Copiare la configurazione dell'identificatore dati originale nell'identificatore dati personalizzato.

Aggiungere il o i criteri, la o le convalide, gli input di dati e il normalizzatore.

Vedere ["Selezione di una copertura dell'identificatore di dati"](#) a pagina 703.

- 4 Salvare l'identificatore dati personalizzato.
- 5 Modificare l'identificatore dati personalizzato in base alle esigenze.

Modifica dell'input di convalida dei criteri

Al livello del sistema è possibile modificare l'immissione di dati che accetta una convalida obbligatoria. Non tutte le convalide accettano l'immissione di dati.

Vedere ["Informazioni sulle convalide criterio"](#) a pagina 696.

Per modificare l'input di convalida obbligatoria

- 1 Modificare l'identificatore dati selezionandolo nella schermata **Gestisci > Politiche > Identificatore dati**.
- 2 Selezionare la **copertura della regola** che si desidera modificare.
 Generalmente le opzioni di copertura media e limitata includono convalide che accettano l'immissione di dati.
- 3 Dall'elenco **Convalide attive** selezionare la convalida modificabile di cui si desidera modificare l'input.
 Ad esempio selezionare **Trova parole chiave**.
 Vedere ["Elenco delle convalide criterio che accettano dati di input"](#) a pagina 727.
- 4 Modificare l'input per la convalida nel campo **Immissione dati e descrizione**.
- 5 Selezionare le caratteristiche desiderate per la parola chiave:
 - **Prossimità** - Per trovare una parola chiave solo nell'ambito della prossimità impostata dei criteri che corrispondono, selezionare questa casella e indicare la **Distanza tra le parole** o prossimità.
 - **Distinzione maiuscole/minuscole** - Selezionare questa casella se si desidera trovare una corrispondenza con distinzione tra maiuscole e minuscole.
 - **Evidenzia parole chiave nell'incidente** - Selezionare questa casella se si desidera evidenziare le parole chiave corrispondenti negli incidenti.
- 6 Fare clic su **Aggiorna convalida** per salvare le modifiche apportate all'input di convalida.
 Fare clic su **Ignora modifiche** per non salvare le modifiche.
- 7 Fare clic su **Salva** per salvare l'identificatore dati.

Elenco delle convalide criterio che accettano dati di input

La seguente tabella elenca tutte le convalide criterio disponibili che richiedono input di dati. I dati di input sono modificabili nella definizione di livello sistema dell'identificatore dati.

Nota: L'input utilizzato per le convalide iniziale e finale riguarda il testo della corrispondenza stessa. L'input utilizzato per le convalide prefisso e suffisso riguarda i caratteri che precedono e seguono il testo oggetto della corrispondenza.

Tabella 27-21 Convalide criterio che accettano dati di input

Convalida	Descrizione
Corrispondenza esatta	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.
Escludi caratteri iniziali	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.
Escludi caratteri finali	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.
Escludi corrispondenza esatta	Immettere un elenco di valori delimitati da virgole. Ogni valore può avere una lunghezza qualsiasi.
Escludi prefisso	Immettere un elenco di valori delimitati da virgole. Ogni valore può avere una lunghezza qualsiasi.
Escludi suffisso	Immettere un elenco di valori delimitati da virgole. Ogni valore può avere una lunghezza qualsiasi.
Trova parole chiave	Immettere un elenco di valori delimitati da virgole. Ogni valore può avere una lunghezza qualsiasi.
Richiedi caratteri iniziali	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.
Richiedi caratteri finali	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.

Modifica delle parole chiave per gli identificatori dati PII internazionali

Gli identificatori dati offrono un ampio supporto per il rilevamento di contenuto internazionale.

Vedere ["Introduzione agli identificatori di dati"](#) a pagina 681.

Alcuni identificatori dati internazionali offrono solo una copertura di rilevamento ampia. In questo caso è possibile implementare la convalida opzionale Trova parole chiave per limitare l'ambito di rilevamento. L'implementazione di questa convalida opzionale può contribuire a eliminare eventuali falsi positivi corrispondenti alla politica.

Vedere ["Selezione di una copertura dell'identificatore di dati"](#) a pagina 703.

Per utilizzare parole chiave per gli identificatori dati internazionali

- 1 Creare una politica utilizzando uno degli identificatori dati internazionali forniti dal sistema elencati nella tabella.

Vedere ["Elenco di parole chiave per gli identificatori dati di sistema internazionali"](#) a pagina 729.

- 2 Selezionare la convalida opzionale **Trova parole chiave**.

Vedere ["Configurazione della condizione Contenuto corrispondente a identificatore dati"](#) a pagina 700.

- 3 Copiare e incollare le parole chiave separate da virgola appropriate dall'elenco nel campo di convalida opzionale **Trova parole chiave**.

Vedere ["Configurazione delle convalide opzionali"](#) a pagina 720.

Elenco di parole chiave per gli identificatori dati di sistema internazionali

La [Tabella 27-22](#) fornisce parole chiave per vari identificatori dati internazionali definiti dal sistema. È possibile modificare l'identificatore dati specificato utilizzando la o le parole chiave corrispondenti.

Vedere ["Estensione e personalizzazione di identificatori di dati"](#) a pagina 693.

Vedere ["Introduzione agli identificatori di dati"](#) a pagina 681.

Vedere ["Selezione di una copertura dell'identificatore di dati"](#) a pagina 703.

Tabella 27-22 Elenco di parole chiave per gli identificatori dati PII internazionali

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di identificazione fiscale argentino	Spagnolo	Número de Identificación Fiscal, número de contribuyente, Número de identificación fiscal Argentina, Argentina número de contribuyente	Numero di identificazione fiscale, numero contribuente, numero di identificazione fiscale argentino, numero contribuente argentino
Numero di passaporto austriaco	Tedesco	REISEPASS, ÖSTERREICHISCH REISEPASS, reisepass	Passaporto, passaporto austriaco
Numero di identificazione fiscale austriaco	Tedesco	Österreich, Steuernummer	Austria, numero fiscale

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di partita IVA austriaco	Tedesco	MwSt, Umsatzsteuernummer, MwSt Nummer, Ust.-Identifikationsnummer, umsatzsteuer, Umsatzsteuer-Identifikationsnummer	IVA, numero IVA, numero di partita IVA, partita IVA, IVA, numero UID
Numero di previdenza sociale austriaco	Tedesco	sozialversicherungsnummer, soziale sicherheit kein, Versicherungsnummer, Österreichischen SSN, Österreichischen Sozialversicherungs	Numero di previdenza sociale, codice fiscale, numero di assicurazione, SSN austriaco, previdenza sociale austriaca
Numero di identificazione nazionale belga	Francese	Numéro national, numéro de sécurité, numéro d'assuré, identifiant national, identifiantnational#, Numéronational#	Numero nazionale, numero di sicurezza, numero dell'assicurato, identificazione nazionale, n. identificazione nazionale, numero nazionale
Numero di patente di guida belga	Tedesco, francese, frisone	Führerschein, Fuhrerschein, Fuehrerschein, Führerscheinnummer, Fuhrerscheinnummer, Fuehrerscheinnummer, Führerscheinnummer, Fuhrerscheinnummer, Fuehrerscheinnummer, Führerschein- Nr, Fuhrerschein- Nr, Fuehrerschein- Nr, permis de conduire, rijbewijs, Rijbewijsnummer, Numéro permis conduire	Patente, numero di patente, patente di guida, numero di patente di guida
Numero di passaporto belga	Olandese, tedesco, francese	Paspoort, paspoort, paspoortnummer, Reisepass kein, Reisepass, Passnummer, Passeport, Passeport livre, Passeport carte, numéro passeport	Passaporto, numero di passaporto, libretto passaporto, tessera passaporto
Numero di identificazione fiscale belga	Olandese, tedesco, francese	Numéro de registre national, numéro d'identification fiscale, belasting aantal, Steuernummer	Numero di registrazione nazionale, numero di identificazione fiscale, numero fiscale

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di partita IVA belga	Tedesco, francese	Numéro T.V.A, Umsatzsteuer-Identifikationsnummer, Umsatzsteuernummer	Partita IVA, numero di identificazione fiscale
Numero di conto bancario brasiliano	Portoghese (Brasile)	Itauaccountno#, número conta bancária, conta n, número conta, Conta bancária Itaú Número, código de conta bancária, Conta Sem, contan#, númeroconta#, Conta Sem	Numero di conto Itaú, numero di conto corrente, numero di conto corrente Itaú, codice di conto corrente, numero di conto
Numero di tessera elettorale brasiliana	Portoghese (Brasile)	número identificação, identificação do eleitor, ID eleitor eleição, número identificação eleitoral, Número identificação eleitoral brasileira, IDeleitoreleição#	Numero di identificazione, identificazione elettorale, numero di identificazione elettorale, numero di identificazione elettorale brasiliano,
Numero del Registro Nazionale delle Persone Giuridiche brasiliano	Portoghese (Brasile)	Brasileira ID Legal, entidades jurídicas ID, Registro Nacional de Pessoas Juridicas n °, BrasileiraIDLegal#	Identificazione legale brasiliana, identificazione delle persone giuridiche, numero del registro nazionale delle persone giuridiche
Codice fiscale per persone fisiche brasiliano	Portoghese (Brasile)	Cadastro de Pessoas Físicas, Brasileiro Pessoa Natural Número de Registro, pessoa natural número de registro, pessoas singulares registro NO	Registrazione delle persone, numero del registro delle persone fisiche brasiliano, numero di registro delle persone fisiche, numero di registrazione individuale
Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica	Francese	MSP nombre, soins de santé no, soins de santé personnels nombre, MSPNombre#, soinsdesanténo#	Numero MSP, n. MSP, numero di assistenza sanitaria personale, n. tessera sanitaria, PHN
Numero di cittadinanza univoco bulgaro (EGN)	Bulgaro	Униформ граждански номер, Униформ ID, Униформ граждански ID, Униформ граждански не., български Униформ граждански номер, УниформгражданскиID#, Униформгражданскине.#	Numero di cittadinanza univoco, identificazione univoca, identificazione di cittadinanza univoca, numero di cittadinanza univoco bulgaro

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Burgerservicenummer (BSN)	Olandese	Persoonsnummer, sofinummer, sociaal-fiscaal nummer, persoonsgebonden	numero persona, numero sociale-fiscale (abbreviazione), numero sociale-fiscale, numero associato alla persona
Numero di identificazione nazionale cileno	Spagnolo	Chilena número identificación, nacional identidad, número identificación, número identificación nacional, identidad número, Número de identificación#, Identidad chilena#, Rol Único Nacional, Rol Único Nacional#, nacional identidad#	Numero di identificazione Chileand, identità nazionale, numero di identificazione, numero di identificazione nazionale, numero di identità, ruolo nazionale unico
Numero di passaporto cinese	Cinese	中国护照, 护照, 护照本	Passaporto cinese, passaporto, libretto passaporto
Codice Fiscale	Italiano	codice fiscale, dati anagrafici, partita I.V.A., p. iva	
Indirizzi colombiani	Spagnolo	Calle, CII, Carrera, Cra, Cr, Avenida, Av, Dg, Diagonal, Diag, Tv, Trans, Transversal, vereda	Via, v., viale, corso, traversa, vicolo
Numero di cellulare colombiano	Spagnolo	numero celular, número de teléfono, teléfono celular no., numero celular#	Numero cellulare, numero di telefono, numero di telefono cellulare
Numero di identificazione personale colombiano	Spagnolo	cedula, cédula, c.c., c.c, C.C., C.C, cc, CC, NIE., NIE, nie., nie, cedula de ciudadanía, cédula de ciudadanía, cc#, CC #, documento de identificación, documento de identificación, Nit.	Carta di identità, carta di cittadinanza, documento di identificazione
Numero di identificazione fiscale colombiano	Spagnolo	NIT., NIT, nit., nit, Nit.	TIN (numero di identificazione fiscale)
Numero di identificazione nazionale croato	Croato	Osobna iskaznica, Nacionalni identifikacijski broj, osobni ID, osobni identifikacijski broj	ID personale, numero di identificazione nazionale, ID personale, numero di identificazione personale

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di identificazione personale ceco	Ceco	Česká Osobní identifikační číslo, Osobní identifikační číslo., identifikační číslo, čeština identifikační číslo	Numero di identificazione personale ceco, numero di identificazione personale, numero di identificazione ceco
Numero di identificazione personale danese	Danese	Nationalt identifikationsnummer, personnummer, unikt identifikationsnummer, identifikationsnummer, centrale personregister, cpr,cpr-nummer,cpr#, cpr-nummer#, identifikationsnummer#, personnummer#	Numero di identificazione nazionale, numero personale, numero di identificazione unico, numero di identificazione, registro centrale delle persone, numero CPR
Numero di partita IVA danese	Danese	moms, momsnummer, moms identifikationsnummer, merværdiafgift	IVA, numero partita IVA, imposta sul valore aggiunto, numero di identificazione IVA
Estone	Estone	isikukood, isikukood#	Codice di identificazione personale
Numero di patente finlandese	Finlandese e svedese	permis de conduire, ajokortti, ajokortin numero, kuljettaja lic., körkort, körkort nummer, förare lic.	Patente, numero di patente, patente di Guida.
Numero di previdenza sociale europea della Finlandia	Finlandese	Suomi EHIC-numero, Sairausvakuutuskortti, sairaanhoitokortin, Sjukförsäkringskort, ehic, sairaanhoitokortin, Suomen sairausvakuutuskortti, Finska sjukförsäkringskort, Terveyskortti, Hälsokort, ehic#, sairausvakuutusnumero, sjukförsäkring nummer	Numero EHIC della Finlandia, tessera assicurazione malattia, tessera sanitaria, EHIC, tessera sanitaria finlandese, tessera sanitaria, numero di previdenza sociale
Numero di passaporto finlandese	Finlandese	Suomen passin numero, suomalainen passi, passin numero, passin numero.#, passin numero#, passin numero, passin numero., passin numero#, passi#	Numero di passaporto finlandese, passaporto finlandese, numero di passaporto, numero di passaporto, n. passaporto
Numero di identificazione fiscale finlandese	Finlandese	verotunniste, verokortti, verotunnus, veronumero	Codice fiscale, codice di identificazione fiscale

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di partita IVA finlandese	Finlandese	arvonlisäveronumero, ALV, arvonlisäverotunniste, ALV nro, ALV numero, alv	IVA, numero partita IVA
Codice identificativo personale finlandese	Finlandese	tunnistenumero, henkilötunnus, yksilöllinen henkilökohtainen tunnistenumero, Ainutlaatuinen henkilökohtainen tunnus, identiteetti numero, Suomen kansallinen henkilötunnus, henkilötunnusnumero#, kansallisen tunnistenumero, tunnusnumero, kansallinen tunnus numero	Numero di identificazione, numero di identificazione personale, numero di identificazione personale unico, numero di identità, numero di identificazione personale finlandese, numero di identificazione nazionale
Numero di patente di guida francese	Francese	permis de conduire	Patente di guida
Numero di previdenza sociale francese	Francese	carte vitale, carte d'assuré social	Libretto sanitario, tessera di previdenza sociale
Numero di identificazione fiscale francese	Francese	numéro d'identification fiscale	Numero di identificazione fiscale
Numero di partita IVA francese	Francese	Numéro d'identification taxe sur valeur ajoutée, Numéro taxe valeur ajoutée, taxe valeur ajoutée, Taxe sur la valeur ajoutée, Numéro de TVA intracommunautaire, n° TVA, numéro de TVA, Numéro de TVA en France, français numéro de TVA, Numéro d'identification SIREN	Numero di identificazione per l'imposta sul valore aggiunto, numero per l'imposta sul valore aggiunto, imposta sul valore aggiunto, partita IVA, partita IVA francese, numero di identificazione SIREN
Codice INSEE francese	Francese	INSEE, numéro de sécu, code sécu	INSEE, numero di previdenza sociale, codice di previdenza sociale
Numero di passaporto francese	Francese	Passeport français, Passeport, Passeport livre, Passeport carte, numéro passeport	Passaporto francese, passaporto, libretto passaporto, tessera passaporto, numero di passaporto

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di previdenza sociale francese	Francese	sécurité sociale non., sécurité sociale numéro, code sécurité sociale, numéro d'assurance, sécuritésocialenon.#, sécuritésocialeNuméro#	Numero di previdenza sociale, codice di previdenza sociale, numero di assicurazione
Numero di passaporto tedesco	Tedesco	Reisepass kein, Reisepass, Deutsch Passnummer, Passnummer, Reisepasskein#, Passnummer#	Numero di passaporto, passaporto, numero di passaporto tedesco, numero di passaporto
Numero di identificazione personale tedesco	Tedesco	persönliche identifikationsnummer, ID-Nummer, Deutsch persönliche-ID-Nummer, persönliche ID Nummer, eindeutige ID-Nummer, persönliche Nummer,identität nummer, Versicherungsnummer, persönlicheNummer#, IDNummer#	Numero di identificazione personale, numero ID, numero di identificazione personale tedesco, numero di identificazione personale, numero di identificazione in chiaro, numero personale, numero di identificazione, numero di assicurazione
Numero di patente di guida tedesca	Tedesco	Führerschein, Fuhrerschein, Fuehrerschein, Führerscheinnummer, Fuhrerscheinnummer, Fuehrerscheinnummer, Führerscheinnummer, Fuhrerscheinnummer, Fuehrerscheinnummer, Führerschein- Nr, Fuhrerschein- Nr, Fuehrerschein- Nr	Patente di guida, numero di patente
Numero di partita IVA tedesca	Tedesco	Mehrwertsteuer, MwSt, Mehrwertsteuer Identifikationsnummer, Mehrwertsteuer nummer	Imposta sul valore aggiunto, numero di identificazione per l'imposta sul valore aggiunto, numero per l'imposta sul valore aggiunto
Codice fiscale della Grecia (AMKA)	Greco	Αριθμού Μητρώου Κοινωνικής Ασφάλισης	Numero di codice fiscale
Codice fiscale greco (AFM)	Greco	Αριθμός Φορολογικού Μητρώου, ΑΦΜ, Φορολογικού Μητρώου Νο., τον αριθμό φορολογικού μητρώου	Numero di identificazione fiscale, TIN, numero del registro fiscale

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
ID Hong Kong	Cinese (tradizionale)	身份證, 三顆星	Carta di identità, carta di identità di residente permanente di Hong Kong
Numero di previdenza sociale ungherese	Ungherese	Magyar társadalombiztosítási szám, Társadalombiztosítási szám, társadalombiztosítási ID, szociális biztonsági kódot, szociális biztonság nincs., társadalombiztosításID#	Numero della previdenza sociale ungherese, codice fiscale, identificazione della previdenza sociale, codice di previdenza sociale
Numero di identificazione fiscale ungherese	Ungherese	Magyar adóazonosító jel no, adóazonosító szám, magyar adószám, Magyar adóhatóság no., azonosító szám, adóazonosító no., adóhatóság no	Numero di identificazione fiscale ungherese, numero di identificazione fiscale, numero fiscale ungherese, numero dell'amministrazione fiscale ungherese, numero fiscale, numero dell'amministrazione fiscale
Numero di partita IVA ungherese	Ungherese	Közösségi adószám, Általános forgalmi adó szám, hozzáadottérték adó, magyar Közösségi adószám	Numero di identificazione per l'imposta sul valore aggiunto, numero fiscale per le vendite, imposta sul valore aggiunto, numero per l'imposta sul valore aggiunto ungherese
Numero di carta di identità indonesiana	Indonesiano, portoghese	Kartu Tanda Penduduk nomor, número do cartão, Kartu identitas Indonesia no, kartu no., Kartu identitas Indonesia nomor, Nomor Induk Kependudukan, número do cartão, kartuno., KartuidentitasIndonesiano	Numero di carta di identità, numero di carta, numero di carta di identità indonesiano, n. carta, numero di carta di identità indonesiano, numero ID
Codice International Bank Account Number (IBAN) paesi centrali	Francese	Code IBAN, numéro IBAN	Codice IBAN, numero IBAN
Codice International Bank Account Number (IBAN) paesi orientali	Francese	Code IBAN, numéro IBAN	Codice IBAN, numero IBAN
Codice International Bank Account Number (IBAN) paesi occidentali	Francese	Code IBAN, numéro IBAN	Codice IBAN, numero IBAN

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di passaporto irlandese	Irlandese	irelande passeport, Éire pas, no de passeport, pas uimh, uimhir pas, numéro de passeport	Passaporto irlandese, numero di passaporto, passaporto
Numero di identificazione fiscale irlandese	Irlandese	uimhir carthanachta, Uimhir chláraithe charthanais, uimhir CHY, CHY uimh., uimhir thagartha cánach, uimhir aitheantais cánach ireland, aitheantais cánach irish, uimhir aitheantais cánach, id cánach, uimhir chánach, cáin #, STÁIN, cáin id uimh.	Numero di beneficenza, numero di registrazione beneficenza, numero CHY, numero di riferimento fiscale, numero di identificazione fiscale irlandese, identificazione fiscale irlandese, numero di identificazione fiscale, codice fiscale, TIN, TIN Irlanda
Numero di partita IVA irlandese	Irlandese	cáin bhreisluacha, CBL, CBL aon, Uimhir CBL, Uimhir CBL hÉireann, bhreisluacha uimhir chánach	Numero di partita IVA irlandese, partita IVA, n. IVA, imposta sul valore aggiunto, numero di partita IVA irlandese
Numero personale di servizio pubblico irlandese	Gaelico	Gaeilge Uimhir Phearsanta Seirbhíse Poiblí, PPS Uimh., uimhir phearsanta seirbhíse poiblí, seirbhíse Uimh, PPS Uimh, PPS seirbhís aon	Numero personale di servizio pubblico irlandese, n. PPS, numero personale di servizio pubblico, n. di servizio, numer PPS, numero servizio PPS
Numero di identificazione personale israeliano	Ebraico, arabo	מספר זיהוי, מספר זיהוי ישראל, זהות ישראלית, هوية اسرائيلية عدد, هوية اسرائيلية, رقم الهوية, عدد هوية فريدة من نوعها	Numero di identificazione israeliano, numero di identificazione, numero di identificazione unico, ID personale, ID personale unico, ID unico
Numero di patente di guida italiana	Italiano	patente guida numero, patente di guida numero, patente di guida, patente guida	Patente di guida, numero di patente
Numero di previdenza sociale italiano	Italiano	TESSERA SANITARIA, tessera sanitaria, tessera sanitaria italiana	Tessera sanitaria, tessera sanitaria italiana
Numero di passaporto italiano	Italiano	Repubblica Italiana Passaporto, Passaporto, Passaporto Italiana, passport number, Italiana Passaporto numero, Passaporto numero, Numéro passeport italien, numéro passeport	Passaporto della repubblica italiana, passaporto, passaporto italiano, numero di passaporto italiano, numero del passaporto

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di partita IVA italiano	Italiano	IVA, numero partita IVA, IVA#, numero IVA	IVA, numero partita IVA, n. IVA, numero IVA
Numero di patente di guida giapponese	Giapponese	公安委員会, 番号, 免許, 交付, 運転免許, 運転免許証, ドライバライセンス, ドライバーズライセンス, ライセンス, 運転免許証番号	Comitato di pubblica sicurezza, patente, patente di guida, numero di patente, n. patente di guida, numero patente, permesso di guida
Numero di identificazione giapponese (Juki Net)	Giapponese	住基ネット識別番号, 住基ネット番号, 識別番号, 個人識別番号	Numero di identificazione Juki-Net, numero Juki-Net, numero di identificazione, numero di identificazione personale
Numero di identificazione personale giapponese - Aziendale	Giapponese	マイナンバー, 共通番号	My number, numero comune
Numero di identificazione personale giapponese - Personale	Giapponese	マイナンバー, 個人番号, 共通番号	My number, numero personale, numero comune
Numero di passaporto giapponese	Giapponese	日本国旅券, パスポート, パスポート数	Passaporto giapponese, passaporto, numero di passaporto
Numero di passaporto coreano	Coreano	한국어 여권, 여권, 여권 번호, 대한민국	Passaporto coreano, passaporto, numero di passaporto, Repubblica Coreana
Numero di registrazione anagrafica coreano per stranieri	Coreano	외국인 등록 번호, 주민번호	Numero di registrazione per stranieri, codice fiscale
Numero di registrazione anagrafica coreano per coreani	Coreano	주민등록번호, 주민번호	Numero di registrazione anagrafica, codice fiscale
Numero di identificazione personale lettone	Lettone	Personas kods, personas kods, latvijas personas kods, Valsts identifikācijas numurs, valsts identifikācijas numurs, identifikācijas numurs, nacionālais id, latvija alva, alva, nodokļu identifikācijas numurs, nodokļu id, alvas nē, nodokļa numurs	Codice personale della Lettonia, codice personale, numero di identificazione nazionale, numero di identificazione, ID nazionale, della Lettonia TIN, TIN, codice fiscale numero, ID fiscale, TIN numero di identificazione, numero fiscale

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di identificazione lussemburghese	Tedesco, francese	Eindeutige ID-Nummer, Eindeutige ID, ID personelle, Numéro d'identification personnel, IDpersonnelle#, Persönliche Identifikationsnummer, EindeutigeID#	Numero di identificazione univoco, identificazione univoca, identificazione personale, numero di identificazione personale
Numero di passaporto lussemburghese	Francese e tedesco	passnummer, ausweisnummer, passeport, reiseepass, pass, pass net, pass nr, no de passeport, passeport nombre, numéro de passeport	Numero di passaporto, passaporto, pass Lussemburgo, passaporto lussemburghese
Numero di identificazione fiscale lussemburghese	Francese e tedesco	Zinn, Zinn Nummer, Luxembourg Tax Identifikatiounsnummer, Steier Nummer, Steier ID, Sozialversicherungsausweis, Zinnzahl, Zinn nein, Zinn#, luxemburgische steueridentifikationsnummer, Steuernummer, Steuer ID, sécurité sociale, carte de sécurité sociale, étain, numéro d'étain, étain non, étain#, Numéro d'identification fiscal luxembourgeois, numéro d'identification fiscale	TIN, numero TIN, numero di identificazione fiscale lussemburghese, codice fiscale, numero di previdenza sociale, numero di identificazione fiscale del Lussemburgo, previdenza sociale
Numero di partita IVA lussemburghese	Tedesco e lussemburghese	TVA kee, TVA#, TVA Aschreiwung kee, T.V.A, stammnummer, bleiwen, geheesch, gitt id, mehrwertsteuer, vat registrierungsnummer, umsatzsteuer-id, wat, umsatzsteuernummer, umsatzsteuer-identifikationsnummer, id de la batterie, lëtzebuerg vat nee, registréierung nummer, numéro de TVA, numéro de enregistrement vat	Numero di partita IVA lussemburghese, numero di partita IVA, IVA, imposta sul valore aggiunto, partita IVA, registrazione IVA

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di carta di identità malese (MyKad)	Malese	nombor kad pengenalan, kad pengenalan no, kad pengenalan Malaysia, bilangan identiti unik, nombor peribadi, nomborperibadi#, kadpengenalanno#	Numero di carta di identità, n. carta di identità, carta di identità malese, numero di identificazione univoco, numero personale
Numero di registrazione e identificazione personale messicano	Spagnolo	Clave de Registro de Identidad Personal, Código de Identificación Personal mexicana, número de identificación personal mexicana	Chiave di registrazione dell'identità personale, codice di identificazione personale messicano, numero di identificazione personale messicano
Numero di identificazione fiscale messicano	Spagnolo	Registro Federal de Contribuyentes, número de identificación de impuestos, Código del Registro Federal de Contribuyentes, Número RFC, Clave del RFC	Registro federale dei contribuenti, numero di identificazione fiscale, numero del registro federale dei contribuenti, numero RFC, chiave RFC
Codice di identificazione personale messicano	Spagnolo	Única de registro de Población, clave única, clave única de identidad, clave personal Identidad, personal Identidad Clave, ClaveÚnica#, clavepersonalIdentidad#	Registro di identificazione univoca, chiave univoca, chiave di identità univoca, identità personale univoca, chiave di identità personale
Numero di conto bancario esteso messicano (CLABE)	Spagnolo	Clave Bancaria Estandarizada, Estandarizado Banco número de clave, número de clave, clave número, clave#	Codice bancario standardizzato, numero di codice bancario standardizzato, numero di codice
Numero di patente di guida dei Paesi Bassi	Olandese	RIJMEWIJS, permis de conduire, rijbewijs, Rijbewijsnummer, RIJBEWIJSNUMMER	Patente di guida, patente, numero di patente
Numero di passaporto dei Paesi Bassi	Olandese	Nederlanden paspoort nummer, Paspoort, paspoort, Nederlanden paspoortnummer, paspoortnummer	Numero di passaporto dei Paesi Bassi, passaporto, numero di passaporto

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di identificazione fiscale dei Paesi Bassi	Olandese, papiamento, norvegese	Nederlands belasting identificatienummer, identificatienummer van belasting, Nederlands belasting identificatie, Nederlands belasting id nummer, Nederlands belastingnummer, btw nummer, Nederlandse belasting identificatie, Nederlands belastingnummer, netherlands tax identification tal, netherlands tax identification tal, tax identification tal, tax tal, Nederl�nske tax identification tal, Holl�nske tax identification, Nederl�nsk tax tal, Holl�nske tax id tal, netherlands impuesto identification number, netherlands impuesto identification number, impuesto identification number, impuesto number, hulandes impuesto identification number, hulandes impuesto identification, hulandes impuesto number, hulandes impuesto id number	Numero di identificazione fiscale dei Paesi Bassi, numero di identificazione fiscale, identificazione fiscale dei Paesi Bassi, numero fiscale dei Paesi Bassi, numero fiscale
Numero di partita IVA dei Paesi Bassi	Olandese, frisona	wearde tafoege tax getal, BTW n�mer, BTW-nummer	Numero per l'imposta sul valore aggiunto, partita IVA
Numero di identificazione personale norvegese	Norvegese	f�dsel nummer, F�dsel nr, f�dsel nei, f�dselnei#, f�dselnummer#	Numero di identificazione personale
Documento di identit� cinese	Cinese (semplificato)	身份证,居民信息,居民身份信息	Carta di identit�, Informazioni del residente, Informazioni di identificazione residente
Numero di previdenza sociale europea della Polonia	Polacco	Karta Ubezpieczenia Zdrowotnego, Europejska Karta Ubezpieczenia Zdrowotnego, numer ubezpieczenia zdrowotnego, numer rachunku medycznego, numer rachunku medycznego	codice fiscale Polonia, numero di previdenza sociale, tessera sanitaria, numero carta di previdenza sociale europea, codice fiscale

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di identificazione polacco	Polacco	owód osobisty, Tożsamości narodowej, osobisty numer identyfikacyjny, niepowtarzalny numer, numer	Carta di identità, identità nazionale, numero di carta di identità, numero unico, numero
Codice statistico polacco (REGON)	Polacco	numer statystyczny, REGON, numeru REGON, numerstatystyczny#, numeruREGON#	Codice statistico, numero REGON
Codice fiscale polacco (PESEL)	Polacco	PESEL Liczba, społeczny bezpieczeństwo liczba, społeczny bezpieczeństwo ID, społeczny bezpieczeństwo kod, PESELliczba#, społecznybezpieczeństwoliczba#	Numero PESEL, codice fiscale, identificazione della previdenza sociale, codice di previdenza sociale
Numero di identificazione fiscale polacco	Polacco	Numer Identyfikacji Podatkowej, Polski numer identyfikacji podatkowej, NumerIdentyfikacjiPodatkowej#	Numero di identificazione fiscale, numero di identificazione fiscale polacco
Numero di patente di guida portoghese	Portoghese	carteira de motorista, carteira motorista, carteira de habilitação, carteira habilitação, número de licença, número licença, permissão de condução, permissão condução, Licença condução Portugal, carta de condução	patente, numero di patente, patente di guida portoghese
Numero di identificazione nazionale portoghese	Portoghese	bilhete de identidade, número de identificação civil, número de cartão de cidadão, documento de identificação, cartão de cidadão, número bi de portugal, número do documento	carta di identità, numero di identificazione di cittadinanza univoco, numero di carta del cittadino, documento di identificazione, carta del cittadino, numero di documento
Numero di passaporto portoghese	Francese e portoghese	passaporte, passeport, portuguese passport, portuguese passeport, portuguese passaporte, passaporte nº, passeport nº	Numero di passaporto, passaporto, passaporto portoghese
Numero di identificazione fiscale portoghese	Portoghese	número identificação fiscal	Numero di identificazione fiscale

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di partita IVA portoghese	Portoghese	imposto sobre valor acrescentado, VAT n°, número iva, vat não, código iva	Imposta sul valore aggiunto, partita IVA, IVA, codice IVA
Numero di identificazione nazionale rumeno	Rumeno	numărul de identificare fiscală, identificarea fiscală nr #, codul fiscal nr.	numero di identificazione fiscale, numero di codice fiscale
Numero di identificazione personale rumeno	Rumeno	Cod Numeric Personal, cod identificare personal, cod unic identificare, număr personal unic, număr identitate, număr identificare personal, număridentitate#, CodNumericPersonal#, numărpersonalunic#	Codice numerico personale, codice di identificazione personale, codice di identificazione unico, numero di identificazione, numero di identificazione personale
Numero di identificazione del passaporto russo	Russo	паспорт нет, паспорт, номер паспорта, паспорт ID, Российской паспорт, Русский номер паспорта, паспорт#, паспортID#, номерпаспорта#	N. di passaporto, passaporto, numero di passaporto, identificazione passaporto, passaporto russo, numero di passaporto russo
Numero di identificazione fiscale russo	Russo	НДС, номер налогоплательщика, Налогоплательщика ИД, налог число, налогчисло#, ИНН#, НДС#	TIN (numero di identificazione fiscale), numero del contribuente, identificazione del contribuente, codice fiscale
Numero di identificazione nazionale slovacco	Ungherese e slovacco	identifikačné číslo, személyi igazolvány száma, személyigazolvány szám, číslo občianskeho preukazu, identifikačná karta č, személyi igazolvány szám, nemzeti személyi igazolvány száma, číslo národnej identifikačnej karty, národná identifikačná karta č, nemzeti személyazonosító igazolvány, nemzeti azonosító szám, národné identifikačné číslo, národná identifikačná značka č, nemzeti azonosító szám, azonosító szám, identifikačné číslo	numero id, numero di carta di identità, numero di carta di identità nazionale, n. carta di identità nazionale, numero di identificazione nazionale, n. di identificazione nazionale, numero di identificazione, n. identificazione

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero identificativo cittadini della Slovenia	Sloveno	EMŠO, emšo, edinstvena številka državljana, enotna identifikacijska številka, Enotna maticna številka obcana, enotna maticna številka obcana, številka državljana, edinstvena identifikacijska številka	Numero di identificazione univoco nazionale, numero di identificazione univoco, numero di registrazione univoco, numero del cittadino
Numero di identificazione personale sudafricano	Afrikaans	nasionale identifikasie nommer, nasionale identiteitsnommer, versekering aantal, persoonlike identiteitsnommer, unieke identiteitsnommer, identiteitsnommer#, identiteitsnommer#, versekeringaantal#, nasionaleidentiteitsnommer#	Numero di identificazione nazionale, numero di identità nazionale, numero di assicurazione, numero di identità personale, numero di identificazione unico, numero di identità
Resident Registration Number (RRN, numero di registrazione anagrafica) sudcoreano	Coreano	주민등록번호, 주민번호	Numero di registrazione residente, numero residente
Numero di patente di guida spagnola	Spagnolo	permiso de conducción, permiso conducción, Número licencia conducir, Número de carnet de conducir, Número carnet conducir, licencia conducir, Número de permiso de conducir, Número de permiso conducir, Número permiso conducir, permiso conducir, licencia de manejo, el carnet de conducir, carnet conducir	Patente, numero di patente, patente di guida, patente guida, numero di patente di guida
Numero di partita IVA spagnolo	Spagnolo	Número IVA España, Número de IVA español, español Número IVA, Número de valor agregado, IVA, Número IVA, Número impuesto sobre valor añadido, Impuesto valor agregado, Impuesto sobre valor añadido, valor añadido el impuesto, valor añadido el impuesto numero	Numero IVA spagnolo, numero IVA Spagna, numero Iva, n. IVA, IVA, numero imposta valore aggiunto, imposta valore aggiunto

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di conto cliente spagnolo	Spagnolo	número cuenta cliente, código cuenta, cuenta cliente ID, número cuenta bancaria cliente, código cuenta bancaria	Numero di conto cliente, codice di conto, identificazione del conto cliente, numero di conto corrente del cliente, codice di conto corrente
Numero di DNI spagnolo	Spagnolo	NIE número, Documento Nacional de Identidad, Identidad único, Número nacional identidad, DNI Número	Numero NIE, documento di identità nazionale, identità univoca, numero di identità nazionale, numero DNI
Numero di passaporto spagnolo	Spagnolo	libreta pasaporte, número pasaporte, Número Pasaporte, España pasaporte, pasaporte	libretto passaporto, numero di passaporto, passaporto spagnolo, passaporto
Numero di previdenza sociale spagnolo	Spagnolo	Número de la Seguridad Social, número de la seguridad social	Numero di codice fiscale
Codice di identificazione fiscale spagnolo (CIF)	Spagnolo	número de contribuyente, número de impuesto corporativo, número de Identificación fiscal, CIF número, CIFnúmero#	numero del contribuente, numero fiscale delle imprese, numero di identificazione fiscale, numero CIF
Numero di patente svedese	Finlandese, rumeno, svedese, yiddish	ajokortti, permis de conduire, ajokortin numero, kuljettajat lic., drivere lic., körkort, numărul permisului de conduce, שא פער דערלויבעניש, נומער, körkort nummer, förare lic., דריווערס דערלויבעניש, körkortsnummer	Patente, numero di patente, numero di patente di guida
Numero di identificazione fiscale svedese	Svedese	skattebetalarens identifikationsnummer, Sverige TIN, TIN-nummer	Numero identificazione fiscale, TIN svedese, codice fiscale
Numero di partita IVA svedese	Svedese	moms#, sverige moms, sverige momsnummer, sverige moms nr, sweden vat nummer, sweden momsnummer, momsregistreringsnummer	Partita IVA svedese, numero di partita IVA svedese, numero di partita IVA
Numero di passaporto svedese	Svedese	Passnummer, pass, sverige pass, SVERIGE PASS, sverige Passnummer	Numero di passaporto, passaporto, passaporto svedese, numero di passaporto svedese

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di identificazione personale svedese	Svedese	personnummer ID, personligt id-nummer, unikt id-nummer, personnummer, identifikationsnumret, personnummer#, identifikationsnumret#	Numero di identificazione, numero di identificazione personale, numero di identificazione univoco, personale, numero di identificazione
Numero AHV svizzero	Francese	Numéro AVS, numéro d'assuré, identifiant national, numéro d'assurance vieillesse, numéro de sécurité sociale, Numéro AVH	Numero AVS, numero di assicurazione, identificatore nazionale, numero di previdenza sociale, numero della previdenza sociale, numero AVH
	Tedesco	AHV-Nummer, Matrikelnumme, Personenidentifikationsnummer	Numero AHV, numero di matricola svizzero, PIN
	Italiano	AVS, AVH	AVS, AVH
ID ROC di Taiwan	Cinese (tradizionale)	中華民國國民身分證	ID Taiwan
Numero di identificazione personale thailandese	Tailandese	ประกันภัยจำนวน, หมายเลขประจำตัวส่วนบุคคล, หมายเลขประจำตัวที่ไม่ซ้ำกัน, ประกันภัยจำนวน#, หมายเลขประจำตัวส่วนบุคคล#, หมายเลขประจำตัวที่ไม่ซ้ำกัน#	Numero di assicurazione, identificazione personale, numero di identificazione
Numero di identificazione turco	Turco	Kimlik Numarası, Türkiye Cumhuriyeti Kimlik Numarası, vatandaş kimliği, kişisel kimlik no, kimlik Numarası#, vatandaş kimlik numarası, Kişisel kimlik Numarası	Numero di identificazione, numero di identificazione della Repubblica Turca, identificazione del cittadino, numero di identificazione personale, numero di identificazione del cittadino
Carta di identità ucraina	Ucraino	посвідчення особи України	Carta di identità ucraina
Numero di passaporto ucraino (interno)	Ucraino	паспорт, паспорт України, номер паспорта, персональний	Passaporto, passaporto ucraino, numero di passaporto
Numero di passaporto ucraino (internazionale)	Ucraino	паспорт, паспорт України, номер паспорта	Passaporto, passaporto ucraino, numero di passaporto
Numero di identificazione personale degli Emirati Arabi Uniti	Arabo	الهوية الشخصية رقم, رقم التعريف الشخصي, فريدة من نوعها هوية رقم, التأمين رقم, التأمير رقم, هوية فريدة#	Numero ID personale, PIN, numero ID univoco, numero di assicurazione, n. identità univoco

Identificatore dati	Lingua	Parole chiave	Traduzione in italiano
Numero di identificazione nazionale venezuelano	Spagnolo	cédula de identidad número, clave única de identidad, personal de identidad clave, personal de identidad, número de identificación nacional, número ID nacional	Numero di ID nazionale, numero di identificazione nazionale, numero di ID personale, identificazione personale, numero di identificazione univoco

Aggiornamento delle politiche per l'utilizzo dell'identificatore dati Social Security Number (SSN) statunitense randomizzato

L'identificatore dati Social Security Number (SSN) statunitense randomizzato rileva i numeri di previdenza sociale tradizionali e randomizzati.

Vedere ["Utilizzo dell'identificatore dati Social Security Number \(SSN\) statunitense randomizzato per rilevare i numeri di previdenza sociale"](#) a pagina 769.

Tutti i modelli di politica che in precedenza utilizzavano l'identificatore dati Social Security Number (SSN) statunitense per rilevare il numero di previdenza sociale sono ora aggiornati all'utilizzo dell'identificatore dati Social Security Number (SSN) statunitense randomizzato. Inoltre l'identificatore dati Social Security Number (SSN) statunitense randomizzato è aggiornato per Symantec Data Loss Prevention versione 14.0.

Vedere ["Aggiornamento delle politiche dopo l'upgrade alla versione più recente"](#) a pagina 459.

Se sono presenti politiche esistenti che utilizzano l'identificatore dati Social Security Number (SSN) statunitense, è consigliabile aggiornare ciascuna politica in modo che utilizzi l'identificatore dati Social Security Number (SSN) statunitense randomizzato. Se sono state create politiche con l'identificatore dati Social Security Number (SSN) statunitense randomizzato versione 12.5, è consigliabile aggiornare ciascuna politica in modo che utilizzi l'identificatore dati Social Security Number (SSN) statunitense randomizzato versione 14.0.

La sezione [Per aggiornare una politica all'utilizzo dell'identificatore dati Social Security Number \(SSN\) statunitense randomizzato](#) illustra la procedura per l'aggiornamento delle politiche del numero di previdenza sociale.

Per aggiornare una politica all'utilizzo dell'identificatore dati Social Security Number (SSN) statunitense randomizzato

- 1 Modificare la politica che implementa l'identificatore dati Social Security Number (SSN) statunitense o l'identificatore dati Social Security Number (SSN) statunitense randomizzato 12.5.
Vedere ["Configurazione di politiche"](#) a pagina 422.
- 2 Modificare la regola che contiene l'identificatore dati Social Security Number (SSN) statunitense.
Vedere ["Configurazione di regole di politica"](#) a pagina 427.
- 3 Rimuovere l'identificatore dati Social Security Number (SSN) statunitense.
- 4 Aggiungere l'identificatore dati Social Security Number (SSN) statunitense randomizzato.
Vedere ["Gestione e aggiunta degli identificatori dati"](#) a pagina 698.
- 5 Salvare la politica.
- 6 Verificare il rilevamento della politica per i Social Security Number (SSN) statunitensi sia tradizionali che randomizzati.
Vedere ["Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze"](#) a pagina 466.
- 7 Distribuire la politica del numero di previdenza sociale (SSN) aggiornata alla produzione.
Vedere ["Distribuzione di politiche"](#) a pagina 378.

Creazione di identificatori dati personalizzati

È possibile creare e cancellare uno o più identificatori dati personalizzati. Un identificatore dati personalizzato può essere un identificatore dati di sistema clonato da modificare o un identificatore creato da zero. Un identificatore dati personalizzato è riutilizzabile in più politiche. Le modifiche apportate a un identificatore dati personalizzato a livello di sistema hanno effetto su tutte le politiche che dichiarano attivamente o in un secondo momento l'identificatore dati personalizzato.

La [Tabella 27-23](#) elenca i componenti degli identificatori dati personalizzati.

Vedere ["Flusso di lavoro per la creazione di identificatori di dati personalizzati"](#) a pagina 749.

Tabella 27-23 Componenti dell'identificatore dati personalizzato

Componente	Descrizione
Modelli	Definire uno o più modelli di espressione regolare, separati da interruzioni di riga. Vedere "Informazioni sui criteri dell'identificatore dati" a pagina 695.

Componente	Descrizione
Convalide	Aggiungere o rimuovere convalide per eseguire controlli di convalida sui dati individuati dal o dai modelli. Vedere " Informazioni sulle convalide criterio " a pagina 696.
Immissione dati	Fornire valori di dati separati da virgole per tutti le convalide che richiedono l'immissione di dati. Vedere " Informazioni sulle convalide criterio " a pagina 696.
Normalizzatore	Selezionare un normalizzatore per standardizzare i dati prima della corrispondenza. Vedere " Selezione di un normalizzatore di dati " a pagina 764.

Flusso di lavoro per la creazione di identificatori di dati personalizzati

È possibile implementare identificatori di dati personalizzati per rilevare contenuto univoco. Per implementare un identificatore di dati personalizzato, è necessario definire almeno un criterio e selezionare un normalizzatore di dati. Le convalide sono facoltative.

Vedere "[Configurazione degli identificatori dati personalizzati](#)" a pagina 751.

Per impostazione predefinita, il sistema assegna un identificatore di dati personalizzato alla copertura Ampia. Ciò non è tuttavia una limitazione, in quanto l'ambito di rilevamento effettivo viene determinato dai criteri e dalle convalide definite.

Tabella 27-24 Implementazione di identificatori di dati personalizzati

Passaggio	Azione	Descrizione
1	Selezionare Gestisci > Politiche > Identificatore dati .	La schermata Identificatore dati elenca tutti gli identificatori di dati disponibili nel sistema.
2	Selezionare Aggiungi identificatore dati .	Immettere un nome per l'identificatore di dati personalizzato. Il nome deve essere univoco. Immettere una descrizione per l'identificatore di dati personalizzato. Per impostazione predefinita, un identificatore di dati personalizzato è assegnato alla categoria Personalizzato . Questa impostazione non può essere modificata. Il campo Descrizione non può includere più di 255 caratteri per riga.

Passaggio	Azione	Descrizione
3	Immettere uno o più criteri per la corrispondenza dei dati.	<p>È necessario immettere almeno un criterio affinché l'identificatore di dati personalizzato sia valido.</p> <p>Separare molteplici criteri con interruzioni di riga.</p> <p>Vedere "Creazione di criteri di identificatore di dati per la corrispondenza con i dati" a pagina 755.</p>
4	Selezionare un normalizzatore di dati .	<p>È necessario selezionare un normalizzatore di dati.</p> <p>Vedere "Selezione di un normalizzatore di dati" a pagina 764.</p> <p>I seguenti normalizzatori sono disponibili:</p> <ul style="list-style-type: none"> ■ Cifre ■ Cifre e lettere ■ Minuscolo ■ Codici Swift ■ Non intervenire <p>Selezionare questa opzione se non si desidera normalizzare i dati.</p>
5	Selezionare zero o più convalide .	<p>L'inclusione di una convalida per controllare e verificare la corrispondenza con il criterio è facoltativa.</p> <p>Vedere "Selezione di convalide dei criteri" a pagina 763.</p>
6	Salvare l'identificatore di dati personalizzato.	<p>Fare clic su Salva nella parte superiore della schermata.</p> <p>Dopo aver definito e salvato un identificatore di dati personalizzato, questo compare ordinato alfabeticamente nell'elenco degli identificatori di dati nella schermata Identificatore dati.</p> <p>Per modificare un identificatore di dati personalizzato, selezionarlo dall'elenco.</p> <p>Vedere "Modifica degli identificatori dati" a pagina 699.</p> <p>Nota: Fare clic su Annulla per non salvare l'identificatore di dati personalizzato.</p>
7	Implementare l'identificatore di dati personalizzato in una o più politiche.	<p>Il sistema elenca tutti gli identificatori di dati personalizzati nella categoria Personalizzato per la condizione "Contenuto corrispondente a identificatore dati" nelle schermate Configura politica - Aggiungi regola e Configura politica - Aggiungi eccezione.</p> <p>Vedere "Configurazione della condizione Contenuto corrispondente a identificatore dati" a pagina 700.</p> <p>Per gli identificatori di dati personalizzati, è possibile configurare convalide opzionali a livello di istanza di politica.</p> <p>Vedere "Configurazione delle convalide opzionali" a pagina 720.</p>

Configurazione degli identificatori dati personalizzati

È possibile creare ed eliminare uno o più identificatori dati personalizzati. Un identificatore dati personalizzato può essere utilizzato in più politiche. Le modifiche apportate a un identificatore dati personalizzato al livello del sistema hanno effetto su tutte le politiche che dichiarano attivamente o in un secondo momento l'identificatore dati personalizzato.

Vedere ["Flusso di lavoro per la creazione di identificatori di dati personalizzati"](#) a pagina 749.

Tabella 27-25 Configurazione degli identificatori dati personalizzati

Configurabile a livello personalizzato	Non configurabile
<ul style="list-style-type: none"> ■ Nome e Descrizione È necessario assegnare un nome univoco a un identificatore dati personalizzato. È buona pratica fornire una descrizione per l'identificatore dati personalizzato. È possibile modificare il nome o la descrizione di un identificatore dati personalizzato quando lo si modifica. ■ Criteri È necessario definire almeno un criterio affinché l'identificatore dati personalizzato sia valido. ■ Convalide attive È possibile aggiungere una o più convalide obbligatorie a un identificatore dati personalizzato. ■ Immissione dati È possibile modificare l'input di una convalida attiva che accetta l'immissione dei dati. ■ Normalizzatore di dati È necessario selezionare un normalizzatore di dati quando si definisce un identificatore dati personalizzato. 	<ul style="list-style-type: none"> ■ Categoria Il sistema assegna un identificatore dati personalizzato alla categoria Personalizzato. Non è possibile modificare questa impostazione. ■ Copertura Il sistema assegna un identificatore dati personalizzato alla copertura della regola Ampia. Non è possibile modificare questa impostazione. ■ Convalide opzionali Gli identificatori dati personalizzati supportano tutte le convalide opzionali, ma sono configurati al livello di istanza di politica.

Utilizzo della lingua dei criteri degli identificatori dati

La lingua dei criteri dell'identificatore dati è un sottoinsieme limitato del lessico delle espressioni regolari. La lingua dei criteri degli identificatori dati non supporta tutti i caratteri e i costrutti delle espressioni regolari. Un criterio di un'espressione regolare convertito in un criterio di un identificatore dati richiede alcune modifiche sintattiche.

I criteri degli identificatori dati sono limitati a 100 caratteri per riga. Il criterio stesso non può contenere più di 100 caratteri, ma una riga non può eccedere i 100 caratteri. È necessario suddividere il criterio in righe lunghe non più di 100 caratteri.

Vedere ["Limiti di immissione caratteri per la configurazione di politiche"](#) a pagina 442.

La [Tabella 27-26](#) elenca le differenze note tra le espressioni regolari e la lingua dei criteri degli identificatori dati. Per informazioni più dettagliate sulla lingua dei criteri degli identificatori dati, vedere [Specifica lingua criterio identificatore dati](#).

Tabella 27-26 Limitazioni della lingua dei criteri degli identificatori dati

Carattere	Descrizione
* .	I caratteri asterisco (*), barra verticale () e punto (.) non sono supportati per i criteri degli identificatori dati.
\w	Il costrutto \w non può essere utilizzato per cercare la corrispondenza con il carattere di sottolineatura (_).
\s	Il costrutto \s non può essere utilizzato per cercare la corrispondenza con un carattere di spazio vuoto. Utilizzare invece uno spazio vuoto effettivo.
\d	Per le cifre utilizzare il costrutto \d.
Raggruppamento	<p>Il raggruppamento funziona solo all'inizio del criterio. Ad esempio:</p> <p>\d{4} - 2049 non funziona; utilizzare invece 2049 - \d{4}</p> <p>\d{2} /19 \d{2} non funziona; utilizzare invece \d{2} /[1][9] \d{2}</p> <p>I raggruppamenti sono consentiti all'inizio del criterio, ad esempio nell'identificatore dati di una carta di credito.</p>

Specifica lingua criterio identificatore dati

È possibile utilizzare tre tipi di token durante la definizione di un criterio identificatore dati. I token sono sequenze di caratteri diversi dallo spazio all'inizio del file o preceduti da uno o più caratteri diversi dallo spazio, seguiti da caratteri diversi dallo spazio o dal termine del file. I tre tipi di token utilizzati nei criteri identificatori dati sono:

- Rappresentazioni formali di caratteri
- Espressioni parentesi quadre
- Caratteri speciali

È possibile seguire ogni token da un quantificatore opzionale.

Vedere [la sezione chiamata "Quantificatori"](#) a pagina 754.

I criteri identificatori dati corrispondono solo a un token completo o a un set di token.

Rappresentazioni formali di caratteri, metacaratteri e caratteri speciali

La maggior parte dei caratteri sono rappresentazioni formali nella lingua del criterio identificatore dati. Ad esempio, il carattere `a` nel criterio identificatore dati corrisponde al carattere `a` nel contenuto. La lingua del criterio identificatore dati include quattro metacaratteri. Per far corrispondere questi metacaratteri come rappresentazioni formali, utilizzare la barra rovesciata per assegnare il carattere escape ai caratteri nel criterio identificatore dati. Consultare [Tabella 27-27](#) per descrizioni di tali metacaratteri.

Tabella 27-27 Metacaratteri

Carattere	Descrizione
[Questo carattere è utilizzato per iniziare un'espressione barra rovesciata.
{	Questo carattere è utilizzato per quantificare il token precedente.
?	Questo carattere è utilizzato per quantificare il token precedente.
\	Questo carattere è utilizzato per assegnare il carattere escape al seguente carattere.

Questa lingua del criterio identificatore dati include cinque caratteri speciali predefiniti. Consultare [Tabella 27-28](#) per descrizioni di tali caratteri speciali.

Tabella 27-28 Caratteri speciali

Carattere	Descrizione
\l	Questo carattere speciale corrisponde a qualsiasi lettera ASCII.
\L	Questo carattere speciale corrisponde a qualsiasi lettera non ASCII, compresi i caratteri Unicode.
\d	Questo carattere corrisponde a qualsiasi cifra ASCII.
\D	Questo carattere speciale corrisponde a qualsiasi cifra non ASCII, compresi i caratteri Unicode.
\w	Questo carattere speciale corrisponde a qualsiasi carattere senza corrispondenza con <code>\l</code> o <code>\d</code> , compresi caratteri Unicode.

Espressioni parentesi quadre

Le espressioni parentesi quadre iniziano con `[` e terminano con `]` e contengono almeno un carattere all'interno del corpo dell'espressione. Ad esempio, l'espressione parentesi quadre `[abcd]` corrisponde a qualsiasi lettera "a", "b", "c" o "d".

È possibile includere un intervallo di caratteri all'interno di un'espressione parentesi quadre separando due caratteri con un trattino: -. Ad esempio, l'espressione parentesi quadre [a-z] corrisponde alle lettere minuscole da "a" a "z". Due caratteri separati da - sono interpretati come un intervallo. Gli ordini relativi dell'intervallo non sono importanti: [a-z] e [z-a] corrispondono agli stessi caratteri.

È possibile includere i caratteri "]" e "-" nell'espressione parentesi quadre se vengono seguite queste regole:

- Il carattere "]" deve essere visualizzato come primo carattere nell'espressione parentesi quadre. Ad esempio: []a-z] corrisponde al carattere "]" o a qualsiasi carattere minuscolo tra "a" e "z."
- Il carattere "-" deve essere visualizzato come primo o ultimo carattere nell'espressione parentesi quadre. Se l'espressione parentesi quadre contiene entrambi i caratteri "]" e "-", "]" deve essere il primo carattere e "-" l'ultimo carattere. Ad esempio: [] -] corrisponde a "]" o "-."

Ordine di interpretazione

I criteri di identificatore dati sono interpretati da sinistra a destra. Ad esempio, l'espressione parentesi quadre [a-d-z] è interpretata come intervallo a-d e quindi come rappresentazioni formali - e z.

Quantificatori

È possibile far seguire qualsiasi token nel criterio identificatore dati con un quantificatore. Il quantificatore specifica quante occorrenze del criterio far corrispondere. Consultare [Tabella 27-29](#) per una descrizione di quantificatori disponibili nella lingua criterio identificatore dati.

Tabella 27-29 Quantificatori

Quantificatore	Descrizione
?	Questo quantificatore specifica che l'espressione dovrebbe corrispondere a zero o a un'occorrenza del token precedente.
{n}	Questo quantificatore specifica che l'espressione dovrebbe corrispondere esattamente a n occorrenze del token precedente.
{n, m}	Questo quantificatore specifica che l'espressione dovrebbe corrispondere a n e m occorrenze del token precedente (incluso).

Creazione di criteri di identificatore di dati per la corrispondenza con i dati

Se si modifica un identificatore di dati esistente, è possibile modificarne i criteri. Se si crea un identificatore di dati personalizzato, è necessario implementare almeno un criterio. I criteri di identificatore di dati vengono implementati con una sintassi simile al linguaggio delle espressioni regolari, con alcune limitazioni. Inoltre, il sistema consente solo l'uso dei caratteri ASCII per i criteri di identificatore di dati.

Vedere ["Informazioni sui criteri dell'identificatore dati"](#) a pagina 695.

Per modificare o implementare un criterio

- 1 Esaminare i criteri per l'identificatore di dati da modificare.
Vedere ["Selezione di una copertura dell'identificatore di dati"](#) a pagina 703.
- 2 Considerare la possibilità di clonare l'identificatore di dati, se si sta modificando un identificatore di dati del sistema.
Vedere ["Clonazione di un identificatore dati di sistema prima della sua modifica "](#) a pagina 726.
- 3 Selezionare **Gestisci > Politiche > Identificatore dati** nella console di amministrazione di Enforce Server.
- 4 Selezionare l'identificatore di dati da modificare.
- 5 Selezionare la copertura per l'identificatore di dati da modificare.
Generalmente, i criteri variano da una copertura all'altra.
- 6 Nel campo **Criteri**, modificare un criterio esistente o immettere uno o più nuovi criteri, separati da interruzioni di riga.
I criteri di identificatore di dati sono implementati come espressioni regolari. Tuttavia, gran parte della sintassi delle espressioni regolari non è supportata.
Vedere ["Utilizzo della lingua dei criteri degli identificatori dati"](#) a pagina 751.
- 7 Fare clic su **Salva** per salvare l'identificatore di dati.

Utilizzo delle convalide criterio

La seguente tabella elenca tutte le convalide criterio disponibili. Le convalide contrassegnate con un asterisco (*) accanto al nome nella tabella che segue richiedono l'immissione di dati.

Tabella 27-30 Convalide disponibili per identificatori dati di sistema e personalizzati

Convalida	Descrizione
Checksum ABA	Tutti i numeri di routing ABA devono iniziare con le coppie di cifre 00-15,21-32,61-72,80 e devono passare un checksum specifico di ABA, basato sulle posizioni.
Convalida KRRN avanzata	Verifica che la 3a e la 4a cifra siano un mese valido, che la 5a e la 6a cifra siano un giorno valido e che il checksum corrisponda alla cifra di controllo.
SSN avanzato	Lo strumento di convalida verifica che i gruppi che compongono il numero SSN contengano zeri, che il numero area (primo gruppo) sia inferiore a 773 e diverso da 666, che il delimitatore dei gruppi sia lo stesso, che il numero non sia costituito da cifre uguali tra loro e che non sia riservato alla pubblicità (123-45-6789, 987-65-432x).
Controllo di convalida del numero di identificazione fiscale argentino.	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice azienda australiano.	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida del numero Medicare australiano.	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione fiscale australiano (ATF)	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di previdenza sociale austriaco	Calcola il checksum e lo utilizza per convalidare il modello.
SSN di base	Esegue una convalida SSN minima
Controllo di convalida del numero di identificazione nazionale belga	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di partita IVA belga	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di tessera elettorale brasiliana	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di conto bancario brasiliano	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida	Descrizione
Controllo di convalida del numero di Registro Nazionale delle Persone Giuridiche brasiliano	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice fiscale per persone fisiche brasiliano	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida Personal Healthcare Number della Columbia Britannica	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di cittadinanza univoco bulgaro	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo Burgerservicenummer	Esegue un controllo per il Burgerservicenummer.
Controllo di convalida numero di identificazione nazionale cileno	Calcola il checksum e lo utilizza per convalidare il modello.
Convalida checksum ID cinese	Calcola il checksum e lo utilizza per convalidare il modello.
Verifica chiave di controllo codice fiscale	Calcola la chiave di controllo e ne verifica la validità.
Convalida CUSIP	Lo strumento di convalida verifica l'esistenza di intervalli CUSIP non validi e calcola il checksum CUSIP (algoritmo di Luhn, noto anche come Modulo 10).
Script personalizzato*	Immettere uno script personalizzato per convalidare le corrispondenze per la copertura di questo identificatore dati. Vedere "Creazione di convalide con script personalizzati" a pagina 765.
Controllo di convalida del numero di identificazione personale ceco	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione personale danese	Calcola il checksum e lo utilizza per convalidare il modello.
Verifica chiave di controllo DNI	Calcola la chiave di controllo e ne verifica la validità.
Controllo di convalida numero di patente di guida - Stato di Washington	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida	Descrizione
Controllo di convalida numero di patente di guida dello Stato del Wisconsin	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero DEA	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione fiscale dei Paesi Bassi	Calcola il checksum e lo utilizza per convalidare il modello.
Corrispondenza esatta*	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.
Escludi caratteri iniziali*	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi. Nota: Le convalide iniziale e finale sono relative al testo della corrispondenza stessa. Le convalide prefisso e suffisso sono relative ai caratteri che precedono e seguono il testo oggetto della corrispondenza.
Escludi caratteri finali*	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.
Escludi corrispondenza esatta*	Immettere un elenco di valori delimitati da virgole. Ogni valore può avere una lunghezza qualsiasi.
Escludi prefisso*	Immettere un elenco di valori delimitati da virgole. Ogni valore può avere una lunghezza qualsiasi. Nota: Le convalide prefisso e suffisso sono relative ai caratteri che precedono e seguono il testo oggetto della corrispondenza. Le convalide iniziale e finale sono relative al testo della corrispondenza stessa.
Escludi suffisso*	Immettere un elenco di valori delimitati da virgole. Ogni valore può avere una lunghezza qualsiasi.
Trova parole chiave*	Immettere un elenco di valori delimitati da virgole. Ogni valore può avere una lunghezza qualsiasi.
Controllo di convalida codice identificativo personale finlandese	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di partita IVA francese	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida	Descrizione
Controllo di convalida numero di previdenza sociale francese	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione tedesco	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida del numero di passaporto tedesco	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di partita IVA tedesca	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice fiscale greco	Calcola il checksum e lo utilizza per convalidare il modello.
ID di Hong Kong	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di previdenza sociale ungherese	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice di identificazione fiscale ungherese	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di partita IVA ungherese	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di carta di identità indonesiana	Calcola il checksum e lo utilizza per convalidare il modello.
Chiave di controllo INSEE	La convalida calcola la chiave di controllo INSEE e la confronta con le ultime due cifre del modello.
Controllo di base IP	Ogni indirizzo IP deve avere il formato x.x.x.x e ogni numero deve essere inferiore a 256.
Verifica ottetti IP	Ogni indirizzo IP deve avere il formato x.x.x.x, deve essere composto da numeri inferiori a 256 e non deve includere numeri a una sola cifra (1.1.1.2).
Controllo intervallo IP riservato	Verifica se l'indirizzo IP rientra in uno qualsiasi degli intervalli "Bogons". In caso affermativo, la corrispondenza non è valida.
Controllo di convalida di base indirizzo IPv6	Ogni indirizzo IPv6 deve avere il formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx e ogni numero deve essere inferiore a ffff.
Controllo di convalida medio indirizzo Ipv6	Ogni indirizzo IPv6 deve avere il formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx e ogni numero deve essere inferiore a ffff. Nessun indirizzo IPv6 può iniziare con 0.

Convalida	Descrizione
Controllo di convalida riservato indirizzo IPv6	Ogni indirizzo IPv6 deve avere il formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx e ogni numero deve essere inferiore a ffff. Nessun indirizzo IPv6 può iniziare con 0. Ogni indirizzo IPv6 deve essere completamente compresso.
Controllo di convalida Personal Public Service Number (numero personale di servizio pubblico) irlandese	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione personale israeliano	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di partita IVA italiano	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione giapponese (Juki-Net)	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione personale giapponese (My Number)	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo Luhn	Lo strumento di convalida calcola il checksum Luhn che tutti i numeri di previdenza sociale canadesi devono superare.
Controllo di convalida numero di identificazione lussemburghese	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero carta di identità malese (MyKad)	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice di identificazione personale messicano	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di conto bancario esteso messicano	Calcola il checksum e lo utilizza per convalidare il modello.
Convalida Mod 97	Calcola il checksum ISO 7064 Mod 97-10 della corrispondenza completa.
Controllo di convalida numero NPI	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida	Descrizione
Controllo di convalida codice ISIN	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida del numero di partita IVA dei Paesi Bassi	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice di assistenza sanitaria della Nuova Zelanda	Calcola il checksum e lo utilizza per convalidare il modello.
Nessuna convalida	Non esegue alcuna convalida.
Controllo di convalida numero di identificazione personale norvegese	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza controllando le cifre circostanti.
Controllo di convalida numero di identificazione polacco	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice statistico polacco (REGON)	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice fiscale polacco	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione fiscale polacco	Calcola il checksum e lo utilizza per convalidare il modello.
Richiedi caratteri iniziali*	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.
Richiedi caratteri finali*	Immettere un elenco di valori delimitati da virgole. Se i valori sono numerici, NON immettere trattini o altri delimitatori. Ogni valore può avere una lunghezza qualsiasi.
Controllo numero di identificazione personale rumeno	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione fiscale russo	Calcola il checksum e lo utilizza per convalidare il modello.
NRIC Singapore	Calcola il checksum del numero NRIC di Singapore e lo utilizza per convalidare il modello.

Convalida	Descrizione
Controllo di convalida numero di identificazione personale sudafricano	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di conto cliente spagnolo	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di previdenza sociale spagnolo	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida codice di identificazione fiscale spagnolo.	Calcola il checksum e lo utilizza per convalidare il modello.
Numero gruppo/area SSN	Per un dato numero area (primo gruppo), è possibile che la SSA non abbia assegnato tutti i numeri gruppo (secondo gruppo). Lo strumento di convalida elimina i numeri SSN con numeri gruppo non validi.
Controllo di convalida numero di identificazione personale svedese	Calcola il checksum e lo utilizza per convalidare il modello.
Numero di previdenza sociale svizzero (AHV)	Checksum Modulo 11 numero di previdenza sociale svizzero (AHV).
Controllo di convalida numero di previdenza sociale svizzero	Calcola il checksum e lo utilizza per convalidare il modello.
ID Taiwan	Checksum ID di Taiwan.
Controllo di convalida numero di identificazione personale thailandese	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida numero di identificazione turco	Calcola il checksum e lo utilizza per convalidare il modello.
Patente di guida del Regno Unito	I numeri di patente di guida britannici devono contenere 16 caratteri e i numeri in 8a e 9a posizione devono essere maggiori di 00 e minori di 32.
NHS Regno Unito	Checksum NHS Regno Unito.
Controllo di convalida numero di identificazione nazionale venezuelano	Calcola il checksum e lo utilizza per convalidare il modello.
Controllo di convalida Verhoeff	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida	Descrizione
Controllo della carta di identità ucraina	Calcola il checksum e lo utilizza per convalidare il modello.

Selezione di convalide dei criteri

Symantec Data Loss Prevention fornisce un set completo di convalide per assicurare l'accuratezza della corrispondenza con criteri.

Vedere ["Informazioni sulle convalide criterio"](#) a pagina 696.

Quando si modifica un identificatore di dati, il sistema espone le convalide attive utilizzate dall'identificatore di dati. Quando si modifica o si crea un identificatore di dati, il sistema visualizza tutte le convalide di dati definite dal sistema che è possibile selezionare.

Nota: Le convalide attive che consentono e definiscono l'input non devono essere confuse con le convalide facoltative, le quali possono essere configurate per qualsiasi istanza di runtime di un particolare identificatore di dati. Le convalide facoltative sono sempre configurabili a livello dell'istanza. Le convalide attive sono configurabili solo a livello del sistema.

Selezionare una convalida dall'elenco Controlli di convalida a sinistra, quindi fare clic su **Aggiungi convalida** a destra. Se la convalida richiede l'input, fornire i dati richiesti utilizzando un elenco separato da virgole e fare clic su **Aggiungi convalida**.

Vedere ["Selezione di convalide dei criteri"](#) a pagina 763.

Per selezionare una convalida dei criteri

- 1 Creare un identificatore di dati personalizzato.
Vedere ["Flusso di lavoro per la creazione di identificatori di dati personalizzati"](#) a pagina 749.
- 2 Nella sezione **Convalide**, selezionare la convalida desiderata.
Vedere ["Informazioni sulle convalide criterio"](#) a pagina 696.
- 3 Se la convalida non richiede l'immissione di dati, fare clic su **Aggiungi convalida**.
La convalida è aggiunta all'elenco **Convalide attive**.
- 4 Se la convalida richiede l'immissione di dati, immettere i valori nel campo **Immissione dati e descrizione**.
- 5 Modificare l'input per la convalida nel campo **Immissione dati e descrizione**. Se si sta utilizzando la convalida **Trova parole chiave**, modificare l'input per la convalida nel campo **Immissione dati e descrizione**. Poi selezionare le caratteristiche desiderate per la parola chiave:

- **Prossimità** : trova una parola chiave solo nell'ambito della prossimità impostata dei criteri che corrispondono. Selezionare questa casella e indicare la **Distanza tra le parole**.
 - **Distinzione maiuscole/minuscole** : selezionare questa casella se si desidera trovare una corrispondenza con distinzione tra maiuscole e minuscole.
 - **Evidenzia parole chiave nell'incidente** : selezionare questa casella se si desidera evidenziare le parole chiave corrispondenti negli incidenti.
- 6 Fare clic su **Aggiungi convalida** dopo aver immesso i valori.
La convalida è aggiunta all'elenco **Convalide attive**.
- 7 Per rimuovere una convalida, selezionarla nell'elenco **Convalide attive** e fare clic sull'icona X rossa.
- 8 Fare clic su **Salva** per salvare la configurazione dell'identificatore di dati.

Selezione di un normalizzatore di dati

Quando si crea un identificatore dati personalizzato, è necessario selezionare un normalizzatore per riconciliare i dati individuati dal criterio con il formato previsto dalle convalide.

Vedere ["Flusso di lavoro per la creazione di identificatori di dati personalizzati"](#) a pagina 749.

La [Tabella 27-31](#) elenca e descrive i normalizzatori implementabili per gli identificatori dati personalizzati.

Nota: Non è possibile modificare il normalizzatore di un identificatore dati definito dal sistema.

Tabella 27-31 Normalizzatori di dati disponibili

Normalizzatore	Descrizione
Cifre	Sono consentiti solo i caratteri numerici.
Cifre e lettere	Sono consentiti i caratteri alfanumerici.
Minuscole	Sono consentite soltanto le lettere, normalizzate a lettere minuscole.
Codici SWIFT	Il codice deve corrispondere ai requisiti SWIFT.
Non intervenire	I dati non vengono normalizzati e vengono valutati come inseriti dall'utente.

Creazione di convalide con script personalizzati

Il controllo di convalida con script personalizzati consente di immettere uno script personalizzato per convalidare le corrispondenze con il criterio. Per implementare una convalida personalizzata, si utilizza il linguaggio di script di Symantec Data Loss Prevention.

È possibile implementare una convalida con script personalizzato in un identificatore di dati del sistema modificato o in un identificatore di dati personalizzato.

Nota: Fare riferimento alla *Guida alla personalizzazione di Symantec Data Loss Prevention* per informazioni dettagliate sull'uso del linguaggio di script di Symantec Data Loss Prevention.

Per implementare una convalida con script personalizzato

- 1 Modificare un identificatore di dati esistente o crearne uno personalizzato.
Vedere ["Flusso di lavoro per la creazione di identificatori di dati personalizzati"](#) a pagina 749.
- 2 Selezionare la convalida **Script personalizzato** dall'elenco **Controlli di convalida**.
- 3 Immettere lo script personalizzato nel campo **Immissione dati e descrizione**.
- 4 Fare clic su **Aggiungi convalida** per aggiungere la convalida personalizzata all'elenco **Convalide attive**.
- 5 Fare clic su **Salva** per salvare la configurazione dell'identificatore di dati.

Best practice per l'utilizzo degli identificatori dati

Gli identificatori di dati sono algoritmi che combinano la corrispondenza dei modelli con le convalide dei dati per rilevare il contenuto. Symantec Data Loss Prevention include vari identificatori dati definiti dal sistema per criteri di dati comuni, quali numeri di previdenza sociale, codici fiscali e così via. Inoltre è possibile definire identificatori dati personalizzati per rilevare la corrispondenza con qualsiasi tipo di dati descritti con il linguaggio dei criteri dell'identificatore dati. Gli identificatori dati sono comunemente utilizzati per rilevare informazioni che consentono l'identificazione dell'utente (PII).

Questa sezione fornisce best practice per l'implementazione delle politiche dell'identificatore dati.

La [Tabella 27-32](#) riepiloga le best practice per questa sezione.

Tabella 27-32 Riepilogo delle best practice per gli identificatori dati

Best practice	Descrizione
Se possibile, utilizzare sempre gli identificatori dati anziché le espressioni regolari.	Vedere "Utilizzo degli identificatori dati invece di espressioni regolari per migliorare la precisione" a pagina 766.
Modificare le definizioni dell'identificatore dati quando si desidera applicare l'ottimizzazione a livello globale.	Vedere "Modifica delle definizioni dell'identificatore dati quando si desidera applicare l'ottimizzazione a livello globale" a pagina 767.
Chiudere gli identificatori dati definiti dal sistema prima di modificarli.	Vedere "Clonare gli identificatori di dati definiti dal sistema prima della modifica per mantenere lo stato originale" a pagina 767.
Considerare la possibilità di utilizzare la copertura di più identificatori dati in parallelo	Vedere "Possibilità di utilizzare parallelamente più coperture per rilevare gravità diverse dei dati riservati" a pagina 768.
Evitare la corrispondenza con la busta HTTP	Vedere "Evitare la corrispondenza con la busta HTTP per ridurre i falsi positivi" a pagina 768.
Utilizzare l'identificatore dati Social Security Number (SSN) statunitense randomizzato per rilevare i numeri di previdenza sociale tradizionali e randomizzati	Vedere "Utilizzo dell'identificatore dati Social Security Number (SSN) statunitense randomizzato per rilevare i numeri di previdenza sociale" a pagina 769.
Utilizzo del conteggio corrispondenze univoche per migliorare l'accuratezza e facilitare le riparazioni	Vedere "Utilizzo del conteggio corrispondenze univoche per migliorare l'accuratezza e facilitare le riparazioni" a pagina 769.

Utilizzo degli identificatori dati invece di espressioni regolari per migliorare la precisione

Gli identificatori dati hanno lo scopo di proteggere le informazioni che consentono l'identificazione dell'utente con un livello di precisione elevato (incidenza di falsi positivi <10%). Se un identificatore dati è disponibile per il tipo di contenuto che si desidera proteggere, è necessario utilizzare l'identificatore dati invece di un'espressione regolare perché gli identificatori dati sono più efficienti delle espressioni regolari. I criteri degli identificatori dati pronti per l'uso sono ottimizzati per la precisione, comprese le sfumature a livello di regione, industria e paese. Inoltre gli identificatori dati comprendono i controlli di convalida per la verifica dei dati corrispondenti al criterio. Questo livello supplementare di informazioni esclude i dati di test e altre attivazioni di incidenti di falsi positivi. Le espressioni regolari, d'altra parte, possono richiedere una certa elaborazione di calcolo e comportare un numero maggiore di falsi positivi.

Ad esempio, se si desidera rilevare i numeri di previdenza sociale, si utilizza l'identificatore dati Social Security Number (SSN) statunitense randomizzato invece di un'espressione regolare.

L'identificatore dati Social Security Number (SSN) statunitense randomizzato è più preciso di qualsiasi espressione regolare che si possa scrivere e molto più facile e veloce da implementare.

Nota: il linguaggio dei criteri dell'identificatore dati è un sottoinsieme limitato del linguaggio delle espressioni regolari. Non tutti i costrutti di espressione regolare o i caratteri sono supportati per i criteri dell'identificatore dati. Vedere ["Utilizzo della lingua dei criteri degli identificatori dati"](#) a pagina 751.

Clonare gli identificatori di dati definiti dal sistema prima della modifica per mantenere lo stato originale

Prima di modificare un identificatore di dati del sistema o creare un identificatore di dati personalizzato, considerare quanto segue:

- Se si desidera modificare un identificatore di dati del sistema, clonarlo manualmente come un identificatore di dati personalizzato e quindi modificare la copia clonata. In questo modo, si mantiene lo stato dell'identificatore di dati del sistema originale.
- Gli identificatori di dati non sono esportati come parte di un modello di politica. Di conseguenza, è necessario aggiungere l'identificatore di dati a una politica ed esportare la politica come modello prima di modificare l'identificatore di dati.
Un modello esportato contiene un riferimento a ogni identificatore di dati implementato in quella politica. Quando importato in un sistema target, il modello utilizza un riferimento per selezionare l'identificatore di dati locale. Se l'identificatore di dati del sistema viene modificato, non può essere riconosciuto dal sistema target al momento dell'importazione.

Vedere ["Clonazione di un identificatore dati di sistema prima della sua modifica"](#) a pagina 726.

Modifica delle definizioni dell'identificatore dati quando si desidera applicare l'ottimizzazione a livello globale

Gli identificatori dati offrono due livelli di configurazione:

- Definizioni
- Istanze

Le definizioni dell'identificatore dati vengono configurate al livello del sistema di Enforce Server. Al livello della definizione è possibile ottimizzare i dati forniti da qualsiasi convalida obbligatoria che la definizione dichiara a questo livello, nonché le convalide da utilizzare.

Le istanze dell'identificatore dati possono venire configurate solo al livello della regola della politica. Eventuali configurazioni eseguite al livello della regola sono locali in termini di ambito e applicabili solo a tale politica. Al livello della regola utilizzare le convalide opzionali, ad

esempio richiedere o escludere i caratteri iniziali o finali, per ottimizzare l'istanza della regola dell'identificatore dati.

A livello generale si consiglia di configurare le definizioni dell'identificatore dati in modo che le modifiche vengano applicate globalmente a qualsiasi istanza della definizione dell'identificatore dati. Tali configurazioni sono riutilizzabili in tutte le politiche. Le convalide opzionali al livello della regola devono venire utilizzate per le politiche univoche.

Possibilità di utilizzare parallelamente più coperture per rilevare gravità diverse dei dati riservati

La corrispondenza di identificatori dati con il contenuto spesso richiede l'ottimizzazione mentre si regola la configurazione per ridurre al minimo i falsi positivi e i falsi negativi. Dopo avere configurato un'istanza della condizione **Contenuto corrispondente a identificatore dati**, esaminare le corrispondenze e regolare la configurazione in modo da ottimizzare la corrispondenza dei dati.

Considerare la possibilità di regolare la copertura dell'identificatore dati in uso se l'identificatore restituisce troppi falsi positivi o falsi negativi. Ad esempio, se si utilizza una copertura ampia e si ricevono molti falsi positivi, si consiglia di utilizzare una copertura media o limitata.

Vedere ["Informazioni sulle coperture degli identificatori di dati"](#) a pagina 694.

Un approccio alternativo consiste nell'utilizzo in parallelo di più coperture dell'identificatore dati nella stessa regola con diversi livelli di gravità per ciascuna regola. Ad esempio, in una singola politica definita per rilevare i numeri di carta di credito è possibile aggiungere tre regole, ciascuna con una copertura diversa (ampia, media e limitata). Quindi impostare la gravità per la copertura limitata su incidenti di gravità elevata e la gravità per la copertura ampia su incidenti di gravità bassa. L'utilizzo di questo approccio a più livelli consente di esaminare i dati a livello dell'azienda con una politica che copre entrambe le estremità dell'intervallo. È possibile usare questo approccio basato sul campionamento per concentrare gli sforzi di risoluzione sugli incidenti con la massima priorità e continuare a rilevare e analizzare gli incidenti di gravità bassa.

Evitare la corrispondenza con la busta HTTP per ridurre i falsi positivi

Talvolta le trasmissioni HTTP contengono nell'intestazione ID di sessione che possono attivare falsi positivi per gli identificatori dati numerici. Ad esempio, alcuni siti di social media quali Facebook e LinkedIn contengono un ID sessione che talvolta corrisponde esattamente agli identificatori dati CCN e SSN, causando falsi positivi.

Per ridurre i falsi positivi associati agli ID sessione HTTP nell'intestazione dei messaggi, la best practice consiste nell'evitare di stabilire la corrispondenza con il componente "Busta" del messaggio quando si implementano identificatori dati numerici, in particolare gli identificatori dati CCN o SSN.

Utilizzo dell'identificatore dati Social Security Number (SSN) statunitense randomizzato per rilevare i numeri di previdenza sociale

Nel 2011 la Social Security Administration (SSA) degli Stati Uniti ha iniziato a distribuire numeri di previdenza sociale randomizzati. Nell'ambito di questo schema, il numero del gruppo (seconda parte del numero di previdenza sociale) non corrisponde più al numero dell'area (prima parte del numero di previdenza sociale). Inoltre l'intervallo del numero dell'area può salire fino a 899 invece di 773. La randomizzazione si applica ai numeri di previdenza sociale emessi a partire dal 25 giugno 2011 compreso. Non si applica ai numeri di previdenza sociale distribuiti prima di tale data.

Per supportare il nuovo schema SSN randomizzato, Symantec Data Loss Prevention fornisce l'identificatore dati **Social Security Number (SSN) statunitense randomizzato** definito dal sistema.

Vedere ["Social Security Number \(SSN\) statunitense randomizzato"](#) a pagina 1218.

L'identificatore dati Social Security Number (SSN) statunitense randomizzato rileva i numeri di previdenza sociale tradizionali e randomizzati. L'identificatore dati Social Security Number (SSN) statunitense randomizzato sostituisce l'identificatore dati Social Security Number (SSN) statunitense, che rileva solo i numeri di previdenza sociale tradizionali. Inoltre i criteri per l'identificatore dati Social Security Number (SSN) statunitense randomizzato vengono aggiornati per la versione 14.0.

Symantec consiglia di utilizzare l'identificatore dati Social Security Number (SSN) statunitense randomizzato per tutte le nuove politiche che si desidera impiegare per rilevare i numeri di previdenza sociale e di aggiornare i criteri SSN esistenti per usare l'identificatore dati Social Security Number (SSN) statunitense randomizzato. Per le politiche esistenti che implementano già l'identificatore dati Social Security Number (SSN) statunitense tradizionale è possibile aggiungere l'identificatore dati Social Security Number (SSN) statunitense randomizzato come regola concatenata con la condizione OR in modo che entrambe vengano eseguite in parallelo mentre si testa la politica per assicurarsi che rilevi accuratamente entrambi gli stili dei numeri di previdenza sociale.

Vedere ["Aggiornamento delle politiche per l'utilizzo dell'identificatore dati Social Security Number \(SSN\) statunitense randomizzato"](#) a pagina 747.

Utilizzo del conteggio corrispondenze univoche per migliorare l'accuratezza e facilitare le riparazioni

La configurazione della regola dell'identificatore dati contiene un'opzione per il conteggio delle sole corrispondenze univoche. Con questa opzione selezionata (anziché con l'impostazione predefinita che conta tutte le corrispondenze), solo le corrispondenze univoche verranno segnalate come prima corrispondenza trovata nel messaggio o nel componente del messaggio. Vengono contate ed evidenziate solo le corrispondenze univoche.

La best practice consiste nell'usare la corrispondenza univoca quando si è interessati esclusivamente alle corrispondenze univoche, e non a quelle duplicate. Se ad esempio si sta utilizzando l'identificatore dati Numeri di carta di credito per proteggere i numeri di carta di credito e interessa solo il fatto che un documento contenga 25 o più numeri univoci, si utilizzerà l'opzione Conta tutte le corrispondenze univoche anziché l'opzione Conta tutte le corrispondenze. Se si utilizza Conta tutte le corrispondenze un documento contenente 25 volte lo stesso numero di carta di credito attiverà la politica e questo non è l'obiettivo della politica stessa.

Vedere ["Informazioni sul conteggio delle corrispondenze univoche"](#) a pagina 697.

Rilevamento del contenuto mediante la corrispondenza di parole chiave

Il capitolo contiene i seguenti argomenti:

- [Introduzione alla corrispondenza con parole chiave](#)
- [Configurazione della corrispondenza di parole chiave](#)
- [Best practice per l'utilizzo della corrispondenza di parole chiave](#)

Introduzione alla corrispondenza con parole chiave

Symantec Data Loss Prevention fornisce la condizione di politica **Contenuto corrispondente a parola chiave** per il rilevamento con parole chiave.

Per rilevare perdite di dati utilizzando la corrispondenza con parole chiave, il motore di rilevamento confronta i messaggi in arrivo o i componenti del messaggio con ogni parola chiave in un elenco di una o più parole o frasi chiave. La corrispondenza con parole chiave supporta la corrispondenza con parole intere o parziali, nonché la prossimità delle parole. La corrispondenza con parole chiave è supportata sul server e sull'endpoint. Il conteggio delle corrispondenze uniche è supportato per le parole chiave.

Vedere ["Utilizzo del totale corrispondenze univoche"](#) a pagina 723.

[Tabella 28-1](#) elenca i casi di utilizzo tipici della corrispondenza con parole chiave.

Tabella 28-1 Casi di utilizzo tipici della corrispondenza con parole chiave

Configurazione	Utilizzo tipico
Corrispondenza con parole intere	Lingue basate sull'alfabeto latino Caratteri UTF-8 Lingue cinese, giapponese e coreano (CJK) con verifica dei token per il server Parole chiave CJK sull'endpoint Vedere "Informazioni sulla corrispondenza di parole chiave per le lingue cinese, giapponese e coreano (CJK)" a pagina 772.
Corrispondenza con parole chiave parziali	Lingue basate sull'alfabeto latino Lingue miste Vedere "Esempi di corrispondenza con parole chiave" a pagina 775.

Informazioni sulla corrispondenza di parole chiave per le lingue cinese, giapponese e coreano (CJK)

I server di rilevamento Symantec Data Loss Prevention 14.0 e versioni successive supportano l'elaborazione della lingua naturale per le parole chiave in cinese, giapponese e coreano (CJK). Quando l'elaborazione della lingua naturale per le lingue CJK è attivata, il server di rilevamento convalida i token CJK prima di segnalare una corrispondenza. Per le lingue CJK, un token è un singolo carattere che costituisce una parola. Quindi la corrispondenza di parole parziale non si applica alle lingue CJK.

La convalida dei token per le parole chiave CJK è supportata solo per i server di rilevamento ed è disattivata per impostazione predefinita. È necessario attivare la convalida dei token per ciascun server di rilevamento. Inoltre è necessario trovare la corrispondenza con parole intere per applicare la convalida dei token.

Sull'endpoint è possibile utilizzare la corrispondenza di parole intere per le parole chiave CJK.

La [Tabella 28-2](#) riassume i casi di utilizzo della corrispondenza di parole chiave per le lingue CJK.

Tabella 28-2 Casi di utilizzo della corrispondenza di parole chiave per le lingue CJK

Componente di rilevamento	Caso di utilizzo
Server	Attivazione della verifica dei token sul server di rilevamento e utilizzo della corrispondenza di parole intere Vedere "Attivazione e utilizzo della verifica dei token CJK per la corrispondenza di parole chiave sul server" a pagina 781.

Componente di rilevamento	Caso di utilizzo
Endpoint	<p>Utilizzo della corrispondenza di parole intere</p> <p>Vedere "Esempi di corrispondenze parole chiave per lingue cinese, giapponese e coreano" a pagina 776.</p>

Informazioni sulla prossimità di parole chiave

Mediante la prossimità di parole chiave, un autore di politiche può definire una coppia di parole chiave e specificare un intervallo di parole tra le stesse. Se le parole rientrano in quell'intervallo, viene generata una corrispondenza. Ad esempio, un'istanza della condizione **Contenuto corrispondente a parola chiave** potrebbe richiedere che qualsiasi istanza delle parole "informazioni" e "riservate" a non più di 10 parole l'una dall'altra generi una corrispondenza.

Alternativamente, è possibile usare la prossimità di parole chiave per escludere le parole corrispondenti entro una distanza specificata utilizzando la condizione **Contenuto corrispondente a parola chiave** come eccezione di rilevamento. In questo caso, qualsiasi occorrenza delle parole "informazioni" e "riservate" entro 10 parole l'una dall'altra viene esclusa dalla corrispondenza.

Per il cinese, il giapponese e il coreano (CJK), un singolo carattere CJK viene conteggiato come una parola.

Vedere ["Sintassi della corrispondenza di parole chiave"](#) a pagina 773.

Vedere ["Esempi di corrispondenza con parole chiave"](#) a pagina 775.

Vedere ["Configurazione della condizione Contenuto corrispondente a parola chiave"](#) a pagina 779.

Sintassi della corrispondenza di parole chiave

Quando si definisce una regola di parole chiave, il sistema confronta ogni parola chiave nell'elenco delle condizioni con ciascun componente del messaggio (intestazione, oggetto, corpo, allegato).

Considerare le seguenti linee guida per la sintassi durante la creazione di elenchi di parole chiave.

Tabella 28-3 Sintassi della corrispondenza di parole chiave

Comportamento	Descrizione
Corrispondenza parola intera	<p>Con la corrispondenza parola intera le parole chiave rilevano la corrispondenza esclusivamente sui limiti della parola (\W nel lessico dell'espressione regolare). Tutti i caratteri all'infuori di A-Z, a-z e 0-9 sono interpretati come limiti della parola.</p> <p>Con la corrispondenza parola intera le parole chiave devono includere almeno un carattere alfanumerico (una lettera o un numero). Una parola chiave costituita solo da caratteri spazio, come ".." viene ignorata.</p>
Virgolette	Non utilizzare le virgolette quando si immettono parole chiave o frasi perché le virgolette vengono interpretate letteralmente e sono quindi richieste nella corrispondenza.
Spazio vuoto	Il sistema rimuove lo spazio vuoto prima e dopo le parole chiave e le frasi. Ogni spazio vuoto all'interno di una parola chiave o frase viene contato. Oltre agli spazi effettivi, tutti i caratteri all'infuori di A-Z, a-z e 0-9 sono interpretati come spazi vuoti.
Distinzione maiuscole/minuscole	L'opzione per la distinzione tra maiuscole e minuscole che si sceglie si applica a tutte le parole chiave nell'elenco per la condizione.
Plurali e flessioni dei verbi	Tutti i plurali e le flessioni dei verbi devono essere specificamente elencati. Se il numero di enumerazioni diventa complesso, utilizzare il carattere jolly (asterisco [*]) per rilevare un suffisso in una parola chiave (solo in modalità parole intere).
Frase chiave	È possibile immettere frasi chiave, ad esempio codice fiscale (senza le virgolette). Il sistema cerca la frase intera senza restituire corrispondenze con singole parole (ad esempio codice o fiscale).
Varianti di parole chiave	Il sistema rileva solo la parola chiave o frase chiave esatta, non le varianti. Ad esempio, se si specifica la frase chiave codice fiscale , il rilevamento non individua una frase che contiene due spazi tra le parole.
Corrispondenza con più parole chiave	Il sistema applica la condizione OR tra le parole chiave. Ovvero, un componente di un messaggio corrisponde se contiene una delle parole chiave e non necessariamente tutte. Per effettuare corrispondenze di parole chiave con la condizione ALL (o AND), combinare più condizioni in una regola o in un'eccezione composta.

Comportamento	Descrizione
Caratteri alfanumerici	<p>Nella corrispondenza di parole chiave, solo una lettera o un numero viene considerato come una posizione iniziale di parola chiave valida. I caratteri speciali (non alfanumerici) vengono considerati come delimitatori (ignorati). Ad esempio, la e commerciale ("&") e il carattere di sottolineatura ("_") sono caratteri speciali e vengono ignorati come posizione iniziale di parole chiave.</p> <p>Ad esempio, si consideri quanto segue:</p> <pre>____keyword__</pre> <pre>Keyword</pre> <pre>&&akeyword&&</pre> <pre>123Keyword__</pre> <p>Per questi esempi, le posizioni iniziali valide delle parole chiave sono le seguenti: k, K, a e 1.</p> <p>Nota: Lo stesso comportamento si applica alla convalida delle parole chiave implementata negli identificatori di dati.</p>
Prossimità	<p>La distanza tra le parole (valore di prossimità) è esclusiva delle parole chiave rilevate. Di conseguenza, una distanza di 10 consente un intervallo di prossimità di 12 parole.</p>

Esempi di corrispondenza con parole chiave

Per implementare la corrispondenza con parole chiave, è possibile immettere una o più parole o frasi chiave, ciascuna separata da una virgola o un carattere di nuova riga. È possibile cercare la corrispondenza con parole intere o parziali e specificare la distinzione maiuscole/minuscole. È possibile usare il carattere jolly (*) per rilevare il suffisso di una parola chiave (solo in modalità parola intera).

Vedere ["Sintassi della corrispondenza di parole chiave"](#) a pagina 773.

Tabella 28-4 Esempi di corrispondenza con parole chiave

Tipo di parola chiave	Parole chiave	Corrisponde con	Non corrisponde
parola chiave	veloce	veloce -veloce; ®"veloce" ®Veloce ®VELOCE	velocemente (solo in modalità parola intera, altrimenti si ha corrispondenza)

Tipo di parola chiave	Parole chiave		Corrisponde con	Non corrisponde
frase chiave	solo per uso interno		solo per uso interno SOLO per uso interno (se la distinzione tra maiuscole e minuscole non è selezionata)	uso interno
elenco di parole chiave	Delimitate da ritorno a capo:	Delimitate da virgole:	crediti credito creditore	creditori accreditato
	credito creditore crediti	credito, creditore, crediti		
parola chiave con carattere jolly	priv*		privato privilegio privacy privilegiare privilegiato privare	primo priorità
dizionario di parole chiave	numero di conto, american express, amex, carta bancaria, n. carta, numero carta, n. cc, ncc, carta assegni, carta di credito, n. carta di credito, numero carta di credito, carta di debito, diners club, dinersclub, discover, enroute, japanese card bureau, jcb, mastercard, mc, visa, (ecc.)		Se una qualsiasi parola chiave o frase è presente, i dati sono corrispondenti:	amx cartacredito master card
			amex carta di credito mastercard	carte

Esempi di corrispondenze parole chiave per lingue cinese, giapponese e coreano

Tabella 28-5 fornisce gli esempi di corrispondenza parole chiave EDM per cinese, giapponese e coreano. Tutti gli esempi presuppongono che la parola chiave sia configurata per corrispondere unicamente a tutte le parole.

Se la verifica token è attivata, le dimensioni del messaggio devono essere sufficienti per il riconoscimento della lingua da parte dello strumento di verifica del token. Ad esempio: il messaggio “東京都市部の人口” è troppo breve perché il processo di convalida del token possa riconoscere la lingua del messaggio. Il seguente messaggio è di dimensione sufficiente per l’elaborazione di convalida del token:

今朝のニュースによると東京都市部の人口は増加傾向にあるとのことでした。全国的な人口減少の傾向の中、東京への一極集中を表しています。

Vedere ["Informazioni sulla corrispondenza di parole chiave per le lingue cinese, giapponese e coreano \(CJK\)"](#) a pagina 772.

La convalida del token per le parole chiave in cinese, giapponese e coreano non è disponibile nell'endpoint. Per far corrispondere cinese, giapponese e coreano nell'endpoint, configurare la condizione per far corrispondere solo le parole intere.

Tabella 28-5 Esempi di corrispondenza parole chiave per cinese, giapponese e coreano

Lingua	Parola chiave	Corrispondenze sul server con convalida token attivata	Corrispondenze sul server con convalida token disattivata	Corrispondenze sull'endpoint
Cinese	通信	数字无线通信	数字无线通信 交通信息网站	数字无线通信 交通信息网站
Giapponese	京都市	京都府京都市左京区	京都府京都市左京区 東京都市部の人口	京都府京都市左京区 東京都市部の人
Coreano	정부	정부의 방침	정부의 방침 의정부 경전철	정부의 방침 의정부 경전철

Informazioni sugli aggiornamenti degli elenchi relativi a medicinali, malattie e cure

Gli elenchi di parole chiave per medicinali, malattie e cure vengono aggiornati con termini attuali basati su informazioni della FDA (Federal Drug Administration) degli Stati Uniti e di altre fonti. Gli elenchi di parole chiave relative a medicinali, malattie e cure sono utilizzati nei modelli di politica **HIPAA e HITECH (incluso PHI)** e **Relazione Caldicott**.

Quando si aggiorna il proprio sistema Data Loss Prevention, i modelli di politica generici HIPAA and Caldicott definiti dal sistema vengono aggiornati con gli elenchi delle parole chiave relativi a medicinali, malattie e cure più recenti. Tuttavia, le politiche create in base ai modelli di politica HIPAA o Caldicott non vengono aggiornate automaticamente. Tale comportamento è previsto in modo tale che qualsiasi modifica o personalizzazione applicata ai modelli di politica HIPAA o Caldicott non venga sovrascritta dagli aggiornamenti dei modelli definiti dal sistema. L'aggiornamento degli elenchi di parole chiave relative a medicinali, malattie e cure per i modelli di politica HIPAA e Caldicott è una procedura manuale che è necessario eseguire per aggiornare le politiche HIPAA o Caldicott.

Vedere ["Aggiornamento degli elenchi di parole chiave Medicinali, Malattie e Cure per le politiche HIPAA e Caldicott"](#) a pagina 782.

Vedere ["Aggiornamento degli elenchi di parole chiave per le politiche HIPAA e Caldicott."](#) a pagina 785.

Vedere ["Modello di politica HIPAA e HITECH \(incluso PHI\)"](#) a pagina 1416.

Vedere ["Modello della politica Relazione Caldicott"](#) a pagina 1319.

Configurazione della corrispondenza di parole chiave

La [Tabella 28-6](#) descrive i componenti per l'implementazione della corrispondenza di parole chiave.

Tabella 28-6 Implementazione della corrispondenza di parole chiave

Funzionalità della corrispondenza di parole chiave	Descrizione
Corrispondenza con parole chiave e frasi chiave intere o parziali	Separare ciascuna parola chiave o frase chiave con una nuova riga o una virgola. Vedere "Esempi di corrispondenza con parole chiave" a pagina 775.
Corrispondenza con il carattere jolly asterisco (*)	Cerca la corrispondenza con il carattere jolly alla fine di una parola chiave, solo nella modalità parola intera. Vedere "Esempi di corrispondenza con parole chiave" a pagina 775.
Corrispondenza prossimità parola chiave	Cerca la corrispondenza in una serie di parole chiave. Vedere "Informazioni sulla prossimità di parole chiave" a pagina 773.
Trova parole chiave	Implementare una o più parole chiave negli identificatori dati per affinare l'ambito di rilevamento. Vedere "Introduzione agli identificatori di dati" a pagina 681.
Regole ed eccezioni di politica	È possibile implementare le condizioni di corrispondenza di parole chiave nelle regole e nelle eccezioni di politica. Vedere "Configurazione della condizione Contenuto corrispondente a parola chiave" a pagina 779.
Corrispondenza di componenti incrociati	La corrispondenza di parole chiave rileva uno o più componenti del messaggio. Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.
Dizionario di parole chiave	Se si dispone di un grande dizionario di parole chiave, è possibile indicizzare l'elenco delle parole chiave. Vedere "Utilizzo di VML per generare e mantenere grandi dizionari di parole chiave" a pagina 786.
Verifica token CJK	Attivarla sul server di rilevamento per le lingue CJK e cercare la corrispondenza solo con parole intere. Vedere Tabella 28-2 a pagina 772.

Configurazione della condizione Contenuto corrispondente a parola chiave

La condizione **Contenuto corrispondente a parola chiave** consente di cercare la corrispondenza con il contenuto utilizzando parole e frasi chiave.

Vedere ["Introduzione alla corrispondenza con parole chiave"](#) a pagina 771.

È possibile implementare le condizioni di corrispondenza con parola chiave nelle regole e nelle eccezioni di politica.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Per configurare la condizione Contenuto corrispondente a parola chiave

- 1 Aggiungere una nuova condizione con parole chiave a una regola o a un'eccezione di politica, oppure modificarne una esistente.

Vedere ["Configurazione di regole di politica"](#) a pagina 427.

Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.

- 2 Configurare i parametri di corrispondenza con parola chiave.

Vedere [Tabella 28-7](#) a pagina 779.

Vedere ["Sintassi della corrispondenza di parole chiave"](#) a pagina 773.

- 3 Salvare la politica.

Tabella 28-7 Configurazione della condizione Contenuto corrispondente a parola chiave

Azione	Descrizione
Immettere il tipo di corrispondenza.	Per la corrispondenza con parola chiave selezionare: Distinzione maiuscole/minuscole o Senza distinzione maiuscole/minuscole Senza distinzione tra maiuscole e minuscole è l'impostazione predefinita.
Scegliere il separatore di parole chiave.	Selezionare il separatore di parole chiave per delimitare molteplici parole chiave: Nuova riga o Virgola . Nuova riga è l'impostazione predefinita.

Azione	Descrizione
Cercare la corrispondenza con qualsiasi parola chiave.	<p>Immettere le parole o frasi chiave per la corrispondenza. Utilizzare il separatore selezionato (nuova linea o virgola) per delimitare molteplici parole o frasi chiave.</p> <p>È possibile usare il carattere jolly (*, asterisco) alla fine di qualsiasi parola chiave per cercare la corrispondenza con uno o più suffissi in quella parola chiave. Se si utilizza il carattere jolly, è necessario cercare la corrispondenza soltanto con parole intere. Ad esempio, se si specifica la parola chiave confid*, verrà restituito "confidenziale" e "confidente" ma non "confine". Se si ha la corrispondenza con il prefisso della parola chiave, il motore di rilevamento cerca la corrispondenza con i caratteri rimanenti utilizzando il carattere jolly.</p> <p>Vedere "Sintassi della corrispondenza di parole chiave" a pagina 773.</p> <p>Vedere "Esempi di corrispondenza con parole chiave" a pagina 775.</p>
Configurare la corrispondenza di prossimità con parole chiave (facoltativo).	<p>La corrispondenza di prossimità con parole chiave consente di specificare un intervallo di rilevamento tra coppie di parole chiave.</p> <p>Vedere "Informazioni sulla prossimità di parole chiave" a pagina 773.</p> <p>Per implementare la corrispondenza di prossimità con le parole chiave:</p> <ul style="list-style-type: none"> ■ Selezionare l'opzione Corrispondenza prossimità parola chiave nella sezione "Condizioni" dell'interfaccia del generatore di regole. ■ Fare clic su Aggiungi coppia di parole chiave. ■ Immettere un coppia di parole chiave. ■ Specificare la Distanza tra le parole. La distanza massima tra le parole chiave è 999, in quanto limitata dalla lunghezza a tre cifre del campo "Distanza tra le parole". La distanza tra le parole è esclusiva delle parole chiave rilevate. Ad esempio, una distanza pari a 10 consente un intervallo di 12 parole, incluse le due parole della coppia di parole chiave. ■ Ripetere il processo per aggiungere ulteriori coppie di parole chiave. Il sistema associa molteplici coppie di parole chiave all'operatore booleano OR, ad indicare che il motore di rilevamento valuta ogni coppia di parole chiave indipendentemente.
Cercare la corrispondenza con parole intere o parziali.	<p>Selezionare l'opzione Solo su parole intere per cercare la corrispondenza solo con parole chiave intere. Questa è l'opzione selezionata per impostazione predefinita.</p> <p>È necessario trovare la corrispondenza con parole intere solo se si utilizza il carattere jolly (*) in una qualsiasi parola chiave inserita nell'elenco.</p> <p>Vedere "Esempi di corrispondenza con parole chiave" a pagina 775.</p> <p>È necessario trovare la corrispondenza con parole intere solo se si è attivata la convalida del token per il server.</p> <p>Vedere "Esempi di corrispondenze parole chiave per lingue cinese, giapponese e coreano" a pagina 776.</p>

Azione	Descrizione
Configurare le condizioni di corrispondenza.	<p>La corrispondenza con parola chiave consente di specificare il modo in cui conteggiare le corrispondenze con la condizione.</p> <p>Selezionare una delle opzioni seguenti:</p> <ul style="list-style-type: none"> ■ Verificare esistenza Il sistema segnala un incidente per tutte le corrispondenze. ■ Conta tutte le corrispondenze e segnala solo gli incidenti con almeno 1 corrispondenze (impostazione predefinita) Con l'impostazione predefinita il sistema segnala un incidente per ogni corrispondenza. In alternativa, è possibile configurare la soglia di corrispondenze sostituendo il valore predefinito 1 con un altro valore. <p>Vedere "Configurazione del conteggio delle corrispondenze" a pagina 431.</p>
Selezionare i componenti in cui cercare la corrispondenza.	<p>Il rilevamento di corrispondenze con parola chiave supporta la ricerca di corrispondenze in molteplici componenti dei messaggi.</p> <p>Vedere "Selezione dei componenti per la corrispondenza" a pagina 433.</p> <p>Selezionare una o più componenti dei messaggi in cui cercare la corrispondenza:</p> <ul style="list-style-type: none"> ■ Busta - Metadati dell'intestazione usati per trasportare il messaggio ■ Oggetto - Oggetto del messaggio (applicabile solo a SMTP) ■ Corpo – Il contenuto del messaggio ■ Allegati - Qualsiasi file allegato al messaggio o inoltrato dallo stesso <p>Nota: Sull'endpoint il DLP Agent cerca la corrispondenza nell'intero messaggio, non nei singoli componenti.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p>
Cercare la corrispondenza anche con una o più condizioni supplementari.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere soddisfatte per segnalare una corrispondenza.</p> <p>È possibile aggiungere qualsiasi condizione disponibile dall'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Attivazione e utilizzo della verifica dei token CJK per la corrispondenza di parole chiave sul server

Per utilizzare la verifica dei token per il cinese, il giapponese e il coreano, è necessario attivarla sul server e utilizzare la corrispondenza di parole intere per la condizione di parola chiave. Inoltre deve esservi un testo di dimensioni sufficienti affinché il sistema riconosca la lingua.

Vedere ["Esempi di corrispondenze parole chiave per lingue cinese, giapponese e coreano"](#) a pagina 776.

La [Tabella 28-8](#) elenca e descrive il parametro del server di rilevamento che consente di attivare la verifica dei token per le lingue CJK.

Tabella 28-8 Parametro di verifica dei token per le parole chiave

Impostazione	Impostazione predefinita	Descrizione
Keyword.TokenVerifierEnabled	false	L'impostazione predefinita è disattivata ("false"). Se attivata ("true"), il server convalida i token per le parole chiave in lingua cinese, giapponese e coreana.

[Per attivare la verifica dei token per le parole chiave CJK](#) descrive come attivare e utilizzare la verifica del token per le parole chiave CJK.

Per attivare la verifica dei token per le parole chiave CJK

- 1 Accedere a Enforce Server come utente amministrativo.
- 2 Accedere alla schermata **Sistema > Server e rilevatori > Panoramica > Dettagli server/rilevatore - Impostazioni avanzate** per il server di rilevamento o il rilevatore che si desidera configurare.
Vedere ["Impostazioni server avanzate"](#) a pagina 279.
- 3 Individuare il parametro **Keyword.TokenVerifierEnabled**.
- 4 Modificare il valore **false** (impostazione predefinita) e impostarlo su **true**.
Se si imposta il parametro del server `Keyword.TokenVerifierEnabled` su **true**, viene attivata la convalida dei token per il rilevamento delle parole chiave CJK.
- 5 **Salvare** la configurazione del server di rilevamento.
- 6 **Riciclare** il server di rilevamento.
- 7 Configurare una condizione di parola chiave utilizzando la corrispondenza di parole intere.
Nella condizione è selezionata l'opzione **Cerca corrispondenza solo con parole intere**.
Vedere ["Configurazione della condizione Contenuto corrispondente a parola chiave"](#) a pagina 779.

Aggiornamento degli elenchi di parole chiave Medicinali, Malattie e Cure per le politiche HIPAA e Caldicott

Se è stata creata una politica derivata dal modello Caldicott o HIPAA e non sono state apportate modifiche o personalizzazioni alla politica derivata, dopo l'aggiornamento è possibile creare una nuova politica dal modello appropriato e rimuovere la politica precedente dalla produzione. Se sono state apportate modifiche a una politica derivata dal modello di politica HIPAA o

Caldicott e si desidera conservare tali modifiche, è possibile copiare gli elenchi di parole chiave aggiornati dal modello di politica HIPAA o Caldicott e utilizzare gli elenchi di parole chiave copiati per aggiornare le politiche HIPAA o Caldicott.

Vedere ["Informazioni sugli aggiornamenti degli elenchi relativi a medicinali, malattie e cure"](#) a pagina 777.

Vedere ["Aggiornamento degli elenchi di parole chiave per le politiche HIPAA e Caldicott."](#) a pagina 785.

La [Per aggiornare gli elenchi di parole chiave Medicinali, Malattie e Cure per le politiche HIPAA e Caldicott](#) fornisce istruzioni per l'aggiornamento degli elenchi di parole chiave per le politiche HIPAA e Caldicott.

Per aggiornare gli elenchi di parole chiave Medicinali, Malattie e Cure per le politiche HIPAA e Caldicott

- 1 Creare una nuova politica da un modello e scegliere il modello HIPAA o Caldicott.
Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.
- 2 Modificare le regole di rilevamento per la politica.
Vedere ["Configurazione di regole di politica"](#) a pagina 427.
- 3 Selezionare la regola **Dati paziente e parole chiave medicinali (Corrispondenza parole chiave)**.
- 4 Selezionare la condizione **Contenuto corrispondente a parola chiave**.
- 5 Selezionare tutte le parole chiave nel campo dati **Corrispondenza con qualsiasi parola chiave** e copiarle negli Appunti.
- 6 Incollare le parole chiave copiate in un file di testo denominato `Drug Keywords.txt`.
- 7 Annullare l'operazione di modifica della regola per tornare alla scheda **Rilevamento** della politica.
- 8 Ripetere lo stesso procedimento per la regola **Dati paziente e parole chiave medicinali (Corrispondenza parole chiave)**.
- 9 Copiare e incollare le parole chiave dalla condizione a un file di testo denominato `Treatment Keywords.txt`.
- 10 Ripetere lo stesso procedimento per la regola **Dati paziente e parole chiave malattia (Corrispondenza parole chiave)**.
- 11 Copiare e incollare le parole chiave dalla condizione a un file di testo denominato `Disease Keywords.txt`.
- 12 Aggiornare le politiche HIPAA e Caldicott derivate dai modelli HIPAA o Caldicott mediante i file `*.txt` di parole chiave creati.
- 13 Verificare le politiche HIPAA e Caldicott aggiornate.

Best practice per l'utilizzo della corrispondenza di parole chiave

La condizione **Contenuto corrispondente a parola chiave** consente di cercare la corrispondenza di contenuto mediante l'uso di parole chiave, frasi chiave ed elenchi di parole chiave o dizionari. Sul server, la regola di parola chiave cerca la corrispondenza con l'intestazione, l'oggetto, il corpo e i componenti del messaggio allegato e supporta la corrispondenza di componenti incrociati. Sull'endpoint la condizione di parola chiave cerca la corrispondenza con l'intero messaggio.

La [Tabella 28-9](#) riepiloga le best practice per la corrispondenza di parole chiave in questa sezione.

Tabella 28-9 Riepilogo delle best practice per la corrispondenza di parole chiave

Best practice	Ulteriori informazioni
Attivare la convalida linguistica per il rilevamento di parole chiave CJK sul server.	Vedere "Attivazione della verifica dei token sul server per ridurre i falsi positivi per il rilevamento delle parole chiave CJK" a pagina 784.
Aggiornare gli elenchi di parole chiave per le politiche Caldicott e HIPAA.	Vedere "Aggiornamento degli elenchi di parole chiave per le politiche HIPAA e Caldicott." a pagina 785.
Ottimizzare le convalide delle parole chiave per migliorare la precisione degli identificatori dati.	Vedere "Ottimizzazione degli elenchi di parole chiave per gli identificatori dati per migliorare la precisione della corrispondenza" a pagina 785.
Utilizzare il VML per creare un profilo per gli elenchi lunghi di parole chiave e i dizionari.	Vedere "Utilizzo di VML per generare e mantenere grandi dizionari di parole chiave" a pagina 786.
Utilizzare la corrispondenza di parole chiave per il rilevamento di metadati.	Vedere "Utilizzo della corrispondenza con parole chiave per il rilevamento di metadati del documento" a pagina 786.

Attivazione della verifica dei token sul server per ridurre i falsi positivi per il rilevamento delle parole chiave CJK

Symantec Data Loss Prevention consente di eseguire la convalida dei token per il cinese, il giapponese e il coreano. La convalida dei token è supportata per i server di rilevamento e deve essere attivata.

Vedere ["Informazioni sulla corrispondenza di parole chiave per le lingue cinese, giapponese e coreano \(CJK\)"](#) a pagina 772.

La convalida dei token consente di trovare parole chiave in cinese, giapponese e coreano utilizzando la corrispondenza di parole intere e migliora la precisione della corrispondenza globale per tali lingue. Sebbene le prestazioni possano risentirne, è necessario attivare la

verifica dei token per ciascun server di rilevamento in cui sono distribuite le condizioni di parole chiave in cinese, giapponese e coreano. Dopo l'attivazione della verifica è possibile utilizzare la corrispondenza di parole intere per le parole chiave CJK.

Vedere ["Attivazione e utilizzo della verifica dei token CJK per la corrispondenza di parole chiave sul server"](#) a pagina 781.

Aggiornamento degli elenchi di parole chiave per le politiche HIPAA e Caldicott.

Per ogni release di Symantec Data Loss Prevention, gli elenchi di parole chiave per medicinali, malattie e cure vengono aggiornati con elenchi di parole chiave corrispondenti a medicinali, malattie e cure basate su informazioni della FDA (Federal Drug Administration) degli Stati Uniti e di altre fonti. Tali elenchi di parole chiave sono utilizzati nei modelli di politica **HIPAA e HITECH (incluso PHI)** e **Relazione Caldicott**.

Vedere ["Informazioni sugli aggiornamenti degli elenchi relativi a medicinali, malattie e cure"](#) a pagina 777.

Se è stato effettuato l'aggiornamento alla versione più recente di Data Loss Prevention e si dispone di politiche esistenti derivate dal modello di politica HIPAA o Caldicott, può risultare utile aggiornare le politiche HIPAA e Caldicott per l'utilizzo degli elenchi di parole chiave per medicinali, malattie e cure forniti con la versione corrente di Data Loss Prevention.

Vedere ["Aggiornamento degli elenchi di parole chiave Medicinali, Malattie e Cure per le politiche HIPAA e Caldicott"](#) a pagina 782.

Ottimizzazione degli elenchi di parole chiave per gli identificatori dati per migliorare la precisione della corrispondenza

Molte definizioni di identificatori dati contengono le convalide delle parole chiave necessarie con elenchi di parole chiave precompilati. Inoltre è possibile aggiungere il proprio elenco di parole chiave a una regola di identificatore dati. La best practice consiste nell'ottimizzare l'elenco di parole chiave con una condizione di corrispondenza di parole chiave prima di aggiungere l'elenco di parole chiave alla condizione di identificatore dati come convalida obbligatoria oppure opzionale.

Vedere ["Utilizzo delle convalide criterio"](#) a pagina 755.

Per ottimizzare l'elenco di parole chiave, individuare le parole chiave che si desidera utilizzare per la convalida e inserirle in una politica e una condizione di regola di corrispondenza di parole chiave separate. Quindi testare la politica utilizzando i dati che devono e non devono corrispondere alle parole chiave. La regola di parola chiave consente di visualizzare l'evidenziazione della corrispondenza e ottimizzare l'elenco di parole chiave. Dopo il test è possibile aggiungere le parole chiave all'identificatore dati e quindi verificare la politica di identificatore dati per garantire la precisione.

Utilizzo della corrispondenza con parole chiave per il rilevamento di metadati del documento

Symantec Data Loss Prevention supporta il rilevamento di metadati per determinati formati di documento, quali DOCX e PDF. I server di rilevamento e i DLP Agent supportano il rilevamento di metadati.

Per individuare metadati del documento, è consigliabile attivarli per il server o l'endpoint e di utilizzare la condizione **Contenuto corrispondente a parola chiave** per la corrispondenza con i tag di metadati.

Utilizzo di VML per generare e mantenere grandi dizionari di parole chiave

A volte è consigliabile proteggere un lungo elenco o un dizionario di parole chiave. Un esempio potrebbe essere un elenco di nomi in codice di progetti. È possibile usare Vector Machine Learning (VML) per automatizzare il rilevamento di lunghi elenchi di parole chiave che sono difficili da generare, ottimizzare e mantenere. Ad esempio, è possibile generare un profilo VML basato su una raccolta di documenti che contengono le parole chiave che si desidera rilevare. Se si desidera rilevare parole comuni, rimuoverle dal file delle parole non significative VML.

Vedere ["Procedure ottimali per l'utilizzo di VML"](#) a pagina 653.

Rilevamento del contenuto mediante espressioni regolari

Il capitolo contiene i seguenti argomenti:

- [Introduzione alla corrispondenza con espressioni regolari](#)
- [Informazioni sul motore aggiornato di espressione regolare](#)
- [Informazioni sulla scrittura di espressioni regolari](#)
- [Configurazione della condizione Contenuto corrispondente a espressione regolare](#)
- [Best practice per l'utilizzo della corrispondenza di espressioni regolari](#)

Introduzione alla corrispondenza con espressioni regolari

Data Loss Prevention fornisce la condizione di corrispondenza di politiche **Contenuto corrispondente a espressione regolare** per cercare la corrispondenza nel contenuto dei messaggi utilizzando espressioni regolari.

Le espressioni regolari forniscono un meccanismo di identificazione di stringhe di testo, come particolari caratteri, parole o criteri di caratteri. È possibile utilizzare la condizione con espressioni regolari per cercare la corrispondenza (o escludere dalla corrispondenza) di caratteri, criteri e stringhe. Il conteggio delle corrispondenze uniche è supportato per le espressioni regolari.

Vedere ["Utilizzo del totale corrispondenze univoche"](#) a pagina 723.

Vedere ["Configurazione della condizione Contenuto corrispondente a espressione regolare"](#) a pagina 789.

Vedere ["Best practice per l'utilizzo della corrispondenza di espressioni regolari"](#) a pagina 791.

Informazioni sul motore aggiornato di espressione regolare

I server di rilevamento e gli agenti di endpoint utilizzano un motore comune di espressione regolare. Questo motore comune esegue la valutazione di espressione regolare più velocemente dei motori precedenti. Si noteranno inoltre miglioramenti delle prestazioni in caso di set di politiche DLP con molte regole regex, poiché l'aggiunta di più regole non rappresenta un alto costo in termini di prestazioni.

Informazioni sulla scrittura di espressioni regolari

Symantec Data Loss Prevention implementa la sintassi delle espressioni regolari compatibili con PCRE per la corrispondenza con le condizioni delle politiche. [Tabella 29-1](#) fornisce alcuni costrutti di riferimento per la scrittura di espressioni regolari per includere o escludere caratteri nei messaggi o nei componenti dei messaggi.

Vedere ["Introduzione alla corrispondenza con espressioni regolari"](#) a pagina 787.

Nota: La corrispondenza con i criteri di identificatore di dati è basata sulla sintassi dell'espressione regolare. Tuttavia, non tutti i costrutti delle espressioni regolari elencati nella tabella seguente sono supportati dai criteri di identificatore di dati. Vedere ["Informazioni sui criteri dell'identificatore dati"](#) a pagina 695.

Tabella 29-1 Costrutti di espressioni regolari

Costrutto di espressioni regolari	Descrizione
.	Qualsiasi singolo carattere (salvo i caratteri di nuova riga) Nota: L'uso del carattere punto (.) non è supportato per i criteri di identificatore di dati.
\d	Qualsiasi cifra (0–9)
\s	Qualsiasi spazio bianco

Costrutto di espressioni regolari	Descrizione
\w	Qualsiasi carattere alfanumerico (a-z, A-Z, 0-9, _) Nota: L'uso del costrutto \w non cerca la corrispondenza con il carattere di sottolineatura (_) quando implementata in un criterio di identificatore di dati.
\D	Qualsiasi cosa all'infuori di una cifra
\S	Qualsiasi cosa all'infuori di uno spazio bianco
[]	Gli elementi tra parentesi quadre sono una classe di caratteri (ad esempio, [abc] cerca la corrispondenza con 1 carattere: a, b o c).
^	All'inizio di una classe di caratteri, la annulla (ad esempio, [^abc] cerca la corrispondenza con qualsiasi cosa tranne a, b o c).
+	Alla fine di un'espressione regolare significa 1 o più (ad esempio, \d+ significa 1 o più cifre).
?	Alla fine di un'espressione regolare significa 0 o 1 (ad esempio, \d? significa 1 o nessuna cifra).
*	Alla fine di un'espressione regolare significa qualsiasi numero (ad esempio, \d* significa 0, 1 o più cifre).
(?i)	All'inizio di un'espressione regolare, disattiva la distinzione maiuscole/minuscole (per impostazione predefinita, le espressioni regolari fanno la distinzione tra maiuscole e minuscole).
(?:)	Raggruppa le espressioni regolari (?: è un leggero potenziamento delle prestazioni).
(?u)	Rende un punto (.) corrispondente anche ai caratteri di nuova riga
	Significa OR (ad esempio, A B significa l'espressione regolare A o l'espressione regolare B).

Configurazione della condizione Contenuto corrispondente a espressione regolare

È possibile utilizzare la condizione **Contenuto corrispondente a espressione regolare** per cercare la corrispondenza (o escludere dalla corrispondenza) caratteri, criteri e stringhe utilizzando le espressioni regolari.

Vedere ["Introduzione alla corrispondenza con espressioni regolari"](#) a pagina 787.

Per configurare la condizione Contenuto corrispondente a espressione regolare

- 1 Aggiungere una condizione **Contenuto corrispondente a espressione regolare** a una politica, o modificarne una esistente.
Vedere ["Configurazione di politiche"](#) a pagina 422.
Vedere ["Configurazione di regole di politica"](#) a pagina 427.
Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.
- 2 Configurare i parametri della condizione **Contenuto corrispondente a espressione regolare**.
Vedere [Tabella 29-2](#) a pagina 790.
- 3 Salvare la configurazione della politica.

Tabella 29-2 Parametri di Contenuto corrispondente a espressione regolare

Azione	Descrizione
Creare corrispondenza con l'espressione regolare.	<p>Specificare un'espressione regolare per la corrispondenza.</p> <p>Vedere "Informazioni sulla scrittura di espressioni regolari" a pagina 788.</p>
Configurare il conteggio delle corrispondenze.	<p>Configurare il metodo di conteggio delle corrispondenze:</p> <p>Vedere "Configurazione del conteggio delle corrispondenze" a pagina 431.</p> <p>Verificare esistenza indica un numero di corrispondenze pari a 1 se vi sono una o più corrispondenze. Per le regole o le eccezioni composte, tutte le condizioni devono essere configurate in questo modo.</p> <p>Contare tutte le corrispondenze indica la somma di tutte le corrispondenze; si applica se una qualunque condizione usa questo parametro.</p>
Creare corrispondenza con uno o più componenti del messaggio.	<p>Configurare la corrispondenza su diversi componenti selezionando una o più componenti dei messaggi in cui cercare la corrispondenza.</p> <ul style="list-style-type: none"> ■ Busta - L'intestazione del messaggio, metadati di trasporto. ■ Oggetto - L'oggetto dell'e-mail (si applica solo ai messaggi e-mail). ■ Corpo - Il contenuto del messaggio. ■ Allegati - Il contenuto di qualsiasi file allegato al messaggio o trasportato dallo stesso. <p>Vedere "Selezione dei componenti per la corrispondenza" a pagina 433.</p>
Cercare la corrispondenza anche con una o più condizioni supplementari.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile dall'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Best practice per l'utilizzo della corrispondenza di espressioni regolari

In questa sezione viene illustrato come implementare la condizione di corrispondenza **Contenuto corrispondente a espressione regolare** nelle politiche di Data Loss Prevention.

Vedere ["Introduzione alla corrispondenza con espressioni regolari"](#) a pagina 787.

La [Tabella 29-3](#) riepiloga le best practice di corrispondenza di espressioni regolari descritte in questa sezione.

Tabella 29-3 Best practice per le espressioni regolari

Best practice	Descrizione
Se possibile, utilizzare gli identificatori dati invece delle espressioni regolari.	Vedere "Utilizzo moderato delle espressioni regolari per prestazioni efficienti" a pagina 792.
Utilizzare le espressioni regolari con moderazione per garantire prestazioni efficienti delle politiche.	Vedere "Verifica delle espressioni regolari prima della distribuzione per migliorare l'accuratezza" a pagina 792.
Utilizzare i caratteri look-ahead e look-behind per migliorare le prestazioni delle espressioni regolari.	Vedere "Utilizzo dei caratteri look-ahead e look-behind per migliorare la precisione delle espressioni regolari" a pagina 791.
Testare le espressioni regolari per verificarne precisione e prestazioni.	Vedere "Verifica delle espressioni regolari prima della distribuzione per migliorare l'accuratezza" a pagina 792.

Quando utilizzare la corrispondenza di espressioni regolari

Gli identificatori dati sono più efficienti delle espressioni regolari, perché i criteri Identificatore dati sono adattati per ottenere la massima accuratezza e i dati sono convalidati. Se ad esempio si desidera cercare i numeri della previdenza sociale, utilizzare l'identificatore dati Social Security Number (SSN) statunitense anziché un'espressione regolare.

La condizione espressione regolare è utile per la corrispondenza o l'esclusione di tipi di dati univoci, per i quali non sono disponibili identificatori dati forniti dal sistema. Esempi di tali tipi di dati possono essere i numeri di conto interni o tipi di dati che possono variare molto in termini di lunghezza, quali gli indirizzi e-mail.

Utilizzo dei caratteri look-ahead e look-behind per migliorare la precisione delle espressioni regolari

Symantec Data Loss Prevention implementa un miglioramento importante per ottimizzare le prestazioni delle espressioni regolari. Per migliorare le prestazioni delle espressioni regolari,

le sezioni look-ahead e look-behind devono corrispondere esattamente a una delle sezioni standard supportate.

La [Tabella 29-4](#) elenca le sezioni look-ahead e look-behind standard supportate da questo miglioramento delle prestazioni. Se una delle sezioni differisce leggermente, viene eseguita nell'ambito dell'espressione regolare senza il miglioramento delle prestazioni.

Vedere ["Informazioni sulla scrittura di espressioni regolari"](#) a pagina 788.

Tabella 29-4 Sezioni look-ahead e look-behind standard

Operazione	Costrutto
Look-ahead	<code>(?= (?: [^-\w]) \$)</code>
Look-behind	<code>(?<= (^ (?: [^]+\d [^-\w+])))</code> <code>e</code> <code>(?<= (^ (?: [^]+\d [^-\w+]) \t))</code>

Utilizzo moderato delle espressioni regolari per prestazioni efficienti

Le espressioni regolari possono richiedere un livello di elaborazione di calcolo notevole. Se si aggiunge una condizione di espressione regolare, osservare il sistema per un'ora. Assicurarsi che il sistema non rallenti e che non vi siano falsi positivi.

Verifica delle espressioni regolari prima della distribuzione per migliorare l'accuratezza

Se si implementa la corrispondenza mediante espressioni regolari, considerare la possibilità di utilizzare uno strumento di terzi per verificare le espressioni regolari prima di distribuire le regole della politica alla produzione. Lo strumento consigliato è [RegexBuddy](#). Un altro strumento ottimale per la verifica delle espressioni regolari è [RegExr](#).

Rilevamento del contenuto utilizzando la corrispondenza di classificazione

Il capitolo contiene i seguenti argomenti:

- [Introduzione alla corrispondenza di classificazione](#)
- [Tipi di file supportati](#)
- [Funzionamento della corrispondenza dei tag](#)
- [Configurazione della condizione Classificazione corrispondenze contenuto](#)

Introduzione alla corrispondenza di classificazione

Symantec Data Loss Prevention fornisce la condizione **Classificazione corrispondenze contenuto** per il rilevamento dei tag Information Centric Tagging applicati al contenuto di vari file ed e-mail.

Un tag comprende tre componenti: organizzazione, ambito e livello di sensibilità. Un esempio potrebbe essere: Symantec-Marketing-Confidenziale, oppure, in formato tag, SYMC-MKTG-CONF. L'organizzazione può corrispondere all'intera azienda o alle divisioni logiche all'interno di un'azienda. Per ambito si intende in genere un gruppo funzionale, ad esempio Paghe o Progettazione. Il livello di sensibilità dei dati contrassegnati varia da 1 a 9, dove 1 indica il livello di sensibilità più basso. I tag vengono definiti da un amministratore ICT, che potrebbe utilizzare termini significativi per l'organizzazione. Ad esempio, l'amministratore

potrebbe chiamare il livello 1 PUBBLICO, il livello 4 RISERVATO e il livello 9 TOPSECRET. La raccolta di tutti i tag comprende la tassonomia di classificazione.

Per utilizzare questa tassonomia ICT in Data Loss Prevention, è necessario importarla nel database di Data Loss Prevention. La tassonomia è disponibile quando viene definita la regola di rilevamento utilizzando l'opzione *Classificazione corrispondenze contenuto*.

Nell'area **Condizioni** per questa opzione della regola, sono disponibili tre opzioni per i criteri di rilevamento: **Contenuto classificato**, **Contenuto non classificato** e **Corrispondenze contenuto**. Se si seleziona **Corrispondenze contenuto**, la tassonomia può essere selezionata nei menu a discesa in **Organizzazione**, **Ambito** e **Livello**. È inoltre possibile selezionare **Qualsiasi** ambito o organizzazione. Per completare la formula di rilevamento, è necessario selezionare l' **Operatore** di ricerca, ad esempio **È diverso da** o **È minore o uguale a**. È possibile combinare operatori multipli (" **OR** " insieme).

Nota: L'espressione **Contenuto classificato** viene attivata solo se il file o il messaggio di posta elettronica è stato classificato all'interno della tassonomia importata. Se un file o un messaggio di posta elettronica è stato classificato utilizzando un'altra tassonomia non importata in Enforce, questa espressione non viene valutata come "true". Analogamente, quello che è stato classificato all'interno di un'altra tassonomia Information Centric Tagging non nota a Enforce viene valutato come **Contenuto non classificato**.

Per rilevare questi tag, il motore di rilevamento di Data Loss Prevention cerca i metadati di e-mail e file supportati. Prima dell'esecuzione della ricerca, gli utenti finali hanno applicato i tag a vari file ed e-mail.

Vedere ["Informazioni sull'integrazione di Information Centric Tagging con Data Loss Prevention"](#) a pagina 231.

Tipi di file supportati

Data Loss Prevention cerca i tag solo nei tipi di file e nei messaggi e-mail supportati. Per i tipi di file supportati, consultare [Tabella 30-1](#).

Tabella 30-1 Tipi di file supportati per la corrispondenza di classificazione

Tipo di file	Formati supportati
Microsoft Office	<ul style="list-style-type: none"> ■ Pre-Office 2007 (CFB) ■ Office 2007 e versioni successive (XML)
Immagini	.png, .gif
PDF	.pdf

Tipo di file	Formati supportati
--------------	--------------------

I file includono allegati di e-mail.

Nessun rilevamento tag eseguito:

- Solo tipi di file supportati a livello nativo da Information Centric Tagging, ma illeggibili da Data Loss Prevention (.jpg, .tiff).
- Con tipi di file non supportati a livello nativo da Information Centric Tagging, dove il tag di classificazione si trova nel flusso di dati alternativo.
- Su dati crittografati, a meno che DLP non sia configurato per eseguire l'ispezione dei *file protetti Microsoft Rights Management*, tra cui documenti MS Office e PDF per la valutazione della politica.

Nota: Anche se i tag possono essere rilevati nei metadati (non crittografati), uno scenario comune per l'utilizzo dell'opzione **Classificazione corrispondenze contenuto** consiste nel combinare questa opzione con le altre opzioni, ad esempio utilizzando la corrispondenza di parole chiave o espressioni regolari per il rilevamento di contenuti riservati, quali i numeri di previdenza sociale. Quindi, se viene rilevato un file con un tag di livello 1 (PUBBLICO), ad esempio, ma il contenuto del documento è riservato, potrebbe essere generato un incidente. Se il contenuto è crittografato, tale tipo di politica che utilizza regole composte non riesce.

Funzionamento della corrispondenza dei tag

Per l'opzione **Classificazione corrispondenze contenuto**, sono disponibili tre scelte:

- **Contenuto classificato**
- **Contenuto non classificato**
- **Corrispondenze contenuto** (**Seleziona operatore**, **Seleziona organizzazione**, **Seleziona ambito**, **Seleziona livello**)

Per capire il funzionamento della corrispondenza dei tag quando vengono cercati tipi di file o e-mail supportati, consultare la tabella seguente.

Nota: Nelle tabelle, il termine *questa tassonomia* fa riferimento alla tassonomia che è stata importata/sincronizzata su questo Enforce Server.

Tabella 30-2 Risultati della ricerca della condizione Contenuto classificato

Vengono generati incidenti quando	Non vengono generati incidenti quando
Il tag appartiene a questa tassonomia.	<ul style="list-style-type: none"> Il tag appartiene a una tassonomia differente. Non ci sono tag di classificazione applicati al contenuto. Il formato del tag è errato.

Tabella 30-3 Risultati della ricerca della condizione Contenuto non classificato

Vengono generati incidenti quando	Non vengono generati incidenti quando
<ul style="list-style-type: none"> Il tag appartiene a una tassonomia differente. Non ci sono tag di classificazione applicati al contenuto. Il formato del tag è errato. 	Il tag appartiene a questa tassonomia.

Tabella 30-4 Risultati della ricerca della condizione Corrispondenze contenuto [specifici operatori e tag selezionati]

Vengono generati incidenti quando	Non vengono generati incidenti quando
Il tag ICT soddisfa i criteri.	<ul style="list-style-type: none"> Il tag in questa tassonomia non corrisponde ai criteri. Il tag appartiene a una tassonomia differente. Non ci sono tag di classificazione applicati al contenuto. Il formato del tag è errato.

[Tabella 30-5](#) elenca un esempio di una tassonomia di classificazione importata, visualizzato nella pagina **Sistema > Impostazioni > Information Centric Tagging**.

[Tabella 30-6](#) mostra i risultati dell'esecuzione di diverse combinazioni di operatori e selezioni di tag rispetto alla tassonomia dalla pagina **Configura politica - Aggiungi regola** o dalla pagina **Configura politica - Modifica regola**, quando viene definita una regola di rilevamento di tipo **Classificazione corrispondenze contenuto**.

Tabella 30-5 Esempio di tassonomia di classificazione ICT importata

Organizzazione	Ambito	Sensibilità	Livello
CLOUD			
	ENG		
		CONFID	4

Organizzazione	Ambito	Sensibilità	Livello
		LIMITA	3
		INTERNO	2
CORE			
	FIN		
		SEGRETO	5
	HR		
		PUB	1
	MKTG		
		CONFID	4
		PUB	1
IN USCITA			
	ENG		
		SEGRETO	4
		CONFID	3
		DEPTONLY	2

Tabella 30-6 Incidenti valutati come true, in base all'operatore e ai requisiti di corrispondenza

Operatore	Organizzazione	Ambito	Livello
È uguale a	CLOUD	Qualsiasi	2
<i>Restituisce true se il contenuto è classificato come:</i>			
			(2) INTERNO
È uguale a	CORE	Qualsiasi	(4) CONFID
<i>Restituisce true se il contenuto è classificato come:</i>			

Operatore	Organizzazione	Ambito	Livello
	CORE	MKTG	(4) CONFID
È diverso da	CORE	MKTG	1
<i>Restituisce true se il contenuto è classificato come:</i>			
	CLOUD	ENG	(4) CONFID
	CLOUD	ENG	(3) LIMITA
	CLOUD	ENG	(2) INTERNO
	CORE	FIN	(5) SEGRETO
	IN USCITA	ENG	(4) SEGRETO
	IN USCITA	ENG	(3) CONFID
	IN USCITA	ENG	(2) DEPTONLY
È minore o uguale a	CORE	FIN	(5) SEGRETO
<i>Restituisce true se il contenuto è classificato come:</i>			
	CORE	FIN	(5) SEGRETO
È maggiore di o uguale a	IN USCITA	ENG	(3) CONFID
<i>Restituisce true se il contenuto è classificato come:</i>			
	IN USCITA	ENG	(4) SEGRETO
	IN USCITA	ENG	(3) CONFID

Configurazione della condizione **Classificazione corrispondenze contenuto**

Per configurare la condizione **Classificazione corrispondenze contenuto**

- 1 Aggiungere una condizione **Classificazione corrispondenze contenuto** a una politica o modificarne una esistente.
- 2 Nell'area **Condizioni**, impostare i parametri:
 - Configurare la condizione **Classificazione corrispondenze contenuto** ([Tabella 30-7](#)).
 - Per il parametro relativo alle **corrispondenze**, **Busta e Allegati** sono sempre selezionati; **Oggetto** e **Corpo** non sono mai selezionati.
- 3 Salvare la politica.

Tabella 30-7 Parametri di Classificazione corrispondenze contenuto

Parametro	Descrizione
Contenuto classificato	Vedere " Funzionamento della corrispondenza dei tag " a pagina 795.
Contenuto non classificato	Vedere " Funzionamento della corrispondenza dei tag " a pagina 795.
Corrispondenze contenuto:	Vedere " Funzionamento della corrispondenza dei tag " a pagina 795.

Parametro	Descrizione
Seleziona operatore	<p>Scegliere un operatore: È uguale a, È diverso da, È minore o uguale a o È maggiore di o uguale a.</p> <p>Nota: Man mano che la tassonomia di classificazione ICT si evolve, l'uso di "È minore di..." o "È maggiore di..." rende l'opzione della regola di rilevamento più duratura. Questi termini comparativi consentono la ricerca classificazioni attuali e future. Se si scrive ogni regola usando "È uguale a", potrebbe essere necessario rivedere spesso le regole.</p>
Seleziona organizzazione	<p>Scegliere un'organizzazione dal menu a discesa, che contiene le organizzazioni importate della tassonomia ICT. È anche possibile scegliere Qualsiasi.</p> <p>Tenere presente che il termine <i>Organizzazione</i> in Data Loss Prevention è riportato come <i>Azienda</i> in Information Centric Tagging.</p>
Seleziona ambito	<p>Scegliere un ambito dal menu a discesa, che contiene gli ambiti importati della tassonomia ICT. È anche possibile scegliere Qualsiasi.</p>

Parametro	Descrizione
Seleziona livello	<p>Scegliere un livello dal menu a discesa, che contiene i livelli di sensibilità importati della tassonomia ICT.</p> <ul style="list-style-type: none"> ■ Se sono stati selezionato un Organizzazione e Ambito specifici, il menu Livello include il livello di sensibilità e il nome, come (1) PUBLIC, (4) CONF e (9) TOPSECRET. ■ Se è stato selezionato Qualsiasi per Organizzazione e Ambito, il menu Livello mostra solo i numeri di livello, da 1 a 9, poiché i nomi dei livelli potrebbero differire tra i vari ambiti. ■ Il Livello viene confrontato solo se i requisiti di Organizzazione e Ambito vengono soddisfatti.
OR	<p>Fare clic su OR per aggiungere un'altra selezione di Operatore, Organizzazione, Ambito e Livello. È possibile aggiungere più istruzioni OR per una regola. Le istruzioni OR sono valutate singolarmente; non devono essere tutte true per creare un incidente.</p>

Rilevamento del contenuto di lingua internazionale

Il capitolo contiene i seguenti argomenti:

- [Rilevazione del contenuto in lingua non inglese](#)
- [Best practice per il rilevamento di contenuti non in inglese](#)

Rilevazione del contenuto in lingua non inglese

Le funzionalità di rilevamento Symantec Data Loss Prevention supportano molte versioni localizzate dei sistemi operativi Microsoft Windows. Per usare i set di caratteri internazionali, il sistema di Windows su cui viene visualizzata la console di amministrazione di Enforce Server deve presentare funzionalità appropriate.

Vedere ["Informazioni sul supporto per impostazioni internazionali, lingue e set di caratteri"](#) a pagina 89.

Vedere ["Utilizzo di caratteri internazionali"](#) a pagina 92.

È possibile creare politiche e rilevare violazioni utilizzando qualsiasi lingua supportata. Per individuare una perdita di dati, è possibile usare parole chiave, espressioni regolari e profili dati localizzati. Inoltre, Symantec Data Loss Prevention offre diversi identificatori di dati e modelli di politica internazionali per la protezione dei dati confidenziali.

Vedere ["Lingue supportate per il rilevamento "](#) a pagina 90.

Vedere ["Utilizzo di modelli di politica internazionali per la creazione di politiche"](#) a pagina 803.

Vedere ["Utilizzo di parole chiave personalizzate per gli identificatori di dati del sistema"](#) a pagina 804.

Best practice per il rilevamento di contenuti non in inglese

Questa sezione fornisce alcune best practice per implementare il rilevamento di contenuti non in lingua inglese.

Aggiornamento all'ultima versione di Data Loss Prevention

Symantec Data Loss Prevention versione 14.0 include vari aggiornamenti per il rilevamento di lingue asiatiche, inclusi EDM multitoken e convalida linguistica per parole chiave in cinese, giapponese e coreano (CJK). Per trarre vantaggio da tali miglioramenti, aggiornare i server all'ultima versione e aggiornare i profili dati esatti.

Vedere ["Aggiornamento degli indici EDM alla versione più recente"](#) a pagina 527.

Vedere ["Attivazione della convalida token per la corrispondenza con parole chiave cinesi, giapponesi e coreane sul server"](#) a pagina 806.

Utilizzo di modelli di politica internazionali per la creazione di politiche

Symantec Data Loss Prevention fornisce diversi modelli di politica internazionali che è possibile distribuire rapidamente nell'azienda.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Tabella 31-1 Modelli internazionali di politica

Modello di politica	Descrizione
Numeri di previdenza sociale canadesi (SIN)	Questa politica rileva i criteri indicanti numeri di previdenza sociale canadesi. Vedere "Modello della politica Numeri di previdenza sociale (SIN) canadesi" a pagina 1321.
Relazione Caldicott	Questa politica protegge le informazioni dei pazienti britannici. Vedere "Modello della politica Relazione Caldicott" a pagina 1319.
Data Protection Act britannico, 1998	Questa politica protegge le informazioni personali identificabili. Vedere "Modello della politica Data Protection Act 1998 (legge sulla protezione dei dati del 1998)" a pagina 1327.
Direttive UE sulla protezione dei dati	Questa politica rileva i dati personali a cui si fa riferimento nelle direttive UE. Vedere "Modello della politica Direttive UE sulla protezione dei dati" a pagina 1329.

Modello di politica	Descrizione
Human Rights Act (legge sui diritti umani) britannico del 1998	Questa politica implementa l'articolo 8 della legge per i cittadini britannici. Vedere "Modello di politica Human Rights Act (legge sui diritti umani) del 1998" a pagina 1421.
PIPEDA (Canada)	Questa politica rileva i dati cliente dei cittadini canadesi. Vedere "Modello di politica PIPEDA" a pagina 1439.
Codici SWIFT (attività bancarie internazionali)	Questa politica rileva i codici che le banche utilizzano per trasferire denaro oltre i confini nazionali. Vedere "Modello della politica Codici SWIFT" a pagina 1455.
Numeri delle patenti di guida britanniche	Questa politica rileva i numeri delle patenti di guida britanniche. Vedere "Modello della politica Numeri Patente di guida del Regno Unito" a pagina 1456.
Numeri di tessera elettorale britannici	Questa politica rileva i numeri delle tessere elettorali britanniche. Vedere "Modello politica Numeri di tessera elettorale britannici" a pagina 1456.
Numeri di previdenza sociale britannici	Questa politica rileva i numeri di previdenza sociale britannici. Vedere "Modello della politica Numeri di previdenza sociale britannici" a pagina 1457.
Numero NHS (National Health Service) britannico	Questa politica rileva i numeri di identificazione personale rilasciati dal servizio sanitario nazionale (NHS) britannico. Vedere "Modello della politica Numero NHS (National Health Service) britannico" a pagina 1457.
Numeri di passaporto britannici	Questa politica rileva i passaporti britannici validi. Vedere "Modello della politica Numeri di passaporto britannici" a pagina 1457.
Codici fiscali britannici	Questa politica rileva i codici fiscali britannici. Vedere "Modello di politica Codici fiscali britannici" a pagina 1458.

Utilizzo di parole chiave personalizzate per gli identificatori di dati del sistema

Gli identificatori di dati offrono un ampio supporto per il rilevamento di contenuto internazionale.
Vedere ["Introduzione agli identificatori di dati"](#) a pagina 681.

Alcuni identificatori dati internazionali offrono solo una copertura di rilevamento ampia. In questo caso è possibile implementare la convalida opzionale Trova parole chiave per limitare

l'ambito di rilevamento. L'implementazione di questa convalida opzionale può contribuire a eliminare eventuali falsi positivi corrispondenti alla politica.

Vedere ["Selezione di una copertura dell'identificatore di dati"](#) a pagina 703.

La seguente tabella fornisce parole chiave per vari identificatori di dati internazionali.

Per usare parole chiave internazionali per identificatori di dati del sistema

- 1 Creare una politica utilizzando uno degli identificatori di dati internazionali forniti dal sistema elencati nella tabella.

[Tabella 31-2](#)

- 2 Selezionare la convalida opzionale **Trova parole chiave**.

Vedere ["Configurazione della condizione Contenuto corrispondente a identificatore dati"](#) a pagina 700.

- 3 Copiare e incollare le parole chiave separate da virgola appropriate dall'elenco nel campo di convalida opzionale **Trova parole chiave**.

Vedere ["Configurazione delle convalide opzionali"](#) a pagina 720.

Tabella 31-2 Elenco di identificatori di dati e parole chiave internazionali

Identificatore dati	Lingua	Parole chiave	Traduzione
Burgerservicenummer (BSN)	Olandese	Persoonsnummer, sofinummer, sociaal-fiscaal nummer, persoonsgebonden	numero persona, numero sociale-fiscale (abbreviazione), numero sociale-fiscale, numero associato alla persona
Codice Fiscale	Italiano	codice fiscale, dati anagrafici, partita I.V.A., p. iva	
Codice INSEE francese	Francese	INSEE, numéro de sécu, code sécu	INSEE, numero della previdenza sociale, codice di previdenza sociale
ID Hong Kong	Cinese (tradizionale)	身份證, 三顆星	Carta di identità, carta di identità di residente permanente di Hong Kong
Codice International Bank Account Number (IBAN) paesi centrali	Francese	Code IBAN, numéro IBAN	Codice IBAN, numero IBAN
Codice International Bank Account Number (IBAN) paesi orientali	Francese	Code IBAN, numéro IBAN	Codice IBAN, numero IBAN

Identificatore dati	Lingua	Parole chiave	Traduzione
Codice International Bank Account Number (IBAN) paesi occidentali	Francese	Code IBAN, numéro IBAN	Codice IBAN, numero IBAN
Documento di identità cinese	Cinese (semplificato)	身份证, 居民信息, 居民身份证	Carta di identità, Informazioni del residente, Informazioni di identificazione residente
Resident Registration Number (RRN, numero di registrazione anagrafica) sudcoreano	Coreano	주민등록번호, 주민번호	Numero di registrazione residente, numero residente
Numero di DNI spagnolo	Spagnolo	DNI	DNI
Numero AHV svizzero	Francese	Numéro AVS, numéro d'assuré, identifiant national, numéro d'assurance vieillesse, numéro de sécurité sociale, Numéro AVH	Numero AVS, numero di assicurazione, identificatore nazionale, numero di previdenza sociale, numero della previdenza sociale, numero AVH
	Tedesco	AHV-Nummer, Matrikelnummer, Personenidentifikationsnummer	Numero AHV, numero di matricola svizzero, PIN
	Italiano	AVS, AVH	
ID Taiwan	Cinese (tradizionale)	中華民國國民身分證	ID Taiwan

Attivazione della convalida token per la corrispondenza con parole chiave cinesi, giapponesi e coreane sul server

La condizione **Contenuto corrispondente a parola chiave** supporta la corrispondenza sia con l'intera parola sia con una parte della parola.

I server di rilevazione Symantec Data Loss Prevention supportano l'elaborazione del linguaggio naturale per le parole chiave in cinese, giapponese e coreano (CJK). Per individuare le parole chiave CJK si consiglia di attivare la convalida token sul server di rilevazione e quindi di utilizzare la corrispondenza con la parola intera come condizione per la parola chiave.

DLP Agent non supporta la convalida token per CJK. Sull'endpoint, per la corrispondenza con parole chiave CJK e in lingue miste, considerare la possibilità di utilizzare la corrispondenza parziale.

Con la corrispondenza parola intera le parole chiave rilevano la corrispondenza esclusivamente sui limiti della parola (l'W nel lessico dell'espressione regolare). Tutti i caratteri all'infuori di

A-Z, a-z e 0-9 sono interpretati come limiti della parola. Con la corrispondenza parola intera le parole chiave devono includere almeno un carattere alfanumerico (una lettera o un numero). Una parola chiave costituita solo da caratteri spazio, come ".." viene ignorata.

Vedere ["Informazioni sulla corrispondenza di parole chiave per le lingue cinese, giapponese e coreano \(CJK\)"](#) a pagina 772.

Rilevamento delle proprietà di file

Il capitolo contiene i seguenti argomenti:

- [Introduzione al rilevamento di proprietà di file](#)
- [Configurazione della corrispondenza delle proprietà del file](#)
- [Best practice per l'utilizzo di corrispondenza delle proprietà file](#)

Introduzione al rilevamento di proprietà di file

Symantec Data Loss Prevention fornisce vari metodi per il rilevamento del contesto di messaggi, file e allegati. È possibile rilevare, tipo, dimensione e nome di file e allegati. È anche possibile usare queste condizioni per escludere file e allegati dalla corrispondenza.

Vedere ["Informazioni sulla corrispondenza con tipi di file"](#) a pagina 808.

Vedere ["Informazioni sulla corrispondenza di dimensione di file"](#) a pagina 810.

Vedere ["Informazioni sulla corrispondenza del nome del file"](#) a pagina 811.

Vedere ["Configurazione della corrispondenza delle proprietà del file"](#) a pagina 811.

Informazioni sulla corrispondenza con tipi di file

Per la corrispondenza con il tipo di file dell'allegato di un messaggio, si utilizza la condizione **Corrispondenza allegato messaggio o tipo file**. Symantec Data Loss Prevention supporta l'identificazione di oltre 300 tipi di file.

Vedere ["Formati supportati per l'identificazione dei tipi di file"](#) a pagina 878.

Gli esempi di corrispondenza tra allegato e tipo di file sono:

- Un certo tipo di documento non deve mai lasciare l'organizzazione (come un documento PGP o un file AutoCAD).
- Un certo tipo di corrispondenza è probabile che acceda solo in un documento di un certo tipo, come un documento Word.

Il motore di rilevamento non considera l'estensione del file per identificare il tipo di formato di file. Ad esempio, se un utente cambia l'estensione del file **.mp3** in **.doc** e invia il file via e-mail, il motore di rilevamento può ancora registrare una corrispondenza perché controlla la firma binaria del file per rilevarlo come file MP3.

Nota: La corrispondenza con il tipo di file non rileva il contenuto del file; rileva solo il tipo di file basato sulla relativa firma binaria. Per rilevare il contenuto, utilizzare una condizione di corrispondenza contenuto.

Vedere ["Configurazione della condizione Corrispondenza allegato messaggio o tipo file."](#) a pagina 812.

Vedere ["Informazioni sull'identificazione di tipi di file personalizzati"](#) a pagina 809.

Informazioni sul supporto dei formati di file per la corrispondenza dei tipi di file

Symantec Data Loss Prevention supporta oltre 300 formati di file per l'identificazione del tipo di file con la condizione della politica **Corrispondenza allegato messaggio o tipo file**.

Fare riferimento al collegamento seguente per un elenco completo dei formati di file che possono essere riconosciuti da questa condizione della politica.

Vedere ["Formati supportati per l'identificazione dei tipi di file"](#) a pagina 878.

Informazioni sull'identificazione di tipi di file personalizzati

Se il tipo di file che si desidera rilevare non è supportato come tipo di file predefinito del sistema, Symantec Data Loss Prevention consente di identificare i tipi di file personalizzati utilizzando degli script.

Per individuare un tipo di file personalizzato, usare il linguaggio di script di Symantec Data Loss Prevention per creare uno script personalizzato che rileva la firma binaria del formato di file che si desidera proteggere. Per implementare questa condizione di corrispondenza è necessario attivarla su Enforce Server.

Vedere ["Attivazione della condizione Firma tipi di file personalizzati nella console della politica"](#) a pagina 817.

Vedere ["Configurazione della condizione Firma tipi di file personalizzati"](#) a pagina 817.

Fare riferimento alla *Guida alla personalizzazione di Symantec Data Loss Prevention* per la sintassi e gli esempi del linguaggio.

Nota: Il linguaggio di script di Symantec Data Loss Prevention identifica solo i formati di file personalizzati; non estrae contenuto dai tipi di file personalizzati.

Informazioni sulla corrispondenza di dimensione di file

Utilizzare **Corrispondenza allegato messaggio o dimensioni file** per rilevare il contenuto in base alla dimensione di specifici componenti del messaggio e-mail.

Vedere ["Messaggi di rilevamento e componenti di messaggio"](#) a pagina 398.

È anche possibile rilevare le corrispondenze per il numero di file allegati all'e-mail per SMTP.

La condizione scelta quando si configura questa regola determina il rilevamento di una corrispondenza. Scegliere da queste opzioni:

- **Singolo** - Questa condizione rileva una corrispondenza quando il corpo di un messaggio e-mail o di un allegato e-mail raggiunge o supera la dimensione di file specificata. Il rilevamento si basa individualmente su ogni componente.

Ad esempio, è possibile specificare una condizione per la quale la dimensione del singolo file è oltre 50 KB (kilobyte). Un messaggio e-mail con un corpo di 20 KB e un singolo allegato e-mail di 51 KB genera una corrispondenza perché l'allegato rilevato supera i 50 KB. Invece, un messaggio e-mail con un corpo di 20 KB e due allegati e-mail di 20 KB non genera una corrispondenza. Anche se l'intero messaggio supera i 50 KB, ogni componente è di meno di 50 KB. Questa regola non combina la dimensione totale del corpo o dei file allegati all'e-mail.

- **Dimensione totale file allegati** - Questa condizione, solo per SMTP, rileva una corrispondenza quando la dimensione di uno o più allegati e-mail combinati raggiunge o supera i criteri di dimensione di file specificati. Il rilevamento si basa solamente sugli allegati di e-mail e non considera il corpo del messaggio e-mail.

Ad esempio, è possibile specificare una condizione per la quale la dimensione totale dei file è oltre 50 KB (kilobyte). Un messaggio e-mail con un corpo di 20 KB e un singolo allegato e-mail di 40 KB non genera una corrispondenza perché, sebbene l'e-mail totale superi i 50 KB, la condizione non considera il corpo del messaggio e-mail. Invece, un messaggio e-mail con un corpo di 20 KB e due allegati e-mail di 30 KB genera una corrispondenza perché i due file allegati superano i 50 KB. Inoltre, un'e-mail con un file ZIP di 40 KB allegato non genererebbe una corrispondenza, anche se la dimensione dei file estratti all'interno dell'archivio superasse 50 KB.

Il valore predefinito per la condizione **Dimensione totale file allegati** è zero. Questa condizione ha un limite di caratteri di quattro cifre. Si verificheranno errori di convalida se si includono punti decimali o altri caratteri quando si specifica questo valore.

- **Numero totale file allegati** - Questa condizione, solo per SMTP, rileva una corrispondenza quando il numero degli allegati e-mail combinati raggiunge o supera i criteri di numero di file specificati. Il rilevamento si basa solamente sul numero combinato di allegati e-mail diretti. Ad esempio, è possibile specificare una condizione per la quale il numero totale dei file è cinque. Un'e-mail con sei file allegati genererebbe una corrispondenza con questa condizione, ma un'e-mail con un solo file ZIP allegato non la genererebbe, anche se il file ZIP contenesse 20 file.

Il valore predefinito per la condizione **Numero totale file allegati** è zero. Questa condizione ha un limite di caratteri di sette cifre. Si verificheranno errori di convalida se si includono punti decimali o altri caratteri quando si specifica questo valore.

Nota: Se le condizioni **Dimensione totale file allegati** e **Numero totale file allegati** sono unite con AND a una regola di corrispondenza del contenuto, le regole si applicheranno a tutti i componenti del messaggio. I componenti genereranno una corrispondenza con una sola condizione in un incidente, anche se ne violano di più.

Le regole **Dimensione totale file allegati** e **Numero totale file allegati** sono disponibili su endpoint sia Windows sia Mac. In Windows, si applicano agli eventi di Microsoft Outlook e di IBM (Lotus) Notes. In Mac, si applicano agli eventi di Outlook per Mac.

Vedere ["Configurazione della condizione Corrispondenza allegato messaggio o dimensioni file"](#) a pagina 813.

Informazioni sulla corrispondenza del nome del file

Utilizzare la condizione **Corrispondenza allegato messaggio o nome file** per individuare i nomi dei file e degli allegati.

Vedere ["Sintassi di corrispondenza dei nomi di file"](#) a pagina 816.

Vedere ["Esempi di corrispondenza dei nomi file"](#) a pagina 816.

Vedere ["Configurazione della condizione Corrispondenza allegato messaggio o nome file"](#) a pagina 815.

Configurazione della corrispondenza delle proprietà del file

La [Tabella 32-1](#) elenca le condizioni disponibili per l'implementazione della corrispondenza delle proprietà del file.

Tabella 32-1 Condizioni delle corrispondenze delle proprietà del file

Condizione di corrispondenza	Descrizione
Corrispondenza allegato messaggio o tipo file	<p>Rileva o esclude file e allegati specifici in base al tipo.</p> <p>Vedere "Informazioni sulla corrispondenza con tipi di file" a pagina 808.</p> <p>Vedere "Configurazione della condizione Corrispondenza allegato messaggio o tipo file." a pagina 812.</p>
Corrispondenza allegato messaggio o dimensioni file	<p>Rileva o esclude file e allegati specifici in base alle dimensioni.</p> <p>Vedere "Informazioni sulla corrispondenza di dimensione di file" a pagina 810.</p> <p>Vedere "Configurazione della condizione Corrispondenza allegato messaggio o dimensioni file" a pagina 813.</p>
Corrispondenza allegato messaggio o nome file	<p>Rileva o esclude file e allegati specifici in base al nome.</p> <p>Vedere "Informazioni sulla corrispondenza del nome del file" a pagina 811.</p> <p>Vedere "Configurazione della condizione Corrispondenza allegato messaggio o nome file" a pagina 815.</p>
Firma tipi di file personalizzati	Rileva o esclude tipi di file personalizzati.

Configurazione della condizione Corrispondenza allegato messaggio o tipo file.

La condizione **Corrispondenza allegato messaggio o tipo file** cerca la corrispondenza con il tipo di file o un allegato del messaggio. È possibile configurare un'istanza di questa condizione nelle regole e nelle eccezioni di politiche.

Vedere ["Informazioni sulla corrispondenza con tipi di file"](#) a pagina 808.

Per configurare la condizione Corrispondenza allegato messaggio o tipo file

- 1 Aggiungere una condizione **Corrispondenza allegato messaggio o tipo file** a una regola o a un'eccezione della politica o modificarne una esistente.
Vedere ["Configurazione di politiche"](#) a pagina 422.
Vedere ["Configurazione di regole di politica"](#) a pagina 427.
Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.
- 2 Configurare i parametri della condizione **Corrispondenza allegato messaggio o tipo file**.
Vedere [Tabella 32-2](#) a pagina 813.
- 3 Fare clic su **Salva** per salvare la politica.

Tabella 32-2 Parametri della condizione Corrispondenza allegato messaggio o tipo file

Azione	Descrizione
Selezionare il tipo o tipi di file per la corrispondenza.	<p>Selezionare tutti i formati desiderati per la corrispondenza.</p> <p>Vedere "Formati supportati per l'identificazione dei tipi di file" a pagina 878.</p> <p>Fare clic su Seleziona tutto o Deseleziona tutto per selezionare o deselezionare tutti i formati.</p> <p>Per selezionare tutti i formati di una determinata categoria (ad esempio, tutti i formati di elaborazione di testo), fare clic sull'intestazione della sezione.</p> <p>Il sistema implica un operatore OR tra tutti i tipi di file selezionati. Ad esempio, se si selezionano allegati di tipo Microsoft Excel e Microsoft Word, il sistema rileva tutti i messaggi con documenti Word o Excel allegati e non i messaggi con entrambi i tipi di allegati.</p>
Cercare la corrispondenza solo negli allegati.	<p>Questa condizione cerca la corrispondenza solo nel componente Allegati dei messaggi.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p>
Cercare la corrispondenza anche a una o più condizioni supplementari.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile nell'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Configurazione della condizione Corrispondenza allegato messaggio o dimensioni file

La condizione **Corrispondenza allegato messaggio o dimensioni file** fa corrispondere o esclude dalla corrispondenza i file di una dimensione specificata. È possibile configurare un'istanza di questa condizione nelle regole e nelle eccezioni di politiche.

Vedere ["Informazioni sulla corrispondenza di dimensione di file"](#) a pagina 810.

Per configurare la condizione **Corrispondenza allegato messaggio o dimensioni file**

- 1 Aggiungere **Corrispondenza allegato messaggio o dimensioni file** a una politica o modificare una politica che già contiene questa regola.
Vedere ["Configurazione di politiche"](#) a pagina 422.
Vedere ["Configurazione di regole di politica"](#) a pagina 427.
Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.
- 2 Selezionare la condizione **Corrispondenza allegato messaggio o tipo file** :
Vedere [Tabella 32-3](#) a pagina 814.
- 3 Fare clic su **Salva** per salvare la politica.

Tabella 32-3 Parametri di Corrispondenza allegato messaggio o dimensioni file

Azione	Descrizione
Dimensione singolo file	Selezionare Più di per specificare la dimensione minima del file o Meno di per specificare la dimensione massima del file per generare una corrispondenza. Immettere un numero e selezionare l'unità di misura: byte , kilobyte (KB), megabyte (MB) o gigabyte (GB).
Dimensione totale file allegati	Immettere un numero e selezionare l'unità di misura: byte , kilobyte (KB), megabyte (MB) o gigabyte (GB) per generare una corrispondenza.
Numero totale file allegati	Immettere un numero per specificare il numero di file per generare una corrispondenza
Cerca corrispondenza con	Selezionare uno o più dei componenti di messaggi su cui basare la corrispondenza: <ul style="list-style-type: none"> ■ Busta - L'opzione non è applicabile per queste opzioni. ■ Oggetto - L'opzione non è applicabile per queste opzioni. ■ Corpo – Il contenuto del messaggio (questa opzione è applicabile solo a Dimensione singolo file). ■ Allegati - Qualsiasi file allegato al messaggio o inoltrato dallo stesso. Vedere "Selezione dei componenti per la corrispondenza" a pagina 433.
Cercare la corrispondenza anche con una o più condizioni supplementari.	Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente. È possibile aggiungere qualsiasi condizione disponibile nell'elenco. Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.

Configurazione della condizione Corrispondenza allegato messaggio o nome file

La condizione **Corrispondenza allegato messaggio o nome file** richiede la corrispondenza con il nome di un file allegato al messaggio. È possibile configurare un'istanza di questa condizione nelle regole e nelle eccezioni di politiche.

Vedere ["Informazioni sulla corrispondenza del nome del file"](#) a pagina 811.

Per configurare la condizione Corrispondenza allegato messaggio o nome file

- 1 Aggiungere una condizione Corrispondenza allegato messaggio o nome file a una politica, o modificarne una esistente.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Configurazione di regole di politica"](#) a pagina 427.

Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.

- 2 Configurare i parametri della condizione Corrispondenza allegato messaggio o tipo file.

Vedere [Tabella 32-4](#) a pagina 815.

- 3 Fare clic su **Salva** per salvare la politica.

Tabella 32-4 Parametri di Corrispondenza allegato messaggio o nome file

Azione	Descrizione
Specificare il nome di file.	<p>Specificare il nome di file per la corrispondenza utilizzando il linguaggio di corrispondenza criteri DOS per rappresentare i criteri nel nome di file.</p> <p>Separare molteplici criteri di corrispondenza con virgole o disponendoli su righe distinte.</p> <p>Vedere "Sintassi di corrispondenza dei nomi di file" a pagina 816.</p> <p>Vedere "Esempi di corrispondenza dei nomi file" a pagina 816.</p>
Cercare la corrispondenza negli allegati.	<p>Questa condizione cerca la corrispondenza solo nel componente Allegati dei messaggi.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p>
Cercare la corrispondenza anche con una o più condizioni supplementari.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile nell'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Sintassi di corrispondenza dei nomi di file

Per la corrispondenza dei nomi di file, il sistema supporta la sintassi di corrispondenza dei criterio DOS per rilevare i nomi di file, compresi i caratteri jolly.

Vedere ["Informazioni sulla corrispondenza del nome del file"](#) a pagina 811.

Tutti i caratteri immessi (diversi dagli operatori DOS) corrispondono esattamente. Per inserire più nomi di file, immetterli come valori separati da virgola o con un'interlinea.

La [Tabella 32-5](#) descrive la sintassi per la condizione **Corrispondenza allegato messaggio o nome file**.

Tabella 32-5 Operatori DOS per il rilevamento dei nomi di file

Operatore	Descrizione
.	Utilizzare un punto per separare il nome di file e l'estensione.
*	Utilizzare un asterisco come carattere jolly per cercare la corrispondenza con qualsiasi numero di caratteri (anche nessuno).
?	Utilizzare un punto interrogativo per cercare la corrispondenza con un singolo carattere.

Esempi di corrispondenza dei nomi file

La [Tabella 32-6](#) elenca alcuni esempi di rilevamento della corrispondenza dei nomi file con la condizione **Corrispondenza allegato messaggio o nome file**.

Vedere ["Informazioni sulla corrispondenza del nome del file"](#) a pagina 811.

Tabella 32-6 Esempi di corrispondenza dei nomi file

Obiettivo della corrispondenza	Esempio
Per la corrispondenza con un nome di file di Word che inizia con ENG- seguito da otto caratteri qualsiasi:	ENG-?????????.doc
Se non si è certi che si tratti di un documento Word:	ENG-?????????.*
Se non si è certi del numero di caratteri presenti nel nome:	ENG-*.*
Per la corrispondenza con tutti i nomi file che iniziano con ENG- e con tutti i nomi file che iniziano con ITA-:	Immettere come valori separati da virgole: ENG-*,ITA-*
	Oppure separare i nomi file con una riga vuota. ENG-*.*
	ITA-*

Attivazione della condizione Firma tipi di file personalizzati nella console della politica

Per impostazione predefinita, la condizione della politica **Firma tipi di file personalizzati** non è attivata. Per implementare la condizione **Firma tipi di file personalizzati**, è necessario prima attivarla.

Vedere ["Informazioni sull'identificazione di tipi di file personalizzati"](#) a pagina 809.

Per attivare la regola Firma tipi di file personalizzati

- 1 Utilizzando un editor di testo, aprire il file `\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\Manager.properties`
- 2 Impostare il valore del parametro seguente su "true":
`com.vontu.manager.policy.showcustomscriptrule=true`
- 3 Interrompere e riavviare il servizio Symantec DLP Manager.
- 4 Accedere di nuovo alla console di amministrazione di Enforce Server e aggiungere una nuova politica vuota.
- 5 Aggiungere una nuova regola o eccezione di rilevamento. Sotto l'intestazione Proprietà file dovrebbe essere visualizzata la condizione **Firma tipi di file personalizzati**.
- 6 Configurare la condizione con lo script personalizzato.

Vedere ["Configurazione della condizione Firma tipi di file personalizzati"](#) a pagina 817.

Configurazione della condizione Firma tipi di file personalizzati

La condizione **Firma tipi di file personalizzati** cerca la corrispondenza con tipi di file personalizzati inclusi in uno script. È possibile implementare la condizione **Firma tipi di file personalizzati** nelle regole e nelle eccezioni di politiche.

Vedere ["Informazioni sull'identificazione di tipi di file personalizzati"](#) a pagina 809.

Vedere ["Attivazione della condizione Firma tipi di file personalizzati nella console della politica"](#) a pagina 817.

Per configurare una condizione Firma tipi di file personalizzati

- 1 Aggiungere una condizione **Firma tipi di file personalizzati** a una regola o a un'eccezione di politica, oppure modificarne una esistente.
Vedere ["Configurazione di regole di politica"](#) a pagina 427.
Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.
- 2 Configurare i parametri della condizione Firma tipi di file personalizzati.
Vedere [Tabella 32-7](#) a pagina 818.
- 3 Fare clic su **Salva** per salvare la politica.

Tabella 32-7 Parametri di Firma tipi di file personalizzati

Azione	Descrizione
Immettere il nome dello script.	Specificare il nome dello script. Il nome deve essere univoco in tutte le politiche.
Immettere lo script del tipo di file personalizzato.	Immettere lo script Tipo di file corrispondente a firma per rilevare la firma binaria del tipo di file personalizzato. Vedere la <i>Guida alla personalizzazione di Symantec Data Loss Prevention Detection</i> per informazioni sulla creazione di script personalizzati.
Cercare la corrispondenza solo negli allegati.	Questa condizione cerca la corrispondenza solo nel componente Allegati dei messaggi . Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.
Cercare la corrispondenza anche con una o più condizioni supplementari.	Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente. È possibile aggiungere qualsiasi condizione disponibile nell'elenco. Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.

Best practice per l'utilizzo di corrispondenza delle proprietà file

Questa sezione fornisce best practice per l'utilizzo di condizioni di corrispondenza con proprietà di file per definire la corrispondenza con formati di file, dimensioni file e nomi file.

Utilizzo delle regole proprietà file composte per proteggere i file di progettazione e multimediali

È possibile usare IDM per proteggere i file oppure utilizzare regole delle proprietà dei file. Salvo se è necessario proteggere un file specifico, in genere è consigliabile utilizzare le regole delle proprietà dei file, in quanto l'impostazione delle regole risulta meno onerosa di altre soluzioni.

Ad esempio, per individuare i file CAD che contengono diagrammi IP, è possibile indicizzare tali file e applicare regole IDM per individuarli. In alternativa, è possibile creare una politica che contiene una regola del tipo di file, la quale rileva il formato di file CAD, più una regola delle dimensioni file che specifica una dimensione limite. L'approccio delle proprietà file è preferibile, perché in questo scenario ciò che importa è impedire la potenziale uscita di file CAD di grandi dimensioni dall'ambiente aziendale. Non è necessario riunire e indicizzare questi file per IDM se è possibile creare semplicemente le regole che rileveranno il tipo di file e le dimensioni desiderate.

Non utilizzo della corrispondenza del tipo di file per rilevare il contenuto

Il riconoscimento del tipo di file non comporta l'accesso al file e il rilevamento del contenuto. Rileva solo il tipo di file in base alla firma binaria del file. Per rilevare il contenuto, utilizzare una regola di rilevamento del contenuto come EDM, IDM, identificatori dati o corrispondenza di parole chiave.

Per il rilevamento dei tipi di file personalizzati utilizzare il linguaggio di script DLP. Consultare la guida *Symantec Data Loss Prevention Detection Customization Guide*.

Calcolo corretto della dimensione del file per migliorare la precisione della corrispondenza

Il metodo relativo alla dimensione del file calcola sia il corpo sia eventuali allegati nella dimensione del file specificata.

Uso dei criteri di espressione per la corrispondenza con i nomi file

Le seguenti espressioni della corrispondenza criteri DOS sono fornite come esempi per la configurazione della condizione Allegato e-mail o Nome file.

Tabella 32-8 Esempi di rilevamento di nome file

Esempio
Tutti i caratteri immessi (salvo gli operatori DOS) corrispondono esattamente.
Ad esempio, per la corrispondenza con un nome di file di Word che inizia con ENG- seguito da otto caratteri qualsiasi, immettere: ENG-?????????.doc
Se non si è certi che si tratti di un documento Word, immettere: ENG-?????????.*
Se non si è certi del numero di caratteri presenti dopo ENG-, immettere: ENG-.*
Per la corrispondenza con tutti i nomi file che iniziano con ENG- e con tutti i nomi file che iniziano con ITA-, immettere: ENG-.*, ITA-* (separati da virgola), oppure separare i nomi file con una riga vuota.

Utilizzo degli script e dei plug-in per rilevare i tipi di file personalizzati

Symantec Data Loss Prevention fornisce due meccanismi per il rilevamento dei tipi di file personalizzati: il linguaggio di script DLP e SPI per l'estrazione di contenuto. Se l'unico requisito è il riconoscimento dei tipi di file, può essere più facile scrivere uno script di un plug-in SPI. Tuttavia possono esservi occasioni in cui l'utilizzo di uno script non è adeguato.

Il linguaggio di script non supporta i loop. Non è possibile iterare i byte dei tipi di file ed eseguire qualche elaborazione. Il linguaggio di script consente di rilevare una firma conosciuta a un offset relativamente noto. Non è possibile utilizzare il linguaggio di script per rilevare i sottotipi dello stesso tipo di documento. Ad esempio, se si volesse rilevare i file PDF protetti tramite password, non si può utilizzare il linguaggio di script. Oppure, se si volesse rilevare solo i documenti Word con la revisione attivata, si dovrebbe scrivere un plug-in. D'altra parte è possibile distribuire uno script all'endpoint. Attualmente i plug-in sono solo basati sul server.

Per ulteriori informazioni, consultare la guida [Symantec Data Loss Prevention Content Extraction Plugin Developers Guide](#) e la Guida alla personalizzazione di Symantec Data Loss Prevention Detection per la scrittura, rispettivamente, di plug-in e script personalizzati.

Rilevamento degli incidenti di rete

Il capitolo contiene i seguenti argomenti:

- [Introduzione al monitoraggio di protocolli per la rete](#)
- [Configurazione della condizione Monitoraggio protocollo per il rilevamento nella rete](#)
- [Best practice per l'utilizzo della corrispondenza di protocolli di rete](#)

Introduzione al monitoraggio di protocolli per la rete

Symantec Data Loss Prevention include la condizione Monitoraggio protocollo, che consente di rilevare messaggi sulla rete in base al metodo di trasporto delle comunicazioni.

[Tabella 33-1](#) elenca i protocolli che Data Loss Prevention supporta per il rilevamento sulla rete.

Tabella 33-1 Protocolli supportati per il monitoraggio della rete

Protocollo	Descrizione
E-mail/SMTP	Simple Mail Transfer Protocol (SMTP) è un protocollo per l'invio di e-mail tra server.
FTP	File Transfer Protocol (FTP) è usato su Internet per il trasferimento di file da un computer a un altro.
HTTP	Hypertext Transfer Protocol (HTTP) è il protocollo che supporta il World Wide Web. HTTP definisce il modo in cui i messaggi sono formattati e trasmessi e quali azioni i browser e i server Web devono eseguire in risposta ai vari comandi.
HTTP/SSL	Il protocollo Hypertext Transfer Protocol su Secure Sockets Layer (HTTPS) è un protocollo per l'invio sicuro di dati tra un client e un server.

Protocollo	Descrizione
NNTP	Network News Transport Protocol (NNTP), che è usato per inviare, distribuire e recuperare messaggi USENET.
TCP:custom_protocol	Transmission Control Protocol (TCP) è usato per scambiare dati in modo affidabile tra computer su Internet. Questa opzione è disponibile solo se una porta TCP personalizzata è stata definita.

Vedere ["Configurazione della condizione Monitoraggio protocollo per il rilevamento nella rete"](#) a pagina 822.

Configurazione della condizione Monitoraggio protocollo per il rilevamento nella rete

La condizione Monitoraggio protocollo consente di rilevare incidenti di rete. È possibile implementare un'istanza della condizione Monitoraggio protocollo in una o più regole o eccezioni di rilevamento di politiche.

Tabella 33-2 Parametri della condizione Monitoraggio protocollo per la rete

Azione	Descrizione
Aggiungere o modificare la condizione Monitoraggio protocollo o endpoint	<p>Aggiungere una nuova condizione Monitoraggio protocollo o endpoint a una regola o un'eccezione della politica o modificare una condizione di regola o eccezione esistente.</p> <p>Vedere "Configurazione di politiche" a pagina 422.</p> <p>Vedere "Configurazione di regole di politica" a pagina 427.</p> <p>Vedere "Configurazione delle eccezioni di politica" a pagina 437.</p>
Selezionare uno o più protocolli per la corrispondenza.	<p>Per individuare gli incidenti di rete, selezionare uno o più protocolli :</p> <ul style="list-style-type: none"> ■ E-mail/SMTP ■ FTP ■ HTTP ■ HTTPS/SSL ■ NNTP
Configurare un protocollo di rete personalizzato.	Selezionare uno o più protocolli personalizzati: TCP:protocollo_personalizzato .
Configurare il monitoraggio di endpoint.	Vedere "Configurazione della condizione di monitoraggio dell'endpoint" a pagina 827.

Azione	Descrizione
Cercare la corrispondenza nell'intero messaggio.	<p>La condizione Monitoraggio protocollo cerca la corrispondenza nell'intero messaggio e non nei singoli componenti del messaggio.</p> <p>L'opzione Busta è selezionata per impostazione predefinita. Non è possibile selezionare i singoli componenti del messaggio.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p>
Cercare la corrispondenza anche con una o più condizioni supplementari.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile nell'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Best practice per l'utilizzo della corrispondenza di protocolli di rete

Questa sezione fornisce le best practice per utilizzare le condizioni di corrispondenza delle proprietà di file per cercare la corrispondenza con i formati, le dimensioni e i nomi di file.

Uso di politiche distinte per specifici protocolli

È possibile utilizzare il rilevamento della corrispondenza con protocolli per rilevare il traffico di rete, come posta Web, social network e protocolli specifici. Per il monitoraggio dei protocolli, considerare l'implementazione di politiche differenti per ogni tipo di protocollo, come SMTP, TCP, HTTP, FTP e così via. La creazione di politiche distinte per specifici protocolli può facilitare la riparazione e l'ottimizzazione delle politiche.

Considerazione del posizionamento in rete del server di rilevazione per il supporto della corrispondenza indirizzi IP

È possibile individuare mittenti/utenti e destinatari in base a uno o più indirizzi IP. Tuttavia, per fare ciò è necessario considerare con attenzione la disposizione del server di rilevazione sulla rete.

Se il server di rilevazione è installato tra il proxy Web e Internet, l'indirizzo IP di tutto il traffico Web degli appartenenti all'organizzazione sembra provenire dal proxy Web. Se il server di rilevazione è installato tra il proxy Web e la rete aziendale interna, gli indirizzi IP di tutto il traffico Web dall'esterno della organizzazione sembrano avere come destinazione il proxy Web.

La best practice è la definizione di una corrispondenza in base ai nomi di dominio anziché in base agli indirizzi IP.

Rilevamento degli eventi endpoint

Il capitolo contiene i seguenti argomenti:

- [Introduzione al rilevamento di eventi endpoint](#)
- [Configurazione delle condizioni di rilevamento eventi dell'endpoint](#)
- [Best practice per l'utilizzo del rilevamento endpoint](#)

Introduzione al rilevamento di eventi endpoint

Il rilevamento di endpoint cerca la corrispondenza con eventi negli endpoint in cui Symantec DLP Agent è installato.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Symantec Data Loss Prevention fornisce vari metodi per il rilevamento e l'esclusione di eventi endpoint e una raccolta di regole di risposta per rispondere a tali eventi.

Vedere ["Azioni delle regole di risposta per il rilevamento di endpoint"](#) a pagina 1470.

Informazioni sul monitoraggio del protocollo endpoint

Sull'endpoint è possibile rilevare perdite di dati in base al protocollo di trasporto, come e-mail (SMTP), Web (HTTP) e trasferimento di file (FTP).

Vedere ["Configurazione della condizione di monitoraggio dell'endpoint"](#) a pagina 827.

Tabella 34-1 Protocolli supportati per il monitoraggio di endpoint

Protocollo	Descrizione
E-mail/SMTP	Simple Mail Transfer Protocol (SMTP) è un protocollo per l'invio di e-mail tra server.

Protocollo	Descrizione
FTP	File Transfer Protocol (FTP) è usato su Internet per il trasferimento di file da un computer a un altro.
HTTP	Hypertext Transfer Protocol (HTTP) è il protocollo che supporta il World Wide Web. HTTP definisce il modo in cui i messaggi sono formattati e trasmessi e quali azioni i browser e i server Web devono eseguire in risposta ai vari comandi.
HTTP/SSL	Il protocollo Hypertext Transfer Protocol su Secure Sockets Layer (HTTPS) è un protocollo per l'invio sicuro di dati tra un client e un server.

Informazioni sul monitoraggio della destinazione endpoint

È anche possibile rilevare la perdita di dati dell'endpoint nella destinazione in cui i dati vengono copiati o spostati, ad esempio nell'unità CD/DVD, nel dispositivo USB o negli Appunti.

Vedere ["Configurazione della condizione di monitoraggio dell'endpoint"](#) a pagina 827.

Tabella 34-2 Destinazioni supportate per il monitoraggio di endpoint

Destinazione	Descrizione
Unità locale	Monitoraggio del disco locale.
CD/DVD	Registratore CD/DVD sul computer endpoint. Questa destinazione può essere qualsiasi tipo di software per la registrazione di CD/DVD di terze parti.
Dispositivo di archiviazione rimovibile	Rileva i dati trasferiti a qualsiasi dispositivo di archiviazione eSATA, FireWire o USB connesso.
Copia in condivisione di rete	Rileva i dati trasferiti a qualsiasi condivisione di rete o accesso remoto ai file.
Stampante/Fax	Rileva i dati trasferiti a una stampante o un fax connesso al computer endpoint. Questa destinazione può anche corrispondere a documenti di tipo stampa su file.
Appunti	Gli Appunti di Windows, utilizzati per copiare e incollare dati tra le applicazioni Windows.

Informazioni sul controllo delle applicazioni endpoint

È possibile creare eccezioni per gli scenari di utilizzo consentiti.

DLP Agent monitora eventuali applicazioni di terze parti che si aggiungono e configurano nella schermata **Sistema > Agenti > Controllo applicazioni**.

DLP Agent controlla le applicazioni quando hanno accesso a file riservati.

Vedere ["Aggiunta di un'applicazione Windows"](#) a pagina 2237.

Vedere ["Configurazione della condizione di monitoraggio dell'endpoint"](#) a pagina 827.

Informazioni sul rilevamento della posizione dell'endpoint

È possibile rilevare o escludere gli eventi in base alla posizione dell'endpoint.

Con il metodo di rilevamento Posizione endpoint è possibile scegliere di rilevare gli incidenti solo quando l'endpoint è in rete o fuori rete.

Ad esempio è possibile configurare questa condizione in modo da cercare la corrispondenza soltanto quando gli utenti non sono sulla rete aziendale perché sono in vigore altre regole per il rilevamento degli incidenti di rete. In questo caso l'implementazione del metodo di rilevamento Posizione endpoint restituisce questo risultato.

Vedere ["Configurazione della condizione Posizione endpoint"](#) a pagina 829.

Informazioni sul rilevamento di dispositivi endpoint

Symantec Data Loss Prevention consente di rilevare o escludere dispositivi endpoint specifici in base ai metadati del dispositivo descritti. È possibile configurare una condizione per consentire agli utenti di endpoint di copiare file in una specifica classe di dispositivi, ad esempio unità USB di un unico produttore.

Ad esempio, un autore di politiche ha un set di unità flash USB con numeri di serie che vanno da 001 a 010. Queste sono le sole unità flash a cui deve essere consentito l'accesso agli endpoint della società. L'amministratore della politica aggiunge i metadati dei numeri di serie a un'eccezione di una politica di modo che la politica sia applicata a tutte le unità flash USB ad eccezione delle unità con il numero di serie che rientra nei metadati 001-010. In questo modo, i metadati dei dispositivi rendono possibile l'archiviazione dei dati della società solo nei "dispositivi attendibili".

Vedere ["Creazione e modifica delle configurazioni di dispositivi endpoint"](#) a pagina 832.

La condizione Classe o ID dispositivo endpoint rileva specifici dispositivi di archiviazione rimovibili in base alle relative definizioni. I parametri della destinazione endpoint nella condizione Monitoraggio endpoint rilevano qualsiasi dispositivo di archiviazione rimovibile sull'endpoint.

Vedere ["Configurazione della condizione Classe o ID dispositivo endpoint"](#) a pagina 830.

Configurazione delle condizioni di rilevamento eventi dell'endpoint

[Tabella 34-3](#) descrive i vari metodi per implementare il monitoraggio eventi dell'endpoint.

Tabella 34-3 Rilevamento degli eventi endpoint

Condizioni di corrispondenza endpoint	Dettagli
Endpoint Protocol Monitoring	<p>Rileva i dati dell'endpoint in base al protocollo.</p> <p>Vedere "Informazioni sul monitoraggio del protocollo endpoint" a pagina 824.</p> <p>Vedere "Configurazione della condizione di monitoraggio dell'endpoint" a pagina 827.</p>
Endpoint Destination Monitoring	<p>Rileva i dati dell'endpoint in base alla destinazione.</p> <p>Vedere "Informazioni sul monitoraggio del protocollo endpoint" a pagina 824.</p> <p>Vedere "Configurazione della condizione di monitoraggio dell'endpoint" a pagina 827.</p>
Endpoint Application Monitoring	<p>Rileva i dati dell'endpoint in base all'applicazione.</p> <p>Vedere "Informazioni sul monitoraggio del protocollo endpoint" a pagina 824.</p> <p>Vedere "Configurazione della condizione di monitoraggio dell'endpoint" a pagina 827.</p>
Dispositivo endpoint o ID classe	<p>Rileva se gli utenti trasferiscono dati dell'endpoint in un dispositivo specifico.</p> <p>Vedere "Informazioni sul rilevamento di dispositivi endpoint" a pagina 826.</p> <p>Vedere "Configurazione della condizione Classe o ID dispositivo endpoint" a pagina 830.</p>
Posizione endpoint	<p>Rileva quando l'endpoint è incluso o non è incluso nella rete aziendale.</p> <p>Vedere "Informazioni sul rilevamento della posizione dell'endpoint" a pagina 826.</p> <p>Vedere "Configurazione della condizione Posizione endpoint" a pagina 829.</p>

Configurazione della condizione di monitoraggio dell'endpoint

La condizione di monitoraggio dell'endpoint cerca la corrispondenza con i protocolli di messaggio, le destinazioni e le applicazioni dell'endpoint.

È possibile implementare un'istanza della condizione di monitoraggio dell'endpoint in una o più regole o eccezioni di rilevamento delle politiche.

Nota: questo argomento non tratta la configurazione del monitoraggio dei protocolli di rete.

Vedere ["Configurazione della condizione Monitoraggio protocollo per il rilevamento nella rete"](#) a pagina 822.

Tabella 34-4 Configurazione della condizione di monitoraggio dell'endpoint

Azione	Descrizione
Aggiungere o modificare la condizione di monitoraggio dell'endpoint.	<p>Aggiungere una nuova condizione Monitoraggio protocollo o endpoint a una regola o eccezione della politica o modificare una condizione di regola o eccezione esistente.</p> <p>Vedere "Configurazione di regole di politica" a pagina 427.</p> <p>Vedere "Configurazione delle eccezioni di politica" a pagina 437.</p> <p>Vedere "Configurazione di politiche" a pagina 422.</p>
Selezionare uno o più protocolli endpoint per cui cercare una corrispondenza.	<p>Per individuare gli incidenti endpoint, selezionare uno o più protocolli endpoint.</p> <ul style="list-style-type: none"> ■ E-mail/SMTP ■ HTTP ■ HTTPS/SSL ■ FTP <p>Vedere "Informazioni sul monitoraggio del protocollo endpoint" a pagina 824.</p>
Selezionare una o più destinazioni endpoint.	<p>Per individuare quando gli utenti spostano i dati sull'endpoint, selezionare una o più destinazioni endpoint.</p> <ul style="list-style-type: none"> ■ Unità locale ■ CD/DVD ■ Dispositivo di archiviazione rimovibile ■ Copia in condivisione di rete ■ Stampante/Fax ■ Appunti <p>Vedere "Informazioni sul monitoraggio del protocollo endpoint" a pagina 824.</p>
Monitorare le applicazioni endpoint.	<p>Per rilevare quando le applicazioni endpoint accedono ai file, selezionare l'opzione Accesso ai file di applicazione.</p> <p>Vedere "Informazioni sul controllo delle applicazioni" a pagina 2231.</p>
Cercare la corrispondenza con l'intero messaggio.	<p>DLP Agent esamina l'intero messaggio e non i singoli componenti del messaggio.</p> <p>L'opzione Busta è selezionata per impostazione predefinita. Non è possibile selezionare gli altri componenti del messaggio.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p>

Azione	Descrizione
Cercare inoltre la corrispondenza con una o più condizioni aggiuntive.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile nell'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Configurazione della condizione Posizione endpoint

La condizione Posizione endpoint cerca la corrispondenza con eventi endpoint in base alla posizione del computer endpoint in cui DLP Agent è installato.

È possibile implementare un'istanza della condizione Posizione endpoint in una o più eccezioni o regole di rilevamento delle politiche.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Tabella 34-5 Configurazione della condizione di rilevamento Posizione endpoint

Azione	Descrizione
Aggiungere o modificare la condizione Posizione endpoint.	<p>Aggiungere una nuova condizione di rilevamento Posizione endpoint a una regola o a un'eccezione della politica, oppure modificarne una esistente.</p> <p>Vedere "Configurazione di regole di politica" a pagina 427.</p> <p>Vedere "Configurazione delle eccezioni di politica" a pagina 437.</p>
Selezionare la posizione da monitorare.	<p>Selezionare una delle seguenti posizioni endpoint da monitorare:</p> <ul style="list-style-type: none"> ■ All'esterno della rete aziendale Selezionare questa opzione per rilevare o escludere eventi quando il computer endpoint è all'esterno della rete aziendale. ■ All'interno della rete aziendale Selezionare questa opzione per rilevare o escludere eventi quando il computer endpoint è all'interno della rete aziendale. Questa opzione è selezionata per impostazione predefinita. <p>Vedere "Informazioni sul rilevamento della posizione dell'endpoint" a pagina 826.</p>
Cercare la corrispondenza nell'intero messaggio.	<p>DLP Agent esamina l'intero messaggio e non i singoli componenti del messaggio.</p> <p>L'opzione Busta è selezionata per impostazione predefinita. Gli altri componenti del messaggio non sono selezionabili.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p>

Azione	Descrizione
Cercare la corrispondenza anche con una o più condizioni supplementari.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile nell'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Vedere ["Informazioni sul rilevamento della posizione dell'endpoint"](#) a pagina 826.

Vedere ["Configurazione della condizione Posizione endpoint"](#) a pagina 829.

Configurazione della condizione Classe o ID dispositivo endpoint

La condizione Classe o ID dispositivo endpoint consente di rilevare quando gli utenti spostano dati endpoint in specifici dispositivi.

È possibile implementare la condizione Classe o ID dispositivo endpoint in una o più eccezioni o regole di rilevamento di politiche.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Tabella 34-6 Configurazione della condizione Classe o ID dispositivo endpoint

Azione	Descrizione
Aggiungere o modificare una condizione Dispositivo endpoint.	<p>Aggiungere una condizione Classe o ID dispositivo endpoint a una regola o a un'eccezione di politica, oppure modificarne una esistente.</p> <p>Vedere "Configurazione di regole di politica" a pagina 427.</p> <p>Vedere "Configurazione delle eccezioni di politica" a pagina 437.</p>
Selezionare uno o più dispositivi.	<p>La condizione è vera quando gli utenti spostano i dati da un computer endpoint nei dispositivi selezionati.</p> <p>Fare clic su Crea dispositivo endpoint per definire uno o più dispositivi.</p> <p>Vedere "Creazione e modifica delle configurazioni di dispositivi endpoint" a pagina 832.</p>
Cercare la corrispondenza nell'intero messaggio.	<p>Il DLP Agent cerca la corrispondenza nell'intero messaggio e non nei singoli componenti del messaggio.</p> <p>L'opzione Busta è selezionata per impostazione predefinita. Non è possibile selezionare altri componenti.</p> <p>Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.</p>

Azione	Descrizione
Cercare la corrispondenza anche con una o più condizioni supplementari.	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare o escludere un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile dall'elenco a discesa.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Vedere ["Informazioni sul rilevamento di dispositivi endpoint"](#) a pagina 826.

Raccolta degli ID dispositivo endpoint per i dispositivi rimovibili

È possibile aggiungere informazioni sui metadati dei dispositivi a Enforce Server e creare uno o più metodi di rilevamento politiche che rilevano o escludono un'istanza specifica o una classe di dispositivi. Il sistema supporta la sintassi delle espressioni regolari per la definizione dei metadati. Il sistema visualizza i metadati del dispositivo nella schermata **Istantanea incidente** durante il riparazione.

Vedere ["Creazione e modifica delle configurazioni di dispositivi endpoint"](#) a pagina 832.

I metadati che il sistema richiede per definire l'istanza del dispositivo o la classe di dispositivo corrispondono all'opzione **ID istanza dispositivo**. In Windows è possibile ottenere "ID istanza dispositivo" in Gestione periferiche.

Inoltre Symantec Data Loss Prevention fornisce `DeviceID.exe` per i dispositivi associati a endpoint Windows e `DeviceID` per i dispositivi associati a endpoint Mac. È possibile usare queste utilità per estrarre le stringhe ID istanza dispositivo e le informazioni regex del dispositivo. Le utilità indicano inoltre quali dispositivi sono riconosciuti dal sistema per il rilevamento. Le utilità sono disponibili con i file di installazione di Enforce Server.

Vedere ["Informazioni sulle utilità ID periferica"](#) a pagina 2266.

Nota: L'ID istanza dispositivo è utilizzato anche da Symantec Endpoint Protection.

Per ottenere ID istanza dispositivo (in Windows)

- 1 Fare clic con il pulsante destro del mouse su **Risorse del computer**.
- 2 Selezionare **Gestisci**.
- 3 Selezionare **Gestione dispositivi**.
- 4 Fare clic sul segno più accanto a qualsiasi dispositivo per espandere l'elenco di istanze del dispositivo.
- 5 Fare doppio clic sull'istanza del dispositivo. In alternativa, fare clic con il pulsante destro del mouse sull'istanza del dispositivo e selezionare **Proprietà**.

- 6 Individuare nella scheda **Dettagli** il valore **ID istanza dispositivo**.
 - 7 Utilizzare l'ID per creare le espressioni di metadati del dispositivo.
Vedere ["Creazione e modifica delle configurazioni di dispositivi endpoint"](#) a pagina 832.
- Vedere ["Informazioni sul rilevamento di dispositivi endpoint"](#) a pagina 826.

Creazione e modifica delle configurazioni di dispositivi endpoint

È possibile configurare uno o più dispositivi per il rilevamento di specifici endpoint. Dopo la configurazione delle espressioni dei dispositivi, si implementa la condizione Classe o ID dispositivo endpoint in una o più eccezioni o regole di rilevamento di politiche per negare o consentire l'uso di specifici dispositivi.

Si potrebbe negare o consentire l'uso di dispositivi se gli utenti endpoint devono copiare informazioni riservate su unità USB o schede SD fornite dalla società.

Vedere ["Raccolta degli ID dispositivo endpoint per i dispositivi rimovibili"](#) a pagina 831.

Nota: È possibile usare l'utilità DeviceID per endpoint Mac e Windows per generare informazioni su dispositivi di archiviazione rimovibili. Vedere ["Informazioni sulle utilità ID periferica"](#) a pagina 2266.

Per creare e modificare espressioni ID di dispositivi endpoint

- 1 Accedere alla schermata **Sistema > Agente > Dispositivi endpoint**.
- 2 Fare clic su **Aggiungi dispositivo**.
- 3 Immettere il nome del dispositivo in **Nome dispositivo**.
- 4 Immettere una descrizione in **Descrizione dispositivo**.
- 5 Immettere l'espressione in **Definizione dispositivo**.
La definizione del dispositivo deve conformarsi alla sintassi delle espressioni regolari.
Vedere [Tabella 34-7](#) a pagina 833.
Vedere ["Informazioni sulla scrittura di espressioni regolari"](#) a pagina 788.
- 6 Fare clic su **Salva** per salvare la configurazione del dispositivo.
- 7 Implementare la condizione **Classe o ID dispositivo endpoint** in una regola o eccezione di rilevamento.
Vedere ["Configurazione della condizione Classe o ID dispositivo endpoint"](#) a pagina 830.

Tabella 34-7 Esempi di espressioni di dispositivo regolari per endpoint Windows

Esempio di classe di dispositivo	Esempio di espressione
Dispositivo USB generico	USBSTOR\DISK&VEN_SANDISK&PROD_ULTRA_BACKUP&REV_8\32\3485731392112B52
iPod generico	USBSTOR\DISK&VEN_APPLE&PROD_IPOD&.*
Lexar generico	USBSTOR\DISK&VEN_LEXAR.*
Unità CD	IDE\DISKST9160412ASG_____0002SDM1\4&F4ACADA&0&0\0\0
Unità disco rigido	USBSTOR\DISK&VEN_MAXTOR&PROD_ONETOUCH_II&REV_023D\B60899082H____&0
Blackberry generico	USBSTOR\DISK&VEN_RIM&PROD_BLACKBERRY...&REV.*
Telefono cellulare	USBSTOR\DISK&VEN_PALM&PROD_PRE&REV_000\FBB4B8FF4CAEFEC1124DED689&0

Tabella 34-8 Esempio di informazioni regex per endpoint Mac

Esempio di classe di dispositivo	Esempio di informazioni regex
USB SanDisk	SanDisk&Cruzer Blade&20051535820CF1302C2E
Scheda SD	SDC&346128262
Unità disco rigido esterna	External&RAID&0000000000702293

Vedere ["Informazioni sul rilevamento di dispositivi endpoint"](#) a pagina 826.

Best practice per l'utilizzo del rilevamento endpoint

Quando si implementano le condizioni di corrispondenza endpoint, tenere a mente quanto riportato di seguito:

- Qualsiasi metodo di rilevamento eseguito sull'endpoint cerca le corrispondenze con l'intero messaggio, non con i singoli componenti del messaggio.
Vedere ["Messaggi di rilevamento e componenti di messaggio"](#) a pagina 398.
- I metodi **Destinazione endpoint** e **Posizione endpoint** sono specifici del computer endpoint e non sono basati sull'utente.
Vedere ["Distinzione della DGM sincronizzata da altri tipi di rilevamento endpoint"](#) a pagina 853.

- È possibile combinare spesso i metodi di gruppo e di rilevamento sull'endpoint. Tenere presente che il linguaggio della politica applica la condizione AND per i metodi di gruppo e di rilevamento mentre applica la condizione OR per i metodi dello stesso tipo, come ad esempio due regole.

Vedere ["Esecuzione del rilevamento di politiche"](#) a pagina 402.

Rilevamento delle identità descritte

Il capitolo contiene i seguenti argomenti:

- [Introduzione alla corrispondenza con identità descritte](#)
- [Esempi di corrispondenza di identità descritti](#)
- [Configurazione delle condizioni della politica di corrispondenza con le identità descritte](#)
- [Best practice per l'utilizzo della corrispondenza di identità descritte](#)

Introduzione alla corrispondenza con identità descritte

Il rilevamento di identità descritte cerca la corrispondenza con criteri in messaggi da mittenti e destinatari di e-mail, utenti Windows, utenti IM, domini URL e indirizzi IP.

Vedere ["Configurazione delle condizioni della politica di corrispondenza con le identità descritte"](#) a pagina 836.

Vedere ["Configurazione della condizione Mittente/utente corrisponde a criterio"](#) a pagina 837.

Vedere ["Configurazione della condizione Destinatario corrispondente a criterio"](#) a pagina 840.

Esempi di corrispondenza di identità descritti

[Tabella 35-1](#) elenca e descrive alcuni esempi di corrispondenza di contenuto.

Tabella 35-1 Esempi di corrispondenza di identità del criterio

Criterio di esempio	Corrispondenze	Non corrisponde
fr, cu	Tutte le e-mail SMTP indirizzate a indirizzi .fr (Francia) o .cu (Cuba).	Qualsiasi e-mail indirizzata a un'azienda francese con l'estensione .com invece di .fr. Qualsiasi post HTTP indirizzato a un indirizzo .fr con un'applicazione di posta basata sul Web, ad esempio la posta di Yahoo.
azienda.com	Tutte le e-mail SMTP indirizzate all'URL di dominio specifico, ad esempio symantec.com.	Qualsiasi e-mail SMTP non indirizzata all'URL di dominio specifico.
terzolivello.azienda.com	Tutte le e-mail SMTP indirizzate al dominio di terzo livello specifico, ad esempio dlp.symantec.com.	Qualsiasi e-mail SMTP non indirizzata al dominio di terzo livello specifico.
mario@azienda.com	Tutte le e-mail SMTP indirizzate a mario@azienda.com. Tutte le e-mail SMTP indirizzate a MARIO@AZIENDA.COM (il criterio non esegue la distinzione tra maiuscole e minuscole).	Qualsiasi e-mail non specificamente indirizzata a mario@azienda.com, ad esempio: <ul style="list-style-type: none"> ■ carla@azienda.com ■ mario.rossi@azienda.com ■ mario@terzolivello.azienda.com
192.168.0.*	Tutto il traffico e-mail, Web o URL indirizzato specificamente a 192.168.0.[0-255]. Questo risultato presuppone che l'indirizzo IP venga mappato al dominio desiderato, ad esempio web.azienda.com.	Nota: se l'indirizzo IP non corrisponde, utilizzare uno o più URL di dominio.
*/local/1/dom/dom2/dom/Sym */Sym* */dlp/qa/test/local/Sym*	Questi sono indirizzi e-mail di esempio di Lotus Notes.	

Configurazione delle condizioni della politica di corrispondenza con le identità descritte

La [Tabella 35-2](#) elenca e descrive le due condizioni fornite da Symantec Data Loss Prevention per la corrispondenza delle identità descritte.

Vedere ["Esempi di corrispondenza di identità descritti"](#) a pagina 835.

Tabella 35-2 Implementazione della corrispondenza per le identità descritte

Condizione di corrispondenza	Descrizione
Mittente/utente corrisponde a criterio	<p>Esegue la corrispondenza in base a un indirizzo e-mail, un indirizzo di dominio, un indirizzo IP, un nome utente di Windows o un nome di handle/schermata IM.</p> <p>Vedere "Configurazione della condizione Mittente/utente corrisponde a criterio" a pagina 837.</p>
Destinatario corrisponde a criterio	<p>Esegue la corrispondenza in base a un indirizzo e-mail, un indirizzo di dominio, un indirizzo IP o un newsgroup.</p> <p>Vedere "Configurazione della condizione Destinatario corrispondente a criterio" a pagina 840.</p>

Informazioni sui criteri di mittente/destinatario riutilizzabili

È possibile creare criteri di mittente/utente e destinatario riutilizzabili per l'uso nelle politiche. I criteri di mittente/destinatario riutilizzabili semplificano la creazione e la gestione delle politiche che li utilizzano. Per informazioni sulla creazione e sull'uso di criteri di mittente/destinatario riutilizzabili, fare riferimento agli argomenti seguenti.

Vedere ["Configurazione di un criterio mittente riutilizzabile"](#) a pagina 839.

Vedere ["Configurazione di un criterio destinatario riutilizzabile"](#) a pagina 842.

Configurazione della condizione Mittente/utente corrisponde a criterio

La condizione **Mittente/utente corrisponde a criterio** cerca la corrispondenza con le identità descritte del mittente del messaggio e dell'utente. È possibile utilizzare questa condizione in un'eccezione o regola di rilevamento politiche.

Vedere ["Introduzione alla corrispondenza con identità descritte"](#) a pagina 835.

Vedere ["Best practice per l'utilizzo della corrispondenza di identità descritte"](#) a pagina 843.

[Configurazione della condizione Mittente/utente corrisponde a criterio](#) descrive il processo per la configurazione della condizione **Mittente/utente corrisponde a criterio**.

Tabella 35-3 Configurazione della condizione Mittente/utente corrisponde a criterio

Azione	Descrizione
<p>Immettere uno o più criteri mittente per la corrispondenza con uno o più mittenti del messaggio.</p> <p>Nota: Nel campo Criteri è possibile immettere una quantità di dati illimitata (limitata solo dal browser).</p>	<p>Criterio indirizzo e-mail</p> <ul style="list-style-type: none"> ■ Per la corrispondenza con un indirizzo e-mail specifico, immettere l'indirizzo e-mail completo: vendite@symantec.com ■ Per la corrispondenza esatta con molteplici indirizzi e-mail, immettere un elenco di indirizzi separati da virgole: gianni.rossi@azienda.com, giannirossi@azienda.com, grossi@azienda.com ■ Per la corrispondenza con indirizzi e-mail parziali, immettere uno o più criteri di dominio: <ul style="list-style-type: none"> ■ Immettere una o più estensioni di dominio di primo livello, ad esempio: .fr, .cu, .in, .jp ■ Immettere uno o più nomi di dominio, ad esempio: azienda.com, symantec.com ■ Immettere uno o più nomi di dominio di terzo livello (o inferiore): web.azienda.com, mail.yahoo.com, smtp.gmail.com, dlp.security.symantec.com <p>Nomi utente di Windows</p> <p>Immettere i nomi di uno o più utenti di Windows, ad esempio: gianni.rossi, grossi</p> <p>Nome schermata IM</p> <p>Immettere uno o più nomi di schermata IM utilizzati nei sistemi di messaggistica istantanea, ad esempio: gianni_rossi, grossi</p> <p>Indirizzo IP</p> <p>Immettere uno o più indirizzi IP che eseguono il mapping al dominio di cui si intende trovare la corrispondenza, ad esempio:</p> <ul style="list-style-type: none"> ■ Corrispondenza esatta con indirizzo IP, ad esempio: 192.168.1.1 o per IPv6 fdcd:c450:e808:3020:abcd:abcd:0000:5000 ■ Corrispondenza con carattere jolly - L'asterisco (*) può sostituire uno o più campi, ad esempio: 192.168.1.* o 192.*.168.* o per IPv6 fdcd:c450:e808:3:*:*:*:* <p>Nota: Per IPv6, utilizzare solo indirizzi con formato lungo.</p>

Azione	Descrizione
Selezionare un criterio mittente riutilizzabile	È possibile selezionare un criterio mittente salvato per riutilizzarlo nelle politiche. Selezionare Seleziona criterio mittente riutilizzabile , quindi scegliere il criterio desiderato dall'elenco a discesa.
Cercare la corrispondenza nell'intero messaggio.	Questa condizione cerca la corrispondenza nell'intero messaggio. L'opzione Busta è selezionata per impostazione predefinita. Non è possibile selezionare gli altri componenti del messaggio. Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.
Cercare la corrispondenza anche con condizioni supplementari.	Selezionare questa opzione per creare una condizione composta. Tutte le condizioni devono essere vere per generare un incidente. È possibile aggiungere qualsiasi condizione disponibile dall'elenco. Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.

Configurazione di un criterio mittente riutilizzabile

Per utilizzare un Criterio mittente in più politiche, configurare un Criterio mittente riutilizzabile. I criteri mittente riutilizzabili possono essere selezionati per l'utilizzo nelle politiche nella pagina **Configura politica - Modifica regola**. È possibile creare, modificare e gestire i Criteri mittente riutilizzabili dalla pagina **Criteri mittente/destinatario**. Ad esempio, se si utilizza un Criterio mittente in 50 politiche, con un Criterio mittente riutilizzabile è possibile immettere il Criterio mittente una sola volta, quindi selezionarlo per ogni politica. Inoltre, se è necessario aggiornare il Criterio mittente per le 50 politiche, è possibile modificarlo nella pagina **Configura criterio mittente riutilizzabile** e le modifiche verranno applicate automaticamente a ogni politica che utilizza tale criterio.

Per configurare un Criterio mittente riutilizzabile

- 1 Eseguire una delle seguenti operazioni:
 - Se si sta configurando una politica con una regola **Mittente/utente corrispondente a criterio**, nella pagina **Gestisci > Politiche > Elenco politiche > Configura politica - Modifica regola**, fare clic su **Crea criterio mittente riutilizzabile**.
 - Nella console di amministrazione di Enforce Server, scegliere **Gestisci > Politiche > Criteri mittente/destinatario**, quindi fare clic su **Aggiungi > Criterio mittente**.
- 2 Nella sezione **Generale** della pagina **Configura criterio mittente riutilizzabile**, immettere **Nome** e **Descrizione** per il Criterio mittente riutilizzabile.
- 3 Nella sezione **Criterio mittente**, immettere i **Criteri utente** e gli **Indirizzi IP** come descritto in "Configurazione della tabella condizioni per Mittente/utente corrisponde a criterio".

Vedere [Tabella 35-3](#) a pagina 838.
- 4 Fare clic su **Salva**.

- 5 Per modificare un Criterio mittente riutilizzabile salvato, nella pagina **Gestisci > Politiche > Criteri mittente/destinatario**, fare clic sulla freccia di selezione accanto al nome del criterio che si desidera modificare, quindi selezionare **Modifica**.
- 6 Per eliminare un Criterio mittente riutilizzabile salvato, nella pagina **Gestisci > Politiche > Criteri mittente/destinatario**, fare clic sulla freccia di selezione accanto al nome del criterio che si desidera eliminare, quindi selezionare **Elimina**.

Nota: Non è possibile eliminare un Criterio mittente riutilizzabile attualmente in uso in una politica.

Configurazione della condizione Destinatario corrispondente a criterio

La condizione **Destinatario corrispondente a criterio** cerca la corrispondenza con l'identità descritta dei destinatari di messaggi. È possibile utilizzare questa condizione nelle regole o nelle eccezioni di rilevamento di politiche.

Vedere ["Introduzione alla corrispondenza con identità descritte"](#) a pagina 835.

Vedere ["Definizione di criteri di identità precisi per la corrispondenza con utenti"](#) a pagina 843.

[Configurazione della condizione Destinatario corrispondente a criterio](#) definisce il processo per la configurazione della condizione **Destinatario corrispondente a criterio**.

Tabella 35-4 Parametri della condizione Destinataro corrispondente a criterio

Azione	Descrizione
<p>Immettere uno o più criteri destinatario per la corrispondenza con uno o più destinatari di messaggi. Separare più voci con virgole.</p> <p>Nota: Nel campo Criteri è possibile immettere una quantità di dati illimitata (limitata solo dal browser).</p>	<p>Criterio newsgroup/indirizzo e-mail</p> <p>Immettere uno o più indirizzi e-mail o newsgroup per la corrispondenza con i destinatari desiderati.</p> <p>Per la corrispondenza con specifici indirizzi e-mail, immettere l'indirizzo completo, ad esempio <code>sales@symantec.com</code>. Per la corrispondenza con gli indirizzi e-mail di uno specifico dominio, immettere solo il nome di dominio, ad esempio <code>symantec.com</code>.</p> <hr/> <p>Indirizzo IP</p> <p>Immettere uno o più criteri indirizzi IP che puntano al dominio selezionato. È possibile utilizzare il carattere jolly asterisco (*) per uno o più campi. È possibile immettere indirizzi IPv4 e IPv6 separati da virgole.</p> <hr/> <p>Dominio URL</p> <p>Immettere uno o più domini URL per la corrispondenza con il traffico basato su Web, compresi messaggi e-mail basati su Web e pubblicazioni su un sito Web. Ad esempio, se si desidera vietare la ricezione di determinati tipi di dati utilizzando Hotmail, immettere <code>hotmail.com</code>.</p>
<p>Selezionare un criterio destinatario riutilizzabile</p>	<p>È possibile selezionare un criterio destinatario salvato per riutilizzarlo nelle politiche. Selezionare Criterio destinatario riutilizzabile, quindi scegliere il criterio desiderato dall'elenco a discesa.</p>
<p>Configurare il conteggio delle corrispondenze.</p>	<p>Selezionare una delle opzioni seguenti per specificare il numero di destinatari che devono corrispondere:</p> <ul style="list-style-type: none"> ■ Tutti i destinatari devono corrispondere (solo e-mail) conteggia una corrispondenza solo se TUTTI i destinatari del messaggio e-mail corrispondono al criterio specificato. ■ Almeno _ destinatari devono corrispondere (solo e-mail) consente di specificare il numero minimo di destinatari del messaggio e-mail che devono corrispondere per essere conteggiati. <p>Selezionare una delle opzioni seguenti per specificare come si desidera contare le corrispondenze:</p> <ul style="list-style-type: none"> ■ Verificare esistenza Indica un numero di corrispondenze pari a 1 se vi sono una o più corrispondenze. ■ Conta tutte le corrispondenze Indica la somma di tutte le corrispondenze. <p>Vedere "Configurazione del conteggio delle corrispondenze" a pagina 431.</p>

Azione	Descrizione
Cercare la corrispondenza nell'intero messaggio.	Questa condizione cerca la corrispondenza nell'intero messaggio. L'opzione Busta è selezionata per impostazione predefinita. Non è possibile selezionare gli altri componenti del messaggio. Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.
Cercare la corrispondenza anche con condizioni supplementari.	Selezionare questa opzione per creare una condizione composta. Tutte le condizioni in una regola o eccezione devono essere vere per generare un incidente. È possibile aggiungere qualsiasi condizione disponibile dall'elenco. Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.

Configurazione di un criterio destinatario riutilizzabile

Per utilizzare un Criterio destinatario in più politiche, configurare un Criterio destinatario riutilizzabile. I Criteri destinatario riutilizzabili possono essere selezionati per l'utilizzo nelle politiche nella pagina **Configura politica - Modifica regola**. È possibile creare, modificare e gestire i Criteri destinatario riutilizzabili dalla pagina **Criteri mittente/destinatario**. Ad esempio, se si utilizza un Criterio destinatario in 50 politiche, con un Criterio destinatario riutilizzabile è possibile immettere il Criterio destinatario una sola volta, quindi selezionarlo per ogni politica. Inoltre, se è necessario aggiornare il Criterio destinatario per le 50 politiche, è possibile modificarlo nella pagina **Configura criterio destinatario riutilizzabile** e le modifiche verranno applicate automaticamente a ogni politica che utilizza tale criterio.

Per configurare un Criterio destinatario riutilizzabile

- Eseguire una delle seguenti operazioni:
 - Se si sta configurando una politica con una regola **Destinatario corrispondente a criterio**, nella pagina **Gestisci > Politiche > Elenco politiche > Configura politica - Modifica regola**, fare clic su **Crea criterio destinatario riutilizzabile**.
 - Nella console di amministrazione di Enforce Server, scegliere **Gestisci > Politiche > Criteri mittente/destinatario**, quindi fare clic su **Aggiungi > Criterio destinatario**.
- Nella sezione **Generale** della pagina **Configura criterio destinatario riutilizzabile**, immettere **Nome** e **Descrizione** per il Criterio destinatario riutilizzabile.
- Nella sezione **Criterio destinatario**, immettere **Indirizzi e-mail**, **Indirizzi IP** e **Domini URL** in come descritto nella tabella delle condizioni "Destinatario corrispondente a criterio".

Vedere [Tabella 35-4](#) a pagina 841.
- Fare clic su **Salva**.

- 5 Per modificare un Criterio destinatario riutilizzabile salvato, nella pagina **Gestisci > Politiche > Criteri mittente/destinatario**, fare clic sulla freccia di selezione accanto al nome del criterio che si desidera modificare, quindi selezionare **Modifica**.
- 6 Per eliminare un Criterio destinatario riutilizzabile salvato, nella pagina **Gestisci > Politiche > Criteri mittente/destinatario**, fare clic sulla freccia di selezione accanto al nome del criterio che si desidera eliminare, quindi selezionare **Elimina**.

Nota: Non è possibile eliminare un Criterio destinatario riutilizzabile attualmente in uso in una politica.

Best practice per l'utilizzo della corrispondenza di identità descritte

Questa sezione fornisce considerazioni per implementare le condizioni Mittente/utente o Destinatario corrisponde a criterio nelle regole o nelle eccezioni di rilevamento delle politiche. Tenere presenti queste considerazioni quando si implementano le condizioni.

Definizione di criteri di identità precisi per la corrispondenza con utenti

Le condizioni Mittente/utente e Destinatario cercano la corrispondenza nell'intero messaggio e non nei singoli componenti del messaggio. Se una delle condizioni è usata come eccezione, una corrispondenza esclude l'intero messaggio, non solo l'intestazione.

Vedere ["Esecuzione del rilevamento di politiche"](#) a pagina 402.

Per entrambe le regole di corrispondenza con identità descritte, il sistema inserisce OR tra tutti gli elementi dell'elenco separati da virgola e tra tutti i campi. Ad esempio, in caso di corrispondenza con un qualsiasi singolo indirizzo e-mail in un elenco di indirizzi e-mail, la condizione segnala (o esclude) un incidente. Oppure, in caso di corrispondenza con un indirizzo e-mail, un nome di dominio o un indirizzo IP, la condizione segnala (o esclude) un incidente.

Vedere ["Messaggi di rilevamento e componenti di messaggio"](#) a pagina 398.

[Tabella 35-5](#) descrive i tipi di criteri che è possibile usare per la corrispondenza con identità descritte.

Tabella 35-5 Criteri per la corrispondenza con identità

Criterio	Mittente/utente corrisponde a criterio	Destinatario corrispondente a criterio
Indirizzo e-mail: completo e parziale	corrisponde	corrisponde

Criterio	Mittente/utente corrisponde a criterio	Destinatario corrispondente a criterio
Indirizzo di dominio: primo livello e sottodomini	corrisponde	corrisponde
Indirizzo IP	corrisponde	corrisponde
Nome utente Windows	corrisponde	non corrisponde
Nome schermata IM/handle	corrisponde	non corrisponde
Criteri di newsgroup	non corrisponde	corrisponde

Specificare esattamente gli indirizzi e-mail per migliorare l'accuratezza

Un indirizzo e-mail deve corrispondere in modo esatto. Ad esempio, `bob@company.com` non corrisponde a `bob@something.company.com`. Tuttavia un criterio di nome dominio quale `company.com` o `something.company.com` corrisponde a `bob@something.company.com`.

Il campo dell'indirizzo e-mail non determina la corrispondenza con il mittente o il destinatario di un post Web. Ad esempio, l'indirizzo e-mail `bob@yahoo.com` non determina corrispondenze se Bob usa un browser Web per inviare o ricevere e-mail. In tal caso, è necessario usare il criterio di dominio `mail.yahoo.com` per determinare la corrispondenza con `bob@yahoo.com`.

Corrispondenza con domini anziché con indirizzi IP per migliorare l'accuratezza

Il criterio Dominio URL rileva nel traffico HTTP corrispondenze con domini URL specifici. Non si specifica l'intero URL. Ad esempio, si specifica `mail.yahoo.com` e non `http://www.mail.yahoo.com`.

Il sistema non risolve i domini URL in indirizzi IP. Ad esempio, si specifica l'indirizzo IP `192.168.1.1` per un dominio specifico. Se gli utenti accedono all'URL del dominio utilizzando di un browser Web, il sistema non rileva corrispondenze con gli e-mail trasmessi dall'indirizzo IP. In questo caso, utilizzare un criterio di dominio anziché un indirizzo IP, ad esempio `internalmemos.com`.

È possibile individuare mittenti/utenti e destinatari in base a uno o più indirizzi IP. Tuttavia, per fare ciò è necessario considerare con attenzione la disposizione del server di rilevazione sulla rete. Se il server di rilevazione è installato tra il proxy Web e Internet, l'indirizzo IP di tutto il traffico Web degli appartenenti all'organizzazione sembra provenire dal proxy Web. Se il server di rilevazione è installato tra il proxy Web e la rete aziendale interna, gli indirizzi IP di tutto il traffico Web dall'esterno della organizzazione sembrano avere come destinazione il

proxy Web. La best practice è la definizione di una corrispondenza in base ai nomi di dominio anziché in base agli indirizzi IP.

Rilevamento delle identità sincronizzate

Il capitolo contiene i seguenti argomenti:

- [Introduzione a Directory Group Matching \(DGM\) sincronizzato](#)
- [Informazioni sul rilevamento in due fasi per DGM sincronizzata](#)
- [Configurazione di gruppi di utenti](#)
- [Configurazione delle condizioni di politica di DGM sincronizzata](#)
- [Best practice per l'utilizzo di condizioni DGM sincronizzate](#)

Introduzione a Directory Group Matching (DGM) sincronizzato

Symantec Data Loss Prevention fornisce il Directory Group Matching (DGM) sincronizzato per rilevare dati in base alle identità esatte di utenti, mittenti e destinatari di quei dati. Utilizzando il DGM sincronizzato, è possibile connettere Enforce Server a un server di directory di gruppo come Microsoft Active Directory e individuare gli utenti in base alla loro affiliazione al gruppo di directory. Ad esempio, è possibile applicare le politiche solo allo staff del reparto tecnico dell'azienda e non a quello delle risorse umane. Il DGM sincronizzato consente di eseguire quanto descritto di seguito.

Il DGM sincronizzato è basato su una configurazione **Gruppo utenti** da popolare con utenti sincronizzati a partire dal server di directory. Quando si crea una politica DGM sincronizzato, si fa riferimento al **gruppo utenti** nella politica. Al runtime, la politica DGM sincronizzato viene applicata solo alle identità nel **gruppo utenti** a cui fa riferimento la politica. Oppure, si consideri un esempio dove si desidera creare una politica che si applica a tutti nella propria organizzazione ad eccezione del CEO. In questo caso, è possibile creare un **gruppo utenti**

che contiene l'identità del CEO come unico membro del gruppo. Si definisce quindi un'eccezione della politica che fa riferimento al **gruppo utenti** del CEO. Al runtime, la politica ignorerà i messaggi che il CEO invia o riceve.

Vedere ["Gruppi utente"](#) a pagina 382.

Informazioni sul rilevamento in due fasi per DGM sincronizzata

Sull'endpoint, la condizione **Destinatario basato su gruppo di server di directory** richiede il rilevamento in due fasi per i DLP Agent. La condizione corrispondente **Mittente/utente basato su gruppo di server di directory** non richiede il rilevamento in due fasi.

Verificare di aver compreso appieno le implicazioni del rilevamento in due fasi prima di distribuire la regola DGM destinatario sincronizzata a uno o più endpoint.

Vedere ["Rilevamento in due fasi per DLP Agent."](#) a pagina 403.

Per verificare se viene utilizzato il rilevamento in due fasi, controllare il file

```
c:\ProgramData\Symantec\Data Loss Prevention\Detection
Server\15.1\Protect\logs\debug\FileReader.log (Windows) o
/var/log/Symantec/DataLossPrevention/Detection Server/15.1/debug (Linux) in Endpoint
Server.
```

Vedere ["Risoluzione dei problemi delle politiche"](#) a pagina 458.

Configurazione di gruppi di utenti

La schermata **Gestisci > Politiche > Gruppi utente** visualizza gruppi di utenti configurati ed è il punto di partenza per creare un nuovo gruppo di utenti. I gruppi di utenti sono usati per implementare il DGM sincronizzato.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

Nota: I DLP Agent installati sugli endpoint Mac non supportano i gruppi di utenti che utilizzano le condizioni di gruppo Active Directory (AD) nelle politiche.

Per creare o modificare un gruppo di utenti

- 1 Stabilire una connessione al server Active Directory da utilizzare per la sincronizzazione.
Vedere ["Configurazione delle connessioni a server di directory"](#) a pagina 162.
- 2 Nella schermata **Gestisci > Politiche > Gruppi utente**, fare clic su **Crea nuovo gruppo**.
Oppure, per modificare un gruppo di utenti esistente, selezionare il gruppo nella schermata **Gruppi utente**.
- 3 Configurare i parametri del gruppo di utenti come richiesto.
Vedere [Tabella 36-1](#) a pagina 848.

Nota: Se questa è la prima volta che si configura il gruppo di utenti, è necessario selezionare l'opzione **Aggiorna indice directory di gruppo al salvataggio** per popolare il gruppo di utenti.

- 4 Dopo aver individuato gli utenti desiderati, utilizzare le opzioni **Aggiungi** e **Rimuovi** per includerli o escluderli dal gruppo di utenti.
- 5 Fare clic su **Salva**.

Tabella 36-1 Configurazione di un gruppo di utenti

Azione	Descrizione
Immettere il nome del gruppo.	Il Nome gruppo è il nome che si desidera usare per identificare questo gruppo. Utilizzare un nome descrittivo in modo da poterlo identificare facilmente in seguito.
Immettere la descrizione del gruppo	Immettere una breve descrizione del gruppo in Descrizione .
Visualizzare le politiche che usano il gruppo.	Inizialmente, quando si crea un nuovo gruppo di utenti, il campo Utilizzato nella politica visualizza Nessuno . Se il gruppo di utenti già esiste e lo si modifica, il sistema visualizza un elenco delle politiche che implementano il gruppo di utenti, presupponendo che una o più politiche basate sui gruppi siano create per questo gruppo di utenti.

Azione	Descrizione
Aggiornare l'indice directory di gruppo al salvataggio.	<p>Selezionare (spuntare) l'opzione Aggiorna indice directory di gruppo al salvataggio per sincronizzare il profilo del gruppo di utenti con l'indice del server di directory più recente al salvataggio del profilo. Se non si seleziona questa casella, il profilo viene sincronizzato con l'indice del server di directory basato sull'impostazione Connessione directory.</p> <p>Vedere "Pianificazione dell'indicizzazione del server di directory" a pagina 164.</p> <p>Se questa è la prima volta che si configura il profilo del gruppo di utenti, è necessario selezionare l'opzione Aggiorna indice directory di gruppo al salvataggio per popolare il profilo con la replica dell'indice del server di directory più recente.</p>
Selezionare il server di directory.	<p>Selezionare il server di directory che si desidera utilizzare dall'elenco Server di directory.</p> <p>È necessario stabilire una connessione al server di directory prima di creare il profilo del gruppo di utenti.</p> <p>Vedere "Configurazione delle connessioni a server di directory" a pagina 162.</p>
Includi alias di posta.	<p>Selezionare la casella Includi alias di posta per indicizzare alias di posta insieme agli indirizzi di posta elettronica primari. Ad esempio, se un utente ha l'indirizzo e-mail primario "giovanni_rossi@azienda.com" e un alias di posta elettronica "gianni_rossi@azienda.com", spuntando questa casella saranno indicizzati entrambi gli indirizzi di posta elettronica. Si tenga presente che l'indicizzazione di alias di posta elettronica aumenta la dimensione dell'indice.</p>
Cercare utenti specifici nella directory.	<p>Immettere la stringa di ricerca nel campo di ricerca e fare clic su Cerca per cercare utenti specifici nella directory. È possibile eseguire la ricerca utilizzando testo letterale o caratteri jolly (*).</p> <p>I risultati della ricerca visualizzano il nome comune (CN) e il nome univoco (DN) del server di directory che contiene l'utente. Questi nomi forniscono l'identità dell'utente specifico. I risultati sono limitati a 1000 voci.</p> <p>Fare clic su Cancella per eliminare i risultati e cominciare una nuova ricerca.</p> <p>Opzioni dei criteri di ricerca con testo letterale:</p> <ul style="list-style-type: none"> ■ Nome del singolo nodo, come "ingegneria" o "contabilità" ■ Indirizzo email, come "goakham@symantec-dlp.com" <p>Opzioni dei criteri di ricerca con caratteri jolly:</p> <ul style="list-style-type: none"> ■ Il carattere jolly supportato è un asterisco (*) ■ Esempi di ricerca con carattere jolly appropriati: <ul style="list-style-type: none"> ■ Gabriel *akha* restituisce "Gabriel Oakham" ■ j* jop* restituisce "Janice Joplin" ■ Ricerca con carattere jolly non appropriata: <ul style="list-style-type: none"> ■ Non cominciare la stringa di ricerca con un carattere jolly, in quanto ciò ostacola la capacità di ricerca del server di directory. ■ Ad esempio, la seguente ricerca non è consigliata: *Gabriel Oakham.

Azione	Descrizione
Cercare gruppi di utenti nella directory.	<p>È possibile cercare gruppi e utenti nella struttura di directory facendo clic sui singoli nodi ed espandendoli fino a che non si individua il gruppo o il nodo desiderato.</p> <p>I risultati della ricerca visualizzano il nome di ogni nodo. Questi nomi forniscono l'identità dell'utente specifico.</p> <p>Per impostazione predefinita, i risultati sono limitati a 20 voci. Fare clic su Altro per visualizzare fino a 1000 risultati.</p>
Aggiungere un gruppo di utenti al profilo.	<p>Per aggiungere un gruppo o un utente al profilo Gruppo utenti, selezionarlo dall'albero e fare clic su Aggiungi.</p> <p>Dopo avere selezionato e aggiunto il nodo alla colonna Gruppi aggiunti, il sistema visualizza il nome comune (CN) e il nome univoco (DN).</p>
Salvare il gruppo di utenti.	Fare clic su Salva per salvare il profilo del gruppo di utenti configurato.

Configurazione delle condizioni di politica di DGM sincronizzata

Per implementare politiche di DGM sincronizzata, definire una **connessione di directory** utilizzando la console di amministrazione di Enforce Server. **Connessione directory** consente di specificare il server di directory da utilizzare come informazioni di origine per definire l'identità esatta di **Gruppi utente**. Definire quindi uno o più **gruppi dell'utente** nella console di amministrazione di Enforce Server e inserire le informazioni per il gruppo sincronizzando il **gruppo di utenti** con il server di directory. A questo punto associare i **gruppi dell'utente** con la regola del gruppo **Mittente/utente basato su gruppo di server di directory** o la regola del gruppo **Destinatario basato su gruppo di server di directory**.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

La [Tabella 36-2](#) descrive il processo per implementare la DGM sincronizzata.

Tabella 36-2 Flusso di lavoro per l'implementazione dalla DGM sincronizzata

Passaggio	Azione	Descrizione
1	Creare la connessione al server di directory.	<p>Stabilire la connessione tra Enforce Server e un server di directory, quale Microsoft Active Directory.</p> <p>Vedere "Configurazione delle connessioni a server di directory" a pagina 162.</p>

Passaggio	Azione	Descrizione
2	Creare il gruppo di utenti .	Creare uno o più gruppi dell'utente su Enforce Server e in Gruppi utente inserire le identità esatte di utenti, gruppi e unità aziendali definiti nel server di directory. Vedere "Configurazione di gruppi di utenti" a pagina 847.
3	Configurare una nuova politica o modificarne una esistente.	Vedere "Configurazione di politiche" a pagina 422.
4	Configurare una o più regole o eccezioni del gruppo.	Scegliere il tipo di regola di DGM sincronizzata che si desidera implementare e creare un riferimento per Gruppo utenti . Dopo il collegamento della politica e del gruppo, la politica viene applicata solo agli identificatori nel gruppo di utenti a cui si fa riferimento. Vedere "Configurazione della condizione Mittente/utente basato su gruppo di server di directory" a pagina 851. Vedere "Configurazione della condizione Destinatario basato su gruppo di server di directory" a pagina 852.

Configurazione della condizione Mittente/utente basato su gruppo di server di directory

La condizione **Mittente/utente basato su gruppo di server di directory** prevede la corrispondenza con le violazioni delle politiche in base ai mittenti dei messaggi e agli utenti endpoint sincronizzati a partire da un gruppo di directory. È possibile implementare questa condizione in una regola o eccezione di gruppo di politiche (identità).

Vedere ["Configurazione di politiche"](#) a pagina 422.

Nota: se l'identità rilevata è un utente, questi deve essere attivamente connesso a un sistema abilitato per DLP Agent affinché la politica corrisponda.

Tabella 36-3 Parametri della condizione Mittente/utente corrisponde a gruppo di utenti

Parametro	Descrizione
Seleziona gruppi di utenti da includere in questa politica	Selezionare uno o più gruppi di utenti che si desidera vengano rilevati da questa politica. Se non si è creato un gruppo di utenti, fare clic su Crea nuovo gruppo di utenti . Vedere "Configurazione di gruppi di utenti" a pagina 847.

Parametro	Descrizione
Cerca corrispondenza con	Questa condizione cerca la corrispondenza con l'intero messaggio. L'opzione Busta è selezionata per impostazione predefinita. Non è possibile selezionare gli altri componenti del messaggio. Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.
Confronta anche	Selezionare questa opzione per creare una condizione composta. Tutte le condizioni in una regola o eccezione devono essere vere per generare un incidente. È possibile aggiungere qualsiasi condizione disponibile dall'elenco. Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

Configurazione della condizione Destinataro basato su gruppo di server di directory

La condizione **Destinataro basato su gruppo di server di directory** richiede la corrispondenza con violazioni di politiche in base a specifici destinatari di messaggi sincronizzati a partire da un server di directory. È possibile implementare questa condizione in un'eccezione o regola di gruppo di politiche.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

Nota: La condizione **Destinataro basato su gruppo di server di directory** richiede il rilevamento in due fasi. Vedere ["Informazioni sul rilevamento in due fasi per DGM sincronizzata"](#) a pagina 847.

Tabella 36-4 Configurazione della condizione Destinataro basato su gruppo di server di directory

Passaggio	Azione	Descrizione
1	Seleziona gruppi di utenti da includere in questa politica	Selezionare i gruppi di utenti da includere nella politica. Se non si è creato un gruppo di utenti, fare clic sull'opzione Crea nuovo gruppo di utenti . Vedere "Configurazione di gruppi di utenti" a pagina 847.
2	Cerca corrispondenza con	Questa regola rileva l'intero messaggio e non i singoli componenti. L'opzione Busta è selezionata per impostazione predefinita. Non è possibile selezionare gli altri componenti del messaggio. Vedere "Messaggi di rilevamento e componenti di messaggio" a pagina 398.

Passaggio	Azione	Descrizione
3	Confronta anche	<p>Selezionare questa opzione per creare una condizione composta. Tutte le condizioni in una regola o eccezione devono essere vere per generare un incidente.</p> <p>È possibile aggiungere qualsiasi condizione disponibile dall'elenco.</p> <p>Vedere "Configurazione delle condizioni di corrispondenza composte" a pagina 440.</p>

Best practice per l'utilizzo di condizioni DGM sincronizzate

Questa sezione contiene alcune considerazioni da tenere presenti quando si implementano condizioni DGM sincronizzate nelle politiche.

Aggiornamento della directory al momento del salvataggio iniziale del gruppo di utenti

Per eseguire una regola di politica basata su un gruppo Active Directory, deve venire inserito prima l'indice definito su Enforce Server. Quando si definisce il gruppo di utenti per la prima volta, si consiglia di selezionare l'opzione Aggiorna indice directory di gruppo al salvataggio. In questo modo si garantisce la sincronizzazione corretta di Active Directory con Enforce Server. Dopo che il gruppo di utenti è stato inserito, è possibile configurare la pianificazione per mantenere il gruppo di utenti su Enforce sincronizzato con il server Active Directory.

Un caso di utilizzo per la mancata indicizzazione immediata è quando si creano più gruppi di utenti e si desidera indicizzarli dopo avere definito tutti i gruppi. In questo caso è possibile utilizzare la pianificazione. Tuttavia si tenga presente che eventuali politiche basate su questi indici non vengono eseguite fino a quando non vengono inserite.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

Vedere ["Configurazione di gruppi di utenti"](#) a pagina 847.

Distinzione della DGM sincronizzata da altri tipi di rilevamento endpoint

Quando le politiche di DGM sincronizzata vengono distribuite ai server endpoint, il rilevamento basato sull'identità viene applicato agli utenti in un gruppo configurato di endpoint basati su DLP Agent. Con i gruppi di utenti basati sull'endpoint, molti utenti diversi possono accedere allo stesso computer secondo le pratiche aziendali. La risposta che ogni utente vede sull'endpoint varia a seconda di come sono raggruppati gli utenti. Contrapporre a questo stile

di rilevamento endpoint i metodi di **destinazione protocollo endpoint** o **posizione endpoint**, che sono specifici dell'endpoint e non basati sull'utente.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

Rilevamento delle identità con profilo

Il capitolo contiene i seguenti argomenti:

- [Introduzione a Directory Group Matching \(DGM\) con profilo](#)
- [Informazioni sul rilevamento in due fasi per DGM con profilo](#)
- [Configurazione di profili dati esatti per DGM](#)
- [Configurazione delle condizioni di politica di DGM con profilo](#)
- [Procedure ottimali per l'utilizzo di DGM con profilo](#)

Introduzione a Directory Group Matching (DGM) con profilo

DGM con profilo si basa sulla tecnologia Exact Data Matching (EDM) per rilevare identità indicizzate nel database o nel server di directory mediante un profilo dati esatti. Ad esempio, è possibile usare DGM con profilo per identificare l'attività dell'utente in rete o per analizzare i contenuti associati a determinati utenti, mittenti o destinatari. Oppure, è possibile escludere dall'analisi determinati indirizzi e-mail. O ancora, impedire a determinati utenti l'invio di informazioni riservate tramite e-mail.

Vedere ["Configurazione di profili dati esatti per DGM"](#) a pagina 856.

DGM con profilo è differente da DGM sincronizzato, in quanto il secondo usa una connessione a un server di directory (quale Microsoft Active Directory) per cercare la corrispondenza con identità.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

Informazioni sul rilevamento in due fasi per DGM con profilo

DGM con profilo si basa su un indice EDM, che è basato su server, e richiede il rilevamento in due fasi per i DLP Agent sull'endpoint.

Vedere ["Informazioni sul rilevamento in due fasi per l'EDM sull'endpoint"](#) a pagina 484.

Non è possibile combinare nessuno dei due tipi di condizione DGM con profilo con una regola di risposta **Endpoint: notifica** o **Endpoint: blocca** in una politica. In caso contrario il sistema segnala che la politica è configurata erroneamente.

Vedere ["Risoluzione dei problemi delle politiche"](#) a pagina 458.

Configurazione di profili dati esatti per DGM

Per implementare DGM con profilo, è necessario esportare record di identità da un database o server di directory, indicizzare i dati e creare un profilo dati esatti. Si fa quindi riferimento a questo profilo nella corrispondente condizione Mittente/Utente o Destinatario.

Vedere ["Introduzione a Directory Group Matching \(DGM\) con profilo"](#) a pagina 855.

[Tabella 37-1](#) descrive la procedura per la configurazione di profili dati esatti per le politiche DGM.

Tabella 37-1 Flusso di lavoro per l'implementazione di DGM

Passaggio	Azione	Descrizione
1	Creare il file origine dati.	<p>Creare un file origine dati dal database o server di directory di cui si desidera creare il profilo. Assicurarsi che il file origine dati contenga i campi appropriati.</p> <p>I seguenti campi sono supportati per DGM con profilo:</p> <ul style="list-style-type: none"> ■ Indirizzo e-mail ■ Indirizzo IP ■ Nome utente Windows (nel formato <code>dominio\utente</code>) ■ Nome schermata IM <p>Vedere "Creazione del file origine dati esatti per DGM con profilo" a pagina 487.</p>
2	Preparare il file origine dati per l'indicizzazione.	<p>Vedere "Configurazione di profili dati esatti" a pagina 484.</p> <p>Vedere "Preparazione del file origine dati esatti per l'indicizzazione" a pagina 488.</p>

Passaggio	Azione	Descrizione
3	Creare il profilo dati esatti.	<p>Ciò include il caricamento del file origine dati su Enforce Server, il mapping dei campi di dati e l'indicizzazione dell'origine dati.</p> <p>Vedere "Caricamento di file origine dati esatti in Enforce Server" a pagina 490.</p> <p>Vedere "Creazione e modifica di profili dati esatti" a pagina 492.</p> <p>Vedere "Mapping dei campi del profilo dati esatti" a pagina 496.</p> <p>Vedere "Pianificazione dell'indicizzazione di profili dati esatti" a pagina 499.</p>
4	Definire la condizione DGM con profilo.	<p>Vedere "Configurazione del Mittente/Utente in base a una condizione della Profiled Directory" a pagina 858.</p> <p>Vedere "Configurazione del destinatario in base a una condizione Profiled Directory" a pagina 859.</p>
5	Verificare la politica DGM con profilo.	<p>Utilizzare un gruppo di politiche di prova e verificare che le corrispondenze generate dalla politica siano accurate.</p> <p>Vedere "Prova e adattamento delle politiche per migliorare l'accuratezza delle corrispondenze" a pagina 466.</p>

Configurazione delle condizioni di politica di DGM con profilo

Symantec Data Loss Prevention fornisce due condizioni di corrispondenza per la DGM con profilo: mittente/utente e destinatario. Entrambe le condizioni possono essere utilizzate come regole o eccezioni della politica. Ad esempio si consideri uno scenario in cui si indicizza un elenco di indirizzi e-mail e si creano politiche di DGM con profilo in base a questi dati indicizzati. È possibile scrivere una regola che richiede che il mittente del messaggio provenga dall'elenco indicizzato per violare la politica. In alternativa è possibile scrivere un'eccezione che non viene violata se il destinatario di un'e-mail proviene dall'elenco indicizzato.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Tabella 37-2 Condizioni di DGM con profilo

Regola di gruppo	Descrizione
Mittente/utente basato su una directory di <profilo EDM>	Se questa condizione viene implementata come regola della politica, viene trovata una corrispondenza solo se il mittente o l'utente dei dati è contenuto nel profilo dell'indice. Se questa condizione viene implementata come eccezione della politica, i dati vengono esclusi dalla corrispondenza se vengono inviati da un mittente/utente elencato nel profilo dell'indice.

Regola di gruppo	Descrizione
Destinatario basato su una directory di <profilo EDM>	Se questa condizione viene implementata come regola della politica, viene trovata una corrispondenza solo se il destinatario dei dati è contenuto nel profilo dell'indice. Se questa condizione viene implementata come eccezione della politica, i dati vengono esclusi dalla corrispondenza se vengono ricevuti da un destinatario elencato nel profilo dell'indice.

Configurazione del Mittente/Utente in base a una condizione della Profiled Directory

La regola di rilevamento **Mittente/utente basato su una directory di** consente di creare le regole di rilevamento basate sull'identità del mittente o (per gli incidenti endpoint) sull'identità dell'utente. Questa condizione richiede un profilo di dati esatti.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Dopo avere selezionato il profilo dati esatti, quando si configura la regola, la directory selezionata e il o gli identificatori del mittente appaiono in alto nella pagina.

[Tabella 37-3](#) descrive i parametri per la configurazione della condizione **Mittente/Utente basato su una directory da un profilo EDM**.

Tabella 37-3 Configurazione della condizione Mittente/Utente basato su una directory da un profilo EDM

Parametro	Descrizione
Dove	<p>Selezionare questa opzione in modo che il sistema cerchi la corrispondenza con i valori dei campi specificati. Specificare i valori selezionando un campo dall'elenco a discesa e digitando i valori per il campo nella casella di testo adiacente. Se si immettono più valori, separarli con virgole.</p> <p>Ad esempio, per un profilo di un gruppo di directory Dipendenti che include un campo Reparto, selezionare Dove, selezionare Reparto dall'elenco a discesa e immettere Marketing, Vendite nella casella di testo. Se la condizione viene implementata come regola, in questo esempio viene trovata una corrispondenza solo se il mittente o l'utente lavora nel reparto Marketing o Vendite (a condizione che l'altro contenuto immesso soddisfi tutti i criteri di rilevamento). Se la condizione viene implementata come eccezione, in questo esempio il sistema esclude dalla corrispondenza i messaggi di un mittente o un utente che lavora nel reparto Marketing o Vendite.</p>
È uno qualsiasi dei seguenti valori	<p>Immettere o modificare le informazioni per cui si desidera cercare la corrispondenza. Ad esempio, se si desidera cercare la corrispondenza con qualsiasi mittente nel reparto Vendite, selezionare Reparto dall'elenco a discesa, quindi immettere Vendite in questo campo (si presupponga che i dati includono una colonna Reparto). Utilizzare un elenco separato da virgole se si desidera specificare più valori.</p>

Configurazione del destinatario in base a una condizione Profiled Directory

La condizione **Destinatario basato su una directory** di consente di creare metodi di rilevamento basati sull'identità del destinatario. Questo metodo richiede un profilo dati esatti.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Dopo avere selezionato il profilo dati esatti, quando si configura la regola, la directory selezionata e i o gli identificatori del destinatario appaiono in alto nella pagina.

[Tabella 37-3](#) descrive i parametri per la configurazione della condizione **Destinatario basato su una directory di un profilo EDM**.

Tabella 37-4 Configurazione della condizione Destinatario basato su una directory di un profilo EDM

Parametro	Descrizione
Dove	<p>Selezionare questa opzione in modo che il sistema cerchi la corrispondenza con i valori dei campi specificati. Specificare i valori selezionando un campo dall'elenco a discesa e digitando i valori per il campo nella casella di testo adiacente. Se si immettono più valori, separarli con i virgole.</p> <p>Ad esempio per un profilo di gruppo directory Dipendenti che include un campo Reparto è possibile selezionare Dove, selezionare Reparto dall'elenco a discesa e digitare Marketing, Vendite nella casella di testo. Per una regola di rilevamento, questo esempio fa sì che il sistema rilevi un incidente solo se almeno un destinatario lavora nel reparto Marketing o Vendite (sempre che il contenuto di input soddisfi tutti gli altri criteri di rilevamento). Per un'eccezione, questo esempio impedisce al sistema di rilevare l'incidente se almeno un destinatario lavora nel reparto Marketing o Vendite.</p>
È uno qualsiasi dei seguenti valori	<p>Immettere o modificare i dati per la corrispondenza. Ad esempio, per rilevare la corrispondenza con qualsiasi destinatario nel reparto Vendite, selezionare Reparto nell'elenco a discesa, quindi digitare Vendite in questo campo (supponendo che i dati includano una colonna Reparto). Se si desidera specificare più di un valore utilizzare un elenco separato da virgole.</p>

Procedure ottimali per l'utilizzo di DGM con profilo

Tenere presenti le considerazioni di questa sezione quando si implementa Directory Group Matching (DGM) con profilo

Osservare le best practice EDM quando si implementa DGM con profili

DGM con profili si basa sulla tecnologia EDM. Osservare le procedure e le best practice EDM quando si implementa DGM con profili.

Vedere ["Informazioni sul rilevamento in due fasi per DGM con profilo"](#) a pagina 856.

Inclusione di un campo per l'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo

È necessario includere i campi appropriati nel profilo di dati esatti per implementare la DGM con profilo.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Se si include il campo dell'indirizzo e-mail nel profilo di dati esatti per la DGM con profilo e lo si mappa alla convalida di dati e-mail, l'indirizzo e-mail viene visualizzato nell'elenco a discesa **Directory EDM** (nella pagina di risoluzione).

Utilizzo della DGM con profilo per il rilevamento di identità di Network Prevent for Web

Se si desidera implementare la DGM per Network Prevent for Web, utilizzare una delle condizioni DGM con profilo per implementare la corrispondenza di identità. Ad esempio è possibile usare la corrispondenza di identità per bloccare tutto il traffico Web per un utente specifico. Per Network Prevent for Web non è possibile utilizzare le condizioni DGM sincronizzate per questo caso di utilizzo.

Vedere ["Creazione del file origine dati esatti per DGM con profilo"](#) a pagina 487.

Vedere ["Configurazione del Mittente/Utente in base a una condizione della Profiled Directory"](#) a pagina 858.

Utilizzo di attributi contestuali per il Rilevamento applicazioni

Il capitolo contiene i seguenti argomenti:

- [Introduzione a attributi contestuali per le applicazioni cloud](#)
- [Configurazione delle condizioni di attributo contestuale](#)

Introduzione a attributi contestuali per le applicazioni cloud

È possibile includere condizioni di attributo contestuali nelle regole di rilevamento politica per gli incidenti di rilevamento applicazione. Questi attributi contestuali specificano gli attributi che sono associati ad applicazioni cloud monitorato o ispezionate per il servizio di rilevamento cloud. Ad esempio, è possibile creare una regola di rilevamento politica che include la condizione **Nome applicazione: Gatelet > Salesforce** per specificare che la regola di rilevamento si applica agli incidenti associati con il Gatelet di Salesforce Symantec CloudSOC.

Vedere "[Configurazione delle condizioni di attributo contestuale](#)" a pagina 861.

Configurazione delle condizioni di attributo contestuale

Per configurare una regola di politica con una condizione di attributo contestuale, seguire questa procedura:

Per configurare condizioni di attributo contestuale

- 1 Aggiungere una condizione **Attributi contestuali (solo applicazioni cloud e dispositivo di rilevamento API)** a una regola di politica o eccezione o modificarne una esistente.
Vedere ["Configurazione di politiche"](#) a pagina 422.
Vedere ["Configurazione di regole di politica"](#) a pagina 427.
Vedere ["Configurazione delle eccezioni di politica"](#) a pagina 437.
- 2 Selezionare una condizione di attributo contestuale dall'elenco a discesa **Attributi**.
Vedere ["Categorie di attributo contestuale"](#) a pagina 862.
- 3 Configurare i parametri della condizione di attributo contestuale appropriati.
Vedere [Tabella 38-1](#) a pagina 863.
Vedere [Tabella 38-2](#) a pagina 867.
Vedere [Tabella 38-3](#) a pagina 868.
Vedere [Tabella 38-4](#) a pagina 871.
Vedere [Tabella 38-5](#) a pagina 875.
- 4 Fare clic su **OK**.

Categorie di attributo contestuale

Gli attributi contestuali sono raggruppati in categorie: **Generale**, **Utente**, **Rivelazione dati**, **Trasferimento dei dati** e **Personalizza**.

Le seguenti tabelle forniscono ulteriori informazioni sugli attributi e i valori di attributo disponibili in ogni categoria.

Attributi generali

Gli attributi generali si applicano a tutti i tipi di dati e le applicazioni.

Tabella 38-1 Attributi generali

Attributo	Valore	Descrizione
Nome applicazione		Specifica il nome del proxy Web cloud, Gatelet o Securlet.

Attributo	Valore	Descrizione
	<p>Securlet:</p> <ul style="list-style-type: none"> ■ Servizi Web Amazon ■ Box ■ Dropbox ■ Microsoft Azure ■ E-mail di Office 365 ■ OneDrive di Office 365 ■ SharePoint di Office 365 ■ Salesforce ■ Google Drive ■ Gmail ■ SAP ■ ServiceNow ■ Slack ■ Workday ■ Yammer ■ Team di Microsoft ■ Workplace di Facebook ■ Google Calendar <p>Gatelet:</p> <ul style="list-style-type: none"> ■ Box ■ Dropbox ■ Dynamics ■ Office 365 ■ OneDrive ■ Salesforce ■ Siti ■ SugarSync ■ SurveyMonkey ■ Yammer ■ 4Shared ■ 4Sync ■ Acrobat.com ■ AIM Mail ■ Alfresco ■ Amazon CloudDrive ■ Servizi Web Amazon ■ Amazon WorkDocs ■ BitCasa 	

Attributo	Valore	Descrizione
	<ul style="list-style-type: none"> ▪ BV ShareX ▪ cCloud ▪ CentralDesktop ▪ CloudProvider ▪ CloudMe ▪ Confluence ▪ Copia ▪ Cubby ▪ Digital Ocean ▪ DocuSign ▪ Egnyte ▪ FilesAnywhere ▪ Flow ▪ Ftopia ▪ Gmail ▪ GroupDocs ▪ Hightail ▪ Huddle ▪ IBM Connections ▪ iCloud ▪ iDrive ▪ Intralinks ▪ Jive ▪ Joyent ▪ Just Cloud ▪ MailerLite ▪ MediaFire ▪ Microsoft Azure ▪ OneHub ▪ OneUbuntu ▪ Outlook.com ▪ OwnCloud ▪ Oxygen ▪ Podio ▪ Rackspace ▪ RapidShare ▪ SafeSync ▪ SeaCloud ▪ ShareFile 	

Attributo	Valore	Descrizione
	<ul style="list-style-type: none"> Slack SmartFile Soonr Syncplicity Uploaded WatchDocs WebCargo Workshare Wuala Xero Yahoo Mail Zoho Docs DigitalBucket <p>Bluecoat WSS:</p> <ul style="list-style-type: none"> Bluecoat WSS (Symantec Web Security Service) <p>Personalizza:</p> <ul style="list-style-type: none"> Personalizza 	
Tipo applicazione	<ul style="list-style-type: none"> Web Security Services (Proxy Cloud) Gatelet Securlet Personalizza 	Specifica il tipo di applicazione: Symantec Web Security Services, Gatelet di Symantec CloudSOC, Securelet di Symantec CloudSOC o un'applicazione personalizzata.
Tipo di dati	<ul style="list-style-type: none"> Dati a riposo Dati in movimento Personalizza 	Specificare il tipo di dati: dati a riposo (memorizzati in un archivio cloud), dati in movimento (dati trasferiti sulla rete) o personalizzati.

Attributi utente

Gli attributi utente includono informazioni specifiche sull'utente associato a un incidente.

Tabella 38-2 Attributi utente

Attributo	Valore	Descrizione
Tipo attività	<ul style="list-style-type: none"> ■ Crea ■ Modifica ■ Rinomina ■ Carica ■ Scarica ■ Personalizza 	<p>Specifica il tipo di azione intrapresa dall'utente sui dati dell'incidente.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Dominio tenant client	Immettere il nome nel campo Crea corrispondenza .	Specifica il dominio tenant client dell'utente. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.
ID utente tenant client	Immettere l'identificatore utente nel campo Crea corrispondenza .	Specifica l'identificatore di tenant client dell'utente. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.
Conteggio documenti rivelati	<ul style="list-style-type: none"> ■ È maggiore di ■ È minore di ■ È maggiore di o uguale a ■ È minore o uguale a ■ È uguale a ■ Intervallo 	<p>Specifica gli utenti con un numero di documenti esposti sopra o sotto un determinato valore o in un intervallo specificato.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
ID utente	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	Specifica un identificatore utente fornito. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.

Attributo	Valore	Descrizione
Nome utente	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	<p>Specifica un identificatore utente fornito. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Punteggio minaccia utente	<ul style="list-style-type: none"> ■ È maggiore di ■ È minore di ■ È maggiore di o uguale a ■ È minore o uguale a ■ È uguale a ■ Intervallo 	<p>Specifica il punteggio di minaccia Shadow IT dell'utente, sopra o sotto un determinato valore o in un intervallo specificato.</p> <p>Questo attributo si applica solo alle politiche di Securllet.</p>
Utente interno	<ul style="list-style-type: none"> ■ True ■ False 	<p>Specifica se l'utente fa parte o meno della propria organizzazione.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>

Attributi di esposizione dei dati

Gli attributi di esposizione dei dati specificano le informazioni sui documenti che sono memorizzati in archivi dati cloud ("dati a riposo"). Symantec Web Security Services non utilizza gli attributi di esposizione dei dati.

Tabella 38-3 Attributi di esposizione dei dati

Attributo	Valore	Descrizione
Data creazione documento	<ul style="list-style-type: none"> ■ Dopo ■ Prima ■ il o dopo il ■ il o prima del ■ Il ■ Intervallo 	<p>Specifica la data in cui il documento è stato creato.</p>

Attributo	Valore	Descrizione
Ultimo accesso documento	<ul style="list-style-type: none"> ■ Dopo ■ Prima ■ il o dopo il ■ il o prima del ■ Il ■ Intervallo 	Specifica la data dell'ultimo accesso al documento.
Ultima modifica documento	<ul style="list-style-type: none"> ■ Dopo ■ Prima ■ il o dopo il ■ il o prima del ■ Il ■ Intervallo 	Specifica la data dell'ultima modifica del documento.
Proprietario documento	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	Specifica il nome del proprietario del documento. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.
Tag documento	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	Specifica il tag di metadati del documento. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.
Tipo documento	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	Specifica il tipo di documento. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.

Attributo	Valore	Descrizione
Documento rivelato	<ul style="list-style-type: none"> ■ True ■ False 	Specifica se il documento è condiviso o accessibile. Il documento è "esposto" quando viene condiviso con o è accessibile da tutti gli utenti all'interno dell'organizzazione, o condiviso con o accessibile da chiunque all'esterno dell'organizzazione. Se il documento è condiviso solo con determinati membri dell'organizzazione, non è considerato un documento esposto.
Documento interno	<ul style="list-style-type: none"> ■ True ■ False 	Specifica se il documento è "interno." Un documento è considerato interno se è stato creato da un membro dell'organizzazione.
Documento condiviso internamente	<ul style="list-style-type: none"> ■ True ■ False 	Specifica se il documento è condiviso con o accessibile da tutti gli utenti all'interno dell'organizzazione.
Documento rivelato pubblicamente	<ul style="list-style-type: none"> ■ True ■ False 	Specifica se il documento è condiviso con o accessibile da tutti gli utenti esterni all'organizzazione. Questi documenti sono disponibili per chiunque su Internet.
ID processo	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	Specifica l'identificatore di processo associato al documento. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.
Classificazione servizio	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	<p>Specifica la classificazione del servizio shadow IT. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>

Attributo	Valore	Descrizione
Valutazione servizio	<ul style="list-style-type: none"> ■ È maggiore di ■ È minore di ■ È maggiore di o uguale a ■ È minore o uguale a ■ È uguale a ■ Intervallo 	<p>Specifica la valutazione del punteggio servizio shadow IT, sopra o sotto un determinato valore o in un intervallo specificato.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Nome sito SharePoint	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	<p>Specifica il nome di un sito di SharePoint. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>

Attributi di trasferimento dei dati

Gli attributi di trasferimento dei dati specificano le informazioni sui dati che vengono spostati tramite la rete ("data in movimento").

Tabella 38-4 Attributi di trasferimento dei dati

Attributo	Valore	Descrizione
Browser	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	<p>Specifica il nome del browser Web associato alla richiesta di rilevamento. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.</p>
Paese	Selezionare un paese dall'elenco a discesa dei nomi di paese.	<p>Specifica il nome del paese associato alla richiesta di rilevamento.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Dispositivo in sede	<ul style="list-style-type: none"> ■ True ■ False 	<p>Specifica se il dispositivo associato alla richiesta di rilevamento si trova all'interno dell'ufficio.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>

Attributo	Valore	Descrizione
Sistema operativo dispositivo	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	<p>Specifica il sistema operativo del dispositivo che è associato alla richiesta di rilevamento. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Tipo di dispositivo	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	<p>Specifica il tipo di dispositivo associato alla richiesta di rilevamento. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Dispositivo conforme	<ul style="list-style-type: none"> ■ True ■ False 	<p>Specifica se il dispositivo è conforme, in base alle informazioni del sistema di gestione dispositivo mobile.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Dispositivo gestito	<ul style="list-style-type: none"> ■ True ■ False 	<p>Specifica se l'organizzazione gestisce il dispositivo, in base alle informazioni del sistema di gestione del dispositivo mobile.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Dispositivo personale	<ul style="list-style-type: none"> ■ True ■ False 	<p>Specifica se l'utente possiede il dispositivo, in base alle informazioni del sistema di gestione del dispositivo mobile.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>

Attributo	Valore	Descrizione
Dispositivo attendibile	<ul style="list-style-type: none"> ■ True ■ False 	<p>Specifica se il dispositivo è attendibile, in base alle informazioni del sistema di gestione del dispositivo mobile.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>
Metodo HTTP	<ul style="list-style-type: none"> ■ GET ■ PUT ■ ELIMINA ■ PUBBLICA ■ Personalizza 	<p>Specifica il metodo utilizzato nel traffico HTTP che viene inoltrato per l'ispezione.</p>
Direzione rete	<ul style="list-style-type: none"> ■ Carica ■ Scarica ■ Personalizza 	<p>Specifica la direzione di rete del messaggio che viene inoltrato per l'ispezione.</p>
IP destinatario	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	<p>Specifica l'indirizzo IP del destinatario del messaggio. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.</p>
Porta destinatario	<ul style="list-style-type: none"> ■ È maggiore di ■ È minore di ■ È maggiore di o uguale a ■ È minore o uguale a ■ È uguale a ■ Intervallo 	<p>Specifica la porta di rete del destinatario del messaggio.</p>
IP mittente	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	<p>Specifica l'indirizzo IP del mittente del messaggio. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.</p>
Porta mittente	<ul style="list-style-type: none"> ■ È maggiore di ■ È minore di ■ È maggiore di o uguale a ■ È minore o uguale a ■ È uguale a ■ Intervallo 	<p>Specifica la porta di rete del mittente del messaggio.</p> <p>Symantec Web Security Service non utilizza questo attributo.</p>

Attributo	Valore	Descrizione
Classificazione sito	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	Specifica il tipo di sito associato alla richiesta di rilevamento, come ad esempio "Social Media." È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.
Punteggio di rischio sito	<ul style="list-style-type: none"> ■ È maggiore di ■ È minore di ■ È maggiore di o uguale a ■ È minore o uguale a ■ È uguale a ■ Intervallo 	Specifica un valore numerico che indica il livello di rischio del sito di destinazione.
Protocollo di origine	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	Specifica il protocollo di rete OSI livello 7 per la richiesta di rilevamento. Ad esempio, SMTP, HTTP, FTP e così via. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.
Agente utente	<ul style="list-style-type: none"> ■ Corrisponde ■ Corrispondenza tipo 	Specifica l'agente utente per la richiesta di rilevamento relativa al traffico HTTP. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.

Attributi personalizzati

Gli attributi personalizzati consentono di immettere tutti gli attributi per le politiche di rilevamento applicazioni che non sono fornite per impostazione predefinita.

Tabella 38-5 Attributi personalizzati

Attributo	Valore	Descrizione
Attributo stringa	<ul style="list-style-type: none"> ■ Nome ■ Corrisponde ■ Corrispondenza tipo 	Specifica un attributo stringa personalizzata. Denominare l'attributo, quindi specificare la corrispondenza e il tipo di corrispondenza per la stringa. È possibile cercare la corrispondenza esatta con o senza distinzione maiuscole/minuscole o cercare la corrispondenza con un'espressione regolare.
Attributo numerico	<ul style="list-style-type: none"> ■ Nome ■ È maggiore di ■ È minore di ■ È maggiore di o uguale a ■ È minore o uguale a ■ È uguale a ■ Intervallo 	Specifica un attributo numerico personalizzato. Denominare l'attributo, quindi specificare la proprietà numerica e il valore.
Attributo booleano	<ul style="list-style-type: none"> ■ Nome ■ True ■ False 	Specifica un attributo booleano personalizzato. Denominare l'attributo, quindi specificare il valore booleano.
Attributo data	<ul style="list-style-type: none"> ■ Nome ■ Dopo ■ Prima ■ il o dopo il ■ il o prima del ■ Il ■ Intervallo 	Specifica un attributo data personalizzato. Denominare l'attributo, quindi specificare la proprietà data e il valore.

Formati di file supportati per rilevamento

Il capitolo contiene i seguenti argomenti:

- [Panoramica del supporto del formato di file di rilevamento](#)
- [Formati supportati per l'identificazione dei tipi di file](#)
- [Formati supportati per l'estrazione di contenuto](#)
- [Formati di incapsulamento supportati per l'estrazione di file secondari](#)
- [Formati di file supportati per l'estrazione di metadati](#)

Panoramica del supporto del formato di file di rilevamento

Il rilevamento di Symantec Data Loss Prevention supporta vari formati di file per le seguenti operazioni:

- Identificazione tipo di file
- Estrazione del contenuto del file
- Estrazione del file secondario
- Estrazione di metadati del documento

Tabella 39-1 riepiloga i formati di file supportati da Symantec Data Loss Prevention per l'identificazione del tipo di file e l'estrazione di contenuto, file secondari e metadati.

È possibile configurare il sistema in modo da identificare i diversi formati di file mediante la condizione **Corrispondenza allegato messaggio o tipo file**. Questa condizione definisce una corrispondenza basata sul contesto che identifica solo il tipo di formato di file, ma non

estrae i contenuti del file. Inoltre è necessario selezionare esplicitamente i singoli formati di file che si desidera rilevare.

Vedere ["Informazioni sulla corrispondenza con tipi di file"](#) a pagina 808.

Quando si utilizza una condizione di rilevamento basata sul contenuto in una politica (quale **Contenuto corrispondente a parola chiave**), il sistema estrae automaticamente il contenuto dei file per i formati di file supportati (ad esempio DOCX, PPTX, XSLX, PDF). Inoltre il sistema estrae automaticamente i file secondari dai formati di compressione file supportati (quali lo ZIP, RAR, TAR).

Vedere ["Condizioni per la corrispondenza del contenuto"](#) a pagina 393.

Infine, è possibile consentire l'estrazione di metadati per un numero limitato di formati di documento (ad esempio DOCX) e utilizzare la corrispondenza di parole chiave per rilevare i metadati del documento.

Vedere ["Informazioni sul rilevamento dei metadati dei documenti"](#) a pagina 903.

Nota: Sebbene i tipi di file supportati per l'estrazione e l'identificazione siano in qualche misura sovrapponibili (se il sistema può interpretare il file deve essere in grado di identificarne il tipo), i formati supportati per ciascuna operazione sono diversi e vengono implementati con condizioni di corrispondenza diverse. Il numero dei formati di file supportati per l'identificazione del tipo è molto più elevato del numero di formati supportati per l'estrazione del contenuto.

Tabella 39-1 Supporto di formati di file per operazioni di rilevamento

Tipo operazione	Descrizione	Configurazione	Formati supportati
Identificazione tipo di file	Symantec Data Loss Prevention non si basa sulle estensioni di file per identificare il formato. Il tipo di file viene identificato mediante la firma binaria unica del formato di file.	In modo esplicito mediante la condizione della proprietà file Corrispondenza allegato messaggio o tipo file .	Vedere "Formati supportati per l'identificazione dei tipi di file" a pagina 878.
Estrazione del contenuto del file	Il contenuto del file è tutto il contenuto basato su testo, visualizzabile mediante l'applicazione nativa o sorgente.	In modo implicito mediante una o più condizioni di corrispondenza del contenuto, inclusi EDM, IDM, VML, identificatori dati, parole chiave, espressioni regolari.	Vedere "Formati supportati per l'estrazione di contenuto" a pagina 893.

Tipo operazione	Descrizione	Configurazione	Formati supportati
Estrazione del file secondario	I file secondari sono file inclusi in un file principale. I file secondari vengono estratti ed elaborati individualmente per l'identificazione e l'estrazione del contenuto. Se il formato del file secondario non è supportato per impostazione predefinita, è possibile utilizzare un metodo personalizzato per individuare e aprire il file.	In modo implicito mediante una o più condizioni di corrispondenza del contenuto, inclusi EDM, IDM, VML, identificatori dati, parole chiave, espressioni regolari.	Vedere "Formati di incapsulamento supportati per l'estrazione di file secondari" a pagina 901.
Estrazione di metadati	I metadati sono informazioni relative al file, quali l'autore, la versione o tag definiti dall'utente. Limitati in genere ai documenti Microsoft Office (con supporto OLE) e ai file Adobe PDF. Il supporto per i metadati può variare a seconda dell'agente e del server. I metadati includono tag per la sicurezza dei dati creati in Information Centric Tagging (ICT).	Disponibile per le condizioni di corrispondenza basate sul contenuto. Deve essere attivata.	Vedere "Formati di file supportati per l'estrazione di metadati" a pagina 902.

Formati supportati per l'identificazione dei tipi di file

La [Tabella 39-2](#) elenca i tipi di file che è possibile identificare con la condizione di politica **Corrispondenza allegato messaggio o tipo file**.

Vedere ["Informazioni sulla corrispondenza con tipi di file"](#) a pagina 808.

Il formato di file sconosciuto identifica i formati sconosciuti a Symantec Data Loss Prevention. Il formato di file sconosciuto è supportato solo per l'identificazione del tipo di file. Il tipo identifica i file che non sono noti a Data Loss Prevention e li blocca utilizzando la regola del tipo di file.

Se il formato di file che si desidera identificare non è supportato, è possibile utilizzare il linguaggio di script di Symantec Data Loss Prevention per identificare i tipi di file personalizzati.

Vedere ["Informazioni sull'identificazione di tipi di file personalizzati"](#) a pagina 809.

Nota: la condizione **Corrispondenza allegato messaggio o tipo file** è una condizione di corrispondenza basata sul contesto che supporta solo l'identificazione dei tipi di file. Questa condizione non supporta l'estrazione di contenuti di file. Per estrarre i contenuti di file per la valutazione della politica, è necessario utilizzare una regola di rilevamento basata sul contesto. Vedere ["Formati supportati per l'estrazione di contenuto"](#) a pagina 893.

Vedere ["Panoramica del supporto del formato di file di rilevamento"](#) a pagina 876.

Tabella 39-2 Formati supportati per l'identificazione dei tipi di file

Formati Corrispondenza allegato messaggio o tipo file
File compresso 7-Zip (7Z)
Ability Office (SS)
Ability Office (DB)
Ability Office (GR)
Ability Office (WP)
Ability Office (COM)
ACT
Adobe FrameMaker
Formato Adobe Maker Interchange (FrameMaker)
Adobe FrameMaker Markup Language
Adobe PDF
AES Multiplus Comm
Aldus Freehand (Macintosh)
Aldus PageMaker (DOS)
Aldus PageMaker (Macintosh)
Amiga IFF-8SVX, audio
Amiga MOD, audio
ANSI
Apple doppio
Apple semplice
Applix Alis
Applix Asterix
Applix Graphics
Applix Presents

Formati Corrispondenza allegato messaggio o tipo file
Applix Spreadsheets
Applix Words
Archivio ARC/PAK
ASCII
Codificato PGP blindato da ASCII
Keyring pubblico PGP blindato da ASCII
Firmato PGP blindato da ASCII
Audio Interchange File Format
AutoCAD Drawing
AutoCAD Drawing Exchange
Animazione FLIC AutoDesk Animator
Animazione FLIC AutoDesk Animator Pro
AutoDesk WHIP
Rendering AutoShade
BinHex
CADAM Drawing (CDD) (solo server)
CADAM Drawing Overlay
CATIA Drawing (CAT) (solo server)
CCITT Group 3 1-Dimensional (G31D)
COMET TOP Word
Valori separati da virgola
Archivio Compactor/Compact Pro
Computer Graphics Metafile
Convergent Tech DEF Comm.
Corel Draw CMX
Corel Presentations

Formati Corrispondenza allegato messaggio o tipo file
Corel Quattro Pro (WB2)
Corel Quattro Pro (WB3)
Corel WordPerfect Linux
Corel WordPerfect Macintosh
Corel WordPerfect Windows (WO)
Corel WordPerfect Windows (WPD)
CorelDRAW
Archivio CPIO (UNIX)
Archivio CPIO (VAX)
Archivio CPIO (SUN)
Comunicazione CPT
Creative Voice (VOC), audio
Immagine schermata Curses (UNIX)
Immagine schermata Curses (VAX)
Immagine schermata Curses (SUN)
Formato interscambio dati
Data Point VISTAWORD
dBase Database
Fax DCX
DCX Fax System
DEC WPS PLUS
DECdx
Desktop Color Separation (DCS)
File indipendente dalla periferica (DVI)
DG CEOwrite
DG Common Data Stream (CDS)

Formati Corrispondenza allegato messaggio o tipo file
Foglio di calcolo DIF
Digital Document Interchange Format (DDIF)
Compressione DiskDoublor
DisplayWrite
Domino XML Language
File contenitore EMC EmailXtender (EMX)
ENABLE
Foglio di calcolo ENABLE (SSF)
Encapsulated PostScript (raster)
Enhanced Metafile
Envoy (EVY)
Eseguibile - Altro
Eseguibile - UNIX
Eseguibile - VAX
Eseguibile - SUN
FileMaker (Macintosh)
File Share Encryption
Folio Flat File
Framework
Framework II
Dati sessione FTP
Fujitsu Oasys
Immagine bitmap GEM
GIF
Graphics Environment Manager (GEM VDI)
GZIP

Formati Corrispondenza allegato messaggio o tipo file
Haansoft Hangul (Hangul 2010 SE+)
Harvard Graphics
Hewlett-Packard
Honey Bull DSA101
HP Graphics Language (HPG) (solo server)
HP Printer Control Language (PCL)
HTML
Stampante di linea IBM 1403
IBM DCA/RFT(Revisable Form Text)
IBM DCA-FFT
IBM DCF Script
iCalendar
Informix SmartWare II
File di comunicazione Informix SmartWare II
Database Informix SmartWare II
Foglio di calcolo Informix SmartWare
Interleaf
Archivio Java
JPEG
File di interscambio JPEG (JFIF)
JustSystems Ichitaro
KW ODA G31D (G31)
KW ODA G4 (G4)
KW ODA Internal G32D (G32)
KW ODA Internal Raw Bitmap (RBM)
Lasergraphics Language

Formati Corrispondenza allegato messaggio o tipo file
Legato Extender
Link Library - Altro
Link Library UNIX
Link Library VAX
Link Library SUN
Lotus 1-2-3 (123)
Lotus 1-2-3 (WK4)
Grafici Lotus 1-2-3
Lotus AMI Pro
Lotus AMI Professional Write Plus
Lotus AMI Draw Graphics
Lotus Freelance Graphics
Lotus Freelance Graphics 2
Lotus Notes Bitmap
Lotus Notes CDF
Database Lotus Notes
Lotus Pic
Lotus ScreenCam
Lotus SmartMaster
Lotus Word Pro
Lyrix MacBinary
MacBinary
Raster Macintosh
MacPaint
Macromedia (Adobe) Director
Macromedia (Adobe) Flash

Formati Corrispondenza allegato messaggio o tipo file
MacWrite
MacWrite II
MASS-11
Micrografx Designer
Microsoft Access
Microsoft Advanced Systems Format (ASF)
Cartella compressa Microsoft (LZH)
Cartella compressa Microsoft (LHA)
Bitmap indipendente dalla periferica Microsoft
Grafici Microsoft Excel
Microsoft Excel Macintosh
Microsoft Excel Windows
Microsoft Excel Windows XML
Microsoft Office Access (ACCDB)
Microsoft Office Drawing
Microsoft OneNote
Cartella personale di Microsoft Outlook
Microsoft Outlook
Microsoft Outlook Express
Microsoft PowerPoint Macintosh
Microsoft PowerPoint PC
Microsoft PowerPoint Windows
Microsoft PowerPoint Windows XML
Microsoft PowerPoint Windows XML con attivazione macro
Modello Microsoft PowerPoint Windows XML
Modello Microsoft PowerPoint Windows XML con attivazione macro

Formati Corrispondenza allegato messaggio o tipo file

Presentazione Microsoft PowerPoint Windows XML

Presentazione Microsoft PowerPoint Windows con attivazione macro

Microsoft Project

Microsoft Publisher

File binario Office con crittografia Microsoft RMS

File Open Packaging Conventions con crittografia Microsoft RMS

Microsoft Visio

Microsoft Visio 2013

Formato di Microsoft Visio 2013_Macro

Formato di Microsoft Visio 2013_Stencil

Formato di Microsoft Visio 2013_Stencil_Macro

Formato di Microsoft Visio 2013_Template

Microsoft Visio _Template_Macro

Microsoft Visio XML

Audio Wave Microsoft

Grafici Microsoft Windows Cursor (CUR)

File di gruppo Microsoft Windows

Microsoft Windows Help File

Microsoft Windows Icon (ICO)

Microsoft Windows OLE 2 Encapsulation

Microsoft Windows Write

Microsoft Word (UNIX)

Microsoft Word Macintosh

Microsoft Word PC

Microsoft Word Windows

Microsoft Word Windows XML

Formati Corrispondenza allegato messaggio o tipo file
Modello Microsoft Word Windows XML
Modello Microsoft Word Windows XML con attivazione macro
Microsoft Works (Macintosh)
Microsoft Works
Microsoft Works Communication (Macintosh)
Microsoft Works Communication (Windows)
Microsoft Works Database (Macintosh)
Microsoft Works Database (PC)
Microsoft Works Database (Windows)
Microsoft Works Spreadsheet (S30)
Microsoft Works Spreadsheet (S40)
Microsoft Works Spreadsheet (Macintosh)
Microstation
MIDI
Funzione di struttura database MORE (Macintosh)
MPEG-1 Audio Layer-3
Video MPEG-1
Audio MPEG-2
Formato file batch MS DOS
Driver di periferica MS DOS
MultiMate 4.0
Multiplan Spreadsheet
Navy DIF
Formato di archivio NBI Async
Formato di archivio NBI Net
File segnalibro Netscape

Formati Corrispondenza allegato messaggio o tipo file
File tipo di carattere NeWS (SUN)
Audio NeXT/Sun
NIOS TOP
Nota Bene
Nurestor Drawing (NUR) (solo server)
Formato Oasis Open Document (ODT)
Formato Oasis Open Document (ODS)
Formato Oasis Open Document (ODP)
Modulo oggetto UNIX
Modulo oggetto VAX
Modulo oggetto SUN
ODA/ODIF
ODA/ODIF (FOD 26)
Office Writer
Oggetto OLE DIB
OLIDIF
OmniOutliner (OO3)
OpenOffice Calc (SXC)
OpenOffice Calc (ODS)
OpenOffice Impress (SXI)
OpenOffice Impress (SXP)
OpenOffice Impress (ODP)
OpenOffice Writer (SXW)
OpenOffice Writer (ODT)
OpenPGP
OS/2 PM Metafile Graphics

Formati Corrispondenza allegato messaggio o tipo file
Paradox (PC) Database
Eseguibile COM PC
Modulo libreria PC
Modulo oggetto PC
PC PaintBrush
Tipi di carattere TrueType PC
Immagine PCD
Foglio di calcolo PeachCalc
Persuasion Presentation
PEX Binary Archive (SUN)
Dati compressi PGP
Dati crittografati PGP
Keyring pubblico PGP
Keyring segreto PGP
Certificato firma PGP
Dati firmati e crittografati PGP
Dati firmati PGP
Script Philips
PKZIP
Plan Perfect
Utilità Portable Bitmap (PBM)
Utilità Portable Greymap (PGM)
Portable Network Graphics
Utilità Portable Pixmap (PPM)
PostScript File
PRIMEWORD

Formati Corrispondenza allegato messaggio o tipo file
File di informazioni sul programma
Q&A per DOS
Q&A per Windows
Quadratron Q-One (V1.93J)
Quadratron Q-One (V2.0)
Quark Express (Macintosh)
QuickDraw 3D Metafile (3DMF)
QuickTime Movie
Archivio RAR
Real Audio
Database Reflex
Rich Text Format
Bitmap indipendente dalla periferica RIFF
RIFF MIDI
RIFF Multimedia Movie
SAMNA Word IV
Incapsulamento Serialized Object Format (SOF)
Immagine RGB SGI
SGML
Simple Vector Format (SVF)
Documento SMTP
SolidWorks Drawing (SLDASM, SLDPRT, SLDDRW)
StarOffice Calc (SXC)
StarOffice Calc (ODS)
StarOffice Impress (SXI)
StarOffice Impress (XPP)

Formati Corrispondenza allegato messaggio o tipo file
StarOffice Impress (ODP)
StarOffice Writer (SXW)
StarOffice Writer (ODT)
Archivio Stuff It (Macintosh)
Immagine raster Sun
Definizione vfont SUN
Foglio di calcolo Supercalc
SYLK Spreadsheet
Foglio di calcolo Symphony
Tagged Image File
Archivio su nastro
Targon Word (V 2.0)
Text Mail (MIME)
Transmission Neutral Encapsulation Format
Truevision Targa
Foglio di calcolo Ultracalc
Testo Unicode
Uniplex (V6.01)
Foglio di calcolo Uniplex Ucalc
UNIX Compress
Unix SHAR Encapsulation
SCONOSCIUTO
Formato Usenet
UUEncoding
Vcard
VCF

Formati Corrispondenza allegato messaggio o tipo file
Volkswriter
VRML
Incapsulamento Wang Office GDL Header
WANG PC
Wang WITA
WANG WPS Comm.
Puntatore animato Windows
Bitmap Windows
Archiviazione oggetti Windows C++
Cursora icona Windows
Windows Metafile
Windows Micrografx Draw (DRW)
Tavolozza Windows
Windows Media Video (WMV)
Windows Media Audio (WMA)
Windows Video (AVI)
WinZip (lettore decompressione)
WinZip
Word Connection
WordERA (V 1.0)
Elaboratore di testi WordMARC
WordPad
File generale WordPerfect
WordPerfect Graphics 1
WordPerfect Graphics 2
WordStar

Formati Corrispondenza allegato messaggio o tipo file
WordStar 2000
WordStar 6.0
WriteNow
Elaboratore di testi Writing Assistant
X Bitmap (XBM)
X Image
X Pixmap (XPM)
Xerox 860 Comm.
Elaboratore di testi Xerox Writer
XHTML
XML (generico)
XML Paper Specification
XyWrite

Formati supportati per l'estrazione di contenuto

Symantec Data Loss Prevention accede a più di 100 formati di file per eseguire l'estrazione di contenuto. Utilizzare le condizioni di rilevamento basato sul contenuto per accedere a un file ed estrarne il contenuto.

Vedere ["Condizioni per la corrispondenza del contenuto"](#) a pagina 393.

La [Tabella 39-3](#) elenca le varie categorie di formato di file di cui Symantec Data Loss Prevention può estrarre il contenuto. Fare riferimento al collegamento associato per i singoli formati di file supportati per la categoria.

Vedere ["Panoramica del supporto del formato di file di rilevamento"](#) a pagina 876.

Tabella 39-3 Categorie di formato di file supportate per l'estrazione di contenuto

Categoria di formato di file	Elenco di supporto predefinito
Formati di file di elaborazione di testo	Vedere "Formati di elaborazione di testi supportati per l'estrazione di contenuto" a pagina 894.

Categoria di formato di file	Elenco di supporto predefinito
Formati di file di presentazione	Vedere "Formati di presentazione supportati per l'estrazione di contenuto" a pagina 896.
Formati di file di foglio di calcolo	Vedere "Formati di foglio di calcolo supportati per l'estrazione di contenuto" a pagina 897.
Formati di file di testo e markup	Vedere "Formati di testo e markup supportati per l'estrazione di contenuto" a pagina 898.
Formati di file e-mail	Vedere "Formati e-mail supportati per l'estrazione di contenuto" a pagina 898.
Formati di file CAD	Vedere "Formati CAD supportati per l'estrazione di contenuto" a pagina 899.
Formati di file di grafica	Vedere "Formati di grafica supportati per l'estrazione di contenuto" a pagina 899.
Formati di file di database	Vedere "Formati di database supportati per l'estrazione di contenuto" a pagina 900.
Altri formati di file	Vedere "Altri formati di file supportati per l'estrazione di contenuto" a pagina 900.
Formati di file di incapsulamento	Vedere "Formati di incapsulamento supportati per l'estrazione di file secondari" a pagina 901.

Formati di elaborazione di testi supportati per l'estrazione di contenuto

La [Tabella 39-4](#) elenca i formati di file di elaborazione di testi di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione della politica.

Tabella 39-4 Formati di file di elaborazione di testi supportati per l'estrazione di contenuto

Nome formato	Estensione formato
Formato Adobe Maker Interchange (FrameMaker)	FIM
Apple iWork Pages	PAGES
Applix Words	AW
Corel WordPerfect Linux	WPS
Corel WordPerfect Macintosh	WPS
Corel WordPerfect Windows	WO
Corel WordPerfect Windows	WPD
DisplayWrite	IP
Folio Flat File	FFF

Nome formato	Estensione formato
Fujitsu Oasys	OA2
Haansoft Hangul	HWP
IBM DCA/RFT (Revisable Form Text)	DC
JustSystems Ichitaro	JTD
Lotus AMI Pro	SAM
Lotus AMI Professional Write Plus	AMI
Lotus Word Pro	LWP
Lotus SmartMaster	MWP
Microsoft Word PC	DOC
Microsoft Word Windows	DOC
Microsoft Word Windows XML	DOCX
Modello Microsoft Word Windows XML	DOTX
Modello Microsoft Word Windows XML con attivazione macro	DOTM
Microsoft Word Macintosh	DOC
Microsoft Works	WPS
Microsoft Windows Write	WRI
Microsoft OneNote	ONE
OpenOffice Writer	SXW
OpenOffice Writer	ODT
StarOffice Writer	SXW
StarOffice Writer	ODT
WordPad	RTF
XML Paper Specification	XPS
XyWrite	XY4

Formati di presentazione supportati per l'estrazione di contenuto

La [Tabella 39-5](#) elenca i formati di file di presentazione di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione della politica.

Tabella 39-5 Formati di presentazione supportati per l'estrazione di contenuti di file

Nome formato	Estensione formato
Apple iWork Keynote	KEYNOTE
Applix Presents	AG
Corel Presentations	SHW
Lotus Freelance Graphics	PRZ
Lotus Freelance Graphics 2	PRE
Macromedia Flash	SWF
Microsoft PowerPoint Windows	PPT
Microsoft PowerPoint PC	PPT
Microsoft PowerPoint Windows XML	PPTX
Microsoft PowerPoint Windows XML con attivazione macro	PPTM
Modello Microsoft PowerPoint Windows XML	POTX
Modello Microsoft PowerPoint Windows XML con attivazione macro	POTM
Presentazione Microsoft PowerPoint Windows XML	PPSX
Presentazione Microsoft PowerPoint Windows con attivazione macro	PPSM
Microsoft PowerPoint Macintosh	PPT
OpenOffice Impress	SXI
OpenOffice Impress	SXP
OpenOffice Impress	ODP
StarOffice Impress	SXI
StarOffice Impress	SXP
StarOffice Impress	ODP

Formati di foglio di calcolo supportati per l'estrazione di contenuto

La [Tabella 39-6](#) elenca i formati di file di foglio di calcolo di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione della politica.

Tabella 39-6 Formati di foglio di calcolo supportati per l'estrazione di contenuti di file

Nome formato	Estensione formato
Apple iWork Numbers	NUMERI
Applix Spreadsheets	AS
Valori separati da virgola	CSV
Corel Quattro Pro	WB2
Corel Quattro Pro	WB3
Formato interscambio dati	DIF
Lotus 1-2-3	123
Lotus 1-2-3	WK4
Grafici Lotus 1-2-3	123
Microsoft Excel Windows	XLS
Microsoft Excel Windows XML	XLSX
Grafici Microsoft Excel	XLS
Cartella di lavoro binaria Microsoft Excel 2007	XLSB
Microsoft Excel Macintosh	XLS
Microsoft Works Spreadsheet	S30
Microsoft Works Spreadsheet	S40
OpenOffice Calc	SXC
OpenOffice Calc	ODS
StarOffice Calc	SXC
StarOffice Calc	ODS

Formati di testo e markup supportati per l'estrazione di contenuto

La [Tabella 39-7](#) elenca i formati di file di testo e markup di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione della politica.

Tabella 39-7 Formati di file di testo e markup supportati per l'estrazione di contenuto

Nome formato	Estensione formato
ANSI	TXT
ASCII	TXT
HTML	HTM
Microsoft Excel Windows XML	XML
Microsoft Word Windows XML	XML
Microsoft Visio XML	VDX
Formato Oasis Open Document	ODT
Formato Oasis Open Document	ODS
Formato Oasis Open Document	ODP
Rich Text Format	RTF
Testo Unicode	TXT
XHTML	HTM
XML (generico)	XML

Formati e-mail supportati per l'estrazione di contenuto

La [Tabella 39-8](#) elenca i formati di file e-mail dai quali Symantec Data Loss Prevention può estrarre contenuto per la valutazione.

Tabella 39-8 Formati di file e-mail supportati per l'estrazione di contenuto

Nome formato	Estensione formato
Domino XML Language	DXL
EMC EmailXtender Native Message	ONM
Microsoft Outlook	MSG
Microsoft Outlook Express	EML

Nome formato	Estensione formato
Text Mail (MIME)	Varie
Transfer Neutral Encapsulation Format	Varie

Formati CAD supportati per l'estrazione di contenuto

La [Tabella 39-9](#) elenca i formati di file CAD di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione.

Tabella 39-9 Formati di file CAD supportati

Nome formato	Estensione formato
AutoCAD Drawing	DWG
AutoCAD Drawing Exchange	DFX
Microsoft Visio 2013	VSD
Microsoft Visio XML	VSDX
Microsoft Visio 2013_Macro	VSDM
Microsoft Visio 2013_Stencil	VSSX
Microsoft Visio 2013_Stencil_Macro	VSSM
Microsoft Visio 2013_Template	VSTX
Microsoft Visio 2013_Template_Macro	VSTM
Microstation	DGN

Formati di grafica supportati per l'estrazione di contenuto

La [Tabella 39-10](#) elenca i formati di file grafica di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione.

Tabella 39-10 Formati di file grafica supportati per l'estrazione di contenuto

Nome formato	Estensione formato
Enhanced Metafile	FME
Lotus Pic	PIC
Tagged Image File (solo metadati)	TIFF

Nome formato	Estensione formato
Windows Metafile	WMF

Formati di database supportati per l'estrazione di contenuto

Nella tabella seguente sono elencati i formati di file di database di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione della politica.

Tabella 39-11 Formati di file di database accessibili

Nome formato	Estensione formato
Microsoft Access	MDB
Microsoft Project	MPP

Altri formati di file supportati per l'estrazione di contenuto

La [Tabella 39-12](#) elenca altri formati di file di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione della politica.

Tabella 39-12 Altri formati supportati per l'estrazione di contenuto

Nome formato	Estensione formato
Adobe PDF	PDF
iCalendar	ICS
MPEG-1 Audio Layer-3 (solo metadati)	MP3
File di utilità di backup Microsoft Windows	BKF
File protetti Microsoft Rights Management	<ul style="list-style-type: none"> ■ PFILE ■ Microsoft Office 2003 e versioni precedenti ■ File che utilizzano la tecnologia Open Packaging Conventions (OPC), compresi Office Open XML (incluso Office 2007 e versioni successive) e XML Paper Specification (XPS) <p>Nota: Questo tipo di estrazione di contenuto è supportato solo sui server di rilevamento in esecuzione sui server Windows</p>

Nome formato	Estensione formato
File Share Encryption (PGP Netshare)	È possibile decrittografare i file crittografati con Symantec File Share ed estrarre i contenuti dei file per la valutazione della politica con il plug-in di File Share. Fare riferimento a <i>Symantec Data Loss Prevention Encryption Insight Implementation Guide</i> . Nota: Encryption Insight è disponibile solo con Network Discover.
Personalizzato	È possibile scrivere un plug-in per estrarre contenuto, file secondari e metadati con formati di file personalizzati. Fare riferimento a <i>Symantec Data Loss Prevention Content Extraction Plug-in Developers Guide</i> . Nota: i plug-in per l'estrazione di contenuto sono limitati ai server di rilevamento.
File Virtual Card	File di biglietto da visita elettronico VCF e VCARD

Formati di incapsulamento supportati per l'estrazione di file secondari

Symantec Data Loss Prevention supporta vari formati di incapsulamento per l'estrazione di file secondari, ad esempio ZIP, RAR e TAR. Il sistema esegue automaticamente l'estrazione di file secondari per i formati supportati utilizzando le condizioni di corrispondenza basata sul contenuto. L'estrazione di file secondari comporta l'estrazione di un sottoinsieme di contenuti. In altre parole, se il sistema riesce a estrarre un file secondario da un file incapsulato supportato, estrae automaticamente i contenuti di file secondari basati sul testo se il formato di file secondario è supportato per l'estrazione di contenuto.

Vedere ["Panoramica del supporto del formato di file di rilevamento"](#) a pagina 876.

La [Tabella 39-13](#) elenca i formati di file di cui Symantec Data Loss Prevention può estrarre il contenuto per la valutazione.

Tabella 39-13 Formati di incapsulamento supportati per l'estrazione di file secondari

Nome formato	Estensione formato
7-Zip	7Z
BinHex	HQX
GZIP	GZ
iCalendar	ICS
Archivio Java	JAR
Microsoft Cabinet	CAB

Nome formato	Estensione formato
Cartella compressa Microsoft	LZH
Cartella compressa Microsoft	LHA
Microsoft Visio 2013	VSD
Microsoft Visio 2013 XML	VSDX
Microsoft Visio 2013_Macro	VSDM
Microsoft Visio 2013_Stencil	VSSX
Microsoft Visio 2013_Stencil_Macro	VSSM
Microsoft Visio 2013_Template	VSTX
Microsoft Visio 2013_Template_Macro	VSTM
PKZIP	ZIP
WinZip	ZIP
Archivio RAR	RAR
Archivio su nastro	TAR
UNIX Compress	Z
UUEncoding	UUE
File Virtual Card	File di biglietto da visita elettronico VCF e VCARD
YENC	YENC (solo server)

Formati di file supportati per l'estrazione di metadati

La [Tabella 39-14](#) elenca alcuni dei formati di file supportati da Symantec Data Loss Prevention per il rilevamento di metadati e fornisce alcuni esempi di campi di metadati restituiti per tali formati.

Questo elenco non è definitivo e viene fornito solo come riferimento rapido. È possibile che siano supportati altri formati di file e che siano restituiti altri campi personalizzati. La best practice consiste nell'usare l'utilità *filter* per verificare il supporto dei metadati per ciascun formato di file che si desidera rilevare.

Vedere ["Utilizzare sempre l'utilità filter per verificare il supporto di metadati di formato di file."](#) a pagina 905.

Tabella 39-14 Formati di file supportati per il rilevamento di metadati

Formati di file	Metadati	Descrizione
Documenti di Microsoft Office, ad esempio: <ul style="list-style-type: none"> Word (DOC, DOCX) Excel (XLS, XLSX) PowerPoint (PPT, PPTX) 	Per i documenti di Microsoft Office, il sistema estrae i metadati Object Linking and Embedding (OLE).	Campi di esempio: <ul style="list-style-type: none"> Title Subject Author Parole chiave Altri campi personalizzati
File PDF di Adobe	Per i file PDF di Adobe, il sistema estrae i metadati Document Information Dictionary (DID). Il sistema non supporta l'estrazione di metadati Adobe Extensible Metadata Platform (XMP).	Campi di esempio: <ul style="list-style-type: none"> Author Title Subject Creation Update dates
Microsoft Visio	Estensioni di formato supportate	
Altri formati di file (inclusi binario e testo)	Utilizzare l'utilità <i>filter</i> per verificare l'estrazione di metadati di altri formati di file.	Vedere "Utilizzare sempre l'utilità filter per verificare il supporto di metadati di formato di file." a pagina 905.
Formati di file personalizzati	Metadati tipi di file personalizzati	Plug-in di estrazione contenuto che supporta l'operazione di estrazione di metadati.

Informazioni sul rilevamento dei metadati dei documenti

Oltre all'estrazione di contenuti di file e file secondari, Symantec Data Loss Prevention supporta l'estrazione dei metadati per molti formati di file. I metadati dei formati di file sono dati di un file archiviati come proprietà del file. Per impostazione predefinita l'estrazione dei metadati è disattivata perché può restituire falsi positivi. Utilizzato correttamente, il rilevamento di metadati può migliorare la precisione delle regole di politica basate sul contenuto.

Ad esempio si consideri un'azienda che utilizza i modelli di Microsoft Office per i documenti Word, Excel e PowerPoint. L'azienda applica le proprietà dei metadati Microsoft OLE sotto forma di parole chiave a ciascun modello. L'azienda ha attivato l'estrazione dei metadati e distribuito politiche di parole chiave per cercare la corrispondenza con le parole chiave dei metadati. Queste politiche possono rilevare le parole chiave nei documenti derivati dai modelli. L'azienda ha inoltre la possibilità di utilizzare le eccezioni di politica per evitare di generare incidenti se sono presenti determinate parole chiave dei metadati.

Attivazione del rilevamento di metadati del server

Per impostazione predefinita, l'estrazione di metadati è disattivata per i server di rilevamento.

Per attivare il rilevamento di metadati del server

- 1 Accedere alla console di amministrazione di Enforce Server come amministratore di sistema.
- 2 Passare alla schermata **Sistema > Server e rilevatori > Panoramica > Dettagli server/rilevatore - Impostazioni avanzate** del server di rilevamento o del rilevatore cloud per il quale si desidera attivare l'estrazione di metadati.
- 3 Fare clic sul pulsante **Impostazioni server**.
- 4 Individuare la proprietà `ContentExtraction.EnableMetaData` nell'elenco.
- 5 Immettere il valore **on** affinché questa proprietà permetta l'estrazione di metadati.
- 6 Fare clic su **Salva** per salvare la configurazione.
- 7 Fare clic su **Riciclare il server?** nella schermata **Dettagli server** per riavviare il server.
- 8 Fare clic su **Fine** nella schermata **Dettagli server** per completare il processo.

Attivazione del rilevamento dei metadati dell'endpoint

Per impostazione predefinita, l'estrazione di metadati è disattivata per gli endpoint.

Per attivare l'estrazione di metadati nell'endpoint

- 1 Accedere alla console di amministrazione di Enforce Server come amministratore di sistema.
- 2 Passare alla schermata **Sistema > Agenti > Configurazione agente** del server endpoint in cui si desidera attivare l'estrazione di metadati.
- 3 Creare una nuova configurazione endpoint per il rilevamento di metadati o selezionare la configurazione predefinita.
 Vedere ["Creare una configurazione di endpoint separata per il rilevamento di metadati"](#) a pagina 910.
- 4 Selezionare la tabella **Impostazioni agente avanzate**.
- 5 Individuare la proprietà `Detection.ENABLE_METADATA.str` nell'elenco.
- 6 Immettere il valore **on** affinché questa proprietà permetta l'estrazione di metadati.
- 7 Fare clic su **Salva e applica** per salvare la modifica alla configurazione.

Best practice per l'utilizzo del rilevamento di metadati

[Best practice per l'utilizzo del rilevamento di metadati](#) elenca le best practice per l'implementazione del rilevamento di metadati con collegamenti agli argomenti corrispondenti per informazioni dettagliate.

Tabella 39-15 Considerazioni per l'implementazione del rilevamento di metadati

Considerazione	Argomento
Utilizzare sempre il <i>filtro</i> per verificare il supporto dei metadati del formato di file.	Vedere "Utilizzare sempre l'utilità filter per verificare il supporto di metadati di formato di file." a pagina 905.
Attivare il rilevamento di metadati solo se è necessario.	Vedere "Distinzione tra i metadati e il contenuto dei file o i dati delle applicazioni" a pagina 908.
Evitare di generare falsi positivi selezionando attentamente le parole chiave.	Vedere "Utilizzo e adattamento degli elenchi di parole chiave per evitare falsi positivi per i metadati" a pagina 909.
Esaminare le implicazioni sulle risorse dell'estrazione di metadati endpoint.	Vedere "Implicazioni sulle prestazioni dell'attivazione del rilevamento di metadati sull'endpoint" a pagina 909.
Creare una configurazione endpoint separata per il rilevamento di metadati.	Vedere "Creare una configurazione di endpoint separata per il rilevamento di metadati" a pagina 910.
Utilizzare le regole di risposta per aggiungere tag di metadati agli incidenti.	Vedere "Utilizzo delle regole di risposta per marcare gli incidenti con i metadati" a pagina 910.

Utilizzare sempre l'utilità filter per verificare il supporto di metadati di formato di file.

Per rendere più facile la creazione di politiche per il rilevamento di metadati del formato di file, è possibile impiegare l'utilità *filter*, disponibile con qualsiasi rilevamento Symantec Data Loss Prevention o installazione Endpoint Server. Questa utilità fornisce un metodo semplice per determinare quali campi di metadati vengono restituiti dal sistema per un dato formato di file. L'utilità genera output contenente i metadati che il sistema estrarrà nel runtime per ciascun formato di file sottoposto a testing mediante *filter*.

[Per verificare il supporto dell'estrazione di metadati del formato di file mediante filter](#) descrive come usare l'utilità *filter*. È consigliabile seguire sempre questo processo per creare e adattare politiche che individuano rilevano in modo accurato i metadati del formato di file.

Nota: I dati di output dell'utilità *filter* sono in formato ASCII. Symantec Data Loss Prevention elabora i dati in formato Unicode. Di conseguenza è possibile fare affidamento sull'esistenza dei campi restituiti dall'utilità *filter*, ma i metadati rilevati da Symantec Data Loss Prevention potrebbero non avere un aspetto identico all'output di *filter*.

Per verificare il supporto dell'estrazione di metadati del formato di file mediante *filter*

- 1 Nel file system in cui è installato un server di rilevamento, avviare una sessione del prompt dei comandi.

- 2 Passare alla directory in cui si trova l'utilità *filter*.

Ad esempio, in un'installazione predefinita di Windows a 64 bit, digitare il seguente comando:

```
cd \Program Files\Symantec\Data Loss Prevention\Enforce
Server\15.1\Protect\plugins\contentextraction\Verity\x64
```

- 3 Digitare il seguente comando per eseguire il programma *filter* e visualizzarne la sintassi e i parametri opzionali.

```
filter -help
```

Come indicato nella guida, la seguente sintassi consente di eseguire l'utilità *filter*:

```
filter [options] inputfile outputfile
```

inputfile è un'istanza del formato di file che si desidera verificare. *outputfile* è un file nel quale l'utilità *filter* salva i dati estratti.

Osservare le seguenti opzioni di estrazione:

- Per verificare l'estrazione di metadati, utilizzare l'opzione "ottieni info di riepilogo del documento":-i
- Per verificare l'estrazione del contenuto, non utilizzare alcuna opzione: *filter inputfile outputfile*

- 4 Eseguire *filter* su un'istanza del formato di file per verificare l'estrazione di metadati.

Ad esempio, in Windows immettere il seguente comando:

```
filter -i \temp\myfile.doc \temp\metadata_output.txt
```

dove *myfile.doc* è un file che contiene i metadati che si desidera verificare, copiato nella directory *\temp*, mentre *metadata_output.txt* è il nome del file che verrà generato dal sistema e conterrà i dati estratti.

5 Esaminare l'output di *filter*. L'output sarà simile all'esempio seguente.

```
1 2 1252 CodePage 1 1 "S" Title 0 0 (null) 1 1 "P" Author 0 0 (null)
0 0 (null) 0 1 "" (null) 1 1 "m" LastAuthor 1 1 "1" RevNumber
1 3 6300 Minutes EditTime 1 3 Mon Aug 27 11:53:07 2007 LastPrinted
```

6 Consultare le tabelle che seguono per la spiegazione di ciascun campo di estrazione metadati prodotto dall'utilità *filter*.

[Tabella 39-16](#) ripete l'output del punto 5, formattato per una maggior leggibilità.

[Tabella 39-17](#) illustra ciascun campo colonna.

Tabella 39-16 Esempio di output di metadati di filter

Colonna 1	Colonna 2	Colonna 3	Colonna 4
1	2	1252	CodePage
1	1	"S"	Title
0	0	(null)	
1	1	"P"	Author
0	0	(null)	
0	0	(null)	
0	1	""	(null)
1	1	"m"	LastAuthor
1	1	"1"	RevNumber
1	3	6300 Minutes	EditTime
1	3	Mon Aug 27 11:53:07 2007	LastPrinted

Tabella 39-17 Campi di metadati generati dall'utilità filter

Colonna 1	Colonna 2	Colonna 3	Colonna 4
<p>1 = campo valido</p> <p>0 = campo non valido</p> <p>Nota: È possibile ignorare le righe in cui la prima colonna è 0.</p>	<p>Tipo di dati:</p> <p>1 = stringa</p> <p>2 = intero</p> <p>3 = Data/ora</p> <p>5 = booleano</p>	<p>Payload dei dati per il campo.</p>	<p>Nome del campo (vuoto o null se il campo non è valido).</p>

Distinzione tra i metadati e il contenuto dei file o i dati delle applicazioni

Evitare di confondere l'estrazione di metadati con l'estrazione di contenuto o i dati delle applicazioni. Determinate parti di testo che hanno l'aspetto di metadati sono in realtà estratte come contenuto o dati delle applicazioni. [Tabella 39-18](#) descrive alcuni tipi di dati che non vengono estratti come metadati di formato di file, per rendere più facile decidere se e quando è necessario attivare il rilevamento di metadati.

Nota: Questo elenco non è definitivo e viene fornito solo come riferimento rapido. Possono esistere altri tipi di dati che non vengono estratti come metadati. La best practice consiste nell'usare l'utilità *filter* per verificare il supporto dei metadati di formato di file. Vedere ["Utilizzare sempre l'utilità filter per verificare il supporto di metadati di formato di file."](#) a pagina 905.

Tabella 39-18 Dati non estratti come metadati

Tipo di contenuto	Metodo di estrazione
Dati applicazione	I dati applicazione, incluse le informazioni di trasporto messaggi, vengono estratti separatamente rispetto all'estrazione del formato file. Per tutti i messaggi in arrivo il sistema estrae la busta del messaggio (intestazione) e le informazioni tematiche come testo a livello di applicazione. Il tipo di dati applicazione estratti dipende dai canali supportati dal server o dall'endpoint di rilevamento.
Intestazioni e piè di pagina	<p>Il testo di intestazioni e piè di pagina dei documenti viene estratto come contenuto, non come metadati. Per evitare i falsi positivi, è consigliabile rimuovere o aggiungere a liste bianche le intestazioni e i piè di pagina dei documenti.</p> <p>Vedere "Utilizzare la lista bianca per escludere il contenuto non sensibile dalla corrispondenza parziale" a pagina 611.</p> <p>Per informazioni dettagliate, vedere il capitolo Indexed Document Matching (IDM) nel <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i>.</p>
Testo di markup	<p>Il testo di markup viene estratto come contenuto, non come metadati. L'estrazione di testo di markup è supportata per i formati HTML, XML, SGML e per altri ancora. L'estrazione del testo di markup è disattivata per impostazione predefinita.</p> <p>Vedere "Impostazioni server avanzate" a pagina 279.</p> <p>Vedere "Impostazioni agente avanzate" a pagina 2133.</p> <p>Per attivarla, vedere l'argomento "Impostazioni server avanzate" nel <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i>.</p>

Tipo di contenuto	Metodo di estrazione
Testo nascosto	<p>Il testo nascosto viene estratto come contenuto, non come metadati. L'estrazione del testo nascosto sotto forma di revisioni è supportata per alcuni formati di file di Microsoft Office. L'estrazione del testo nascosto è disattivata per impostazione predefinita.</p> <p>Vedere "Impostazioni server avanzate" a pagina 279.</p> <p>Vedere "Impostazioni agente avanzate" a pagina 2133.</p> <p>Per attivarla, vedere l'argomento "Impostazioni server avanzate" nel <i>Manuale dell'amministratore di Symantec Data Loss Prevention</i>.</p>
Filigrane	<p>Le filigrane basate sul testo vengono estratte come contenuto, non come metadati. Il rilevamento di filigrane basate sul testo è supportato per i documenti Microsoft Word (versioni 2003 e 2007). Non è supportato per altri formati di file.</p>

Utilizzo e adattamento degli elenchi di parole chiave per evitare falsi positivi per i metadati

Se si attiva l'estrazione di metadati è possibile che vengano registrati falsi positivi, perché la corrispondenza viene ricercata in una quantità di testo maggiore. Ad esempio, se è presente una politica che rileva le parole chiave ed è attivata l'estrazione di metadati, la politica segnala una corrispondenza se una parola chiave è presente nel contenuto o nei metadati. Una volta che il sistema ha estratto il contenuto e i metadati, il testo è viene normalizzato e inviato al componente di rilevamento per la corrispondenza. Il componente di rilevamento non può determinare l'origine del testo, ad esempio dati applicazione, contenuto o metadati.

Per rilevare i metadati del formato di file si definiscono condizioni parola chiave per regole o eccezioni contenenti parole chiave specifiche di uno o più formati di file. Per evitare di generare falsi positivi, definire in modo chiaro gli elenchi di parole chiave nelle politiche. Le parole chiave utilizzate per individuare i metadati devono essere uniche e distinte dalle parole chiave o dalle frasi utilizzate per individuare il contenuto. Collaudare e adattare gli elenchi di parole chiave per migliorare l'accuratezza del rilevamento di metadati.

Implicazioni sulle prestazioni dell'attivazione del rilevamento di metadati sull'endpoint

Sull'endpoint l'attivazione dell'estrazione di metadati non aggiunge sovraccarico se non è distribuita alcuna regola del contenuto. Se le regole del contenuto vengono distribuite all'endpoint, l'attivazione dell'estrazione di metadati può generare un leggero sovraccarico perché vi sono extra dati da esaminare. Testare e ottimizzare gli elenchi di parole chiave della politica endpoint per assicurarsi che il rilevamento di metadati sia efficiente.

Creare una configurazione di endpoint separata per il rilevamento di metadati

Quando si attiva il rilevamento metadati negli endpoint, considerare la possibilità di creare una configurazione personalizzata di endpoint specifica per il rilevamento di metadati. In tal modo è possibile tornare facilmente alla configurazione predefinita se necessario.

Utilizzo delle regole di risposta per marcare gli incidenti con i metadati

Non è possibile utilizzare il rilevamento dei metadati per applicare tag a file o documenti in entrata che generano incidenti. Se si desidera disporre di questa opzione, considerare la possibilità di utilizzare un plug-in FlexResponse.

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Per ulteriori informazioni, consultare il *Manuale dell'amministratore di Symantec Data Loss Prevention*.

Libreria degli identificatori di dati del sistema

Il capitolo contiene i seguenti argomenti:

- Libreria degli identificatori di dati del sistema
- Numero di routing ABA
- Numero di identificazione fiscale argentino
- Australian Business Number (partita IVA australiana)
- Codice azienda australiano (ACN)
- Numero Medicare australiano
- Numero di passaporto australiano
- Tax File Number (codice fiscale) australiano
- Numero di passaporto austriaco
- Numero di identificazione fiscale austriaco
- Numero di partita IVA austriaco
- Numero di previdenza sociale austriaco
- Numero di identificazione nazionale belga
- Numero di patente di guida belga
- Numero di passaporto belga
- Numero di identificazione fiscale belga

- Numero di partita IVA belga
- Numero di conto bancario brasiliano
- Numero di tessera elettorale brasiliana
- Numero del Registro Nazionale delle Persone Giuridiche brasiliano
- Codice fiscale per persone fisiche brasiliano (CPF)
- Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica
- Numero di cittadinanza univoco bulgaro (EGN)
- Burgerservicenummer
- Social Insurance Number (numero di previdenza sociale) canadese
- Numero di identificazione nazionale cileno
- Numero di passaporto cinese
- Codice Fiscale
- Indirizzi colombiani
- Numero di cellulare colombiano
- Numero di identificazione personale colombiano
- Tax Identification Number (codice fiscale) colombiano
- Dati banda magnetica per carte di credito
- Numero carta di credito
- Numero CUSIP
- Numero di identificazione personale ceco
- Numero di identificazione personale danese
- Numero di identificazione fiscale danese
- Numero di partita IVA danese
- Numero patente di guida - Stato della California
- Numero di patente di guida - Stati della Florida, del Michigan e del Minnesota
- Numero patente di guida - Stato dell'Illinois
- Numero patente di guida - Stato del New Jersey

- Numero patente di guida - Stato di New York
- Numero di patente di guida - Stato di Washington
- Numero di patente di guida - Stato del Wisconsin
- Numero DEA (Drug Enforcement Agency)
- Numero di patente di guida finlandese
- Numero di previdenza sociale europea della Finlandia
- Numero di passaporto finlandese
- Numero di identificazione fiscale finlandese
- Numero di partita IVA finlandese
- Codice identificativo personale finlandese
- Numero di patente di guida francese
- Numero di previdenza sociale francese
- Numero di identificazione fiscale francese
- Numero di partita IVA francese
- Codice INSEE francese
- Numero di passaporto francese
- Numero di previdenza sociale francese
- Numero di passaporto tedesco
- Numero di identificazione personale tedesco
- Numero di patente di guida tedesca
- Numero di identificazione fiscale tedesco
- Numero di partita IVA tedesca
- Codice fiscale della Grecia (AMKA)
- Codice fiscale greco (AFM)
- Healthcare Common Procedure Coding System (codice CPT HCPCS).
- Numero di assicurazione sanitaria
- ID Hong Kong

- Numero di previdenza sociale ungherese
- Numero di identificazione fiscale ungherese
- Numero di partita IVA ungherese
- IBAN paesi centrali
- IBAN paesi orientali
- IBAN paesi occidentali
- Numero tessera Aadhaar indiana
- Codice di identificazione fiscale indiano (PAN)
- Numero di carta di identità indonesiana (KTP)
- Numero IMEI
- Codice ISIN (International Securities Identification Number)
- Indirizzo IP
- Indirizzo IPv6
- Numero di passaporto irlandese
- Numero di identificazione fiscale irlandese
- Numero di partita IVA irlandese
- Numero personale di servizio pubblico irlandese
- Numero di identificazione personale israeliano
- Numero di patente di guida italiana
- Numero di previdenza sociale italiano
- Numero di passaporto italiano
- Numero di partita IVA italiano
- Numero di patente di guida giapponese
- Numero di passaporto giapponese
- Numero di identificazione giapponese (Juki Net)
- Numero di identificazione personale giapponese - Aziendale
- Numero di identificazione personale giapponese - Personale

- Numero di passaporto coreano
- Numero di registrazione anagrafica coreano per stranieri.
- Numero di registrazione anagrafica coreano per coreani
- Numero di identificazione personale lettone
- Numero di identificazione lussemburghese (RNPP)
- Numero di passaporto lussemburghese
- Numero di identificazione fiscale lussemburghese
- Numero di partita IVA lussemburghese
- Numero di carta di identità malese (MyKad)
- Identificatore beneficiario di assistenza sanitaria
- Numero di registrazione e identificazione personale messicano
- Numero di identificazione fiscale messicano
- Codice di identificazione personale messicano (CURP)
- Numero di conto bancario esteso messicano (CLABE)
- National Drug Code (NDC, codici identificativi dei farmaci)
- Numero NPI
- Numero di patente di guida dei Paesi Bassi
- Numero di passaporto dei Paesi Bassi
- Numero di identificazione fiscale dei Paesi Bassi
- Numero di partita IVA dei Paesi Bassi
- Codice di assistenza sanitaria della Nuova Zelanda (NHI)
- Numero di identificazione personale norvegese
- Documento di identità cinese
- Numero di carta di identità polacca
- Codice statistico polacco (REGON)
- Codice fiscale polacco (PESEL)
- Numero di identificazione fiscale polacco (NIP)

- Numero di patente di guida portoghese
- Numero di identificazione nazionale portoghese
- Numero di passaporto portoghese
- Numero di identificazione fiscale portoghese
- Numero di partita IVA portoghese
- Social Security Number (SSN) statunitense randomizzato
- Numero di identificazione nazionale rumeno
- Numero di identificazione personale rumeno (CNP)
- Numero di passaporto russo interno
- Numero di identificazione fiscale russo (INN)
- Identificatore di dati NRIC Singapore
- Numero di identificazione nazionale slovacco
- Numero identificativo cittadini della Slovenia
- Numero di identificazione personale sudafricano
- Numero di patente di guida spagnola
- Numero di partita IVA spagnolo
- Numero di conto cliente spagnolo
- Numero di DNI spagnolo
- Numero di passaporto spagnolo
- Numero di previdenza sociale spagnolo
- Codice fiscale spagnolo (CIF)
- Numero di patente di guida svedese
- Numero di identificazione fiscale svedese
- Numero di partita IVA svedese
- Numero di passaporto svedese
- Numero di identificazione personale svedese
- Codice SWIFT

- Numero AHV svizzero
- Numero di previdenza sociale svizzero (AHV)
- ID ROC Taiwan
- Numero di identificazione personale thailandese
- Numero di identificazione turco
- Coordinate bancarie di un numero di conto britannico
- Numero di patente di guida britannica
- Numero di tessera elettorale britannico
- Numero NHS (National Health Service) del Regno Unito
- Numero di previdenza sociale britannico
- Numero di passaporto britannico
- Codice fiscale britannico
- Numero di partita IVA britannico (VAT)
- Passaporto ucraino (interno)
- Carta di identità ucraina
- Passaporto ucraino (internazionale)
- Numero di identificazione personale degli Emirati Arabi Uniti
- US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)
- Numero di passaporto statunitense
- Social Security Number (SSN) statunitense
- Codici di avviamento postale Zip+4 statunitensi
- Numero di identificazione nazionale venezuelano

Libreria degli identificatori di dati del sistema

In questa sezione sono elencati tutti gli identificatori dati forniti dal sistema Data Loss Prevention.

Numero di routing ABA

Il numero di routing dell'American Banking Association (ABA), noto anche come Routing Transit Number (RTN, numero d'instradamento) viene utilizzato per l'identificazione di istituzioni finanziarie e l'elaborazione delle transazioni.

L'identificatore di dati del Numero di routing ABA rileva un numero di nove cifre che corrisponde al formato del numero ABA.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre con la convalida del checksum.
Vedere ["Copertura ampia Numero di routing ABA"](#) a pagina 918.
- La copertura media rileva un numero di nove cifre con la convalida del checksum ed elimina i numeri di prova comuni.
Vedere ["Copertura media Numero di routing ABA"](#) a pagina 918.
- La copertura limitata rileva un numero a nove cifre con convalida del checksum, elimina i numeri di test comuni e richiede la presenza di parole chiave correlate.
Vedere ["Copertura limitata Numero di routing ABA"](#) a pagina 919.

Copertura ampia Numero di routing ABA

La copertura ampia rileva un numero di nove cifre con la convalida del checksum.

Tabella 40-1 Modelli copertura ampia Numero di routing ABA

Modello
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

Tabella 40-2 Strumenti di convalida copertura ampia Numero di routing ABA

Strumento di convalida obbligatorio	Descrizione
Checksum ABA	Tutti i numeri di routing ABA devono iniziare con le coppie di cifre 00-15,21-32,61-72,80 e devono passare un checksum specifico di ABA, basato sulle posizioni.

Copertura media Numero di routing ABA

La copertura media rileva un numero di nove cifre con la convalida del checksum ed elimina i numeri di prova comuni.

Tabella 40-3 Modelli copertura media Numero di routing ABA

Modello
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

Tabella 40-4 Strumenti di convalida copertura media Numero di routing ABA

Strumento di convalida obbligatorio	Descrizione
Checksum ABA	Tutti i numeri di routing ABA devono iniziare con le coppie di cifre 00-15,21-32,61-72,80 e devono passare un checksum specifico di ABA, basato sulle posizioni.
Escludi caratteri iniziali	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti quando si utilizza questa opzione. Input: 123456789
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata Numero di routing ABA

La copertura limitata rileva un numero a nove cifre con convalida del checksum, elimina i numeri di test comuni e richiede la presenza di parole chiave correlate.

Tabella 40-5 Modelli copertura limitata Numero di routing ABA

Modello
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

Tabella 40-6 Strumenti di convalida copertura limitata Numero di routing ABA

Strumento di convalida obbligatorio	Descrizione
Checksum ABA	Tutti i numeri di routing ABA devono iniziare con le coppie di cifre 00-15,21-32,61-72,80 e devono passare un checksum specifico di ABA, basato sulle posizioni.

Strumento di convalida obbligatorio	Descrizione
Escludi caratteri iniziali	Quando questa opzione è selezionata, i dati che iniziano con uno qualsiasi dei valori seguenti saranno ignorati. Input: 123456789
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	Quando si utilizza questa opzione, è necessario utilizzare almeno una delle parole o frasi chiave seguenti per ottenere dati corrispondenti. aba, aba #, aba routing #, aba routing number, aba#, abarouting#, abaroutingnumber, american bank association routing #, american bank association routing number, americanbankassociationrouting#, americanbankassociationroutingnumber, bank routing #, bank routing number, bankrouting#, bankroutingnumber
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Numero di identificazione fiscale argentino

L'Argentina rilascia un DNI (Documento Nacional de Identidad) come forma di identificazione nazionale. Viene assegnato alla nascita dal Registro Nacional de las Personas. Ai fini contributivi vengono rilasciati i numeri CUIT e CUIL, basati sul DNI.

L'identificatore di dati Numero di identificazione fiscale argentino rileva un numero di 11 cifre che corrisponde al formato del numero di identificazione fiscale argentino.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.
Vedere ["Copertura ampia numero di identificazione fiscale argentino"](#) a pagina 921.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum. Inoltre verifica la presenza di numeri di test comuni e cifre duplicate.
Vedere ["Copertura media numero di identificazione fiscale argentino"](#) a pagina 921.
- La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum. Inoltre verifica l'esistenza di numeri di prova comuni, cifre doppie e richiede la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di identificazione fiscale argentino"](#) a pagina 922.

Copertura ampia numero di identificazione fiscale argentino

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-7 Criteri copertura ampia numero di identificazione fiscale argentino

Criterio
20-\d{8}-\d
23-\d{8}-\d
27-\d{8}-\d
30-\d{8}-\d
33-\d{8}-\d
34-\d{8}-\d

Tabella 40-8 Strumenti di convalida di copertura ampia del numero di identificazione fiscale argentino

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione fiscale argentino

La copertura media rileva un numero di 11 cifre con la convalida del checksum. Inoltre verifica la presenza di numeri di test comuni e cifre duplicate.

Tabella 40-9 Criteri copertura media numero di identificazione fiscale argentino

Criterio
20-\d{8}-\d
23-\d{8}-\d
27-\d{8}-\d
30-\d{8}-\d
33-\d{8}-\d
34-\d{8}-\d

Tabella 40-10 Convalide copertura media numero di identificazione fiscale argentino

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di identificazione fiscale argentino.	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione fiscale argentino

La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum. Inoltre verifica l'esistenza di numeri di prova comuni, cifre doppie e richiede la presenza di parole chiave associate.

Tabella 40-11 Criteri della copertura limitata del numero di identificazione fiscale argentino

Criterio
20-\d{8}-\d
23-\d{8}-\d
27-\d{8}-\d
30-\d{8}-\d
33-\d{8}-\d
34-\d{8}-\d

Tabella 40-12 Convalide della copertura limitata del numero di identificazione fiscale argentino

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di identificazione fiscale argentino.	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>ID fiscale, codice fiscale, cod. fiscale, ID contribuente, numero di identità fiscale, n. identificazione fiscale, numero di identificazione fiscale, n.IDfiscale, n.idfiscale, numero contribuente, ID contribuente argentino</p> <p>Número de Identificación Fiscal, número de contribuyente</p>

Australian Business Number (partita IVA australiana)

L'Australian Business Number, o ABN, è un identificatore univoco rilasciato dall'Australian Business Register (ABR), gestito dall'Australian Taxation Office (ATO).

L'identificatore di dati Australian Business Number rileva un numero di 11 cifre che corrisponde al formato dell'Australian Business Number.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.
Vedere ["Copertura ampia Australian Business Number"](#) a pagina 923.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum. Elimina inoltre i numeri di prova comuni e gli intervalli riservati per usi futuri.
Vedere ["Copertura media dell'Australian Business Number \(partita IVA australiana\)"](#) a pagina 924.
- La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum. Elimina inoltre i numeri di prova comuni, gli intervalli riservati per usi futuri e le cifre duplicate e richiede la presenza di parole chiave associate all'ABN.
Vedere ["Copertura limitata Australian Business Number \(partita IVA australiana\)"](#) a pagina 925.

Copertura ampia Australian Business Number

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-13 Criteri copertura ampia Australian Business Number (partita IVA australiana)

Criterio
$\backslash d\{11\}$
$\backslash d\{2\}[-]\backslash d\{3\}[-]\backslash d\{3\}[-]\backslash d\{3\}$

Tabella 40-14 Strumenti convalida copertura ampia Australian Business Number (partita IVA australiana)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media dell'Australian Business Number (partita IVA australiana)

La copertura media rileva un numero di 11 cifre con la convalida del checksum. Inoltre, elimina i numeri di prova più comuni, quali 123456789 e gli intervalli riservati per usi futuri.

Tabella 40-15 Criteri della copertura media dell'Australian Business Number (partita IVA australiana)

Criterio
$\backslash d\{11\}$
$\backslash d\{2\}[-]\backslash d\{3\}[-]\backslash d\{3\}[-]\backslash d\{3\}$

Tabella 40-16 Convalida della copertura media dell'Australian Business Number (partita IVA australiana)

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida Australian Business Number (partita IVA australiana)	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata Australian Business Number (partita IVA australiana)

La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum. Inoltre, elimina i numeri di prova più comuni, quali 123456789, gli intervalli numerici riservati per usi futuri, cifre doppie e richiede la presenza di parole chiave relative all'ABN.

Tabella 40-17 Criteri copertura limitata Australian Business Number (partita IVA australiana)

Criterio
<code>\d{11}</code>
<code>\d{2}[-]\d{3}[-]\d{3}[-]\d{3}</code>

Tabella 40-18 Convalide copertura limitata Australian Business Number (partita IVA australiana)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida Australian Business Number (partita IVA australiana)	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Australian Business Number, Business Number, BusinessNumber#, Business Number, Australia Business N., ABN, abn#, businessID#, ID business, abn, ABN#, business number, businessn.#</p>

Codice azienda australiano (ACN)

Il Codice azienda australiano (ACN) è un numero di identificazione univoco di nove cifre rilasciato dall'Australian Securities and Investments Commission a ogni azienda australiana registrata ai sensi del Commonwealth Corporations Act 2001.

L'identificatore di dati per il Numero azienda australiano rileva un numero di nove cifre che corrisponde al formato dell'Australian Company Number.

L'identificatore di dati relativo al codice azienda australiano fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum. Vedere "[Copertura ampia dell'Australian Company Number \(ACN, codice azienda australiano\)](#)" a pagina 926.
- La copertura media rileva un numero di nove cifre con la convalida del checksum. Vedere "[Copertura media Australian Company Number \(ACN, codice azienda australiano\)](#)" a pagina 926.
- La copertura limitata rileva un numero a nove cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate all'ACN. Vedere "[Copertura limitata Australian Company Number \(ACN, codice azienda australiano\)](#)" a pagina 927.

Copertura ampia dell'Australian Company Number (ACN, codice azienda australiano)

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-19 Criterio della copertura ampia dell'Australian Company Number (ACN, codice azienda australiano)

Criterio
\d{3} \d{3} \d{3}

Tabella 40-20 Convalida della copertura ampia dell'Australian Company Number (ACN, codice azienda australiano)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media Australian Company Number (ACN, codice azienda australiano)

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-21 Criterio copertura media Australian Company Number (ACN, codice azienda australiano)

Criterio
\d{3} \d{3} \d{3}

Tabella 40-22 Convalide di copertura media Australian Company Number (ACN, codice azienda australiano)

Convalida obbligatoria	Descrizione
Controllo di convalida codice azienda australiano.	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata Australian Company Number (ACN, codice azienda australiano)

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-23 Criterio copertura limitata Australian Company Number (ACN, codice azienda australiano)

Criterio
\d{3} \d{3} \d{3}

Tabella 40-24 Convalide copertura limitata Australian Company Number (ACN, codice azienda australiano)

Convalida obbligatoria	Descrizione
Controllo di convalida codice azienda australiano.	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: Codice azienda australiano, ACN, N. azienda Australia., N. ACN, ACN No#, Australia Company No#, Numero ACN

Numero Medicare australiano

Il numero Medicare australiano è un codice di identificazione personale australiano assegnato dalla Australian Health Insurance Commission alle persone ritenute idonee nell'ambito del piano Medicare. Questo numero è indicato sulla carta del Medicare australiano.

L'identificatore di dati per il Numero Medicare australiano rileva un numero di 8 o 9 cifre che corrisponde al formato del Numero Medicare australiano.

L'identificatore di dati per il Numero Medicare australiano fornisce tre coperture di rilevazione:

- La copertura ampia rileva un numero di 8 o 9 cifre senza la convalida del checksum. Vedere "[Copertura ampia numero Medicare australiano](#)" a pagina 928.
- La copertura media rileva un numero di 8 o 9 cifre con la convalida del checksum. Vedere "[Copertura media numero Medicare australiano](#)" a pagina 929.
- La copertura limitata rileva un numero di 8 o 9 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata del numero Medicare australiano](#)" a pagina 929.

Copertura ampia numero Medicare australiano

La copertura ampia rileva un numero di 8 o 9 cifre senza la convalida del checksum.

Tabella 40-25 Criteri copertura ampia numero Medicare australiano

Criterio
[2-6]\d{10}
[2-6]\d{9}
[2-6]\d{3} \d{5} \d{1}
[2-6]\d{3}-\d{5}-\d{1}
[2-6]\d{9}[-/]\d{1}
[2-6]\d{3} \d{5} \d{1}[-/]\d{1}
[2-6]\d{3}-\d{5}-\d{1}[-/]\d{1}
[2-6]\d{3} \d{5} \d{1}
[2-6]\d{3}-\d{5}-\d{1}

Tabella 40-26 Convalida copertura ampia numero Medicare australiano

Convalida	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero Medicare australiano

La copertura media rileva un numero di 8 o 9 cifre con la convalida del checksum.

Tabella 40-27 Criteri copertura media numero Medicare australiano

Criterio
[2-6]\d{10}
[2-6]\d{9}
[2-6]\d{3} \d{5} \d{1}
[2-6]\d{3}-\d{5}-\d{1}
[2-6]\d{9} [-/]\d{1}
[2-6]\d{3} \d{5} \d{1} [-/]\d{1}
[2-6]\d{3}-\d{5}-\d{1} [-/]\d{1}
[2-6]\d{3} \d{5} \d \d
[2-6]\d{3}-\d{5}-\d-\d

Tabella 40-28 Convalida copertura media numero Medicare australiano

Convalida	Descrizione
Controllo di convalida del numero Medicare australiano.	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero Medicare australiano

La copertura limitata rileva un numero di 8 o 9 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-29 Criteri di copertura limitata del numero Medicare australiano

Criterio
[2-6]\d{10}
[2-6]\d{9}
[2-6]\d{3} \d{5} \d{1}

Criterio
[2-6]\d{3}-\d{5}-\d{1}
[2-6]\d{9} [-/]\d{1}
[2-6]\d{3} \d{5} \d{1} [-/]\d{1}
[2-6]\d{3}-\d{5}-\d{1} [-/]\d{1}
[2-6]\d{3} \d{5} \d \d
[2-6]\d{3}-\d{5}-\d-\d

Tabella 40-30 Convalide di copertura limitata del numero Medicare australiano

Convalida	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida del numero Medicare australiano.	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero Medicare australiano, numero Medicare, n. Medicare, num. Medicare, n. Medicare australiano, num. Medicare australiano

Numero di passaporto australiano

I passaporti australiani sono documenti di viaggio rilasciati ai cittadini australiani dall’Australian Passport Office of the Department of Foreign Affairs and Trade.

L’identificatore di dati per il Numero di passaporto australiano rileva una stringa alfanumerica di otto caratteri e cifre che corrisponde al formato del Numero di passaporto australiano.

L’identificatore di dati del numero di passaporto australiano fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di otto caratteri senza la convalida del checksum.

Vedere " [Copertura ampia del numero di passaporto australiano](#)" a pagina 931.

- La copertura limitata rileva un modello alfanumerico di otto caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Vedere "[Copertura limitata del numero di passaporto australiano](#)" a pagina 931.

Copertura ampia del numero di passaporto australiano

La copertura ampia rileva una stringa alfanumerica di otto caratteri senza la convalida del checksum.

Tabella 40-31 Criteri copertura ampia numero di passaporto australiano

Criterio
[XBCEGTHJLMNP] \d{7}
[XBCEGTHJLMNP] \d{7}

Tabella 40-32 Convalida copertura ampia del numero di passaporto australiano

Convalida obbligatoria	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 0000000, 1111111, 2222222, 3333333, 4444444, 5555555, 6666666, 7777777, 8888888, 9999999

Copertura limitata del numero di passaporto australiano

La copertura limitata rileva una stringa alfanumerica di otto caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-33 Criteri di copertura limitata del numero di passaporto australiano

Criterio
[XBCEGTHJLMNP] \d{7}
[XBCEGTHJLMNP] \d{7}

Tabella 40-34 Convalide di copertura limitata del numero di passaporto australiano

Convalida obbligatoria	Descrizione
Escludi caratteri finali	Questa convalida esclude i seguenti caratteri nella parte finale del numero: 0000000, 1111111, 2222222, 3333333, 4444444, 5555555, 6666666, 7777777, 8888888, 9999999
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: n. di passaporto australiano, numero di passaporto australiano, numero di passaporto, n.dipassaporto, numerodipassaportoaustraliano

Tax File Number (codice fiscale) australiano

Il Tax File Number (TFN) è un numero di 8 o 9 cifre rilasciato dall'Australian Taxation Office (ATO) ai contribuenti (singoli, aziende, fondi pensione, associazioni o trust) per identificarne le operazioni fiscali effettuate in territorio australiano.

L'identificatore di dati per il Tax File Number (codice fiscale) australiano rileva un numero di 8 o 9 cifre che corrisponde al formato del Tax File Number.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 8 o 9 cifre con la convalida del checksum. Vedere [Tabella 40-35](#) a pagina 932.
- La copertura limitata rileva un numero di 8 o 9 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata Tax File Number \(codice fiscale\) australiano"](#) a pagina 933.

Copertura ampia Tax File Number (codice fiscale) australiano

La copertura ampia rileva un numero di 8 o 9 cifre con la convalida del checksum.

Tabella 40-35 Criteri copertura ampia Tax File Number (codice fiscale) australiano

Modelli
\d{8}
\d{9}

Tabella 40-36 Convalide copertura ampia Tax File Number (codice fiscale) australiano

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione fiscale australiano (ATF)	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata Tax File Number (codice fiscale) australiano

La copertura limitata rileva un numero di 8 o 9 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-37 Criteri copertura limitata Tax File Number (codice fiscale) australiano

Modelli
\d{8}
\d{9}

Tabella 40-38 Strumenti di convalida copertura limitata Tax File Number (codice fiscale) australiano

Convalide obbligatorie	Descrizione
Controllo di convalida numero di identificazione fiscale australiano (ATF)	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: TFN, codice fiscale, Australia TFN, codice fiscale Australia, ATO, ATO TFN, codice fiscale ATO

Numero di passaporto austriaco

I passaporti austriaci sono documenti di viaggio rilasciati ai cittadini austriaci dalle autorità preposte in Austria e all'estero e consentono di effettuare viaggi internazionali.

L'identificatore di dati Numero di passaporto austriaco rileva una stringa alfanumerica di otto caratteri che corrisponde al formato di Numero di passaporto austriaco.

L'identificatore di dati del numero di passaporto austriaco fornisce due coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di otto caratteri senza la convalida del checksum.

Vedere ["Copertura ampia del numero di passaporto austriaco"](#) a pagina 934.

- La copertura limitata rileva una stringa alfanumerica di otto caratteri. Richiede inoltre la presenza di parole chiave associate al passaporto.

Vedere ["Copertura limitata del numero di passaporto austriaco"](#) a pagina 934.

Copertura ampia del numero di passaporto austriaco

La copertura ampia rileva una stringa alfanumerica di otto caratteri senza la convalida del checksum.

Tabella 40-39 Modelli copertura ampia numero di passaporto austriaco

Modelli
<code>\1[]\d{7}</code>
<code>\1\d{7}</code>

Tabella 40-40 Convalida copertura ampia del numero di passaporto austriaco

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata del numero di passaporto austriaco

La copertura limitata rileva una stringa alfanumerica di otto caratteri. Richiede inoltre la presenza di parole chiave associate al passaporto.

Tabella 40-41 Modelli di copertura limitata del numero di passaporto austriaco

Modello
<code>\1[]\d{7}</code>
<code>\1\d{7}</code>

Tabella 40-42 Convalide di copertura limitata del numero di passaporto austriaco

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>REISEPASS, passaporto, ÖSTERREICHISCH REISEPASS, reisePASS</p>

Numero di identificazione fiscale austriaco

L'Austria rilascia numeri di identificazione fiscale di nove cifre a ogni cittadino in base alla loro area di residenza per identificare i contribuenti e agevolare le imposte nazionali.

L'identificatore di dati per il Numero di identificazione fiscale austriaco rileva un numero di nove cifre che corrisponde al formato del Numero di identificazione fiscale austriaco.

Il numero di identificazione fiscale austriaco fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione fiscale austriaco"](#) a pagina 935.
- La copertura limitata rileva un numero di nove cifre. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di identificazione fiscale austriaco"](#) a pagina 936.

Copertura ampia del numero di identificazione fiscale austriaco

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-43 Modelli copertura ampia del numero di identificazione fiscale austriaco

Modello
$\backslash d\{2\}-\backslash d\{3\}/\backslash d\{4\}$
$\backslash d\{2\} \backslash d\{3\} \backslash d\{4\}$
$\backslash d\{9\}$

Tabella 40-44 Convalide di copertura ampia del numero di identificazione fiscale austriaco

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di identificazione fiscale austriaco

La copertura limitata rileva un numero di nove cifre. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-45 Modelli di copertura limitata del numero di identificazione fiscale austriaco

Modelli
$\backslash d\{2\}-\backslash d\{3\}/\backslash d\{4\}$
$\backslash d\{2\} \backslash d\{3\} \backslash d\{4\}$
$\backslash d\{9\}$

Tabella 40-46 Convalide di copertura limitata del numero di identificazione fiscale austriaco

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: Austria, TIN, numero identificazione fiscale, codice fiscale, Codice Fiscale Austriaco, Österreich, Steuernummer

Numero di partita IVA austriaco

L'imposta sul valore aggiunto (IVA) è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Austria, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.

L'identificatore di dati della partita IVA austriaca rileva un modello alfanumerico di 11 caratteri che corrisponde al formato del Numero di partita IVA austriaco.

L'identificatore di dati della partita IVA austriaca fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 11 caratteri preceduto da **ATU** senza la convalida del checksum.
Vedere "[Copertura ampia numero di partita IVA austriaco](#)" a pagina 937.
- La copertura media rileva un modello alfanumerico di 11 caratteri preceduto da **ATU** con la convalida del checksum.
Vedere "[Copertura media del numero di partita IVA austriaco](#)" a pagina 937.
- La copertura limitata rileva un modello alfanumerico di 11 caratteri preceduto da **ATU** con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di partita IVA austriaco](#)" a pagina 938.

Copertura ampia numero di partita IVA austriaco

La copertura ampia rileva un modello alfanumerico di 11 caratteri preceduto da **ATU** senza la convalida del checksum.

Tabella 40-47 Modelli di copertura ampia numero di partita IVA austriaco

Modelli
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{3} \d{4} \d
[Aa] [Tt] [Uu] \d{2} \d{4} \d{2}

Tabella 40-48 Convalide di copertura ampia numero di partita IVA austriaco

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	Esclude le seguenti stringhe di caratteri finali: 00000000, 11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999

Copertura media del numero di partita IVA austriaco

La copertura media rileva un modello alfanumerico di 11 caratteri preceduto da **ATU** con la convalida del checksum.

Tabella 40-49 Modelli di copertura media del numero di partita IVA austriaco

Modelli
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{3} \d{4} \d
[Aa] [Tt] [Uu] \d{2} \d{4} \d{2}

Tabella 40-50 Convalide di copertura media del numero di partita IVA austriaco

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA austriaco	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di partita IVA austriaco

La copertura limitata rileva un modello alfanumerico di 11 caratteri preceduto da ATU con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate all'IVA.

Tabella 40-51 Modelli di copertura limitata del numero di partita IVA austriaco

Modelli
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{8}
[Aa] [Tt] [Uu] \d{3} \d{4} \d
[Aa] [Tt] [Uu] \d{2} \d{4} \d{2}

Tabella 40-52 Convalide di copertura limitata del numero di partita IVA austriaco

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di partita IVA austriaco	Calcola il checksum e lo utilizza per convalidare il modello.

Convalide obbligatorie	Descrizione
Escludi caratteri finali	Esclude le seguenti stringhe di caratteri finali: 00000000, 11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero partita iva, iva, n. partita iva, numero partita iva austriaco, num. partita iva, numiva, numero imposta valore aggiunto, MwSt, Umsatzsteuernummer, MwStNummer, Ust.Umsatzsteuer -Identifikationsnummer,, Umsatzsteuer-Identifikationsnummer, numero di identificazione IVA, numero atu, numero uid

Numero di previdenza sociale austriaco

Il numero di previdenza sociale austriaco è composto da 10 cifre ed è assegnato ai cittadini austriaci che usufruiscono di prestazioni di assistenza sociale. È rilasciato da un'associazione ombrello dell'ente di previdenza sociale austriaco.

L'identificatore di dati per il Numero di previdenza sociale austriaco rileva un numero 10 cifre che corrisponde al formato del Numero di previdenza sociale austriaco.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum. Vedere ["Portata ampia del numero di previdenza sociale austriaco"](#) a pagina 939.
- La copertura media rileva un numero di 10 cifre che supera la convalida del checksum. Elimina inoltre i numeri di prova comuni e gli intervalli riservati per usi futuri. Vedere ["Copertura media del numero di previdenza sociale austriaco"](#) a pagina 940.
- La copertura limitata rileva un numero di 10 cifre che supera la convalida del checksum. Inoltre, elimina i numeri di prova più comuni, gli intervalli numerici riservati per usi futuri, cifre doppie e richiede la presenza di parole chiave relative al numero di previdenza sociale austriaco. Vedere ["Copertura limitata del numero di previdenza sociale austriaco"](#) a pagina 940.

Portata ampia del numero di previdenza sociale austriaco

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-53 Criteri di copertura ampia del numero di previdenza sociale austriaco

Criterio
\d{10}
\d{4}-\d{6}
\d{4} \d{6}

Tabella 40-54 Convalide di copertura ampia del numero di previdenza sociale austriaco

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di previdenza sociale austriaco

La copertura limitata rileva un numero di 10 cifre che supera la convalida del checksum. Inoltre, elimina i numeri di prova più comuni, quali 123456789 e gli intervalli riservati per usi futuri.

Tabella 40-55 Criteri copertura media del numero di previdenza sociale austriaco

Criterio
\d{10}
\d{4}-\d{6}
\d{4} \d{6}

Tabella 40-56 Convalida copertura media del numero di previdenza sociale austriaco

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di previdenza sociale austriaco	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di previdenza sociale austriaco

La copertura limitata rileva un numero di 10 cifre che supera la convalida del checksum. Inoltre, elimina i numeri di prova più comuni, gli intervalli numerici riservati per usi futuri, cifre doppie e richiede la presenza di parole chiave relative al numero di previdenza sociale austriaco.

Tabella 40-57 Criteri di copertura limitata del numero di previdenza sociale austriaco

Criterio
\d{10}
\d{4}-\d{6}
\d{4} \d{6}

Tabella 40-58 Convalide di copertura limitata del numero di previdenza sociale austriaco

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di previdenza sociale austriaco	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>n di previdenza sociale, numero di previdenza sociale, codice di previdenza sociale, SSN austriaco, SSN#, ssn#, SSN, ssn, previdenzasociale#, sozialversicherungsnummer, soziale sicherheit kein, sozialversicherungsnummer#, sozialesicherheitkein#</p> <p>numero di previdenza sociale, codice di previdenza sociale#, n previdenza sociale, numero assicurazione sanitaria, assicurazione sanitaria, n assicurazione sanitaria, numero EHIC, n EHIC</p> <p>versicherungsnummer, versicherungscode, nationale versicherungsnummer, krankenkassennummer, krankenversicherung</p> <p>zdravstveno zavarovanje</p> <p>EHIC Nummer, Österreichischen SSN, Österreichischen Sozialversicherungs kein</p> <p>številka zavarovanja, biztosítási szám, zavarovalna šifra, biztosítási kód, társadalombiztosítási azonosító jel, nacionalna številka zavarovanja, egészségbiztosítási szám, številka zdravstvenega zavarovanja, egészségbiztosítás, EHIC szám, Številka EHIC</p>

Numero di identificazione nazionale belga

Tutti i cittadini del Belgio hanno un numero di identificazione nazionale. I belgi di età superiore ai 12 anni possiedono una carta d'identità belga. Il numero di identificazione nazionale belga è utilizzato inoltre come numero di codice fiscale per i cittadini in Belgio.

L'identificatore di dati per il Numero di identificazione nazionale belga rileva un numero di 11 cifre che corrisponde al formato del Numero di identificazione nazionale belga.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.
Vedere "[Copertura ampia numero di identificazione nazionale belga](#)" a pagina 943.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Vedere ["Copertura media del numero di identificazione nazionale belga"](#) a pagina 943.

- La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Vedere ["Copertura limitata numero di identificazione nazionale belga"](#) a pagina 944.

Copertura ampia numero di identificazione nazionale belga

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-59 Criteri copertura ampia numero di identificazione nazionale belga

Criterio
$\backslash d\{11\}$
$\backslash d\{6\} \backslash d\{3\} \backslash d\{2\}$
$\backslash d\{2\}.\backslash d\{2\}.\backslash d\{2\}-\backslash d\{3\}.\backslash d\{2\}$
$\backslash d\{2\}[\ .] [012345] \backslash d[\ .] [0123] \backslash d[\ -.] \backslash d\{3\}[\ -.] \backslash d\{2\}$

Tabella 40-60 Convalide copertura ampia numero di identificazione nazionale belga

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione nazionale belga

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-61 Criteri di copertura media del numero di identificazione nazionale belga

Criterio
$\backslash d\{11\}$
$\backslash d\{6\} \backslash d\{3\} \backslash d\{2\}$
$\backslash d\{2\}.\backslash d\{2\}.\backslash d\{2\}-\backslash d\{3\}.\backslash d\{2\}$
$\backslash d\{2\}[\ .] [012345] \backslash d[\ .] [0123] \backslash d[\ -.] \backslash d\{3\}[\ -.] \backslash d\{2\}$

Tabella 40-62 Convalida copertura media del numero di identificazione nazionale belga

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di identificazione nazionale belga	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di identificazione nazionale belga

La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-63 Criterio copertura limitata numero di identificazione nazionale belga

Criterio
<code>\d{11}</code>
<code>\d{6} \d{3} \d{2}</code>
<code>\d{2}.\d{2}.\d{2}-\d{3}.\d{2}</code>
<code>\d{2}[.][012345]\d[.][0123]\d[-.]\d{3}[.-]\d{2}</code>

Tabella 40-64 Strumenti di convalida copertura limitata numero di identificazione nazionale belga

Convalida obbligatoria	Descrizione
Controllo di convalida del numero di identificazione nazionale belga	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numero di identificazione nazionale belga, numero di identificazione nazionale, codice fiscale, numeroidentificazione#, ssn#, ssn, numeroidentificazione, bnn#, n, numero di identificazione personale, numeroIDpersonale#</p> <p>Numéro national, numéro de sécurité, numéro d'assuré, identifiant national, identifiantnational#, Numéronational#</p>

Numero di patente di guida belga

Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Belgio.

L'identificatore di dati per il Numero di patente di guida belga rileva un numero 10 cifre che corrisponde al formato del Numero di patente di guida belga.

L'identificatore di dati del numero di patente di guida belga fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum. Vedere ["Copertura ampia del Numero di patente di guida belga"](#) a pagina 945.
- La copertura limitata rileva un numero di 10 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata del Numero di patente di guida belga"](#) a pagina 946.

Copertura ampia del Numero di patente di guida belga

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-65 Modello di copertura ampia del Numero di patente di guida belga

Modello
<code>\d{10}</code>

Tabella 40-66 Convalide di copertura ampia del Numero di patente di guida belga

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del Numero di patente di guida belga

La copertura limitata rileva un numero di 10 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-67 Modello di copertura limitata del Numero di patente di guida belga

Modello
<code>\d{10}</code>

Tabella 40-68 Convalide di copertura limitata del numero di patente di guida belga

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Führerschein, Fuhrerschein, Fuehrerschein, Führerscheinnnummer, Fuhrerscheinnnummer, Fuehrerscheinnnummer, Führerscheinnnummer, Fuhrerscheinnnummer, Fuehrerscheinnnummer, Führerschein- Nr, Fuhrerschein- Nr, Fuehrerschein-Nr</p> <p>Num. patente, Patente di guida, Numero Patente di Guida, numero patente di guida, Patente Guida, Pat. Guida, Patente di guida, Patente guida, Pat. di guida, Numero pat. guida, numero pat. guida, num. patente di guida, Num. Pat. guida, numero patente guida, Num. Patente, num. patente</p> <p>permis de conduire, rijbewijs, Rijbewijsnummer, Numéro permis conduire</p>

Numero di passaporto belga

Il passaporto belga è rilasciato dallo stato belga ai suoi cittadini per consentire loro di viaggiare all'estero. Il Servizio pubblico federale degli Affari Esteri, in precedenza noto come Ministero degli Affari Esteri, è responsabile del rilascio e del rinnovo dei passaporti belgi.

L'identificatore di dati per il Numero di passaporto belga rileva una stringa alfanumerica di otto caratteri che corrisponde al formato di Numero di passaporto belga.

L'identificatore di dati del numero di passaporto belga fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di otto caratteri senza la convalida del checksum.
Vedere ["Copertura ampia numero di passaporto belga"](#) a pagina 947.
- La copertura limitata rileva un modello alfanumerico di otto caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di passaporto belga"](#) a pagina 948.

Copertura ampia numero di passaporto belga

La copertura ampia rileva una stringa alfanumerica di otto caratteri senza la convalida del checksum.

Tabella 40-69 Modello copertura ampia numero di passaporto belga

Modello
\1{2}\d{6}

Tabella 40-70 Convalida di copertura ampia numero di passaporto belga

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata numero di passaporto belga

La copertura limitata rileva una stringa alfanumerica di otto caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-71 Modelli di copertura limitata del numero di passaporto belga

Criteri
\1{2}\d{6}

Tabella 40-72 Modelli di copertura limitata del numero di passaporto belga

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di passaporto</p> <p>Paspoort, paspoort, paspoortnummer, Reisepass kein, Reisepass, Passnummer, Passeport, Passeport livre, Passeport carte, numéro passeport</p> <p>Numero di passaporto belga, numero di passaporto belga, n passaporto</p>

Numero di identificazione fiscale belga

Il Belgio rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Belgio.

L'identificatore di dati per il Numero di identificazione fiscale belga rileva un numero di 11 cifre che corrisponde al formato del Numero di identificazione fiscale belga.

L'identificatore dati del numero di identificazione fiscale belga fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura ampia del numero di identificazione fiscale belga](#)" a pagina 949.
- La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di identificazione fiscale belga](#)" a pagina 950.

Copertura ampia del numero di identificazione fiscale belga

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-73 Modelli copertura ampia numero di identificazione fiscale belga

Modelli
$\backslash d\{2\}[01]\backslash d[0123]\backslash d\{6\}$
$\backslash d\{2\}[01]\backslash d[0123]\backslash d\ \backslash d\{3\}\ \backslash d\{2\}$
$\backslash d\{2\}.\{01\}\backslash d.\{0123\}\backslash d-\backslash d\{3\}.\backslash d\{2\}$
$\backslash d\{2\}[\ .][01]\backslash d[\ .][0123]\backslash d[\ -.]\backslash d\{3\}[\ .-]\backslash d\{2\}$

Tabella 40-74 Convalide copertura ampia numero di identificazione fiscale belga

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero fiscale, numero di registrazione nazionale, Numero di Registrazione Nazionale, numero di registrazione fiscale, id fiscale, ID fiscale, Numero Fiscale</p> <p>Numéro de registre national, numéro d'identification fiscale, belasting aantal, Steuernummer, NIF, nif, NIF#, nif#</p>

Copertura limitata del numero di identificazione fiscale belga

La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum.
 Richiede inoltre la presenza di parole chiave associate.

Tabella 40-75 Modelli copertura limitata numero di identificazione fiscale belga

Modelli
$\backslash d\{2\}[01]\backslash d[0123]\backslash d\{6\}$
$\backslash d\{2\}[01]\backslash d[0123]\backslash d\ \backslash d\{3\}\ \backslash d\{2\}$
$\backslash d\{2\}.\ [01]\backslash d.\ [0123]\backslash d-\backslash d\{3\}.\ \backslash d\{2\}$
$\backslash d\{2\}[\ .][01]\backslash d[\ .][0123]\backslash d[\ -.]\backslash d\{3\}[\ .-]\backslash d\{2\}$

Tabella 40-76 Convalide copertura limitata del numero di identificazione fiscale belga

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione fiscale belga	Convalida checksum per il numero di identificazione fiscale belga
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero fiscale, numero di registrazione nazionale, Numero di Registrazione Nazionale, numero di registrazione fiscale, id fiscale, ID fiscale, Numero Fiscale</p> <p>Numéro de registre national, numéro d'identification fiscale, belasting aantal, Steuernummer, NIF, nif, NIF#, nif#</p>

Numero di partita IVA belga

L'imposta sul valore aggiunto (IVA) è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Belgio, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.

Il numero di partita IVA belga (IVA) rileva una stringa alfanumerica di 12 caratteri che corrisponde al formato del Numero di partita IVA belga (IVA).

L'identificatore di dati della partita IVA belga fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 12 caratteri che iniziano con **BE** senza la convalida del checksum.
Vedere ["Copertura ampia numero di partita IVA belga"](#) a pagina 951.
- La copertura media rileva una stringa alfanumerica di 12 caratteri che iniziano con **BE** con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA belga"](#) a pagina 952.
- La copertura limitata rileva una stringa alfanumerica di 12 caratteri che iniziano con **BE** con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di partita IVA belga"](#) a pagina 952.

Copertura ampia numero di partita IVA belga

La copertura ampia rileva una stringa alfanumerica di 12 caratteri che iniziano con **BE** senza la convalida del checksum.

Tabella 40-77 Modelli di copertura ampia numero di partita IVA belga

Modelli
[Bb] [Ee] [0] [123456789] \d{8}
[Bb] [Ee] [0] [123456789] . \d{4} . \d{4}
[Bb] [Ee] [0] [123456789] - \d{4} - \d{4}
[Bb] [Ee] [0] [123456789] \d{4} \d{4}

Tabella 40-78 Convalida di copertura ampia numero di partita IVA belga

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero di partita IVA belga

La copertura media rileva un modello alfanumerico di 12 caratteri che inizia con **BE** con la convalida del checksum.

Tabella 40-79 Modelli di copertura media del numero di partita IVA belga

Modelli
[Bb] [Ee] [0] [123456789] \d{8}
[Bb] [Ee] [0] [123456789] . \d{4} . \d{4}
[Bb] [Ee] [0] [123456789] - \d{4} - \d{4}
[Bb] [Ee] [0] [123456789] \d{4} \d{4}

Tabella 40-80 Convalide di copertura media del numero di partita IVA belga

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA belga	Convalida checksum per il numero di partita IVA belga.

Copertura limitata numero di partita IVA belga

La copertura limitata rileva una stringa alfanumerica di 12 cifre che iniziano con **BE** con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-81 Modelli copertura limitata numero di partita IVA belga

Modello
[Bb] [Ee] [0] [123456789] \d{8}
[Bb] [Ee] [0] [123456789] . \d{4} . \d{4}
[Bb] [Ee] [0] [123456789] - \d{4} - \d{4}
[Bb] [Ee] [0] [123456789] \d{4} \d{4}

Tabella 40-82 Convalide di copertura limitata numero di partita IVA belga

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di partita IVA belga	Convalida checksum per il numero di partita IVA belga.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numéro T.V.A., numero BTW, N° TVA, BTW NR, partita IVA, p.IVA, partita iva, Numéro T.V.A, Umsatzsteuer-Identifikationsnummer, Umsatzsteuernummer, BTW, BTW#, n.IVA, n.iva</p>

Numero di conto bancario brasiliano

È il numero di conto bancario utilizzato comunemente in Brasile.

L'identificatore di dati per il Numero di conto bancario brasiliano rileva un numero di 9 o 10 cifre che corrisponde al formato del Numero di conto bancario brasiliano.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 9 o 10 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di conto bancario brasiliano"](#) a pagina 954.
- La copertura media rileva un numero di 9 o 10 cifre con la convalida del checksum. Vedere ["Copertura media numero di conto bancario brasiliano"](#) a pagina 954.
- La copertura limitata rileva un numero di 9 o 10 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata del numero di conto bancario brasiliano"](#) a pagina 954.

Copertura ampia del numero di conto bancario brasiliano

La copertura ampia rileva un numero di 9 o 10 cifre senza la convalida del checksum.

Tabella 40-83 Criteri di copertura ampia del numero di conto bancario brasiliano

Criterio
$\backslash d \backslash d \backslash d [, -] \backslash d \backslash d \backslash d \backslash d [, -] \backslash d$
$\backslash d \backslash d \backslash d [, -] \backslash d \backslash d \backslash d \backslash d [, -] \backslash d$
$\backslash d \backslash d \backslash d [, -] \backslash d \backslash d \backslash d \backslash d [, -] \backslash d$

Tabella 40-84 Convalida della copertura ampia del numero di conto bancario brasiliano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di conto bancario brasiliano

La copertura media rileva un numero di 9 o 10 cifre con la convalida del checksum.

Tabella 40-85 Criteri copertura media numero di conto bancario brasiliano

Criterio
$\backslash d \backslash d \backslash d [, -] \backslash d \backslash d \backslash d \backslash d [, -] \backslash d$
$\backslash d \backslash d \backslash d [, -] \backslash d \backslash d \backslash d \backslash d [, -] \backslash d$
$\backslash d \backslash d \backslash d [, -] \backslash d \backslash d \backslash d \backslash d [, -] \backslash d$

Tabella 40-86 Strumento di convalida copertura media numero di conto bancario brasiliano

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di conto bancario brasiliano	Lo strumento di convalida calcola il checksum che ogni numero di conto bancario brasiliano deve superare.

Copertura limitata del numero di conto bancario brasiliano

La copertura limitata rileva un numero di 9 o 10 cifre che supera la convalida del checksum.
 Richiede inoltre la presenza di parole chiave associate.

Tabella 40-87 Criteri di copertura limitata del numero di conto bancario brasiliano

Criterio
\d\d\d\d[;-]\d\d\d\d\d[;-]\d
\d\d\d[d,;-]\d\d\d\d\d[d,;-]\d
\d\d\d[d,;-]\d\d\d\d\d[d,;-]\d

Tabella 40-88 Convalida di copertura limitata del numero di conto bancario brasiliano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di conto bancario brasiliano	Lo strumento di convalida calcola il checksum che ogni numero di conto bancario brasiliano deve superare.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numero di conto bancario, n. conto bancario, n. conto, numero conto, n. conto bancario Itau, n.conto, n.contobancario, n.contoltau</p> <p>número conta bancária, número da conta, conta n, Conta bancária Itaú Número, código de conta bancária, Conta Sem</p>

Numero di tessera elettorale brasiliana

In Brasile il voto è obbligatorio per tutti i cittadini di età compresa tra i 18 e i 70 anni. Per avere diritto al voto, i cittadini devono essere registrati e presentare un documento di identità valido, in genere la tessera elettorale.

Il Numero di tessera elettorale brasiliana rileva un numero che va dalle 9 alle 14 cifre, che corrisponde al formato del Numero di tessera elettorale brasiliana.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero contenente da 9 a 14 cifre senza la convalida del checksum.
Vedere ["Copertura ampia numero di tessera elettorale brasiliana"](#) a pagina 956.

- La copertura media rileva un numero contenente da 9 a 14 cifre che supera la convalida del checksum.
Vedere "Copertura media numero di tessera elettorale brasiliana" a pagina 957.
- La copertura limitata rileva un numero che va dalle 9 alle 14 cifre e che supera la convalida del checksum, e richiede la presenza di parole chiave associate.
Vedere "Copertura limitata numero di tessera elettorale brasiliana" a pagina 958.

Copertura ampia numero di tessera elettorale brasiliana

La copertura ampia rileva un numero contenente da 9 a 14 cifre senza la convalida del checksum.

Tabella 40-89 Criteri copertura ampia numero di tessera elettorale brasiliana

Modelli
\d{5}[0]\d{3}
\d{5}[12]\d\d{2}
\d{6}[0]\d{3}
\d{6}[0]\d[/]\d{2}
\d{6}[12]\d\d{2}
\d{6}[12]\d[/]\d{2}
\d{7}[0]\d{3}
\d{7}[0]\d[/]\d{2}
\d{7}[12]\d[/]\d{2}
\d{7}[12]\d\d{2}
\d{8}[0]\d{3}
\d{8}[0]\d[/]\d{2}
\d{8}[0]\d{3}[/]\d{2}
\d{8}[12]\d[/]\d{2}
\d{8}[12]\d\d{2}
\d{8}[12]\d\d{2}[/]\d{2}

Tabella 40-90 Strumento di convalida copertura ampia numero di tessera elettorale brasiliana

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di tessera elettorale brasiliana

La copertura media rileva un numero contenente da 9 a 14 cifre che supera la convalida del checksum.

Tabella 40-91 Criteri copertura media numero di tessera elettorale brasiliana

Modelli
\d{5}[0]\d{3}
\d{5}[12]\d\d{2}
\d{6}[0]\d{3}
\d{6}[0]\d[/]\d{2}
\d{6}[12]\d\d{2}
\d{6}[12]\d[/]\d{2}
\d{7}[0]\d{3}
\d{7}[0]\d[/]\d{2}
\d{7}[12]\d[/]\d{2}
\d{7}[12]\d\d{2}
\d{8}[0]\d{3}
\d{8}[0]\d[/]\d{2}
\d{8}[0]\d{3}[/]\d{2}
\d{8}[12]\d[/]\d{2}
\d{8}[12]\d\d{2}
\d{8}[12]\d\d{2}[/]\d{2}

Tabella 40-92 Convalide di copertura media Numero di tessera elettorale brasiliana

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di tessera elettorale brasiliana	Calcola il checksum che ogni numero di tessera elettorale brasiliana deve superare.

Copertura limitata numero di tessera elettorale brasiliana

La copertura limitata rileva un numero da 9 a 14 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-93 Criteri copertura limitata numero di tessera elettorale brasiliana

Modelli
$\backslash d\{5\}[0]\backslash d\{3\}$
$\backslash d\{5\}[12]\backslash d\backslash d\{2\}$
$\backslash d\{6\}[0]\backslash d\{3\}$
$\backslash d\{6\}[0]\backslash d[/]\backslash d\{2\}$
$\backslash d\{6\}[12]\backslash d\backslash d\{2\}$
$\backslash d\{6\}[12]\backslash d[/]\backslash d\{2\}$
$\backslash d\{7\}[0]\backslash d\{3\}$
$\backslash d\{7\}[0]\backslash d[/]\backslash d\{2\}$
$\backslash d\{7\}[12]\backslash d[/]\backslash d\{2\}$
$\backslash d\{7\}[12]\backslash d\backslash d\{2\}$
$\backslash d\{8\}[0]\backslash d\{3\}$
$\backslash d\{8\}[0]\backslash d[/]\backslash d\{2\}$
$\backslash d\{8\}[0]\backslash d\{3\}[/]\backslash d\{2\}$
$\backslash d\{8\}[12]\backslash d[/]\backslash d\{2\}$
$\backslash d\{8\}[12]\backslash d\backslash d\{2\}$
$\backslash d\{8\}[12]\backslash d\backslash d\{2\}[/]\backslash d\{2\}$

Tabella 40-94 Convalide di copertura limitata Numero di tessera elettorale brasiliana

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di tessera elettorale brasiliana	Calcola il checksum che ogni numero di tessera elettorale brasiliana deve superare.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>ID elettorale, numero di identificazione, num. elettorale, ID votante, numero identificazione elettorale, ID votanti, numero elettorale, ID votante elezioni, numero elettorale, num. elett., numero identificativo, num. identificativo elezioni</p> <p>número de identificação, identificação do eleitor, número de identificação eleitoral, ID eleitor eleição, Número identificação eleitoral brasileira</p>

Numero del Registro Nazionale delle Persone Giuridiche brasiliano

Il numero del Registro Nazionale delle Persone Giuridiche (CNPJ) è un numero univoco che identifica un'entità o un altro istituto giuridico privi di personalità giuridica rilasciato dal Brazilian Internal Revenue Service (un'agenzia del Ministero delle Finanze).

L'identificatore di dati per il Numero del Registro Nazionale delle Persone Giuridiche brasiliano (CNPJ) rileva un numero di 14 cifre che corrisponde al formato del Numero del Registro Nazionale delle Persone Giuridiche brasiliano (CNPJ).

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 14 cifre senza la convalida del checksum. Vedere ["Copertura ampia numero del Registro Nazionale delle Persone Giuridiche brasiliano"](#) a pagina 960.
- La copertura media rileva un numero a 14 cifre con la convalida del checksum. Vedere ["Copertura media numero del Registro Nazionale delle Persone Giuridiche brasiliano"](#) a pagina 960.

- La copertura limitata rileva un numero di 14 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero del Registro Nazionale delle Persone Giuridiche brasiliano](#)" a pagina 961.

Copertura ampia numero del Registro Nazionale delle Persone Giuridiche brasiliano

La copertura ampia rileva un numero di 14 cifre senza la convalida del checksum.

Tabella 40-95 Criteri copertura ampia numero del Registro Nazionale delle Persone Giuridiche brasiliano

Criterio
$\backslash d\{14\}$
$\backslash d\{8\}[/]\backslash d\{6\}$
$\backslash d\{8\}[/]\backslash d\{4\}-\backslash d\{2\}$
$\backslash d\{2\}.\backslash d\{3}.\backslash d\{3\}[/]\backslash d\{4\}-\backslash d\{2\}$

Tabella 40-96 Strumento di convalida copertura ampia numero del Registro Nazionale delle Persone Giuridiche brasiliano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero del Registro Nazionale delle Persone Giuridiche brasiliano

La copertura media rileva un numero a 14 cifre con la convalida del checksum.

Tabella 40-97 Criteri copertura media numero del Registro Nazionale delle Persone Giuridiche brasiliano

Criterio
$\backslash d\{14\}$
$\backslash d\{8\}[/]\backslash d\{6\}$
$\backslash d\{8\}[/]\backslash d\{4\}-\backslash d\{2\}$

Criterio
$\backslash d\{2\}.\backslash d\{3}.\backslash d\{3}\left[/\right] \backslash d\{4\}-\backslash d\{2\}$

Tabella 40-98 Strumento di convalida copertura media numero del Registro Nazionale delle Persone Giuridiche brasiliano

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di Registro Nazionale delle Persone Giuridiche brasiliano	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero del Registro Nazionale delle Persone Giuridiche brasiliano

La copertura limitata rileva un numero di 14 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-99 Criteri copertura limitata numero del Registro Nazionale delle Persone Giuridiche brasiliano

Criterio
$\backslash d\{14\}$
$\backslash d\{8\}\left[/\right] \backslash d\{6\}$
$\backslash d\{8\}\left[/\right] \backslash d\{4\}-\backslash d\{2\}$
$\backslash d\{2\}.\backslash d\{3}.\backslash d\{3}\left[/\right] \backslash d\{4\}-\backslash d\{2\}$

Tabella 40-100 Convalida copertura limitata numero del Registro Nazionale delle Persone Giuridiche brasiliano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di Registro Nazionale delle Persone Giuridiche brasiliano	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero persone giuridiche brasiliane, n. persone giuridiche, ID giuridico, n. giuridico, numero persone giuridiche, numero giuridico, n. giuridico, numero persone giuridiche, CNPJ, CNPJ:, CNPJ#, cnpj#, n. cnpj CNPJ, n. Registro Nacional de Pessoas Jurídicas, entidades jurídicas ID</p>

Codice fiscale per persone fisiche brasiliano (CPF)

Il Cadastro de Pessoas Físicas (CPF, "Codice fiscale per persone fisiche") è un numero attribuito dall'agenzia delle entrate ai brasiliani e alle persone residenti in Brasile che pagano le tasse o che prendono parte, direttamente o indirettamente, ad attività che producono reddito e sono soggette a una qualsiasi delle numerose imposte esistenti in Brasile.

L'identificatore di dati per il Codice fiscale per persone fisiche brasiliano (CPF) rileva un numero di 11 cifre che corrisponde al formato del Codice fiscale per persone fisiche brasiliano (CPF).

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.
Vedere "[Copertura ampia codice fiscale per persone fisiche brasiliano \(CPF\)](#)" a pagina 962.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum.
Vedere "[Copertura media codice fiscale per persone fisiche brasiliano \(CPF\)](#)" a pagina 963.
- La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata codice fiscale per persone fisiche brasiliano \(CPF\)](#)" a pagina 963.

Copertura ampia codice fiscale per persone fisiche brasiliano (CPF)

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-101 Criteri copertura ampia codice fiscale per persone fisiche brasiliano (CPF)

Criterio
\d{11}
\d{9}[-]\d{2}

Criterio

\d{3}[\.]\d{3}[\.]\d{3}[-]\d{2}

Tabella 40-102 Strumento di convalida copertura ampia codice fiscale per persone fisiche brasiliano (CPF)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media codice fiscale per persone fisiche brasiliano (CPF)

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-103 Criteri copertura media codice fiscale per persone fisiche brasiliano (CPF)

Criterio

\d{11}

\d{9}[-]\d{2}

\d{3}[\.]\d{3}[\.]\d{3}[-]\d{2}

Tabella 40-104 Strumento di convalida copertura media codice fiscale per persone fisiche brasiliano (CPF)

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice fiscale per persone fisiche brasiliano	Calcola il checksum che ogni codice fiscale per persone fisiche brasiliano deve superare.

Copertura limitata codice fiscale per persone fisiche brasiliano (CPF)

La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.

Tabella 40-105 Criteri copertura limitata codice fiscale per persone fisiche brasiliano (CPF)

Criterio

\d{11}

Criterio
\d{9} [-] \d{2}
\d{3} [.] \d{3} [.] \d{3} [-] \d{2}

Tabella 40-106 Strumenti di convalida copertura limitata codice fiscale per persone fisiche brasiliano (CPF)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice fiscale per persone fisiche brasiliano	Calcola il checksum che ogni codice fiscale per persone fisiche brasiliano deve superare.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>registro di identificazione, n.CPF, num. cpf, num. CPF, number di registrazione, n. registro persone fisiche, n. cpf, n. record persone fisiche, num.cpf, num.CPF</p> <p>Cadastro de Pessoas Físicas, pessoas singulares</p> <p>registro NO pessoa natural número de registro</p>

Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

I residenti della Columbia Britannica (BC) devono, per legge, registrarsi a un MSP (Medical Service Plan, piano sanitario) per accedere alle strutture di assistenza medica di base.

La tessera MSP è denominata Care Card e il numero MSP è un numero di assistenza sanitaria personale.

L'identificatore di dati per il Personal Healthcare Number (numero di tessera sanitaria) della Columbia britannica rileva un numero di 10 cifre che corrisponde al formato del Personal Healthcare Number della Columbia britannica.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Vedere "Copertura ampia Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica " a pagina 965.

- La copertura media rileva un numero di 10 cifre che supera la convalida del checksum.
Vedere " Copertura media Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica" a pagina 965.
- La copertura limitata rileva un numero di 10 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere "Copertura limitata Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica" a pagina 966.

Copertura ampia Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-107 Criteri copertura ampia Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

Criterio
[9]\d{9}
[9]\d{3} \d{3} \d{3}

Tabella 40-108 Convalida copertura ampia Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

La copertura media rileva un numero di 10 cifre che supera la convalida del checksum.

Tabella 40-109 Criteri copertura media Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

Criterio
[9]\d{9}

Criterio

[9]\d{3} \d{3} \d{3}

Tabella 40-110 Convalida copertura media Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida Personal Healthcare Number della Columbia Britannica	Calcola il checksum che ogni Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica deve superare.

Copertura limitata Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

La copertura limitata rileva un numero di 10 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-111 Criteri di copertura limitata Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

Criterio

[9]\d{9}

[9]\d{3} \d{3} \d{3}

Tabella 40-112 Convalida di copertura limitata Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida Personal Healthcare Number della Columbia Britannica	Calcola il checksum che ogni Personal Healthcare Number (numero di tessera sanitaria) della Columbia Britannica deve superare.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numero MSP, numero msp, n MSP, numero di tessera sanitaria, n sanitario, numero sanità,PHN,phn,phn#,msp#,mspno#,PHN#,numero sanità</p> <p>Nombre MSP, soins de santé no, soins de santé personnels nombre, MSPNombre#, soinsdesanténo#</p>

Numero di cittadinanza univoco bulgaro (EGN)

Il numero di cittadinanza univoco (EGN) è un numero univoco assegnato ai cittadini bulgari o agli stranieri residenti nel paese. Funge da numero di identificazione nazionale. L'EGN viene assegnato ai cittadini bulgari alla nascita o al momento del rilascio del certificato di nascita.

L'identificatore di dati Numero di cittadinanza univoco bulgaro (EGN) rileva un numero di 10 cifre che corrisponde al formato del Numero di cittadinanza univoco bulgaro (EGN).

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.
Vedere "[Copertura ampia numero di cittadinanza univoco bulgaro \(EGN\)](#)" a pagina 967.
- La copertura media rileva un numero di 10 cifre che supera la convalida del checksum.
Vedere "[Copertura media numero di cittadinanza univoco bulgaro \(EGN\)](#)" a pagina 968.
- La copertura limitata rileva un numero di 10 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero di cittadinanza univoco bulgaro \(EGN\)](#)" a pagina 969.

Copertura ampia numero di cittadinanza univoco bulgaro (EGN)

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-113 Criterio copertura ampia numero di cittadinanza univoco bulgaro (EGN)

Criterio
<code>\d\d[024][123456789]0[123456789]\d{4}</code>
<code>\d\d[135][012]0[123456789]\d{4}</code>

Criterio
\d\d[024][123456789][12]\d{5}
\d\d[135][012][12]\d{5}
\d\d[024][123456789]3[01]\d{4}
\d\d[135][012]3[01]\d{4}

Tabella 40-114 Strumento di convalida copertura ampia numero di cittadinanza univoco bulgaro (EGN)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di cittadinanza univoco bulgaro (EGN)

La copertura media rileva un numero di 10 cifre che supera la convalida del checksum.

Tabella 40-115 Criterio copertura media numero di cittadinanza univoco bulgaro (EGN)

Criterio
\d\d[024][123456789]0[123456789]\d{4}
\d\d[135][012]0[123456789]\d{4}
\d\d[024][123456789][12]\d{5}
\d\d[135][012][12]\d{5}
\d\d[024][123456789]3[01]\d{4}
\d\d[135][012]3[01]\d{4}

Tabella 40-116 Convalida copertura media numero di cittadinanza univoco bulgaro (EGN)

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di cittadinanza univoco bulgaro	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di cittadinanza univoco bulgaro (EGN)

La copertura limitata rileva un numero di 10 cifre che supera la convalida del checksum.
 Richiede inoltre la presenza di parole chiave associate.

Tabella 40-117 Criterio di copertura limitata numero di cittadinanza univoco bulgaro (EGN)

Criterio
<code>\d\d[024][123456789]0[123456789]\d{4}</code>
<code>\d\d[135][012]0[123456789]\d{4}</code>
<code>\d\d[024][123456789][12]\d{5}</code>
<code>\d\d[135][012][12]\d{5}</code>
<code>\d\d[024][123456789]3[01]\d{4}</code>
<code>\d\d[135][012]3[01]\d{4}</code>

Tabella 40-118 Strumento di convalida copertura limitata numero di cittadinanza univoco bulgaro (EGN)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di cittadinanza univoco bulgaro	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>BUCN, numero di cittadinanza, numero ID di cittadinanza, n di cittadinanza, EGN, numero di cittadinanza univoco bulgaro, numerounivococittadinanza#, BUCN#, EGN#, bucn, egcn#, bucn#, uniformcivilnumber#, numero personale, n personale, numero di identificazione, id personale, id nazionale</p> <p>Униформ граждански номер, Униформ ID, Униформ граждански ID, Униформ граждански не., български Униформ граждански номер, УниформгражданскиID#, Униформгражданскине.#, личен номер, лично не, идентификационен номер, лична идентификация, национален номер</p>

Burgerservicenummer

Nei Paesi Bassi, il Burgerservicenummer è utilizzato per identificare in modo univoco i cittadini ed è stampato su patenti di guida, passaporti e documenti d'identità internazionali sotto l'intestazione Numero personale.

L'identificatore di dati del Burgerservicenummer rileva un numero di 8 o 9 cifre che corrisponde al formato del Burgerservicenummer e supera la convalida del checksum.

L'identificatore di dati Burgerservicenummer fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di otto o nove cifre che supera la convalida del checksum.
Vedere ["Copertura ampia Burgerservicenummer"](#) a pagina 970.
- La copertura limitata rileva un numero di 8 o 9 cifre, conforme alla convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata burgerservicenummer"](#) a pagina 971.

Copertura ampia Burgerservicenummer

La copertura ampia rileva un numero di otto o nove cifre che supera la convalida del checksum.

Tabella 40-119 Criterio di copertura ampia Burgerservicenummer

Criterio
\d{9}

Tabella 40-120 Convalida copertura ampia Burgerservicenummer

Convalida obbligatoria	Descrizione
Controllo Burgerservicenummer	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata burgerservicenummer

La copertura limitata rileva un numero di 8 o 9 cifre, conforme alla convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-121 Criterio di copertura limitata burgerservicenummer

Criterio
\d{9}

Tabella 40-122 Convalide di copertura limitata burgerservicenummer

Convalida obbligatoria	Descrizione
Controllo Burgerservicenummer	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: Persoonsnummer, sofinummer, sociaal-fiscaal nummer, persoonsgebonden, numero persona, numero sociale-fiscale, numero associato alla persona

Social Insurance Number (numero di previdenza sociale) canadese

Numero di identificazione personale rilasciato dallo Human Resources and Skills Development Canada principalmente per la gestione dei piani occupazionali e pensionistici nazionali.

L'identificatore di dati del Social Insurance Number (numero di previdenza sociale) canadese rileva un numero di nove cifre che corrisponde al formato del numero di previdenza sociale canadese.

L'identificatore di dati Social Insurance Number (numero di previdenza sociale) canadese fornisce tre coperture di rilevamento:

- La copertura ampia rileva numeri a nove cifre nel formato DDD-DDD-DDD con trattini, spazi, punti o barre di separazione o senza separatori. Esegue inoltre la convalida del controllo Luhn.
Vedere ["Copertura ampia Social Insurance Number \(numero di previdenza sociale\) canadese"](#) a pagina 972.
- Copertura media rileva numeri a nove cifre nel formato DDD-DDD-DDD, con trattini, spazi o punti di separazione. Inoltre, esegue la convalida di controllo Luhn ed elimina i numeri non assegnati e i numeri di prova comuni.
Vedere ["Copertura media Social Insurance Number \(numero di previdenza sociale\) canadese"](#) a pagina 973.
- La copertura limitata rileva numeri a nove cifre nel formato DDD-DDD-DDD, con trattini, spazi o punti di separazione. Inoltre, esegue la convalida di controllo Luhn, elimina i numeri non assegnati, i numeri assegnati in modo fittizio e i numeri di prova comuni e richiede la presenza di parole chiave correlate.
Vedere ["Copertura limitata Social Insurance Number \(numero di previdenza sociale\) canadese"](#) a pagina 974.

Copertura ampia Social Insurance Number (numero di previdenza sociale) canadese

La copertura ampia rileva numeri a nove cifre nel formato DDD-DDD-DDD con trattini, spazi, punti o barre di separazione o senza separatori. Esegue inoltre la convalida del controllo Luhn.

Tabella 40-123 Modelli copertura ampia Social Insurance Number (numero di previdenza sociale) canadese

Criteri
\d{3} \d{3} \d{3}
\d{9}
\d{3}/\d{3}/\d{3}
\d{3}.\d{3}.\d{3}
\d{3}-\d{3}-\d{3}

Tabella 40-124 Strumento di convalida copertura ampia Social Insurance Number (numero di previdenza sociale) canadese

Strumento di convalida obbligatorio	Descrizione
Controllo Luhn	Lo strumento di convalida calcola il checksum Luhn che tutti i numeri di previdenza sociale canadesi devono superare.

Copertura media Social Insurance Number (numero di previdenza sociale) canadese

Copertura media rileva numeri a nove cifre nel formato DDD-DDD-DDD, con trattini, spazi o punti di separazione. Inoltre, esegue la convalida di controllo Luhn ed elimina i numeri non assegnati e i numeri di prova comuni.

Tabella 40-125 Modelli copertura media Social Insurance Number (numero di previdenza sociale) canadese

Criteri
\d{3} \d{3} \d{3}
\d{3}.\d{3}.\d{3}
\d{3}-\d{3}-\d{3}

Tabella 40-126 Strumenti di convalida copertura media Social Insurance Number (numero di previdenza sociale) canadese

Convalide obbligatorie	Descrizione
Controllo Luhn	Lo strumento di convalida calcola il checksum Luhn che tutti i numeri di previdenza sociale canadesi devono superare.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Escludi caratteri iniziali	Quando questa opzione è selezionata, i dati che iniziano con uno qualsiasi dei valori seguenti saranno ignorati. Input: 8, 123456789

Copertura limitata Social Insurance Number (numero di previdenza sociale) canadese

La copertura limitata rileva numeri a nove cifre nel formato DDD-DDD-DDD, con trattini, spazi o punti di separazione. Inoltre, esegue la convalida di controllo Luhn, elimina i numeri non assegnati, i numeri assegnati in modo fittizio e i numeri di prova comuni e richiede la presenza di parole chiave correlate.

Tabella 40-127 Modelli copertura limitata Social Insurance Number (numero di previdenza sociale) canadese

Criteri
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$

Tabella 40-128 Strumenti di convalida copertura limitata Social Insurance Number (numero di previdenza sociale) canadese

Convalide obbligatorie	Descrizione
Controllo Luhn	Lo strumento di convalida calcola il checksum Luhn che tutti i numeri di previdenza sociale canadesi devono superare.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Escludi caratteri iniziali	Quando questa opzione è selezionata, i dati che iniziano con uno qualsiasi dei valori seguenti saranno ignorati. Input: 0, 8, 123456789
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: pensione, pensioni, prev soc, prev #, prev socil, CSIN, SSN, previdenza sociale, previdenza sociale, Canada, canadese

Numero di identificazione nazionale cileno

Il numero di identificazione nazionale cileno o ruolo unico nazionale (RUN), è l'unico numero di identificazione assegnato a tutti i cittadini cileni residenti in Cile o in altri paesi e ai cittadini stranieri con residenza temporanea o permanente nel paese.

L'identificatore di dati per il Numero di identificazione nazionale cileno rileva un numero di 8 o 9 cifre che corrisponde al formato del Numero di identificazione nazionale cileno.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 8 o 9 cifre senza la convalida del checksum. Vedere ["Copertura ampia numero di identificazione nazionale cileno"](#) a pagina 975.
- La copertura media rileva un numero di 8 o 9 cifre con la convalida del checksum. Vedere ["Copertura media numero di identificazione nazionale cileno"](#) a pagina 976.
- La copertura limitata rileva un numero di 8 o 9 cifre, conforme alla convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata numero di identificazione nazionale cileno"](#) a pagina 976.

Copertura ampia numero di identificazione nazionale cileno

La copertura ampia rileva un numero di 8 o 9 cifre senza la convalida del checksum.

Tabella 40-129 Criteri copertura ampia numero di identificazione nazionale cileno

Modelli
<code>\d{7} [0123456789Kk]</code>
<code>\d{7} [-] [0123456789Kk]</code>
<code>\d[.]\d{3} [.] \d{3} [-] [0123456789Kk]</code>
<code>\d{8} [0123456789Kk]</code>
<code>\d{8} [-] [0123456789Kk]</code>
<code>\d{2} [.] \d{3} [.] \d{3} [-] [0123456789Kk]</code>

Tabella 40-130 Strumento di convalida copertura ampia del numero di identificazione nazionale cileno

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione nazionale cileno

La copertura media rileva un numero di 8 o 9 cifre con la convalida del checksum.

Tabella 40-131 Criteri copertura media numero di identificazione nazionale cileno

Modelli
$\backslash d\{7\} [0123456789Kk]$
$\backslash d\{7\} [-] [0123456789Kk]$
$\backslash d[.] \backslash d\{3\} [.] \backslash d\{3\} [-] [0123456789Kk]$
$\backslash d\{8\} [0123456789Kk]$
$\backslash d\{8\} [-] [0123456789Kk]$
$\backslash d\{2\} [.] \backslash d\{3\} [.] \backslash d\{3\} [-] [0123456789Kk]$

Tabella 40-132 Convalida copertura media numero di identificazione nazionale cileno

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione nazionale cileno	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di identificazione nazionale cileno

La copertura limitata rileva un numero di 8 o 9 cifre, conforme alla convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-133 Criteri di copertura limitata numero di identificazione nazionale cileno

Modelli
$\backslash d\{7\} [0123456789Kk]$
$\backslash d\{7\} [-] [0123456789Kk]$
$\backslash d[.] \backslash d\{3\} [.] \backslash d\{3\} [-] [0123456789Kk]$
$\backslash d\{8\} [0123456789Kk]$
$\backslash d\{8\} [-] [0123456789Kk]$
$\backslash d\{2\} [.] \backslash d\{3\} [.] \backslash d\{3\} [-] [0123456789Kk]$

Tabella 40-134 Convalide di copertura limitata Numero di identificazione nazionale cileno

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione nazionale cileno	Calcola il checksum e lo utilizza per convalidare il criterio.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>RUT, RUN, numero di identificazione nazionale, n. identità cileno, ruolo univoco nazionale, n.rut, n.run, numeroidentificazione, num.identità#, numero di identità</p> <p>nationaluniqueroleID #, nacional identidad, número identificación, número identificación nacional, identidad número ;"</p>

Numero di passaporto cinese

I passaporti della Repubblica Popolare Cinese, comunemente chiamati passaporti cinesi, sono i passaporti rilasciati ai cittadini della Repubblica Popolare Cinese che non hanno una residenza permanente a Hong Kong o Macao per consentire i viaggi internazionali.

L'identificatore di dati per il Numero di passaporto cinese rileva un codice identificatore di 9 o 10 caratteri che corrisponde al formato del Numero di passaporto cinese.

L'identificatore di dati del numero di passaporto australiano fornisce due coperture di rilevamento:

- La copertura ampia rileva un identificatore da 9 a 10 caratteri.
Vedere ["Copertura ampia numero di passaporto cinese"](#) a pagina 977.
- La copertura limitata rileva un identificatore da 9 a 10 caratteri. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di passaporto cinese"](#) a pagina 978.

Copertura ampia numero di passaporto cinese

La copertura ampia rileva un identificatore da 9 a 10 caratteri.

Tabella 40-135 Criteri copertura ampia numero di passaporto cinese

Modelli
\d{9}
\1\d{8}
\1{2}\d{8}

Tabella 40-136 Convalida di copertura ampia numero di passaporto cinese

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata numero di passaporto cinese

La copertura ampia rileva un identificatore da 9 a 10 caratteri. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-137 Criteri copertura limitata numero di passaporto cinese

Modelli
\d{9}
\1\d{8}
\1{2}\d{8}

Tabella 40-138 Convalide copertura limitata numero di passaporto cinese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>中国护照, 护照, 护照本</p> <p>passaporto, Passaporto, PASSAPORTO CINESE, Passaporto cinese, passaporto cinese, Libretto passaporto, libretto passaporto</p>

Codice Fiscale

Il codice fiscale identifica in modo univoco i cittadini italiani o gli stranieri con residenza permanente in Italia e viene rilasciato a livello centralizzato dal Ministero del Tesoro. In Italia il codice fiscale viene rilasciato a tutti i cittadini alla nascita.

L'identificatore di dati codice fiscale rileva una stringa di 16 caratteri che corrisponde al formato del codice fiscale.

L'identificatore di dati Codice Fiscale offre due coperture di rilevamento:

- La copertura media rileva un identificatore di 16 caratteri con convalida del checksum. Vedere ["Copertura ampia Codice Fiscale"](#) a pagina 979.
- La copertura limitata rileva un identificativo di 16 caratteri con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata Codice Fiscale"](#) a pagina 979.

Copertura ampia Codice Fiscale

La copertura ampia rileva un identificatore di 16 caratteri che supera la convalida del checksum

Tabella 40-139 Criteri copertura ampia Codice Fiscale

Modelli
[A-Z] { 6 } [0-9LMNPQRSTU] { 2 } [ABCDEHLMPRST] [0-9LMNPQRSTU] { 2 } [A-Z] [0-9LMNPQRSTU] { 3 } [A-Z]
[A-Z] { 3 } [A-Z] { 3 } [0-9LMNPQRSTU] { 2 } [ABCDEHLMPRST] [0-9LMNPQRSTU] { 2 }
[A-Z] [0-9LMNPQRSTU] { 3 } [A-Z]

Tabella 40-140 Convalida copertura ampia Codice Fiscale

Convalida obbligatoria	Descrizione
Verifica chiave di controllo codice fiscale	Calcola la chiave di controllo e ne verifica la validità.

Copertura limitata Codice Fiscale

La copertura limitata rileva un identificatore di 16 caratteri che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-141 Criteri copertura limitata Codice Fiscale

Modelli
[A-Z] { 6 } [0-9LMNPQRSTU] { 2 } [ABCDEHLMPRST] [0-9LMNPQRSTU] { 2 } [A-Z] [0-9LMNPQRSTU] { 3 } [A-Z]

Modelli

[A-Z]{3} [A-Z]{3} [0-9LMNPQRSTUVWXYZ]{2}[ABCDEHLMPRST][0-9LMNPQRSTUVWXYZ]{2}
[A-Z][0-9LMNPQRSTUVWXYZ]{3}[A-Z]

Tabella 40-142 Convalide di copertura limitata Codice Fiscale

Convalide obbligatorie	Descrizione
Verifica chiave di controllo codice fiscale	Calcola la chiave di controllo e ne verifica la validità.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: codice fiscale, dati anagrafici, partita I.V.A., p. iva, tax code, personal data, VAT number

Indirizzi colombiani

L'identificatore di dati Indirizzi colombiani rileva gli indirizzi di casa e le posizioni fisiche in Colombia.

L'identificatore di dati Indirizzi colombiani fornisce due coperture di rilevamento:

- La copertura ampia rileva un indirizzo senza convalida.
Vedere "[Copertura ampia indirizzi colombiani](#)" a pagina 980.
- La copertura limitata rileva un indirizzo con la convalida di parole chiave.
Vedere "[Copertura limitata indirizzi colombiani](#)" a pagina 981.

Copertura ampia indirizzi colombiani

La copertura ampia rileva un indirizzo senza convalida.

Tabella 40-143 Criteri di copertura ampia di indirizzi colombiani

Modelli
\d{1,3} No. \d{1,3}-\d{1,3}
\d{1,3} \d{1,3}-\d{1,3}
\d{1,3} Bis \d{1,3}[A-Za-z]-\d{1,3}
\d{1,3}[A-Za-z] Bis \d{1,3}[A-Za-z]-\d{1,3}

Modelli
$\backslash d\{1,3\}[A-Za-z] \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\} \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\} \text{ Bis No } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\} \text{ Bis No. } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ Bis No. } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ Bis \# } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ No. } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\} \text{ \# } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\} \text{ No. } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ Bis No } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ No } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\} \text{ \# } \backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ \# } \backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\} \text{ No } \backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ No. } \backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ No } \backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\} \text{ Bis \# } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z] \text{ \# } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\} \text{ No } \backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$

La copertura ampia dell'identificatore dati relativo agli indirizzi colombiani non include una convalida.

Copertura limitata indirizzi colombiani

La copertura limitata rileva un indirizzo con la convalida di parole chiave.

Tabella 40-144 Criteri di copertura limitata indirizzi colombiani

Modelli
$\backslash d\{1,3\}$ No. $\backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ $\backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ Bis $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ Bis $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ $\backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ Bis No $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ Bis No. $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ Bis No. $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ Bis # $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ No. $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ # $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ No. $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ Bis No $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ No $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ # $\backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ # $\backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ No $\backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ No. $\backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ No $\backslash d\{1,3\}-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ Bis # $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}[A-Za-z]$ # $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$
$\backslash d\{1,3\}$ No $\backslash d\{1,3\}[A-Za-z]-\backslash d\{1,3\}$

Tabella 40-145 Convalida di copertura limitata Indirizzi colombiani

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Calle, Cll, Carrera, Cra, Cr, Avenida, Av, Dg, Diagonal, Diag, Tv, Trans, Transversal, vereda</p>

Numero di cellulare colombiano

L'identificatore dati Numero di cellulare colombiano rileva numeri di cellulare colombiani.

L'identificatore di dati Numero di cellulare colombiano offre due coperture di rilevazione:

- La copertura ampia rileva un numero che include da 8 a 10 cifre con la doppia convalida delle cifre.
Vedere ["Copertura ampia numero di cellulare colombiano"](#) a pagina 983.
- La copertura limitata rileva un numero che include da 8 a 10 cifre con i caratteri richiesti all'inizio. Inoltre verifica la presenza di cifre doppie e richiede la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di cellulare colombiano"](#) a pagina 984.

Copertura ampia numero di cellulare colombiano

La copertura ampia rileva un numero che include da 8 a 10 cifre con la doppia convalida delle cifre.

Tabella 40-146 Criteri copertura ampia numero di cellulare colombiano

Modelli
$\backslash d\{8\}$
$\backslash d\{2\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{2\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{2\}/\backslash d\{3\}/\backslash d\{3\}$
$\backslash d\{2\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{2\},\backslash d\{3\},\backslash d\{3\}$

Modelli
$\backslash d\{9\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\},\backslash d\{3\},\backslash d\{3\}$
$\backslash d\{3\}/\backslash d\{3\}/\backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{10\}$
$\backslash d\{1\}/\backslash d\{3\}/\backslash d\{3\}/\backslash d\{3\}$
$\backslash d\{1\},\backslash d\{3\},\backslash d\{3\},\backslash d\{3\}$
$\backslash d\{1\}.\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{1\}-\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{1\} \backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$

Tabella 40-147 Strumento di convalida copertura ampia numero di cellulare colombiano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata numero di cellulare colombiano

La copertura limitata rileva un numero che include da 8 a 10 cifre con i caratteri richiesti all'inizio. Inoltre verifica la presenza di cifre doppie e richiede la presenza di parole chiave associate.

Tabella 40-148 Criteri copertura limitata numero di cellulare colombiano

Modelli
$\backslash d\{8\}$
$\backslash d\{2\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{2\} \backslash d\{3\} \backslash d\{3\}$

Modelli
$\backslash d\{2\} / \backslash d\{3\} / \backslash d\{3\}$
$\backslash d\{2\} - \backslash d\{3\} - \backslash d\{3\}$
$\backslash d\{2\}, \backslash d\{3\}, \backslash d\{3\}$
$\backslash d\{9\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\} - \backslash d\{3\} - \backslash d\{3\}$
$\backslash d\{3\}, \backslash d\{3\}, \backslash d\{3\}$
$\backslash d\{3\} / \backslash d\{3\} / \backslash d\{3\}$
$\backslash d\{3\} . \backslash d\{3\} . \backslash d\{3\}$
$\backslash d\{10\}$
$\backslash d\{1\} / \backslash d\{3\} / \backslash d\{3\} / \backslash d\{3\}$
$\backslash d\{1\}, \backslash d\{3\}, \backslash d\{3\}, \backslash d\{3\}$
$\backslash d\{1\} . \backslash d\{3\} . \backslash d\{3\} . \backslash d\{3\}$
$\backslash d\{1\} - \backslash d\{3\} - \backslash d\{3\} - \backslash d\{3\}$
$\backslash d\{1\} \backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$

Tabella 40-149 Strumenti di convalida copertura limitata numero di cellulare colombiano

Convalide obbligatorie	Descrizione
Richiedi caratteri iniziali	Questo strumento di convalida richiede i seguenti caratteri all'inizio del numero: 300, 301, 302, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 350
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero celular, número de teléfono, teléfono celular no., numero celular#</p>

Numero di identificazione personale colombiano

Il numero di identificazione personale colombiano è un numero di 8 o 10 cifre alfanumerico assegnato ai cittadini colombiani alla nascita.

L'identificatore di dati per il Numero di identificazione personale colombiano rileva un numero di 8 o 10 cifre che corrisponde al formato del Numero di identificazione personale colombiano.

L'identificatore dati del numero di identificazione personale colombiano fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero che include da 8 a 10 cifre con la doppia convalida delle cifre.
Vedere ["Copertura ampia numero di identificazione personale colombiano"](#) a pagina 986.
- La copertura limitata rileva un numero che include da 8 a 10 cifre con la doppia convalida delle cifre, esclusione di prefissi e suffissi ed esclusione dei caratteri iniziali. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di identificazione personale colombiano"](#) a pagina 987.

Copertura ampia numero di identificazione personale colombiano

La copertura ampia rileva un numero che include da 8 a 10 cifre con la doppia convalida delle cifre.

Tabella 40-150 Criteri copertura ampia numero di identificazione personale colombiano

Modelli
\d{9}
\d{3} \d{3} \d{3}
\d{3}-\d{3}-\d{3}
\d{3},\d{3},\d{3}

Modelli
$\backslash d\{3\} / \backslash d\{3\} / \backslash d\{3\}$
$\backslash d\{3\} . \backslash d\{3\} . \backslash d\{3\}$

Tabella 40-151 Strmento di convalida copertura ampia numero di identificazione personale colombiano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata numero di identificazione personale colombiano

La copertura limitata rileva un numero che include da 8 a 10 cifre con la doppia convalida delle cifre, esclusione di prefissi e suffissi ed esclusione dei caratteri iniziali. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-152 Criteri copertura limitata numero di identificazione personale colombiano

Modelli
$\backslash d\{9\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\} - \backslash d\{3\} - \backslash d\{3\}$
$\backslash d\{3\} , \backslash d\{3\} , \backslash d\{3\}$
$\backslash d\{3\} / \backslash d\{3\} / \backslash d\{3\}$
$\backslash d\{3\} . \backslash d\{3\} . \backslash d\{3\}$

Tabella 40-153 Convalida copertura limitata numero di identificazione personale colombiano

Convalide obbligatorie	Descrizione
Escludi caratteri iniziali	Consente di escludere i seguenti caratteri dall'inizio del numero: 300, 301, 302, 310, 310, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 350
Escludi prefisso	Esclude i seguenti prefissi: \$, \$

Convalide obbligatorie	Descrizione
Escludi suffisso	Esclude il seguente suffisso: .00
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: cedula, cédula, c.c., c.c, C.C., C.C, cc, CC, NIE., NIE, nie., nie, cedula de ciudadanía, cédula de ciudadanía, cc#, CC #, documento de identificacion, documento de identificación, Nit.

Tax Identification Number (codice fiscale) colombiano

Il numero di identificazione fiscale colombiano è un numero di nove cifre assegnato alle persone che devono pagare le imposte in Colombia.

L'identificatore di dati per il Numero di identificazione fiscale colombiano rileva un numero di nove cifre che corrisponde al formato del Numero di identificazione fiscale colombiano.

L'identificatore di dati del Tax Identification Number (codice fiscale) colombiano offre due coperture di rilevazione:

- La copertura ampia rileva un numero di nove cifre con la doppia convalida delle cifre. Vedere "[Copertura ampia Tax Identification Number \(codice fiscale\) colombiano](#)" a pagina 988.
- La copertura limitata rileva un numero di nove cifre con la doppia convalida delle cifre, i caratteri d'inizio richiesti e l'esclusione del prefisso. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata Tax Identification Number \(codice fiscale\) colombiano](#)" a pagina 989.

Copertura ampia Tax Identification Number (codice fiscale) colombiano

La copertura ampia rileva un numero di 9 cifre con la doppia convalida delle cifre.

Tabella 40-154 Criteri copertura ampia Tax Identification Number (codice fiscale) colombiano

Modelli
$\backslash d\{9\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\}, \backslash d\{3\}, \backslash d\{3\}$
$\backslash d\{3\} / \backslash d\{3\} / \backslash d\{3\}$
$\backslash d\{3\} . \backslash d\{3\} . \backslash d\{3\}$

Tabella 40-155 Convalida copertura ampia Tax Identification Number (codice fiscale) colombiano

Convalida obbligatoria	Descrizione
Duplicate digits	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata Tax Identification Number (codice fiscale) colombiano

La copertura limitata rileva un numero di nove cifre con la doppia convalida delle cifre, i caratteri d'inizio richiesti e l'esclusione del prefisso. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-156 Criteri copertura limitata Tax Identification Number (codice fiscale) colombiano

Modelli
$\backslash d\{9\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\}, \backslash d\{3\}, \backslash d\{3\}$
$\backslash d\{3\} / \backslash d\{3\} / \backslash d\{3\}$
$\backslash d\{3\} . \backslash d\{3\} . \backslash d\{3\}$

Tabella 40-157 Convalide copertura limitata Tax Identification Number (codice fiscale) colombiano

Convalide obbligatorie	Descrizione
Richiedi caratteri iniziali	Necessita dei seguenti caratteri all'inizio del numero: 800, 860, 890, 900
Escludi prefisso	Esclude il seguente prefisso: \$
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: NIT., NIT, nit., nit, Nit.

Dati banda magnetica per carte di credito

La banda magnetica di una carta di credito contiene informazioni sulla carta. L'archiviazione della versione completa di questi dati rappresenta una violazione dello standard Payment Card Industry (PCI) Data Security Standard (DSS).

L'identificatore Dati banda magnetica carta di credito rileva i seguenti dati non elaborati dalla banda magnetica della carta di credito:

- I dati della traccia uno, formato B, che generalmente contiene numero di conto, nome, data di scadenza e possibilmente Card Verification Value o Card Verification Code 1 (CVV1/CVC1).
- I dati dalla traccia due, che generalmente contiene il numero di conto e possibilmente data di scadenza, codice di servizio e Card Verification Value o Card Verification Code 1 (CVV1/CVC1).

L'identificatore Dati banda magnetica carta di credito rileva il criterio di dati caratteristico per i dati della traccia due contenente sentinel di inizio, codice formato, numero di conto principale, nome, data di scadenza, codice di servizio, dati discrezionali e sentinel di fine. Include inoltre separatori di campi standard. Convalida i dati utilizzando una convalida di controllo Luhn.

Tabella 40-158 Criteri copertura media dati banda magnetica carta di credito

Criteri	Criteri (continua)
	%B3[068]\d{12}^[A-Z]{1}
	%B3[068]\d{2} \d{6} \d{4}^[A-Z]{1}
	%B3[068]\d{2}-\d{6}-\d{4}^[A-Z]{1}
	%B4\d{12}^[A-Z]{1}
	%B3[47]\d{2}-\d{6}-\d{5}^[A-Z]{1}
	%B4\d{3} \d{4} \d{4} \d{4}^[A-Z]{1}
	%B3[47]\d{2} \d{6} \d{5}^[A-Z]{1}
	%B4\d{15}^[A-Z]{1}
	%B3[47]\d{13}^[A-Z]{1}
	%B5[1-5]\d{2}-\d{4}-\d{4}-\d{4}^[A-Z]{1}
	%B4\d{3}-\d{4}-\d{4}-\d{4}^[A-Z]{1}
	%B5[1-5]\d{2} \d{4} \d{4} \d{4}^[A-Z]{1}
	%B5[1-5]\d{14}^[A-Z]{1}
	%B2131\d{11}^[A-Z]{1}
	%B3\d{3}-\d{4}-\d{4}-\d{4}^[A-Z]{1}
	%B3\d{3} \d{4} \d{4} \d{4}^[A-Z]{1}
	%B3\d{15}^[A-Z]{1}
	%B2149\d{11}^[A-Z]{1}
	%B2149 \d{6} \d{5}^[A-Z]{1}
	%B2149-\d{6}-\d{5}^[A-Z]{1}
	%B2014\d{11}^[A-Z]{1}
	%B2014 \d{6} \d{5}^[A-Z]{1}
	%B2014-\d{6}-\d{5}^[A-Z]{1}

Criteri	Criteri (continua)
;1800\d{11}= ;6011-\d{4}-\d{4}-\d{4}= ;6011 \d{4} \d{4} \d{4}= ;6011\d{12}= ;3[068]\d{12}= ;3[068]\d{2} \d{6} \d{4}= ;3[068]\d{2}-\d{6}-\d{4}= ;4\d{12}= ;3[47]\d{2}-\d{6}-\d{5}= ;4\d{3} \d{4} \d{4} \d{4}= ;3[47]\d{2} \d{6} \d{5}= ;4\d{15}= ;3[47]\d{13}= ;5[1-5]\d{2}-\d{4}-\d{4}-\d{4}= ;4\d{3}-\d{4}-\d{4}-\d{4}= ;5[1-5]\d{2} \d{4} \d{4} \d{4}= ;5[1-5]\d{14}= ;2131\d{11}= ;3\d{3}-\d{4}-\d{4}-\d{4}= ;3\d{3} \d{4} \d{4} \d{4}= ;3\d{15}= ;2149\d{11}= ;2149 \d{6} \d{5}= ;2149-\d{6}-\d{5}= ;2014\d{11}= ;2014 \d{6} \d{5}= ;2014-\d{6}-\d{5}= %B1800\d{11}^[A-Z]{1} %B6011-\d{4}-\d{4}-\d{4}^[A-Z]{1} %B6011 \d{4} \d{4} \d{4}^[A-Z]{1} %B6011\d{12}^[A-Z]{1}	

Tabella 40-159 Convalida copertura media dati banda magnetica carta di credito

Convalida	Descrizione
Controllo Luhn	Calcola il checksum Luhn che ogni istanza deve superare.

Numero carta di credito

Numero di conto necessario per l'elaborazione delle transazioni della carta di credito. Generalmente abbreviato con CCN. Noto anche come numero di conto principale (PAN).

L'identificatore dati Numero carta di credito rileva i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori

L'identificatore di dati Numero carta di credito offre tre coperture di rilevamento:

- La copertura ampia consente di rilevare i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori. Esegue inoltre la convalida del controllo Luhn. Vedere ["Copertura ampia Numero carta di credito"](#) a pagina 993.
- La copertura media rileva i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori. Inoltre verifica la presenza di numeri di prova comuni ed esegue la convalida del controllo Luhn. Vedere ["Copertura media numero carta di credito"](#) a pagina 994.
- La copertura limitata rileva i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori. Inoltre verifica la presenza di numeri di prova comuni, esegue la convalida del controllo Luhn e richiede la presenza di parole chiave associate al numero di carta di credito. Vedere ["Copertura limitata numero carta di credito"](#) a pagina 997.

Copertura ampia Numero carta di credito

La copertura ampia consente di rilevare i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori.

Questo strumento di convalida include i formati per American Express, Diners Club, Discover, Japan Credit Bureau (JCB), MasterCard e Visa.

Questo strumento di convalida esegue il controllo di convalida Luhn.

Tabella 40-160 Modelli copertura ampia Numero carta di credito

Criteri	Criteri (continua)
2149 \d{6} \d{5}	4\d{12}
2149-\d{6}-\d{5}	\d{16}
2014\d{11}	\d{4}.\d{4}.\d{4}.\d{4}
2014 .\d{6}.\d{5}	\d{4}-\d{4}-\d{4}-\d{4}
2014 \d{6} \d{5}	\d{4} \d{4} \d{4} \d{4}
2014-\d{6}-\d{5}	1800\d{11}
3[47]\d{2}.\d{6}.\d{5}	2131\d{11}
3[068]\d{2}.\d{6}.\d{4}	2149\d{11}
3[47]\d{2}-\d{6}-\d{5}	2149.\d{6}.\d{5}
3[068]\d{2}-\d{6}-\d{4}	
3[47]\d{13}	
3[068]\d{2} \d{6} \d{4}	
3[47]\d{2} \d{6} \d{5}	
3[068]\d{12}	

Tabella 40-161 Strumento di convalida copertura ampia Numero carta di credito

Strumento di convalida obbligatorio	Descrizione
Controllo Luhn	Lo strumento di convalida calcola il checksum Luhn che tutti i numeri di carta di credito devono superare.

Copertura media numero carta di credito

La copertura media rileva i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori. Questa convalida esegue il controllo di convalida Luhn. Questo strumento di convalida include i formati per American Express, Diners Club, Discover, Japan Credit Bureau (JCB), MasterCard e Visa. Rimuove i numeri di prova comuni, compresi quelli riservati ai test eseguiti dagli emittenti di carte di credito.

Tabella 40-162 Criteri copertura media numero carta di credito

Criteri	Criteri (continua)
---------	--------------------

Criteria	Criteria (continua)
1800\d{11}	2720.\d{4}.\d{4}.\d{4}
2131\d{11}	2720-\d{4}-\d{4}-\d{4}
3\d{3}.\d{4}.\d{4}.\d{4}	2720 \d{4} \d{4} \d{4}
3\d{3}-\d{4}-\d{4}-\d{4}	2720\d{12}
3\d{3} \d{4} \d{4} \d{4}	6221[2][6-8]\d{10}
3\d{15}	6221.[2][6-8]\d{2}.\d{4}.\d{4}
4\d{3}.\d{4}.\d{4}.\d{4}	6221-[2][6-8]\d{2}-\d{4}-\d{4}
4\d{3}-\d{4}-\d{4}-\d{4}	6221 [2][6-8]\d{2} \d{4} \d{4}
4\d{3} \d{4} \d{4} \d{4}	622[2-8]\d{12}
4\d{15}	622[2-8].\d{4}.\d{4}.\d{4}
4\d{12}	622[2-8]-\d{4}-\d{4}-\d{4}
5[1-5]\d{2}.\d{4}.\d{4}.\d{4}	622[2-8] \d{4} \d{4} \d{4}
5[1-5]\d{2}-\d{4}-\d{4}-\d{4}	6229[2][0-5]\d{10}
2149.\d{6}.\d{5}	6229.[2][0-5]\d{2}.\d{4}.\d{4}
5[1-5]\d{2} \d{4} \d{4}	6229-[2][0-5]\d{2}-\d{4}-\d{4}
\d{4}	6229 [2][0-5]\d{2} \d{4} \d{4}
2149 \d{6} \d{5}	2014 \d{6} \d{5}
5[1-5]\d{14}	2014-\d{6}-\d{5}
2149-\d{6}-\d{5}	2014\d{11}
2149\d{11}	6011.\d{4}.\d{4}.\d{4}
2014.\d{6}.\d{5}	6011-\d{4}-\d{4}-\d{4}
222[1-9]\d{12}	6011 \d{4} \d{4} \d{4}
222[1-9][.-]\d{4}[.-]\d{4}[.-]\d{4}	6011\d{12}
22[3-9]\d{13}	3[068]\d{2}.\d{6}.\d{4}
22[3-9]\d{13}[.-]\d{4}[.-]\d{4}[.-]\d{4}	3[068]\d{2}-\d{6}-\d{4}
2[3-6]\d{14}	3[068]\d{2} \d{6} \d{4}
2[3-6]\d{2}.\d{4}.\d{4}.\d{4}	3[068]\d{12}
2[3-6]\d{2}-\d{4}-\d{4}-\d{4}	3[47]\d{13}
2[3-6]\d{2} \d{4} \d{4}	3[47]\d{2}.\d{6}.\d{5}
\d{4}	3[47]\d{2} \d{6} \d{5}
27[0-1]\d{13}	

Criteri	Criteri (continua)
27[0-1]\d.\d{4}.\d{4}.\d{4}	3[47]\d{2}-\d{6}-\d{5}
27[0-1]\d-\d{4}-\d{4}-\d{4}	
27[0-1]\d \d{4} \d{4} \d{4}	

Tabella 40-163 Convalide copertura media numero carta di credito

Convalide obbligatorie	Descrizione
Escludi corrispondenza esatta	<p>Esclude ogni corrispondenza con il testo specificato.</p> <p>Input:</p> <p>0111111111111111, 1234567812345670, 180025848680889, 180026939516875, 2014000000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 300000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 3088000000000000, 3088000000000009, 3088272824427380, 3096666928988980, 3158060990195830, 3400000000000009, 341019464477148, 3411111111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 3700000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 40070000000027, 4012888888881880, 4024007116284, 4111111111111110, 4111111111111111, 4222222222222, 4242424242424242, 4485249610564758, 4539399050593, 4539475158333170, 4539603277651940, 4539687075612974, 4539890911376230, 4556657397647250, 4716733846619930, 4716976758661, 4916437046413, 4916451936094420, 4916491104658550, 4916603544909870, 4916759155933, 5105105105105100, 5119301340696760, 5263386793750340, 5268196752489640, 5283145597742620, 5424000000000015, 5429800397359070, 5431111111111111, 5455780586062610, 5472715456453270, 5500000000000004, 5539878514522540, 5547392938355060, 5555555555554440, 5555555555554444, 5556722757422205, 6011000000000000, 6011000000000004, 6011000000000012, 6011000990139420, 6011111111111110, 6011111111111117, 6011312054074430, 6011354276117410, 6011601160116611, 6011905056260500, 869908581608894, 869933317208876, 869989278167071</p>
Controllo Luhn	Lo strumento di convalida calcola il checksum Luhn che tutti i numeri di carta di credito devono superare.
Delimitatore numero	Convalida una corrispondenza verificando il numero vicino.

Copertura limitata numero carta di credito

La copertura limitata rileva i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori. Esegue il controllo di convalida Luhn. Include i formati per American Express, Diners Club, Discover, Japan Credit Bureau (JCB), MasterCard e Visa.

Rimuove i numeri di prova comuni, compresi quelli riservati ai test eseguiti dagli emittenti di carte di credito. Richiede inoltre la presenza di una parola chiave associata alla carta di credito.

Tabella 40-164 Criteri copertura limitata numero carta di credito

Criteri	Criteri (continua)
	222[1-9]\d{12}
	222[1-9][.-]\d{4}[.-]\d{4}[.-]\d{4}
	22[3-9]\d{13}
	22[3-9]\d[.-]\d{4}[.-]\d{4}[.-]\d{4}
	2[3-6]\d{14}
	2[3-6]\d{2}.\d{4}.\d{4}.\d{4}
	2[3-6]\d{2}-\d{4}-\d{4}-\d{4}
	2[3-6]\d{2} \d{4} \d{4} \d{4}
	27[0-1]\d{13}
	27[0-1]\d.\d{4}.\d{4}.\d{4}
	27[0-1]\d-\d{4}-\d{4}-\d{4}
	27[0-1]\d \d{4} \d{4} \d{4}
	2720.\d{4}.\d{4}.\d{4}
	2720-\d{4}-\d{4}-\d{4}
	2720 \d{4} \d{4} \d{4}
	2720\d{12}
	6221[2][6-8]\d{10}
	6221.[2][6-8]\d{2}.\d{4}.\d{4}
	6221-[2][6-8]\d{2}-\d{4}-\d{4}
	6221 [2][6-8]\d{2} \d{4} \d{4}
	622[2-8]\d{12}
	622[2-8].\d{4}.\d{4}.\d{4}
	622[2-8]-\d{4}-\d{4}-\d{4}
	622[2-8] \d{4} \d{4} \d{4}
	6229[2][0-5]\d{10}
	6229.[2][0-5]\d{2}.\d{4}.\d{4}
	6229-[2][0-5]\d{2}-\d{4}-\d{4}
	6229 [2][0-5]\d{2} \d{4} \d{4}

Criteri	Criteri (continua)
2149 \d{6} \d{5}	
2149-\d{6}-\d{5}	
2014\d{11}	
2014 \d{6} \d{5}	
2014-\d{6}-\d{5}	
6011-\d{4}-\d{4}-\d{4}	
6011 \d{4} \d{4} \d{4}	
6011\d{12}	
3[068]\d{12}	
3[068]\d{2} \d{6} \d{4}	
3[068]\d{2}-\d{6}-\d{4}	
3[47]\d{2}-\d{6}-\d{5}	
3[47]\d{2} \d{6} \d{5}	
3[47]\d{13}	
4\d{3}-\d{4}-\d{4}-\d{4}	
3\d{3}.\d{4}.\d{4}.\d{4}	
2149.\d{6}.\d{5}	
2014.\d{6}.\d{5}	
6011.\d{4}.\d{4}.\d{4}	
3[068]\d{2}.\d{6}.\d{4}	
3[47]\d{2}.\d{6}.\d{5}	
4\d{3}.\d{4}.\d{4}.\d{4}	
1800\d{11}	
4\d{12}	
4\d{3} \d{4} \d{4} \d{4}	
4\d{15}	
5[1-5]\d{2}-\d{4}-\d{4}-\d{4}	
5[1-5]\d{2} \d{4} \d{4} \d{4}	
\d{4}	
5[1-5]\d{14}	

Criteri	Criteri (continua)
5[1-5]\d{2}.\d{4}.\d{4}.\d{4}	
2131\d{11}	
3\d{3}-\d{4}-\d{4}-\d{4}	
3\d{3} \d{4} \d{4} \d{4}	
3\d{15}	
2149\d{11}	

Tabella 40-165 Convalide copertura limitata numero carta di credito

Convalide obbligatorie	Descrizione
Escludi corrispondenza esatta	<p>Esclude ogni corrispondenza con il testo specificato.</p> <p>Input:</p> <p>0111111111111111, 1234567812345670, 180025848680889, 180026939516875, 201400000000009, 201411032364438, 201431736711288, 210002956344412, 214906110040367, 300000000000004, 30175572836108, 30203642658706, 30374367304832, 30569309025904, 3088000000000000, 3088000000000009, 3088272824427380, 3096666928988980, 3158060990195830, 340000000000009, 341019464477148, 3411111111111111, 341132368578216, 343510064010360, 344400377306201, 3530111333300000, 3566002020360500, 370000000000002, 371449635398431, 374395534374782, 378282246310005, 378282246310005, 378282246310005, 378734493671000, 38520000023237, 40070000000027, 4012888888881880, 4024007116284, 4111111111111110, 4111111111111111, 4222222222222, 4242424242424242, 4485249610564758, 4539399050593, 4539475158333170, 4539603277651940, 4539687075612974, 4539890911376230, 4556657397647250, 4716733846619930, 4716976758661, 4916437046413, 4916451936094420, 4916491104658550, 4916603544909870, 4916759155933, 5105105105105100, 5119301340696760, 5263386793750340, 5268196752489640, 5283145597742620, 5424000000000015, 5429800397359070, 5431111111111111, 5455780586062610, 5472715456453270, 5500000000000004, 5539878514522540, 5547392938355060, 5555555555554440, 5555555555554444, 5556722757422205, 6011000000000000, 6011000000000004, 6011000000000012, 6011000990139420, 6011111111111110, 6011111111111117, 6011312054074430, 6011354276117410, 6011601160116611, 6011905056260500, 869908581608894, 869933317208876, 869989278167071</p>
Controllo Luhn	Lo strumento di convalida calcola il checksum Luhn che tutti i numeri di carta di credito devono superare.
Delimitatore numero	Convalida una corrispondenza verificando il numero vicino.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di conto, american express, amex, carta bancaria, n. carta, numero carta, n. cc, ncc, carta assegni, carta di credito, n. carta di credito, numero carta di credito, carta di debito, diners club, dinersclub, discover, enrout, japanese card bureau, jcb, mastercard, mc, visa</p>

Numero CUSIP

Il numero CUSIP è un identificatore univoco assegnato ai titoli azionari statunitensi o ad altri titoli. È rilasciato dal CUSIP per fornire assistenza nella liquidazione e negoziazione di transazioni. Il CINS è un'estensione del CUSIP ed è utilizzato per identificare i titoli al di fuori del Nord America.

L'identificatore di dati del numero CUSIP rileva una stringa alfanumerica di nove caratteri che corrisponde al formato del numero CUSIP.

Questo identificatore di dati fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 9 caratteri con la convalida del checksum.
Vedere ["Copertura ampia Numero CUSIP"](#) a pagina 1002.
- La copertura media rileva un modello alfanumerico di 9 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura media numero CUSIP"](#) a pagina 1003.
- La copertura limitata rileva un modello alfanumerico di 9 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate, con l'esclusione della parola chiave **NNA**.
Vedere ["Copertura limitata numero CUSIP"](#) a pagina 1004.

Copertura ampia Numero CUSIP

La copertura ampia rileva un modello alfanumerico di 9 caratteri con la convalida del checksum. Il 5°, 6°, 7° e 8° carattere possono essere sia lettere che numeri, mentre gli altri sono cifre.

Tabella 40-166 Modello copertura ampia Numero CUSIP

Modello
w\d\w{6}\d

Modello
\w\d\w{4} \w{2} \d

Tabella 40-167 Strumento di convalida copertura ampia Numero CUSIP

Strumento di convalida obbligatorio	Descrizione
Convalida CUSIP	Lo strumento di convalida verifica l'esistenza di intervalli CUSIP non validi e calcola il checksum CUSIP (algoritmo di Luhn, noto anche come Modulo 10).

Copertura media numero CUSIP

La copertura media rileva un modello alfanumerico di 9 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Il 5°, 6°, 7° e 8° carattere possono essere sia lettere che numeri, mentre gli altri sono cifre.

Tabella 40-168 Criterio copertura media numero CUSIP

Criterio
w\d\w{6}\d
\w\d\w{4} \w{2} \d

Tabella 40-169 Convalida copertura media numero CUSIP

Convalida obbligatoria	Descrizione
Convalida CUSIP	Lo strumento di convalida verifica l'esistenza di intervalli CUSIP non validi e calcola il checksum CUSIP (algoritmo di Luhn, noto anche come Modulo 10).
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: cusip, c.u.s.i.p., Committee on Uniform Security Identification Procedures, American Bankers Association, Standard & Poor's, S&P, National Numbering Association, NNA, National Securities Identification Number

Copertura limitata numero CUSIP

La copertura limitata rileva un modello alfanumerico di 9 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate, con l'esclusione della parola chiave **NNA**. Il 5°, 6°, 7° e 8° carattere possono essere sia lettere che numeri, mentre gli altri sono cifre.

Tabella 40-170 Criterio copertura limitata numero CUSIP

Criterio
w\d\w{6}\d
\w\d\w{4} \w{2} \d

Tabella 40-171 Convalide copertura limitata numero CUSIP

Convalida obbligatoria	Descrizione
Convalida CUSIP	Lo strumento di convalida verifica l'esistenza di intervalli CUSIP non validi e calcola il checksum CUSIP (algoritmo di Luhn, noto anche come Modulo 10).
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: cusip, c.u.s.i.p., Committee on Uniform Security Identification Procedures, American Bankers Association, Standard & Poor's, S&P, National Numbering Association, National Securities Identification Number

Numero di identificazione personale ceco

A tutti i cittadini della repubblica Ceca viene assegnato un numero di identificazione personale univoco rilasciato dal Ministero dell'Interno.

L'identificatore di dati per il Numero di identificazione personale ceco rileva un numero di 9 o 10 cifre che corrisponde al formato del Numero di identificazione personale ceco.

Questo identificatore di dati fornisce tre coperture di convalida:

- La copertura ampia rileva un numero di 9 o 10 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di identificazione personale ceco"](#) a pagina 1005.
- La copertura media rileva un numero di 9 o 10 cifre con la convalida del checksum. Vedere ["Copertura media numero di identificazione personale ceco"](#) a pagina 1005.
- La copertura media rileva un numero di 9 o 10 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Vedere ["Copertura limitata numero di identificazione personale ceco"](#) a pagina 1006.

Copertura ampia del numero di identificazione personale ceco

La copertura ampia rileva un numero di 9 o 10 cifre senza la convalida del checksum.

Tabella 40-172 Criteri di copertura ampia del numero di identificazione personale ceco

Criterio
\d\d[0156]\d[0123]\d[/]\d\d\d
\d\d[0156]\d[0123]\d[/]\d\d\d\d
\d\d[0156]\d[0123]\d\d\d\d
\d\d[0156]\d[0123]\d\d\d\d\d
\d\d[0156]\d[012345678]\d[/]\d\d\d
\d\d[0156]\d[012345678]\d[/]\d\d\d\d
\d\d[0156]\d[012345678]\d\d\d\d
\d\d[0156]\d[012345678]\d\d\d\d\d

Tabella 40-173 Convalida di copertura ampia del numero di identificazione personale ceco

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione personale ceco

La copertura media rileva un numero di 9 o 10 cifre con la convalida del checksum.

Tabella 40-174 Criterio di copertura media del numero di identificazione personale ceco

Criterio
\d\d[0156]\d[0123]\d[/]\d\d\d
\d\d[0156]\d[0123]\d[/]\d\d\d\d
\d\d[0156]\d[0123]\d\d\d\d
\d\d[0156]\d[0123]\d\d\d\d\d

Criterio
\d\d[0156]\d[012345678]\d[/]\d\d\d
\d\d[0156]\d[012345678]\d[/]\d\d\d\d
\d\d[0156]\d[012345678]\d\d\d\d
\d\d[0156]\d[012345678]\d\d\d\d\d

Tabella 40-175 Convalide copertura media numero di identificazione personale ceco

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di identificazione personale ceco	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri iniziali	5555555555, 1111111111, 111111111

Copertura limitata numero di identificazione personale ceco

La copertura media rileva un numero di 9 o 10 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-176 Criteri copertura limitata numero di identificazione personale ceco

Criterio
\d\d[0156]\d[0123]\d[/]\d\d\d
\d\d[0156]\d[0123]\d[/]\d\d\d\d
\d\d[0156]\d[0123]\d\d\d\d
\d\d[0156]\d[0123]\d\d\d\d\d
\d\d[0156]\d[012345678]\d[/]\d\d\d
\d\d[0156]\d[012345678]\d[/]\d\d\d\d
\d\d[0156]\d[012345678]\d\d\d\d
\d\d[0156]\d[012345678]\d\d\d\d\d

Tabella 40-177 convalida copertura limitata numero di identificazione personale ceco

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di identificazione personale ceco	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero ID personale, PID, numero identità personale, numero ID personale ceco, num identità, ID Repubblica Ceca, numero identità repubblica, numero nazionale, numero previdenza sociale, numero identificazione univoco, N.PID, num.idceco, num.identità</p> <p>Osobní identifikační číslo, Pojištění číslo, unikátní identifikační číslo , Osobní identifikační číslo, identifikační číslo</p>

Numero di identificazione personale danese

Ogni cittadino danese ha un numero di identificazione nazionale. Tale numero viene utilizzato come prova dell'identità di una persona in molti ambiti.

L'identificatore di dati per il Numero di identificazione personale danese rileva un numero a 10 cifre che corrisponde al formato del Numero di identificazione personale danese.

L'identificatore di dati per il Numero di identificazione personale danese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione personale danese"](#) a pagina 1008.
- La copertura media rileva un numero a 10 cifre con la convalida del checksum.
Vedere ["Copertura media del numero di identificazione personale danese"](#) a pagina 1008.
- La copertura media rileva un numero a 10 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di identificazione personale danese"](#) a pagina 1009.

Copertura ampia del numero di identificazione personale danese

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-178 Modelli copertura ampia del numero di identificazione personale danese

Modelli
$\backslash d\{6\}[-]\backslash d\{4\}$
$\backslash d\{6\}[-]\backslash 1\{4\}$
$\backslash d\{10\}$

Tabella 40-179 Convalida di copertura ampia del numero di identificazione personale danese

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione personale danese

La copertura media rileva un numero a 10 cifre con la convalida del checksum.

Tabella 40-180 Modelli di copertura media del numero di identificazione personale danese

Modelli
$\backslash d\{6\}[-]\backslash d\{4\}$
$\backslash d\{6\}[-]\backslash 1\{4\}$
$\backslash d\{10\}$

Tabella 40-181 Convalide di copertura media del numero di identificazione personale danese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione personale danese	Convalida checksum del numero di identificazione personale danese.

Copertura limitata numero di identificazione personale danese

La copertura media rileva un numero di dieci cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-182 Modelli copertura limitata numero di identificazione personale danese

Modelli
$\backslash d\{6\}[-]\backslash d\{4\}$
$\backslash d\{6\}[-]\backslash 1\{4\}$
$\backslash d\{10\}$

Tabella 40-183 Convalide copertura limitata codice identificativo personale danese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione personale danese	Convalida checksum del numero di identificazione personale danese.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di identificazione nazionale, numero di identità nazionale, numero di identità personale, numero di identificazione personale, n.identità nazionale, n.identità personale, numero di identità univoco, n.identità univoco</p> <p>Nationalt identifikationsnummer, personnummer, unikt identifikationsnummer, identifikationsnummer, centrale personregister, cpr, cpr-nummer, cpr#, cpr-nummer#, identifikationsnummer#, personnummer#</p>

Numero di identificazione fiscale danese

La Danimarca rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Danimarca. Il numero di identificazione fiscale funge anche da numero di assicurazione sanitaria personale.

L'identificatore di dati del numero di identificazione fiscale danese rileva un numero di 10 cifre che corrisponde al formato del numero di identificazione fiscale danese.

L'identificatore di dati del numero di identificazione fiscale danese offre tre coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione fiscale danese"](#) a pagina 1010.
- La copertura media rileva un numero a 10 cifre con la convalida del checksum.
Vedere ["Copertura media del numero di identificazione fiscale danese"](#) a pagina 1010.
- La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di identificazione fiscale danese"](#) a pagina 1011.

Copertura ampia del numero di identificazione fiscale danese

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-184 Modello di copertura ampia del numero di identificazione fiscale danese

Criterio
$\backslash d\{6\}-\backslash d\{4\}$

Tabella 40-185 Convalide di copertura ampia del numero di identificazione fiscale danese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione fiscale danese

La copertura media rileva un numero a 10 cifre con la convalida del checksum.

Tabella 40-186 Modello di copertura media del numero di identificazione fiscale danese

Criterio
$\backslash d\{6\}-\backslash d\{4\}$

Tabella 40-187 Convalida di copertura media del numero di identificazione fiscale danese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione fiscale danese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione fiscale danese

La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-188 Modello di copertura limitata del numero di identificazione fiscale danese

Criterio
$\backslash d\{6\}-\backslash d\{4\}$

Tabella 40-189 Convalide di copertura limitata del numero di identificazione fiscale danese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione fiscale danese	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>cod. fiscale, codice fiscale, codice di identificazione fiscale</p> <p>skat id, skattnummer, skat identifikationsnummer, skat kode</p> <p>numero cpr, n. cpr, numero id fisc, cpr, CPR, assicurazione sanitaria, numero di assicurazione sanitaria, numero di tessera sanitaria, tessera sanitaria, tessera sanitaria di viaggio, numero tessera di assicurazione sanitaria</p> <p>sygesikring, Sundhedsforsikringsnummer, sundhedskortnummer, sundhedskort, REJSESYGESIKRINGSKORT, Sundhedsforsikringskort, sygesikringkortnummer, Krankenkassennummer, Gesundheitskarte Nummer, ReisekrankenversicherungskarteNummer, GesundheitsVersicherungskarte Nummer</p>

Numero di partita IVA danese

L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Danimarca, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.

Il numero di partita IVA danese rileva una stringa alfanumerica di 10 caratteri che corrisponde al formato del numero di partita IVA danese.

L'identificatore di dati della partita IVA danese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 10 caratteri preceduto da **DK** senza la convalida del checksum.
Vedere ["Copertura ampia del numero di partita IVA danese"](#) a pagina 1013.
- La copertura media rileva un modello alfanumerico di 10 caratteri preceduto da **DK** con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA danese"](#) a pagina 1013.
- La copertura limitata rileva un modello alfanumerico di 10 caratteri preceduto da **DK** con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Vedere ["Copertura limitata del numero di partita IVA danese"](#) a pagina 1014.

Copertura ampia del numero di partita IVA danese

La copertura ampia rileva un modello alfanumerico di 10 caratteri preceduto da DK senza la convalida del checksum.

Tabella 40-190 Modelli di copertura ampia del numero di partita IVA danese

Modelli
[Dd] [Kk] \d{8}
[Dd] [Kk] \d{8}
[Dd] [Kk] \d{3} \d{3} \d{2}
[Dd] [Kk] \d{3}-\d{3}-\d{2}
[Dd] [Kk] \d{3}.\d{3}.\d{2}
[Dd] [Kk] -\d{8}
[Dd] [Kk] \d{3},\d{3},\d{2}

Tabella 40-191 Convalide di copertura ampia del numero di partita IVA danese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	Esclude le seguenti stringhe di caratteri finali: 00000000, 11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999

Copertura media del numero di partita IVA danese

La copertura media rileva un modello alfanumerico di 10 caratteri preceduto da DK con la convalida del checksum.

Tabella 40-192 Modelli di copertura media del numero di partita IVA danese

Modelli
[Dd] [Kk] \d{8}
[Dd] [Kk] \d{8}

Modelli
[Dd] [Kk] \d{3} \d{3} \d{2}
[Dd] [Kk] \d{3}-\d{3}-\d{2}
[Dd] [Kk] \d{3}.\d{3}.\d{2}
[Dd] [Kk]-\d{8}
[Dd] [Kk] \d{3},\d{3},\d{2}

Tabella 40-193 Convalide di copertura media del numero di partita IVA danese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA danese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di partita IVA danese

La copertura limitata rileva un modello alfanumerico di 10 caratteri preceduto da DK con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate

Tabella 40-194 Modelli di copertura limitata numero di partita IVA danese

Modelli
[Dd] [Kk] \d{8}
[Dd] [Kk] \d{8}
[Dd] [Kk] \d{3} \d{3} \d{2}
[Dd] [Kk] \d{3}-\d{3}-\d{2}
[Dd] [Kk] \d{3}.\d{3}.\d{2}
[Dd] [Kk]-\d{8}
[Dd] [Kk] \d{3},\d{3},\d{2}

Tabella 40-195 Convalide di copertura limitata del numero di partita IVA danese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalide obbligatorie	Descrizione
Escludi caratteri finali	Esclude le seguenti stringhe di caratteri finali: 00000000, 11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999
Controllo di convalida numero di partita IVA danese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero partita IVA, n. partita IVA, n. IVA, numero imposta sul valore aggiunto, numero di identificazione IVA moms, momsnummer, moms identifikationsnummer, merværdiafgift

Numero patente di guida - Stato della California

L'identificatore del numero di patente di guida dello Stato della California (CA) identifica la patente di guida emessa dallo stato della California.

L'identificatore del numero di patente di guida dello stato della California rileva una stringa alfanumerica di 8 caratteri che corrisponde al formato del numero della patente di guida dello stato della California.

Questo identificatore di dati fornisce due coperture di convalida:

- La copertura ampia rileva un modello alfanumerico di otto caratteri che inizia con una lettera seguita da sette numeri.
Vedere ["Copertura ampia Numero patente di guida - Stato della California"](#) a pagina 1015.
- La copertura media convalida un numero utilizzando delle parole chiave.
Vedere ["Copertura media numero patente di guida - Stato della California"](#) a pagina 1016.

Copertura ampia Numero patente di guida - Stato della California

La copertura ampia rileva una stringa alfanumerica di otto caratteri che inizia con una lettera seguita da sette numeri.

Nota: L'opzione di copertura ampia non include nessuno strumento di convalida.

Tabella 40-196 Criterio di copertura ampia del numero di patente di guida

Criterio
\1\d{7}

Copertura media numero patente di guida - Stato della California

La copertura media rileva un modello alfanumerico di otto caratteri che inizia con una lettera seguita da sette numeri. Convalida un numero rilevato richiedendo una parola chiave relativa alla patente di guida E una parola chiave relativa alla California.

Tabella 40-197 Criterio copertura media numero patente di guida - Stato della California

Criterio
\1\d{7}

Tabella 40-198 Convalide copertura media numero patente di guida - Stato della California

Convalide obbligatorie	Descrizione
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics# (patente di guida, patenti di guida, n.pg, n.pat., n.p., n.p.g.)
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: ca, calif, california

Numero di patente di guida - Stati della Florida, del Michigan e del Minnesota

Gli identificatori dei numeri di patente di guida degli stati della Florida (FL), Michigan (MI) e Minnesota (MN) identificano la patente rilasciata da uno di questi stati americani. Questi stati vengono raggruppati insieme perché presentano lo stesso formato per questo numero.

Questo identificatore di dati rileva una stringa alfanumerica di 13 caratteri che corrisponde al formato del numero di patente degli stati della Florida, Michigan e Minnesota.

Questo identificatore di dati fornisce due coperture di convalida:

- La copertura ampia rileva una stringa alfanumerica di 13 caratteri con una lettera seguita da 12 cifre.
Vedere ["Copertura ampia numero patente di guida - Stati Florida, Michigan, Minnesota"](#) a pagina 1017.
- La copertura media limita l'ambito richiedendo la presenza di parole chiave.
Vedere ["Copertura media numero patente di guida - Stati della Florida, del Michigan e del Minnesota"](#) a pagina 1017.

Copertura ampia numero patente di guida - Stati Florida, Michigan, Minnesota

La copertura ampia di questo identificatore di dati rileva una stringa di 13 caratteri con una lettera seguita da 12 cifre.

Per il numero di patente di guida dello stato del Minnesota, viene cercata la corrispondenza con il seguente formato: L-DDD-DDD-DDD-DDD.

Nota: L'opzione di copertura ampia non include nessuno strumento di convalida.

Tabella 40-199 Modelli copertura ampia numero di patente di guida degli stati Florida, Michigan, Minnesota

Criteri
$\backslash 1 \backslash d\{3\} \backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash 1 \backslash d\{12\}$
$\backslash 1 \backslash d\{3\} - \backslash d\{3\} - \backslash d\{2\} - \backslash d\{3\} - \backslash d\{3\}$
$\backslash 1 - \backslash d\{3\} - \backslash d\{3\} - \backslash d\{3\} - \backslash d\{3\}$

Copertura media numero patente di guida - Stati della Florida, del Michigan e del Minnesota

La copertura media di questo identificatore di dati impiega degli identificatori di dati per rilevare una stringa di 13 caratteri con una lettera seguita da 12 cifre. Per il numero di patente di guida dello stato del Minnesota, viene cercata la corrispondenza con il seguente formato: L-DDD-DDD-DDD-DDD.

Questo identificatore di dati convalida il numero richiedendo una parola chiave associata alla patente di guida E una parola chiave relativa allo stato.

Tabella 40-200 Criteri copertura media numero patente di guida - Stati della Florida, del Michigan e del Minnesota

Criteri
\1 \d{3} \d{3} \d{3} \d{3}
\1\d{12}
\1\d{3}-\d{3}-\d{2}-\d{3}-\d{3}
\1-\d{3}-\d{3}-\d{3}-\d{3}

Tabella 40-201 Convalide copertura media numero patente di guida - Stati della Florida, del Michigan e del Minnesota

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Richiede che almeno una delle parole o frasi chiave sia presente nei dati corrispondenti.</p> <p>Input:</p> <p>driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics# (patente di guida, patenti di guida, n.pg, n.pat., n.p., n.p.g.)</p>
Trova parole chiave	<p>Richiede che almeno una delle parole o frasi chiave sia presente nei dati corrispondenti.</p> <p>Input:</p> <p>fla, fl, florida, michigan, mi, minnesota, mn</p>

Numero patente di guida - Stato dell'Illinois

Il numero di patente di guida dello stato dell'Illinois (IL) è una stringa alfanumerica di 12 caratteri che identifica la patente di guida rilasciata dallo stato americano del dell'Illinois.

L'identificatore del numero di patente di guida dello stato dell'Illinois rileva una stringa alfanumerica di 12 caratteri che corrisponde al formato del numero della patente di guida dello stato dell'Illinois.

Questo identificatore di dati fornisce due coperture di convalida:

- La copertura ampia rileva una stringa alfanumerica di 12 caratteri senza convalida. Vedere ["Copertura ampia Numero patente di guida - Stato dell'Illinois"](#) a pagina 1019.
- La copertura media limita l'ambito richiedendo la presenza di parole chiave. Vedere ["Copertura media numero patente di guida - Stato dell'Illinois"](#) a pagina 1019.

Copertura ampia Numero patente di guida - Stato dell'Illinois

La copertura ampia rileva una stringa alfanumerica di 12 caratteri che inizia con una lettera (la prima lettera del cognome del titolare) seguita da 11 cifre.

Nota: L'opzione di copertura ampia non include nessuno strumento di convalida.

Tabella 40-202 Modelli copertura ampia Numero patente di guida - Stato dell'Illinois

Criteri
\1\d{3}-\d{4}-\d{4}
\1\d{11}

Copertura media numero patente di guida - Stato dell'Illinois

La copertura media rileva una stringa di 12 caratteri che inizia con una lettera (la prima lettera del cognome del titolare) seguita da 11 cifre.

Richiede inoltre una parola chiave associata alla patente di guida E una parola chiave relativa all'Illinois.

Tabella 40-203 Criteri copertura media numero patente di guida - Stato dell'Illinois

Criteri
\1\d{3}-\d{4}-\d{4}
\1\d{11}

Tabella 40-204 Convalide copertura media numero patente di guida - Stato dell'Illinois

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Richiede che almeno una delle parole o frasi chiave sia presente nei dati corrispondenti.</p> <p>Input:</p> <p>driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics# (patente di guida, patenti di guida, n.pg, n.pat., n.p., n.p.g.)</p>

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Richiede che almeno una delle parole o frasi chiave sia presente nei dati corrispondenti.</p> <p>Input:</p> <p>il, illinois</p>

Numero patente di guida - Stato del New Jersey

Il numero di patente di guida dello stato del New Jersey (NJ) è una stringa alfanumerica di 15 caratteri che identifica la patente di guida rilasciata dallo stato americano del New Jersey.

L'identificatore del numero di patente di guida dello stato del New Jersey rileva una stringa alfanumerica di 15 caratteri che corrisponde al formato del numero della patente di guida dello stato del New Jersey.

Questo identificatore di dati fornisce due coperture di convalida:

- La copertura ampia rileva un modello alfanumerico di 15 caratteri senza la convalida del Vedere ["Copertura ampia per Numero patente di guida - Stato del New Jersey"](#) a pagina 1020.
- La copertura media limita l'ambito richiedendo la presenza di parole chiave correlate. Vedere ["Copertura media numero patente di guida - Stato del New Jersey"](#) a pagina 1020.

Copertura ampia per Numero patente di guida - Stato del New Jersey

La copertura ampia rileva una stringa alfanumerica di 15 caratteri che inizia con una lettera (la prima lettera del cognome del titolare) seguita da 14 cifre.

Nota: L'opzione di copertura ampia non include nessuno strumento di convalida.

Tabella 40-205 Modelli copertura ampia per Numero patente di guida - Stato del New Jersey

Criteri
<code>\1\d{4} \d{5} \d{5}</code>
<code>\1\d{14}</code>

Copertura media numero patente di guida - Stato del New Jersey

La copertura media rileva una stringa alfanumerica di 15 caratteri che inizia con una lettera (la prima lettera del cognome del titolare) seguita da 14 cifre.

Questa copertura richiede inoltre una parola chiave associata alla patente di guida E una parola chiave relativa al New Jersey.

Tabella 40-206 Criteri copertura media numero patente di guida - Stato del New Jersey

Criteri
\1\d{3}-\d{4}-\d{4}
\1\d{11}

Tabella 40-207 Convalide copertura media numero patente di guida - Stato del New Jersey

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Richiede che almeno una delle parole o frasi chiave sia presente nei dati corrispondenti.</p> <p>Input:</p> <p>driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics# (patente di guida, patenti di guida, n.pg, n.pat., n.p., n.p.g.)</p>
Trova parole chiave	<p>Richiede che almeno una delle parole o frasi chiave sia presente nei dati corrispondenti.</p> <p>Input:</p> <p>nj, new jersey, newjersey</p>

Numero patente di guida - Stato di New York

Il numero di patente di guida dello Stato di New York (NY) è un identificativo di nove cifre per la patente di guida emessa dallo stato di New York.

L'identificatore di dati per il Numero di patente di guida-Stato dello Stato di New York (NY) rileva un numero di nove cifre che corrisponde al formato del numero di patente di guida dello stato di New York.

L'identificatore di dati rileva la presenza di un numero di patente dello Stato di New York.

Questo identificatore di dati fornisce due coperture di convalida:

- La copertura ampia rileva una stringa di 9 cifre senza convalida.
Vedere ["Copertura ampia Numero patente di guida - Stato di New York"](#) a pagina 1022.
- La copertura media limita l'ambito richiedendo la presenza di parole chiave correlate.
Vedere ["Copertura media numero patente di guida - Stato del New Jersey"](#) a pagina 1020.

Copertura ampia Numero patente di guida - Stato di New York

La copertura ampia rileva un numero di nove cifre senza la convalida.

Nota: L'opzione di copertura ampia non include nessuno strumento di convalida.

Tabella 40-208 Criteri di copertura ampia del numero di patente di guida - Stato di New York

Criteri
\d{3} \d{3} \d{3}
\d{9}

Copertura media numero patente di guida - Stato di New York

La copertura limitata rileva un numero di nove cifre.

Questa copertura richiede inoltre una parola chiave associata alla patente di guida E una parola chiave relativa a New York.

Tabella 40-209 Criteri copertura media numero patente di guida - Stato di New York

Criteri
\d{3} \d{3} \d{3}
\d{9}

Tabella 40-210 Convalide copertura media numero patente di guida - Stato di New York

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Richiede che almeno una delle parole o frasi chiave sia presente nei dati corrispondenti.</p> <p>Input:</p> <p>driver license, drivers license, driver's license, driver licenses, drivers licenses, driver's licenses, dl#, dls#, lic#, lics# (patente di guida, patenti di guida, n.pg, n.pat., n.p., n.p.g.)</p>
Trova parole chiave	<p>Richiede che almeno una delle parole o frasi chiave sia presente nei dati corrispondenti.</p> <p>Input:</p> <p>new york, ny, newyork</p>

Numero di patente di guida - Stato di Washington

Numero di identificazione della patente di guida individuale rilasciata dallo Stato di Washington.

L'identificatore di dati per il Numero di patente di guida-Stato di Washington rileva le stringhe alfanumerici che corrispondono al formato del Numero di patente di guida-Stato di Washington.

L'identificatore di dati relativo al numero di patente di guida - Stato di Washington fornisce tre coperture di rilevamento.

- La copertura ampia rileva una patente di guida dello Stato di Washington senza alcuna convalida.
Vedere "[Copertura ampia del numero di patente di guida - Stato di Washington](#)" a pagina 1023.
- La copertura media rileva una patente di guida dello Stato di Washington con convalida del checksum.
Vedere "[Copertura media numero di patente di guida - Stato di Washington](#)" a pagina 1024.
- La copertura limitata rileva una patente di guida dello Stato di Washington con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero di patente di guida - Stato di Washington](#)" a pagina 1024.

Copertura ampia del numero di patente di guida - Stato di Washington

La copertura ampia rileva una patente di guida dello Stato di Washington senza alcuna convalida.

Tabella 40-211 Criteri di copertura ampia del numero di patente di guida - Stato di Washington

Criterio
$\backslash 1\{5\} \backslash 1[A-Za-z^*] \backslash d\{3\} \backslash w\{2\}$
$\backslash 1\{4\} [*] \backslash 1[A-Za-z^*] \backslash d\{3\} \backslash w\{2\}$
$\backslash 1\{3\} [*] \{2\} \backslash 1[A-Za-z^*] \backslash d\{3\} \backslash w\{2\}$
$\backslash 1\{2\} [*] \{3\} \backslash 1[A-Za-z^*] \backslash d\{3\} \backslash w\{2\}$
$\backslash 1\{1\} [*] \{4\} \backslash 1[A-Za-z^*] \backslash d\{3\} \backslash w\{2\}$

La copertura ampia dell'identificatore dati relativo al numero di patente di guida - Stato di Washington non include una convalida.

Copertura media numero di patente di guida - Stato di Washington

La copertura media rileva una patente di guida dello Stato di Washington con convalida del checksum.

Tabella 40-212 Criteri copertura media numero di patente di guida - Stato di Washington

Criterio
$\setminus 1\{5\} \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$
$\setminus 1\{4\} [*] \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$
$\setminus 1\{3\} [*]\{2\} \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$
$\setminus 1\{2\} [*]\{3\} \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$
$\setminus 1\{1\} [*]\{4\} \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$

Tabella 40-213 Convalide copertura media numero di patente di guida - Stato di Washington

Convalida obbligatoria	Descrizione
Controllo di convalida numero di patente di guida - Stato di Washington	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di patente di guida - Stato di Washington

La copertura limitata rileva una patente di guida dello Stato di Washington con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-214 Criteri di copertura limitata del numero di patente di guida - Stato di Washington

Criterio
$\setminus 1\{5\} \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$
$\setminus 1\{4\} [*] \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$
$\setminus 1\{3\} [*]\{2\} \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$
$\setminus 1\{2\} [*]\{3\} \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$
$\setminus 1\{1\} [*]\{4\} \setminus 1[A-Za-z^*] \setminus d\{3\} \setminus w\{2\}$

Tabella 40-215 Convalide di copertura limitata del numero di patente di guida - Stato di Washington

Convalida obbligatoria	Descrizione
Controllo di convalida numero di patente di guida - Stato di Washington	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: patente di guida, patenti di guida, n.pg, n.pat, wash, washington, wa

Numero di patente di guida - Stato del Wisconsin

Il Numero di patente di guida - Stato del Wisconsin è un numero di identificazione della patente di guida individuale rilasciata dallo stato del Wisconsin.

L'identificatore di dati per il Numero di patente di guida-Stato del Wisconsin rileva i modelli alfanumerici che corrispondono al formato del Numero di patente di guida-Stato del Wisconsin.

L'identificatore di dati Numero di patente di guida - Stato del Wisconsin fornisce tre coperture di rilevamento.

- La copertura ampia rileva un numero di 13 cifre con convalida di esclusione del carattere finale.
Vedere "[Copertura ampia numero patente di guida - Stato del Wisconsin](#)" a pagina 1025.
- La copertura ampia rileva un numero di 13 cifre con esclusione del carattere finale e convalida del checksum.
Vedere "[Copertura media numero patente di guida - Stato del Wisconsin](#)" a pagina 1026.
- La copertura ampia rileva un numero di 13 cifre con esclusione del carattere finale e convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero patente di guida - Stato del Wisconsin](#)" a pagina 1027.

Copertura ampia numero patente di guida - Stato del Wisconsin

La copertura ampia rileva un numero di 13 cifre con convalida di esclusione del carattere finale.

Tabella 40-216 Criteri copertura ampia numero patente di guida - Stato del Wisconsin

Criterio
$\backslash 1 \backslash d\{3\} - \backslash d\{4\} - \backslash d\{4\} - \backslash d\{2\}$
$\backslash 1 \backslash d\{13\}$

Tabella 40-217 Convalida copertura ampia numero di patente di guida - Stato del Wisconsin

Convalida obbligatoria	Descrizione
Escludi caratteri finali	Consente di escludere i seguenti caratteri dalla fine del numero: 0000000000000, 1111111111111, 2222222222222, 3333333333333, 4444444444444, 5555555555555, 6666666666666, 7777777777777, 8888888888888, 9999999999999

Copertura media numero patente di guida - Stato del Wisconsin

La copertura ampia rileva un numero di 13 cifre con esclusione del carattere finale e convalida del checksum.

Tabella 40-218 Criteri copertura media numero patente di guida - Stato del Wisconsin

Criterio
$\backslash 1 \backslash d\{3\} - \backslash d\{4\} - \backslash d\{4\} - \backslash d\{2\}$
$\backslash 1 \backslash d\{13\}$

Tabella 40-219 Strumenti di convalida copertura media numero patente di guida - Stato del Wisconsin

Convalida obbligatoria	Descrizione
Controllo di convalida numero di patente di guida dello Stato del Wisconsin.	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri finali	Consente di escludere i seguenti caratteri dalla fine del numero: 0000000000000, 1111111111111, 2222222222222, 3333333333333, 4444444444444, 5555555555555, 6666666666666, 7777777777777, 8888888888888, 9999999999999

Copertura limitata numero patente di guida - Stato del Wisconsin

La copertura ampia rileva un numero di 13 cifre con esclusione del carattere finale e convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-220 Criteri copertura limitata numero patente di guida - Stato del Wisconsin

Criterio
$\backslash 1 \backslash d\{3\} - \backslash d\{4\} - \backslash d\{4\} - \backslash d\{2\}$
$\backslash 1 \backslash d\{13\}$

Tabella 40-221 Strumenti di convalida copertura limitata numero patente di guida - Stato del Wisconsin

Convalida obbligatoria	Descrizione
Controllo di convalida numero di patente di guida dello Stato del Wisconsin.	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri finali	Consente di escludere i seguenti caratteri dalla fine del numero: 0000000000000, 1111111111111, 2222222222222, 3333333333333, 4444444444444, 5555555555555, 6666666666666, 7777777777777, 8888888888888, 9999999999999
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: patente di guida, patente guidatore, patenti di guida, patenti guidatore, n.pg, n.pat., n.p., n.p.g., wisc., wisconsin, wi

Numero DEA (Drug Enforcement Agency)

Un numero DEA è un numero assegnato ai fornitori di servizi sanitari (come medici, dentisti o veterinari) dall'agenzia Drug Enforcement Administration statunitense, che consente loro di prescrivere ricette per sostanze controllate.

L'identificatore di dati per il Numero DEA (Drug Enforcement Agency) rileva una stringa alfanumerica di otto o nove caratteri che corrisponde al formato del Numero DEA.

L'identificatore di dati per il Numero DEA (Drug Enforcement Agency) fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di otto o nove caratteri senza la convalida.
Vedere "[Copertura ampia del numero DEA \(Drug Enforcement Agency\)](#)" a pagina 1028.
- La copertura media rileva una stringa alfanumerica di otto o nove caratteri con esclusione del carattere finale e convalida del checksum.
Vedere "[Copertura media numero DEA \(Drug Enforcement Agency\)](#)" a pagina 1028.
- La copertura limitata rileva una stringa alfanumerica di otto o nove caratteri con esclusione del carattere finale e convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero DEA \(Drug Enforcement Agency\)](#)" a pagina 1029.

Copertura ampia del numero DEA (Drug Enforcement Agency)

La copertura ampia rileva una stringa alfanumerica di otto o nove caratteri senza la convalida.

Tabella 40-222 Criteri di copertura ampia del numero DEA (Drug Enforcement Agency)

Criterio
[ABFGMPR]\1\d{7}
[ABFGMPR]\d{8}

La copertura ampia dell'identificatore dati del numero DEA (Drug Enforcement Agency) non include alcuna convalida.

Copertura media numero DEA (Drug Enforcement Agency)

La copertura media rileva una stringa alfanumerica di otto o nove caratteri con esclusione del carattere finale e convalida del checksum.

Tabella 40-223 Criteri copertura media numero DEA (Drug Enforcement Agency)

Criterio
[ABFGMPR]\1\d{7}
[ABFGMPR]\d{8}

Tabella 40-224 Strumenti di convalida copertura media numero DEA (Drug Enforcement Agency)

Convalida obbligatoria	Descrizione
Controllo di convalida numero DEA	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri finali	Esclude questi caratteri finali: 5555555, 55555555

Copertura limitata numero DEA (Drug Enforcement Agency)

La copertura limitata rileva una stringa alfanumerica di otto o nove caratteri con esclusione del carattere finale e convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-225 Criteri copertura limitata numero DEA (Drug Enforcement Agency)

Criterio
[ABFGMPR]\1\d{7}
[ABFGMPR]\d{8}

Tabella 40-226 Convalida copertura limitata numero DEA (Drug Enforcement Agency)

Convalida obbligatoria	Descrizione
Controllo di convalida numero DEA	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri finali	Esclude questi caratteri finali: 5555555, 55555555
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero dea, DEA, num. DEA, numero di registrazione DEA, n. registrazione DEA, n. DEA, numero Drug Enforcement Agency, n. Drug Enforcement Agency

Numero di patente di guida finlandese

Il numero di patente di guida finlandese è il modello alfanumerico di 10 caratteri che identifica una singola patente di guida finlandese.

L'identificatore di dati del numero di patente di guida finlandese rileva un modello alfanumerico di 10 caratteri che corrisponde al formato del numero di patente di guida finlandese.

L'identificatore di dati del numero di patente di guida finlandese offre tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 10 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di patente di guida finlandese"](#) a pagina 1030.
- La copertura media rileva un modello alfanumerico di 10 caratteri con la convalida del checksum.
Vedere ["Copertura media del numero patente di guida finlandese"](#) a pagina 1030.
- La copertura limitata rileva un modello alfanumerico di 10 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di patente di guida finlandese"](#) a pagina 1031.

Copertura ampia del numero di patente di guida finlandese

La copertura ampia rileva un modello alfanumerico di 10 caratteri senza la convalida del checksum.

Tabella 40-227 Modello di copertura ampia del numero di patente di guida finlandese

Modelli
$\backslash d\{6\}-\backslash d\{4\}$
$\backslash d\{6\}-\backslash d\{3\}\backslash 1$

Tabella 40-228 Convalida della copertura ampia del numero di patente di guida finlandese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero patente di guida finlandese

La copertura media rileva un modello alfanumerico di 10 caratteri con la convalida del checksum.

Tabella 40-229 Criteri di copertura media del numero patente di guida finlandese

Modelli
$\backslash d\{6\}-\backslash d\{4\}$

Modelli

\d{6}-\d{3}\1

Tabella 40-230 Convalida della copertura media del numero di patente di guida finlandese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di patente di guida finlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di patente di guida finlandese

La copertura limitata rileva un modello alfanumerico di 10 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-231 Modelli di copertura limitata del numero di patente di guida finlandese

Modelli

\d{6}-\d{4}

\d{6}-\d{3}\1

Tabella 40-232 Convalide di copertura limitata del numero di patente di guida finlandese

Convalide obbligatorie	Descrizione
Controllo di convalida numero di patente di guida finlandese	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>patente di guida, numero patente di guida, pat. di guida, patente guida, numero patente guida, patente di guida numero, n. pat. guida, num. pat., patente permis de conduire, ajokortti, ajokortin numero, kuljettaja lic., körkort, körkort nummer, förare lic.</p>

Numero di previdenza sociale europea della Finlandia

Il numero di previdenza sociale europea della Finlandia è un identificatore numerico univoco di 20 cifre assegnato a tutte le persone che usufruiscono dei servizi sanitari in Finlandia.

L'identificatore di dati del numero di previdenza sociale europea della Finlandia rileva un numero di 20 cifre che corrisponde al formato del numero di previdenza sociale europea della Finlandia.

L'identificatore di dati del numero di previdenza sociale europea della Finlandia fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 20 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di previdenza sociale europea della Finlandia"](#) a pagina 1032.
- La copertura limitata rileva un numero di 20 cifre senza la convalida del checksum. Richiede la disponibilità di parole chiave associate. Vedere ["Copertura limitata del numero di previdenza sociale europea della Finlandia"](#) a pagina 1033.

Copertura ampia del numero di previdenza sociale europea della Finlandia

La copertura ampia rileva un numero di 20 cifre senza la convalida del checksum.

Tabella 40-233 Modelli di copertura ampia del numero di previdenza sociale europea della Finlandia

Modelli
8024680246\d{10}
8024680246[-]\d{10}

Tabella 40-234 Convalide di copertura ampia del numero di previdenza sociale europea della Finlandia

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalide obbligatorie	Descrizione
Escludi caratteri iniziali	<p>Esclude le seguenti stringhe di caratteri iniziali:</p> <p>80246802460000000000, 80246802461111111111, 80246802462222222222, 80246802463333333333, 80246802464444444444, 80246802465555555555, 80246802466666666666, 80246802467777777777, 80246802468888888888, 80246802469999999999</p>

Copertura limitata del numero di previdenza sociale europea della Finlandia

La copertura limitata rileva un numero di 20 cifre senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-235 Modelli di copertura limitata del numero di previdenza sociale europea della Finlandia

Modelli
8024680246\d{10}
8024680246[-]\d{10}

Tabella 40-236 Convalide di copertura limitata del numero di previdenza sociale europea della Finlandia

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri iniziali	<p>Esclude le seguenti stringhe di caratteri iniziali:</p> <p>80246802460000000000, 80246802461111111111, 80246802462222222222, 80246802463333333333, 80246802464444444444, 80246802465555555555, 80246802466666666666, 80246802467777777777, 80246802468888888888, 80246802469999999999</p>

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Suomi EHIC-numero, health insurance card, Sairausvakuutuskortti, sairaanhoitokortin, Sjukförsäkringskort, ehic, sairaanhoitokortin, Finland health insurance card, Suomen sairausvakuutuskortti, Finska sjukförsäkringskort, health card number, Terveyskortti, Hälsokort, health card, FinlandEHICNumber#, ehic#, EHIC, sairausvakuutusnumero, health insurance number, sjukförsäkring nummer, EHIC#</p>

Numero di passaporto finlandese

Il passaporto finlandese viene rilasciato alle persone di nazionalità finlandese per viaggiare all'estero. Inoltre facilita le procedure di assistenza fornite dai funzionari consolari finlandesi all'estero.

L'identificatore di dati per il numero di passaporto finlandese rileva una stringa alfanumerica di nove cifre che corrisponde al formato del numero di passaporto finlandese.

L'identificatore di dati del numero di passaporto finlandese fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di nove caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di passaporto finlandese"](#) a pagina 1034.
- La copertura limitata rileva un modello alfanumerico di nove caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.
Vedere ["Copertura limitata del numero di passaporto finlandese"](#) a pagina 1035.

Copertura ampia del numero di passaporto finlandese

La copertura ampia rileva un modello alfanumerico di nove caratteri senza la convalida del checksum.

Tabella 40-237 Modello di copertura ampia del numero di passaporto finlandese

Criterio
[A-Za-z]{2}\d{7}

Tabella 40-238 Convalida di copertura ampia del numero di passaporto finlandese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di passaporto finlandese

La copertura limitata rileva un modello alfanumerico di nove caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-239 Modello di copertura limitata del numero di passaporto finlandese

Criterio
[A-Za-z]{2}\d{7}

Tabella 40-240 Convalide di copertura limitata del numero di passaporto finlandese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di passaporto finlandese, n. di passaporto finlandese, n. passaporto finlandese, n. passaporto Finlandia, numero passaporto finlandese</p> <p>Suomen passin numero, suomalainen passi, passin numero, passin numero.#, passin numero#</p> <p>numero di passaporto, n. di passaporto, n. passaporto, num. passaporto, numero passaporto</p> <p>passin numero, passin numero., passin numero#, passi#</p>

Numero di identificazione fiscale finlandese

La Finlandia rilascia un numero di identificazione fiscale per individui che hanno IDENT_RIGHT_SINGLE_QUOTEobbligo di dichiarazione fiscale in Finlandia.

L'identificatore di dati del numero di identificazione fiscale finlandese rileva una stringa alfanumerica di 8 o 11 caratteri che corrisponde al formato del numero di identificazione fiscale finlandese.

Il numero di identificazione fiscale finlandese fornisce tre coperture di rilevamento::

- La copertura ampia rileva un modello alfanumerico di 8 o 11 caratteri senza la convalida del checksum.
Vedere "[Copertura ampia del numero di identificazione fiscale finlandese](#)" a pagina 1036.
- La copertura media rileva un modello alfanumerico di 8 o 11 caratteri con la convalida del checksum.
Vedere "[Copertura media del numero di identificazione fiscale finlandese](#)" a pagina 1036.
- La copertura limitata rileva un modello alfanumerico di 8 o 11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di identificazione fiscale finlandese](#)" a pagina 1037.

Copertura ampia del numero di identificazione fiscale finlandese

La copertura ampia rileva un modello alfanumerico di 8 o 11 caratteri senza la convalida del checksum.

Tabella 40-241 Criteri copertura ampia numero di identificazione fiscale finlandese

Modelli
<code>\d{6}[Aa+-]\d{3}\w</code>
<code>\d{7}[-]\d</code>

Tabella 40-242 Convalida copertura ampia numero di identificazione fiscale finlandese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero di identificazione fiscale finlandese

La copertura media rileva un modello alfanumerico di 8 o 11 caratteri con la convalida del checksum.

Tabella 40-243 Criteri copertura media numero di identificazione fiscale finlandese

Modelli
<code>\d{6}[Aa+-]\d{3}\w</code>

Modelli

`\d{7}[-]\d`

Tabella 40-244 Convalida di copertura media del numero di identificazione fiscale finlandese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione fiscale finlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione fiscale finlandese

La copertura limitata rileva un modello alfanumerico di 8 o 11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-245 Modelli di copertura limitata del numero di identificazione fiscale finlandese

Modelli

`\d{6}[Aa+-]\d{3}\w`

`\d{7}[-]\d`

Tabella 40-246 Convalide della copertura limitata del numero di identificazione fiscale finlandese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione fiscale finlandese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di identificazione fiscale, codice fiscale, cod. fiscale, cod. fisc., codicefiscale</p> <p>verotunniste, verokortti, verotunnus, veronumero</p>

Numero di partita IVA finlandese

L'imposta sul valore aggiunto (IVA) è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.

L'identificatore di dati del numero di partita IVA finlandese rileva un modello alfanumerico di 10 cifre che corrisponde al formato del numero di partita IVA finlandese.

L'identificatore di dati della partita IVA finlandese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 10 caratteri che iniziano con FI senza la convalida del checksum.
Vedere ["Copertura ampia del numero di partita IVA finlandese"](#) a pagina 1038.
- La copertura media rileva un modello alfanumerico di 10 caratteri che iniziano con FI con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA finlandese"](#) a pagina 1039.
- La copertura limitata rileva un modello alfanumerico di 10 caratteri che iniziano con FI con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di partita IVA finlandese"](#) a pagina 1039.

Copertura ampia del numero di partita IVA finlandese

La copertura ampia rileva un modello alfanumerico di 10 caratteri che iniziano con FI senza la convalida del checksum.

Tabella 40-247 Modelli di copertura ampia del numero di partita IVA finlandese

Modelli
[Ff] [Ii] \d{8}
[Ff] [Ii] \d{8}
[Ff] [Ii] \d{7}-\d
[Ff] [Ii] \d{7}-\d

Tabella 40-248 Convalide di copertura ampia del numero di partita IVA finlandese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	Esclude i seguenti caratteri finali: 00000000, 11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999

Copertura media del numero di partita IVA finlandese

La copertura media rileva un modello alfanumerico di 10 caratteri che iniziano con FI con la convalida del checksum.

Tabella 40-249 Modelli di copertura media del numero di partita IVA finlandese

Modelli
[Ff][Ii]\d{8}
[Ff][Ii] \d{8}
[Ff][Ii]\d{7}-\d
[Ff][Ii] \d{7}-\d

Tabella 40-250 Convalida di copertura media del numero di partita IVA finlandese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA finlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di partita IVA finlandese

La copertura limitata rileva un modello alfanumerico di 10 caratteri che iniziano con FI con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-251 Modelli di copertura limitata numero di partita IVA finlandese

Modelli
[Ff][Ii]\d{8}
[Ff][Ii] \d{8}
[Ff][Ii]\d{7}-\d
[Ff][Ii] \d{7}-\d

Tabella 40-252 Convalide di copertura limitata numero di partita IVA finlandese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalide obbligatorie	Descrizione
Escludi caratteri finali	Esclude i seguenti caratteri finali: 00000000, 11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999
Controllo di convalida numero di partita IVA finlandese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: IVA, numero di partita IVA, n. IVA arvonlisäveronumero, ARVONLISÄVERO, ALV, arvonlisäverotunniste, ALV nro, ALV numero, alv

Codice identificativo personale finlandese

Il numero di identificazione personale finlandese o il codice identificativo personale è un identificatore personale univoco utilizzato per l'identificazione dei cittadini all'interno del governo e di molte altre transazioni.

L'identificatore di dati per il Codice identificativo personale finlandese rileva una stringa alfanumerica che corrisponde al formato del Codice identificativo personale finlandese.

L'identificatore di dati di sistema codice identificativo personale finlandese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un codice identificativo personale finlandese senza convalida. Vedere "[Copertura ampia codice identificativo personale finlandese](#)" a pagina 1040.
- La copertura media rileva un numero di codice identificativo personale finlandese con convalida checksum. Vedere "[Copertura media codice identificativo personale finlandese](#)" a pagina 1041.
- La copertura limitata rileva un numero di codice identificativo personale finlandese con convalida checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata codice identificativo personale finlandese](#)" a pagina 1041.

Copertura ampia codice identificativo personale finlandese

La copertura ampia rileva un codice identificativo personale finlandese senza convalida.

Tabella 40-253 Criterio copertura ampia codice identificativo personale finlandese

Criterio
<code>\d{6} [-+Aa] \d{3} \w</code>

La copertura ampia del codice identificativo personale finlandese non comprende strumenti di convalida.

Copertura media codice identificativo personale finlandese

La copertura media rileva un numero di codice identificativo personale finlandese con convalida checksum.

Tabella 40-254 Criterio di copertura media del codice identificativo personale finlandese

Criterio
<code>\d{6} [-+Aa] \d{3} \w</code>

Tabella 40-255 Convalida copertura media codice identificativo personale finlandese

Convalida obbligatoria	Descrizione
Controllo di convalida codice identificativo personale finlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata codice identificativo personale finlandese

La copertura limitata rileva un numero di codice identificativo personale finlandese con convalida checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-256 Criterio copertura limitata codice identificativo personale finlandese

Criterio
<code>\d{6} [-+Aa] \d{3} \w</code>

Tabella 40-257 Convalide copertura limitata codice identificativo personale finlandese

Convalida obbligatoria	Descrizione
Controllo di convalida codice identificativo personale finlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>codice identificativo, ID personale, codice identità, codice ID nazionale finlandese, numerocodiceIDpersonale, codice identificativo nazionale, codice id, cod. ID nazionale, codice ID nazionale, n. ID</p> <p>tunnistenumero, henkilötunnus, yksilöllinen henkilökohtainen tunnistenumero, Ainutlaatuinen henkilökohtainen tunnus, identiteetti numero, Suomen kansallinen henkilötunnus, henkilötunnusnumero#, kansallisen tunnistenumero, tunnusnumero,kansallinen tunnus numero</p>

Numero di patente di guida francese

Il numero di patente di guida francese è l'identificatore di 12 cifre per la patente di guida individuale rilasciata dall'autorità preposta in Francia.

L'identificatore di dati del numero di patente di guida francese rileva un numero di 12 cifre che corrisponde al formato del numero di patente di guida francese.

L'identificatore di dati del numero di patente di guida francese fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di patente di guida francese"](#) a pagina 1042.
- La copertura limitata rileva un numero di 12 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata del numero di patente di guida francese"](#) a pagina 1043.

Copertura ampia del numero di patente di guida francese

La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum.

Tabella 40-258 Modello di copertura ampia del numero di patente di guida francese

Criterio
$\backslash d\{12\}$

Tabella 40-259 Convalide di copertura ampia del numero di patente di guida francese

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di patente di guida francese

La copertura limitata rileva un numero di 12 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-260 Modello di copertura limitata del numero di patente di guida francese

Criterio
\d{12}

Tabella 40-261 Convalide di copertura limitata del numero di patente di guida francese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero patente di guida, numero di patente di guida permis de conduire</p> <p>Patente di guida, Numero Patente di Guida, numero patente di guida, permis de conduire, Patente Guida, Pat. Guida, Patente di guida, Patente guida, Pat. di guida, Numero pat. guida, numero pat. guida, num. patente di guida, Num. Pat. guida, numero patente guida, n. patente, numero patente</p>

Numero di previdenza sociale francese

La Carte Vitale è una tessera di previdenza sociale utilizzata in Francia che contiene le informazioni mediche del titolare. Ha un numero di serie univoco di 21 cifre.

L'identificatore di dati per il Numero di previdenza sociale francese rileva un numero a 21 cifre che corrisponde al formato del Numero di previdenza sociale francese.

L'identificatore di dati del numero di previdenza sociale francese fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 21 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di previdenza sociale francese"](#) a pagina 1044.
- La copertura limitata rileva un numero di 21 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata del numero di previdenza sociale francese"](#) a pagina 1044.

Copertura ampia del numero di previdenza sociale francese

La copertura ampia rileva un numero di 21 caratteri senza la convalida del checksum.

Tabella 40-262 Modelli di copertura ampia del numero di previdenza sociale francese

Modello
\d{10} \d{10} \d
\d{21}

Tabella 40-263 Convalide di copertura ampia del numero di previdenza sociale francese

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di previdenza sociale francese

La copertura limitata rileva un numero di 21 caratteri senza convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-264 Modelli di copertura limitata del numero di previdenza sociale francese

Modello
\d{10} \d{10} \d
\d{21}

Tabella 40-265 Convalide di copertura limitata del numero di previdenza sociale francese

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: tessera di previdenza, tessera di previdenza sociale, carte vitale, carte d'assuré social

Numero di identificazione fiscale francese

La Francia rilascia un numero di identificazione fiscale a chiunque abbia l'obbligo di dichiarazione fiscale in Francia.

L'identificatore di dati Numero di identificazione fiscale francese rileva un numero a 13 cifre che corrisponde al formato del Numero di identificazione fiscale francese.

L'identificatore dati del numero di identificazione fiscale francese fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di identificazione fiscale francese"](#) a pagina 1045.
- La copertura media rileva un numero di 13 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata del numero di identificazione fiscale francese"](#) a pagina 1046.

Copertura ampia del numero di identificazione fiscale francese

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-266 Modelli copertura ampia numero di identificazione fiscale francese

Modelli
[0123]\d{12}
[0123]\d{1} \d{2} \d{3} \d{3} \d{3}

Tabella 40-267 Convalide di copertura ampia numero di identificazione fiscale francese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di identificazione fiscale francese

La copertura media rileva un numero di 13 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-268 Modelli di copertura limitata del numero di identificazione fiscale francese

Modelli
[0123]\d{12}
[0123]\d{1} \d{2} \d{3} \d{3} \d{3}

Tabella 40-269 Convalide della copertura limitata del numero di identificazione fiscale francese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero di identificazione fiscale, numero fiscale, id fiscale numéro d'identification fiscale

Numero di partita IVA francese

L'imposta sul valore aggiunto (IVA) è un'imposta applicata ai beni e servizi forniti in Francia e viene addebitata al cliente finale. Le aziende devono registrarsi nel registro per il commercio e le aziende in Francia per ottenere il numero di partita IVA.

L'identificatore di dati per il Numero di partita IVA della Francia rileva una stringa alfanumerica di 13 cifre che corrisponde al formato del Numero di partita IVA della Francia.

L'identificatore di dati della partita IVA francese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 13 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia numero di partita IVA francese"](#) a pagina 1047.
- La copertura media rileva un modello alfanumerico di 13 caratteri con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA francese"](#) a pagina 1048.
- La copertura limitata rileva un modello alfanumerico di 13 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di partita IVA francese"](#) a pagina 1048.

Copertura ampia numero di partita IVA francese

La copertura ampia rileva un modello alfanumerico di 13 caratteri senza la convalida del checksum.

Tabella 40-270 Modelli di copertura ampia numero di partita IVA francese

Modelli
[Ff] [Rr] [0-9A-Za-z]{2}\d{9}
[Ff] [Rr] [0-9A-Za-z]{2} \d{9}
[Ff] [Rr] [0-9A-Za-z]{2}\d{9}
[Ff] [Rr] -[0-9A-Za-z]{2}\d{9}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3}-\d{3}-\d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3}.\d{3}.\d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3},\d{3},\d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3} \d{3} \d{3}

Tabella 40-271 Convalide di copertura ampia numero di partita IVA francese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero di partita IVA francese

La copertura media rileva un modello alfanumerico di 13 caratteri con la convalida del checksum.

Tabella 40-272 Modelli di copertura media del numero di partita IVA francese

Modelli
[Ff] [Rr] [0-9A-Za-z]{2}\d{9}
[Ff] [Rr] [0-9A-Za-z]{2} \d{9}
[Ff] [Rr] [0-9A-Za-z]{2}\d{9}
[Ff] [Rr]-[0-9A-Za-z]{2}\d{9}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3}-\d{3}-\d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3}.\d{3}.\d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3},\d{3},\d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3} \d{3} \d{3}

Tabella 40-273 Convalide di copertura media del numero di partita IVA francese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA francese	Convalida checksum per il numero di partita IVA francese.

Copertura limitata numero di partita IVA francese

La copertura limitata rileva un modello alfanumerico di 13 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-274 Modelli copertura limitata numero di partita IVA francese

Modelli
[Ff] [Rr] [0-9A-Za-z]{2}\d{9}

Modelli
[Ff] [Rr] [0-9A-Za-z]{2} \d{9}
[Ff] [Rr] [0-9A-Za-z]{2}\d{9}
[Ff] [Rr] - [0-9A-Za-z]{2} \d{9}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3} - \d{3} - \d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3} . \d{3} . \d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3} , \d{3} , \d{3}
[Ff] [Rr] [0-9A-Za-z]{2} \d{3} \d{3} \d{3}

Tabella 40-275 Convalide di copertura limitata numero di partita IVA francese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di partita IVA francese	Convalida checksum per il numero di partita IVA francese.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di partita IVA della Francia, numero di partita IVA francese, numero di partita IVA, part. IVA, p.IVA, numero per l'imposta sul valore aggiunto, imposta sul valore aggiunto, numero di identificazione SIREN</p> <p>Numéro d'identification taxe sur valeur ajoutée, Numéro taxe valeur ajoutée, taxe valeur ajoutée, Taxe sur la valeur ajoutée, Numéro de TVA intracomunautaire, n° TVA, numéro de TVA, Numéro de TVA en France, français numéro de TVA, Numéro d'identification SIREN</p>

Codice INSEE francese

In Francia il codice INSEE viene utilizzato come numero di previdenza sociale, un numero di identificazione nazionale, e a scopi fiscali e lavorativi.

L'identificatore di dati Codice INSEE francese rileva un numero 15 cifre che corrisponde al formato del codice INSEE francese.

L'identificatore di dati Codice INSEE francese rileva la presenza dei numeri INSEE.

L'identificatore di dati Codice INSEE francese fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 15 cifre che supera la convalida del checksum.
- La copertura limitata rileva un numero di 15 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Copertura ampia codice INSEE francese

La copertura ampia rileva un numero di 15 cifre che codifica data di nascita, provincia di origine, comune di origine e numero d'ordine. L'aggiunta di uno spazio di delimitazione dopo le prime 13 cifre è facoltativa. Le ultime due cifre del codice INSEE codificano una chiave di controllo utilizzata per la convalida di un checksum.

Tabella 40-276 Criteri di copertura ampia codice INSEE francese

Modelli
\d{13} \d{2}
d{15}

Tabella 40-277 Convalida copertura ampia codice INSEE francese

Convalida obbligatoria	Descrizione
Chiave di controllo INSEE	La convalida calcola la chiave di controllo INSEE e la confronta con le ultime due cifre del criterio.

Copertura limitata codice INSEE francese

La copertura limitata rileva un numero di 15 cifre che codifica data di nascita, provincia di origine, comune di origine e numero d'ordine. L'aggiunta di uno spazio di delimitazione dopo le prime 13 cifre è facoltativa. Le ultime due cifre del codice INSEE codificano una chiave di controllo utilizzata per la convalida di un checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-278 Criteri copertura limitata codice INSEE francese

Criterio
\d{13} \d{2}
d{15}

Tabella 40-279 Convalide copertura limitata codice INSEE francese

Convalida obbligatoria	Descrizione
Chiave di controllo INSEE	La convalida calcola la chiave di controllo INSEE e la confronta con le ultime due cifre del criterio.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: INSEE, numéro de sécu, code sécu numero di previdenza sociale, codice di previdenza sociale

Numero di passaporto francese

Il passaporto francese è un documento di identità rilasciato ai cittadini francesi. Oltre a consentire al portatore di viaggiare all'estero e servire come indicazione della cittadinanza francese, il passaporto assicura l'assistenza del consolato francese all'estero o, se necessario, di altri stati membri dell'Unione Europea, nel caso in cui il console francese non sia presente.

L'identificatore di dati per il Numero di passaporto francese rileva una stringa alfanumerica di nove caratteri che corrisponde al formato di Numero di passaporto francese.

L'identificatore di dati del numero di passaporto francese fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di nove caratteri senza la convalida del checksum.
Vedere "[Copertura ampia Numero di passaporto francese](#)" a pagina 1051.
- La copertura limitata rileva un modello alfanumerico di nove caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata Numero di passaporto francese](#)" a pagina 1052.

Copertura ampia Numero di passaporto francese

La copertura ampia rileva una stringa alfanumerica di nove caratteri senza la convalida del checksum.

Tabella 40-280 Criterio copertura ampia Numero di passaporto francese

Criterio
$\backslash d\{2\}\backslash w\{2\}\backslash w\{5\}$

Tabella 40-281 Convalida di copertura ampia Numero di passaporto francese

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata Numero di passaporto francese

La copertura limitata rileva un modello alfanumerico di nove caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-282 Criterio copertura limitata Numero di passaporto francese

Criterio
$\backslash d\{2\}\backslash w\{2\}\backslash w\{5\}$

Tabella 40-283 Convalide copertura limitata Numero di passaporto francese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>passaporto, Passaporto, Passaporto francese, passaporto francese, Tessera passaporto, Libretto passaporto, tessera passaporto, libretto passaporto, numero passaporto, n. passaporto</p> <p>Passeport français, Passeport, Passeport livre, Passeport carte, numéro passeport</p>

Numero di previdenza sociale francese

Il numero di previdenza sociale francese (FSSN) è un numero univoco assegnato ai cittadini francesi o agli stranieri residenti nel paese. Funge da numero di identificazione nazionale.

L'identificatore di dati per il Numero di previdenza sociale francese rileva una stringa alfanumerica di 15 caratteri che corrisponde al formato del Numero di previdenza sociale francese.

L'identificatore di dati per il Numero di previdenza sociale francese fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 15 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di previdenza sociale francese"](#) a pagina 1053.
- La copertura media rileva una stringa alfanumerica di 15 caratteri con la convalida del checksum.
Vedere ["Copertura media numero di previdenza sociale francese"](#) a pagina 1053.
- La copertura limitata rileva una stringa alfanumerica di 15 caratteri, conforme alla convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di previdenza sociale francese"](#) a pagina 1054.

Copertura ampia del numero di previdenza sociale francese

La copertura ampia rileva una stringa alfanumerica di 15 caratteri senza la convalida del checksum.

Tabella 40-284 Criterio della copertura ampia del numero di previdenza sociale francese

Criterio
[12]\d{2}[012]\d{2}[AB1234567890]\d{8}

Tabella 40-285 Convalida della copertura ampia del numero di previdenza sociale francese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di previdenza sociale francese

La copertura media rileva una stringa alfanumerica di 15 caratteri con la convalida del checksum.

Tabella 40-286 Criterio copertura media numero di previdenza sociale francese

Criterio
[12]\d{2}[012]\d{2}[AB1234567890]\d{8}

Tabella 40-287 Strumento di convalida copertura media numero di previdenza sociale francese

Convalida obbligatoria	Descrizione
Controllo di convalida numero di previdenza sociale francese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di previdenza sociale francese

La copertura limitata rileva una stringa alfanumerica di 15 caratteri, conforme alla convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-288 Criterio di copertura limitata del numero di previdenza sociale francese

Criterio
[12]\d{2}[012]\d{2}[AB1234567890]\d{8}

Tabella 40-289 Convalide di copertura limitata del numero di previdenza sociale francese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di previdenza sociale francese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: Numero di previdenza sociale francese, numero di previdenza sociale, n.FSSN, n.SSN, ssn, n.ssn, numerodiprevidenzasociale, numerodiprevidenza, numero di identificazione nazionale, n.diidentificazionenazionale sécurité sociale non., sécurité sociale numéro, code sécurité sociale, numéro d'assurance

Numero di passaporto tedesco

Il numero di passaporto tedesco viene rilasciato alle persone di nazionalità tedesca, in genere per viaggiare all'estero. Un passaporto tedesco è un documento ufficialmente riconosciuto che le autorità tedesche accettano come prova dell'identità dai cittadini tedeschi.

L'identificatore di dati per il Numero di passaporto tedesco rileva una stringa alfanumerica che corrisponde al formato del Numero di passaporto tedesco.

L'identificatore di dati di sistema Numero di passaporto tedesco fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" senza la convalida del checksum.
Vedere ["Copertura ampia numero di passaporto tedesco"](#) a pagina 1055.
- La copertura Media rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" con la convalida del checksum.
Vedere ["Copertura media del numero di passaporto tedesco"](#) a pagina 1055.
- La copertura limitata rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di passaporto tedesco"](#) a pagina 1056.

Copertura ampia numero di passaporto tedesco

La copertura ampia rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" senza la convalida del checksum.

Tabella 40-290 Criteri copertura ampia numero di passaporto tedesco

Modelli
<code>\w{9}\dD</code>
<code>\w{10}[dD]</code>

Tabella 40-291 Convalida di copertura ampia Numero di passaporto tedesco

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di passaporto tedesco

La copertura Media rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" con la convalida del checksum.

Tabella 40-292 Criteri di copertura media del numero di passaporto tedesco

Modelli
<code>\w{9}\dD</code>
<code>\w{10}[dD]</code>

Tabella 40-293 Convalida di copertura media del numero di passaporto tedesco

Convalida obbligatoria	Descrizione
Controllo di convalida del numero di passaporto tedesco	Calcola il checksum che ogni numero di passaporto tedesco deve superare.

Copertura limitata numero di passaporto tedesco

La copertura limitata rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-294 Criteri di copertura limitata del numero di passaporto tedesco

Modelli
<code>\w{9}\dD</code>
<code>\w{10}[\dD]</code>

Tabella 40-295 Convalide di copertura limitata del numero di passaporto tedesco

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida del numero di passaporto tedesco	Calcola il checksum che ogni numero di passaporto tedesco deve superare.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. numero passaporto tedesco, numero passaporto, n. passaporto, n.passaporto#, numeropassaporto# Reisepass kein, Reisepass, Passnummer;"

Numero di identificazione personale tedesco

Il numero di identificazione personale tedesco è rilasciato a tutti i cittadini tedeschi.

L'identificatore di dati per il Numero di identificazione personale tedesco rileva una stringa alfanumerica di 11 caratteri che corrisponde al formato del Numero di identificazione personale tedesco.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" senza la convalida del checksum.
Vedere "[Copertura ampia numero di identificazione personale tedesco](#)" a pagina 1057.
- La copertura Media rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" con la convalida del checksum.
Vedere "[Copertura media numero di identificazione personale tedesco](#)" a pagina 1057.
- La copertura limitata rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero di identificazione personale tedesco](#)" a pagina 1058.

Copertura ampia numero di identificazione personale tedesco

La copertura ampia rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" senza la convalida del checksum.

Tabella 40-296 Criterio copertura ampia numero di identificazione personale tedesco

Criterio
<code>\w{9}\dD</code>

Tabella 40-297 Convalida copertura ampia numero di identificazione personale tedesco

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione personale tedesco

La copertura Media rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" con la convalida del checksum.

Tabella 40-298 Criterio copertura media numero di identificazione personale tedesco

Criterio
<code>\w{9}\dD</code>

Tabella 40-299 Strumento di convalida copertura media numero di identificazione personale tedesco

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione tedesco	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di identificazione personale tedesco

La copertura limitata rileva una stringa alfanumerica di 11 caratteri che termina con la lettera "D" con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-300 Criterio della copertura limitata numero di identificazione personale tedesco

Criterio
<code>\w{9}\dD</code>

Tabella 40-301 Convalide della copertura limitata numero di identificazione personale tedesco

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione tedesco	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Se si seleziona questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numero di identificazione, numero ID, ID personale, identificazione personale, GPID, GPID#, numero ID personale univoco, numero ID personale, numero di previdenza sociale, numero personale di identificazione tedesco</p> <p>persönliche identifikationsnummer, ID-Nummer, Deutsch persönliche-ID-Nummer, persönliche ID Nummer, eindeutige ID-Nummer, persönliche Nummer, identität nummer, Versicherungsnummer</p>

Numero di patente di guida tedesca

Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Germania.

L'identificatore di dati del numero di patente di guida tedesca rileva un modello alfanumerico di 13 caratteri che corrisponde al formato del numero di patente di guida tedesca.

L'identificatore di dati del numero di patente di guida tedesca fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 13 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di patente di guida tedesca"](#) a pagina 1059.
- La copertura limitata rileva un modello alfanumerico di 13 caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di patente di guida tedesca"](#) a pagina 1059.

Copertura ampia del numero di patente di guida tedesca

La copertura ampia rileva un modello alfanumerico di 13 caratteri senza la convalida del checksum.

Tabella 40-302 Modello copertura ampia del numero di patente di guida tedesca

Modello
<code>\w\d{2}\w{6}\d\w</code>

Tabella 40-303 Convalide di copertura ampia del numero di patente di guida tedesca

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di patente di guida tedesca

La copertura limitata rileva un modello alfanumerico di 13 caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-304 Modelli di copertura limitata del numero di patente di guida tedesca

Modello
<code>\w\d{2}\w{6}\d\w</code>

Tabella 40-305 Convalide di copertura limitata del numero di patente di guida tedesca

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Führerschein, Fuhrerschein, Fuehrerschein, Führerscheinnummer, Fuhrerscheinnummer, Fuehrerscheinnummer, Fuhrerscheinnummer, Führerschein- Nr, Fuhrerschein- Nr, Fuehrerschein-Nr</p> <p>Patente di Guida, Numero Patente di Guida, numero patente di guida, Patente di guida, Pat. Guida, Patente Guida, Patente guida, Pat. di guida, N. Patente di Guida, n. patente di guida, N. patente di guida, numero Patente di guida, numero patente guida, DL#, dl#, DLNO#, dlnO#, pat. guida, patente guida</p>

Numero di identificazione fiscale tedesco

La Germania rilascia un numero di identificazione fiscale di 11 cifre per individui che hanno l'obbligo di dichiarazione fiscale in Germania.

L'identificatore di dati per il numero di identificazione fiscale tedesco rileva un numero di 11 cifre che corrisponde al formato del numero di identificazione fiscale tedesco.

L'identificatore di dati del numero di identificazione fiscale tedesco fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum. Vedere ["Copertura ampia numero di identificazione fiscale tedesco"](#) a pagina 1061.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Vedere ["Copertura media numero di identificazione fiscale tedesco"](#) a pagina 1061.

- La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
 Vedere ["Copertura limitata del numero di identificazione fiscale tedesco"](#) a pagina 1062.

Copertura ampia numero di identificazione fiscale tedesco

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-306 Modello di copertura ampia del numero di identificazione fiscale tedesco

Modelli
$\backslash d\{11\}$
$\backslash d\{2\} \backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{2\}-\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{2\}.\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{2\},\backslash d\{3\},\backslash d\{3\},\backslash d\{3\}$

Tabella 40-307 Convalide di copertura ampia del numero di identificazione fiscale tedesco

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione fiscale tedesco

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-308 Criteri di copertura media del numero di identificazione fiscale tedesco

Modelli
$\backslash d\{11\}$
$\backslash d\{2\} \backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{2\}-\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{2\}.\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$

Modelli
$\backslash d\{2\}, \backslash d\{3\}, \backslash d\{3\}, \backslash d\{3\}$

Tabella 40-309 Convalida di copertura media del numero di identificazione fiscale tedesco

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero fiscale tedesco	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione fiscale tedesco

La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-310 Modelli di copertura limitata del numero di identificazione fiscale tedesco

Modelli
$\backslash d\{11\}$
$\backslash d\{2\} \backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{2\} - \backslash d\{3\} - \backslash d\{3\} - \backslash d\{3\}$
$\backslash d\{2\} . \backslash d\{3\} . \backslash d\{3\} . \backslash d\{3\}$
$\backslash d\{2\}, \backslash d\{3\}, \backslash d\{3\}, \backslash d\{3\}$

Tabella 40-311 Convalide della copertura limitata del numero di identificazione fiscale tedesco

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero fiscale tedesco	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>tin, numero tin, n. tin, num. tin, numero di identificazione fiscale tedesco, numero di identificazione fiscale Germania, codice fiscale, num. identificazione fiscale</p> <p>Zinn, Zinnnummer, Zinn Nr, Zinn#, Steueridentifikationsnummer, Steuer Identifikationsnummer, Steuernummer, Steuer ID, Identifikationsnummer</p>

Numero di partita IVA tedesca

L'imposta sul valore aggiunto (IVA) è un'imposta applicata ai beni e servizi forniti in Germania e viene addebitata al cliente finale.

L'identificatore di dati della partita IVA tedesca rileva un modello alfanumerico di 11 caratteri che corrisponde al formato del Numero di partita IVA della Germania.

L'identificatore di dati della partita IVA tedesca fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 11 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia numero di partita IVA tedesca"](#) a pagina 1063.
- La copertura media rileva un modello alfanumerico di 11 caratteri con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA tedesca"](#) a pagina 1064.
- La copertura limitata rileva un modello alfanumerico di 11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di partita IVA tedesca"](#) a pagina 1064.

Copertura ampia numero di partita IVA tedesca

La copertura ampia rileva un modello alfanumerico di 11 caratteri senza la convalida del checksum.

Tabella 40-312 Modelli di copertura ampia numero di partita IVA tedesca

Modelli
[Dd] [Ee] \d{9}
[Dd] [Ee] \d{9}
[Dd] [Ee] \d{3}[,]\d{3}[,]\d{3}
[Dd] [Ee] \d{3}[,]\d{3}[,]\d{3}

Tabella 40-313 Convalida di copertura ampia numero di partita IVA dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero di partita IVA tedesca

La copertura media rileva un modello alfanumerico di 11 caratteri con la convalida del checksum.

Tabella 40-314 Modelli di copertura media del numero di partita IVA tedesca

Modelli
[Dd] [Ee] \d{9}
[Dd] [Ee] \d{9}
[Dd] [Ee] \d{3}[,]\d{3}[,]\d{3}
[Dd] [Ee] \d{3}[,]\d{3}[,]\d{3}

Tabella 40-315 Convalida di copertura media del numero di partita IVA tedesca

Controllo di convalida numero di partita IVA tedesca	Convalida checksum per il numero di partita IVA tedesca.

Copertura limitata numero di partita IVA tedesca

La copertura limitata rileva un modello alfanumerico di 11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-316 Modelli copertura limitata numero di partita IVA tedesca

Modelli
[Dd] [Ee] \d{9}
[Dd] [Ee] \d{9}
[Dd] [Ee] \d{3}[,]\d{3}[,]\d{3}
[Dd] [Ee] \d{3}[,]\d{3}[,]\d{3}

Tabella 40-317 Convalide di copertura limitata numero di partita IVA tedesca

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di partita IVA tedesca	Convalida checksum per il numero di partita IVA tedesca.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Partita IVA, part. iva, partita iva, p.IVA, p.iva</p> <p>Mehrwertsteuer, MwSt, Mehrwertsteuer</p> <p>Identifikationsnummer, Mehrwertsteuer nummer</p>

Codice fiscale della Grecia (AMKA)

Il codice fiscale della Grecia (AMKA) è il numero identificativo di lavoro e di assicurazione di 11 cifre di ogni lavoratore, pensionato e membro della famiglia protetto in Grecia.

Il codice fiscale della Grecia (AMKA) rileva un numero di 11 cifre che corrisponde al formato del codice fiscale della Grecia (AMKA).

L'identificatore di dati del codice fiscale della Grecia (AMKA) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum. Vedere ["Copertura ampia del codice fiscale della Grecia \(AMKA\)"](#) a pagina 1066.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum. Vedere ["Copertura media codice fiscale della Grecia \(AMKA\)"](#) a pagina 1066.
- La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Vedere ["Copertura limitata codice fiscale della Grecia \(AMKA\)"](#) a pagina 1066.

Copertura ampia del codice fiscale della Grecia (AMKA)

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-318 Criterio della copertura ampia del codice fiscale della Grecia (AMKA)

Criterio
\d{11}

Tabella 40-319 Criterio della copertura ampia del codice fiscale della Grecia (AMKA)

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media codice fiscale della Grecia (AMKA)

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-320 Modello copertura media codice fiscale della Grecia (AMKA)

Criterio
\d{11}

Tabella 40-321 Convalida di copertura media del codice fiscale della Grecia (AMKA)

Strumento di convalida obbligatorio	Descrizione
Codice fiscale della Grecia (AMKA)	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata codice fiscale della Grecia (AMKA)

La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-322 Modello di copertura limitata del codice fiscale della Grecia (AMKA)

Criterio
\d{11}

Tabella 40-323 Convalide di copertura limitata del codice fiscale della Grecia (AMKA)

Convalide obbligatorie	Descrizione
Codice fiscale della Grecia (AMKA)	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>codice fiscale greco, cf greco, cf Grecia, cod. fiscale Grecia, cod. fiscale greco, cf, amka, amka greco</p> <p>Αριθμού Μητρώου Κοινωνικής Ασφάλισης</p>

Codice fiscale greco (AFM)

L'Arithmo Forologiko Mitro (AFM) è un codice fiscale personale univoco assegnato a ogni persona residente o proprietaria di beni in Grecia.

L'identificatore di dati Codice fiscale greco rileva un numero di nove cifre che corrisponde al formato del Codice fiscale greco.

L'identificatore di dati di sistema Numero di identificazione personale svedese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum. Vedere "[Copertura ampia del codice fiscale greco \(AFM\)](#)" a pagina 1067.
- La copertura media rileva un numero di nove cifre con la convalida del checksum. Vedere "[Copertura media codice fiscale greco \(AFM\)](#)" a pagina 1068.
- La copertura limitata rileva un numero di nove cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata codice fiscale greco \(AFM\)](#)" a pagina 1068.

Copertura ampia del codice fiscale greco (AFM)

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-324 Criterio di copertura ampia del codice fiscale greco (AFM)

Criterio
\d{9}

Tabella 40-325 Convalida di copertura ampia del codice fiscale greco (AFM)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media codice fiscale greco (AFM)

La copertura media rileva un numero di nove cifre con la convalida del checksum.

Tabella 40-326 Criterio copertura media codice fiscale greco (AFM)

Criterio
\d{9}

Tabella 40-327 Convalida copertura media codice fiscale greco (AFM)

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice fiscale greco	Calcola il checksum che ogni codice fiscale greco deve superare.

Copertura limitata codice fiscale greco (AFM)

La copertura limitata rileva un numero di nove cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-328 Criterio copertura limitata codice fiscale greco (AFM)

Criterio
\d{9}

Tabella 40-329 Strumenti di convalida copertura limitata codice fiscale greco (AFM)

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice fiscale greco	Calcola il checksum che ogni codice fiscale greco deve superare.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>AFM, TIN, N. ID fiscale., n. id fiscale, numero di identificazione fiscale, num. id fiscale, numero registro tasse, num. registro tasse, AFM#, TIN#, codice fiscale, codfiscale, n.id.fiscale</p> <p>Αριθμός Φορολογικού Μητρώου, ΑΦΜ, ΑΦΜ αριθμός, Φορολογικού Μητρώου Νο., τον αριθμό φορολογικού μητρώου</p>

Healthcare Common Procedure Coding System (codice CPT HCPCS).

Il sistema di codifica delle procedure comuni per l'assistenza sanitaria (HCPCS) è un insieme di codici di procedure mediche basati sulla Current Procedural Terminology (CPT) dell'American Medical Association.

L'identificatore di dati Healthcare Common Procedure Coding System (codice CPT HCPCS) rileva un modello alfanumerico di due o cinque caratteri che corrisponde al formato del codice CPT HCPCS.

L'identificatore di dati Healthcare Common Procedure Coding System (codice CPT HCPCS) fornisce due coperture di rilevamento:

- La copertura media rileva un modello alfanumerico di due o cinque caratteri con la convalida del checksum.
Vedere ["Copertura media Healthcare Common Procedure Coding System \(codice CPT HCPCS\)." a pagina 1070.](#)
- La copertura limitata rileva un modello alfanumerico di due o cinque caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Vedere ["Copertura limitata Healthcare Common Procedure Coding System \(codice CPT HCPCS\)"](#) a pagina 1071.

Copertura media Healthcare Common Procedure Coding System (codice CPT HCPCS).

La copertura media rileva un modello alfanumerico di due o cinque caratteri con la convalida del checksum.

Tabella 40-330 Modelli di copertura media Healthcare Common Procedure Coding System (codice CPT HCPCS).

Modelli	Modelli (continua)
[A] [AD-KMO-Z1-9]	[V] [1-35-9P]
[B] [ALOPRU]	[X] [EPSU]
[C] [A-NPR-T]	[Z] [AB]
[D] [A]	[L] \d{4}
[E] [1-4A-EJMPTXY]	[A] [04-9] \d{3}
[F] [1-9A-CPX]	[B] [459] [0-29] \d{2}
[G] [1-9A-HJ-Z]	[C] [12589] \d{3}
[H] [9A-Z]	[E] [0128] \d{3}
[J] [1-4A-FW]	[G] [03689] \d{3}
[K] [1-4A-Z]	[H] [0-2] 0 [0-5] \d
[Q] [1-9C-HJ-NPSTW-Z]	[J] [0-37-9] \d{3}
[QK] 0	[K] [0] [0-14-9] \d{2}
[L] [1CDLMR-T]	[M] 0 [013] [067] [01456]
[M] [2S]	[P] [2379] [06] [0-7] \d
[N] [BRU]	[Q] [0-59] [01459] \d{2}
[P] [1-6A-DIL-OST]	[R] 007 [056]
[R] [A-EIRT]	[S] [0-589] \d{3}
[S] [A-HJ-NQS-Z]	[T] [1245] [0159] [0-49] \d

Modelli	Modelli (continua)
[T] [1-9AC-HJ-NP-W]	[V] [25] [0-7] \d{2}
[U] [1-9A-HJKNP-S]	

Tabella 40-331 Convalida di copertura media Healthcare Common Procedure Coding System (codice CPT HCPCS).

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida codice CPT HCPCS	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata Healthcare Common Procedure Coding System (codice CPT HCPCS)

La copertura limitata rileva un modello alfanumerico di due o cinque caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-332 Modelli di copertura limitata Healthcare Common Procedure Coding System (codice HCPCS CPT)

Modelli	Modelli (continua)
[A] [AD-KMO-Z1-9]	[V] [1-35-9P]
[B] [ALOPRU]	[X] [EPSU]
[C] [A-NPR-T]	[Z] [AB]
[D] [A]	[L] \d{4}
[E] [1-4A-EJMPTXY]	[A] [04-9] \d{3}
[F] [1-9A-CPX]	[B] [459] [0-29] \d{2}
[G] [1-9A-HJ-Z]	[C] [12589] \d{3}
[H] [9A-Z]	[E] [0128] \d{3}
[J] [1-4A-FW]	[G] [03689] \d{3}
[K] [1-4A-Z]	[H] [0-2] 0 [0-5] \d
[Q] [1-9C-HJ-NPSTW-Z]	[J] [0-37-9] \d{3}
[QK] 0	[K] [0] [0-14-9] \d{2}
[L] [1CDLMR-T]	[M] 0 [013] [067] [01456]

Modelli	Modelli (continua)
[M] [2S]	[P] [2379] [06] [0-7] \d
[N] [BRU]	[Q] [0-59] [01459] \d{2}
[P] [1-6A-DIL-OST]	[R] 007 [056]
[R] [A-EIRT]	[S] [0-589] \d{3}
[S] [A-HJ-NQS-Z]	[T] [1245] [0159] [0-49] \d
[T] [1-9AC-HJ-NP-W]	[V] [25] [0-7] \d{2}
[U] [1-9A-HJKNP-S]	

Tabella 40-333 Convalide di copertura limitata Healthcare Common Procedure Coding System (codice HCPCS CPT)

Convalide obbligatorie	Descrizione
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: codice hcpcs cpt, HCPCS, hcpcs, cpt, CPT, healthcare common procedure coding system, terminologia operativa attuale
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice CPT HCPCS	Calcola il checksum e lo utilizza per convalidare il modello.

Numero di assicurazione sanitaria

Il numero di assicurazione sanitaria (HICN) viene assegnato dall'amministrazione della previdenza sociale statunitense a un individuo allo scopo di identificarlo come beneficiario di assistenza sanitaria.

L'identificatore di dati del numero di assicurazione sanitaria rileva un modello alfanumerico di 7-12 caratteri che corrisponde al formato del numero di assicurazione sanitaria.

L'identificatore di dati del numero di assicurazione sanitaria fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 7-12 caratteri senza la convalida del checksum.

Vedere ["Copertura ampia del numero di assicurazione sanitaria"](#) a pagina 1073.

- La copertura media rileva un modello alfanumerico di 7-12 caratteri con la convalida del checksum.
Vedere ["Copertura media del numero di assicurazione sanitaria"](#) a pagina 1074.
- La copertura limitata rileva un modello alfanumerico di 7-12 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di assicurazione sanitaria"](#) a pagina 1074.

Copertura ampia del numero di assicurazione sanitaria

La copertura ampia rileva un modello alfanumerico di 7-12 caratteri senza la convalida del checksum.

Tabella 40-334 Modelli di copertura ampia del numero di assicurazione sanitaria

Modelli
$[a-zA-Z]\{1,3\}-\backslash d\{6\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}\backslash d\{1\}[1-9]\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{3\}[1-9]\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}[1-9]\backslash d\{5\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}-\backslash d\{1\}[1-9]-\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}-[1-9]\backslash d\{1\}-\backslash d\{4\}$
$[0-8]\backslash d\{2\}\backslash d\{1\}[1-9]\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{3\}[1-9]\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{5\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}-\backslash d\{1\}[1-9]-\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}-[1-9]\backslash d\{1\}-\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}-[a-zA-Z][0-9]$

Tabella 40-335 Convalida di copertura ampia del numero di assicurazione sanitaria

Strumento di convalida obbligatorio	
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero di assicurazione sanitaria

La copertura media rileva un modello alfanumerico di 7-12 caratteri con la convalida del checksum.

Tabella 40-336 Modelli di copertura media del numero di assicurazione sanitaria

Modelli
$[a-zA-Z]\{1,3\}-\backslash d\{6\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}\backslash d\{1\}[1-9]\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{3\}[1-9]\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}[1-9]\backslash d\{5\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}-\backslash d\{1\}[1-9]-\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}-[1-9]\backslash d\{1\}-\backslash d\{4\}$
$[0-8]\backslash d\{2\}\backslash d\{1\}[1-9]\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{3\}[1-9]\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{5\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}-\backslash d\{1\}[1-9]-\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}-[1-9]\backslash d\{1\}-\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}-[a-zA-Z][0-9]$

Tabella 40-337 Convalida di copertura media del numero di assicurazione sanitaria

Strumento di convalida obbligatorio	
Controllo numero di previdenza sociale	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di assicurazione sanitaria

La copertura limitata rileva un modello alfanumerico di 7-12 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-338 Modelli di copertura limitata del numero di assicurazione sanitaria

Modelli
$[a-zA-Z]\{1,3\}-\backslash d\{6\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}\backslash d\{1\}[1-9]\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{3\}[1-9]\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}[1-9]\backslash d\{5\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}-\backslash d\{1\}[1-9]-\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}$
$[a-zA-Z]\{1,3\}-[0-8]\backslash d\{2\}-[1-9]\backslash d\{1\}-\backslash d\{4\}$
$[0-8]\backslash d\{2\}\backslash d\{1\}[1-9]\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{3\}[1-9]\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{5\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}-\backslash d\{1\}[1-9]-\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}-[1-9]\backslash d\{1\}-\backslash d\{4\}-[a-zA-Z]\{1,3\}$
$[0-8]\backslash d\{2\}[1-9]\backslash d\{1\}\backslash d\{4\}-[a-zA-Z][0-9]$

Tabella 40-339 Convalide di copertura limitata del numero di assicurazione sanitaria

Convalide obbligatorie	
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo numero di previdenza sociale	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di assicurazione sanitaria, hicn, numero hic, n. hic, n.hic, num hic, hicn#</p>

ID Hong Kong

L'ID Hong Kong è l'identificatore univoco per tutti i residenti di Hong Kong riportato sul documento d'identità di Hong Kong.

L'identificatore di dati dell'ID Hong Kong rileva i criteri di otto caratteri che corrispondono al formato dell'ID Hong Kong.

L'identificatore di dati ID Hong Kong fornisce due coperture di rilevamento:

- La copertura ampia rileva otto caratteri in formato LDDDDDD(D) o LDDDDDD(A). L'ultimo carattere nella stringa rilevata viene utilizzato per convalidare il checksum. Vedere ["Copertura ampia dell'ID Hong Kong"](#) a pagina 1076.
- La copertura limitata rileva otto caratteri in formato LDDDDDD(D) o LDDDDDD(A). L'ultimo carattere nella stringa rilevata viene utilizzato per convalidare il checksum. Richiede inoltre la presenza di parole chiave associate all'ID Hong Kong. Vedere ["Copertura limitata ID Hong Kong"](#) a pagina 1077.

Copertura ampia dell'ID Hong Kong

La copertura ampia rileva otto caratteri in formato LDDDDDD(D) o LDDDDDD(A). L'ultimo carattere nella stringa rilevata viene utilizzato per convalidare il checksum.

Tabella 40-340 Criteri della copertura ampia dell'ID Hong Kong

Criteri
$\backslash w \backslash d \{ 6 \} (\backslash d)$
$\backslash U \backslash w \backslash d \{ 6 \} (\backslash d)$
$\backslash w \{ 2 \} \backslash d \{ 6 \} (\backslash d)$
$\backslash w \backslash d \{ 6 \} (A)$
$\backslash U \backslash w \backslash d \{ 6 \} (A)$
$\backslash w \{ 2 \} \backslash d \{ 6 \} (A)$
$\backslash w \backslash d \{ 7 \}$
$\backslash w \{ 2 \} \backslash d \{ 7 \}$
$\backslash w \backslash d \{ 6 \} [A a]$
$\backslash w \{ 2 \} \backslash d \{ 6 \} [A a]$

Tabella 40-341 Convalida della copertura ampia dell'ID Hong Kong

Convalida obbligatoria	Descrizione
ID Hong Kong	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata ID Hong Kong

La copertura limitata rileva otto caratteri in formato LDDDDDD(D) o LDDDDDD(A). L'ultimo carattere nella stringa rilevata viene utilizzato per convalidare il checksum. Richiede inoltre la presenza di parole chiave associate all'ID Hong Kong.

Tabella 40-342 Criteri copertura limitata ID Hong Kong

Criteri
$\backslash w \backslash d \{ 6 \} (\backslash d)$
$\cup \backslash w \backslash d \{ 6 \} (\backslash d)$
$\backslash w \{ 2 \} \backslash d \{ 6 \} (\backslash d)$
$\backslash w \backslash d \{ 6 \} (A)$
$\cup \backslash w \backslash d \{ 6 \} (A)$
$\backslash w \{ 2 \} \backslash d \{ 6 \} (A)$
$\backslash w \backslash d \{ 7 \}$
$\backslash w \{ 2 \} \backslash d \{ 7 \}$
$\backslash w \backslash d \{ 6 \} [A a]$
$\backslash w \{ 2 \} \backslash d \{ 6 \} [A a]$

Tabella 40-343 Strumenti di convalida copertura limitata ID Hong Kong

Convalide obbligatorie	Descrizione
ID Hong Kong	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>身份證, 三顆星, carta di identità, carta di identità di residente permanente di Hong Kong, HKID</p>

Numero di previdenza sociale ungherese

Il numero di previdenza sociale ungherese (TAJ) è un identificatore univoco rilasciato dal governo ungherese.

L'identificatore di dati per il Numero di previdenza sociale ungherese rileva un numero di nove cifre che corrisponde al formato del Numero di previdenza sociale ungherese.

L'identificatore di dati di sistema per il numero di previdenza sociale ungherese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum. Vedere ["Copertura ampia numero di previdenza sociale ungherese"](#) a pagina 1078.
- La copertura media rileva un numero di nove cifre con la convalida del checksum. Vedere ["Copertura media del numero di previdenza sociale ungherese"](#) a pagina 1078.
- La copertura limitata rileva un numero di nove cifre che supera la convalida del checksum. Richiede inoltre parole chiave associate. Vedere ["Copertura limitata numero di previdenza sociale ungherese"](#) a pagina 1079.

Copertura ampia numero di previdenza sociale ungherese

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-344 Criteri copertura ampia numero di previdenza sociale ungherese

Criterio
\d{9}

Tabella 40-345 Convalida copertura ampia numero di previdenza sociale ungherese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di previdenza sociale ungherese

La copertura media rileva un numero di nove cifre con la convalida del checksum.

Tabella 40-346 Criterio copertura media numero di previdenza sociale ungherese

Criterio
\d{9}

Tabella 40-347 Convalide copertura media del numero di previdenza sociale ungherese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di previdenza sociale ungherese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di previdenza sociale ungherese

La copertura limitata rileva un numero di nove cifre che supera la convalida del checksum. Richiede inoltre parole chiave associate.

Tabella 40-348 Criterio di copertura limitata del numero di previdenza sociale ungherese

Criterio
\d{9}

Tabella 40-349 Strumenti di convalida di copertura limitata del numero di previdenza sociale ungherese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di previdenza sociale ungherese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di previdenza sociale ungherese, numero di previdenza sociale, numeroprevidenzasociale, hssn#, HSSN#, numprevidenzasociale, HSSN, TAJ, TAJ#, SSN, SSN#, num. previdenza sociale</p> <p>ÁFA, Közösségi adószám, Általános forgalmi adószám, hozzáadottérték adó, ÁFA szám, magyar ÁFA szám</p>

Numero di identificazione fiscale ungherese

Il numero di identificazione ungherese è un numero di 10 cifre che comincia sempre con la cifra “8”.

L'identificatore di dati per il Numero di identificazione fiscale ungherese rileva un numero di 10 cifre che corrisponde al formato del Numero di identificazione fiscale ungherese.

L'identificatore di dati di sistema Numero di identificazione fiscale ungherese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre che inizia con “8” senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione fiscale ungherese"](#) a pagina 1080.
- La copertura media rileva un numero a 10 cifre che inizia con la cifra “8” con la convalida del checksum.
Vedere ["Copertura media numero di identificazione fiscale ungherese"](#) a pagina 1080.
- La copertura limitata rileva un numero di 10 cifre che inizia con la cifra “8” e supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di identificazione fiscale ungherese"](#) a pagina 1081.

Copertura ampia del numero di identificazione fiscale ungherese

La copertura ampia rileva un numero di 10 cifre che inizia con “8” senza la convalida del checksum.

Tabella 40-350 Criterio di copertura ampia del numero di identificazione fiscale ungherese

Criterio
[8] \d{9}

Tabella 40-351 Convalida di copertura ampia del numero di identificazione fiscale ungherese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione fiscale ungherese

La copertura media rileva un numero a 10 cifre che inizia con la cifra “8” con la convalida del checksum.

Tabella 40-352 Criterio copertura media numero di identificazione fiscale ungherese

Criterio
[8] \d{9}

Tabella 40-353 Strumenti di convalida copertura media numero di identificazione fiscale ungherese

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice di identificazione fiscale ungherese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di identificazione fiscale ungherese

La copertura limitata rileva un numero di 10 cifre che inizia con la cifra “8” e supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-354 Criterio copertura limitata numero di identificazione fiscale ungherese

Criterio
[8] \d{9}

Tabella 40-355 Convalide della copertura limitata del numero di identificazione fiscale ungherese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice di identificazione fiscale ungherese	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>codice di identificazione fiscale ungherese, CIF ungherese, numero ID fiscale, codice fiscale, n. autorità fiscale, ID fiscale numero identità fiscale, numeroidfiscale, n.CIF, num.CIF, n.CIFungherese, n.identificazione fiscale, n.IDfiscale, adóazonosító szám, adószám, adóhatóság szám</p>

Numero di partita IVA ungherese

Tutte le imprese ungheresi (incluse le organizzazioni non profit) registrate presso l'agenzia delle entrate nazionale hanno un numero di partita IVA.

L'identificatore di dati per il Numero di partita IVA ungherese rileva una stringa alfanumerica di otto caratteri che corrisponde al formato del Numero di partita IVA ungherese.

L'identificatore di dati di sistema Numero di partita IVA ungherese fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di otto caratteri che inizia con le lettere "HU/hu" senza la convalida del checksum.
Vedere ["Copertura ampia numero di partita IVA ungherese"](#) a pagina 1082.
- La copertura media rileva una stringa alfanumerica di otto caratteri che inizia con le lettere "HU/hu" con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA ungherese"](#) a pagina 1083.
- La copertura limitata rileva una stringa alfanumerica di otto caratteri che inizia con le lettere "HU/hu" e supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di partita IVA ungherese"](#) a pagina 1083.

Copertura ampia numero di partita IVA ungherese

La copertura ampia rileva una stringa alfanumerica di otto caratteri che inizia con le lettere "HU/hu" senza la convalida del checksum.

Tabella 40-356 Modelli di copertura ampia Numero di partita IVA ungherese

Modelli
HU\d{8}
hu\d{8}

Tabella 40-357 Strumenti di convalida copertura ampia numero di partita IVA ungherese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di partita IVA ungherese

La copertura media rileva una stringa alfanumerica di otto caratteri che inizia con le lettere "HU/hu" con la convalida del checksum.

Tabella 40-358 Modelli di copertura media Numero di partita IVA ungherese

Modelli
HU\d{8}
hu\d{8}

Tabella 40-359 Convalide della copertura media del numero di partita IVA ungherese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di partita IVA ungherese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di partita IVA ungherese

La copertura limitata rileva una stringa alfanumerica di otto caratteri che inizia con le lettere "HU/hu" e supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-360 Modelli di copertura limitata Numero di partita IVA ungherese

Modelli
HU\d{8}

Modelli

hu\d{8}

Tabella 40-361 Strumenti di convalida copertura limitata numero di partita IVA ungherese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di partita IVA ungherese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>IVA, N. partita IVA, numero partita IVA, n.IVA, num.IVA, num.IVAungherese, cod. fiscale, numero IVA, Imposta sul Valore Aggiunto</p> <p>ÁFA, Közösségi adószám, Általános forgalmi adószám, hozzáadottérték adó, ÁFA szám, magyar ÁFA szám</p>

IBAN paesi centrali

Il numero International Bank Account Number (IBAN) è uno standard internazionale per l'identificazione di conti bancari internazionali.

L'IBAN paesi centrali rileva i numeri IBAN per Andorra, Austria, Belgio, Germania, Italia, Liechtenstein, Lussemburgo, Malta, Monaco, San Marino e Svizzera.

L'identificatore di dati IBAN paesi occidentali offre due coperture di rilevamento:

- La copertura ampia rileva un numero IBAN del Paese specifico con la convalida del checksum.
Vedere ["Copertura ampia IBAN paesi centrali"](#) a pagina 1085.
- La copertura limitata rileva un numero a IBAN del Paese specifico con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata dell'IBAN paesi centrali"](#) a pagina 1086.

Nota: Non aggiungere la convalida NIB ad alcun identificatore dati IBAN che si applica a DLP Agent. La convalida NIB va utilizzata solo con il rilevamento lato server.

Copertura ampia IBAN paesi centrali

La copertura ampia rileva un numero IBAN del Paese specifico con la convalida del checksum. I numeri IBAN possono includere spazi o trattini come delimitatori oppure non presentare alcun delimitatore.

Tabella 40-362 Criteri copertura ampia IBAN paesi centrali

Modelli	Descrizione
AD\d{2}\d{4}\d{4}\w{4}\w{4}\w{4} AD\d{2} \d{4} \d{4} \w{4} \w{4} \w{4} AD\d{2}-\d{4}-\d{4}-\w{4}-\w{4}-\w{4}	Criteri Andorra
AT\d{2}\d{4}\d{4}\d{4}\d{4} AT\d{2} \d{4} \d{4} \d{4} \d{4} AT\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Austria
BE\d{2}\d{4}\d{4}\d{4} BE\d{2} \d{4} \d{4} \d{4} BE\d{2}-\d{4}-\d{4}-\d{4}	Criteri Belgio
CH\d{2}\d{4}\d{w{3}}\w{4}\w{4}\w CH\d{2} \d{4} \d{w{3}} \w{4} \w{4} \w CH\d{2}-\d{4}-\d{w{3}}-\w{4}-\w{4}-\w	Criteri Svizzera
DE\d{2}\d{4}\d{4}\d{4}\d{4}\d{2} DE\d{2} \d{4} \d{4} \d{4} \d{4} \d{2} DE\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Germania
IT\d{2}[A-Z]\d{3}\d{4}\d{3}\w{w{4}}\w{4}\w{3} IT\d{2} [A-Z]\d{3} \d{4} \d{3}\w \w{4} \w{4} \w{3} IT\d{2}-[A-Z]\d{3}-\d{4}-\d{3}\w-\w{4}-\w{4}-\w{3}	Criteri Italia
LI\d{2}\d{4}\d{w{3}}\w{4}\w{4}\w LI\d{2} \d{4} \d{w{3}} \w{4} \w{4} \w LI\d{2}-\d{4}-\d{w{3}}-\w{4}-\w{4}-\w	Criteri Liechtenstein

Modelli	Descrizione
$LU\{2\}\{3\}w\{4\}w\{4\}w\{4\}$ $LU\{2\}\{3\}w\{4\}w\{4\}w\{4\}$ $LU\{2\}-\{3\}w-w\{4\}-w\{4\}-w\{4\}$	Criteri Lussemburgo
$MC\{2\}\{4\}\{4\}\{2\}w\{2\}w\{4\}w\{4\}w\{2\}$ $MC\{2\}\{4\}\{4\}\{2\}w\{2\}w\{4\}w\{4\}w\{2\}$ $MC\{2\}-\{4\}-\{4\}-\{2\}w\{2\}-w\{4\}-w\{4\}-w\{2\}$	Criteri Monaco
$MT\{2\}[A-Z]\{4\}\{4\}\{3\}w\{4\}w\{4\}w\{4\}w\{3\}$ $MT\{2\}[A-Z]\{4\}\{4\}\{3\}w\{4\}w\{4\}w\{3\}$ $MT\{2\}-[A-Z]\{4\}-\{4\}-\{3\}w-w\{4\}-w\{4\}-w\{3\}$	Criteri Malta
$SM\{2\}[A-Z]\{3\}\{4\}\{3\}w\{4\}w\{4\}w\{3\}$ $SM\{2\}[A-Z]\{3\}\{4\}\{3\}w\{4\}w\{4\}w\{3\}$ $SM\{2\}-[A-Z]\{3\}-\{4\}-\{3\}w-w\{4\}-w\{4\}-w\{3\}$	Criteri San Marino

Tabella 40-363 Strumento di convalida copertura ampia IBAN paesi centrali

Strumento di convalida	Descrizione
Convalida Mod 97	Calcola il checksum ISO 7064 Mod 97-10 della corrispondenza completa.

Copertura limitata dell'IBAN paesi centrali

La copertura limitata rileva un numero a IBAN del Paese specifico con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-364 Criteri della copertura limitata dell'IBAN paesi centrali

Modelli	Descrizione
$AD\{2\}\{4\}\{4\}w\{4\}w\{4\}w\{4\}$ $AD\{2\}\{4\}\{4\}w\{4\}w\{4\}w\{4\}$ $AD\{2\}-\{4\}-\{4\}-w\{4\}-w\{4\}-w\{4\}$	Criteri Andorra

Modelli	Descrizione
AT\d{2}\d{4}\d{4}\d{4}\d{4} AT\d{2} \d{4} \d{4} \d{4} \d{4} AT\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Austria
BE\d{2}\d{4}\d{4}\d{4} BE\d{2} \d{4} \d{4} \d{4} BE\d{2}-\d{4}-\d{4}-\d{4}	Criteri Belgio
CH\d{2}\d{4}\d{w{3}}\w{4}\w{4}\w CH\d{2} \d{4} \d{w{3}} \w{4} \w{4} \w CH\d{2}-\d{4}-\d{w{3}}-\w{4}-\w{4}-\w	Criteri Svizzera
DE\d{2}\d{4}\d{4}\d{4}\d{4}\d{2} DE\d{2} \d{4} \d{4} \d{4} \d{4} \d{2} DE\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Germania
IT\d{2}[A-Z]\d{3}\d{4}\d{3}\w\w{4}\w{4}\w{3} IT\d{2} [A-Z]\d{3} \d{4} \d{3}\w \w{4} \w{4} \w{3} IT\d{2}-[A-Z]\d{3}-\d{4}-\d{3}\w-\w{4}-\w{4}-\w{3}	Criteri Italia
LI\d{2}\d{4}\d{w{3}}\w{4}\w{4}\w LI\d{2} \d{4} \d{w{3}} \w{4} \w{4} \w LI\d{2}-\d{4}-\d{w{3}}-\w{4}-\w{4}-\w	Criteri Liechtenstein
LU\d{2}\d{3}\w\w{4}\w{4}\w{4} LU\d{2} \d{3}\w \w{4} \w{4} \w{4} LU\d{2}-\d{3}\w-\w{4}-\w{4}-\w{4}	Criteri Lussemburgo
MC\d{2}\d{4}\d{4}\d{2}\w{2}\w{4}\w{4}\w\d{2} MC\d{2} \d{4} \d{4} \d{2}\w{2} \w{4} \w{4} \w\d{2} MC\d{2}-\d{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{4}-\w\d{2}	Criteri Monaco
MT\d{2}[A-Z]{4}\d{4}\d{w{3}}\w{4}\w{4}\w{4}\w{3} MT\d{2} [A-Z]{4} \d{4} \d{w{3}} \w{4} \w{4} \w{4} \w{3} MT\d{2}-[A-Z]{4}-\d{4}-\d{w{3}}-\w{4}-\w{4}-\w{4}-\w{3}	Criteri Malta

Modelli	Descrizione
SM\d{2}[A-Z]\d{3}\d{4}\d{3}\w{4}\w{4}\w{3}	Criteri San Marino
SM\d{2}[A-Z]\d{3}\d{4}\d{3}\w{4}\w{4}\w{3}	
SM\d{2}-[A-Z]\d{3}-\d{4}-\d{3}\w{4}\w{4}\w{3}	

Tabella 40-365 Convalide di copertura limitata IBAN paesi centrali

Convalide	Descrizione
Convalida Mod 97	Calcola il checksum ISO 7064 Mod 97-10 della corrispondenza completa.
Trova parole chiave	Quando si utilizza questa opzione, è necessario utilizzare almeno una delle parole o frasi chiave seguenti per ottenere dati corrispondenti. Input: Code IBAN, numéro IBAN, codice IBAN, numero IBAN

IBAN paesi orientali

Il numero International Bank Account Number (IBAN) è uno standard internazionale per l'identificazione di conti all'estero.

L'identificatore di dati IBAN paesi orientali rileva numeri IBAN per Bosnia, Bulgaria, Croazia, Cipro, Estonia, Grecia, Israele, Lettonia, Lituania, Macedonia, Montenegro, Polonia, Repubblica Ceca, Romania, Serbia, Slovacchia, Slovenia, Turchia, Tunisia e Ungheria.

L'identificatore di dati IBAN paesi occidentali offre due coperture di rilevamento:

- La copertura ampia rileva un numero IBAN del Paese specifico con la convalida del checksum.
Vedere ["Copertura ampia dell'IBAN paesi orientali"](#) a pagina 1089.
- La copertura limitata rileva un numero a IBAN del Paese specifico con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata IBAN paesi orientali"](#) a pagina 1091.

Nota: Non aggiungere la convalida NIB ad alcun identificatore dati IBAN che si applica a DLP Agent. La convalida NIB va utilizzata solo con il rilevamento lato server.

Copertura ampia dell'IBAN paesi orientali

La copertura ampia rileva un numero IBAN del Paese specifico con la convalida del checksum. I numeri IBAN possono includere spazi o trattini come delimitatori oppure non presentare alcun delimitatore.

Tabella 40-366 Criteri di copertura ampia IBAN paesi orientali

Modelli	Descrizione
BA\d{2}\d{4}\d{4}\d{4}\d{4} BA\d{2} \d{4} \d{4} \d{4} \d{4} BA\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Bosnia
BG\d{2}[A-Z]{4}\d{4}\d{2}\w{2}\w{4}\w{2} BG\d{2} [A-Z]{4} \d{4} \d{2}\w{2} \w{4} \w{2} BG\d{2}-[A-Z]{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{2}	Criteri Bulgaria
CY\d{2}\d{4}\d{4}\w{4}\w{4}\w{4}\w{4} CY\d{2} \d{4} \d{4} \w{4} \w{4} \w{4} \w{4} CY\d{2}-\d{4}-\d{4}-\w{4}-\w{4}-\w{4}-\w{4}	Criteri Cipro
CZ\d{2}\d{4}\d{4}\d{4}\d{4}\d{4} CZ\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} CZ\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Repubblica Ceca
EE\d{2}\d{4}\d{4}\d{4}\d{4} EE\d{2} \d{4} \d{4} \d{4} \d{4} EE\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Estonia
GR\d{2}\d{4}\d{3}\w\w{4}\w{4}\w{4}\w{3} GR\d{2} \d{4} \d{3}\w \w{4} \w{4} \w{4} \w{3} GR\d{2}-\d{4}-\d{3}\w-\w{4}-\w{4}-\w{4}-\w{3}	Criteri Grecia
HR\d{2}\d{4}\d{4}\d{4}\d{4}\d{4} HR\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} HR\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Croazia
HU\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4} HU\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{4} HU\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Ungheria

Modelli	Descrizione
IL\d{2}\d{4}\d{4}\d{4}\d{4}\d{3} IL\d{2} \d{4} \d{4} \d{4} \d{4} \d{3} IL\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{3}	Criteri Israele
LT\d{2}\d{4}\d{4}\d{4}\d{4} LT\d{2} \d{4} \d{4} \d{4} \d{4} LT\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Lituania
LV\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w{4} LV\d{2} [A-Z]{4} \w{4} \w{4} \w{4} \w{4} LV\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{4}-\w{4}	Criteri Lettonia
ME\d{2}\d{4}\d{4}\d{4}\d{4}\d{2} ME\d{2} \d{4} \d{4} \d{4} \d{4} \d{2} ME\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Montenegro
MK\d{2}\d{3}\w{4}\w{4}\w{4}\d{2} MK\d{2} \d{3}\w{4} \w{4} \w{4} \w{4}\d{2} MK\d{2}-\d{3}\w{4}-\w{4}-\w{4}-\w{4}\d{2}	Criteri Macedonia
PL\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4} PL\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{4} \d{4} PL\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Polonia
RO\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w{4} RO\d{2} [A-Z]{4} \w{4} \w{4} \w{4} \w{4} RO\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{4}-\w{4}	Criteri Romania
RS\d{2}\d{4}\d{4}\d{4}\d{4}\d{2} RS\d{2} \d{4} \d{4} \d{4} \d{4} \d{2} RS\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Serbia
SI\d{2}\d{4}\d{4}\d{4}\d{3} SI\d{2} \d{4} \d{4} \d{4} \d{3} SI\d{2}-\d{4}-\d{4}-\d{4}-\d{3}	Criteri Slovenia

Modelli	Descrizione
SK\d{2}\d{4}\d{4}\d{4}\d{4}\d{4} SK\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} SK\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Repubblica Slovacca
TN59\d{4}\d{4}\d{4}\d{4}\d{4} TN59 \d{4} \d{4} \d{4} \d{4} \d{4} TN59-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Tunisia
TR\d{2}\d{4}\d{w{3}}\w{4}\w{4}\w{4}\w{2} TR\d{2} \d{4} \d{w{3}} \w{4} \w{4} \w{4} \w{2} TR\d{2}-\d{4}-\d{w{3}}-\w{4}-\w{4}-\w{4}-\w{2}	Criteri Turchia

Tabella 40-367 Convalida della copertura ampia dell'IBAN paesi orientali

Convalida	Descrizione
Convalida Mod 97	Calcola il checksum ISO 7064 Mod 97-10 della corrispondenza completa.

Copertura limitata IBAN paesi orientali

La copertura limitata rileva un numero a IBAN del Paese specifico con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-368 Criteri copertura limitata IBAN paesi orientali

Modelli	Descrizione
BA\d{2}\d{4}\d{4}\d{4}\d{4} BA\d{2} \d{4} \d{4} \d{4} \d{4} BA\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Bosnia
BG\d{2}[A-Z]{4}\d{4}\d{2}\w{2}\w{4}\w{2} BG\d{2} [A-Z]{4} \d{4} \d{2}\w{2} \w{4} \w{2} BG\d{2}-[A-Z]{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{2}	Criteri Bulgaria
CY\d{2}\d{4}\d{4}\w{4}\w{4}\w{4}\w{4} CY\d{2} \d{4} \d{4} \w{4} \w{4} \w{4} \w{4} CY\d{2}-\d{4}-\d{4}-\w{4}-\w{4}-\w{4}-\w{4}	Criteri Cipro

Modelli	Descrizione
CZ\d{2}\d{4}\d{4}\d{4}\d{4}\d{4} CZ\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} CZ\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Repubblica Ceca
EE\d{2}\d{4}\d{4}\d{4}\d{4} EE\d{2} \d{4} \d{4} \d{4} \d{4} EE\d{2}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Estonia
GR\d{2}\d{4}\d{3}\w{4}\w{4}\w{4}\w{3} GR\d{2} \d{4} \d{3}\w \w{4} \w{4} \w{4} \w{3} GR\d{2}-\d{4}-\d{3}\w-\w{4}-\w{4}-\w{4}-\w{3}	Criteri Grecia
HR\d{2}\d{4}\d{4}\d{4}\d{4}\d{4} HR\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} HR\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Croazia
HU\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4} HU\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{4} HU\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Ungheria
IL\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{3} IL\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{3} IL\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{3}	Criteri Israele
LT\d{2}\d{4}\d{4}\d{4}\d{4}\d{4} LT\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} LT\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Lituania
LV\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w{4} LV\d{2} [A-Z]{4} \w{4} \w{4} \w{4} \w{4} \w{4} LV\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{4}-\w{4}	Criteri Lettonia
ME\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{2} ME\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{2} ME\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Montenegro

Modelli	Descrizione
$MK\backslash d\{2\}\backslash d\{3\}\backslash w\backslash w\{4\}\backslash w\{4\}\backslash w\backslash d\{2\}$ $MK\backslash d\{2\}\backslash d\{3\}\backslash w\backslash w\{4\}\backslash w\{4\}\backslash w\backslash d\{2\}$ $MK\backslash d\{2\}-\backslash d\{3\}\backslash w-\backslash w\{4\}-\backslash w\{4\}-\backslash w\backslash d\{2\}$	Criteri Macedonia
$PL\backslash d\{2\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}$ $PL\backslash d\{2\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}$ $PL\backslash d\{2\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}$	Criteri Polonia
$RO\backslash d\{2\}[A-Z]\{4\}\backslash w\{4\}\backslash w\{4\}\backslash w\{4\}\backslash w\{4\}$ $RO\backslash d\{2\}[A-Z]\{4\}\backslash w\{4\}\backslash w\{4\}\backslash w\{4\}\backslash w\{4\}$ $RO\backslash d\{2\}-[A-Z]\{4\}-\backslash w\{4\}-\backslash w\{4\}-\backslash w\{4\}-\backslash w\{4\}$	Criteri Romania
$RS\backslash d\{2\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{2\}$ $RS\backslash d\{2\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{2\}$ $RS\backslash d\{2\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{2\}$	Criteri Serbia
$SI\backslash d\{2\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{3\}$ $SI\backslash d\{2\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{3\}$ $SI\backslash d\{2\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{3\}$	Criteri Slovenia
$SK\backslash d\{2\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}$ $SK\backslash d\{2\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}$ $SK\backslash d\{2\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}$	Criteri Repubblica Slovacca
$TN59\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}$ $TN59\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}\backslash d\{4\}$ $TN59-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}$	Criteri Tunisia
$TR\backslash d\{2\}\backslash d\{4\}\backslash d\backslash w\{3\}\backslash w\{4\}\backslash w\{4\}\backslash w\{4\}\backslash w\{2\}$ $TR\backslash d\{2\}\backslash d\{4\}\backslash d\backslash w\{3\}\backslash w\{4\}\backslash w\{4\}\backslash w\{4\}\backslash w\{2\}$ $TR\backslash d\{2\}-\backslash d\{4\}-\backslash d\backslash w\{3\}-\backslash w\{4\}-\backslash w\{4\}-\backslash w\{4\}-\backslash w\{2\}$	Criteri Turchia

Tabella 40-369 Convalide copertura limitata IBAN paesi orientali

Convalide	Descrizione
Convalida Mod 97	Calcola il checksum ISO 7064 Mod 97-10 della corrispondenza completa.

Convalide	Descrizione
Trova parole chiave	<p>Quando si utilizza questa opzione, è necessario utilizzare almeno una delle parole o frasi chiave seguenti per ottenere dati corrispondenti.</p> <p>Input:</p> <p>Code IBAN, numéro IBAN, codice IBAN, numero IBAN</p>

IBAN paesi occidentali

Il numero International Bank Account Number (IBAN) è uno standard internazionale per l'identificazione di conti all'estero.

L'identificatore di dati IBAN paesi occidentali rileva i numeri IBAN per Danimarca, Fær Øer, Finlandia, Francia, Gibilterra, Groenlandia, Irlanda, Islanda, Norvegia, Paesi Bassi, Portogallo, Regno Unito, Spagna e Svezia.

L'identificatore di dati IBAN paesi occidentali offre due coperture di rilevamento:

- La copertura ampia rileva un numero IBAN del Paese specifico con la convalida del checksum.
Vedere ["Copertura ampia dell'IBAN paesi occidentali"](#) a pagina 1094.
- La copertura limitata rileva un numero a IBAN del Paese specifico con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata IBAN paesi occidentali"](#) a pagina 1096.

Nota: Non aggiungere la convalida NIB ad alcun identificatore dati IBAN che si applica a DLP Agent. La convalida NIB va utilizzata solo con il rilevamento lato server.

Copertura ampia dell'IBAN paesi occidentali

La copertura ampia rileva un numero IBAN specifico di un paese che ha superato un checksum. I numeri IBAN possono includere spazi o trattini come delimitatori o possono non presentare alcun delimitatore.

Tabella 40-370 Criteri per copertura ampia dell'IBAN paesi occidentali

Modelli	Descrizione
DK\d{2}\d{4}\d{4}\d{4}\d{2}	Criteri Danimarca
DK\d{2} \d{4} \d{4} \d{4} \d{2}	
DK\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	

Modelli	Descrizione
ES\d{2}\d{4}\d{4}\d{4}\d{4}\d{4} ES\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} ES\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Spagna
FI\d{2}\d{4}\d{4}\d{4}\d{2} FI\d{2} \d{4} \d{4} \d{4} \d{2} FI\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Finlandia
FO\d{2}\d{4}\d{4}\d{4}\d{2} FO\d{2} \d{4} \d{4} \d{4} \d{2} FO\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Isole Fær Øer
FR\d{2}\d{4}\d{4}\d{2}\w{2}\w{4}\w{4}\w{d{2}} FR\d{2} \d{4} \d{4} \d{2}\w{2} \w{4} \w{4} \w{d{2}} FR\d{2}-\d{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{4}-\w{d{2}}	Criteri Francia
GB\d{2}[A-Z]{4}\d{4}\d{4}\d{4}\d{2} GB\d{2} [A-Z]{4} \d{4} \d{4} \d{4} \d{2} GB\d{2}-[A-Z]{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Regno Unito
GI\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w{3} GI\d{2} [A-Z]{4} \w{4} \w{4} \w{4} \w{3} GI\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{4}-\w{3}	Criteri Gibilterra
GL\d{2}\d{4}\d{4}\d{4}\d{2} GL\d{2} \d{4} \d{4} \d{4} \d{2} GL\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Groenlandia
IE\d{2}[A-Z]{4}\d{4}\d{4}\d{4}\d{2} IE\d{2} [A-Z]{4} \d{4} \d{4} \d{4} \d{2} IE\d{2}-[A-Z]{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Irlanda
IS\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{2} IS\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{2} IS\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Islanda

Modelli	Descrizione
$NL\{2\} [A-Z] \{4\} \{4\} \{4\} \{2\}$ $NL\{2\} [A-Z] \{4\} \{4\} \{4\} \{2\}$ $NL\{2\} - [A-Z] \{4\} - \{4\} - \{4\} - \{2\}$	Criteri Paesi Bassi
$NO\{2\} \{4\} \{4\} \{3\}$ $NO\{2\} \{4\} \{4\} \{3\}$ $NO\{2\} - \{4\} - \{4\} - \{3\}$	Criteri Montenegro
$PT\{2\} \{4\} \{4\} \{4\} \{4\} \{4\} \{4\}$ $PT\{2\} \{4\} \{4\} \{4\} \{4\} \{4\} \{4\}$ $PT\{2\} - \{4\} - \{4\} - \{4\} - \{4\} - \{4\} - \{4\}$	Criteri Portogallo
$SE\{2\} \{4\} \{4\} \{4\} \{4\} \{4\}$ $SE\{2\} \{4\} \{4\} \{4\} \{4\} \{4\}$ $SE\{2\} - \{4\} - \{4\} - \{4\} - \{4\} - \{4\}$	Criteri Svezia

Tabella 40-371 Convalida della copertura ampia dell'IBAN paesi occidentali

Convalida	Descrizione
Convalida Mod 97	Calcola il checksum ISO 7064 Mod 97-10 della corrispondenza completa.

Copertura limitata IBAN paesi occidentali

La copertura limitata rileva un numero IBAN specifico per un paese che ha superato un checksum. Richiede inoltre la presenza di parole chiave associate all'IBAN.

Tabella 40-372 Criteri di copertura limitata IBAN paesi occidentali

Modelli	Descrizione
$DK\{2\} \{4\} \{4\} \{4\} \{2\}$ $DK\{2\} \{4\} \{4\} \{4\} \{2\}$ $DK\{2\} - \{4\} - \{4\} - \{4\} - \{2\}$	Criteri Danimarca
$ES\{2\} \{4\} \{4\} \{4\} \{4\} \{4\}$ $ES\{2\} \{4\} \{4\} \{4\} \{4\} \{4\}$ $ES\{2\} - \{4\} - \{4\} - \{4\} - \{4\} - \{4\}$	Criteri Spagna

Modelli	Descrizione
FI\d{2}\d{4}\d{4}\d{4}\d{2} FI\d{2} \d{4} \d{4} \d{4} \d{2} FI\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Finlandia
FO\d{2}\d{4}\d{4}\d{4}\d{2} FO\d{2} \d{4} \d{4} \d{4} \d{2} FO\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Isole Fær Øer
FR\d{2}\d{4}\d{4}\d{2}\w{2}\w{4}\w{4}\w{d{2}} FR\d{2} \d{4} \d{4} \d{2}\w{2} \w{4} \w{4} \w{d{2}} FR\d{2}-\d{4}-\d{4}-\d{2}\w{2}-\w{4}-\w{4}-\w{d{2}}	Criteri Francia
GB\d{2}[A-Z]{4}\d{4}\d{4}\d{4}\d{2} GB\d{2} [A-Z]{4} \d{4} \d{4} \d{4} \d{2} GB\d{2}-[A-Z]{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Regno Unito
GI\d{2}[A-Z]{4}\w{4}\w{4}\w{4}\w{3} GI\d{2} [A-Z]{4} \w{4} \w{4} \w{4} \w{3} GI\d{2}-[A-Z]{4}-\w{4}-\w{4}-\w{4}-\w{3}	Criteri Gibilterra
GL\d{2}\d{4}\d{4}\d{4}\d{2} GL\d{2} \d{4} \d{4} \d{4} \d{2} GL\d{2}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Groenlandia
IE\d{2}[A-Z]{4}\d{4}\d{4}\d{4}\d{2} IE\d{2} [A-Z]{4} \d{4} \d{4} \d{4} \d{2} IE\d{2}-[A-Z]{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Irlanda
IS\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{2} IS\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{2} IS\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{2}	Criteri Islanda
NL\d{2}[A-Z]{4}\d{4}\d{4}\d{2} NL\d{2} [A-Z]{4} \d{4} \d{4} \d{2} NL\d{2}-[A-Z]{4}-\d{4}-\d{4}-\d{2}	Criteri Paesi Bassi

Modelli	Descrizione
NO\d{2}\d{4}\d{4}\d{3} NO\d{2} \d{4} \d{4} \d{3} NO\d{2}-\d{4}-\d{4}-\d{3}	Criteri Montenegro
PT\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4} PT\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{4} PT\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Portogallo
SE\d{2}\d{4}\d{4}\d{4}\d{4}\d{4}\d{4} SE\d{2} \d{4} \d{4} \d{4} \d{4} \d{4} \d{4} SE\d{2}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}-\d{4}	Criteri Svezia

Tabella 40-373 Convalide di copertura limitata IBAN paesi occidentali

Convalide	Descrizione
Convalida Mod 97	Calcola il checksum ISO 7064 Mod 97-10 della corrispondenza completa.
Trova parole chiave	Quando si utilizza questa opzione, è necessario utilizzare almeno una delle parole o frasi chiave seguenti per ottenere dati corrispondenti. Input: Code IBAN, numéro IBAN, codice IBAN, numero IBAN

Numero tessera Aadhaar indiana

Lo UIDAI ha il compito di assegnare un numero UID da 12 cifre chiamato Aadhaar a tutti i residenti dell'India. Il numero Aadhaar è sufficientemente affidabile per eliminare le identità duplicate e contraffatte e può essere verificato e autenticato online in maniera economica.

L'identificatore di dati per il Numero tessera Aadhaar indiana rileva un numero di 12 cifre che corrisponde al formato del Numero tessera Aadhaar indiana.

L'identificatore di dati Numero tessera Aadhaar indiana fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum. Vedere ["Copertura ampia Numero tessera Aadhaar indiana"](#) a pagina 1099.
- La copertura media rileva un numero di 12 cifre con la convalida del checksum. Vedere ["Copertura media Numero tessera Aadhaar indiana"](#) a pagina 1099.

- La copertura limitata rileva un numero a 12 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
 Vedere ["Copertura limitata Numero tessera Aadhaar indiana"](#) a pagina 1100.

Copertura ampia Numero tessera Aadhaar indiana

La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum.

Tabella 40-374 Criteri copertura ampia Numero tessera Aadhaar indiana

Modelli
$[2-9]\backslash d\{11\}$
$[2-9]\backslash d\{3\} \backslash d\{4\} \backslash d\{4\}$

Tabella 40-375 Convalida copertura ampia Numero tessera Aadhaar indiana

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media Numero tessera Aadhaar indiana

La copertura media rileva un numero di 12 cifre con la convalida del checksum.

Tabella 40-376 Criteri copertura media Numero tessera Aadhaar indiana

Modelli
$[2-9]\backslash d\{11\}$
$[2-9]\backslash d\{3\} \backslash d\{4\} \backslash d\{4\}$

Tabella 40-377 Convalide copertura media Numero tessera Aadhaar indiana

Convalide obbligatorie	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 333333333333, 666666666666, 999999999999
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo di convalida Verheoff	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata Numero tessera Aadhaar indiana

La copertura limitata rileva un numero a 12 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-378 Criteri copertura limitata Numero tessera Aadhaar indiana

Modelli
[2-9]\d{11}
[2-9]\d{3} \d{4} \d{4}

Tabella 40-379 Convalide copertura limitata Numero tessera Aadhaar indiana

Convalide obbligatorie	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 333333333333, 666666666666, 999999999999
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo di convalida Verheoff	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: aadhar card no.,uidai,aadhar no.,Aadhar Number,Aadhar#,Aadhar Card#

Codice di identificazione fiscale indiano (PAN)

Il codice di identificazione fiscale indiano (PAN) è un identificatore alfanumerico univoco di 10 caratteri rilasciato dall'anagrafe tributaria indiana a un individuo.

Il Numero di identificazione fiscale indiano rileva una stringa alfanumerica di 10 caratteri che corrisponde al formato del Numero di identificazione fiscale indiano.

Questo identificatore di dati fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 10 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia codice di identificazione fiscale indiano \(PAN\)"](#) a pagina 1101.

- La copertura limitata rileva un modello alfanumerico di 10 caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del codice di identificazione fiscale indiano \(PAN\)](#)" a pagina 1101.

Copertura ampia codice di identificazione fiscale indiano (PAN)

La copertura ampia rileva una stringa alfanumerica di 10 caratteri senza la convalida del checksum.

Tabella 40-380 Criterio copertura ampia codice di identificazione fiscale indiano (PAN)

Criterio
<code>[A-Za-z]{3}[CPHFATBLJGcphfatbljg][A-Za-z]\d{4}[A-Za-z]</code>

Tabella 40-381 Convalida copertura ampia codice di identificazione fiscale indiano (PAN)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata del codice di identificazione fiscale indiano (PAN)

La copertura limitata rileva una stringa alfanumerica di 10 caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-382 Criterio di copertura limitata del codice di identificazione fiscale indiano (PAN)

Criterio
<code>[A-Za-z]{3}[CPHFATBLJGcphfatbljg][A-Za-z]\d{4}[A-Za-z]</code>

Tabella 40-383 Convalide di copertura limitata Numero di identificazione fiscale indiano

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>PAN, numero di identificazione, pan, n.pan, n.PAN, numero scheda PAN, n. scheda pan, n.schedapan, n. scheda PAN, n.IDPAN</p>

Numero di carta di identità indonesiana (KTP)

Il numero di carta di identità indonesiana (Kartu Tanda Penduduk, or KTP) viene utilizzato per il rilascio di passaporto, patente di guida, codice identificativo del contribuente, polizza assicurativa, certificato di proprietà fondiaria e documenti di identità.

L'identificatore di dati per il Numero di carta di identità indonesiana rileva un numero di 16 cifre che corrisponde al formato del Numero di carta di identità indonesiana.

L'identificatore di dati di sistema del numero di carta di identità indonesiana (KTP) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 16 cifre senza la convalida del checksum.
Vedere "[Copertura ampia numero di carta di identità indonesiana \(KTP\)](#)" a pagina 1102.
- La copertura media rileva un numero a 16 cifre con la convalida del checksum.
Vedere "[Copertura media numero di carta di identità indonesiana \(KTP\)](#)" a pagina 1103.
- La copertura limitata rileva un numero di 16 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di carta di identità indonesiana \(KTP\)](#)" a pagina 1103.

Copertura ampia numero di carta di identità indonesiana (KTP)

La copertura ampia rileva un numero di 16 cifre senza la convalida del checksum.

Tabella 40-384 Criterio copertura ampia numero di carta di identità indonesiana (KTP)

Criterio
<code>\d{2}[01237]\d{3}[01234567]\d{01}\d{7}</code>

Tabella 40-385 Convalida copertura ampia numero di carta di identità indonesiana (KTP)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di carta di identità indonesiana (KTP)

La copertura media rileva un numero a 16 cifre con la convalida del checksum.

Tabella 40-386 Criterio copertura media numero di carta di identità indonesiana (KTP)

Criterio
$\backslash d\{2\}[01237]\backslash d\{3\}[01234567]\backslash d[01]\backslash d\{7\}$

Tabella 40-387 Strumento di convalida copertura media numero di carta di identità indonesiana (KTP)

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di carta di identità indonesiana	La convalida calcola il checksum che ogni numero di carta di identità indonesiana (KTP) deve superare.

Copertura limitata del numero di carta di identità indonesiana (KTP)

La copertura limitata rileva un numero di 16 cifre che supera la convalida del checksum.
 Richiede inoltre la presenza di parole chiave associate.

Tabella 40-388 Criterio della copertura limitata del numero di carta di identità indonesiana (KTP)

Criterio
$\backslash d\{2\}[01237]\backslash d\{3\}[01234567]\backslash d[01]\backslash d\{7\}$

Tabella 40-389 Convalide della copertura limitata del numero di carta di identità indonesiana (KTP)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di carta di identità indonesiana	La convalida calcola il checksum che ogni numero di carta di identità indonesiana (KTP) deve superare.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di carta di identità, n. carta di identità indonesiana, numero di carta di identità indonesiana, NIK, KTP, ID univoco, numero di identità univoco, numero di identificazione nazionale, n. di identità nazionale, numero di identità</p> <p>kartu tanda penduduk nomor, nomor Induk Kependudukan, tanda penduduk nomor, kartu identitas Indonesia no, kartu identitas Indonesia nomor, nomor identitas unik</p>

Numero IMEI

Il numero IMEI (International Mobile Equipment Identity) è un identificatore univoco per cellulari 3GPP (GSM, UMTS e LTE) e iDEN, nonché alcuni telefoni satellitari.

Il Numero IMEI rileva un numero di 15 cifre che corrisponde al formato del Numero IMEI.

L'identificatore di dati per il Numero IMEI fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 15 cifre con la doppia convalida delle cifre. Vedere ["Copertura ampia del numero IMEI"](#) a pagina 1104.
- La copertura media rileva un numero a 15 cifre con il controllo di convalida Luhn ed esclusione caratteri iniziali. Vedere ["Copertura media numero IMEI"](#) a pagina 1105.
- La copertura limitata rileva un numero a 15 cifre con convalida del controllo Luhn e cifra duplicata. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata numero IMEI"](#) a pagina 1105.

Copertura ampia del numero IMEI

La copertura ampia rileva un numero di 15 cifre con la doppia convalida delle cifre.

Tabella 40-390 Criteri di copertura ampia del numero IMEI

Modelli
$\backslash d\{15\}$
$\backslash d\{2\}-\backslash d\{6\}-\backslash d\{6\}-\backslash d$

Tabella 40-391 Convalida di copertura ampia del numero IMEI

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero IMEI

La copertura media rileva un numero a 15 cifre con il controllo di convalida Luhn ed esclusione caratteri iniziali.

Tabella 40-392 Criteri copertura media numero IMEI

Modelli
$\backslash d\{15\}$
$\backslash d\{2\}-\backslash d\{6\}-\backslash d\{6\}-\backslash d$

Tabella 40-393 Convalida numero IMEI

Convalide obbligatorie	Descrizione
Controllo Luhn	Calcola il checksum Luhn e lo utilizza per convalidare il criterio.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Escludi caratteri iniziali	Consente di escludere i seguenti caratteri dall'inizio del numero: 0000000000000000

Copertura limitata numero IMEI

La copertura limitata rileva un numero a 15 cifre con convalida del controllo Luhn e cifra duplicata. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-394 Criteri copertura limitata numero IMEI

Modelli
\d{15}
\d{2}-\d{6}-\d{6}-\d{6}

Tabella 40-395 Convalida copertura limitata numero IMEI

Convalide obbligatorie	Descrizione
Controllo Luhn	Calcola il checksum Luhn e lo utilizza per convalidare il criterio.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: imei, IMEI, n. imei, n. IMEI, Numero IMEI, numero imei, Numero International Mobile Station Equipment Identity, International Mobile Station Equipment Identity

Codice ISIN (International Securities Identification Number)

Un codice ISIN (International Securities Identification Number) è una stringa alfanumerica di 12 caratteri che identifica in modo univoco i valori mobiliari, ovvero obbligazioni, titoli di credito, azioni e warrant.

L'identificatore di dati per il Codice ISIN (International Securities Identification Number) rileva una stringa alfanumerica di 12 caratteri che corrisponde al formato del Codice ISIN (International Securities Identification Number).

- La copertura ampia rileva una stringa alfanumerica di 12 caratteri senza la convalida del checksum. Vedere "[Copertura ampia codice ISIN \(International Securities Identification Number\)](#)" a pagina 1107.
- La copertura media rileva una stringa alfanumerica di 12 caratteri con la convalida del checksum.

Vedere ["Copertura media codice ISIN \(International Securities Identification Number\)"](#) a pagina 1107.

- La copertura limitata rileva una stringa alfanumerica di 12 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata Codice ISIN \(International Securities Identification Number\)"](#) a pagina 1108.

Copertura ampia codice ISIN (International Securities Identification Number)

La copertura ampia rileva una stringa alfanumerica di 12 caratteri senza la convalida del

Tabella 40-396 Criterio copertura ampia codice ISIN (International Securities Identification Number)

Criterio
<code>\l{2}\w{9}\d</code>
La copertura ampia del codice ISIN (International Securities Identification Number) non comprende convalide.

Copertura media codice ISIN (International Securities Identification Number)

La copertura media rileva una stringa alfanumerica di 12 caratteri con la convalida del checksum.

Tabella 40-397 Modello di copertura media Codice ISIN (International Securities Identification Number)

Criterio
<code>\l{2}\w{9}\d</code>
Tabella 40-398 Convalida copertura media codice ISIN (International Securities Identification Number)

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida codice ISIN	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata Codice ISIN (International Securities Identification Number)

La copertura limitata rileva una stringa alfanumerica di 12 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-399 Criterio copertura limitata codice ISIN

Criterio
\1{2}\w{9}\d

Tabella 40-400 Convalide copertura limitata codice ISIN (International Securities Identification Number)

Convalide obbligatorie	Descrizione
Controllo di convalida codice ISIN	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: isin, i.s.i.n, International Securities Identification Number, Standard & Poor's, S&P, National Numbering Association, NNA ID, ID, codice identificativo, cod. Id, codice fiscale internazionale, codici fiscali internazionali

Indirizzo IP

L'indirizzo IP è il codice di rete del computer utilizzato per identificare i dispositivi e semplificare le comunicazioni.

L'identificatore dell'indirizzo IP rileva gli indirizzi IPv4.

Questo identificatore di dati offre tre coperture di rilevazione:

- La copertura ampia rileva gli indirizzi IP e ne convalida il formato.
Vedere ["Copertura ampia indirizzo IP"](#) a pagina 1109.
- La copertura media rileva gli indirizzi IP, ne convalida il formato ed elimina gli indirizzi fittizi.
Vedere ["Copertura media indirizzo IP"](#) a pagina 1109.
- La copertura limitata rileva gli indirizzi IP, ne convalida il formato ed elimina gli indirizzi fittizi e non assegnati.
Vedere ["Copertura limitata dell'indirizzo IP"](#) a pagina 1110.

Copertura ampia indirizzo IP

La copertura ampia dell'identificatore dati dell'indirizzo IP rileva numeri nel formato DDD.DDD.DDD.DDD con /DD opzionale. Ogni gruppo di tre cifre deve essere compreso tra 0 e 255 inclusi e /DD deve essere compreso tra 0 e 32. Inoltre, 0.0.0.0 non è consentito.

Tabella 40-401 Modelli di copertura ampia dell'indirizzo IP

Criteri
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[0-9]$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[1-2][0-9]?$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[3][0-2]?$

Tabella 40-402 Strumento di convalida di copertura ampia dell'indirizzo IP

Strumento di convalida obbligatorio	Descrizione
Controllo di base IP	Ogni indirizzo IP deve avere il formato x.x.x.x e ogni numero deve essere inferiore a 256.

Copertura media indirizzo IP

La copertura media dell'identificatore di dati Indirizzo IP rileva numeri nel formato DDD.DDD.DDD.DDD con /DD opzionale. Ogni gruppo di tre cifre deve essere compreso tra 0 e 255 inclusi e /DD deve essere compreso tra 0 e 32. 0.0.0.0 non è consentito. Elimina inoltre come esempi fittizi comuni tutti i gruppi corrispondenti a 1 cifra, quali 1.1.1.2.

Tabella 40-403 Criteri copertura media indirizzo IP

Criteri
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[0-9]$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[1-2][0-9]?$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[3][0-2]?$

Tabella 40-404 Convalida copertura media indirizzo IP

Convalida obbligatoria	Descrizione
Verifica ottetti IP	Ogni indirizzo IP deve avere il formato x.x.x.x, deve essere composto da numeri inferiori a 256 e non deve includere numeri a una sola cifra (1.1.1.2).

Copertura limitata dell'indirizzo IP

La copertura limitata dell'identificatore di dati Indirizzo IP rileva numeri nel formato DDD.DDD.DDD.DDD con /DD opzionale. Ogni gruppo di tre cifre deve essere compreso tra 0 e 255 inclusi e /DD deve essere compreso tra 0 e 32. 0.0.0.0 non è consentito. Elimina inoltre come esempi fittizi comuni tutti i gruppi corrispondenti a 1 cifra, ad esempio 1.1.1.2, e gli indirizzi IP non assegnati ("Bogons").

Tabella 40-405 Modelli di copertura limitata dell'indirizzo IP

Criteri
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[0-9]$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[1-2][0-9]?$
$\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}.\backslash d\{1,3\}/[3][0-2]?$

Tabella 40-406 Convalide della copertura limitata dell'indirizzo IP

Convalide obbligatorie	Descrizione
Verifica ottetti IP	Ogni indirizzo IP deve avere il formato x.x.x.x, deve essere composto da numeri inferiori a 256 e non deve includere numeri a una sola cifra (1.1.1.2).
Controllo intervallo IP riservato	Verifica se l'indirizzo IP rientra in uno qualsiasi degli intervalli "Bogons". In caso affermativo la corrispondenza non è valida.

Indirizzo IPv6

La versione 6 di Internet Protocol (IPv6) è l'ultima versione dell'Internet Protocol (IP), ossia il protocollo di comunicazione che fornisce un sistema di identificazione e localizzazione per i computer sulle reti e dirige il traffico tramite Internet.

L'identificatore di dati dell'indirizzo Ipv6 rileva gli indirizzi IPv6.

Questo identificatore di dati offre tre coperture di rilevazione:

- La copertura ampia rileva gli indirizzi IPv6 e ne convalida il formato.

Vedere ["Copertura ampia dell'indirizzo IPv6"](#) a pagina 1111.

- La copertura media rileva gli indirizzi IPv6 e ne convalida il formato. Conferma inoltre che non comincino con il numero 0.

Vedere ["Copertura media indirizzo IPv6."](#) a pagina 1111.

- La copertura limitata rileva gli indirizzi IPv6 e ne convalida il formato. Conferma inoltre che non comincino con il numero 0. Le stringhe di indirizzo sono totalmente compresse, non normalizzate.

Vedere ["Copertura limitata dell'indirizzo IPv6"](#) a pagina 1112.

Copertura ampia dell'indirizzo IPv6

La copertura ampia rileva gli indirizzi IPv6 e conferma che corrispondano al formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

Tabella 40-407 Criteri di copertura ampia dell'indirizzo IPv6

Modelli
[0-9A-Fa-f:./%]{11,19}
[0-9A-Fa-f:./%]{2,10}
[0-9A-Fa-f:./%]{20,28}
[0-9A-Fa-f:./%]{29,37}
[0-9A-Fa-f:./%]{38,46}
[0-9A-Fa-f:./%]{47,48}

Tabella 40-408 Convalida di copertura ampia dell'indirizzo IPv6

Convalida	Descrizione
Controllo di convalida di base indirizzo IPv6	Controlla ciascun indirizzo IPv6 e verifica che corrisponda al formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

Copertura media indirizzo IPv6.

La copertura media rileva gli indirizzi IPv6 e conferma che corrispondano al formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. Conferma inoltre che non comincino con il numero 0.

Tabella 40-409 Criteri copertura media indirizzi IPv6

Modelli
[0-9A-Fa-f:./%]{11,19}
[0-9A-Fa-f:./%]{2,10}
[0-9A-Fa-f:./%]{20,28}
[0-9A-Fa-f:./%]{29,37}
[0-9A-Fa-f:./%]{38,46}
[0-9A-Fa-f:./%]{47,48}

Tabella 40-410 Convalida copertura media indirizzi IPv6

Convalida obbligatoria	Descrizione
Controllo di convalida medio indirizzo ipv6	Controlla ciascun indirizzo IPv6 e verifica che corrisponda al formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx: e che non cominci con il numero 0.

Copertura limitata dell'indirizzo IPv6

La copertura limitata rileva gli indirizzi IPv6 e conferma che corrispondano al formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx. Conferma inoltre che non comincino con il numero 0. Le stringhe di indirizzo sono totalmente compresse, non normalizzate.

Tabella 40-411 Criteri di copertura limitata dell'indirizzo IPv6

Modelli
[0-9A-Fa-f:./%]{11,19}
[0-9A-Fa-f:./%]{2,10}
[0-9A-Fa-f:./%]{20,28}
[0-9A-Fa-f:./%]{29,37}
[0-9A-Fa-f:./%]{38,46}
[0-9A-Fa-f:./%]{47,48}

Tabella 40-412 Convalida di copertura limitata dell'indirizzo IPv6

Convalida obbligatoria	Descrizione
Controllo di convalida riservato indirizzo IPv6	Controlla ciascun indirizzo IPv6 e verifica che corrisponda al formato xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx e che non cominci con il numero 0 e sia totalmente compresso.

Tabella 40-413 Normalizzatore di copertura limitata dell'indirizzo IPv6

Normalizzatore	Descrizione
Noop (Nessuna operazione)	La stringa è passata così com'è senza normalizzazione.

Numero di passaporto irlandese

Un passaporto irlandese è il passaporto rilasciato ai cittadini irlandesi. Un passaporto irlandese consente al portatore di viaggiare a livello internazionale e serve come prova della cittadinanza irlandese e della cittadinanza dell'Unione Europea. Facilita inoltre l'accesso all'assistenza consolare delle ambasciate irlandesi e di quelle di qualsiasi altro stato membro dell'Unione Europea all'estero.

L'identificatore di dati per il numero di passaporto irlandese rileva una stringa alfanumerica di sette o nove caratteri che corrisponde al formato del numero di passaporto irlandese.

L'identificatore di dati del numero di passaporto irlandese fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di sette o nove caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di passaporto irlandese"](#) a pagina 1113.
- La copertura limitata rileva un modello alfanumerico di sette o nove caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.
Vedere ["Copertura limitata del numero di passaporto irlandese"](#) a pagina 1114.

Copertura ampia del numero di passaporto irlandese

La copertura ampia rileva un modello alfanumerico di sette o nove caratteri senza la convalida del checksum.

Tabella 40-414 Modelli di copertura ampia del numero di passaporto irlandese

Modelli
[a-zA-Z]{2}\d{7}
[a-zA-Z]\d{6}

Modelli

[a-zA-Z]\d{8}

Tabella 40-415 Convalida di copertura ampia del numero di passaporto irlandese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di passaporto irlandese

La copertura limitata rileva un modello alfanumerico di sette o nove caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-416 Criteri di copertura limitata del numero di passaporto irlandese

Modelli

[a-zA-Z]{2}\d{7}

[a-zA-Z]\d{6}

[a-zA-Z]\d{8}

Tabella 40-417 Convalide di copertura limitata del numero di passaporto irlandese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>passport number, passport, passport no, pas, passeport, ireland passport, irelande passeport, Éire pas, no de passeport, pas uimh, uimhir pas, numéro de passeport</p>

Numero di identificazione fiscale irlandese

Il numero di identificazione fiscale irlandese è rilasciato dal dipartimento della protezione sociale per le persone fisiche e dal commissario per le entrate per le persone giuridiche. Le

persone giuridiche possono essere aziende, società di persone, trust ed enti non costituiti in società.

L'identificatore di dati del numero di identificazione fiscale irlandese rileva una stringa alfanumerica di 6-9 caratteri che corrisponde al formato del numero di identificazione fiscale irlandese.

Il numero di identificazione fiscale irlandese fornisce tre coperture di rilevamento::

- La copertura ampia rileva un modello alfanumerico di 6-9 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione fiscale irlandese"](#) a pagina 1115.
- La copertura media rileva un modello alfanumerico di 6-9 caratteri con la convalida del checksum.
Vedere ["Copertura media numero di identificazione fiscale irlandese"](#) a pagina 1116.
- La copertura limitata rileva un modello alfanumerico di 6-9 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di identificazione fiscale irlandese"](#) a pagina 1117.

Copertura ampia del numero di identificazione fiscale irlandese

La copertura ampia rileva un modello alfanumerico di 6-9 caratteri senza la convalida del checksum.

Tabella 40-418 Criteri copertura ampia numero di identificazione fiscale irlandese

Modelli
\d{7} [A-Wa-w]
\d{7} [A-Wa-w]
\d{3} \d{2} \d{2} [A-Wa-w]
\d{3} \d{2} \d{2} [A-Wa-w]
\d{7} [A-Wa-w] [A-Ia-iWw]
\d{7} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
[Cc] [Hh] [Yy] \d{3}

Modelli
[Cc] [Hh] [Yy] \d{3}
[Cc] [Hh] [Yy] \d{4}
[Cc] [Hh] [Yy] \d{4}
[Cc] [Hh] [Yy] \d{5}
[Cc] [Hh] [Yy] \d{5}

Tabella 40-419 Convalida copertura ampia numero di identificazione fiscale irlandese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media numero di identificazione fiscale irlandese

La copertura media rileva un modello alfanumerico di 6-9 caratteri con la convalida del checksum.

Tabella 40-420 Modelli di copertura media del numero di identificazione fiscale irlandese

Modelli
\d{7} [A-Wa-w]
\d{7} [A-Wa-w]
\d{3} \d{2} \d{2} [A-Wa-w]
\d{3} \d{2} \d{2} [A-Wa-w]
\d{7} [A-Wa-w] [A-Ia-iWw]
\d{7} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
[Cc] [Hh] [Yy] \d{3}
[Cc] [Hh] [Yy] \d{3}
[Cc] [Hh] [Yy] \d{4}

Modelli
[Cc] [Hh] [Yy] \d{4}
[Cc] [Hh] [Yy] \d{5}
[Cc] [Hh] [Yy] \d{5}

Tabella 40-421 Convalida di copertura media del numero di identificazione fiscale irlandese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione fiscale irlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione fiscale irlandese

La copertura limitata rileva un modello alfanumerico di 6-9 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-422 Modelli di copertura limitata del numero di identificazione fiscale irlandese

Modelli
\d{7} [A-Wa-w]
\d{7} [A-Wa-w]
\d{3} \d{2} \d{2} [A-Wa-w]
\d{3} \d{2} \d{2} [A-Wa-w]
\d{7} [A-Wa-w] [A-Ia-iWw]
\d{7} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
\d{3} \d{2} \d{2} [A-Wa-w] [A-Ia-iWw]
[Cc] [Hh] [Yy] \d{3}
[Cc] [Hh] [Yy] \d{3}
[Cc] [Hh] [Yy] \d{4}
[Cc] [Hh] [Yy] \d{4}

Modelli
[Cc] [Hh] [Yy] \d{5}
[Cc] [Hh] [Yy] \d{5}

Tabella 40-423 Convalide della copertura limitata del numero di identificazione fiscale irlandese

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Organizzazione benefica, numero organizzazione benefica, numero org. benefica, n. org. ben, num. org. ben., num org ben, NIF, n.NIF, numero di identificazione fiscale, numero di identificazione fiscale irlandese, identificazione fiscale irlandese, numero identificazione fiscale, id fiscale, idfisc, n. id fisc., codice fiscale, cod. fiscale, codfisc, TIN, n.TIN, tin irlandese, codice di identificazione fiscale, codice di identificazione fiscale, cod. id fiscale.</p> <p>uimhir carthanachta, Uimhir chláraithe charthanais, uimhir CHY, CHY uimh., uimhir thagartha cánach, uimhir aitheantais cánach ireland, aitheantais cánach irish, uimhir aitheantais cánach, id cánach, uimhir chánach, cáin #, STÁIN, cáin id uimh.</p>
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione fiscale irlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Numero di partita IVA irlandese

L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Per l'Irlanda, la partita IVA è emessa dall'autorità fiscale irlandese.

L'identificatore di dati del numero di partita IVA irlandese rileva un modello alfanumerico 9-11 cifre che corrisponde al formato del numero di partita IVA irlandese.

L'identificatore di dati della partita IVA irlandese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 9-11 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di partita IVA irlandese"](#) a pagina 1119.
- La copertura media rileva un modello alfanumerico di 9-11 caratteri con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA irlandese"](#) a pagina 1120.
- La copertura limitata rileva un modello alfanumerico di 9-11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di partita IVA irlandese"](#) a pagina 1120.

Copertura ampia del numero di partita IVA irlandese

La copertura ampia rileva un modello alfanumerico di 9-11 caratteri senza la convalida del checksum.

Tabella 40-424 Modelli di copertura ampia del numero di partita IVA irlandese

Modelli
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]

Tabella 40-425 Convalida di copertura ampia del numero di partita IVA irlandese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero di partita IVA irlandese

La copertura media rileva un modello alfanumerico di 9-11 caratteri con la convalida del checksum.

Tabella 40-426 Modelli di copertura media del numero di partita IVA irlandese

Modelli
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]

Tabella 40-427 Convalida di copertura media del numero di partita IVA irlandese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA irlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di partita IVA irlandese

La copertura limitata rileva un modello alfanumerico di 9-11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-428 Modelli di copertura limitata del numero di partita IVA irlandese

Modelli
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w]
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]

Modelli
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]
[Ii] [Ee] \d{7} [A-Wa-w] [HhAa]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]
[Ii] [Ee] [0-9] [A-Za-z+*] \d{5} [A-Wa-w]

Tabella 40-429 Convalide di copertura limitata del numero di partita IVA irlandese

Convalide obbligatorie	Descrizione
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero di partita iva irlandese, numero partita iva, n. partita iva, n. IVA, IVA, numero imposta valore aggiunto, imposta valore aggiunto, iva irlandese cáin bhreisluacha, CBL, CBL aon, Uimhir CBL, Uimhir CBL hÉireann, bhreisluacha uimhir chánach
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di partita IVA irlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Numero personale di servizio pubblico irlandese

Il formato del numero è una stringa alfanumerica univoco di otto caratteri che termina con una lettera, ad esempio 8765432A. Viene assegnato alla registrazione del neonato, è indicato sulla carta dei servizi sociali ed è univoco.

Il Numero personale di servizio pubblico irlandese rileva una stringa alfanumerica di otto caratteri che corrisponde al formato del Numero personale di servizio pubblico irlandese.

L'identificatore di dati del numero personale di servizio pubblico irlandese fornisce tre coperture di rilevamento:

- La copertura ampia individua una stringa alfanumerica di otto caratteri che termina con una lettera senza convalida del checksum.
Vedere "[Copertura ampia del numero personale di servizio pubblico irlandese \(PPS\)](#)" a pagina 1122.

- La copertura media individua una stringa alfanumerica di otto caratteri che termina con una lettera e con convalida del checksum.
Vedere "[Copertura media del numero personale di servizio pubblico irlandese \(PPS\)](#)" a pagina 1122.
- La copertura limitata rileva una stringa alfanumerica di otto caratteri che termina con una lettera e che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero personale di servizio pubblico irlandese \(PPS\)](#)" a pagina 1123.

Copertura ampia del numero personale di servizio pubblico irlandese (PPS)

La copertura ampia individua una stringa alfanumerica di otto caratteri che termina con una lettera senza convalida del checksum.

Tabella 40-430 Criterio di copertura ampia del numero personale di servizio pubblico irlandese (PPS)

Criterio
<code>\d{7}[a-zA-W]</code>

Tabella 40-431 Convalida di copertura ampia del numero personale di servizio pubblico irlandese (PPS)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero personale di servizio pubblico irlandese (PPS)

La copertura media individua una stringa alfanumerica di otto caratteri che termina con una lettera e con convalida del checksum.

Tabella 40-432 Criterio di copertura media del numero personale di servizio pubblico irlandese (PPS)

Criterio
<code>\d{7}[a-zA-W]</code>

Tabella 40-433 Convalida di copertura media del numero personale di servizio pubblico irlandese (PPS)

Convalida obbligatoria	Descrizione
Controllo di convalida del Numero personale di servizio pubblico irlandese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero personale di servizio pubblico irlandese (PPS)

La copertura limitata rileva una stringa alfanumerica di otto caratteri che termina con una lettera e con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-434 Criterio copertura limitata numero personale di servizio pubblico irlandese (PPS)

Criterio
<code>\d{7}[a-zA-W]</code>

Tabella 40-435 Strumenti di convalida copertura limitata numero personale di servizio pubblico irlandese (PPS)

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida Personal Public Service Number (numero personale di servizio pubblico) irlandese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>n. servizio pubblico, num personale servizio pubblico, n. pps, n. PPS, n. servizio personale, n. servizio PPS, ppsno#, n. PPS irlandese, n. pps irlandese, PPSNO#, publicserviceno#, numero servizio pubblico personale uimhir phearsanta seirbhíse poiblí, pps uimh, Uimhir aitheantais phearsanta</p>

Numero di identificazione personale israeliano

Il Numero di identificazione personale israeliano è un numero di nove cifre rilasciato a tutti i cittadini israeliani alla nascita dal Ministero dell'Interno. Il numero di identificazione personale viene inoltre rilasciato a tutti i residenti di età superiore ai 16 anni in possesso della residenza temporanea o permanente.

L'identificatore di dati Numero di identificazione personale israeliano rileva un numero di nove cifre che corrisponde al formato del Numero di identificazione personale israeliano.

L'identificatore di dati Numero di identificazione personale israeliano fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.
Vedere ["Copertura ampia del Numero di identificazione personale israeliano"](#) a pagina 1124.
- La copertura media rileva un numero di nove cifre con la convalida del checksum.
Vedere ["Copertura media del Numero di identificazione personale israeliano"](#) a pagina 1124.
- La copertura limitata rileva un numero a nove cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata Numero di identificazione personale israeliano"](#) a pagina 1125.

Copertura ampia del Numero di identificazione personale israeliano

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-436 Criterio copertura ampia Numero di identificazione personale israeliano

Criterio
$\backslash d\{9\}$

Tabella 40-437 Convalida di copertura ampia del Numero di identificazione personale israeliano

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del Numero di identificazione personale israeliano

La copertura media rileva un numero di nove cifre con la convalida del checksum.

Tabella 40-438 Modello di copertura media del Numero di identificazione personale israeliano

Criterio
\d{9}

Tabella 40-439 Convalide di copertura media del Numero di identificazione personale israeliano

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione personale israeliano	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata Numero di identificazione personale israeliano

La copertura limitata rileva un numero a nove cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-440 Criterio copertura limitata Numero di identificazione personale israeliano

Criterio
\d{9}

Tabella 40-441 Convalide copertura limitata Numero di identificazione personale israeliano

Convalide obbligatorie	Descrizione
Controllo di convalida numero di identificazione personale israeliano	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di identità, n.ID, numerodiidentitàisraeliano, n.identità, num. identità, numero di identità israeliano, ID personale univoco, ID personale, ID univoco, numero di identità univoco</p> <p>מספר זיהוי, מספר זיהוי ישראל, זהות ישראלית, הויה ישראלית عدد, هوية إسرائيل, يلية, رقم الهوية, عدد هوية فريدة من نوعها</p>

Numero di patente di guida italiana

Il numero di patente di guida italiana è l'identificatore per la patente di guida individuale rilasciata dall'autorità preposta in Italia.

L'identificatore di dati del numero di patente di guida italiana rileva un modello alfanumerico di 10 caratteri che corrisponde al formato del numero di patente di guida italiana.

L'identificatore di dati del numero di patente di guida italiana offre due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 10 caratteri senza la convalida del checksum.
Vedere "[Copertura ampia del numero di patente di guida italiana](#)" a pagina 1126.
- La copertura limitata rileva un modello alfanumerico di 10 caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di patente di guida italiana](#)" a pagina 1127.

Copertura ampia del numero di patente di guida italiana

La copertura ampia rileva un modello alfanumerico di 10 caratteri senza la convalida del checksum.

Tabella 40-442 Modello di copertura ampia del numero di patente di guida italiana

Criterio
$[A-Za-z][A-Za-z]\{d{7}\}[A-Za-Z]$

Tabella 40-443 Convalida della copertura ampia del numero di patente di guida italiana

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di patente di guida italiana

La copertura limitata rileva un modello alfanumerico di 10 caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-444 Modelli di copertura limitata del numero di patente di guida italiana

Criterio
[A-Za-z] [A-Za-z] \d{7} [A-Za-Z]

Tabella 40-445 Convalide della copertura limitata del numero di patente di guida italiana

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>drivers licence number, drivers license number, driving licence number, driving license number, drivers license, driving licence, driving license</p> <p>patente guida numero, patente di guida numero, patente di guida, patente guida</p> <p>Driver's License, Driver's License Number, driver's license number, Driver's Licence Number</p>

Numero di previdenza sociale italiano

La tessera sanitaria italiana è rilasciata a tutti i cittadini italiani dal Ministero italiano dell'Economia e della Finanza, in collaborazione con l'agenzia italiana delle entrate. L'obiettivo della tessera è quello di migliorare i servizi di previdenza sociale tramite il controllo delle spese e delle prestazioni, e di ottimizzare l'utilizzo dei servizi sanitari per i cittadini.

L'identificatore di dati del numero di previdenza sociale italiano rileva un modello alfanumerico di 16 caratteri che corrisponde al formato del numero di previdenza sociale italiano.

L'identificatore di dati del numero di previdenza sociale italiano fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 16 caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura ampia del numero di previdenza sociale italiano"](#) a pagina 1128.
- La copertura ampia rileva un modello alfanumerico di 16 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di previdenza sociale italiano"](#) a pagina 1128.

Copertura ampia del numero di previdenza sociale italiano

La copertura ampia rileva un modello alfanumerico di 16 caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-446 Modello di copertura ampia del numero di previdenza sociale italiano

Modello
[A-Z] { 6 } [0-9LMNPQRSTUVWXYZ] { 2 } [ABCDEHLMPRST] [0-9LMNPQRSTUVWXYZ]
{ 2 } [A-Z] [0-9LMNPQRSTUVWXYZ] { 3 } [A-Z]
[A-Z] { 3 } [A-Z] { 3 } [0-9LMNPQRSTUVWXYZ] { 2 } [ABCDEHLMPRST]
[0-9LMNPQRSTUVWXYZ] { 2 } [A-Z] [0-9LMNPQRSTUVWXYZ] { 3 } [A-Z]

Tabella 40-447 Convalide di copertura ampia del numero di previdenza sociale italiano

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti quando si utilizza questa opzione. TESSERA SANITARIA, tessera sanitaria, tessera sanitaria italiana, Health Insurance Card, Italian health insurance card, health insurance card, EHIC, health card, ehic, Health Card

Copertura limitata del numero di previdenza sociale italiano

La copertura ampia rileva un modello alfanumerico di 16 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-448 Modelli di copertura limitata del numero di previdenza sociale italiano

Modello
[A-Z] { 6 } [0-9LMNPQRSTUVWXYZ] { 2 } [ABCDEHLMPRST] [0-9LMNPQRSTUVWXYZ]
{ 2 } [A-Z] [0-9LMNPQRSTUVWXYZ] { 3 } [A-Z]
[A-Z] { 3 } [A-Z] { 3 } [0-9LMNPQRSTUVWXYZ] { 2 } [ABCDEHLMPRST]
[0-9LMNPQRSTUVWXYZ] { 2 } [A-Z] [0-9LMNPQRSTUVWXYZ] { 3 } [A-Z]

Tabella 40-449 Convalide di copertura limitata del numero di previdenza sociale italiano

Strumento di convalida obbligatorio	Descrizione
Verifica chiave di controllo codice fiscale	Calcola la chiave di controllo e ne verifica la validità.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	<p>Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti quando si utilizza questa opzione.</p> <p>TESSERA SANITARIA, tessera sanitaria, tessera sanitaria italiana, Health Insurance Card, Italian health insurance card, health insurance card, EHIC, health card, ehic, Health Card</p>

Numero di passaporto italiano

Il passaporto italiano viene rilasciato ai cittadini italiani per viaggiare all'estero.

L'identificatore di dati del numero di passaporto italiano rileva un modello alfanumerico di nove caratteri che corrisponde al formato del numero di passaporto italiano.

L'identificatore di dati del numero di passaporto italiano fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di nove caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di passaporto italiano"](#) a pagina 1130.
- La copertura limitata rileva un modello alfanumerico di nove caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di passaporto italiano"](#) a pagina 1130.

Copertura ampia del numero di passaporto italiano

La copertura ampia rileva un modello alfanumerico di nove caratteri senza la convalida del checksum.

Tabella 40-450 Modello di copertura ampia del numero di passaporto italiano

Modello
\l{2}\d{7}

Tabella 40-451 Convalida di copertura ampia del numero di passaporto italiano

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata del numero di passaporto italiano

La copertura limitata rileva un modello alfanumerico di nove caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-452 Modelli di copertura limitata del numero di passaporto italiano

Modello
\l{2}\d{7}

Tabella 40-453 Convalide di copertura limitata del numero di passaporto italiano

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Repubblica Italiana Passaporto, Passaporto, Passaporto Italiana, passport number, Italiana Passaporto numero, Passaporto numero, Numéro passeport italien, numéro passeport, Italian passport number</p>

Numero di partita IVA italiano

L'imposta sul valore aggiunto (IVA) è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Italia, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.

L'identificatore di dati del numero di partita IVA italiano rileva un modello alfanumerico di 13 caratteri che corrisponde al formato del numero di partita IVA italiano.

L'identificatore di dati della partita IVA italiana fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 13 caratteri preceduto da `IT` senza la convalida del checksum.
Vedere ["Copertura ampia numero di partita IVA italiana"](#) a pagina 1131.
- La copertura media rileva un modello alfanumerico di 13 caratteri preceduto da `IT` con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA italiana"](#) a pagina 1132.
- La copertura limitata rileva un modello alfanumerico di 13 caratteri preceduto da `IT` con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di partita IVA italiana"](#) a pagina 1132.

Copertura ampia numero di partita IVA italiana

La copertura ampia rileva un modello alfanumerico di 13 caratteri preceduto da `IT` senza la convalida del checksum.

Tabella 40-454 Modello di copertura ampia numero di partita IVA italiana

Modello
[Ii] [Tt] \d{11}
[Ii] [Tt] \d{11}
[Ii] [Tt] .\d{11}
[Ii] [Tt] -\d{11}
[Ii] [Tt] ,\d{11}

Tabella 40-455 Convalida di copertura ampia numero di partita IVA italiana

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura media del numero di partita IVA italiana

La copertura media rileva un modello alfanumerico di 13 caratteri preceduto da **IT** con la convalida del checksum.

Tabella 40-456 Modelli di copertura media del numero di partita IVA italiana

[Ii] [Tt] \d{11}
[Ii] [Tt] \d{11}
[Ii] [Tt] .\d{11}
[Ii] [Tt] -\d{11}
[Ii] [Tt] ,\d{11}

Tabella 40-457 Convalida di copertura media del numero di partita IVA italiana

Controllo di convalida numero di partita IVA italiano	Convalida checksum per il numero di partita IVA italiana.

Copertura limitata numero di partita IVA italiana

La copertura limitata rileva un modello alfanumerico di 13 caratteri preceduto da **IT** con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-458 Modelli copertura limitata numero di partita IVA italiana

Modello
[Ii] [Tt] \d{11}
[Ii] [Tt] \d{11}
[Ii] [Tt] .\d{11}
[Ii] [Tt] -\d{11}
[Ii] [Tt] ,\d{11}

Tabella 40-459 Convalide di copertura limitata numero di partita IVA italiana

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo di convalida numero di partita IVA italiano	Convalida checksum per il numero di partita IVA italiana.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>VAT Number, vat no, VAT#, IVA, numero partita IVA, IVA#, numero IVA</p>

Numero di patente di guida giapponese

In Giappone, la patente di guida è necessaria quando si conduce un'auto, un motociclo o un ciclomotore su strade pubbliche. Le patenti di guida sono emesse dalle commissioni di sicurezza pubblica delle prefetture e sono supervisionate su base nazionale dall'ente nazionale di polizia.

L'identificatore di dati del numero di patente di guida giapponese rileva un numero di 12 cifre che corrisponde al formato del numero di patente di guida giapponese.

L'identificatore di dati del numero di patente di guida giapponese fornisce tre coperture di rilevamento::

- La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di patente di guida giapponese"](#) a pagina 1133.
- La copertura media rileva un numero di 12 cifre con la convalida del checksum. Vedere ["Copertura media del numero di patente di guida giapponese"](#) a pagina 1134.
- La copertura limitata rileva un numero a 12 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata del numero di patente di guida giapponese"](#) a pagina 1134.

Copertura ampia del numero di patente di guida giapponese

La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum.

Tabella 40-460 Modello di copertura ampia del numero di patente di guida giapponese

Criterio
\d{12}

Tabella 40-461 Convalida del numero di patente di guida giapponese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di patente di guida giapponese

La copertura media rileva un numero di 12 cifre con la convalida del checksum.

Tabella 40-462 Modello di copertura media del numero di patente di guida giapponese

Criterio
$\backslash d\{12\}$

Tabella 40-463 Convalida di copertura media del numero di patente di guida giapponese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di patente di guida giapponese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di patente di guida giapponese

La copertura limitata rileva un numero a 12 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-464 Modello di copertura limitata del numero di patente di guida giapponese

Criterio
$\backslash d\{12\}$

Tabella 40-465 Convalide di copertura limitata del numero di patente di guida giapponese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di patente di guida giapponese	Calcola il checksum e lo utilizza per convalidare il modello.

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>公安委員会,番号,免許,交付,運転免許,運転免許証,ドライバライセンス,ドライバズライセンス,ライセンス,運転免許証番号</p> <p>patente di guida, patente guida, numero di patente, numero patente di guida, patente</p>

Numero di passaporto giapponese

I numeri di passaporto giapponese vengono rilasciati ai cittadini giapponesi per i viaggi internazionali

Il Numero di passaporto giapponese rileva un criterio valido per il numero di passaporto giapponese.

L'identificatore di dati del numero di passaporto giapponese fornisce due coperture di rilevamento:

- La copertura ampia rileva un criterio valido del numero di passaporto giapponese. Vedere ["Copertura ampia Numero di passaporto giapponese"](#) a pagina 1135.
- La copertura limitata rileva un criterio valido del numero di passaporto giapponese. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata Numero di passaporto giapponese"](#) a pagina 1136.

Copertura ampia Numero di passaporto giapponese

La copertura ampia rileva un criterio valido del numero di passaporto giapponese.

Tabella 40-466 Criteri copertura ampia Numero di passaporto giapponese

Criteri
$\backslash 1\{2\}\backslash d\{3\}\backslash 1\backslash d\{2\}\backslash 1\backslash d$
$\backslash 1\{2\}\backslash d\{4\}\backslash 1\backslash d\backslash 1\backslash d$
$\backslash 1\backslash d\{4\}\backslash 1\backslash d\{2\}\backslash 1\backslash d$

Criteri
$\backslash 1 \backslash d\{4\} \backslash 1 \backslash d\{2\} \backslash 1\{2\} \backslash d$
$\backslash 1\{2\} \backslash d\{3\} \backslash 1 \backslash d\{2\} \backslash 1\{2\} \backslash d$
$\backslash 1\{2\} \backslash d\{8\}$
$\backslash 1\{2\} \backslash d\{7\}$
$\backslash 1 \backslash d\{8\}$

Tabella 40-467 Convalida di copertura ampia Numero di passaporto giapponese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata Numero di passaporto giapponese

La copertura limitata rileva un criterio valido del numero di passaporto giapponese. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-468 Criteri copertura limitata Numero di passaporto giapponese

Criteri
$\backslash 1\{2\} \backslash d\{3\} \backslash 1 \backslash d\{2\} \backslash 1 \backslash d$
$\backslash 1\{2\} \backslash d\{4\} \backslash 1 \backslash d \backslash 1 \backslash d$
$\backslash 1 \backslash d\{4\} \backslash 1 \backslash d\{2\} \backslash 1 \backslash d$
$\backslash 1 \backslash d\{4\} \backslash 1 \backslash d\{2\} \backslash 1\{2\} \backslash d$
$\backslash 1\{2\} \backslash d\{3\} \backslash 1 \backslash d\{2\} \backslash 1\{2\} \backslash d$
$\backslash 1\{2\} \backslash d\{8\}$
$\backslash 1\{2\} \backslash d\{7\}$
$\backslash 1 \backslash d\{8\}$

Tabella 40-469 Convalide copertura limitata Numero di passaporto giapponese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: 日本国旅券, パスポート, パスポート数, passaporto , Passaporto , PASSAPORTO GIAPPONESE , Passaporto giapponese , passaporto giapponese , Libretto passaporto , libretto passaporto

Numero di identificazione giapponese (Juki Net)

Il numero di identificazione Juki Net è un numero univoco assegnato ai giapponesi e agli stranieri residenti in Giappone utilizzato come strumento di identificazione.

Il numero di identificazione giapponese (Juki-Net) rileva un numero di 11 caratteri che corrisponde al formato del Numero di identificazione giapponese (Juki-Net).

L'identificatore di dati di sistema del numero di identificazione giapponese (Juki Net) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.
Vedere "[Copertura ampia numero di identificazione giapponese \(Juki Net\)](#)" a pagina 1137.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum.
Vedere "[Copertura media numero di identificazione giapponese \(Juki Net\)](#)" a pagina 1138.
- La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero di identificazione giapponese \(Juki Net\)](#)" a pagina 1138.

Copertura ampia numero di identificazione giapponese (Juki Net)

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-470 Criterio di copertura ampia numero di identificazione giapponese (Juki Net)

Criterio
\d{11}

Tabella 40-471 Convalida copertura ampia numero di identificazione giapponese (Juki Net)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione giapponese (Juki Net)

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-472 Criterio copertura media numero di identificazione giapponese (Juki Net)

Criterio
$\backslash d\{11\}$

Tabella 40-473 Strumento di convalida copertura media numero di identificazione giapponese (Juki Net)

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione giapponese (Juki-Net)	Lo strumento di convalida calcola il checksum che ogni numero di identificazione giapponese deve superare.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata numero di identificazione giapponese (Juki Net)

La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum.
 Richiede inoltre la presenza di parole chiave associate.

Tabella 40-474 Criterio di copertura limitata numero di identificazione giapponese (Juki Net)

Criterio
$\backslash d\{11\}$

Tabella 40-475 Convalide di copertura limitata numero di identificazione giapponese (Juki-Net)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione giapponese (Juki-Net)	Lo strumento di convalida calcola il checksum che ogni numero di identificazione giapponese deve superare.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero identificazione juki net, numero juki net, numero identificazione, N. Juki Net, numero identificazione personale jukinet, n. juki net, numerojukinet, ID jukinet univoco</p> <p>住基ネット識別番号, 住基ネット番号, 識別番号, 個人識別番号, ID番号, ユニークID番号</p>

Numero di identificazione personale giapponese - Aziendale

Il numero di identificazione personale giapponese - Aziendale è un identificatore unico relativo alle aziende giapponesi utilizzato per la gestione del pagamento delle tasse, della previdenza sociale e degli interventi di risposta a eventi catastrofici.

L'identificatore di dati Numero di identificazione personale giapponese - Aziendale rileva un numero 13 cifre che corrisponde al formato del Numero di identificazione personale giapponese - Aziendale.

L'identificatore di dati Numero di identificazione personale giapponese-Aziendale fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre con la convalida del checksum.
Vedere "[Copertura ampia numero di identificazione personale giapponese - Aziendale](#)" a pagina 1139.
- La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero di identificazione personale giapponese - Aziendale](#)" a pagina 1140.

Copertura ampia numero di identificazione personale giapponese - Aziendale

La copertura ampia rileva un numero di 13 cifre con la convalida del checksum.

Tabella 40-476 Criterio copertura ampia numero di identificazione personale giapponese - Aziendale

Criterio
\d{13}

Tabella 40-477 Convalide copertura ampia numero di identificazione personale giapponese - Aziendale

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione personale giapponese (My Number)	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata numero di identificazione personale giapponese - Aziendale

La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di una parola chiave relativa al numero di identificazione personale giapponese.

Tabella 40-478 Criterio copertura limitata numero di identificazione personale giapponese - Aziendale

Criterio
\d{13}

Tabella 40-479 Strumenti di convalida copertura limitata numero di identificazione personale giapponese - Aziendale

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione personale giapponese (My Number)	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri iniziali	Consente di escludere i seguenti caratteri dalla fine del numero: 000000000000

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>マイナンバー, 共通番号</p>

Numero di identificazione personale giapponese - Personale

Il numero di identificazione personale giapponese - Personale è un identificatore unico relativo ai cittadini e residenti giapponesi utilizzato per la gestione del pagamento delle tasse, della previdenza sociale e degli interventi di risposta a eventi catastrofici.

L'identificatore di dati Numero di identificazione personale giapponese-Personale rileva un numero di 12 cifre che corrisponde al formato del Numero di identificazione personale giapponese-Personale.

- La copertura ampia rileva un numero di 12 cifre con la convalida del checksum. Vedere "[Copertura ampia del numero di identificazione personale giapponese - Personale](#)" a pagina 1141.
- La copertura media rileva un numero di 12 cifre con la convalida del checksum. Vedere "[Copertura media del numero di identificazione personale giapponese - Personale](#)" a pagina 1142.
- La copertura limitata rileva un numero a 12 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata del numero di identificazione personale giapponese - Personale](#)" a pagina 1142.

Copertura ampia del numero di identificazione personale giapponese - Personale

La copertura ampia rileva un numero di 12 cifre con la convalida del checksum.

Tabella 40-480 Criterio di copertura ampia del numero di identificazione personale giapponese - Personale

Criterio
\d{12}

Tabella 40-481 Convalide della copertura ampia del numero di identificazione personale giapponese - Personale

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione personale giapponese (My Number)	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri iniziali	Consente di escludere i seguenti caratteri dalla fine del numero: 000000000000

Copertura media del numero di identificazione personale giapponese - Personale

La copertura media rileva un numero di 12 cifre con la convalida del checksum.

Tabella 40-482 Criteri di copertura media del numero di identificazione personale giapponese - Personale

Criterio
$\backslash d\{12\}$
$\backslash d\{4\} \backslash d\{4\} \backslash d\{4\}$
$\backslash d\{4\}-\backslash d\{4\}-\backslash d\{4\}$
$\backslash d\{4\}.\backslash d\{4\}.\backslash d\{4\}$

Tabella 40-483 Convalide di copertura media del numero di identificazione personale giapponese - Personale

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione personale giapponese (My Number)	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri iniziali	Consente di escludere i seguenti caratteri dalla fine del numero: 000000000000

Copertura limitata del numero di identificazione personale giapponese - Personale

La copertura limitata rileva un numero a 12 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-484 Criteri di copertura limitata del numero di identificazione personale giapponese
 - Personale

Criterio
\d{12}
\d{4} \d{4} \d{4}
\d{4}-\d{4}-\d{4}
\d{4}.\d{4}.\d{4}

Tabella 40-485 Convalide di copertura limitata del numero di identificazione personale giapponese - Personale

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione personale giapponese (My Number)	Calcola il checksum e lo utilizza per convalidare il modello.
Escludi caratteri iniziali	Consente di escludere i seguenti caratteri dalla fine del numero: 000000000000
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: マイナンバー, 個人番号, 共通番号

Numero di passaporto coreano

I passaporti coreani sono rilasciati ai cittadini coreani per consentire i viaggi internazionali.

L'identificatore di dati per il Numero di passaporto coreano rileva un valore valido come Numero di passaporto coreano.

L'identificatore di dati del numero di passaporto coreano fornisce due coperture di rilevamento:

- La copertura ampia rileva un criterio valido del numero di passaporto coreano.
 Vedere ["Copertura ampia Numero di passaporto coreano"](#) a pagina 1144.
- La copertura limitata rileva un criterio valido del numero di passaporto coreano. Richiede inoltre la presenza di parole chiave associate.
 Vedere ["Copertura limitata Numero di passaporto coreano"](#) a pagina 1144.

Copertura ampia Numero di passaporto coreano

La copertura ampia rileva un criterio valido del numero di passaporto coreano.

Tabella 40-486 Criteri copertura ampia Numero di passaporto coreano

Criteri
$\backslash 1\{2\}\backslash d\{7\}$
$\backslash 1\backslash d\{8\}$
$\backslash d\{9\}$

Tabella 40-487 Convalida di copertura ampia Numero di passaporto coreano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata Numero di passaporto coreano

La copertura limitata rileva un criterio valido del numero di passaporto coreano. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-488 Criteri copertura limitata Numero di passaporto coreano

Criteri
$\backslash 1\{2\}\backslash d\{7\}$
$\backslash 1\backslash d\{8\}$
$\backslash d\{9\}$

Tabella 40-489 Convalide copertura limitata Numero di passaporto coreano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>한국어 여권, 여권, 여권 번호, 조선 민주주의 인민 공화국, 대한민국</p> <p>passaporto, passaporto, coreano, passaporto coreano, Corea passaporto, libretto passaporto Corea del Sud, Repubblica di Corea</p>

Numero di registrazione anagrafica coreano per stranieri.

Il numero di registrazione anagrafica per stranieri è un numero di 13 cifre rilasciato a tutti i residenti stranieri della Repubblica di Corea. È usato per identificare i soggetti che intervengono nelle transazioni private relative, ad esempio, ad attività bancarie o rapporti di lavoro e a scopo di identificazione online.

L'identificatore di dati per il Numero di registrazione anagrafica coreano per stranieri rileva un numero di 13 cifre che corrisponde al formato del Numero di registrazione anagrafica coreano per stranieri.

L'identificatore di dati Numero di registrazione anagrafica coreano per stranieri fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.
Vedere ["Copertura ampia Numero di registrazione anagrafica coreano per stranieri"](#) a pagina 1146.
- La copertura media rileva un numero a 13 cifre con la convalida del checksum.
Vedere ["Copertura media Numero di registrazione anagrafica coreano per stranieri"](#) a pagina 1146.
- La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata Numero di registrazione anagrafica coreano per stranieri"](#) a pagina 1147.

Copertura ampia Numero di registrazione anagrafica coreano per stranieri

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-490 Criteri di copertura ampia Numero di registrazione anagrafica coreano per stranieri

Criteri
\d{2}[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d{8}
\d\d[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d[]\d{7}

Tabella 40-491 Convalide di copertura ampia Numero di registrazione anagrafica coreano per stranieri

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media Numero di registrazione anagrafica coreano per stranieri

La copertura media rileva un numero a 13 cifre con la convalida del checksum.

Tabella 40-492 Criteri di copertura media Numero di registrazione anagrafica coreano per stranieri

Criteri
\d{2}[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d{8}
\d\d[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d[]\d{7}

Tabella 40-493 Convalide di copertura media Numero di registrazione anagrafica coreano per stranieri

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida KRRN per stranieri	Convalida che la terza e la quarta cifra rappresentino un mese valido e che la quinta e la sesta cifra rappresentino un giorno valido. Convalida il checksum del criterio.

Copertura limitata Numero di registrazione anagrafica coreano per stranieri

La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-494 Criteri di copertura limitata Numero di registrazione anagrafica coreano per stranieri

Criteri
\d{2}[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d{8}
\d\d[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d[]\d{7}

Tabella 40-495 Convalide di copertura limitata Numero di registrazione anagrafica coreano per stranieri

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida KRRN per stranieri	Convalida che la terza e la quarta cifra rappresentino un mese valido e che la quinta e la sesta cifra rappresentino un giorno valido. Convalida il checksum del criterio.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>외국인 등록 번호, 주민번호, Numero di registrazione per stranieri, Numero per i residenti stranieri</p>

Numero di registrazione anagrafica coreano per coreani

Il Resident Registration Number è un numero di 13 cifre rilasciato a tutti i residenti della Repubblica di Corea. Analogo ai numeri di identificazione nazionale rilasciati da altri paesi, il numero RRN consente di identificare i soggetti che intervengono nelle transazioni private relative, ad esempio, ad attività bancarie o rapporti di lavoro. È inoltre ampiamente utilizzato a scopo di identificazione degli utenti che effettuano transazioni online.

L'identificatore dati per il Numero di registrazione anagrafica coreano per cittadini coreani rileva un numero 13 cifre che corrisponde al formato del numero di registrazione anagrafica.

L'identificatore di dati Numero di registrazione anagrafica coreano per coreani fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum. Vedere ["Copertura ampia Numero di registrazione anagrafica coreano per coreani"](#) a pagina 1148.
- La copertura media rileva un numero a 13 cifre con la convalida del checksum. Vedere ["Copertura media Numero di registrazione anagrafica coreano per coreani"](#) a pagina 1149.
- La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata Numero di registrazione anagrafica coreano per coreani"](#) a pagina 1150.

Copertura ampia Numero di registrazione anagrafica coreano per coreani

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-496 Criteri di copertura ampia Numero di registrazione anagrafica coreano per coreani

Criteri
\d{2}[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d{8}
\d\d[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d[]\d{7}

Tabella 40-497 Convalida di copertura ampia Numero di registrazione anagrafica coreano per coreani

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media Numero di registrazione anagrafica coreano per coreani

La copertura media rileva un numero a 13 cifre con la convalida del checksum.

Tabella 40-498 Criteri di copertura media Numero di registrazione anagrafica coreano per coreani

Criteri
\d{2}[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d{8}
\d\d[01]\d[0123]\d-\d{7}
\d{2}[01]\d[0123]\d[]\d{7}

Tabella 40-499 Convalide di copertura media Numero di registrazione anagrafica coreano per coreani

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalida obbligatoria	Descrizione
Convalida KRRN avanzata	Convalida che la terza e la quarta cifra rappresentino un mese valido e che la quinta e la sesta cifra rappresentino un giorno valido. Convalida il checksum del criterio.

Copertura limitata Numero di registrazione anagrafica coreano per coreani

La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-500 Criteri di copertura limitata Numero di registrazione anagrafica coreano per coreani

Modelli
<code>\d{2}[01]\d[0123]\d-\d{7}</code>
<code>\d{2}[01]\d[0123]\d{8}</code>
<code>\d\d[01]\d[0123]\d-\d{7}</code>
<code>\d{2}[01]\d[0123]\d[]\d{7}</code>

Tabella 40-501 Convalide di copertura limitata Numero di registrazione anagrafica coreano per coreani

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Convalida KRRN avanzata	Convalida che la terza e la quarta cifra rappresentino un mese valido e che la quinta e la sesta cifra rappresentino un giorno valido. Convalida il checksum del criterio.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>주민등록번호, 주민번호</p> <p>Numero di registrazione residente, numero residente</p>

Numero di identificazione personale lettone

Il numero di identificazione personale lettone viene utilizzato come numero di identificazione nazionale e codice fiscale per scopi finanziari. Viene emesso dall'ufficio per la cittadinanza e la migrazione del Ministero degli Interni.

L'identificatore di dati per il numero di identificazione personale lettone rileva un numero di 11 cifre che corrisponde al formato del numero di identificazione personale lettone.

Il numero di identificazione personale lettone fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.
Vedere "[Copertura ampia del numero di identificazione personale lettone](#)" a pagina 1151.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum.
Vedere "[Copertura media del numero di identificazione personale lettone](#)" a pagina 1151.
- La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di identificazione personale lettone](#)" a pagina 1152.

Copertura ampia del numero di identificazione personale lettone

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-502 Modelli di copertura ampia del numero di identificazione personale lettone

Modelli
$\backslash d\{2\}[01]\backslash d\{3\}-[012]\backslash d\{4\}$
$\backslash d\{2\}[01]\backslash d\{3\}[012]\backslash d\{4\}$
$32\backslash d\{9\}$

Tabella 40-503 Convalide di copertura ampia del numero di identificazione personale lettone

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione personale lettone

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-504 Modelli di copertura media del numero di identificazione personale lettone

Modelli
$\backslash d\{2\} [01] \backslash d\{3\} - [012] \backslash d\{4\}$
$\backslash d\{2\} [01] \backslash d\{3\} [012] \backslash d\{4\}$
$32 \backslash d\{9\}$

Tabella 40-505 Convalida di copertura media del numero di identificazione personale lettone

Strumento di convalida obbligatorio	Descrizione
Controllo codice personale della Lettonia	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione personale lettone

La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-506 Modelli di copertura limitata del numero di identificazione personale lettone

Modelli
$\backslash d\{2\} [01] \backslash d\{3\} - [012] \backslash d\{4\}$
$\backslash d\{2\} [01] \backslash d\{3\} [012] \backslash d\{4\}$
$32 \backslash d\{9\}$

Tabella 40-507 Convalide di copertura limitata del numero di identificazione personale lettone

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo codice personale della Lettonia	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di identificazione personale lettone, numero di identificazione personale, numero di identificazione nazionale, numero di identificazione, id nazionale, num id, tin lettone, tin, codice fiscale, n. tin, id fiscale, numero tin, cod. fiscale</p> <p>Personas kods, personas kods, latvijas personas kods, Valsts identifikācijas numurs, valsts identifikācijas numurs, identifikācijas numurs, nacionālais id, latvija alva, alva, nodokļu identifikācijas numurs, nodokļu id, alvas nē, nodokļa numurs</p>

Numero di identificazione lussemburghese (RNPP)

Il numero di identificazione lussemburghese è un numero di identificazione di 11 cifre rilasciato a tutti i cittadini del Lussemburgo all'età di 15 anni.

L'identificatore di dati per il Numero di identificazione lussemburghese rileva un numero di 11 cifre che corrisponde al formato del Numero di identificazione lussemburghese.

L'identificatore di dati di sistema del numero di identificazione lussemburghese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.
Vedere "[Copertura ampia numero di identificazione lussemburghese \(RNPP\)](#)" a pagina 1153.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum.
Vedere "[Copertura media numero di identificazione lussemburghese \(RNPP\)](#)" a pagina 1154.
- La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di identificazione lussemburghese \(RNPP\)](#)" a pagina 1154.

Copertura ampia numero di identificazione lussemburghese (RNPP)

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-508 Criterio copertura ampia numero di identificazione lussemburghese (RNPP)

Criterio
\d{11}

Tabella 40-509 Strumento di convalida copertura ampia numero di identificazione lussemburghese (RNPP)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione lussemburghese (RNPP)

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-510 Criteri copertura media numero di identificazione lussemburghese (RNPP)

Criterio
\d{11}

Tabella 40-511 Convalida copertura media numero di identificazione lussemburghese (RNPP)

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione lussemburghese	Lo strumento di convalida calcola il numero di checksum che ogni numero del Registre national des personnes physiques del Lussemburgo deve superare.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di identificazione lussemburghese (RNPP)

La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-512 Criteri di copertura limitata del numero di identificazione lussemburghese (RNPP)

Criterio
\d{11}

Tabella 40-513 Convalida copertura limitata del numero di identificazione lussemburghese (RNPP)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione lussemburghese	Lo strumento di convalida calcola il numero di checksum che ogni numero del Registre national des personnes physiques del Lussemburgo deve superare.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>ID personale, numero di identificazione personale, nidpersonale#, numero di identificazione univoco, numeoidpersonale, chiave ID univoca, codice di identificazione personale, chiaveidunivoca #, codice personale, ID personale</p> <p>Eindeutige ID-Nummer, Eindeutige ID, ID personelle, Numéro d'identification personnel, IDpersonnelle#, Persönliche Identifikationsnummer, EindeutigeID#</p>

Numero di passaporto lussemburghese

Un passaporto lussemburghese è un documento di viaggio internazionale rilasciato ai cittadini del Granducato di Lussemburgo che può anche servire come prova della cittadinanza lussemburghese.

L'identificatore di dati del numero di passaporto lussemburghese rileva una stringa alfanumerica di sette o otto caratteri che corrisponde al formato del numero di passaporto lussemburghese.

L'identificatore di dati del numero di passaporto lussemburghese fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di sette o otto caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di passaporto lussemburghese"](#) a pagina 1156.
- La copertura limitata rileva un modello alfanumerico di sette o otto caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.
Vedere ["Copertura limitata numero di passaporto lussemburghese"](#) a pagina 1156.

Copertura ampia del numero di passaporto lussemburghese

La copertura ampia rileva un modello alfanumerico di sette o otto caratteri senza la convalida del checksum.

Tabella 40-514 Modelli di copertura ampia del numero di passaporto lussemburghese

Modelli
<code>\1\w{5}[0-9]</code>
<code>\1\w{5}[0-9][0-9A-Za-z]</code>

Tabella 40-515 Convalida di copertura ampia del numero di passaporto lussemburghese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata numero di passaporto lussemburghese

La copertura limitata rileva un modello alfanumerico di sette o otto caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-516 Modelli di copertura limitata del numero di passaporto lussemburghese

Modelli
<code>\1\w{5}[0-9]</code>
<code>\1\w{5}[0-9][0-9A-Za-z]</code>

Tabella 40-517 Convalide di copertura limitata del numero di passaporto lussemburghese

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di passaporto, passaporto, num. passaporto, pass. lussemburghese, passaporto lussemburghese, passaporto del Lussemburgo</p> <p>passnummer, ausweisnummer, passeport, reisepass, pass, pass net, pass nr, no de passeport, passeport nombre, numéro de passeport</p>

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Numero di identificazione fiscale lussemburghese

Questo numero è emesso dal dipartimento delle entrate interne lussemburghesi (Administration des contributions directes, ACD) e viene utilizzato a fini fiscali per le persone fisiche e giuridiche.

L'identificatore di dati del numero di identificazione fiscale lussemburghese rileva un numero di 11 o 13 cifre che corrisponde al formato del numero di identificazione fiscale lussemburghese.

L'identificatore di dati del numero di identificazione fiscale lussemburghese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 o 13 cifre senza convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione fiscale lussemburghese"](#) a pagina 1157.
- La copertura media rileva un numero di 11 o 13 cifre con convalida checksum.
Vedere ["Copertura media del numero di identificazione fiscale lussemburghese"](#) a pagina 1158.
- La copertura limitata rileva un numero di 11 o 13 cifre con convalida checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di identificazione fiscale lussemburghese"](#) a pagina 1159.

Copertura ampia del numero di identificazione fiscale lussemburghese

La copertura ampia rileva un numero di 11 o 13 cifre senza convalida del checksum.

Tabella 40-518 Modelli di copertura ampia del numero di identificazione fiscale lussemburghese

Modelli
[1] [89] \d{2} [01] \d[0123] \d\d{5}
[1] [89] \d{2} [01] \d[0123] \d \d{5}
[1] [89] \d{2} [01] \d[0123] \d-\d{5}
[1] [89] \d{2} [01] \d[0123] \d,\d{5}
[1] [89] \d{2} [01] \d[0123] \d.\d{5}
[2] [0] \d{2} [01] \d[0123] \d\d{5}
[2] [0] \d{2} [01] \d[0123] \d \d{5}

Modelli
[2][0]\d{2}[01]\d[0123]\d-\d{5}
[2][0]\d{2}[01]\d[0123]\d,\d{5}
[2][0]\d{2}[01]\d[0123]\d.\d{5}
\d{11}
\d{2} \d{3} \d{3} \d{3}
\d{2}-\d{3}-\d{3}-\d{3}
\d{2}.\d{3}.\d{3}.\d{3}
\d{2},\d{3},\d{3},\d{3}

Tabella 40-519 Convalide di copertura ampia del numero di identificazione fiscale lussemburghese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero di identificazione fiscale lussemburghese

La copertura media rileva un numero di 11 o 13 cifre con convalida checksum.

Tabella 40-520 Modelli di copertura media del numero di identificazione fiscale lussemburghese

Modelli
[1][89]\d{2}[01]\d[0123]\d\d{5}
[1][89]\d{2}[01]\d[0123]\d \d{5}
[1][89]\d{2}[01]\d[0123]\d-\d{5}
[1][89]\d{2}[01]\d[0123]\d,\d{5}
[1][89]\d{2}[01]\d[0123]\d.\d{5}
[2][0]\d{2}[01]\d[0123]\d\d{5}

Modelli
[2][0]\d{2}[01]\d[0123]\d\d{5}
[2][0]\d{2}[01]\d[0123]\d-\d{5}
[2][0]\d{2}[01]\d[0123]\d,\d{5}
[2][0]\d{2}[01]\d[0123]\d.\d{5}
\d{11}
\d{2}\d{3}\d{3}\d{3}
\d{2}-\d{3}-\d{3}-\d{3}
\d{2}.\d{3}.\d{3}.\d{3}
\d{2},\d{3},\d{3},\d{3}

Tabella 40-521 Convalida di copertura media del numero di identificazione fiscale lussemburghese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione fiscale lussemburghese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione fiscale lussemburghese

La copertura limitata rileva un numero di 11 o 13 cifre con convalida checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-522 Modelli di copertura limitata del numero di identificazione fiscale lussemburghese

Modelli
[1][89]\d{2}[01]\d[0123]\d\d{5}
[1][89]\d{2}[01]\d[0123]\d\d{5}
[1][89]\d{2}[01]\d[0123]\d-\d{5}
[1][89]\d{2}[01]\d[0123]\d,\d{5}
[1][89]\d{2}[01]\d[0123]\d.\d{5}

Modelli
[2] [0] \d{2} [01] \d[0123] \d\d{5}
[2] [0] \d{2} [01] \d[0123] \d \d{5}
[2] [0] \d{2} [01] \d[0123] \d-\d{5}
[2] [0] \d{2} [01] \d[0123] \d,\d{5}
[2] [0] \d{2} [01] \d[0123] \d.\d{5}
\d{11}
\d{2} \d{3} \d{3} \d{3}
\d{2}-\d{3}-\d{3}-\d{3}
\d{2}.\d{3}.\d{3}.\d{3}
\d{2},\d{3},\d{3},\d{3}

Tabella 40-523 Convalide di copertura limitata del numero di identificazione fiscale lussemburghese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione fiscale lussemburghese	Calcola il checksum e lo utilizza per convalidare il modello.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>previdenza sociale, tin, numero tin, n. tin, n.tin, numero di identificazione fiscale lussemburghese, numero fiscale, numero identificazione fiscale</p> <p>Zinn, Zinn Nummer, Luxembourg Tax Identifikationsnummer, Steier Nummer, Steier ID, Sozialversicherungsausweis, Zinnzahl, Zinn nein, Zinn#, luxemburgische steueridentifikationsnummer, Steuernummer, Steuer ID</p> <p>sécurité sociale, carte de sécurité sociale, étain, numéro d'étain, étain non, étain#, Numéro d'identification fiscal luxembourgeois, numéro d'identification fiscale, identifiant d'impôt, Sozialunterstützung, Sozialversicherung</p>
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Numero di partita IVA lussemburghese

L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.

L'identificatore di dati della partita IVA lussemburghese rileva un modello alfanumerico di otto caratteri che corrisponde al formato del numero di partita IVA lussemburghese.

L'identificatore di dati della partita IVA lussemburghese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di otto caratteri che inizia con **LU** senza la convalida del checksum.
Vedere ["Copertura ampia numero di partita IVA lussemburghese"](#) a pagina 1162.
- La copertura media rileva un modello alfanumerico di otto caratteri che inizia con **LU** con convalida del checksum.
Vedere ["Copertura media del numero di partita IVA lussemburghese"](#) a pagina 1162.
- La copertura limitata rileva un modello alfanumerico di otto caratteri che inizia con **LU** la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di partita IVA lussemburghese"](#) a pagina 1163.

Copertura ampia numero di partita IVA lussemburghese

La copertura ampia rileva un modello alfanumerico di otto caratteri che inizia con LU senza la convalida del checksum.

Tabella 40-524 Modelli di copertura ampia del numero di partita IVA lussemburghese

Modelli
[Lu] [Uu] \d{8}
[Lu] [Uu] \d{8}
[Lu] [Uu] -\d{8}
[Lu] [Uu] \d{3} \d{3} \d{2}
[Lu] [Uu] \d{4} \d{4}
[Lu] [Uu] \d{4} -\d{4}
[Lu] [Uu] \d{4} .\d{4}
[Lu] [Uu] \d{4} ,\d{4}

Tabella 40-525 Convalide di copertura ampia del numero di partita IVA lussemburghese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	Consente di escludere le seguenti stringhe di caratteri dalla fine del numero: 00000000, 11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999

Copertura media del numero di partita IVA lussemburghese

La copertura media rileva un modello alfanumerico di otto caratteri che inizia con LU con convalida del checksum.

Tabella 40-526 Modelli di copertura media del numero di partita IVA lussemburghese

Modelli
[Lu] [Uu] \d{8}
[Lu] [Uu] \d{8}

Modelli
[Lu] [Uu] -\d{8}
[Lu] [Uu] \d{3} \d{3} \d{2}
[Lu] [Uu] \d{4} \d{4}
[Lu] [Uu] \d{4}-\d{4}
[Lu] [Uu] \d{4}.\d{4}
[Lu] [Uu] \d{4},\d{4}

Tabella 40-527 Convalida di copertura media del numero di partita IVA lussemburghese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA lussemburghese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di partita IVA lussemburghese

La copertura limitata rileva un modello alfanumerico di otto caratteri che inizia con LU la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-528 Modelli di copertura limitata del numero di partita IVA lussemburghese

Modelli
[Lu] [Uu] \d{8}
[Lu] [Uu] \d{8}
[Lu] [Uu] -\d{8}
[Lu] [Uu] \d{3} \d{3} \d{2}
[Lu] [Uu] \d{4} \d{4}
[Lu] [Uu] \d{4}-\d{4}
[Lu] [Uu] \d{4}.\d{4}
[Lu] [Uu] \d{4},\d{4}

Tabella 40-529 Convalide di copertura limitata del numero di partita IVA lussemburghese

Convalide obbligatorie	Descrizione
Controllo di convalida numero di partita IVA lussemburghese	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	Consente di escludere le seguenti stringhe di caratteri dalla fine del numero: 00000000, 11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero di partita iva lussemburghese, num iva lussemburghese, n. partita iva, n. IVA, IVA, numero imposta valore aggiunto, id iva, numero di registrazione iva, imposta sul valore aggiunto TVA kee, TVA#, TVA Aschreiwung kee, T.V.A, stammnummer, bleiwen, geheesch, gitt id, mehrwertsteuer, vat registrierungsnummer, umsatzsteuer-id, wat, umsatzsteuernummer, umsatzsteuer-identifikationsnummer id de la batterie, lëtzebuerg vat nee, registréierung nummer, numéro de TVA, numéro de enregistrement vat

Numero di carta di identità malese (MyKad)

Il numero di carta di identità malese (abbreviato in n. NRIC) è un codice univoco di 12 cifre e viene rilasciato ai cittadini malesi e ai residenti permanenti per scopi di identificazione, indicizzazione e rilevamento.

L'identificatore di dati per il Numero di carta di identità malese (MyKad) rileva un numero di 12 cifre che corrisponde al formato del MyKad.

L'identificatore di dati del sistema relativo al numero di carta di identità malese (MyKad) fornisce tre coperture di rilevamento:

L'identificatore di dati del sistema relativo al numero di carta di identità malese (MyKad) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum.
Vedere "[Copertura ampia del numero di carta di identità malese \(MyKad\)](#)" a pagina 1165.
- La copertura media rileva un numero di 12 cifre con la convalida del checksum.
Vedere "[Copertura media numero di carta di identità malese \(MyKad\)](#)" a pagina 1165.
- La copertura limitata rileva un numero di 12 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate al MyKad.
Vedere "[Copertura limitata numero di carta di identità malese \(MyKad\)](#)" a pagina 1166.

Copertura ampia del numero di carta di identità malese (MyKad)

La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum.

Tabella 40-530 Criteri di copertura ampia del numero di carta di identità malese (MyKad)

Modelli
$\backslash d\{12\}$
$\backslash d\{6\}-\backslash d\{2\}-\backslash d\{4\}$

Tabella 40-531 Convalida di copertura ampia del numero di carta di identità malese (MyKad)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di carta di identità malese (MyKad)

La copertura media rileva un numero di 12 cifre con la convalida del checksum.

Tabella 40-532 Criteri copertura media numero di carta di identità malese (MyKad)

Modelli
$\backslash d\{12\}$
$\backslash d\{6\}-\backslash d\{2\}-\backslash d\{4\}$

Tabella 40-533 Strumenti di convalida copertura media numero di carta di identità malese (MyKad)

Convalide obbligatorie	Descrizione
Controllo di convalida numero di carta di identità malese	Lo strumento di convalida calcola il numero di checksum che ogni numero di carta di identità malese deve superare.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata numero di carta di identità malese (MyKad)

La copertura limitata rileva un numero di 12 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate al MyKad.

Tabella 40-534 Criteri copertura limitata numero di carta di identità malese (MyKad)

Modelli
$\backslash d\{12\}$
$\backslash d\{6\}-\backslash d\{2\}-\backslash d\{4\}$

Tabella 40-535 Convalida copertura limitata numero di carta di identità malese (MyKad)

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero carta di identità malese (MyKad)	Lo strumento di convalida calcola il checksum che ogni numero di carta di identità malese deve superare.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>N. NRIC, nricno#, N Mykad, n mykad, cartadiidentità#, n carta di identità, MyKadno#, mykad, mykad#, numero carta di identità, nric no</p> <p>nombor kad pengenalan, kad pengenalan no, kad pengenalan Malaysia, bilangan identiti unik, nombor peribadi, nomborperibadi#, kadpengenalanno#</p>

Identificatore beneficiario di assistenza sanitaria

L'identificatore beneficiario di assistenza sanitaria (MBI) è assegnato a un individuo allo scopo di identificarlo come beneficiario di assistenza sanitaria. Entro aprile 2019 l'MBI sostituirà il numero di assicurazione sanitaria (HICN) su tutte le tessere Medicare.

L'identificatore beneficiario di assistenza sanitaria rileva un modello alfanumerico di 11 caratteri che corrisponde al formato dell'identificatore beneficiario di assistenza sanitaria.

L'identificatore di dati dell'Identificatore beneficiario di assistenza sanitaria fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 11 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia Identificatore beneficiario di assistenza sanitaria"](#) a pagina 1167.
- La copertura media rileva un modello alfanumerico di 11 caratteri con la convalida del checksum.
Vedere ["Copertura media Identificatore beneficiario di assistenza sanitaria"](#) a pagina 1167.
- La copertura limitata rileva un modello alfanumerico di 11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata Identificatore beneficiario di assistenza sanitaria"](#) a pagina 1168.

Copertura ampia Identificatore beneficiario di assistenza sanitaria

La copertura ampia rileva un modello alfanumerico di 11 caratteri senza la convalida del checksum.

Tabella 40-536 Modello copertura ampia Identificatore beneficiario di assistenza sanitaria

Criterio
[1-9] [A-Za-z] [0-9A-Za-z] [0-9] [A-Za-z] [0-9A-Za-z] [0-9] [A-Za-z] {2} [0-9] {2}

Tabella 40-537 Convalida di copertura ampia Identificatore beneficiario di assistenza sanitaria

Strumento di convalida obbligatorio	
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media Identificatore beneficiario di assistenza sanitaria

La copertura media rileva un modello alfanumerico di 11 caratteri con la convalida del checksum.

Tabella 40-538 Modello copertura media Identificatore beneficiario di assistenza sanitaria

Criterio
[1-9] [A-Za-z] [0-9A-Za-z] [0-9] [A-Za-z] [0-9A-Za-z] [0-9] [A-Za-z] {2} [0-9] {2}

Tabella 40-539 Convalida di copertura media Identificatore beneficiario di assistenza sanitaria

Strumento di convalida obbligatorio	
Controllo di convalida numero di identificazione beneficiario di assistenza sanitaria.	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata Identificatore beneficiario di assistenza sanitaria

La copertura limitata rileva un modello alfanumerico di 11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-540 Modello copertura limitata Identificatore beneficiario di assistenza sanitaria

Criterio
[1-9] [A-Za-z] [0-9A-Za-z] [0-9] [A-Za-z] [0-9A-Za-z] [0-9] [A-Za-z] {2} [0-9] {2}

Tabella 40-541 Convalide di copertura limitata Identificatore beneficiario di assistenza sanitaria

Convalide obbligatorie	
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione beneficiario di assistenza sanitaria.	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Identificatore beneficiario di assistenza sanitaria, identificatore beneficiario di assistenza sanitaria, numero mbi, n. mbi, numero# mbi, numero# mbi, n.# mbi, identificatore beneficiario di assistenza sanitaria, ident. beneficiario di assistenza sanitaria, n. beneficiario di assistenza sanitaria</p>

Numero di registrazione e identificazione personale messicano

Il Numero di registrazione e identificazione personale messicano è un numero usato negli stati messicani (a eccezione di Città del Messico) come codice di identificazione personale.

Il Numero di registrazione e identificazione personale messicano rileva una stringa alfanumerica di 15 caratteri che corrisponde al formato del Numero di registrazione e identificazione personale messicano.

L'identificatore di dati Numero di registrazione e identificazione personale messicano fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 15 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del Numero di registrazione e identificazione personale messicano"](#) a pagina 1169.
- La copertura media rileva una stringa alfanumerica di 15 caratteri con la convalida del checksum.
Vedere ["Copertura media Numero di registrazione e identificazione personale messicano"](#) a pagina 1170.
- La copertura limitata rileva una stringa alfanumerica di 15 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata Numero di registrazione e identificazione personale messicano"](#) a pagina 1170.

Copertura ampia del Numero di registrazione e identificazione personale messicano

La copertura ampia rileva una stringa alfanumerica di 15 caratteri senza la convalida del checksum.

Tabella 40-542 Criterio della copertura ampia del Numero di registrazione e identificazione personale messicano

Criterio
\{2}-\{3}-\{2}-\{7}-w

Tabella 40-543 Convalida della copertura ampia del Numero di registrazione e identificazione personale messicano

Convalida obbligatoria	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 00000000000000, 11111111111111, 22222222222222, 33333333333333, 44444444444444, 55555555555555, 66666666666666, 77777777777777, 88888888888888, 99999999999999

Copertura media Numero di registrazione e identificazione personale messicano

La copertura media rileva una stringa alfanumerica di 15 caratteri con la convalida del checksum.

Tabella 40-544 Criterio di copertura media Numero di registrazione e identificazione personale messicano

Criterio
$\{d\}_2 - \{d\}_3 - \{d\}_2 - \{d\}_7 - w$

Tabella 40-545 Convalida di copertura media Numero di registrazione e identificazione personale messicano

Convalida obbligatoria	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 00000000000000, 11111111111111, 22222222222222, 33333333333333, 44444444444444, 55555555555555, 66666666666666, 77777777777777, 88888888888888, 99999999999999
Controllo convalida numero di registrazione e di identità messicano	Calcola il checksum per la corrispondenza e lo utilizza per convalidare il modello.

Copertura limitata Numero di registrazione e identificazione personale messicano

La copertura limitata rileva una stringa alfanumerica di 15 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-546

Criterio di copertura limitata Numero di registrazione e identificazione personale messicano

Criterio
$\backslash d\{2\}-\backslash d\{3\}-\backslash d\{2\}-\backslash d\{7\}-\backslash w$

Tabella 40-547

Convalida di copertura limitata Numero di registrazione e identificazione personale messicano

Convalida obbligatoria	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 00000000000000, 11111111111111, 22222222222222, 33333333333333, 44444444444444, 55555555555555, 66666666666666, 77777777777777, 88888888888888, 99999999999999
Controllo convalida numero di registrazione e di identità messicano	Calcola il checksum per ogni numero corrispondente e lo utilizza per convalidare il criterio.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: Codice di registrazione e identificazione personale, CRIP, crip, N. CRIP, n. crip, Codice di identificazione personale messicano, numero identificativo personale messicano Clave de Registro de Identidad Personal, Código de Identificación Personal mexicana, número de identificación personal mexicana

Numero di identificazione fiscale messicano

In Messico, a una persona giuridica, quale un'azienda o un individuo, viene assegnato un numero di identificazione fiscale. Il numero RFC di un'azienda è formato da 12 caratteri, mentre quello di una persona è formato da 13 caratteri.

L'identificatore di dati Numero di identificazione fiscale messicano rileva una stringa alfanumerica di 12 o 13 caratteri che corrisponde al formato del Numero di identificazione fiscale messicano.

L'identificatore di dati Numero di identificazione fiscale messicano fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 12 o 13 caratteri senza convalida. Vedere ["Copertura ampia Numero di identificazione fiscale messicano"](#) a pagina 1172.
- La copertura media rileva una stringa alfanumerica di 12 o 13 caratteri con la convalida del checksum. Vedere ["Copertura media Numero di identificazione fiscale messicano"](#) a pagina 1172.
- La copertura limitata rileva una stringa alfanumerica di 12 o 13 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata Numero di identificazione fiscale messicano"](#) a pagina 1173.

Copertura ampia Numero di identificazione fiscale messicano

La copertura ampia rileva una stringa alfanumerica di 12 o 13 caratteri senza convalida.

Tabella 40-548 Criteri copertura ampia Numero di identificazione fiscale messicano

Criteri
$\backslash 1\{4\}\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{4\}[-]\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{3\}\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{3\}[-]\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$

Copertura media Numero di identificazione fiscale messicano

La copertura media rileva una stringa alfanumerica di 12 o 13 caratteri con la convalida del checksum.

Tabella 40-549 Criteri di copertura media Numero di identificazione fiscale messicano

Criteri
$\backslash 1\{4\}\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{4\}[-]\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{3\}\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{3\}[-]\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$

Tabella 40-550 Convalida di copertura media Numero di identificazione fiscale messicano

Convalida obbligatoria	Descrizione
Controllo convalida numero di identificazione fiscale messicano	Calcola il checksum per ogni numero corrispondente e lo utilizza per convalidare il criterio.

Copertura limitata Numero di identificazione fiscale messicano

La copertura limitata rileva una stringa alfanumerica di 12 o 13 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-551 Criteri di copertura limitata Numero di identificazione fiscale messicano

Criteri
$\backslash 1\{4\}\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{4\}[-]\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{3\}\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$
$\backslash 1\{3\}[-]\backslash d\{2\}[01]\backslash d[0-3]\backslash d\backslash w\{3\}$

Tabella 40-552 Convalide di copertura limitata Numero di identificazione fiscale messicano

Convalida obbligatoria	Descrizione
Controllo convalida numero di identificazione fiscale messicano	Calcola il checksum per ogni numero corrispondente e lo utilizza per convalidare il criterio.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numero di identificazione fiscale, codice fiscale, numero di codice fiscale, numero RFC, TIN, N. TIN, codice del registro federale dei contribuenti</p> <p>Registro Federal de Contribuyentes, número de identificación de impuestos, Código del Registro Federal de Contribuyentes, Número RFC, Clave del RFC</p>

Codice di identificazione personale messicano (CURP)

Il Codice di identificazione personale messicano (Clave Única de Registro de Población o CURP) è l'identificatore alfanumerico univoco assegnato a ogni messicano o straniero residente in Messico, nonché ai messicani che vivono all'estero.

L'identificatore di dati per il Codice di identificazione personale messicano (CURP) rileva una stringa alfanumerica di 18 caratteri che corrisponde al formato del CURP.

L'identificatore di dati di sistema codice di identificazione personale messicano (CURP) fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 18 caratteri senza la convalida del Vedere "[Copertura ampia del codice di identificazione personale messicano \(CURP\)](#)" a pagina 1174.
- La copertura media rileva una stringa alfanumerica di 18 caratteri con la convalida del checksum. Vedere "[Copertura media del codice di identificazione personale messicano \(CURP\)](#)" a pagina 1174.
- La copertura limitata rileva una stringa alfanumerica di 18 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata codice di identificazione personale messicano \(CURP\)](#)" a pagina 1175.

Copertura ampia del codice di identificazione personale messicano (CURP)

La copertura ampia rileva una stringa alfanumerica di 18 caratteri senza la convalida del

Tabella 40-553 Criterio di copertura ampia del codice di identificazione personale messicano (CURP)

Criterio
<code>\w[AEIOUaeiou]\w{2}\d{2}[0-1]\d[0-3]\d[HMhm]\w{7}</code>

Copertura media del codice di identificazione personale messicano (CURP)

La copertura media rileva una stringa alfanumerica di 18 caratteri con la convalida del checksum.

Tabella 40-554 Criterio di copertura media del codice di identificazione personale messicano (CURP)

Criterio
\w[AEIOUaeiou]\w{2}\d{2}[0-1]\d[0-3]\d[HMhm]\w{7}

Tabella 40-555 Convalida di copertura media del codice di identificazione personale messicano (CURP)

Convalida obbligatoria	Descrizione
Controllo di convalida codice di identificazione personale messicano	Lo strumento di convalida calcola il numero di checksum che ogni codice di identificazione personale messicano deve superare.

Copertura limitata codice di identificazione personale messicano (CURP)

La copertura limitata rileva una stringa alfanumerica di 18 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-556 Criteri copertura limitata codice di identificazione personale messicano (CURP)

Criterio
\w[AEIOUaeiou]\w{2}\d{2}[0-1]\d[0-3]\d[HMhm]\w{7}

Tabella 40-557 Convalida copertura limitata codice di identificazione personale messicano (CURP)

Convalida obbligatoria	Descrizione
Controllo di convalida codice di identificazione personale messicano	Lo strumento di convalida calcola il numero di checksum che ogni codice di identificazione personale messicano deve superare.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>ID Personale, numero ID personale, ID personale, numero ID univoco, chiave ID univoca, codice ID personale, codice di identificazione personale univoco, codice di identificazione univoco, idpersonale#, numeroidpersonale#, chiaveidunivoca#</p> <p>CURP, curp#, clave Única de registro de Población, clave única, clave única de identidad, clave personal Identidad, personal Identidad Clave, ClaveÚnica#, clavepersonalIdentidad#</p>

Numero di conto bancario esteso messicano (CLABE)

Il Numero di conto bancario esteso messicano (CLABE, Clave Bancaria Estandarizada) è un numero di 18 cifre utilizzato come standard per la numerazione di conti bancari in Messico.

L'identificatore di dati per il Numero di conto bancario esteso messicano (CLABE) rileva un numero di 18 cifre che corrisponde al formato del Numero CLABE.

L'identificatore di dati Numero di conto bancario esteso messicano (CLABE) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 18 cifre senza la convalida del checksum. Vedere "[Copertura ampia numero di conto bancario esteso messicano \(CLABE\)](#)" a pagina 1176.
- La copertura media rileva un numero di 18 cifre con la convalida del checksum. Vedere "[Copertura media numero di conto bancario esteso messicano \(CLABE\)](#)" a pagina 1177.
- La copertura limitata rileva un numero a 18 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata del numero di conto bancario esteso messicano \(CLABE\)](#)" a pagina 1177.

Copertura ampia numero di conto bancario esteso messicano (CLABE)

La copertura ampia rileva un numero di 18 cifre senza la convalida del checksum.

Tabella 40-558 Criteri copertura ampia numero di conto bancario esteso messicano (CLABE)

Criterio
\d{18}

Tabella 40-559 Convalida copertura ampia numero di conto bancario esteso messicano (CLABE)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di conto bancario esteso messicano (CLABE)

La copertura media rileva un numero di 18 cifre con la convalida del checksum.

Tabella 40-560 Criteri copertura media numero di conto bancario esteso messicano (CLABE)

Criterio
\d{18}

Tabella 40-561 Convalida copertura media numero di conto bancario esteso messicano (CLABE)

Convalida obbligatoria	Descrizione
Controllo di convalida numero di conto bancario esteso messicano	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Escludi caratteri iniziali	Esclude i seguenti caratteri dall'inizio del numero: 5555555555555555

Copertura limitata del numero di conto bancario esteso messicano (CLABE)

La copertura limitata rileva un numero a 18 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-562 Criteri di copertura limitata del numero di conto bancario esteso messicano (CLABE)

Criterio
\d{18}

Tabella 40-563 Convalide di copertura limitata del numero di conto bancario esteso messicano (CLABE)

Convalida obbligatoria	Descrizione
Controllo di convalida numero di conto bancario esteso messicano	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: Numero di conto bancario esteso messicano (CLABE), numero di conto bancario esteso messicano (CLABE), numero clabe, n. clabe, N. CLABE messicano, n. clabe messicano, N. CLABE Clave Bancaria Estandarizada, Estandarizado Banco número de clave, número de clave, clave número, clave#

National Drug Code (NDC, codici identificativi dei farmaci)

Il National Drug Code (NDC, codici identificativi dei farmaci) è un codice di identificazione rilasciato dalla Food and Drug Administration (FDA) per i farmaci negli Stati Uniti. Un formato alternativo è definito inoltre dalle normative HIPAA.

L'identificatore di dati National Drug Code (NDC, codici identificativi dei farmaci) rileva l'esistenza di un NDC e la versione di HIPAA.

Questo identificatore di dati fornisce tre coperture di rilevamento:

- La copertura ampia controlla l'esistenza di un numero NDC o della relativa versione HIPAA.

Vedere ["Copertura ampia National Drug Code \(NDC, codici identificativi dei farmaci\)"](#) a pagina 1179.

- La larghezza media limita i criteri per il rilevamento dei numeri.
Vedere ["Copertura media National Drug Code \(NDC\)"](#) a pagina 1179.
- La copertura limitata necessita della corrispondenza con una parola chiave.
Vedere ["Copertura limitata National Drug Code \(NDC, codici identificativi dei farmaci\)"](#) a pagina 1180.

Copertura ampia National Drug Code (NDC, codici identificativi dei farmaci)

La copertura ampia rileva il formato FDA standard, ovvero un numero di 10 cifre nel formato 4-4-2, 5-4-1 o 5-3-2, con i numeri separati da trattini o spazi.

Tale identificatore dati rileva inoltre il formato HIPAA, un numero di 11 cifre nel formato 5-4-2. Il formato HIPAA può includere un asterisco per indicare una cifra mancante.

Tabella 40-564 Criteri di copertura ampia National Drug Code (NDC, codici identificativi dei farmaci)

Criteri
*?\d{4} \d{4} \d{2}
*?\d{4}-\d{4}-\d{2}
\d{5} *?\d{3} \d{2}
\d{5}-*?\d{3}-\d{2}
\d{5} \d{4} *?\d
\d{5}-\d{4}-*?\d
\d{5} \d{4} \d{2}
\d{5}-\d{4}-\d{2}

Copertura media National Drug Code (NDC)

La copertura media rileva il formato FDA standard, ovvero un numero di 10 cifre nel formato 4-4-2, 5-4-1 o 5-3-2, con i numeri separati da trattini.

Tale identificatore dati rileva inoltre il formato HIPAA, un numero di 11 cifre nel formato 5-4-2. Il formato HIPAA può includere un asterisco per indicare una cifra mancante.

Nota: La copertura media dell'identificatore dati non include alcuno strumento di convalida.

Tabella 40-565 Criteri copertura media National Drug Code (NDC)

Criterio
*?\d{4}-\d{4}-\d{2}
\d{5}-*?\d{3}-\d{2}
\d{5}-\d{4}-*?\d
\d{5}-\d{4}-\d{2}

Copertura limitata National Drug Code (NDC, codici identificativi dei farmaci)

La copertura limitata rileva il formato FDA standard, ovvero un numero di 10 cifre nel formato 4-4-2, 5-4-1 o 5-3-2, con i numeri separati da trattini.

Tale identificatore dati rileva inoltre il formato HIPAA, un numero di 11 cifre nel formato 5-4-2. Il formato HIPAA può includere un asterisco per indicare una cifra mancante. Questo identificatore di dati richiede inoltre la presenza di una parola chiave associata a NDC.

Tabella 40-566 Criteri copertura limitata National Drug Code (NDC, codici identificativi dei farmaci)

Criterio
*?\d{4}-\d{4}-\d{2}
\d{5}-*?\d{3}-\d{2}
\d{5}-\d{4}-*?\d
\d{5}-\d{4}-\d{2}

Tabella 40-567 Convalide copertura limitata National Drug Code (NDC, codici identificativi dei farmaci)

Convalida obbligatoria	Descrizione
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.
Input Trova parole chiave	ndc, national drug code

Numero NPI

Il numero NPI (National Provider Identifier) è un numero identificativo di 10 cifre rilasciato ai fornitori di servizi medici negli Stati Uniti dall'agenzia Centers for Medicare and Medicaid Services.

L'identificatore di dati per il Numero NPI rileva un numero 10 cifre che corrisponde al formato del numero NPI.

L'identificatore di dati del numero NPI fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum. Vedere "[Copertura ampia del numero NPI](#)" a pagina 1181.
- La copertura media rileva un numero a 10 cifre con la convalida del checksum. Vedere "[Copertura media numero NPI](#)" a pagina 1181.
- La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata numero NPI](#)" a pagina 1182.

Copertura ampia del numero NPI

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-568 Criteri di copertura ampia del numero NPI

Criterio
$\backslash d\{10\}$
80840 $\backslash d\{10\}$

Tabella 40-569 Convalida di copertura ampia del numero NPI

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero NPI

La copertura media rileva un numero a 10 cifre con la convalida del checksum.

Tabella 40-570 Criteri di copertura media numero NPI

Criterio
\d{10}
80840\d{10}

Tabella 40-571 Convalide di copertura media numero NPI

Convalida obbligatoria	Descrizione
Controllo di convalida numero NPI	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata numero NPI

La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-572 Criteri copertura limitata numero NPI

Criterio
\d{10}
80840\d{10}

Tabella 40-573 Strumenti di convalida copertura limitata numero NPI

Convalida obbligatoria	Descrizione
Controllo di convalida numero NPI	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: NPI (National Provider Identifier), NPI, np, n.p.i, hipaa, ID National Provider, npid, numero national provider, ID NPI

Numero di patente di guida dei Paesi Bassi

Numero di identificazione della patente di guida individuale rilasciata dall'autorità preposta nei Paesi Bassi.

L'identificatore di dati del numero di patente di guida dei Paesi Bassi rileva un numero di 10 cifre che corrisponde al formato del numero di patente di guida dei Paesi Bassi.

L'identificatore di dati del numero di patente di guida dei Paesi Bassi fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum. Vedere "[Copertura ampia del numero di patente di guida dei Paesi Bassi](#)" a pagina 1183.
- La copertura limitata rileva un numero di 10 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata del numero di patente di guida dei Paesi Bassi](#)" a pagina 1183.

Copertura ampia del numero di patente di guida dei Paesi Bassi

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-574 Modello copertura ampia del numero di patente di guida dei Paesi Bassi

Criterio
$\backslash d\{10\}$

Tabella 40-575 Convalide di copertura ampia del numero di patente di guida dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di patente di guida dei Paesi Bassi

La copertura limitata rileva un numero di 10 cifre senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-576 Modello copertura limitata del numero di patente di guida dei Paesi Bassi

Criterio
$\backslash d\{10\}$

Tabella 40-577 Convalide di copertura limitata del numero di patente di guida dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>RIJMEWIJS, Patente di guida, Numero Patente di Guida, numero patente di guida, Patente Guida, Pat. Guida, Patente di guida, Patente guida, Pat. di guida, Numero pat. guida, numero pat. guida, num. patente di guida, Num. Pat. guida, numero patente guida, DLNo#, dIno#</p> <p>permis de conduire, rijbewijs, Rijbewijsnummer, DL#, RIJBEWIJSNUMMER</p>

Numero di passaporto dei Paesi Bassi

Il passaporto dei Paesi Bassi viene rilasciato ai cittadini dei Paesi Bassi per viaggiare all'estero.

L'identificatore di dati del numero di passaporto dei Paesi Bassi rileva un numero di nove cifre che corrisponde al formato del numero di passaporto dei Paesi Bassi.

L'identificatore di dati del numero di passaporto dei Paesi Bassi fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum. Vedere ["Copertura ampia numero di passaporto dei Paesi Bassi"](#) a pagina 1184.
- La copertura limitata rileva un numero di nove cifre. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata numero di passaporto dei Paesi Bassi"](#) a pagina 1185.

Copertura ampia numero di passaporto dei Paesi Bassi

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-578 Modello di copertura ampia numero di passaporto dei Paesi Bassi

Modello
\w{9}

Tabella 40-579 Convalida di copertura ampia numero di passaporto dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata numero di passaporto dei Paesi Bassi

La copertura limitata rileva un numero di nove cifre. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-580 Modello di copertura limitata del numero di passaporto dei Paesi Bassi

Modello
\w{9}

Tabella 40-581 Convalide di copertura limitata del numero di passaporto dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numero di passaporto dei Paesi Bassi, numero di passaporto dei Paesi Bassi, numero di passaporto, numero di passaporto olandese</p> <p>Nederlanden paspoort nummer, Paspoort, paspoort, Nederlanden paspoortnummer, paspoortnummer</p>

Numero di identificazione fiscale dei Paesi Bassi

I Paesi Bassi emettono un numero di identificazione fiscale al momento della nascita o della registrazione presso l'anagrafe.

L'identificatore di dati del numero di identificazione fiscale dei Paesi Bassi rileva un numero di nove cifre che corrisponde al formato del numero di identificazione fiscale dei Paesi Bassi.

L'identificatore di dati del numero di identificazione fiscale dei Paesi Bassi fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione fiscale dei Paesi Bassi"](#) a pagina 1186.
- La copertura media rileva un numero di nove cifre con la convalida del checksum.
Vedere ["Copertura media del numero di identificazione fiscale dei Paesi Bassi"](#) a pagina 1186.
- La copertura limitata rileva un numero a nove cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di identificazione fiscale dei Paesi Bassi"](#) a pagina 1187.

Copertura ampia del numero di identificazione fiscale dei Paesi Bassi

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-582 Modelli di copertura ampia del numero di identificazione fiscale dei Paesi Bassi

Criterio
$\backslash d\{9\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$

Tabella 40-583 Convalide di copertura ampia del numero di identificazione fiscale dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione fiscale dei Paesi Bassi

La copertura media rileva un numero di nove cifre con la convalida del checksum.

Tabella 40-584 Modelli di copertura media del numero di identificazione fiscale dei Paesi Bassi

Criterio
$\backslash d\{9\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$

Tabella 40-585 Convalida di copertura media del numero di identificazione fiscale dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione fiscale dei Paesi Bassi	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione fiscale dei Paesi Bassi

La copertura limitata rileva un numero a nove cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-586 Modelli di copertura limitata del numero di identificazione fiscale dei Paesi Bassi

Criterio
$\backslash d\{9\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$

Tabella 40-587 Convalide di copertura limitata del numero di identificazione fiscale dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione fiscale dei Paesi Bassi	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di identificazione fiscale dei Paesi Bassi, identificazione fiscale dei Paesi Bassi, numero di identificazione fiscale olandese, identificazione fiscale olandese, numero di identificazione fiscale, codice fiscale olandese, numero di codice fiscale olandese, codice fiscale, numero di codice fiscale, numero fiscale, n. fiscale, cod. fiscale, n. fiscale, num. fiscale, numero fiscale, n.fiscale, numero fiscale Paesi Bassi, numero fiscale dei Paesi Bassi</p> <p>Nederlands belasting identificatienummer, identificatienummer van belasting, identificatienummer belasting, Nederlands belasting identificatie, Nederlands belasting id nummer, Nederlands belastingnummer, btw nummer, Nederlandse belasting identificatie, Nederlands belastingnummer</p> <p>netherlands tax identification tal, netherlands tax identification tal, tax identification tal, tax tal, Nederlands tax identification tal, Hollands tax identification, Nederlansk tax tal, Hollands tax id tal</p> <p>netherlands impuesto identification number, netherlands impuesto identification number, impuesto identification number, impuesto number, hulandes impuesto identification number, hulandes impuesto identification, hulandes impuesto number, hulandes impuesto id number</p>

Numero di partita IVA dei Paesi Bassi

L'imposta sul valore aggiunto (IVA) è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Nei Paesi Bassi, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.

L'identificatore di dati del numero di partita IVA dei Paesi Bassi rileva un modello alfanumerico di 14 caratteri che corrisponde al formato del numero di partita IVA dei Paesi Bassi.

L'identificatore di dati della partita IVA dei Paesi Bassi fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 14 caratteri che iniziano con **NL** senza la convalida del checksum.
Vedere "[Copertura ampia numero di partita IVA dei Paesi Bassi](#)" a pagina 1189.
- La copertura media rileva un modello alfanumerico di 14 caratteri che iniziano con **NL** con la convalida del checksum.
Vedere "[Copertura media del numero di partita IVA dei Paesi Bassi](#)" a pagina 1190.
- La copertura limitata rileva un modello alfanumerico di 14 caratteri che iniziano con **NL** con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero di partita IVA dei Paesi Bassi](#)" a pagina 1190.

Copertura ampia numero di partita IVA dei Paesi Bassi

La copertura ampia rileva un modello alfanumerico di 14 caratteri che iniziano con **NL** senza la convalida del checksum

Tabella 40-588 Modelli di copertura ampia numero di partita IVA dei Paesi Bassi

Modello
[Nn] [Ll] \d{9} [Bb] \d{2}
[Nn] [Ll] -\d{9} - [Bb] \d{2}
[Nn] [Ll] \d{9} [Bb] \d{2}
[Nn] [Ll] .\d{9} . [Bb] \d{2}

Tabella 40-589 Convalida di copertura ampia numero di partita IVA dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura media del numero di partita IVA dei Paesi Bassi

La copertura media rileva un modello alfanumerico di 14 caratteri che iniziano con **NL** con la convalida del checksum.

Tabella 40-590 Modelli di copertura media del numero di partita IVA dei Paesi Bassi

Modello
[Nn] [Ll] \d{9} [Bb] \d{2}
[Nn] [Ll] -\d{9} - [Bb] \d{2}
[Nn] [Ll] \d{9} [Bb] \d{2}
[Nn] [Ll] .\d{9} . [Bb] \d{2}

Tabella 40-591 Convalida di copertura media del numero di partita IVA dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida del numero di partita IVA dei Paesi Bassi	Convalida checksum per il numero di partita IVA dei Paesi Bassi.

Copertura limitata numero di partita IVA dei Paesi Bassi

La copertura limitata rileva un modello alfanumerico di 14 caratteri che iniziano con **NL** con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-592 Modelli copertura limitata numero di partita IVA dei Paesi Bassi

Modello
[Nn] [Ll] \d{9} [Bb] \d{2}
[Nn] [Ll] -\d{9} - [Bb] \d{2}
[Nn] [Ll] \d{9} [Bb] \d{2}
[Nn] [Ll] .\d{9} . [Bb] \d{2}

Tabella 40-593 Convalide di copertura limitata del numero di partita IVA dei Paesi Bassi

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo di convalida del numero di partita IVA dei Paesi Bassi	Convalida checksum per il numero di partita IVA dei Paesi Bassi.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Partita IVA, part. iva, partita iva, p.IVA, p.iva</p> <p>BTW, wearde tafoege tax getal, BTW nùmer, BTW-nummer</p>

Codice di assistenza sanitaria della Nuova Zelanda (NHI)

Il codice di assistenza sanitaria della Nuova Zelanda è un identificatore alfanumerico univoco di sette caratteri assegnato a ogni persona che utilizza i servizi sanitari in Nuova Zelanda.

Il Codice di assistenza sanitaria della Nuova Zelanda (NHI) rileva una stringa alfanumerica di sette caratteri che corrisponde al formato del numero NHI.

L'identificatore di dati relativo al codice di assistenza sanitaria della Nuova Zelanda (NHI) fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di sette caratteri senza convalida. Vedere ["Copertura ampia codice di assistenza sanitaria della Nuova Zelanda \(NHI\)"](#) a pagina 1191.
- La copertura media rileva una stringa alfanumerica di sette caratteri con la convalida del checksum. Vedere ["Copertura media del codice di assistenza sanitaria della Nuova Zelanda \(NHI\)"](#) a pagina 1192.
- La copertura limitata rileva una stringa alfanumerica di sette caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata del codice di assistenza sanitaria della Nuova Zelanda \(NHI\)"](#) a pagina 1192.

Copertura ampia codice di assistenza sanitaria della Nuova Zelanda (NHI)

La copertura ampia rileva una stringa alfanumerica di sette caratteri senza convalida.

Tabella 40-594 Criterio copertura ampia codice di assistenza sanitaria della Nuova Zelanda (NHI)

Criterio
\1{3}\d{4}

La copertura ampia non include nessuno strumento di convalida.

Copertura media del codice di assistenza sanitaria della Nuova Zelanda (NHI)

La copertura media rileva una stringa alfanumerica di sette caratteri con la convalida del checksum.

Tabella 40-595 Criterio della copertura media del codice di assistenza sanitaria della Nuova Zelanda (NHI)

Criterio
\1{3}\d{4}

Tabella 40-596 Convalide della copertura media del codice di assistenza sanitaria della Nuova Zelanda (NHI)

Convalida obbligatoria	Descrizione
Controllo di convalida codice di assistenza sanitaria della Nuova Zelanda	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata del codice di assistenza sanitaria della Nuova Zelanda (NHI)

La copertura limitata rileva una stringa alfanumerica di sette caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-597 Criteri di copertura limitata del codice di assistenza sanitaria della Nuova Zelanda (NHI)

Criterio
\1{3}\d{4}

Tabella 40-598 Convalide di copertura limitata del codice di assistenza sanitaria della Nuova Zelanda (NHI)

Convalida obbligatoria	Descrizione
Controllo di convalida codice di assistenza sanitaria della Nuova Zelanda	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Controllo di convalida codice di assistenza sanitaria della Nuova Zelanda Trova parole chiave: codice di assistenza sanitaria, codice nhi, Codice NHI, n. nhi, codice NHI, cod. di assistenza sanitaria, identificativo codice di assistenza sanitaria</p>

Numero di identificazione personale norvegese

Il numero di identificazione personale norvegese viene assegnato alla nascita o al momento della registrazione all'anagrafe nazionale. Questo numero è riportato sui documenti di identità, rendendo possibile l'identificazione di una persona, ad esempio nel caso di operazioni bancarie o amministrative.

L'identificatore di dati per il Numero di identificazione personale norvegese rileva un numero di 11 cifre che corrisponde al formato del Numero di identificazione personale norvegese.

L'identificatore di dati di sistema Numero di identificazione personale norvegese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.
Vedere "[Copertura ampia del numero di identificazione personale norvegese](#)" a pagina 1194.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum.
Vedere "[Copertura media numero di identificazione personale norvegese](#)" a pagina 1194.
- La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura media numero di identificazione personale norvegese](#)" a pagina 1195.

Copertura ampia del numero di identificazione personale norvegese

La copertura ampia rileva un numero di 11 cifre senza convalida del checksum.

Tabella 40-599 Criteri di copertura ampia del numero di identificazione personale norvegese

Criterio
[01234567]\d[012345]\d[56789]\d[567]\d{4}
[01234567]\d[012345]\d\d\d[01234]\d{4}
[01234567]\d[012345]\d[456789]\d[9]\d{4}
[01234567]\d[012345]\d[0123]\d[56789]\d{4}

Tabella 40-600 Convalida di copertura ampia del numero di identificazione personale norvegese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione personale norvegese

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-601 Criteri copertura media numero di identificazione personale norvegese

Criterio
[01234567]\d[012345]\d[56789]\d[567]\d{4}
[01234567]\d[012345]\d\d\d[01234]\d{4}
[01234567]\d[012345]\d[456789]\d[9]\d{4}
[01234567]\d[012345]\d[0123]\d[56789]\d{4}

Tabella 40-602 Strumento di convalida copertura media numero di identificazione personale norvegese

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini. Il controllo di convalida del numero di identificazione personale norvegese calcola il checksum e convalida il criteri rispetto alla copertura limitata Limitato - Copertura limitata numero di identificazione personale norvegese.

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione personale norvegese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura media numero di identificazione personale norvegese

La copertura limitata rileva un numero di 11 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate al numero di identificazione personale norvegese.

Tabella 40-603 Criteri copertura media numero di identificazione personale norvegese

Criterio
[01234567]\d[012345]\d[56789]\d[567]\d{4}
[01234567]\d[012345]\d\d\d[01234]\d{4}
[01234567]\d[012345]\d[456789]\d[9]\d{4}
[01234567]\d[012345]\d[0123]\d[56789]\d{4}

Tabella 40-604 Convalide copertura media numero di identificazione personale norvegese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione personale norvegese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numero di identificazione personale norvegese, numero di identificazione, n identificazione, numidentificazioner, nidentificazione</p> <p>fødselsnummer#, fødsel nummer, Fødsel nr, fødsel nei, fødselnei#</p>

Documento di identità cinese

Il documento di identità cinese è utilizzato per la registrazione del domicilio, l'arruolamento nell'esercito, la registrazione di matrimoni/divorzi, i viaggi all'estero, la partecipazione a esami nazionali e altre questioni sociali o civili in Cina.

L'identificatore di dati per il documento di identità cinese rileva un numero di 18 cifre che corrisponde al formato del documento di identità cinese.

L'identificatore di dati Documento di identità cinese fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 18 cifre con convalida del checksum. Vedere "[Copertura ampia documento di identità cinese](#)" a pagina 1196.
- La copertura limitata rileva un numero di 18 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate al documento di identità cinese. Vedere "[Copertura limitata del documento di identità cinese](#)" a pagina 1196.

Copertura ampia documento di identità cinese

La copertura ampia rileva un numero a 18 cifre con convalida del checksum.

Tabella 40-605 Criterio copertura ampia documento di identità cinese

Criterio
\d{17}[Xx]
\d{18}

Tabella 40-606 Strumento di convalida copertura ampia documento di identità cinese

Convalida obbligatoria	Descrizione
Convalida checksum ID cinese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del documento di identità cinese

La copertura limitata rileva un numero a 18 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate al documento di identità cinese.

Tabella 40-607

Criterio
\d{17}[Xx]
\d{18}

Tabella 40-608

Strumento di convalida obbligatorio	Descrizione
Convalida checksum ID cinese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input: 身份证,居民信息,居民身份证</p> <p>Carta di identità, Informazioni del residente, Informazioni di identificazione residente</p>

Numero di carta di identità polacca

Ogni cittadino polacco che ha compiuto i 18 anni di età e che risiede in modo permanente in Polonia deve avere una carta di identità con un numero personale univoco. Tale numero viene utilizzato come strumento di identificazione in parecchi ambiti.

Il Numero di carta di identità polacca rileva una stringa alfanumerica di nove cifre che corrisponde al formato del Numero di carta di identità polacca.

L'identificatore di dati di sistema del numero di carta d'identità polacco fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di nove caratteri e cifre senza la convalida del checksum.
 Vedere "[Copertura ampia numero di carta di identità polacca](#)" a pagina 1197.
- La copertura media rileva una stringa alfanumerica di nove caratteri e cifre con la convalida del checksum.
 Vedere "[Copertura media numero di carta di identità polacca](#)" a pagina 1198.
- La copertura limitata rileva una stringa alfanumerica di nove caratteri e cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
 Vedere "[Copertura limitata numero di carta di identità polacca](#)" a pagina 1198.

Copertura ampia numero di carta di identità polacca

La copertura ampia rileva una stringa alfanumerica di nove caratteri e cifre senza la convalida del checksum.

Tabella 40-609 Criterio copertura ampia numero di carta di identità polacca

Criterio
[A-Z]{3}\d{6}

Tabella 40-610 Convalida copertura ampia numero di carta di identità polacca

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di carta di identità polacca

La copertura media rileva una stringa alfanumerica di nove caratteri e cifre con la convalida del checksum.

Tabella 40-611 Criterio di copertura media numero di carta di identità polacca

Criterio
[A-Z]{3}\d{6}

Tabella 40-612 Convalide copertura media numero di carta di identità polacca

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione polacco	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di carta di identità polacca

La copertura limitata rileva una stringa alfanumerica di nove caratteri e cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-613 Criterio copertura limitata numero di carta d'identità polacca

Criterio
[A-Z]{3}\d{6}

Tabella 40-614 Convalide copertura limitata numero di carta di identità polacca

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione polacco	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di identificazione personale, n. identità personale, numero identità univoco, n. carta identità nazionale, ID personale, identità personale, n.identitàpersonale, idunivoco, idnazionale, identitànazionale, #</p> <p>Dowód osobisty, Tożsamości narodowej, osobisty numer identyfikacyjny, niepowtarzalny numer, numer identyfikacyjny, Dowódosobisty#, niepowtarzalnynumer#</p>

Codice statistico polacco (REGON)

In Polonia ogni entità economica deve essere registrata nel Registro delle attività nazionali denominato REGON. È l'unico registro integrato del paese in cui sono elencate tutte le imprese nazionali. Ogni società ha un numero REGON univoco.

L'identificatore di dati Codice statistico polacco (REGON) rileva un numero 14 cifre che corrisponde al formato del numero REGON.

L'identificatore di dati di sistema Codice statistico polacco (REGON) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 14 cifre senza la convalida del checksum. Vedere ["Copertura ampia codice statistico polacco \(REGON\)"](#) a pagina 1200.
- La copertura media rileva un numero a 14 cifre con la convalida del checksum. Vedere ["Copertura media codice statistico polacco \(REGON\)"](#) a pagina 1200.
- La copertura limitata rileva un numero a 14 cifre con la convalida del checksum. Richiede inoltre la presenza parole chiave associate. Vedere ["Copertura limitata codice statistico polacco \(REGON\)"](#) a pagina 1200.

Copertura ampia codice statistico polacco (REGON)

La copertura ampia rileva un numero di 14 cifre senza la convalida del checksum.

Tabella 40-615 Criteri copertura ampia codice statistico polacco (REGON)

Modelli
$\backslash d\{14\}$
$\backslash d\{9\}-\backslash d\{5\}$

Tabella 40-616 Convalida copertura ampia codice statistico polacco (REGON)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media codice statistico polacco (REGON)

La copertura media rileva un numero a 14 cifre con la convalida del checksum.

Tabella 40-617 Criteri copertura media codice statistico polacco (REGON)

Modelli
$\backslash d\{14\}$
$\backslash d\{9\}-\backslash d\{5\}$

Tabella 40-618 Convalide copertura media codice statistico polacco (REGON)

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice statistico polacco (REGON)	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata codice statistico polacco (REGON)

La copertura limitata rileva un numero a 14 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-619 Criteri copertura limitata codice statistico polacco (REGON)

Modelli
\d{14}
\d{9}-\d{5}

Tabella 40-620 Convalide copertura limitata codice statistico polacco (REGON)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice statistico polacco (REGON)	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>ID REGON, numero statistico, ID statistico, n. statistico, codice REGON, idregon, IDREGON, n.regon, ID azienda, n.IDazienda, n. ID azienda, numero ID azienda, num.IDazienda, #</p> <p>numer statystyczny, REGON, numeru REGON, numerstatystyczny#, numeruREGON#</p>

Codice fiscale polacco (PESEL)

Il codice fiscale polacco (PESEL) è il numero di identificazione nazionale utilizzato in Polonia. Il numero PESEL è obbligatorio per tutte le persone residenti in modo permanente o temporaneo in Polonia. Esso identifica unicamente una persona e non può essere trasferito a un altro individuo.

L'identificatore di dati Codice fiscale polacco (PESEL) rileva un numero di 11 cifre che corrisponde al formato del PESEL.

L'identificatore di dati di sistema Codice fiscale polacco (PESEL) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum. Vedere ["Copertura ampia codice fiscale polacco \(PESEL\)"](#) a pagina 1202.

- La copertura media rileva un numero di 11 cifre con la convalida del checksum. Vedere "[Copertura media codice fiscale polacco \(PESEL\)](#)" a pagina 1202.
- La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza parole chiave associate. Vedere "[Copertura limitata del codice fiscale polacco \(PESEL\)](#)" a pagina 1202.

Copertura ampia codice fiscale polacco (PESEL)

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-621 Criterio copertura ampia codice fiscale polacco (PESEL)

Criterio

$\backslash d\{2\}[012389]\backslash d[0-3]\backslash d\{6\}$

Tabella 40-622 Convalida copertura ampia codice fiscale polacco (PESEL)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media codice fiscale polacco (PESEL)

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-623 Criterio copertura media codice fiscale polacco (PESEL)

Criterio

$\backslash d\{2\}[012389]\backslash d[0-3]\backslash d\{6\}$

Tabella 40-624 Convalida copertura media codice fiscale polacco (PESEL)

Convalida obbligatoria	Descrizione
Controllo di convalida codice fiscale polacco	Lo strumento di convalida calcola il checksum che ogni codice fiscale polacco deve superare.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del codice fiscale polacco (PESEL)

La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-625 Criteri copertura limitata del codice fiscale polacco (PESEL)

Criterio
<code>\d{2}[012389]\d[0-3]\d{6}</code>

Tabella 40-626 Convalida copertura limitata del codice fiscale polacco (PESEL)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice fiscale polacco	Lo strumento di convalida calcola il checksum che ogni codice fiscale polacco deve superare. Lo strumento di convalida calcola il checksum che ogni codice fiscale polacco deve superare.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: ID PESEL, sistema sanitario polacco, codice fiscale, cod. fiscale, numero codice fiscale, n.IDPESEL, n. pesel, codice pesel, codice di previdenza sociale PESEL Liczba, społeczny bezpieczeństwo liczba, społeczny bezpieczeństwo ID, społeczny bezpieczeństwo kod, PESELliczba#, społecznybezpieczeństwoliczba#

Numero di identificazione fiscale polacco (NIP)

Il numero di identificazione fiscale polacco (NIP) è un numero che il governo assegna a ogni cittadino polacco che lavora o svolge un'attività commerciale in Polonia. Questo codice è denominato NIP.

L'identificatore di dati per il Numero di identificazione fiscale polacco (NIP) rileva un numero 10 cifre che corrisponde al formato del NIP.

L'identificatore di dati di sistema Numero di identificazione fiscale polacco (NIP) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.
Vedere ["Copertura ampia numero di identificazione fiscale polacco \(NIP\)"](#) a pagina 1204.

- La copertura media rileva un numero a 10 cifre con la convalida del checksum.
Vedere ["Copertura media numero di identificazione fiscale polacco \(NIP\)"](#) a pagina 1204.
- La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di identificazione fiscale polacco \(NIP\)"](#) a pagina 1205.

Copertura ampia numero di identificazione fiscale polacco (NIP)

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-627 Criteri copertura ampia numero di identificazione fiscale polacco (NIP)

Criterio
$\backslash d\{10\}$
$\backslash d\{3\} [-] \backslash d\{3\} [-] \backslash d\{2\} [-] \backslash d\{2\}$
$\backslash d\{3\} [-] \backslash d\{2\} [-] \backslash d\{2\} [-] \backslash d\{3\}$

Tabella 40-628 Convalida copertura ampia numero di identificazione fiscale polacco (NIP)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione fiscale polacco (NIP)

La copertura media rileva un numero a 10 cifre con la convalida del checksum.

Tabella 40-629 Criteri copertura media numero di identificazione fiscale polacco (NIP)

Criterio
$\backslash d\{10\}$
$\backslash d\{3\} [-] \backslash d\{3\} [-] \backslash d\{2\} [-] \backslash d\{2\}$
$\backslash d\{3\} [-] \backslash d\{2\} [-] \backslash d\{2\} [-] \backslash d\{3\}$

Tabella 40-630 Strumenti di convalida copertura media numero di identificazione fiscale polacco (NIP)

Convalida obbligatoria	Descrizione
Controllo di convalida codice fiscale polacco	Lo strumento di convalida calcola il numero di checksum che ogni numero di identificazione fiscale polacco deve superare.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata numero di identificazione fiscale polacco (NIP)

La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-631 Criteri copertura limitata numero di identificazione fiscale polacco (NIP)

Criterio
$\backslash d\{10\}$
$\backslash d\{3\}[-]\backslash d\{3\}[-]\backslash d\{2\}[-]\backslash d\{2\}$
$\backslash d\{3\}[-]\backslash d\{2\}[-]\backslash d\{2\}[-]\backslash d\{3\}$

Tabella 40-632 Strumenti di convalida copertura limitata numero di identificazione fiscale polacco (NIP)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione fiscale polacco	Lo strumento di convalida calcola il numero di checksum che ogni numero di identificazione fiscale polacco deve superare.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Codice Fiscale, codice fiscale, cod. fiscale, n.codfiscale, n. codice fiscale, codicefiscale, NIP, n.NIP, identificazione fiscale, n.identificazionefiscale, TAXID#, ID NIP, n.IDNIP, n.nip, numero di identificazione fiscale, n. identificazione fiscale, numero IVA, n. IVA, vatno#, P. I.V.A., n.p.IVA#</p> <p>Numer Identyfikacji Podatkowej, Polski numer identyfikacji podatkowej, NumeridentyfikacjiPodatkowej#, NIP</p>

Numero di patente di guida portoghese

LDENT_RIGHT_SINGLE_QUOTE Istituto per la mobilità e il trasporto terrestre (IMTT) rilascia le patenti di guida in Portogallo.

L'identificatore di dati del numero di patente di guida portoghese rileva un modello alfanumerico di 8-10 caratteri che corrisponde al formato del numero di patente di guida portoghese.

L'identificatore di dati del numero di patente di guida portoghese fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 8-10 caratteri senza la convalida del checksum.
Vedere "[Copertura ampia del numero di patente di guida portoghese](#)" a pagina 1206.
- La copertura limitata rileva un modello alfanumerico di 8-10 caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.
Vedere "[Copertura limitata del numero di patente di guida portoghese](#)" a pagina 1207.

Copertura ampia del numero di patente di guida portoghese

La copertura ampia rileva un modello alfanumerico di 8-10 caratteri senza la convalida del checksum.

Tabella 40-633 Modello di copertura ampia del numero di patente di guida portoghese

Modelli
[A-Za-z]{2}-\d{5,6} \d

Modelli

[A-Za-z]-\d{6,8} \d

Tabella 40-634 Convalida di copertura ampia del numero di patente di guida portoghese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di patente di guida portoghese

La copertura limitata rileva un modello alfanumerico di 8-10 caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-635 Modelli di copertura limitata del numero di patente di guida portoghese

Modelli

[A-Za-z]{2}-\d{5,6} \d

[A-Za-z]-\d{6,8} \d

Tabella 40-636 Convalide di copertura limitata del numero di patente di guida portoghese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>N. PATENTE, n. patente, N. PATENTE DI GUIDA, pat. di guida, patente di guida, numero patente, permesso di guida, patente di guida portoghese</p> <p>carteira de motorista, carteira motorista, carteira de habilitação, carteira habilitação, número de licença, número licença, permissão de condução, permissão condução, Licença condução Portugal, carta de condução</p>

Numero di identificazione nazionale portoghese

Il numero di identificazione nazionale è un numero di identificazione univoco solitamente presente in documenti come la carta del cittadino che il governo portoghese rilascia ai propri cittadini. Può essere utilizzato come documento di viaggio all'interno dell'UE e in altri paesi europei.

L'identificatore di dati per il numero di identificazione nazionale portoghese rileva un una stringa alfanumerica di 7-9 caratteri e cifre che corrisponde al formato del numero di identificazione nazionale portoghese.

L'identificatore di dati per il numero di identificazione nazionale portoghese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 7-9 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia numero di identificazione nazionale portoghese"](#) a pagina 1208.
- La copertura media rileva un modello alfanumerico di 7-9 caratteri con la convalida del checksum.
Vedere ["Copertura media numero di identificazione nazionale portoghese"](#) a pagina 1209.
- La copertura limitata rileva un modello alfanumerico di 7-9 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di identificazione nazionale portoghese"](#) a pagina 1210.

Copertura ampia numero di identificazione nazionale portoghese

La copertura ampia rileva un modello alfanumerico di 7-9 caratteri senza la convalida del checksum.

Tabella 40-637 Criteri copertura ampia numero di identificazione nazionale portoghese

Modelli
\d{8}
\d{7} \d
\d{7}-\d
\d{9}
\d{9}\l{2}\d
\d{8} \d
\d{8}-\d

Modelli
\d{8} \d \l{2}\d
\d{8}-\d-\l{2}\d

Tabella 40-638 Convalide di copertura ampia del numero di identificazione nazionale portoghese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media numero di identificazione nazionale portoghese

La copertura media rileva un modello alfanumerico di 7-9 caratteri con la convalida del checksum.

Tabella 40-639 Criteri copertura media numero di identificazione nazionale portoghese

Modelli
\d{8}
\d{7} \d
\d{7}-\d
\d{9}
\d{9}\l{2}\d
\d{8} \d
\d{8}-\d
\d{8} \d \l{2}\d
\d{8}-\d-\l{2}\d

Tabella 40-640 Convalida copertura media numero di identificazione nazionale portoghese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione nazionale portoghese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di identificazione nazionale portoghese

La copertura limitata rileva un modello alfanumerico di 7-9 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-641 Criteri di copertura limitata numero di identificazione nazionale portoghese

Modelli
\d{8}
\d{7} \d
\d{7}-\d
\d{9}
\d{9}\l{2}\d
\d{8} \d
\d{8}-\d
\d{8} \d \l{2}\d
\d{8}-\d-\l{2}\d

Tabella 40-642 Convalide di copertura limitata numero di identificazione nazionale portoghese

Convalide obbligatorie	Descrizione
Controllo di convalida numero di identificazione nazionale portoghese	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero id, numero bi portoghese, NIC, nic, numero di documento, carta del cittadino, numero di carta di identità, n. carta di identità, numero di carta di identità nazionale, n. carta di identità nazionale, numero di identificazione nazionale, n. di identificazione nazionale, numero di identificazione, n. identificazione bilhete de identidade, número de identificação civil, número de cartão de cidadão, documento de identificação, cartão de cidadão, número bi de portugal, número do documento</p>
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Numero di passaporto portoghese

Il passaporto portoghese viene rilasciato ai cittadini portoghesi per viaggiare all'estero. Il passaporto, insieme alla carta di identità nazionale, dà diritto di movimento e residenza liberi in uno qualsiasi degli stati dell'IDENT_RIGHT_SINGLE_QUOTEUnione Europea e dello Spazio Economico Europeo.

L'identificatore di dati per il numero di passaporto portoghese rileva una stringa alfanumerica di sette cifre che corrisponde al formato del numero di passaporto portoghese.

L'identificatore di dati del numero di passaporto portoghese fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di sette caratteri senza convalida. Vedere ["Copertura ampia del numero di passaporto portoghese"](#) a pagina 1211.
- La copertura limitata rileva un modello alfanumerico di sette caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate. Vedere ["Copertura limitata del numero di passaporto portoghese"](#) a pagina 1212.

Copertura ampia del numero di passaporto portoghese

La copertura ampia rileva un modello alfanumerico di sette caratteri senza convalida.

Tabella 40-643 Numero di passaporto portoghese

Criterio
[a-zA-Z]\d{6}

Copertura limitata del numero di passaporto portoghese

La copertura limitata rileva un modello alfanumerico di sette caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-644 Modelli di copertura limitata del numero di passaporto portoghese

Criterio
[a-zA-Z]\d{6}

Tabella 40-645 Convalide di copertura limitata del numero di passaporto portoghese

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero passaporto, passaporto, n. passaporto, passaporte, passeport, portoghese passport, portoghese passeport, portoghese passaporte, passaporte n°, passeport n°
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Numero di identificazione fiscale portoghese

Un codice fiscale è un numero di identificazione fiscale rilasciato in Portogallo a chiunque desideri intraprendere qualsiasi attività ufficiale in Portogallo.

L'identificatore di dati del numero di identificazione fiscale portoghese rileva un numero di nove cifre nel formato del numero di identificazione fiscale portoghese.

L'identificatore di dati del numero di identificazione fiscale portoghese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione fiscale portoghese"](#) a pagina 1213.

- La copertura media rileva un numero di nove cifre con la convalida del checksum.
Vedere ["Copertura media del numero di identificazione fiscale portoghese"](#) a pagina 1213.
- La copertura limitata rileva un numero a nove cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di identificazione fiscale portoghese"](#) a pagina 1214.

Copertura ampia del numero di identificazione fiscale portoghese

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-646 Modelli di copertura ampia del numero di identificazione fiscale portoghese

Modelli
$\backslash d\{9\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$

Tabella 40-647 Convalide di copertura ampia del numero di identificazione fiscale portoghese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione fiscale portoghese

La copertura media rileva un numero di nove cifre con la convalida del checksum.

Tabella 40-648 Modelli di copertura media del numero di identificazione fiscale portoghese

Modelli
$\backslash d\{9\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$

Modelli
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$

Tabella 40-649 Convalida di copertura media del numero di identificazione fiscale portoghese

Strumento di convalida obbligatorio	Descrizione
Escludi caratteri finali	I numeri con i seguenti caratteri finali verranno esclusi dalla corrispondenza:: 000000000,111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999
Controllo di convalida del numero di identificazione fiscale e IVA portoghese	Calcola il checksum e lo utilizza per convalidare la corrispondenza.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero di identificazione fiscale portoghese

La copertura limitata rileva un numero a nove cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-650 Modelli di copertura limitata del numero di identificazione fiscale portoghese

Modelli
$\backslash d\{9\}$
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{3\}$
$\backslash d\{3\} \backslash d\{3\} \backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{3\}$

Tabella 40-651 Convalide di copertura limitata del numero di identificazione fiscale portoghese

Strumento di convalida obbligatorio	Descrizione
Escludi caratteri finali	I numeri con i seguenti caratteri finali verranno esclusi dalla corrispondenza:: 000000000,111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida del numero di identificazione fiscale e IVA portoghese	Calcola il checksum e lo utilizza per convalidare la corrispondenza.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: N.TIN, N.NIF, codice fiscale, codice fiscale contribuente, numero id fiscale, num. id fiscale, id fiscale CPF, CPF#, NIF, número identificação fiscal
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Numero di partita IVA portoghese

L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.

L'identificatore di dati della partita IVA portoghese rileva un modello alfanumerico di 11 caratteri che corrisponde al formato del numero di partita IVA portoghese.

L'identificatore di dati della partita IVA portoghese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 11 caratteri che inizia con **PT** ed è seguito da nove cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di partita IVA portoghese"](#) a pagina 1216.
- La copertura media rileva un modello alfanumerico di 11 caratteri che inizia con **PT** ed è seguito da nove cifre con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA portoghese"](#) a pagina 1216.
- La copertura limitata rileva un modello alfanumerico di 11 caratteri che inizia con **PT** ed è seguito da nove cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di partita IVA portoghese"](#) a pagina 1217.

Copertura ampia del numero di partita IVA portoghese

La copertura ampia rileva un modello alfanumerico di 11 caratteri che inizia con **PT** ed è seguito da nove cifre senza la convalida del checksum.

Tabella 40-652 Modelli di copertura ampia del numero di partita IVA portoghese

Modelli
[Pp] [Tt] \d{9}
[Pp] [Tt] \d{9}
[Pp] [Tt] -\d{9}
[Pp] [Tt] \d{3} \d{4} \d{2}
[Pp] [Tt] \d{3} -\d{3} -\d{3}
[Pp] [Tt] \d{3} \d{3} \d{3}

Tabella 40-653 Convalide di copertura ampia del numero di partita IVA portoghese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	I numeri con i seguenti caratteri finali verranno esclusi dalla corrispondenza:: 00000000,11111111, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 88888888, 99999999

Copertura media del numero di partita IVA portoghese

La copertura media rileva un modello alfanumerico di 11 caratteri che inizia con **PT** ed è seguito da nove cifre con la convalida del checksum.

Tabella 40-654 Modelli di copertura media del numero di partita IVA portoghese

Modelli
[Pp] [Tt] \d{9}
[Pp] [Tt] \d{9}
[Pp] [Tt] -\d{9}

Modelli
[Pp] [Tt] \d{3} \d{4} \d{2}
[Pp] [Tt] \d{3}-\d{3}-\d{3}
[Pp] [Tt] \d{3} \d{3} \d{3}

Tabella 40-655 Convalida di copertura media del numero di partita IVA portoghese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida del numero di identificazione fiscale e IVA portoghese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di partita IVA portoghese

La copertura limitata rileva un modello alfanumerico di 11 caratteri che inizia con PT ed è seguito da nove cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-656 Modelli di copertura limitata del numero di partita IVA portoghese

Modelli
[Pp] [Tt] \d{9}
[Pp] [Tt] \d{9}
[Pp] [Tt] -\d{9}
[Pp] [Tt] \d{3} \d{4} \d{2}
[Pp] [Tt] \d{3}-\d{3}-\d{3}
[Pp] [Tt] \d{3} \d{3} \d{3}

Tabella 40-657 Convalide di copertura limitata del numero di partita IVA portoghese

Convalide obbligatorie	Descrizione
Controllo di convalida del numero di identificazione fiscale e IVA portoghese	Calcola il checksum e lo utilizza per convalidare il modello.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di partita iva portoghese, num iva portoghese, n. partita iva, NUPC n. iva, iva, n. IVA, codice iva, numero imposta valore aggiunto, id iva, numero di registrazione iva, imposta sul valore aggiunto, n. registrazione iva</p> <p>imposto sobre valor acrescentado, VAT nº, número iva, vat não, cuba, código iva</p>
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	<p>I numeri con i seguenti caratteri finali verranno esclusi dalla corrispondenza::</p> <p>000000000,111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999</p>

Social Security Number (SSN) statunitense randomizzato

L'identificatore dati **Social Security Number (SSN) statunitense randomizzato** rileva numeri a 9 cifre nel formato DDD-DD-DDDD, con trattini o spazi di separazione o senza separatori. Il numero deve essere compreso negli intervalli numerici assegnati validi. Le convalide criteri eliminano i numeri di prova comuni, quali 123456789 o quelli con tutte le cifre uguali. L'identificatore dati presenta una copertura limitata e richiede inoltre la presenza di una parola chiave correlata all'SSN.

In Symantec Data Loss Prevention versione 12.5 l'identificatore dati Social Security Number (SSN) statunitense randomizzato sostituisce l'identificatore dati Social Security Number (SSN) statunitense. Tutti i modelli di politica che utilizzavano l'identificatore dati Social Security Number (SSN) statunitense vengono aggiornati all'utilizzo dell'identificatore dati Social Security Number (SSN) statunitense randomizzato. Inoltre nella versione 14.0 i criteri e le convalide per l'identificatore dati Social Security Number (SSN) statunitense randomizzato sono stati aggiornati rispetto alla versione 12.5. Symantec consiglia di aggiornare le politiche per utilizzare l'identificatore dati Social Security Number (SSN) statunitense randomizzato versione 14.0 o successiva.

Vedere ["Aggiornamento delle politiche per l'utilizzo dell'identificatore dati Social Security Number \(SSN\) statunitense randomizzato"](#) a pagina 747.

Vedere ["Utilizzo dell'identificatore dati Social Security Number \(SSN\) statunitense randomizzato per rilevare i numeri di previdenza sociale"](#) a pagina 769.

L'identificatore dati Social Security Number (SSN) statunitense randomizzato fornisce due coperture di rilevamento.

- La copertura media rileva un numero a 9 cifre nel formato DDD-DD-DDDD. Le cifre devono trovarsi in intervalli di numeri assegnati.
Vedere ["Copertura media Social Security Number \(SSN\) statunitense randomizzato"](#) a pagina 1219.
- La copertura limitata rileva un numero a 9 cifre nel formato DDD-DD-DDDD. Le cifre devono trovarsi in intervalli di numeri assegnati. Richiede inoltre la presenza di parole chiave associate al SSN.
Vedere ["Copertura limitata Social Security Number \(SSN\) statunitense randomizzato"](#) a pagina 1220.

Copertura media Social Security Number (SSN) statunitense randomizzato

La copertura media rileva un numero a 9 cifre nel formato DDD-DD-DDDD. Le cifre devono trovarsi in intervalli di numeri assegnati.

Tabella 40-658 Criteri e normalizzatore copertura media Stati Uniti SSN randomizzati

Componente	Valore	Descrizione
Criteri	<div>[0-8]\d{2} \d{1} [1-9] \d{4}</div> <div>[0-8]\d{3} [1-9]\d{4}</div> <div>[0-8]\d{2} [1-9]\d{5}</div> <div>[0-8]\d{2}-\d{1} [1-9]-\d{4}</div> <div>[0-8]\d{2} [1-9]\d{1} \d{4}</div> <div>[0-8]\d{2}-[1-9]\d{1}-\d{4}</div>	Rileva numeri a 9 cifre nel formato DDD-DD-DDDD, separati da trattini o spazi oppure senza separazione. Il numero deve essere compreso negli intervalli numerici assegnati validi
Normalizzatore di dati	Cifre	Vedere "Informazioni sui normalizzatori di dati" a pagina 696.

Tabella 40-659 Strumenti di convalida e input copertura media Stati Uniti SSN randomizzati

Convalide attive	Input (se presenti)	Descrizione
Escludi caratteri iniziali	666, 000, 123456789, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888	Vedere "Utilizzo delle convalide criterio" a pagina 755.
Delimitatore numero		
Escludi caratteri finali	0000	
Controllo di convalida casuale del numero di previdenza sociale statunitense		Calcola il checksum e lo utilizza per convalidare il criterio.

Copertura limitata Social Security Number (SSN) statunitense randomizzato

La copertura limitata rileva un numero a 9 cifre nel formato DDD-DD-DDDD. Le cifre devono trovarsi in intervalli di numeri assegnati. Richiede inoltre la presenza di parole chiave associate al SSN.

Tabella 40-660 Criteri copertura limitata Social Security Number (SSN) statunitense randomizzato

Criterio
[0-8]\d{2} \d{1}[1-9] \d{4}
[0-8]\d{3}[1-9]\d{4}
[0-8]\d{2}[1-9]\d{5}
[0-8]\d{2}-\d{1}[1-9]-\d{4}
[0-8]\d{2} [1-9]\d{1} \d{4}
[0-8]\d{2}-[1-9]\d{1}-\d{4}

Tabella 40-661

Convalida	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalida	Descrizione
Escludi caratteri iniziali	Esclude i seguenti caratteri iniziali: 666, 000, 123456789, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888
Escludi caratteri finali	Esclude i seguenti caratteri finali: 0000
Trova parole chiave	Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: codice fiscale, cod. fisc., cf#
Controllo di convalida casuale del numero di previdenza sociale statunitense	Calcola il checksum e lo utilizza per convalidare il criterio.

Numero di identificazione nazionale rumeno

A ogni cittadino rumeno viene assegnato un codice numerico personale (Cod Numeric Personal, CNP) come numero univoco di identificazione nazionale. Questo numero viene anche utilizzato come numero di identificazione fiscale per scopi finanziari.

L'identificatore di dati numero di identificazione nazionale rumeno rileva un numero di 13 cifre che corrisponde al formato CNP.

L'identificatore di dati per il numero di identificazione nazionale rumeno fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di identificazione nazionale rumeno"](#) a pagina 1221.
- La copertura media rileva un numero a 13 cifre con la convalida del checksum. Vedere ["Copertura media del numero di identificazione nazionale rumeno"](#) a pagina 1222.
- La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata numero di identificazione nazionale rumeno"](#) a pagina 1222.

Copertura ampia del numero di identificazione nazionale rumeno

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-662 Modello di copertura ampia del numero di identificazione nazionale rumeno

Criterio
\d{13}

Tabella 40-663 Convalide di copertura ampia del numero di identificazione nazionale rumeno

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione nazionale rumeno

La copertura media rileva un numero a 13 cifre con la convalida del checksum.

Tabella 40-664 Modello di copertura media del numero di identificazione nazionale rumeno

Criterio
\d{13}

Tabella 40-665 Convalida di copertura media del numero di identificazione nazionale rumeno

Strumento di convalida obbligatorio	Descrizione
Controllo del numero di identificazione nazionale rumeno	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di identificazione nazionale rumeno

La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-666 Modello di copertura limitata del numero di identificazione nazionale rumeno

Criterio
\d{13}

Tabella 40-667 Convalide di copertura limitata del numero di identificazione nazionale rumeno

Convalide obbligatorie	Descrizione
Controllo del numero di identificazione nazionale rumeno	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di identificazione fiscale rumeno, numero di identificazione fiscale, tin, n.tin, numero tin, n. tin, numărul de identificare fiscală, identificarea fiscală nr #, codul fiscal nr.</p> <p>ID nazionale, n. ID nazionale, n. ID, numero di identificazione nazionale, Cod Numeric Personal, cnp, CNP</p>

Numero di identificazione personale rumeno (CNP)

A ogni cittadino rumeno viene assegnato un numero di identificazione personale. Tale numero è utilizzato come strumento di riconoscimento da autorità, assistenza sanitaria, scuole, università, banche e compagnie di assicurazione.

L'identificatore di dati per il Numero di identificazione personale rumeno (CNP) rileva un numero 13 cifre che corrisponde al formato del CNP.

L'identificatore di dati di sistema del numero di identificazione personale rumeno (CNP) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum. Vedere "[Copertura ampia del numero di identificazione personale rumeno \(CNP\)](#)" a pagina 1224.
- La copertura media rileva un numero a 13 cifre con la convalida del checksum. Vedere "[Copertura media numero di identificazione personale rumeno \(CNP\)](#)" a pagina 1224.
- La copertura limitata rileva un numero di 13 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate al CNP. Vedere "[Copertura limitata numero di identificazione personale rumeno \(CNP\)](#)" a pagina 1224.

Copertura ampia del numero di identificazione personale rumeno (CNP)

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-668 Criterio di copertura ampia del numero di identificazione personale rumeno (CNP)

Criterio
<code>[1-9]\d\d[0-1]\d[0-3]\d{7}</code>

Tabella 40-669 Convalida di copertura ampia del numero di identificazione personale rumeno (CNP)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione personale rumeno (CNP)

La copertura media rileva un numero a 13 cifre con la convalida del checksum.

Tabella 40-670 Criterio copertura media numero di identificazione personale rumeno (CNP)

Criterio
<code>[1-9]\d\d[0-1]\d[0-3]\d{7}</code>

Tabella 40-671 Convalida copertura media numero di identificazione personale rumeno (CNP)

Convalida obbligatoria	Descrizione
Controllo numero di identificazione personale rumeno	Lo strumento di convalida calcola il numero di checksum che ogni numero di identificazione personale rumeno (CNP) deve superare.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata numero di identificazione personale rumeno (CNP)

La copertura limitata rileva un numero di 13 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-672 Criterio copertura limitata numero di identificazione personale rumeno (CNP)

Criterio
[1-9]\d\d[0-1]\d[0-3]\d{7}

Tabella 40-673 Strumenti di convalida copertura limitata numero di identificazione personale rumeno (CNP)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo numero di identificazione personale rumeno	Lo strumento di convalida calcola il checksum che ogni numero di identificazione personale rumeno (CNP) deve superare.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: numero di identificazione personale, numero di identificazione unico, CNP, n.CNP, PIN, n.PIN, numero di assicurazione, numeroassicurazione, numero identità unico, numidentitaunico, num. id. personale, cod identificare personal,cod unic identificare,număr personal unic,număr identitate,număr identificare personal, număridentitate#, CodNumericPersonal#, numărpersonalunic#

Numero di passaporto russo interno

In Russia esistono due tipi di passaporti: quello interno e quello internazionale. Ogni cittadino russo dispone di un passaporto interno. Esso è il documento principale utilizzato per l'identificazione personale.

L'identificatore di dati per il Numero di passaporto russo interno rileva un numero 10 cifre che corrisponde al formato del Numero di passaporto russo interno.

L'identificatore di dati del numero di identificazione del passaporto russo fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum. Vedere ["Copertura ampia numero di passaporto russo interno"](#) a pagina 1226.

- La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero di passaporto russo interno](#)" a pagina 1226.

Copertura ampia numero di passaporto russo interno

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-674 Criteri copertura ampia numero di passaporto russo interno

Criterio
$\backslash d\{10\}$
$\backslash d\{4\}[]\backslash d\{6\}$
$\backslash d\{2\}[-]\backslash d\{2\}[]\backslash d\{6\}$

Tabella 40-675 Convalida copertura ampia numero di passaporto russo interno

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata numero di passaporto russo interno

La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-676 Criteri copertura limitata numero di passaporto russo interno

Criterio
$\backslash d\{10\}$
$\backslash d\{4\}[]\backslash d\{6\}$
$\backslash d\{2\}[-]\backslash d\{2\}[]\backslash d\{6\}$

Tabella 40-677 Convalide copertura limitata numero di passaporto russo interno

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Se si seleziona questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero passaporto, n passaporto, ID passaporto, numeropassaporto, n.passaporto, ID passaporto russo, паспорт нет, паспорт, номер паспорта, паспорт ID, Российской паспорт, Русский номер паспорта, паспорт#, паспортID#, номерпаспорта#</p>

Numero di identificazione fiscale russo (INN)

Il numero di identificazione fiscale russo (TIN or INN) è un numero a più cifre che consente al fisco di identificare la condizione fiscale di individui ed entità legali.

L'identificatore di dati per il Numero di identificazione fiscale russo (INN) rileva un numero di 10 o 12 cifre che corrisponde al formato del Numero di identificazione fiscale russo (INN).

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 10 o 12 cifre senza la convalida del checksum. Vedere ["Copertura ampia numero di identificazione fiscale russo \(INN\)"](#) a pagina 1227.
- La copertura media convalida il numero rilevato utilizzando la cifra di controllo finale ed elimina i numeri di prova comuni. Vedere ["Copertura media numero di identificazione fiscale russo \(INN\)"](#) a pagina 1228.
- La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata numero di identificazione fiscale russo \(INN\)"](#) a pagina 1228.

Copertura ampia numero di identificazione fiscale russo (INN)

La copertura ampia rileva un numero di 10 o 12 cifre senza la convalida del checksum.

Tabella 40-678 Criteri copertura ampia numero di identificazione fiscale russo (INN)

Criterio
$\backslash d\{10\}$
$\backslash d\{12\}$
$\backslash d\{3\} [-] \backslash d\{3\} [-] \backslash d\{3\} [-] \backslash d\{3\}$

Tabella 40-679 Convalida copertura ampia numero di identificazione fiscale russo (INN)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione fiscale russo (INN)

La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum.

Tabella 40-680 Criteri copertura media numero di identificazione fiscale russo (INN)

Criterio
$\backslash d\{10\}$
$\backslash d\{12\}$
$\backslash d\{3\}[-]\backslash d\{3\}[-]\backslash d\{3\}[-]\backslash d\{3\}$

Tabella 40-681 Strumenti di convalida copertura media numero di identificazione fiscale russo (INN)

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione fiscale russo	Lo strumento di convalida calcola il checksum che ogni numero di identificazione fiscale russo (INN) deve superare.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata numero di identificazione fiscale russo (INN)

La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-682 Criteri copertura limitata numero di identificazione fiscale russo

Criterio
$\backslash d\{10\}$
$\backslash d\{12\}$
$\backslash d\{3\}[-]\backslash d\{3\}[-]\backslash d\{3\}[-]\backslash d\{3\}$

Tabella 40-683 Convalide copertura limitata numero di identificazione fiscale russo (INN)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione fiscale russo	Lo strumento di convalida calcola il checksum che ogni numero di identificazione fiscale russo (INN) deve superare.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	<p>Se si seleziona questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>TIN, numero di identificazione fiscale, ID fiscale, num. identificazione fiscale, ID fiscale, tin, num.tin, num-tin, inn, n.inn, num.id.fiscale, id.fiscale, n.id.fiscale, n.id.fisc., НДС, номер налогоплательщика, Налогоплательщика ИД, налог число, налогчисло#, ИНН#, НДС#</p>

Identificatore di dati NRIC Singapore

L'NRIC (National Registration Identity Card, carta di identità di registrazione nazionale) è il documento d'identità utilizzato a Singapore. L'NRIC è obbligatorio per alcune procedure governative, per transazioni commerciali quali l'apertura di un conto bancario o per ottenere il rilascio di un pass di accesso ad alcuni locali previa consegna di detto documento.

La copertura ampia dell'identificatore di dati NRIC Singapore rileva nove caratteri nel criterio LDDDDDDDL. L'ultimo carattere viene utilizzato per convalidare il checksum.

Tabella 40-684 Criterio copertura ampia NRIC Singapore

Criterio
[SFTGsftg]\d{7}\w

Tabella 40-685 Convalida copertura ampia NRIC Singapore

Convalida obbligatoria	Descrizione
NRIC Singapore	Calcola il checksum del numero NRIC di Singapore e lo utilizza per convalidare il modello.

Numero di identificazione nazionale slovacco

In Slovacchia, le carte di identità sono rilasciate dalle autorità statali a ogni cittadino all'età di 15 anni. Questo numero viene utilizzato nella Repubblica Slovacca come principale identificatore univoco di ogni persona da istituzioni governative, banche e così via.

L'identificatore di dati del numero di identificazione nazionale slovacco rileva una stringa alfanumerica di 8 caratteri o un numero di 9 o 10 cifre che corrisponde al formato del numero di identificazione nazionale slovacco.

L'identificatore di dati per il numero di identificazione nazionale slovacco fornisce tre coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 8 caratteri o un numero di 9 o 10 cifre senza la convalida del checksum.
Vedere "[Copertura ampia del numero di identificazione nazionale slovacco](#)" a pagina 1230.
- La copertura media rileva una stringa alfanumerica di 8 caratteri o un numero di 9 o 10 cifre con la convalida del checksum.
Vedere "[Copertura media del numero di identificazione nazionale slovacco](#)" a pagina 1231.
- La copertura limitata rileva una stringa alfanumerica di 8 caratteri o un numero di 9 o 10 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero di identificazione nazionale slovacco](#)" a pagina 1232.

Copertura ampia del numero di identificazione nazionale slovacco

La copertura ampia rileva una stringa alfanumerica di 8 caratteri o un numero di 9 o 10 cifre senza la convalida del checksum.

Tabella 40-686 Criteri copertura ampia numero di identificazione nazionale slovacco

Modelli
$\backslash d\{10\}$
$\backslash d\{9\}$
$[A-Za-z]\{2\} \backslash d\{6\}$

Modelli
$[A-Za-z]\{2\}/\backslash d\{6\}$
$[A-Za-z]\{2\}/\backslash d\{6\}$
$\backslash d\{6\}/\backslash d\{3\}$
$\backslash d\{6\}-\backslash d\{3\}$
$\backslash d\{6\} \backslash d\{3\}$
$\backslash d\{6\}/\backslash d\{4\}$
$\backslash d\{6\}-\backslash d\{4\}$
$\backslash d\{6\} \backslash d\{4\}$

Tabella 40-687 Convalide di copertura ampia del numero di identificazione nazionale slovacco

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura media del numero di identificazione nazionale slovacco

La copertura media rileva una stringa alfanumerica di 8 caratteri o un numero di 9 o 10 cifre con la convalida del checksum.

Tabella 40-688 Criteri copertura media numero di identificazione nazionale slovacco

Modelli
$\backslash d\{10\}$
$\backslash d\{9\}$
$[A-Za-z]\{2\} \backslash d\{6\}$
$[A-Za-z]\{2\}/\backslash d\{6\}$
$[A-Za-z]\{2\}/\backslash d\{6\}$
$\backslash d\{6\}/\backslash d\{3\}$
$\backslash d\{6\}-\backslash d\{3\}$

Modelli
$\backslash d\{6\} \backslash d\{3\}$
$\backslash d\{6\} / \backslash d\{4\}$
$\backslash d\{6\} - \backslash d\{4\}$
$\backslash d\{6\} \backslash d\{4\}$

Tabella 40-689 Convalide di copertura media del numero di identificazione nazionale slovacco

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione nazionale slovacco	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di identificazione nazionale slovacco

La copertura limitata rileva una stringa alfanumerica di 8 caratteri o un numero di 9 o 10 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-690 Criteri di copertura limitata numero di identificazione nazionale slovacco

Modelli
$\backslash d\{10\}$
$\backslash d\{9\}$
$[A-Za-z]\{2\} \backslash d\{6\}$
$[A-Za-z]\{2\} / \backslash d\{6\}$
$[A-Za-z]\{2\} / \backslash d\{6\}$
$\backslash d\{6\} / \backslash d\{3\}$
$\backslash d\{6\} - \backslash d\{3\}$
$\backslash d\{6\} \backslash d\{3\}$
$\backslash d\{6\} / \backslash d\{4\}$
$\backslash d\{6\} - \backslash d\{4\}$

Modelli

\d{6} \d{4}

Tabella 40-691 Convalide di copertura limitata del numero di identificazione nazionale slovacco

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione nazionale slovacco	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	<p>Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti quando si utilizza questa opzione.</p> <p>Input:</p> <p>numero id, numero di carta di identità, numero di carta di identità nazionale, n. carta di identità nazionale, numero di identificazione nazionale, n. di identificazione nazionale, numero di identificazione, n. identificazione</p> <p>identifikačné číslo, személyi igazolvány száma, személyigazolvány szám, číslo občianskeho preukazu, identifikačná karta č, személyi igazolvány szám, nemzeti személyi igazolvány száma, číslo národnej identifikačnej karty, národná identifikačná karta č, nemzeti személyazonosító igazolvány, nemzeti azonosító szám, národné identifikačné číslo, národná identifikačná značka č, nemzeti azonosító szám, azonosító szám, identifikačné číslo, rodné číslo, RČ</p>
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Numero identificativo cittadini della Slovenia

Il numero identificativo dei cittadini è un numero di identificazione univoco assegnato a tutti i cittadini sloveni alla nascita o all'acquisizione della cittadinanza.

Il numero identificativo dei cittadini della Slovenia rileva un numero di 13 cifre che corrisponde al formato del numero identificativo dei cittadini della Slovenia.

L'identificatore di dati del numero identificativo dei cittadini della Slovenia fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero identificativo cittadini della Slovenia"](#) a pagina 1234.
- La copertura media rileva un numero a 13 cifre con la convalida del checksum.
Vedere ["Copertura media del numero identificativo dei cittadini della Slovenia"](#) a pagina 1234.
- La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero identificativo dei cittadini della Slovenia"](#) a pagina 1235.

Copertura ampia del numero identificativo cittadini della Slovenia

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-692 Modello di copertura ampia del numero identificativo dei cittadini della Slovenia

Criterio
$\backslash d\{7\}[05]\backslash d\{5\}$

Tabella 40-693 Convalide di copertura ampia del numero identificativo dei cittadini della Slovenia

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura media del numero identificativo dei cittadini della Slovenia

La copertura media rileva un numero a 13 cifre con la convalida del checksum.

Tabella 40-694 Modello di copertura media del numero identificativo dei cittadini della Slovenia

Criterio
$\backslash d\{7\}[05]\backslash d\{5\}$

Tabella 40-695 Convalida di copertura media del numero identificativo dei cittadini della Slovenia

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero identificativo cittadini della Slovenia	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero identificativo dei cittadini della Slovenia

La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-696 Modello di copertura limitata del numero identificativo dei cittadini della Slovenia

Criterio
<code>\d{7}[05]\d{5}</code>

Tabella 40-697 Convalide di copertura limitata del numero identificativo dei cittadini della Slovenia

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo di convalida numero identificativo cittadini della Slovenia	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	<p>Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti quando si utilizza questa opzione.</p> <p>Input:</p> <p>numero identificativo dei cittadini univoco, numero identificativo univoco, numero id univoco, numero identificativo dei cittadini</p> <p>EMŠO, emšo, edinstvena številka državljana, enotna identifikacijska številka, Enotna maticna številka obcana, enotna maticna številka obcana, številka državljana, edinstvena identifikacijska številka</p>

Numero di identificazione personale sudafricano

Ogni cittadino sudafricano ha un numero di identificazione nazionale. Tale numero viene soprattutto utilizzato come prova dell'identificazione.

Il Numero di identificazione personale sudafricano rileva un numero di 13 cifre che corrisponde al formato del Numero di identificazione personale sudafricano.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.
Vedere "[Copertura ampia numero di identificazione personale sudafricano](#)" a pagina 1236.
- La copertura media rileva un numero a 13 cifre con la convalida del checksum.
Vedere "[Copertura media numero di identificazione personale sudafricano](#)" a pagina 1236.
- La copertura limitata rileva un numero di 13 cifre che supera la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di identificazione personale sudafricano](#)" a pagina 1237.

Copertura ampia numero di identificazione personale sudafricano

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-698 Criteri copertura ampia numero di identificazione personale sudafricano

Modelli
[0123678]\d{8}
[0123678]\d{3}-\d{4}-\d

Tabella 40-699 Convalida copertura ampia numero di identificazione personale sudafricano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione personale sudafricano

La copertura media rileva un numero a 13 cifre con la convalida del checksum.

Tabella 40-700 Criteri copertura media numero di identificazione personale sudafricano

Modelli
\d{6}[-]\d{4}[-][01]\d{2}
\d{10}[01]\d{2}

Tabella 40-701 Convalide copertura media numero di identificazione personale sudafricano

Convalide obbligatorie	Descrizione
Controllo di convalida numero di identificazione personale sudafricano	La convalida calcola il checksum che ogni numero di identificazione personale sudafricano deve superare.

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata del numero di identificazione personale sudafricano

La copertura limitata rileva un numero di 13 cifre che supera la convalida del checksum.
 Richiede inoltre la presenza di parole chiave associate.

Tabella 40-702 Criteri della copertura limitata del numero di identificazione personale sudafricano

Modelli
$\{6\}[-]\{4\}[-][01]\{2\}$
$\{10\}[01]\{2\}$

Tabella 40-703 Convalide della copertura limitata del numero di identificazione personale sudafricano

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione personale sudafricano	La convalida calcola il checksum che ogni numero di identificazione personale sudafricano deve superare.
Trova parole chiave	<p>Se si seleziona questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero di identificazione nazionale, numero di identità nazionale, numero di previdenza sociale nazionale, numero di identità personale, numero di identificazione personale, numero di assicurazione, n.identitànazionale, n.identitàpersonale, numero di identità univoco, n.identitàunivoco, #</p> <p>nasionale identifikasie nommer, nasionale identiteitsnommer, versekering aantal, persoonlike identiteitsnommer, unieke identiteitsnommer, identiteitsnommer, identiteitsnommer#, versekeringaantal#, nasionaleidentiteitsnommer#</p>

Numero di patente di guida spagnola

Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Spagna.

L'identificatore di dati del numero di patente di guida spagnola rileva un modello alfanumerico di 9 caratteri che corrisponde al formato del numero di patente di guida spagnola.

L'identificatore di dati del numero di patente di guida spagnola fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di nove caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura ampia del numero di patente di guida spagnola](#)" a pagina 1238.
- La copertura limitata rileva un modello alfanumerico di nove caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di patente di guida spagnola](#)" a pagina 1239.

Copertura ampia del numero di patente di guida spagnola

La copertura ampia rileva un modello alfanumerico di nove caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-704 Modello di copertura ampia del numero di patente di guida spagnola

Modelli
<code>\d{8}\w</code>
<code>\d{8}[-]\w</code>
<code>\d{8}[][-]\w</code>
<code>\d{8}[][-][]\w</code>

Tabella 40-705 Convalide di copertura ampia del numero di patente di guida spagnola

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>N.PG, num.PG, n.pg, pat. guida, patente guida, patente di guida, numero patente di guida, numero di patente di guida</p> <p>permiso de conducción, permiso conducción, Número licencia conducir, Número de carnet de conducir, Número carnet conducir, licencia conducir, Número de permiso de conducir, Número de permiso conducir, Número permiso conducir, permiso conducir, licencia de manejo, el carnet de conducir, carnet conducir</p>

Copertura limitata del numero di patente di guida spagnola

La copertura limitata rileva un modello alfanumerico di nove caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-706 Modelli di copertura limitata del numero di patente di guida spagnola

Modelli
<code>\d{8}\w</code>
<code>\d{8}[-]\w</code>
<code>\d{8}[-][-]\w</code>
<code>\d{8}[-][-][-]\w</code>

Tabella 40-707 Convalide di copertura limitata del numero di patente di guida spagnola

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Verifica chiave di controllo DNI	Calcola la chiave di controllo e ne verifica la validità.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>N.PG, num.PG, n.pg, pat. guida, patente guida, patente di guida, numero patente di guida, numero di patente di guida</p> <p>permiso de conducción, permiso conducción, Número licencia conducir, Número de carnet de conducir, Número carnet conducir, licencia conducir, Número de permiso de conducir, Número de permiso conducir, Número permiso conducir, permiso conducir, licencia de manejo, el carnet de conducir, carnet conducir</p>

Numero di partita IVA spagnolo

L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. L'IVA in Spagna è controllata dall'ente statale di amministrazione fiscale.

L'identificatore di dati del numero di partita IVA spagnolo rileva un modello alfanumerico di 11 caratteri che corrisponde al formato del codice di partita IVA spagnolo.

L'identificatore di dati del numero di partita IVA spagnolo fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 11 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia del numero di partita IVA spagnolo"](#) a pagina 1240.
- La copertura media rileva un modello alfanumerico di 11 caratteri con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA spagnolo"](#) a pagina 1241.
- La copertura limitata rileva un modello alfanumerico di 11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di partita IVA spagnolo"](#) a pagina 1242.

Copertura ampia del numero di partita IVA spagnolo

La copertura ampia rileva un modello alfanumerico di 11 caratteri senza la convalida del checksum.

Tabella 40-708 Modelli di copertura ampia del numero di partita IVA spagnolo

Modelli
[Ee] [Ss] [0-9A-Za-z] \d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] \d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} . \d{3} . \d{2} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} , \d{3} , \d{2} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} /\d{5} [0-9A-Za-z]

Tabella 40-709 Convalide di copertura ampia del numero di partita IVA spagnolo

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	Esclude i numeri che terminano con i seguenti caratteri dalla corrispondenza: 000000000, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999

Copertura media del numero di partita IVA spagnolo

La copertura media rileva un modello alfanumerico di 11 caratteri con la convalida del checksum.

Tabella 40-710 Modelli di copertura media del numero di partita IVA spagnolo

Modelli
[Ee] [Ss] [0-9A-Za-z] \d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] \d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} . \d{3} . \d{2} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} , \d{3} , \d{2} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} /\d{5} [0-9A-Za-z]

Tabella 40-711 Convalida di copertura media del numero di partita IVA spagnolo

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA spagnolo	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di partita IVA spagnolo

La copertura limitata rileva un modello alfanumerico di 11 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-712 Modelli di copertura limitata del numero di partita IVA spagnolo

Modelli
[Ee] [Ss] [0-9A-Za-z] \d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] \d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{7} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} . \d{3} . \d{2} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} , \d{3} , \d{2} [0-9A-Za-z]
[Ee] [Ss] [0-9A-Za-z] -\d{2} / \d{5} [0-9A-Za-z]

Tabella 40-713 Convalide di copertura limitata del numero di partita IVA spagnolo

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero iva spagnolo, numero iva Spagna, numero Iva, n. iva, n.IVA, IVA, numero imposta valore aggiunto, imposta valore aggiunto</p> <p>Número IVA España, Número de IVA español, español Número IVA, Número de valor agregado, IVA, Número IVA, Número impuesto sobre valor añadido, Impuesto valor agregado, Impuesto sobre valor añadido, valor añadido el impuesto, valor añadido el impuesto numero</p>
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalide obbligatorie	Descrizione
Escludi caratteri finali	Esclude i numeri che terminano con i seguenti caratteri dalla corrispondenza: 000000000, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999
Controllo di convalida numero di partita IVA spagnolo	Calcola il checksum e lo utilizza per convalidare il modello.

Numero di conto cliente spagnolo

Il numero di conto cliente spagnolo è il numero di conto bancario standard utilizzato in Spagna.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero di 20 cifre senza la convalida del checksum. Vedere "[Copertura ampia numero di conto cliente spagnolo](#)" a pagina 1243.
- La copertura media rileva un numero a 20 cifre con la convalida del checksum. Vedere "[Modello copertura media numero di conto cliente spagnolo](#)" a pagina 1244.
- La copertura limitata rileva un numero a 20 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata numero di conto cliente spagnolo](#)" a pagina 1244.

Copertura ampia numero di conto cliente spagnolo

La copertura ampia rileva un numero di 20 cifre senza la convalida del checksum.

Tabella 40-714 Criteri copertura ampia numero di conto cliente spagnolo

Modelli
$\backslash d\{20\}$
$\backslash d\{4\}[-/\backslash d\{4\}[-/\backslash d\{2\}[-/\backslash d\{10\}$
0128[-/\backslash d\{4\}[-/\backslash d\{2\}[-/\backslash d\{10\}
0128\backslash d\{16\}

Tabella 40-715 Convalide copertura ampia numero di conto cliente spagnolo

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Modello copertura media numero di conto cliente spagnolo

La copertura media rileva un numero a 20 cifre con la convalida del checksum.

Tabella 40-716 Criteri copertura media numero di conto cliente spagnolo

Modelli
$\backslash d\{20\}$
$\backslash d\{4\}[-/]\backslash d\{4\}[-/]\backslash d\{2\}[-/]\backslash d\{10\}$
0128[-/]\backslash d\{4\}[-/]\backslash d\{2\}[-/]\backslash d\{10\}
0128 $\backslash d\{16\}$

Tabella 40-717 Convalida copertura media numero di conto cliente spagnolo

Convalida obbligatoria	Descrizione
Controllo di convalida numero di conto cliente spagnolo	Lo strumento di convalida calcola il checksum che ogni numero di conto cliente spagnolo deve superare.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata numero di conto cliente spagnolo

La copertura limitata rileva un numero a 20 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-718 Criteri copertura limitata numero di conto cliente spagnolo

Criterio
$\backslash d\{20\}$
$\backslash d\{4\}[-/]\backslash d\{4\}[-/]\backslash d\{2\}[-/]\backslash d\{10\}$
0128[-/]\backslash d\{4\}[-/]\backslash d\{2\}[-/]\backslash d\{10\}
0128 $\backslash d\{16\}$

Tabella 40-719 Convalide copertura limitata numero di conto cliente spagnolo

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di conto cliente spagnolo	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando si utilizza questa opzione, è necessario utilizzare almeno una delle parole o frasi chiave seguenti per ottenere i dati corrispondenti.</p> <p>Input:</p> <p>numero conto cliente, codice conto, ID conto cliente, ID conto corrente cliente, numero conto corrente, codice bancario cliente spagnolo, numero conto, n.conto, numeroconto,</p> <p>número cuenta cliente, código cuenta, cuenta cliente ID, número cuenta bancaria cliente, código cuenta bancaria</p>

Numero di DNI spagnolo

Il numero di DNI spagnolo è riportato sul Documento nacional de identidad (DNI) ed è rilasciato dall'Hacienda Publica spagnola a tutti i cittadini spagnoli. È il più importante identificatore univoco utilizzato in Spagna per l'apertura di conti, la firma di contratti, le tasse e le elezioni.

L'identificatore di dati del numero di DNI spagnolo offre due coperture di rilevamento:

- La copertura ampia rileva un numero di 8 cifre seguito da un trattino e da una lettera. L'ultima lettera deve corrispondere a un algoritmo di checksum.
Vedere ["Copertura ampia del numero di DNI spagnolo"](#) a pagina 1245.
- La copertura limitata rileva un numero di 8 cifre seguito da un trattino e una lettera. L'ultima lettera deve corrispondere a un algoritmo di checksum. Richiede inoltre la presenza di parole chiave associate al DNI spagnolo.
Vedere ["Copertura limitata del numero di DNI spagnolo"](#) a pagina 1246.

Copertura ampia del numero di DNI spagnolo

La copertura ampia rileva un numero di 8 cifre seguito da un trattino e da una lettera. L'ultima lettera deve corrispondere a un algoritmo di checksum.

Tabella 40-720 Criteri di copertura ampia del numero di DNI spagnolo

Criterio
$\backslash d\{7\}\backslash w$
$\backslash d\{7\}[-]\backslash w$
$\backslash d\{7\}[][-]\backslash w$
$\backslash d\{7\}[][-][]\backslash w$

Tabella 40-721 Convalida di portata ampia del numero di DNI spagnolo

Convalida obbligatoria	Descrizione
Verifica chiave di controllo DNI	Calcola la chiave di controllo e ne verifica la validità.

Copertura limitata del numero di DNI spagnolo

La copertura limitata rileva un numero di 8 cifre seguito da un trattino e una lettera. L'ultima lettera deve corrispondere a un algoritmo di checksum. Richiede inoltre la presenza di parole chiave associate al DNI spagnolo.

Tabella 40-722 Criteri della copertura limitata del numero di DNI spagnolo

Criterio
$\backslash d\{7\}\backslash w$
$\backslash d\{7\}[-]\backslash w$
$\backslash d\{7\}[][-]\backslash w$
$\backslash d\{7\}[][-][]\backslash w$

Tabella 40-723 Convalide della copertura limitata del numero di DNI spagnolo

Verifica chiave di controllo DNI	Calcola la chiave di controllo e ne verifica la validità.

Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>DNI, numero di identificazione nazionale, numero di identità nazionale, numero di assicurazione, numero di identificazione personale, identità nazionale, n. di identità personale, numero di identità univoco, n.idnazionale, n.idunivoco, n.DNI, n.IDnazionale, DNINúmero#, Identidadúnico#, ID NIE, ID NIE spagnolo, numero NIE spagnolo, NIE, n.NIE, NIEnúmero#, NIE número, Documento Nacional de Identidad, Identidad único, Número nacional identidad, DNI Número</p>

Numero di passaporto spagnolo

I passaporti spagnolo sono rilasciati ai cittadini spagnoli per viaggiare all'esterno della Spagna.

L'identificatore di dati Numero di passaporto spagnolo fornisce due coperture di rilevamento:

- La copertura ampia rileva un criterio valido del Numero di passaporto spagnolo.
Vedere ["Copertura ampia Numero di passaporto spagnolo"](#) a pagina 1247.
- La copertura limitata rileva un criterio valido del Numero di passaporto spagnolo. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata Numero di passaporto spagnolo"](#) a pagina 1248.

Copertura ampia Numero di passaporto spagnolo

La copertura ampia rileva un criterio valido del Numero di passaporto spagnolo.

Tabella 40-724 Criteri di copertura ampia Numero di passaporto spagnolo

Criteri
\1{2}\d{6}
\1{2}-\d{6}
\1{2} \d{6}
\1{3}\d{6}
\1{3}-\d{6}

Criteri
\l{3} \d{6}

Tabella 40-725 Convalida di copertura ampia Numero di passaporto spagnolo

Convalida obbligatoria	Descrizione
Delimitatore di numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata Numero di passaporto spagnolo

La copertura limitata rileva un criterio valido del Numero di passaporto spagnolo. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-726 Criteri di copertura limitata Numero di passaporto spagnolo

Criteri
\l{2}\d{6}
\l{2}-\d{6}
\l{2} \d{6}
\l{3}\d{6}
\l{3}-\d{6}
\l{3} \d{6}

Tabella 40-727 Convalide di copertura limitata Numero di passaporto spagnolo

Convalida obbligatoria	Descrizione
Delimitatore di numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>passaporto, Passaporto, Passaporto spagnolo, passaporto spagnolo, libretto passaporto, Libretto passaporto, numero passaporto, n. passaporto, Numero passaporto, libreta pasaporte, número pasaporte, Número Pasaporte, España pasaporte, pasaporte</p>

Numero di previdenza sociale spagnolo

Il numero di previdenza sociale spagnolo è un numero a 12 cifre assegnato ai lavoratori spagnoli per consentire l'accesso al sistema sanitario spagnolo.

L'identificatore di dati Numero di previdenza sociale spagnolo fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum. Vedere ["Copertura ampia numero di previdenza sociale spagnolo"](#) a pagina 1249.
- La copertura media rileva un numero di 12 cifre con la convalida del checksum. Vedere ["Copertura media del numero di previdenza sociale spagnolo"](#) a pagina 1249.
- La copertura limitata rileva un numero di 12 cifre che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave relative al numero di previdenza sociale spagnolo. Vedere ["Copertura limitata numero di previdenza sociale spagnolo"](#) a pagina 1250.

Copertura ampia numero di previdenza sociale spagnolo

La copertura ampia rileva un numero di 12 cifre senza la convalida del checksum.

Tabella 40-728 Criteri copertura ampia numero di previdenza sociale spagnolo

Criterio
$\backslash d\{12\}$
$\backslash d\{2\}[/]\backslash d\{8\}[/]\backslash d\{2\}$
$\backslash d\{2\}[-]\backslash d\{8\}[-]\backslash d\{2\}$

Tabella 40-729 Convalida copertura ampia numero di previdenza sociale spagnolo

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di previdenza sociale spagnolo

La copertura media rileva un numero di 12 cifre con la convalida del checksum.

Tabella 40-730 Criteri copertura media del numero di previdenza sociale spagnolo

Criterio
$\backslash d\{12\}$
$\backslash d\{2\}[/]\backslash d\{8\}[/]\backslash d\{2\}$
$\backslash d\{2\}[-]\backslash d\{8\}[-]\backslash d\{2\}$

Tabella 40-731 Convalida copertura media del numero di previdenza sociale spagnolo

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di previdenza sociale spagnolo	Calcola il checksum e lo utilizza per convalidare il criterio.

Copertura limitata numero di previdenza sociale spagnolo

La copertura limitata rileva un numero di 12 cifre che supera la convalida del checksum.
 Richiede inoltre la presenza di parole chiave relative al numero di previdenza sociale spagnolo.

Tabella 40-732 Criteri copertura limitata numero di previdenza sociale spagnolo

Criterio
$\backslash d\{12\}$
$\backslash d\{2\}[/]\backslash d\{8\}[/]\backslash d\{2\}$
$\backslash d\{2\}[-]\backslash d\{8\}[-]\backslash d\{2\}$

Tabella 40-733 Strumenti di convalida copertura limitata numero di previdenza sociale spagnolo

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di previdenza sociale spagnolo	Calcola il checksum e lo utilizza per convalidare il criterio.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>SSN, numero di previdenza sociale, SSN#, n. di previdenza sociale, n.previdenzasociale, Social Security Number, n. di previdenza sociale Número de la Seguridad Social, número de la seguridad social</p>

Codice fiscale spagnolo (CIF)

Il codice fiscale spagnolo (CIF) è equivalente alla partita IVA ed è necessario per svolgere un'attività lavorativa in Spagna. Esso è il numero identificativo di un'azienda per scopi fiscali ed è obbligatorio per qualsiasi transazione giuridica.

L'identificatore di dati di sistema Codice fiscale spagnolo (CIF) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un identificativo alfanumerico di 9 cifre senza convalida del checksum.
Vedere ["Copertura ampia del codice fiscale spagnolo \(CIF\)"](#) a pagina 1251.
- La copertura media rileva un identificativo alfanumerico di 9 cifre con convalida del checksum.
Vedere ["Copertura media codice fiscale spagnolo \(CIF\)"](#) a pagina 1252.
- La copertura limitata rileva un identificativo alfanumerico di 9 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate al CIF.
Vedere ["Copertura limitata codice fiscale spagnolo \(CIF\)"](#) a pagina 1252.

Copertura ampia del codice fiscale spagnolo (CIF)

La copertura ampia rileva un identificativo alfanumerico di 9 cifre senza convalida del checksum.

Tabella 40-734 Criteri copertura ampia del codice fiscale spagnolo (CIF)

Criterio
[KPQS] \d{7} [A-J]
[KPQS] - \d{7} [A-J]
[ABEH] \d{7} [0-9]

Criterio
[ABEH] - \d{7} [0-9]
[CDFGJLMNRUVW] \d{7} [A-J0-9]
[CDFGJLMNRUVW] - \d{7} [A-J0-9]

Tabella 40-735 Convalida di copertura media del codice fiscale spagnolo (CIF)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media codice fiscale spagnolo (CIF)

La copertura media rileva un identificativo alfanumerico di 9 cifre con convalida del checksum.

Tabella 40-736 Criteri copertura media codice fiscale spagnolo (CIF)

Criterio
[KPQS] \d{7} [A-J]
[KPQS] - \d{7} [A-J]
[ABEH] \d{7} [0-9]
[ABEH] - \d{7} [0-9]
[CDFGJLMNRUVW] \d{7} [A-J0-9]
[CDFGJLMNRUVW] - \d{7} [A-J0-9]

Tabella 40-737 Convalida copertura media codice fiscale spagnolo (CIF)

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice di identificazione fiscale spagnolo.	Calcola il checksum e lo utilizza per convalidare il criterio.

Copertura limitata codice fiscale spagnolo (CIF)

La copertura limitata rileva un identificativo alfanumerico di 9 cifre con convalida del checksum.
 Richiede inoltre la presenza di parole chiave associate al CIF.

Tabella 40-738 Criteri copertura limitata codice fiscale spagnolo (CIF)

Criterio
[KPQS] \d{7} [A-J]
[KPQS] - \d{7} [A-J]
[ABEH] \d{7} [0-9]
[ABEH] - \d{7} [0-9]
[CDFGJLMNRUVW] \d{7} [A-J0-9]
[CDFGJLMNRUVW] - \d{7} [A-J0-9]

Tabella 40-739 Convalide copertura limitata codice fiscale spagnolo (CIF)

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida codice di identificazione fiscale spagnolo.	Calcola il checksum e lo utilizza per convalidare il criterio.
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>identificazione fiscale, codice di identificazione fiscale, identificazione CIF, cod. CIF, identificazione CIF spagnolo, cod. cif, cod. file fiscale, codice CIF spagnolo, codice file fiscale, cod. CIF spagnolo, cod. fiscale, codice fiscale, identificazione fiscale, cod.identificazionefiscale, cod.fiscale, cod.identificazioneCIF, cod.CIF, cod.identificazioneCIFspagnolo, cod.CIFspagnolo, cod.identificazionecif, número de contribuyente, número de impuesto corporativo, número de Identificación fiscal, CIF número, CIFnúmero#</p>

Numero di patente di guida svedese

In Svezia, la patente di guida è necessaria quando si conduce un'auto, un motociclo o un ciclomotore su strade pubbliche. Le patenti di guida sono emesse dalle commissioni di sicurezza pubblica delle prefetture e sono supervisionate su base nazionale dall'ente nazionale di polizia.

L'identificatore di dati del numero di patente di guida svedese rileva un numero 10 cifre che corrisponde al formato del numero di patente di guida svedese.

L'identificatore di dati del numero di patente di guida svedese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum. Vedere ["Copertura ampia del numero di patente di guida svedese"](#) a pagina 1254.
- La copertura media rileva un numero a 10 cifre con la convalida del checksum. Vedere ["Copertura media del numero patente di guida svedese"](#) a pagina 1254.
- La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata del numero di patente di guida svedese"](#) a pagina 1255.

Copertura ampia del numero di patente di guida svedese

La copertura ampia rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-740 Modelli di copertura ampia del numero di patente di guida svedese

Modelli
$\backslash d\{6\}-\backslash d\{4\}$
$\backslash d\{6\}+\backslash d\{4\}$

Tabella 40-741 Convalide di copertura ampia del numero di patente di guida svedese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero patente di guida svedese

La copertura media rileva un numero a 10 cifre con la convalida del checksum.

Tabella 40-742 Criteri di copertura media del numero patente di guida svedese

Modelli
$\backslash d\{6\}-\backslash d\{4\}$
$\backslash d\{6\}+\backslash d\{4\}$

Tabella 40-743 Convalida della copertura media del numero di patente di guida svedese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione fiscale svedese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di patente di guida svedese

La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-744 Modelli di copertura limitata del numero di patente di guida svedese

Modelli
$\backslash d\{6\}-\backslash d\{4\}$
$\backslash d\{6\}+\backslash d\{4\}$

Tabella 40-745 Convalide di copertura limitata del numero di patente di guida svedese

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Controllo di convalida numero di identificazione fiscale svedese	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalide obbligatorie	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>patente di guida, numero patente di guida, pat. di guida, patente guida, numero patente guida, patente di guida numero, n. pat. guida</p> <p>ajokortti, permis de conduire, ajokortin numero, kuljettajat lic., drivere lic., körkort, numărul permisului de conduce, שא, פער דערלויבעניש נומער, körkort nummer, förare lic., דריווערס דערלויבעניש, körkortsnummer</p>

Numero di identificazione fiscale svedese

La Svezia utilizza i numeri di identificazione fiscale (TIN) per identificare i contribuenti e facilitare l'amministrazione delle questioni fiscali nazionali. I TIN sono anche utili per identificare i contribuenti che investono in altri paesi dell'UE e sono più affidabili di altri identificatori come il nome e l'indirizzo.

L'identificatore di dati del numero di identificazione fiscale svedese rileva un numero di 10 o 12 cifre che corrisponde al formato del numero di identificazione fiscale svedese.

L'identificatore di dati del numero di identificazione fiscale svedese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 10 o 12 cifre senza la convalida del checksum. Vedere "[Copertura ampia del numero di identificazione fiscale svedese](#)" a pagina 1256.
- La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum. Vedere "[Copertura media del numero di identificazione fiscale svedese](#)" a pagina 1257.
- La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata del numero di identificazione fiscale svedese](#)" a pagina 1257.

Copertura ampia del numero di identificazione fiscale svedese

La copertura ampia rileva un numero di 10 o 12 cifre senza la convalida del checksum.

Tabella 40-746 Modelli di copertura ampia del numero di identificazione fiscale svedese

Modelli
$\backslash d\{8\} - \backslash d\{4\}$
$\backslash d\{6\} - \backslash d\{4\}$
$\backslash d\{8\} + \backslash d\{4\}$
$\backslash d\{6\} + \backslash d\{4\}$

Tabella 40-747 Convalida copertura ampia del numero di identificazione fiscale svedese

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura media del numero di identificazione fiscale svedese

La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum.

Tabella 40-748 Modelli di copertura media del numero di identificazione fiscale svedese

Modelli
$\backslash d\{8\} - \backslash d\{4\}$
$\backslash d\{6\} - \backslash d\{4\}$
$\backslash d\{8\} + \backslash d\{4\}$
$\backslash d\{6\} + \backslash d\{4\}$

Tabella 40-749 Convalida di copertura media del numero di identificazione fiscale svedese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di identificazione fiscale svedese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione fiscale svedese

La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-750 Modelli di copertura limitata del numero di identificazione fiscale svedese

Modelli
$\backslash d\{8\}-\backslash d\{4\}$
$\backslash d\{6\}-\backslash d\{4\}$
$\backslash d\{8\}+\backslash d\{4\}$
$\backslash d\{6\}+\backslash d\{4\}$

Tabella 40-751 Convalide di copertura limitata del numero di identificazione fiscale svedese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione fiscale svedese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>tin, numero tin, n. tin, n.tin, tin svedese, numero tin svedese, n. tin svedese, n.tin svedese</p> <p>skattebetalarens identifikationsnummer, sverige TIN,T IN-nummer, nummer</p>

Numero di partita IVA svedese

L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.

L'identificatore di dati del numero di partita IVA svedese rileva un modello alfanumerico di 14 caratteri che corrisponde al formato del numero di partita IVA svedese.

L'identificatore di dati del numero di partita IVA svedese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 14 caratteri che inizia con **SE** ed è seguito da 12 cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di partita IVA svedese"](#) a pagina 1259.
- La copertura media rileva un modello alfanumerico di 14 caratteri che inizia con **SEED** è seguito da 12 cifre con la convalida del checksum.
Vedere ["Copertura media del numero di partita IVA svedese"](#) a pagina 1259.

- La copertura limitata rileva un modello alfanumerico di 14 caratteri che inizia con **SEED** è seguito da 12 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di partita IVA svedese](#)" a pagina 1260.

Copertura ampia del numero di partita IVA svedese

La copertura ampia rileva un modello alfanumerico di 14 caratteri che inizia con **SE** ed è seguito da 12 cifre senza la convalida del checksum.

Tabella 40-752 Modello di copertura ampia numero di partita IVA svedese

Criterio
[Ss][Ee]\d{12}

Tabella 40-753 Convalide di copertura ampia numero di partita IVA svedese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	I modelli che terminano con le seguenti stringhe di caratteri vengono esclusi dalla corrispondenza: 000000000000, 111111111111, 222222222222, 333333333333, 444444444444, 555555555555, 666666666666, 777777777777, 888888888888, 999999999999

Copertura media del numero di partita IVA svedese

La copertura media rileva un modello alfanumerico di 14 caratteri che inizia con **SEED** è seguito da 12 cifre con la convalida del checksum.

Tabella 40-754 Modello di copertura media del numero di partita IVA svedese

Criterio
[Ss][Ee]\d{12}

Tabella 40-755 Convalida di copertura media del numero di partita IVA svedese

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA svedese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di partita IVA svedese

La copertura limitata rileva un modello alfanumerico di 14 caratteri che inizia con **SEED** è seguito da 12 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-756 Modello di copertura limitata del numero di partita IVA svedese

Criterio
[Ss][Ee]\d{12}

Tabella 40-757 Convalida di copertura limitata del numero di partita IVA svedese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	I modelli che terminano con le seguenti stringhe di caratteri vengono esclusi dalla corrispondenza: 000000000000, 111111111111, 222222222222, 333333333333, 444444444444, 555555555555, 666666666666, 777777777777, 888888888888, 999999999999
Controllo di convalida numero di partita IVA svedese	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: n. iva, numero iva, moms#, n.iva, numero imposta valore aggiunto, num iva, iva svedese, sverige moms, numero iva svedese, sverige momsnummer, n. iva svedese, sverige moms nr, n.iva svedese, sweden vat nummer, sweden momsnummer, num iva svedese, numero imposta sul valore aggiunto svedese, momsregistreringsnummer

Numero di passaporto svedese

Il passaporto svedese viene rilasciato alle persone di nazionalità svedese per viaggiare all'estero. Oltre a servire quale prova della cittadinanza svedese, assicura l'assistenza del consolato svedese all'estero o, se necessario, di altri stati membri dell'Unione Europea, nel caso in cui sia il console svedese non sia presente.

L'identificatore di dati Numero di passaporto svedese rileva un criterio valido del Numero di passaporto svedese.

L'identificatore di dati Numero di passaporto svedese fornisce due coperture di rilevamento:

- La copertura ampia rileva un criterio valido del Numero di passaporto svedese. Vedere "[Copertura ampia Numero di passaporto svedese](#)" a pagina 1261.
- La copertura limitata rileva un criterio valido del Numero di passaporto svedese. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata Numero di passaporto svedese](#)" a pagina 1261.

Copertura ampia Numero di passaporto svedese

La copertura ampia rileva un criterio valido del Numero di passaporto svedese.

Tabella 40-758 Criteri di copertura ampia Numero di passaporto svedese

Criteri
$\backslash d\{8\}$
$\backslash d\{2\}-\backslash d\{6\}$
$\backslash l\{2\}-\backslash d\{6\}$

Tabella 40-759 Convalida di copertura ampia Numero di passaporto svedese

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata Numero di passaporto svedese

La copertura limitata rileva un criterio valido del Numero di passaporto svedese. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-760 Criteri di copertura limitata Numero di passaporto svedese

Criteri
$\backslash d\{8\}$
$\backslash d\{2\}-\backslash d\{6\}$
$\backslash l\{2\}-\backslash d\{6\}$

Tabella 40-761 Convalide di copertura limitata Numero di passaporto svedese

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>passaporto, Passaporto, Passaporto svedese, Passaporto Svezia, numero passaporto, n. passaporto, Numero passaporto</p> <p>Passnummer, pass, sverige pass, SVERIGE PASS, sverige Passnummer</p>

Numero di identificazione personale svedese

Il numero di identificazione personale svedese è l'identificazione nazionale univoca per ogni cittadino svedese. Tale numero è utilizzato come strumento di riconoscimento da autorità, assistenza sanitaria, scuole, università, banche e compagnie di assicurazione.

L'identificatore di dati per il Numero di identificazione personale svedese rileva un numero di 10 o 12 cifre che corrisponde al formato del Numero di identificazione personale svedese.

L'identificatore di dati di sistema Numero di identificazione personale svedese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 10 o 12 cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione personale svedese"](#) a pagina 1262.
- La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum.
Vedere ["Copertura media del numero di identificazione personale svedese"](#) a pagina 1263.
- La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum.
Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata numero di identificazione personale svedese"](#) a pagina 1264.

Copertura ampia del numero di identificazione personale svedese

La copertura ampia rileva un numero di 10 o 12 cifre senza la convalida del checksum.

Tabella 40-762 Criteri della copertura ampia del numero di identificazione personale svedese

Criterio
\d\d[01]\d[01236789]\d[-]\d\d\d\d
\d\d[01]\d[01236789]\d[+]\d\d\d\d
\d\d[01]\d[01236789]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d[-]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d[+]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d\d\d\d

Tabella 40-763 Convalida della copertura ampia del numero di identificazione personale svedese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione personale svedese

La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum.

Tabella 40-764 Criteri di copertura media del numero di identificazione personale svedese

Criterio
\d\d[01]\d[01236789]\d[-]\d\d\d\d
\d\d[01]\d[01236789]\d[+]\d\d\d\d
\d\d[01]\d[01236789]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d[-]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d[+]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d\d\d\d

Tabella 40-765 Convalide copertura media del numero di identificazione personale svedese

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione personale svedese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di identificazione personale svedese

La copertura media rileva un numero di 10 o 12 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-766 Criteri copertura limitata numero di identificazione personale svedese

Criterio
\d\d[01]\d[01236789]\d[-]\d\d\d\d
\d\d[01]\d[01236789]\d[+]\d\d\d\d
\d\d[01]\d[01236789]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d[-]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d[+]\d\d\d\d
[12][098]\d\d[01]\d[01236789]\d\d\d\d

Tabella 40-767 Convalide copertura limitata numero di identificazione personale svedese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione personale svedese	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero ID personale, numero identificazione, n. ID personale, n. id personale, n. identità, n. identificazione, n. identificazione personale, n. id personale</p> <p>personnummer ID, personligt id-nummer, unikt id-nummer, personnummer, identifikationsnumret, personnummer#, identifikationsnumret#</p>

Codice SWIFT

Il codice SWIFT è un identificatore univoco per le banche ed è gestito dalla Society for Worldwide Interbank Financial Telecommunications (SWIFT). Il codice SWIFT è richiesto per i trasferimenti di denaro tra istituzioni finanziarie. È noto anche come codice BIC (codice di identificazione bancaria).

L'identificatore di dati del codice SWIFT rileva una stringa alfanumerica di 8 o 11 caratteri che corrisponde al formato del codice SWIFT.

Questo identificatore di dati fornisce due coperture di convalida:

- La copertura ampia rileva una stringa alfanumerica di 8 o 11 caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.
Vedere ["Copertura ampia Codice SWIFT"](#) a pagina 1265.
- La copertura limitata rileva una stringa alfanumerica di 8 o 11 caratteri senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.
Vedere ["Copertura limitata codice SWIFT"](#) a pagina 1266.

Copertura ampia Codice SWIFT

La copertura ampia dell'identificatore dati del Codice SWIFT rileva stringhe alfanumeriche da 8 o 11 caratteri. Il 5° e il 6° carattere sono lettere del indicano il codice paese. Questa copertura richiede inoltre la presenza di una parola chiave relativa allo SWIFT.

Tabella 40-768 Modelli copertura ampia Codice SWIFT

Modello
[A-Z]{6}\w{2}

Modello
[A-Z] { 6 } \w { 5 }

Tabella 40-769 Strumenti di convalida copertura ampia Codice SWIFT

Convalide obbligatorie	Descrizione
Richiedi caratteri iniziali	<p>Quando questa opzione è selezionata, uno qualsiasi dei valori seguenti deve trovarsi all'inizio dei dati corrispondenti.</p> <p>Input:</p> <p>af, ax, al, dz, as, ad, ao, ai, aq, ag, ar, am, aw, au, at, az, bs, bh, bd, bb, by, be, bz, bj, bm, bt, bo, ba, bw, bv, br, io, bn, bg, bf, bi, kh, cm, ca, cv, ky, cf, td, cl, cn, cx, cc, co, km, cg, cd, ck, cr, ci, hr, cu, cy, cz, dk, dj, dm, do, ec, eg, sv, gq, er, ee, et, fk, fo, fj, fi, fr, gf, pf, tf, ga, gm, ge, de, gh, gi, gr, gl, gd, gp, gu, gt, gg, gn, gw, gy, ht, hm, va, hn, hk, hu, is, in, id, ir, iq, ie, im, il, it, jm, jp, je, jo, kz, ke, ki, kp, kr, kw, kg, la, lv, lb, ls, lr, ly, li, lt, lu, mo, mk, mg, mw, my, mv, ml, mt, mh, mq, mr, mu, yt, mx, md, mc, mn, me, ms, ma, mz, mm, na, nr, np, nl, an, nc, nz, ni, ne, ng, nu, nf, mp, no, om, pk, pw, ps, pa, pg, py, pe, ph, pn, pl, pt, pr, qa, re, ro, ru, rw, sh, kn, lc, pm, vc, ws, sm, st, sa, sn, rs, sc, sl, sg, sk, si, sb, so, za, gs, es, lk, sd, sr, sj, sz, se, ch, sy, tw, tj, tz, th, tl, tg, tk, to, tt, tn, tr, tm, tc, tv, ug, ua, ae, gb, us, um, uy, uz, vu, ve, vn, vg, vi, wf, eh, ye, zm, zw</p>
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>bic, bic#, international organization for standardization 9362, iso 9362, iso9362, swift, swift#, swiftcode, swiftnumber, swiftroutingnumber</p>

Copertura limitata codice SWIFT

La copertura limitata dell'identificatore di dati Codice SWIFT rileva stringhe di 8 o 11 caratteri. Il 5° e il 6° carattere sono lettere che si riferiscono a un codice paese. Questa copertura richiede inoltre la presenza di parole chiave associate al codice SWIFT.

Tabella 40-770 Criteri di copertura limitata codice SWIFT

Criteri
[A-Z] { 6 } \w { 2 }
[A-Z] { 6 } \w { 5 }

Tabella 40-771 Convalide copertura limitata codice SWIFT

Convalide	Descrizione
Richiedi caratteri iniziali	<p>Quando questa opzione è selezionata, uno qualsiasi dei valori seguenti deve trovarsi all'inizio dei dati corrispondenti.</p> <p>Input:</p> <p>af, ax, al, dz, as, ad, ao, ai, aq, ag, ar, am, aw, au, at, az, bs, bh, bd, bb, by, be, bz, bj, bm, bt, bo, ba, bw, bv, br, io, bn, bg, bf, bi, kh, cm, ca, cv, ky, cf, td, cl, cn, cx, cc, co, km, cg, cd, ck, cr, ci, hr, cu, cy, cz, dk, dj, dm, do, ec, eg, sv, gq, er, ee, et, fk, fo, fj, fi, fr, gf, pf, tf, ga, gm, ge, de, gh, gi, gr, gl, gd, gp, gu, gt, gg, gn, gw, gy, ht, hm, va, hn, hk, hu, is, in, id, ir, iq, ie, im, il, it, jm, jp, je, jo, kz, ke, ki, kp, kr, kw, kg, la, lv, lb, ls, lr, ly, li, lt, lu, mo, mk, mg, mw, my, mv, ml, mt, mh, mq, mr, mu, yt, mx, md, mc, mn, me, ms, ma, mz, mm, na, nr, np, nl, an, nc, nz, ni, ne, ng, nu, nf, mp, no, om, pk, pw, ps, pa, pg, py, pe, ph, pn, pl, pt, pr, qa, re, ro, ru, rw, sh, kn, lc, pm, vc, ws, sm, st, sa, sn, rs, sc, sl, sg, sk, si, sb, so, za, gs, es, lk, sd, sr, sj, sz, se, ch, sy, tw, tj, tz, th, tl, tg, tk, to, tt, tn, tr, tm, tc, tv, ug, ua, ae, gb, us, um, uy, uz, vu, ve, vn, vg, vi, wf, eh, ye, zm, zw</p>
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>bic#, international organization for standardization 9362, iso 9362, iso9362, swift#, swiftcode, swiftnumber, swiftroutingnumber, swift code, swift number, swift routing number, bic number, bic code, bic # (n.bic, organizzazione internazionale per la normazione 9362, iso 9362, iso9362, n.swift, codiceswift, numeroswift, numerodiroutingswift, n. swift, codice swift, numero swift, numero di routing swift, numero bic, codice bic, n. bic)</p>

Numero AHV svizzero

In Svizzera, il numero di assicurazione per la vecchiaia e i superstiti (numero AHV o Alters- und Hinterlassenenversicherungsnummer) è il numero di identificazione pubblico più importante.

L'identificatore di dati per il Numero AHV svizzero rileva un numero di 11 cifre che corrisponde al formato del Numero AHV.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva un numero a 11 cifre con convalida del checksum.
Vedere ["Copertura ampia numero di previdenza sociale svizzero \(AHV\)"](#) a pagina 1268.
- La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero AHV svizzero"](#) a pagina 1268.

Copertura ampia numero di previdenza sociale svizzero (AHV)

La copertura ampia rileva un numero a 11 cifre con convalida del checksum.

Tabella 40-772 Criterio copertura ampia numero AHV svizzero

Criterio
\d{3}.\d{2}.\d{3}.\d{3}
\d{11}

Tabella 40-773 Convalide copertura ampia numero di previdenza sociale svizzero (AHV)

Convalida obbligatoria	Descrizione
Numero di previdenza sociale svizzero (AHV)	Calcola il Checksum Modulo 11 numero di previdenza sociale svizzero (AHV) e lo utilizza per convalidare il criterio.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata del numero AHV svizzero

La copertura limitata rileva un numero a 11 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-774 Criteri di copertura limitata del numero AHV svizzero

Criterio
\d{3}.\d{2}.\d{3}.\d{3}
\d{11}

Tabella 40-775 Convalide della copertura limitata del numero AHV svizzero

Convalida obbligatoria	Descrizione
Numero di previdenza sociale svizzero (AHV)	Calcola il Checksum Modulo 11 numero di previdenza sociale svizzero (AHV) e lo utilizza per convalidare il criterio.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numéro AVS, identifiant national, numéro de sécurité sociale, Numéro AVH, numero AVS, numero di assicurazione, identificatore nazionale, numero di previdenza sociale, numero di codice fiscale, numero AVH, AHV-Nummer, Personenidentifikationsnummer, Schweizer Registrierungsnummer, numero AHV, numero di matricola svizzero, PIN, AVH, AVS, numéro d'assurance vieillesse, numéro d'assuré</p>

Numero di previdenza sociale svizzero (AHV)

Il numero di previdenza sociale svizzero (AHV) consente ai cittadini svizzeri di usufruire del sistema previdenziale svizzero.

L'identificatore di dati per il numero di codice fiscale svizzero (AHV) rileva un numero di 13 cifre che corrisponde al formato di AHV.

L'identificatore di dati di sistema per il numero di previdenza sociale svizzero fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre con la convalida del checksum. Vedere ["Copertura ampia del numero di codice fiscale svizzero \(AHV\)"](#) a pagina 1269.
- La copertura media rileva un numero di 13 cifre senza la convalida del checksum. Vedere ["Copertura media del numero di previdenza sociale svizzero \(AHV\)"](#) a pagina 1270.
- La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata numero di previdenza sociale svizzero \(AHV\)"](#) a pagina 1270.

Copertura ampia del numero di codice fiscale svizzero (AHV)

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-776 Criteri di copertura ampia del numero di codice fiscale svizzero (AHV)

Criterio
[7] [5] [6] \d{10}

Criterio
[7] [5] [6] [.] \d{4} [.] \d{4} [.] \d{2}

Tabella 40-777 Convalida di copertura ampia del numero di codice fiscale svizzero (AHV)

Convalida	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di previdenza sociale svizzero (AHV)

La copertura media rileva un numero a 13 cifre con la convalida del checksum.

Tabella 40-778 Criteri copertura media del numero di previdenza sociale svizzero (AHV)

Criterio
[7] [5] [6] \d{10}
[7] [5] [6] [.] \d{4} [.] \d{4} [.] \d{2}

Tabella 40-779 Convalide copertura media del numero di previdenza sociale svizzero (AHV)

Convalida	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo di convalida numero di previdenza sociale svizzero	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata numero di previdenza sociale svizzero (AHV)

La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza parole chiave associate.

Tabella 40-780 Criteri di copertura limitata numero di previdenza sociale svizzero (AHV)

Criterio
[7] [5] [6] \d{10}
[7] [5] [6] [.] \d{4} [.] \d{4} [.] \d{2}

Tabella 40-781 Convalide di copertura limitata numero di previdenza sociale svizzero (AHV)

Convalida	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo di convalida numero di previdenza sociale svizzero	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>AHV, numero di previdenza sociale, PID, numero di assicurazione, n.IDpersonale, numero di previdenza sociale, n. ID personale, n. identificazione personale, n.assicurazione, n.IDunivoco, n. identificazione univoco, AVS, numero AHV, numero AVS, numero di previdenza sociale, n.idpersonale, n. identità personale</p> <p>Versicherungsnummer, Identifikationsnummer, einzigartige Identität nicht, Sozialversicherungsnummer, identification personnelle ID, numéro de sécurité sociale</p>

ID ROC Taiwan

A Taiwan, tutti i cittadini di età superiore ai 14 anni sono tenuti a richiedere il rilascio del documento di identità. Dal 1965, per tutti i documenti di identità viene adottata una numerazione uniforme.

L'identificatore di dati ID ROC Taiwan rileva la presenza del numero di identificazione di Taiwan in base su due tipi di criteri di identificazione comuni. L'ultimo carattere corrispondente è usato per convalidare un checksum.

L'identificatore di dati ID ROC Taiwan fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero ID RDC Taiwan con convalida del checksum. Vedere ["Copertura ampia ID RDC Taiwan"](#) a pagina 1272.
- La copertura limitata rileva un numero ID RDC Taiwan con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata dell'ID RDC Taiwan"](#) a pagina 1272.

Copertura ampia ID RDC Taiwan

La copertura ampia rileva un numero ID RDC Taiwan con convalida checksum.

Tabella 40-782 Criteri copertura ampia ID RDC Taiwan

Criteri
[A-Z] [12] [0-3] \d{7}
[A-Z] [ABCD] \d{8}

Tabella 40-783 Convalida copertura ampia ID RDC Taiwan

Convalida	Descrizione
ID Taiwan	Checksum ID di Taiwan.

Copertura limitata dell'ID RDC Taiwan

La copertura limitata rileva un numero ID RDC Taiwan con convalida checksum. Richiede inoltre la presenza di parole chiave associate all'ID RDC Taiwan.

Tabella 40-784 Criteri della copertura limitata dell'ID RDC Taiwan

Criteri
[A-Z] [12] [0-3] \d{7}
[A-Z] [ABCD] \d{8}

Tabella 40-785 Convalide della copertura limitata dell'ID RDC Taiwan

Convalida	Descrizione
ID Taiwan	Checksum ID di Taiwan.
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>中華民國國民身分證</p> <p>ROC ID, carta di identificazione nazionale, ROCID #</p>

Numero di identificazione personale thailandese

Il numero di identificazione personale thailandese è un identificatore personale univoco assegnato alla nascita o quando si riceve la cittadinanza thailandese.

L'identificatore di dati per il Numero di identificazione personale thailandese rileva un numero 13 cifre che corrisponde al formato del Numero di identificazione personale thailandese.

L'identificatore di dati Numero di identificazione personale thailandese fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.
Vedere ["Copertura ampia del numero di identificazione personale thailandese"](#) a pagina 1273.
- La copertura media rileva un numero a 13 cifre con la convalida del checksum.
Vedere ["Copertura media numero di identificazione personale thailandese"](#) a pagina 1273.
- La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata codice identificativo personale thailandese"](#) a pagina 1274.

Copertura ampia del numero di identificazione personale thailandese

La copertura ampia rileva un numero di 13 cifre senza la convalida del checksum.

Tabella 40-786 Criteri della copertura ampia del numero di identificazione personale thailandese

Criterio
[1-8]\d{12}
[1-8][-]\d{4}[-]\d{5}[-]\d{2}[-]\d

Tabella 40-787 Convalida della copertura ampia del numero di identificazione personale thailandese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione personale thailandese

La copertura ampia rileva un numero di 13 cifre con la convalida del checksum.

Tabella 40-788 Criteri di copertura media del numero di identificazione personale thailandese

Criterio
[1-8]\d{12}
[1-8][-]\d{4}[-]\d{5}[-]\d{2}[-]\d

Tabella 40-789 Convalide di copertura media del numero di identificazione personale thailandese

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di identificazione personale thailandese	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata codice identificativo personale thailandese

La copertura limitata rileva un numero a 13 cifre con convalida del checksum. Richiede inoltre la presenza di una parola chiave associata al numero di identificazione personale thailandese.

Tabella 40-790 Criteri copertura limitata codice identificativo personale thailandese

Criterio
[1-8]\d{12}
[1-8][-]\d{4}[-]\d{5}[-]\d{2}[-]\d

Tabella 40-791 Convalide copertura limitata codice identificativo personale thailandese

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida del numero di identificazione personale thailandese	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>PID, numero di previdenza, numero ID personale, n. identificazione personale, n. identificazione univoco, N.IDpersonale, n.previdenza, n.IDprevidenza, n.IDunivoco, n. identificativo personale</p> <p>ประกันภัยจำนวน, หมายเลขประจำตัวส่วนบุคคล, หมายเลขประจำตัวที่ไม่ซ้ำกัน, ประกันภัยจำนวน#, หมายเลขประจำตัวส่วนบุคคล#, หมายเลขประจำตัวที่ไม่ซ้ำกัน#</p>

Numero di identificazione turco

Il numero di identificazione turco (T.C. Kimlik No.) è un numero univoco di 11 cifre assegnato a ogni cittadino turco.

L'identificatore di dati per il Numero di identificazione turco rileva un numero 11-digit che corrisponde al formato di Numero di identificazione turco.

L'identificatore di dati per il Numero di identificazione turco fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum. Vedere "[Copertura ampia del numero di identificazione turco](#)" a pagina 1275.
- La copertura media rileva un numero di 11 cifre con la convalida del checksum. Vedere "[Copertura media del numero di identificazione turco](#)" a pagina 1276.
- La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata di numero di identificazione turco](#)" a pagina 1276.

Copertura ampia del numero di identificazione turco

La copertura ampia rileva un numero di 11 cifre senza la convalida del checksum.

Tabella 40-792 Criterio della copertura ampia del numero di identificazione turco

Criterio
[123456789]\d{10}

Tabella 40-793 Convalida della copertura ampia del numero di identificazione turco

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media del numero di identificazione turco

La copertura media rileva un numero di 11 cifre con la convalida del checksum.

Tabella 40-794 Criterio di copertura media del numero di identificazione turco

Criterio
[123456789]\d{10}

Tabella 40-795 Convalide di copertura media del numero di identificazione turco

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione turco	Calcola il checksum e lo utilizza per convalidare il modello.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Copertura limitata di numero di identificazione turco

La copertura limitata rileva un numero a 11 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate

Tabella 40-796 Criteri copertura limitata numero di identificazione turco

Criterio
[123456789]\d{10}

Tabella 40-797 Strumenti di convalida copertura limitata numero di carta di identità turca

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione turco	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Convalida obbligatoria	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Numero di identificazione, numero di identificazione personale, ID cittadino, n id personale, id n#, id cittadino no, numero identità, n identità personale.</p> <p>Kimlik Numarası, Türkiye Cumhuriyeti Kimlik Numarası, vatandaş kimliği, kişisel kimlik no, kimlik Numarası#, vatandaş kimlik numarası, Kişisel kimlik Numarası</p>

Coordinate bancarie di un numero di conto britannico

Le coordinate bancarie sono codici bancari utilizzati per instradare i trasferimenti di denaro tra banche all'interno dei rispettivi paesi attraverso le rispettive organizzazioni di liquidazione.

L'identificatore di dati delle coordinate bancarie di un numero di conto britannico rileva un numero di sei cifre che corrisponde al formato delle coordinate bancarie di un numero di conto britannico.

L'identificatore di dati delle coordinate bancarie di un numero di conto britannico fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 6 cifre senza la convalida del checksum. Vedere ["Copertura ampia delle Coordinate bancarie di un numero di conto britannico."](#) a pagina 1277.
- La copertura media rileva un numero di 6 cifre con la convalida del checksum. Vedere ["Copertura media delle coordinate bancarie di un numero di conto britannico"](#) a pagina 1278.
- La copertura limitata rileva un numero di 6 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata delle coordinate bancarie di un numero di conto britannico"](#) a pagina 1278.

Copertura ampia delle Coordinate bancarie di un numero di conto britannico.

La copertura ampia rileva un numero di 6 cifre senza la convalida del checksum.

Tabella 40-798 Modelli di copertura ampia delle coordinate bancarie di un numero di conto britannico

Modelli
$\backslash d\{2\}-\backslash d\{2\}-\backslash d\{2\}$
$\backslash d\{6\}$

Tabella 40-799 Convalide di copertura ampia delle coordinate bancarie di un numero di conto britannico

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media delle coordinate bancarie di un numero di conto britannico

La copertura media rileva un numero di 6 cifre con la convalida del checksum.

Tabella 40-800 Modelli di copertura media delle coordinate bancarie di un numero di conto britannico

Modelli
$\backslash d\{2\}-\backslash d\{2\}-\backslash d\{2\}$
$\backslash d\{6\}$

Tabella 40-801 Convalida di copertura media delle coordinate bancarie di un numero di conto britannico

Strumento di convalida obbligatorio	Descrizione
Controllo delle coordinate bancarie di un numero di conto britannico	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata delle coordinate bancarie di un numero di conto britannico

La copertura limitata rileva un numero di 6 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-802 Modelli di copertura limitata delle coordinate bancarie di un numero di conto britannico

Modelli
$\backslash d\{2\}-\backslash d\{2\}-\backslash d\{2\}$
$\backslash d\{6\}$

Tabella 40-803 Convalide di copertura limitata delle coordinate bancarie di un numero di conto britannico

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo delle coordinate bancarie di un numero di conto britannico	Calcola il checksum e lo utilizza per convalidare il modello.
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: Input: coordinate bancarie di un numero di conto britannico, coordinate bancarie del Regno Unito, coordinate, coord.

Numero di patente di guida britannica

È il numero di identificazione della patente di guida individuale rilasciata dalla Driver and Vehicle Licensing Agency del Regno Unito.

L'identificatore di dati del numero di patente di guida del Regno Unito rileva un modello alfanumerico di 16 caratteri che corrisponde al formato del numero di patente di guida del Regno Unito.

L'identificatore di dati del numero di patente di guida del Regno Unito fornisce tre coperture di convalida:

- La copertura ampia rileva un modello alfanumerico di 16 caratteri senza la convalida. Vedere ["Copertura ampia numeri delle patenti di guida britanniche"](#) a pagina 1280.
- La copertura media rileva un modello alfanumerico di 16 caratteri con la convalida del checksum. Vedere ["Copertura media numero patente di guida britannica"](#) a pagina 1280.

- La copertura limitata rileva un modello alfanumerico di 16 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
 Vedere "[Copertura limitata del numero di patente di guida britannica](#)" a pagina 1281.

Copertura ampia numeri delle patenti di guida britanniche

La copertura ampia rileva stringhe di 16 caratteri alfanumerici nel seguente formato: AAAAAD[0,1,5,6]DDDDAAALL, dove A indica un carattere alfanumerico, D una cifra e L una lettera.

Nota: L'opzione di copertura ampia non include nessuno strumento di convalida.

Tabella 40-804 Modelli copertura ampia numeri delle patenti di guida britanniche

Modello
$\backslash w\{5\} \backslash d[0156] \backslash d\{4\} \backslash w\{3\} \backslash l\{2\}$
$\backslash w\{5\} \backslash d[0156] \backslash d\{4\} \backslash w\{3\} \backslash l\{2\}$
$\backslash w\{5\} \backslash d[0156] \backslash d\{4\} \backslash w\{3\} \backslash l\{2\} \backslash d\{2\}$
$\backslash w\{5\} \backslash d[0156] \backslash d\{4\} \backslash w\{3\} \backslash l\{2\} \backslash d\{2\}$

Copertura media numero patente di guida britannica

La copertura media rileva stringhe di 16 caratteri alfanumerici nel seguente formato: AAAAAD[0,1,5,6]DDDDAAALL, dove A indica un carattere alfanumerico, D una cifra e L una lettera.

La prima cifra della sezione numerica può essere solo 0, 1, 5 o 6. Inoltre, la 4° e la 5° cifra della sezione numerica devono essere comprese tra 01 e 31 inclusi.

Tabella 40-805 Criteri copertura media numero patente di guida britannica

Criterio
$\backslash w\{5\} \backslash d[0156] \backslash d\{4\} \backslash w\{3\} \backslash l\{2\}$
$\backslash w\{5\} \backslash d[0156] \backslash d\{4\} \backslash w\{3\} \backslash l\{2\}$
$\backslash w\{5\} \backslash d[0156] \backslash d\{4\} \backslash w\{3\} \backslash l\{2\} \backslash d\{2\}$
$\backslash w\{5\} \backslash d[0156] \backslash d\{4\} \backslash w\{3\} \backslash l\{2\} \backslash d\{2\}$

Tabella 40-806 Convalida copertura media numero patente di guida britannica

Convalida obbligatoria	Descrizione
Patente di guida del Regno Unito	I numeri di patente di guida britannici devono contenere 16 caratteri e i numeri in 8a e 9a posizione devono essere maggiori di 00 e minori di 32.

Copertura limitata del numero di patente di guida britannica

La copertura limitata rileva stringhe di 16 caratteri alfanumerici nel seguente formato: AAAAAD[0,1,5,6]DDDDAAALL, dove A indica un carattere alfanumerico, D una cifra e L una lettera.

La prima cifra può essere solo 0, 1, 5 o 6. Inoltre la 4^a e la 5^a cifra della sezione numerica devono essere comprese tra 01 e 31 inclusi.

La copertura limitata richiede altresì la presenza di una parola chiave associata alla patente di guida E una parola chiave associata al Regno Unito.

Tabella 40-807 Modelli di copertura limitata del numero di patente di guida britannica

Modello
<code>\w{5}\d[0156]\d{4}\w{3}\l{2}</code>
<code>\w{5} \d[0156]\d{4} \w{3}\l{2}</code>
<code>\w{5}\d[0156]\d{4}\w{3}\l{2}\d{2}</code>
<code>\w{5} \d[0156]\d{4} \w{3}\l{2}\d{2}</code>

Tabella 40-808 Convalide della copertura limitata del numero di patente di guida britannica

Convalida obbligatoria	Descrizione
Patente di guida del Regno Unito	I numeri di patente di guida britannici devono contenere 16 caratteri e i numeri in 8a e 9a posizione devono essere maggiori di 00 e minori di 32.
Trova parole chiave : associate alla patente di guida	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: Input: patente di guida, patenti di guida, n.pg, n.pat., n.p., n.p.g.
Trova parole chiave : correlate al Regno Unito	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: Input: britannica, il regno unito, uk, regno unito, regnounito

Numero di tessera elettorale britannico

Il numero di tessera elettorale britannico è il numero di identificazione rilasciato ai cittadini per la registrazione elettorale. Il formato di questo numero è specificato dagli standard governativi dell'Ufficio del Gabinetto del Regno Unito.

L'identificatore di dati Numero di tessera elettorale britannico rileva la presenza del numero di tessera elettorale britannico. Implementa un criterio per rilevare le stringhe che includono da 2 a 3 lettere, seguite da 1 a 4 cifre.

Tabella 40-809 Criterio copertura limitata numero di tessera elettorale britannico

Criterio
$\backslash 1\{2,3\}\backslash d\{1,4\}$

La copertura limitata dell'identificatore di dati Numero di tessera elettorale implementa due convalide per richiedere la presenza di una parola chiave associata al numero di tessera elettorale e una associata al Regno Unito.

Tabella 40-810 Convalide copertura limitata numero di tessera elettorale britannico

Convalide obbligatorie	Descrizione
Trova parole chiave : correlate al numero elettorale	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: electoral #, electoral number, electoral roll #, electoral roll no., electoral roll number, electoral roll#, electoral#, electoralnumber, electoralroll#, electoralrollno (n. elettorale, numero elettorale, n. tessera elettorale, numero tessera elettorale, n.tesseraelettorale, numerotesseraelettorale, numeroelettorale)
Trova parole chiave : correlate al Regno Unito	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: british, the united kingdom, uk, united kingdom, unitedkingdom (britannico, il regno unito, uk, regno unito, regnounito)

Numero NHS (National Health Service) del Regno Unito

Il numero NHS (National Health Service) del Regno Unito è il numero di identificazione personale rilasciato dal National Health Service (NHS, sistema sanitario nazionale) britannico per la gestione dell'assistenza medica.

L'identificatore dati numero NHS (National Health Service) britannico rileva la presenza di un numero di 10 cifre che corrisponde al formato del numero NHS (National Health Service) britannico.

Questo identificatore di dati fornisce due coperture di convalida:

- La copertura media rileva un numero a 10 cifre con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura media Numero NHS \(National Health Service\) britannico](#)" a pagina 1283.
- La copertura limitata rileva un numero a 10 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata numero NHS \(National Health Service\) britannico](#)" a pagina 1284.

Nota: Questo identificatore di dati non fornisce l'opzione di copertura ampia.

Copertura media Numero NHS (National Health Service) britannico

La copertura media include modelli per rilevare i numeri nei formati NHS attualmente definiti: DDD-DDD-DDDD (dove D indica una cifra), con diversi tipi di separatori.

Tabella 40-811 Formati copertura media Numero NHS (National Health Service) britannico

Modello	Descrizione
$\backslash d\{3\}.\backslash d\{3\}.\backslash d\{4\}$	Il formato per il rilevamento del formato DDD-DDD-DDDD separato da punti.
$\backslash d\{3\} \backslash d\{3\} \backslash d\{4\}$	Criterio per il rilevamento del formato DDD-DDD-DDDD separato da spazi.
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{4\}$	Il formato per il rilevamento del formato DDD-DDD-DDDD separato da trattini.

La copertura media include tre strumenti di convalida: uno per convalidare il checksum dell'NHS, un altro per eseguire la convalida numerica utilizzando la cifra finale e l'ultimo per verificare la presenza di una parola chiave correlata all'NHS.

Tabella 40-812 Strumenti di convalida copertura media Numero NHS (National Health Service) britannico

Strumento di convalida	Descrizione
NHS Regno Unito	Checksum NHS Regno Unito.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Strumento di convalida	Descrizione
Trova parole chiave : correlate a NHS	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: servizio sanitario nazionale, NHS

Copertura limitata numero NHS (National Health Service) britannico

La copertura limitata implementa criteri per rilevare numeri nei formati attualmente definiti: DDD-DDD-DDDD (dove D è una cifra), con trattini o spazi di separazione.

Tabella 40-813 Criteri copertura limitata numero NHS (National Health Service) britannico

Criterio	Descrizione
$\backslash d\{3\} \backslash d\{3\} \backslash d\{4\}$	Criterio per il rilevamento del formato DDD-DDD-DDDD separato da spazi.
$\backslash d\{3\}-\backslash d\{3\}-\backslash d\{4\}$	Criterio per il rilevamento del formato DDD-DDD-DDDD separato da trattini.

La copertura limitata implementa quattro convalide: una per convalidare il checksum dell'NHS, un'altra per eseguire la convalida numerica utilizzando la cifra finale, una terza che richiede la presenza di una parola chiave correlata all'NHS e l'ultima per richiedere la presenza di una parola chiave correlata al Regno Unito.

Tabella 40-814 Convalide copertura limitata numero NHS (National Health Service) britannico

Convalida obbligatoria	Descrizione
NHS Regno Unito	Checksum NHS Regno Unito.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave : correlate a NHS	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: servizio sanitario nazionale, NHS
Trova parole chiave : correlate al Regno Unito	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: uk, regno unito, britannico, inghilterra, gb

Numero di previdenza sociale britannico

Il numero di previdenza sociale britannico viene rilasciato dal Department for Work and Pensions (dipartimento per il lavoro e le pensioni) del Regno Unito ai fini dell'identificazione degli individui nell'ambito del programma di previdenza sociale nazionale. È noto anche come numero NI, NINO o NINO.

L'identificatore dati numero di previdenza sociale britannico rileva un criterio alfanumerico di nove caratteri che corrisponde al formato del numero di previdenza sociale britannico.

L'identificatore dati numero di previdenza sociale britannico fornisce tre coperture di convalida:

- La copertura ampia rileva un criterio alfanumerico di nove caratteri senza la convalida. Vedere ["Copertura ampia Numero di previdenza sociale britannico"](#) a pagina 1285.
- La copertura media rileva un criterio alfanumerico di nove caratteri senza la convalida. Vedere ["Copertura media numero di previdenza sociale britannico"](#) a pagina 1286.
- La copertura limitata rileva un modello alfanumerico di nove caratteri senza la convalida. Richiede la disponibilità di parole chiave associate. Vedere ["Copertura limitata numero di previdenza sociale britannico"](#) a pagina 1286.

Copertura ampia Numero di previdenza sociale britannico

La copertura ampia rileva i criteri alfanumerici di nove caratteri nel formato LL DD DD DD L (dove L corrisponde a una lettera e D è una cifra), separati da spazi, punti, trattini o insieme nella stessa stringa.

La prima e la seconda lettera non possono essere D, F, I, Q, U e V. La seconda lettera non può essere O.

Tabella 40-815 Modelli copertura ampia Numero di previdenza sociale britannico

Criteri	Descrizione
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] . \d{2} . \d{2} . \d{2} - [ABCD]	Separato da punti.
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Non separato.
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Separato da spazi.
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] - \d{2} - \d{2} - \d{2} - [ABCD]	Separato dai trattini.
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Cifre in una stringa.

Copertura media numero di previdenza sociale britannico

La copertura media rileva i criteri alfanumerici di nove caratteri nel formato LL DD DD DD L (dove L corrisponde a una lettera e D è una cifra), separati da spazi o insieme nella stessa stringa.

La prima e la seconda lettera non possono essere D, F, I, Q, U e V. La seconda lettera non può essere O.

Tabella 40-816 Criteri copertura media numero di previdenza sociale britannico

Criteri	Descrizione
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Non delimitato.
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Separato da spazi.
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Caratteri in una stringa.

Copertura limitata numero di previdenza sociale britannico

La copertura limitata rileva i criteri alfanumerici di nove caratteri nel formato LL DD DD DD L (dove L corrisponde a una lettera e D è una cifra), separati da spazi o insieme nella stessa stringa.

La prima e la seconda lettera non possono essere D, F, I, Q, U e V. La seconda lettera non può essere O.

Tabella 40-817 Criteri copertura limitata numero di previdenza sociale britannico

Criterio	Descrizione
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Non delimitato.
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{2} \d{2} \d{2} [ABCD]	Separato da spazi.
[A-CEGHJ-PR-TW-Z] [A-CEGHJ-NPR-TW-Z] \d{6} [ABCD]	Caratteri in una stringa.

Tabella 40-818 Convalida copertura limitata numero di previdenza sociale britannico

Convalida obbligatoria	Descrizione
Trova parole chiave : correlate alla previdenza sociale	<p>Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti:</p> <p>insurance no., insurance number, insurance#, insurancenumber, national insurance number, nationalinsurance#, nationalinsurancenumber, nin, nino (n. previdenza sociale, numero previdenza sociale, n.previdenza sociale, numeroprevidenzasociale, numero previdenza sociale nazionale, n.previdenzasocialenazionale, numeroprevidenzasocialenazionale, nin, nino)</p>

Numero di passaporto britannico

Il numero di passaporto britannico identifica un passaporto britannico utilizzando la specifica ufficiale corrente degli standard governativi dell'Ufficio del Gabinetto del Regno Unito.

L'identificatore di dati del numero di passaporto del Regno Unito rileva un numero di nove cifre che corrisponde al formato del numero di passaporto del Regno Unito.

Questo identificatore di dati fornisce tre coperture di convalida:

- La copertura ampia rileva un numero di nove cifre senza la convalida del
Vedere "[Copertura ampia Numero di passaporto britannico](#)" a pagina 1287.
- La copertura media rileva un numero di nove cifre senza la convalida del checksum.
Richiede la disponibilità di parole chiave associate.
Vedere "[Copertura media numero di passaporto britannico](#)" a pagina 1288.
- La copertura limitata rileva un numero di nove cifre senza la convalida del checksum.
Richiede la disponibilità di parole chiave associate.
Vedere "[Copertura limitata numero di passaporto britannico](#)" a pagina 1288.

Copertura ampia Numero di passaporto britannico

La copertura ampia rileva un numero di nove cifre senza la convalida del

Nota: La copertura ampia non include nessuno strumento di convalida.

Tabella 40-819 Modello copertura ampia Numero di passaporto britannico

Modello	Descrizione
\d{9}	Modello per il rilevamento di numeri a 9 cifre.

Copertura media numero di passaporto britannico

La copertura media rileva un numero di nove cifre senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-820 Criterio copertura media numero di passaporto britannico

Criterio	Descrizione
\d{9}	Modello per il rilevamento di numeri a 9 cifre.

Tabella 40-821 Convalide copertura media numero di passaporto britannico

Convalida obbligatoria	Descrizione
Escludi caratteri iniziali	I dati che iniziano con uno qualsiasi dei valori seguenti saranno ignorati: 123456789
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave : correlate a passaporto	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: passaporto, numero di passaporto, n. di passaporto, n.passaporto, numeropassaporto, IDpassaporto

Copertura limitata numero di passaporto britannico

La copertura limitata rileva un numero di nove cifre senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-822 Criterio copertura limitata numero di passaporto britannico

Criterio	Descrizione
\d{9}	Modello per il rilevamento di numeri a 9 cifre.

Tabella 40-823 Convalide copertura limitata numero di passaporto britannico

Convalida obbligatoria	Descrizione
Escludi caratteri iniziali	I dati che iniziano con uno qualsiasi dei valori seguenti saranno ignorati: 123456789
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Convalida obbligatoria	Descrizione
Trova parole chiave : correlate a passaporto	<p>Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>passaporto, numero di passaporto, n. di passaporto, n.passaporto, numeropassaporto, IDpassaporto</p>
Trova parole chiave : correlate al Regno Unito	<p>Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>uk, regno unito, britannico, inghilterra, gb</p>

Codice fiscale britannico

I codice fiscale britannico è un numero di identificazione personale fornito dagli standard governativi dell'Ufficio del Gabinetto del Regno Unito.

L'identificatore di dati codice fiscale britannico rileva un numero di 10 cifre che corrisponde al formato del codice fiscale britannico.

L'identificatore di dati codice fiscale britannico fornisce tre coperture di convalida:

- La copertura ampia rileva un numero di 10 cifre senza la convalida del
Vedere ["Copertura ampia codice fiscale britannico"](#) a pagina 1289.
- La copertura media rileva un numero di 10 cifre senza la convalida del checksum.
Vedere ["Copertura media codice fiscale britannico"](#) a pagina 1290.
- La copertura limitata rileva un numero di 10 cifre senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.
Vedere ["Copertura limitata codice fiscale britannico"](#) a pagina 1290.

Copertura ampia codice fiscale britannico

La copertura ampia rileva un numero di 10 cifre senza la convalida del

Nota: La copertura ampia dell'identificatore dati del Codice fiscale britannico non include nessuno strumento di convalida.

Tabella 40-824 Modello copertura ampia Numero di passaporto britannico

Modello	Descrizione
\d{10}	Modello per il rilevamento di numeri a 10 cifre.

Copertura media codice fiscale britannico

La copertura media rileva un numero di 10 cifre senza la convalida del checksum.

Tabella 40-825 Criterio copertura media codice fiscale britannico

Criterio	Descrizione
\d{10}	Modello per il rilevamento di numeri a 10 cifre.

Tabella 40-826 Convalide di copertura media del codice fiscale britannico

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Escludi caratteri iniziali	I dati che iniziano con uno qualsiasi dei valori seguenti saranno ignorati: 0123456789, 1234567890, 9876543210, 0987654321

Copertura limitata codice fiscale britannico

La copertura limitata rileva un numero di 10 cifre senza la convalida del checksum. Richiede la disponibilità di parole chiave associate.

Tabella 40-827 Criterio copertura limitata codice fiscale britannico

Criterio	Descrizione
\d{10}	Modello per il rilevamento di numeri a 10 cifre.

Tabella 40-828 Convalide copertura limitata codice fiscale britannico

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Convalida obbligatoria	Descrizione
Escludi caratteri iniziali	I dati che iniziano con uno qualsiasi dei valori seguenti saranno ignorati: 0123456789, 1234567890, 9876543210, 0987654321
Trova parole chiave : correlate al codice fiscale	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: tax id, tax id no., tax id number, tax identification, tax identification#, tax no., tax#, taxid# (codice fiscale)

Numero di partita IVA britannico (VAT)

L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Nel Regno Unito, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.

L'identificatore di dati del numero di partita IVA britannico (VAT) rileva un modello alfanumerico di 7-14 caratteri che corrisponde al formato del numero di partita IVA britannico (VAT).

L'identificatore di dati del Numero di partita IVA britannico (VAT) fornisce tre coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di 7-14 caratteri che iniziano con **GB** senza la convalida del checksum.
Vedere "[Copertura ampia del numero di partita IVA britannico \(VAT\)](#)" a pagina 1291.
- La copertura media rileva un modello alfanumerico di 7-14 caratteri che iniziano con **GB** con la convalida del checksum.
Vedere "[Copertura media del numero di partita IVA britannico \(VAT\)](#)" a pagina 1292.
- La copertura limitata rileva un modello alfanumerico di 7-14 caratteri che iniziano con **GB** con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del numero di partita IVA britannico \(VAT\)](#)" a pagina 1293.

Copertura ampia del numero di partita IVA britannico (VAT)

La copertura ampia rileva un modello alfanumerico di 7-14 caratteri senza la convalida del checksum.

Tabella 40-829 Modelli di copertura ampia numero di partita IVA britannico (VAT)

Modelli
[Gg] [Bb] [Gg] [Dd] \d{3}

Modelli
[Gg] [Bb] [Hh] [Aa] \d{3}
[Gg] [Bb] [Gg] [Dd] \d{3}
[Gg] [Bb] [Hh] [Aa] \d{3}
[Gg] [Bb] \d{9}
[Gg] [Bb] \d{12}
[Gg] [Bb] \d{9}
[Gg] [Bb] \d{12}
[Gg] [Bb] \d{3} \d{4} \d{2}
[Gg] [Bb] \d{3} \d{4} \d{2} \d{3}

Tabella 40-830 Convalide di copertura ampia del numero di partita IVA britannico (VAT)

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	<p>I modelli che terminano con le seguenti stringhe di carattere verranno esclusi dalla corrispondenza:</p> <p>000000000, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999, 000000000000, 111111111111, 222222222222, 333333333333, 444444444444, 555555555555, 666666666666, 777777777777, 888888888888, 999999999999, 000, 111, 222, 333, 444, 555, 666, 777, 888, 999</p>

Copertura media del numero di partita IVA britannico (VAT)

La copertura media rileva un modello alfanumerico di 7-14 caratteri con la convalida del checksum.

Tabella 40-831 Modelli di copertura media del numero di partita IVA britannico (VAT)

Modelli
[Gg] [Bb] [Gg] [Dd] \d{3}
[Gg] [Bb] [Hh] [Aa] \d{3}

Modelli
[Gg] [Bb] [Gg] [Dd] \d{3}
[Gg] [Bb] [Hh] [Aa] \d{3}
[Gg] [Bb] \d{9}
[Gg] [Bb] \d{12}
[Gg] [Bb] \d{9}
[Gg] [Bb] \d{12}
[Gg] [Bb] \d{3} \d{4} \d{2}
[Gg] [Bb] \d{3} \d{4} \d{2} \d{3}

Tabella 40-832 Convalida di copertura media del numero di partita IVA britannico (VAT)

Strumento di convalida obbligatorio	Descrizione
Controllo di convalida numero di partita IVA del Regno Unito	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di partita IVA britannico (VAT)

La copertura limitata rileva un modello alfanumerico di 7-14 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-833 Modelli di copertura limitata del numero di partita IVA britannico (VAT)

Criterio
[Gg] [Bb] [Gg] [Dd] \d{3}
[Gg] [Bb] [Hh] [Aa] \d{3}
[Gg] [Bb] [Gg] [Dd] \d{3}
[Gg] [Bb] [Hh] [Aa] \d{3}
[Gg] [Bb] \d{9}
[Gg] [Bb] \d{12}
[Gg] [Bb] \d{9}
[Gg] [Bb] \d{12}

Criterio
[Gg] [Bb] \d{3} \d{4} \d{2}
[Gg] [Bb] \d{3} \d{4} \d{2} \d{3}

Tabella 40-834 Convalide di copertura limitata del numero di partita IVA britannico (VAT)

Strumento di convalida obbligatorio	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Escludi caratteri finali	<p>I modelli che terminano con le seguenti stringhe di carattere verranno esclusi dalla corrispondenza:</p> <p>000000000, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999, 000000000000, 111111111111, 222222222222, 333333333333, 444444444444, 555555555555, 666666666666, 777777777777, 888888888888, 999999999999, 000, 111, 222, 333, 444, 555, 666, 777, 888, 999</p>
Controllo di convalida numero di partita IVA del Regno Unito	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	<p>Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti:</p> <p>Input:</p> <p>n. partita iva, numero di partita iva, n.iva, numero imposta sul valore aggiunto, n. iva;"</p>

Passaporto ucraino (interno)

Un documento di identità rilasciato ai cittadini ucraini per l'uso nazionale. È stato sostituito dalla carta di identità ucraina a partire dal 2016, ma i passaporti esistenti sono ancora validi.

L'identificatore di dati del passaporto Ucraino (interno) rileva un numero di nove cifre che corrisponde al formato del passaporto Ucraino (interno).

L'identificatore di dati del passaporto ucraino (interno) fornisce due coperture di rilevamento:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum. Vedere "[Copertura ampia del passaporto ucraino \(interno\)](#)" a pagina 1295.
- La copertura limitata rileva un numero di nove cifre. Richiede inoltre la presenza di parole chiave associate.

Vedere ["Copertura limitata del passaporto ucraino \(interno\)"](#) a pagina 1295.

Copertura ampia del passaporto ucraino (interno)

La copertura ampia rileva un numero di nove cifre senza la convalida del checksum.

Tabella 40-835 Criterio della copertura ampia del passaporto ucraino (interno)

Criterio
$\backslash d\{9\}$

Tabella 40-836 Convalida di copertura ampia del passaporto ucraino (interno)

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata del passaporto ucraino (interno)

La copertura limitata rileva un numero di nove cifre. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-837 Modello di copertura limitata del passaporto ucraino (interno)

Criterio
$\backslash d\{9\}$

Tabella 40-838 Convalide di copertura limitata del passaporto ucraino (interno)

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.

Strumento di convalida obbligatorio	Descrizione
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>passaporto, Passaporto ucraino, numero di passaporto, numero passaporto</p> <p>паспорт, паспорт України, номер паспорта, персональний</p>

Carta di identità ucraina

La carta di identità ucraina presenta un numero di 15 cifre rilasciato ai cittadini ucraini. È utilizzato come documento identificativo al posto del passaporto interno ucraino a partire da gennaio 2016.

L'identificatore di dati della carta di identità ucraina rileva un numero 15 cifre che corrisponde al formato della carta di identità ucraina.

L'identificatore di dati della carta di identità ucraina fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 15 cifre senza la convalida del checksum. Vedere "[Copertura ampia della carta di identità ucraina](#)" a pagina 1296.
- La copertura media rileva un numero a 15 cifre con la convalida del checksum. Vedere "[Copertura media della carta di identità ucraina](#)" a pagina 1297.
- La copertura limitata rileva un numero a 15 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata della carta di identità ucraina](#)" a pagina 1297.

Copertura ampia della carta di identità ucraina

La copertura ampia rileva un numero di 15 cifre senza la convalida del checksum.

Tabella 40-839 Modelli di copertura ampia della carta di identità ucraina

Modello
<code>\d{4}[01]\d[0123]\d-\d{7}</code>
<code>\d{4}[01]\d[0123]\d{8}</code>
<code>\d{4}[01]\d[0123]\d \d{7}</code>

Tabella 40-840 Convalida di copertura ampia della carta di identità ucraina

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media della carta di identità ucraina

La copertura media rileva un numero a 15 cifre con la convalida del checksum.

Tabella 40-841 Modelli di copertura media della carta di identità ucraina

$\backslash d\{4\}[01]\backslash d[0123]\backslash d-\backslash d\{7\}$
$\backslash d\{4\}[01]\backslash d[0123]\backslash d\{8\}$
$\backslash d\{4\}[01]\backslash d[0123]\backslash d \backslash d\{7\}$

Tabella 40-842 Convalide di copertura media della carta di identità ucraina

Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo della carta di identità ucraina	Verifica che le prime otto cifre siano una data formattata correttamente.

Copertura limitata della carta di identità ucraina

La copertura limitata rileva un numero a 15 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-843 Modelli di copertura limitata della carta di identità ucraina

Modello
$\backslash d\{4\}[01]\backslash d[0123]\backslash d-\backslash d\{7\}$
$\backslash d\{4\}[01]\backslash d[0123]\backslash d\{8\}$
$\backslash d\{4\}[01]\backslash d[0123]\backslash d \backslash d\{7\}$

Tabella 40-844 Convalide di copertura limitata della carta di identità ucraina

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Controllo della carta di identità ucraina	Verifica che le prime otto cifre siano una data formattata correttamente.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>Carta di identità ucraina, carta di identità посвідчення особи України</p>

Passaporto ucraino (internazionale)

Il passaporto internazionale ucraino è un documento utilizzato dai cittadini ucraini per viaggiare all'estero.

L'identificatore di dati del passaporto ucraino (internazionale) rileva un modello alfanumerico di otto caratteri che corrisponde al formato del passaporto ucraino (internazionale).

L'identificatore di dati del passaporto ucraino (internazionale) fornisce due coperture di rilevamento:

- La copertura ampia rileva un modello alfanumerico di otto caratteri senza la convalida del checksum.
Vedere "[Copertura ampia del passaporto ucraino \(internazionale\)](#)" a pagina 1298.
- La copertura limitata rileva un modello alfanumerico di otto caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere "[Copertura limitata del passaporto ucraino \(internazionale\)](#)" a pagina 1299.

Copertura ampia del passaporto ucraino (internazionale)

La copertura ampia rileva un modello alfanumerico di otto caratteri senza la convalida del checksum.

Tabella 40-845 Modello di copertura ampia del passaporto ucraino (internazionale)

Modello
\w{2}\d{6}

Tabella 40-846 Convalida di copertura ampia del passaporto ucraino (internazionale)

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura limitata del passaporto ucraino (internazionale)

La copertura limitata rileva un modello alfanumerico di otto caratteri senza la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-847 Modello di copertura limitata del passaporto ucraino (internazionale)

Modello
\w{2}\d{6}

Tabella 40-848 Convalide di copertura limitata del passaporto ucraino (internazionale)

Strumento di convalida obbligatorio	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i numeri vicini.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: passaporto, Passaporto ucraino, numero di passaporto, numero passaporto паспорт, паспорт України, номер паспорта

Numero di identificazione personale degli Emirati Arabi Uniti

Negli Emirati Arabi Uniti, ogni cittadino o residente ha un numero di identificazione personale unico. Il numero di identificazione personale degli Emirati Arabi Uniti viene utilizzato come strumento di identificazione dal governo e alcuni enti privati.

L'identificatore di dati per il Numero di identificazione personale degli Emirati Arabi Uniti rileva un numero di 15 cifre che corrisponde al formato del Numero di identificazione personale degli Emirati Arabi Uniti.

L'identificatore di dati di sistema del numero di identificazione personale degli Emirati Arabi Uniti fornisce tre coperture di rilevamento:

- La copertura ampia rileva un numero di 15 cifre senza la convalida del checksum. Vedere "[Copertura ampia numero di identificazione personale degli Emirati Arabi Uniti](#)" a pagina 1300.
- La copertura media rileva un numero a 15 cifre con la convalida del checksum. Vedere "[Copertura media numero di identificazione personale degli Emirati Arabi Uniti](#)" a pagina 1301.
- La copertura limitata rileva un numero a 15 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate. Vedere "[Copertura limitata numero di identificazione personale degli Emirati Arabi Uniti](#)" a pagina 1301.

Copertura ampia numero di identificazione personale degli Emirati Arabi Uniti

La copertura ampia rileva un numero di 15 cifre senza la convalida del checksum.

Tabella 40-849 Motivi copertura ampia numero di identificazione personale degli Emirati Arabi Uniti

Criterio
\d{15}
\d{3}-\d{4}-\d{7}-\d{1}

Tabella 40-850 Convalide copertura ampia numero di identificazione personale degli Emirati Arabi Uniti

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione personale degli Emirati Arabi Uniti

La copertura media rileva un numero a 15 cifre con la convalida del checksum.

Tabella 40-851 Criteri copertura media numero di identificazione personale degli Emirati Arabi Uniti

Criterio
$\backslash d\{15\}$
$\backslash d\{3\}-\backslash d\{4\}-\backslash d\{7\}-\backslash d\{1\}$

Tabella 40-852 Convalida copertura media numero di identificazione personale degli Emirati Arabi Uniti

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo Luhn	Calcola il checksum Luhn e lo utilizza per convalidare il criterio.

Copertura limitata numero di identificazione personale degli Emirati Arabi Uniti

La copertura limitata rileva un numero a 15 cifre con convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-853 Criteri copertura limitata numero di identificazione personale degli Emirati Arabi Uniti

Criterio
$\backslash d\{15\}$
$\backslash d\{3\}-\backslash d\{4\}-\backslash d\{7\}-\backslash d\{1\}$

Tabella 40-854 Strumenti di convalida copertura limitata numero di identificazione personale degli Emirati Arabi Uniti

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo Luhn	Calcola il checksum Luhn e lo utilizza per convalidare il criterio.
Trova parole chiave	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>PID, numero di previdenza, numero ID personale, n. identificazione personale, n. identificazione univoco, n. identificativo personale, N.IDpersonale, n.previdenza, n.IDprevidenza, n.IDunivoco</p> <p>الهوية الشخصية رقم, فريدة من نوعها هوية رقم, التأمين رقم, هوية فريدة, ##التأمين رقم</p>

US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

Il codice di identificazione fiscale statunitense (ITIN) è utilizzato per l'elaborazione delle imposte e rilasciato dall'Internal Revenue Service (IRS) statunitense. L'IRS rilascia questi codici per registrare le persone non idonee ai Social Security Number (SSN).

L'identificatore dati US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense) individua numeri di nove cifre che corrispondono al formato del codice ITIN statunitense.

L'identificatore dati US Individual Tax Identification Number fornisce tre coperture di convalida:

- La copertura ampia rileva un numero di nove cifre senza la convalida del
Vedere "[Copertura ampia US Individual Tax Identification Number \(ITIN - codice di identificazione fiscale statunitense\)](#)" a pagina 1303.
- La copertura media rileva un numero di nove cifre senza la convalida del checksum.
Vedere "[Copertura media US Individual Tax Identification Number \(ITIN - codice di identificazione fiscale statunitense\)](#)" a pagina 1303.

- La copertura limitata rileva un numero di nove cifre senza la convalida del checksum. Richiede la disponibilità di parole chiave associate. Vedere "Copertura limitata US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)" a pagina 1304.

Copertura ampia US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

La copertura ampia rileva numeri a nove cifre nel formato DDD-DDD-DDD con trattini, spazi, punti o barre di separazione o senza separatori.

Il numero deve iniziare con 9 e avere 7 o 8 come quarta cifra.

Nota: La copertura ampia dell'identificatore dati dell'US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense) non include nessuno strumento di convalida.

Tabella 40-855 Modelli copertura ampia US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

Criteri	Descrizione
9\{2}[78]\d{4}	Modello per il rilevamento del formato ITIN senza separatori.
9\{2}\[\[78]\d\]\d{4}	Modello per il rilevamento del formato ITIN senza separatori.
9\d{2}/[78]\d/\d{4}	Modello per il rilevamento del formato ITIN separato da barre.
9\d{2}].[78]\d.\d{4}	Criterio per il rilevamento del formato ITIN separato da punti.
9\d{2} [78]\d \d{4}	Criterio per il rilevamento del formato ITIN separato da spazi.
9\d{2}-[78]\d-\d{4}	Modello per il rilevamento del formato ITIN separato da trattini.

Copertura media US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

La copertura media rileva numeri di nove cifre nel formato DDD-DD-DDDD separati con trattini, spazi o punti.

Il numero deve iniziare con 9 e avere 7 o 8 come quarta cifra.

Tabella 40-856

Criteri copertura media US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

Criteri	Descrizione
9\d{2}.[78]\d.\d{4}	Criterio per il rilevamento del formato ITIN separato da punti.
9\d{2} [78]\d \d{4}	Criterio per il rilevamento del formato ITIN separato da spazi.
9\d{2}-[78]\d-\d{4}	Modello per il rilevamento del formato ITIN separato da trattini.

Tabella 40-857

Convalida copertura media US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

La copertura limitata rileva numeri a nove cifre con il criterio DDD-DD-DDDD separati da trattini o spazi.

Il numero deve iniziare con 9 e avere 7 o 8 come quarta cifra.

Tabella 40-858

Criteri copertura limitata US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

Criteri	Descrizione
9\d{2} [78]\d \d{4}	Criterio per il rilevamento del formato ITIN separato da spazi.
9\d{2}-[78]\d-\d{4}	Modello per il rilevamento del formato ITIN separato da trattini.

Tabella 40-859

Convalide copertura limitata US Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense)

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Trova parole chiave : correlate a ITIN	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: Input: individual taxpayer identification number, itin, i.t.i.n. (numero di identificazione contribuente singolo)

Numero di passaporto statunitense

I passaporti degli Stati Uniti sono rilasciati ai cittadini degli Stati Uniti d'America. Sono rilasciati unicamente dal Dipartimento di Stato degli Stati Uniti.

L'identificatore di dati Numero di passaporto statunitense rileva un numero di 8 o 9 cifre che corrisponde al formato del Numero di passaporto statunitense.

L'identificatore di dati Numero di passaporto statunitense fornisce due coperture di rilevamento:

- La copertura ampia rileva un criterio valido del Numero di passaporto statunitense. Vedere ["Copertura ampia Numero di passaporto statunitense"](#) a pagina 1305.
- La copertura limitata rileva un criterio valido del Numero di passaporto statunitense. Richiede inoltre la presenza di parole chiave associate. Vedere ["Copertura limitata Numero di passaporto statunitense"](#) a pagina 1306.

Copertura ampia Numero di passaporto statunitense

La copertura ampia rileva un criterio valido del Numero di passaporto statunitense.

Tabella 40-860 Modelli di copertura ampia Numero di passaporto statunitense

Modelli
\d{8}
\d{9}

Tabella 40-861 Convalide di copertura ampia Numero di passaporto statunitense

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Convalide obbligatorie	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Copertura limitata Numero di passaporto statunitense

La copertura limitata rileva un criterio valido del Numero di passaporto statunitense. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-862 Criteri di copertura limitata Numero di passaporto statunitense

Criteri
\d{8}
\d{9}

Tabella 40-863 Convalide di copertura limitata Numero di passaporto statunitense

Convalide obbligatorie	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Trova parole chiave	<p>Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>passport, Passport, U.S. Passport, u.s. passport, Passport Card, Passport Book, passport card, passport book, passaporto, Passaporto, Passaporto statunitense, passaporto USA, Tessera passaporto, Libretto passaporto, tessera passaporto, libretto passaporto</p>

Social Security Number (SSN) statunitense

Nota: A partire dalla versione 12.5 di Symantec Data Loss Prevention, l'identificatore dati del Social Security Number (SSN) statunitense è sostituito dall'identificatore dati Social Security Number (SSN) statunitense randomizzato. I modelli di politica che utilizzano l'identificatore dati del Social Security Number (SSN) statunitense sono aggiornati per l'utilizzo dell'identificatore dati del Social Security Number (SSN) statunitense randomizzato. Symantec consiglia di aggiornare le politiche SSN per utilizzare l'identificatore dati Social Security Number (SSN) statunitense randomizzato. Vedere "[Social Security Number \(SSN\) statunitense randomizzato](#)" a pagina 1218.

L'Individual Tax Identification Number (ITIN - codice di identificazione fiscale statunitense) statunitense è un numero di identificazione personale rilasciato dalla Social Security Administration del governo degli Stati Uniti. Questo numero, utilizzato principalmente per la gestione del programma di previdenza sociale, è largamente impiegato come numero di identificazione personale in numerose occasioni.

L'identificatore dati Social Security Number (SSN) statunitense individua numeri di nove cifre che corrispondono al formato del numero di previdenza sociale degli Stati Uniti.

L'identificatore dati Social Security Number (SSN) statunitense fornisce tre coperture di convalida:

- La copertura ampia rileva un numero di nove cifre senza la convalida del checksum. Vedere "[Copertura ampia del numero di previdenza sociale \(SSN\) statunitense](#)" a pagina 1307.
- La copertura media rileva un numero di nove cifre senza la convalida del checksum. Vedere "[Copertura media Social Security Number \(SSN\) statunitense](#)" a pagina 1308.
- La copertura limitata rileva un numero di nove cifre senza la convalida del checksum. Richiede la disponibilità di parole chiave associate. Vedere "[Copertura limitata Social Security Number \(SSN\) statunitense](#)" a pagina 1309.

Copertura ampia del numero di previdenza sociale (SSN) statunitense

La copertura ampia rileva numeri a nove cifre nel formato DDD-DDD-DDD con trattini, spazi, punti o barre di separazione o senza separatori.

Il numero deve iniziare con 9 e avere 7 o 8 come quarta cifra.

Tabella 40-864 Modelli a copertura ampia del numero di previdenza sociale (SSN)

Modello	Descrizione
<code>\d{3}-\d{2}-\d{4}</code>	Cerca la corrispondenza con il formato standard SSN, ovvero tre cifre seguite da un trattino, due cifre, un trattino e altre quattro cifre.

Modello	Descrizione
\d{3}.\d{2}.\d{4}	Cerca la corrispondenza del formato SSN delimitato da punti.
\d{3} \d{2} \d{4}	Cerca la corrispondenza del formato SSN delimitato da spazi.
\d{3}\\\d{2}\\\d{4}	Cerca la corrispondenza del formato SSN delimitato da barre rovesciate.
\d{3}/\d{2}/\d{4}	Cerca la corrispondenza del formato SSN delimitato da barre rovesciate.
\d{9}	Cerca la corrispondenza di qualsiasi numero di 9 cifre non delimitato.

Tabella 40-865 Strumenti di convalida copertura ampia del numero di previdenza sociale (SSN)

Strumento di convalida	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
SSN avanzato	Verifica che i gruppi che compongono il numero SSN contengano zeri, che il numero area (primo gruppo) sia inferiore a 773 e diverso da 666, che il delimitatore dei gruppi sia lo stesso, che il numero non sia costituito da cifre uguali tra loro e che non sia riservato alla pubblicità (123-45-6789, 987-65-432x).
Numero gruppo/area SSN	Per un dato numero area (primo gruppo), è possibile che la SSA non abbia assegnato tutti i numeri gruppo (secondo gruppo). Lo strumento di convalida elimina i numeri SSN con numeri gruppo non validi.

Copertura media Social Security Number (SSN) statunitense

La copertura media rileva numeri di nove cifre nel formato DDD-DD-DDDD separati con trattini, spazi o punti.

Tabella 40-866 Criteri copertura media Social Security Number (SSN) statunitense

Criterio	Descrizione
\d{3}-\d{2}-\d{4}	Cerca la corrispondenza con il formato standard SSN, ovvero tre cifre seguite da un trattino, due cifre, un trattino e altre quattro cifre.
\d{3}.\d{2}.\d{4}	Cerca la corrispondenza del formato SSN delimitato da punti.
\d{3} \d{2} \d{4}	Cerca la corrispondenza del formato SSN delimitato da spazi.

Tabella 40-867 Convalida copertura media Social Security Number (SSN) statunitense

Convalida	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalida	Descrizione
SSN avanzato	Verifica che i gruppi che compongono il numero SSN contengano zeri, che il numero area (primo gruppo) sia inferiore a 773 e diverso da 666, che il delimitatore dei gruppi sia lo stesso, che il numero non sia costituito da cifre uguali tra loro e che non sia riservato alla pubblicità (123-45-6789, 987-65-432x).
Numero gruppo/area SSN	Per un dato numero area (primo gruppo), è possibile che la SSA non abbia assegnato tutti i numeri gruppo (secondo gruppo). Lo strumento di convalida elimina i numeri SSN con numeri gruppo non validi.

Copertura limitata Social Security Number (SSN) statunitense

La copertura limitata rileva numeri a nove cifre con il criterio DDD-DD-DDDD separati da trattini o spazi o senza separatori.

Tabella 40-868 Criteri copertura limitata Social Security Number (SSN) statunitense

Criterio	Descrizione
\d{3}-\d{2}-\d{4}	Cerca la corrispondenza con il formato standard SSN, ovvero tre cifre seguite da un trattino, due cifre, un trattino e altre quattro cifre.
\d{3} \d{2} \d{4}	Cerca la corrispondenza del formato SSN delimitato da spazi.
\d{9}	Cerca la corrispondenza con un qualsiasi numero di 9 cifre non delimitato.

Tabella 40-869 Convalide copertura limitata Social Security Number (SSN)

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
SSN avanzato	Verifica che i gruppi che compongono il numero SSN contengano zeri, che il numero area (primo gruppo) sia inferiore a 773 e diverso da 666, che il delimitatore dei gruppi sia lo stesso, che il numero non sia costituito da cifre uguali tra loro e che non sia riservato alla pubblicità (123-45-6789, 987-65-432x).
Numero gruppo/area SSN	Per un dato numero area (primo gruppo), è possibile che la SSA non abbia assegnato tutti i numeri gruppo (secondo gruppo). Lo strumento di convalida elimina i numeri SSN con numeri gruppo non validi.
Trova parole chiave : associate al numero SSN	Almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti: social security number, ssn, ss# (numero di previdenza sociale, ssn)

Codici di avviamento postale Zip+4 statunitensi

Negli Stati Uniti, un codice ZIP+4 utilizza il normale codice a 5 cifre più 4 cifre addizionali per identificare un segmento geografico all'interno dell'area di consegna da 5 cifre che potrebbe utilizzare un ulteriore identificatore per consentire un'efficiente organizzazione e consegna della posta.

L'identificatore di dati Codici di avviamento postale Zip+4 statunitensi rileva criteri validi dei Codici di avviamento postale Zip+4 statunitensi.

L'identificatore di dati Codici di avviamento postale Zip+4 statunitensi fornisce tre coperture di rilevamento:

- La copertura ampia rileva un criterio valido del Codice di avviamento postale Zip+4 statunitense senza la convalida del checksum.
Vedere ["Copertura ampia Codici di avviamento postale Zip+4 statunitensi"](#) a pagina 1310.
- La copertura media rileva un criterio valido del Codice di avviamento postale Zip+4 statunitense con la convalida del checksum.
Vedere ["Copertura media Codici di avviamento postale Zip+4 statunitensi"](#) a pagina 1311.
- La copertura limitata rileva un criterio valido del Codice di avviamento postale Zip+4 statunitense con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata Codici di avviamento postale Zip+4 statunitensi"](#) a pagina 1311.

Copertura ampia Codici di avviamento postale Zip+4 statunitensi

La copertura ampia rileva un criterio valido del Codice di avviamento postale Zip+4 statunitense senza la convalida del checksum.

Tabella 40-870 Criteri di copertura ampia Codici di avviamento postale Zip+4 statunitensi

Criterio
$\set{1}{2}[\]\set{5}[-]\set{4}$
$\set{1}{2}[\]\set{9}$

Tabella 40-871 Convalida di copertura ampia Codici di avviamento postale Zip+4 statunitensi

Convalida obbligatoria	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 000000000, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999

Copertura media Codici di avviamento postale Zip+4 statunitensi

La copertura media rileva un criterio valido del Codice di avviamento postale Zip+4 statunitense con la convalida del checksum.

Tabella 40-872 Criteri di copertura media Codici di avviamento postale Zip+4 statunitensi

Criteri
$\backslash 1\{2\}[]\backslash d\{5\}[-]\backslash d\{4\}$
$\backslash 1\{2\}[]\backslash d\{9\}$

Tabella 40-873 Convalide di copertura media Codici di avviamento postale Zip+4 statunitensi

Convalida obbligatoria	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 000000000, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999
Verifica di convalida codici di avviamento postale Zip+4	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata Codici di avviamento postale Zip+4 statunitensi

La copertura limitata rileva un criterio valido del Codice di avviamento postale Zip+4 statunitense con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-874 Criteri di copertura limitata Codici di avviamento postale Zip+4 statunitensi

Criteri
$\backslash 1\{2\}[]\backslash d\{5\}[-]\backslash d\{4\}$

Criteri	
\l{2}[]\d{9}	
Tabella 40-875 Convalide di copertura limitata Codici di avviamento postale Zip+4 statunitensi	
Convalida obbligatoria	Descrizione
Escludi caratteri finali	Qualunque numero che termina con i seguenti caratteri è escluso dalla corrispondenza: 000000000, 111111111, 222222222, 333333333, 444444444, 555555555, 666666666, 777777777, 888888888, 999999999
Verifica di convalida codici di avviamento postale Zip+4	Calcola il checksum e lo utilizza per convalidare il modello.
Trova parole chiave	Quando questa opzione è selezionata, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti. Input: US zip code, zip code, zip+4 code, US zip+4 code, codice postale statunitense, codice postale, codice Zip+4, codice Zip+4 statunitense

Numero di identificazione nazionale venezuelano

In Venezuela, ogni cittadino e residente ha un numero di identificazione nazionale venezuelano (Venezuela Cédula de Identidad). Il numero di identificazione nazionale venezuelano è utilizzato sui documenti di identità e rende possibile abbinare il numero a una persona.

L'identificatore di dati per il Numero di identificazione nazionale venezuelano rileva una stringa alfanumerica di 10 caratteri e cifre che corrisponde al formato del Numero di identificazione nazionale venezuelano.

Questo identificatore di dati fornisce le seguenti coperture di rilevamento:

- La copertura ampia rileva una stringa alfanumerica di 10 caratteri senza la convalida del checksum.
Vedere ["Copertura ampia numero di identificazione nazionale venezuelano"](#) a pagina 1313.
- La copertura media rileva una stringa alfanumerica di 10 caratteri con la convalida del checksum.
Vedere ["Copertura media numero di identificazione nazionale venezuelano"](#) a pagina 1313.

- La copertura limitata rileva una stringa alfanumerica di 10 caratteri che supera la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.
Vedere ["Copertura limitata del numero di identificazione nazionale venezuelano"](#) a pagina 1314.

Copertura ampia numero di identificazione nazionale venezuelano

La copertura ampia rileva una stringa alfanumerica di 10 caratteri senza la convalida del checksum.

Tabella 40-876 Criteri copertura ampia numero di identificazione nazionale venezuelano

Criterio
[VEJPGvejpg] [-]\d{2}.\d{3}.\d{3} [-]\d
[VEJPGvejpg] [-]\d{8} [-]\d
[VEJPGvejpg]\d{9}

Tabella 40-877 Convalida copertura ampia numero di identificazione nazionale venezuelano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.

Copertura media numero di identificazione nazionale venezuelano

La copertura media rileva una stringa alfanumerica di 10 caratteri con la convalida del checksum.

Tabella 40-878 Criteri copertura media numero di identificazione nazionale venezuelano

Criterio
[VEJPGvejpg] [-]\d{2}.\d{3}.\d{3} [-]\d
[VEJPGvejpg] [-]\d{8} [-]\d
[VEJPGvejpg]\d{9}

Tabella 40-879 Convalida copertura media numero di identificazione nazionale venezuelano

Convalida obbligatoria	Descrizione
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.

Convalida obbligatoria	Descrizione
Controllo di convalida numero di identificazione nazionale venezuelano	Calcola il checksum e lo utilizza per convalidare il modello.

Copertura limitata del numero di identificazione nazionale venezuelano

La copertura limitata rileva una stringa alfanumerica di 10 caratteri con la convalida del checksum. Richiede inoltre la presenza di parole chiave associate.

Tabella 40-880 Criteri di copertura limitata del numero di identificazione nazionale venezuelano

Criterio
[VEJPGvejpg] [-]\d{2}.\d{3}.\d{3} [-]\d
[VEJPGvejpg] [-]\d{8} [-]\d
[VEJPGvejpg]\d{9}

Tabella 40-881 Convalide di copertura limitata del numero di identificazione nazionale venezuelano

Convalida obbligatoria	Descrizione
Cifre duplicate	Consente di verificare che una stringa non sia composta da cifre tutte uguali.
Delimitatore numero	Convalida una corrispondenza verificando i caratteri vicini.
Controllo di convalida numero di identificazione nazionale venezuelano	Calcola il checksum e lo utilizza per convalidare il modello.

Convalida obbligatoria	Descrizione
<p>Trova parole chiave</p>	<p>Quando si utilizza questa opzione, almeno una delle parole o frasi chiave seguenti deve essere presente nei dati corrispondenti.</p> <p>Input:</p> <p>numero ID nazionale, NID, numero di identificazione nazionale, n ID nazionale, PID, numero di previdenza sociale, numero di identificazione personale, n identificazione personale, n identificazione univoca, n idpersonale#, IDunivoco #, n. nazionale di identità#, numero nazionale identità#</p> <p>cédula de identidad número, clave única de identidad, personal de identidad clave, personal de identidad, número de identificación nacional, número ID nacional</p>

Libreria dei modelli di politica

Il capitolo contiene i seguenti argomenti:

- Modello della politica Relazione Caldicott
- Modello della politica Numeri di previdenza sociale (SIN) canadesi
- Modello di politica CAN-SPAM Act
- Modello della politica della legge colombiana sulla protezione dei dati personali 1581
- Modello politica Siti caricamento spyware comuni
- Modello di politica Comunicazioni con i concorrenti
- Modello della politica Documenti riservati
- Modello della politica Numeri di carta di credito
- Modello di politica Protezione dei dati dei clienti
- Modello della politica Data Protection Act 1998 (legge sulla protezione dei dati del 1998)
- Modello della politica Direttive UE sulla protezione dei dati
- Modello di politica Classificazione GENSER Defense Message System (DMS)
- Modello della politica Documenti di progettazione
- Modello di politica Protezione dei dati dei dipendenti
- Modello della politica Dati crittografati
- Modello di politica Export Administration Regulations (EAR)

- Modello di politica FACTA 2003 (regole Red Flag)
- Modello di politica Informazioni finanziarie
- Modello della politica Siti Web non consentiti
- Modello politica Gioco d'azzardo
- Regolamento generale per la protezione dei dati (attività bancarie e finanza)
- Regolamento generale per la protezione dei dati (identità digitale)
- Regolamento generale per la protezione dei dati (identificazione governativa)
- Regolamento generale per la protezione dei dati (sanità e assicurazioni)
- Regolamento generale per la protezione dei dati (profilo personale)
- Regolamento generale per la protezione dei dati (viaggi)
- Modello di politica Gramm-Leach-Bliley
- Modello di politica HIPAA e HITECH (incluso PHI)
- Modello di politica Human Rights Act (legge sui diritti umani) del 1998
- Modello di politica Sostanze illegali
- Modello della politica Codici identificativi dei contribuenti (ITIN)
- Modello di politica International Traffic in Arms Regulations (ITAR)
- Modello della politica File multimediali
- Medicare e Medicaid (incluso PHI)
- Modello della politica Contratti di acquisizione e fusione
- Modello di politica Regola NASD 2711 e regole NYSE 351 e 472
- Modello di politica Regola NASD 3010 e regola NYSE 342
- Modello di politica Linee guida sulla sicurezza del NERC per le società elettriche
- Modello della politica Diagrammi di rete
- Modello della politica Sicurezza di rete
- Modello di politica Linguaggio offensivo
- Modello di politica OFAC (Ufficio per il Controllo dei Fondi Stranieri)
- Modello di politica Memorandum OMB 06-16 e disposizioni FIPS 199

- Modello della politica File di password
- Modello della politica Payment Card Industry (PCI) Data Security Standard
- Modello di politica PIPEDA
- Modello di politica Informazioni sui prezzi
- Modello della politica Dati di progetto
- Modello di politica File multimediali proprietari
- Modello della politica Documenti di pubblicazione
- Modello politica Linguaggio razzista
- Modello della politica File con restrizioni
- Modello della politica Destinatari con restrizioni
- Modello della politica Curriculum
- Modello della politica Sarbanes-Oxley
- Modello della politica Normativa sull'imparzialità della trasparenza SEC
- Modello di politica Linguaggio sessualmente esplicito
- Modello di politica Codice sorgente
- Modello di privacy dei dati relativi allo stato
- Modello della politica Codici SWIFT
- Modello della politica Compatibilità Symantec DLP e Prevenzione
- Modello della politica Numeri Patente di guida del Regno Unito
- Modello politica Numeri di tessera elettorale britannici
- Modello della politica Numero NHS (National Health Service) britannico
- Modello della politica Numeri di previdenza sociale britannici
- Modello della politica Numeri di passaporto britannici
- Modello di politica Codici fiscali britannici
- Marchi di controllo dei servizi di intelligence degli Stati Uniti (CAPCO) e modello della politica DCID 1/7
- Modello di politica Social Security Number statunitense

- [Modello della politica Violenza e armi](#)
- [Modello della politica di Webmail](#)
- [Modello di politica Attività della bacheca messaggi di Yahoo](#)
- [Modello di politica Yahoo e MSN Messenger sulla porta 80](#)

Modello della politica Relazione Caldicott

Il Chief Medical Officer del Regno Unito ha commissionato la Relazione Caldicott (dicembre 1997) per migliorare le modalità di trattamento e tutela dei dati dei pazienti da parte del National Health Service (sistema sanitario nazionale). Il Caldicott Committee ha monitorato il grado di riservatezza di dati all'interno dell'NHS per scopi diversi dall'assistenza diretta e dalla ricerca medica o in tutti i casi in cui la condivisione di determinate informazioni non sia obbligatoria per legge. Oggi queste raccomandazioni vengono messe in pratica dall'NHS e dall'Health Protection Agency.

Gli elenchi di parole chiave per medicinali, malattie e cure vengono aggiornati con parole chiave aggiornate basate su informazioni della FDA (Federal Drug Administration) degli Stati Uniti e di altre fonti.

Vedere ["Aggiornamento degli elenchi di parole chiave per le politiche HIPAA e Caldicott."](#) a pagina 785.

Tabella 41-1 Regole del modello della politica Relazione Caldicott

Regola	Tipo	Descrizione
Dati paziente e parole chiave medicinali	Regola composta di parola chiave ed EDM	<p>Questa regola composta cerca una corrispondenza tra i seguenti campi dati EDM insieme a una parola chiave dal dizionario "Nomi medicinale con ricetta". Entrambe le condizioni devono essere soddisfatte affinché la regola attivi un incidente.</p> <ul style="list-style-type: none"> ■ Numero di conto ■ E-mail ■ Numero di carta d'identità ■ Cognome ■ Telefono ■ Numero NHS Regno Unito (servizio nazionale sanitario) ■ NIN Regno Unito (numero di assicurazione nazionale)

Regola	Tipo	Descrizione
Dati paziente e parole chiave malattia	Regola composta di parola chiave ed EDM	<p>Questa regola composta cerca una corrispondenza tra i seguenti campi dati EDM insieme a una parola chiave dal dizionario "Nomi malattie". Entrambe le condizioni devono essere soddisfatte affinché la regola attivi un incidente.</p> <ul style="list-style-type: none"> ■ Numero di conto ■ E-mail ■ Numero di carta d'identità ■ Cognome ■ Telefono ■ Numero NHS Regno Unito (servizio nazionale sanitario) ■ NIN Regno Unito (numero di assicurazione nazionale)
Dati paziente e parole chiave trattamento	Regola composta di parola chiave ed EDM	<p>Questa regola composta cerca una corrispondenza tra i seguenti campi dati EDM insieme a una parola chiave dal dizionario "Parole chiave cura". Entrambe le condizioni devono essere soddisfatte affinché la regola attivi un incidente:</p> <ul style="list-style-type: none"> ■ Numero di conto ■ E-mail ■ Numero di carta d'identità ■ Cognome ■ Telefono ■ Numero NHS Regno Unito (servizio nazionale sanitario) ■ NIN Regno Unito (numero di assicurazione nazionale)
Numero NHS britannico e parole chiave medicinali	Regola DCM semplice	Questa regola cerca una parola chiave dal dizionario "Parole chiave NIN britannico" insieme a un formato che corrisponda all'identificatore dati del NIN britannico e a una parola chiave del dizionario "Nomi medicinali con ricetta".
Numero NHS britannico e parole chiave malattia	Regola DCM semplice	Questa regola cerca una parola chiave dal dizionario "Parole chiave NIN britannico" insieme a un formato che corrisponda all'identificatore dati del NIN britannico e a una parola chiave del dizionario "Nomi malattie".
Numero NHS britannico e parole chiave cura	Regola DCM semplice	Questa regola cerca una parola chiave dal dizionario "Parole chiave NIN britannico" insieme a un formato che corrisponda all'identificatore dati del NIN britannico e a una parola chiave del dizionario "Parole chiave cura".

Vedere ["Scelta di un profilo dati esatti"](#) a pagina 417.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Numeri di previdenza sociale (SIN) canadesi

Questa politica rileva i modelli indicanti numeri di previdenza sociale canadesi a rischio di divulgazione.

Regola DCM

Numeri di previdenza sociale (SIN) canadesi

Questa regola ricerca una corrispondenza con l'identificatore dati del numero previdenza sociale canadese e una parola chiave dal dizionario "Parole Numeri di previdenza sociale canadesi".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica CAN-SPAM Act

La politica Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM) definisce requisiti per l'invio di e-mail commerciale.

Il modello CAN-SPAM Act rileva l'attività del mailer bulk di un'organizzazione per contribuire a garantire la conformità ai requisiti CAN-SPAM Act.

L'eccezione di rilevamento **Escludi le e-mail contenenti le parole chiave obbligatorie** consente il passaggio di messaggi con una o più parole chiave incluse nel dizionario definito dall'utente "CAN-SPAM Exception Keywords".

Tabella 41-2 Eccezione di rilevamento: Escludi le e-mail contenenti le parole chiave obbligatorie

Metodo	Condizione	Configurazione
Eccezione semplice	Contenuto corrispondente a parola chiave (DCM)	<p>Escludi le e-mail contenenti le parole chiave obbligatorie (corrispondenza parole chiave):</p> <ul style="list-style-type: none"> ■ Cerca corrispondenza con parola chiave da "[indirizzo postale fisico]" o "annuncio". ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere. <p>Nota: Una volta definite le parole chiave, è possibile scegliere di contare tutte le corrispondenze e di richiedere la corrispondenza con 2 parole chiave dell'elenco.</p>

L'eccezione di rilevamento **A eccezione delle e-mail conformi a CAN-SPAM** esclude dal rilevamento il contenuto del documento presente nell'indice IDM selezionato con un grado di corrispondenza non inferiore al 90%.

Tabella 41-3 Eccezione di rilevamento: A eccezione delle e-mail conformi a CAN-SPAM

Metodo	Condizione	Configurazione
Eccezione semplice	Contenuto corrispondente a profilo documento (IDM)	<p>A eccezione delle e-mail conformi a CAN-SPAM (IDM):</p> <ul style="list-style-type: none"> ■ Corrispondenza esatta contenuto (100%) ■ Cerca nel testo del messaggio e negli allegati. ■ Verificare esistenza. <p>Vedere "Scelta di un profilo documento indicizzato" a pagina 419.</p>

Se un'eccezione non è soddisfatta, la regola di rilevamento **Monitora le e-mail inviate dal software per l'invio di e-mail di massa** cerca l'indirizzo e-mail di un mittente che corrisponde a uno di quelli presenti nell'elenco "Indirizzo e-mail del software per l'invio di e-mail di massa", definito dall'utente.

Tabella 41-4 Regola di rilevamento: Monitora le e-mail inviate dal software per l'invio di e-mail di massa

Metodo	Condizione	Configurazione
Regola semplice	Mittente/utente corrispondente a criterio (DCM)	<p>Monitora le e-mail inviate dal software per l'invio di e-mail di massa (mittente):</p> <ul style="list-style-type: none"> ■ Mittente corrispondente a criterio: [bulk-mailer@company.com] (definito dall'utente) ■ Gravità: Alta.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica della legge colombiana sulla protezione dei dati personali 1581

Il modello della politica della legge colombiana sulla protezione dei dati personali 1581 rileva i dati personali dei cittadini colombiani a rischio di divulgazione.

Tabella 41-5

Regola	Tipo	Descrizione
Numero civico colombiano (identificatori dati)	Regola DCM	Questa regola rileva gli indirizzi colombiani tramite l'identificatore dati degli indirizzi colombiani.
Numero di cellulare colombiano (identificatori dati)	Regola DCM	Questa regola rileva i numeri di cellulari colombiani tramite l'identificatore dati Numero di cellulare colombiano.
Numero di identificazione personale colombiano (identificatori dati)	Regola DCM	Questa regola rileva i numeri di identificazione personali colombiani tramite l'identificatore dati Numero di identificazione personale colombiano.
Tax Identification Number (codice fiscale) colombiano (identificatori dati)	Regola DCM	Questa regola rileva i numeri di identificazione fiscali colombiani tramite l'identificatore dati Tax Identification Number (codice fiscale) colombiano.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello politica Siti caricamento spyware comuni

La politica Siti caricamento spyware comuni rileva l'accesso ai siti Web di caricamento spyware comuni.

Regola DCM **Siti Web non consentiti 1**

Si tratta di una regola composta che cerca gli indirizzi IP o URL specificati nel dizionario "Siti Web non consentiti 1".

Regola DCM **Siti Web non consentiti 2**

Questa regola cerca una corrispondenza di un URL specificato nel dizionario "Siti Web non consentiti 2".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Comunicazioni con i concorrenti

La politica Comunicazioni con i concorrenti rileva le comunicazioni non consentite con i concorrenti.

Regola DCM

Elenco concorrenti

Questa regola cerca le parole chiave (domini) dal dizionario "Domini dei concorrenti" definito dall'utente.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Documenti riservati

Questa politica rileva i documenti aziendali riservati a rischio di divulgazione.

Tabella 41-6 Regole che comprendono il modello Documenti riservati

Regola	Tipo	Descrizione
Documenti riservati, indicizzati	Regola IDM semplice con una condizione	Questa regola cerca il contenuto in specifici documenti registrati come riservati e restituisce una corrispondenza se l'80% o più del documento di origine viene trovato. Se il profilo documento indicizzato non è configurato, questa regola viene scartata.
Documenti riservati	Regola DCM composta: tipo di allegato/file e corrispondenza con parole chiave. Entrambe le condizioni devono corrispondere affinché la regola attivi un incidente.	Questa regola cerca una combinazione di parole chiave presenti nell'elenco "Parole chiave riservate" insieme ai seguenti tipi di file: <ul style="list-style-type: none"> ■ Microsoft Excel Macro ■ Microsoft Excel ■ Microsoft Works Spreadsheet ■ SYLK Spreadsheet ■ Corel Quattro Pro ■ Multiplan Spreadsheet ■ Valori separati da virgola ■ Applix Spreadsheets ■ Lotus 1-2-3 ■ Microsoft Word ■ Adobe PDF ■ Microsoft PowerPoint
Documenti proprietari	Regola composta DCM: Tipo di allegato/file e Corrispondenza parole chiave	Questa regola cerca una combinazione di parole chiave nel dizionario "Parole chiave proprietarie" insieme ai tipi di file sopra specificati.

Regola	Tipo	Descrizione
Documenti riservati esclusivamente a uso interno	Regola composta DCM: Tipo di allegato/file e Corrispondenza parole chiave	Questa regola cerca una combinazione di parole chiave nel dizionario "Parole chiave esclusivamente a uso interno" insieme ai tipi di file sopra specificati.
Documenti non destinati alla distribuzione	Regola composta DCM: Tipo di allegato/file e Corrispondenza parole chiave	Questa regola cerca una combinazione di parole chiave nel dizionario "Parole non destinati alla distribuzione" insieme ai tipi di file sopra specificati.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Numeri di carta di credito

Questa politica rileva i modelli indicanti numeri di carta di credito a rischio di divulgazione.

Regola DCM

Numeri di carta di credito, tutti

Questa regola ricerca una corrispondenza nel modello di sistema del numero di carta di credito e una parola chiave dal dizionario "Parole chiave Numero carta di credito".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Protezione dei dati dei clienti

Questa politica rileva i dati dei clienti a rischio di divulgazione.

Tabella 41-7 Modello di politica Condizioni EDM per la protezione dei dati dei clienti

Nome regola	Tipo	Descrizione	Dettagli
Combinazioni nome utente/password	Regola EDM	<p>Questa regola cerca i nomi utenti e le password in combinazione con tre o più dei seguenti campi:</p> <ul style="list-style-type: none"> ■ Numero di previdenza sociale ■ Telefono ■ E-mail ■ Nome ■ Cognome ■ Numero di carta di credito ■ Numero di conto ■ Numero di routing ABA ■ Social Insurance Number (numero di previdenza sociale) canadese ■ Numero di previdenza sociale britannico 	<p>Tuttavia le seguenti combinazioni non rappresentano una violazione:</p> <ul style="list-style-type: none"> ■ Telefono, e-mail e cognome ■ E-mail, nome e cognome ■ Telefono, nome e cognome
Data di nascita	Regola EDM	<p>Questa regola cerca tre dei seguenti campi di dati in combinazione:</p> <ul style="list-style-type: none"> ■ Numero di previdenza sociale ■ Telefono ■ E-mail ■ Nome ■ Cognome ■ Numero di carta di credito ■ Numero di conto ■ Numero di routing ABA ■ Social Insurance Number (numero di previdenza sociale) canadese ■ Numero di previdenza sociale britannico ■ Data di nascita 	<p>Tuttavia le seguenti combinazioni non rappresentano una violazione:</p> <ul style="list-style-type: none"> ■ Telefono, e-mail e nome ■ Telefono, e-mail e cognome ■ E-mail, nome e cognome ■ Telefono, nome e cognome
SSN o CCN esatto	Regola EDM	Questa regola cerca un numero di previdenza sociale esatto o un numero di carta di credito.	
Directory clienti	Regola EDM	Questa regola cerca il telefono o l'e-mail.	

Tabella 41-8 Modello di politica Condizioni (DCM) per la protezione dei dati dei clienti

Nome regola	Tipo	Descrizione	Dettagli
Formati Social Security Number (codice fiscale) statunitense	Regola DCM composta	Questa regola ricerca una corrispondenza mediante l'identificatore dati Social Security Number statunitense randomizzato e una parola chiave dal dizionario "Parole chiave SSN statunitense".	Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218.
Numeri di carta di credito, tutti	Regola DCM composta	Questa regola ricerca una corrispondenza nel modello di sistema del numero di carta di credito e una parola chiave dal dizionario "Parole chiave Numero carta di credito".	Vedere "Numero carta di credito" a pagina 993.
Numeri di routing ABA	Regola DCM composta	Questa regola ricerca una corrispondenza mediante l'identificatore dati del numero di routing ABA e una parola chiave dal dizionario "Parole chiave numero di routing ABA".	Vedere "Numero di routing ABA" a pagina 918.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Data Protection Act 1998 (legge sulla protezione dei dati del 1998)

Il Data Protection Act del 1998 (che ha sostituito quello del 1984) fissa degli standard che devono essere soddisfatti in fase di raccolta, conservazione, utilizzo o eliminazione dei dati personali nel Regno Unito. Il Data Protection Act del 1998 riguarda tutte le banche dati contenenti informazioni di identificazione personale (ad es. dati su salute personale, impiego, salute sul lavoro, finanza, fornitori e appaltatori).

Tabella 41-9 Data Protection Act 1998, regola di rilevamento dati personali

Descrizione	
<p>Questa regola EDM cerca tre delle seguenti colonne di dati:</p> <ul style="list-style-type: none"> ■ NIN (Numero di assicurazione nazionale) ■ Numero di conto ■ Pin ■ Numero di carta di credito ■ Nome ■ Cognome ■ Patente di guida ■ Password ■ ID contribuente ■ Numero NHS Regno Unito ■ Data di nascita ■ Il cognome da nubile della madre ■ Indirizzo e-mail ■ Numero di telefono 	<p>Tuttavia, le seguenti combinazioni non generano un incidente:</p> <ul style="list-style-type: none"> ■ Nome, cognome, pin ■ Nome, cognome, password ■ Nome, cognome, e-mail ■ Nome, cognome, telefono ■ Nome, cognome, cognome da nubile della madre

Tabella 41-10 Regole di rilevamento supplementari nel modello Data Protection Act (legge sulla protezione dei dati) del 1998

Descrizione
<p>La regola Numeri di tessera elettorale britannici implementa l'identificatore di dati Numero di tessera elettorale britannico.</p> <p>Vedere "Numero di tessera elettorale britannico" a pagina 1282.</p>
<p>La regola Numeri di previdenza sociale britannici implementa l'edizione a copertura limitata dell'identificatore di dati del Numero di previdenza sociale britannico.</p> <p>Vedere "Numero di previdenza sociale britannico" a pagina 1285.</p>
<p>La regola Codici fiscali britannici implementa l'edizione a copertura limitata dell'identificatore di dati del Codice fiscale britannico.</p> <p>Vedere "Codice fiscale britannico" a pagina 1289.</p>
<p>La regola Numeri di Patente di guida del Regno Unito implementa l'edizione a copertura limitata dell'identificatore di dati del numero di Patente di guida del Regno Unito.</p> <p>Vedere "Numero di patente di guida britannica" a pagina 1279.</p>
<p>La regola Numeri di passaporto britannici implementa l'edizione a copertura limitata dell'identificatore di dati del Numero di passaporto britannico.</p> <p>Vedere "Numero di passaporto britannico" a pagina 1287.</p>

Descrizione

La regola **Numeri NHS britannici** implementa l'edizione a copertura limitata dell'identificatore di dati del Numero NHS (National Health Service) britannico.

Vedere ["Numero NHS \(National Health Service\) del Regno Unito"](#) a pagina 1282.

Vedere ["Scelta di un profilo dati esatti"](#) a pagina 417.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Direttive UE sulla protezione dei dati

Le direttive 95/46/EC del Parlamento Europeo riguardano la tutela delle persone fisiche in relazione al trattamento e alla libera circolazione dei dati personali. Questa politica rileva i dati personali a cui si fa riferimento nelle direttive UE.

Nota: Il Regolamento generale per la protezione dei dati (GDPR) sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Tabella 41-11 Regola di rilevamento delle Direttive UE sulla protezione dei dati

Metodo	Descrizione
Regola EDM	<p>Direttive UE sulla protezione dei dati</p> <p>Questa regola cerca due delle seguenti colonne di dati:</p> <ul style="list-style-type: none"> ■ Cognome ■ Numero di carta di credito ■ Numero di patente di guida ■ Numero di conto ■ PIN ■ Codice fiscale ■ Numero ID libretto sanitario ■ Nome utente ■ Password ■ Numero di routing ABA ■ E-mail ■ Telefono ■ Il cognome da nubile della madre <p>Tuttavia, le seguenti combinazioni non creano una corrispondenza:</p> <ul style="list-style-type: none"> ■ Cognome, e-mail ■ Cognome, telefono ■ Cognome, numero di conto ■ Cognome, nome utente
Regola EDM	<p>Protezione dei dati UE, informazioni di contatto</p> <p>Questa regola cerca due delle seguenti colonne di dati: cognome, telefono, numero di conto, nome utente e e-mail.</p>
Eccezione	<p>A eccezione delle e-mail interne all'UE</p> <p>Questa regola è un'eccezione se il destinatario si trova all'interno dell'UE. La regola è valida per i destinatari con codici di paese indicati nel dizionario "Codici paese UE".</p>

Vedere ["Scelta di un profilo dati esatti"](#) a pagina 417.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Classificazione GENSER Defense Message System (DMS)

La Defense Information Systems Agency ha stabilito linee guida per i marchi, le categorie e le classificazioni dei messaggi GENSER (servizi generali) di DMS (Defense Message System). Questi standard specificano come contrassegnare i documenti classificati e riservati secondo le norme degli Stati Uniti. Forniscono inoltre l'interoperabilità con i paesi NATO e gli altri alleati degli Stati Uniti.

Il modello di politica GENSER applica le linee guida di GENSER rilevando le informazioni classificate come riservate. Il modello contiene quattro semplici regole di rilevamento (DCM) di corrispondenze di parole chiave (condizione singola). Se viene trovata una corrispondenza di una condizione di regola qualsiasi, la politica segnala un incidente.

La regola di rilevamento **Informazioni top secret** (corrispondenza di parole chiave) cerca qualsiasi parola chiave nel dizionario "Informazioni top secret".

Tabella 41-12 Regola di rilevamento Informazioni top secret (corrispondenza di parole chiave)

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave (DCM)	Informazioni top secret (corrispondenza di parole chiave): <ul style="list-style-type: none"> ■ Dizionario di parole chiave: "TOP SECRET//" ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Eseguire la ricerca in busta, oggetto, corpo e allegati. ■ Distinzione maiuscole/minuscole. ■ Cercare la corrispondenza con parole intere o parziali.

La regola di rilevamento **Informazioni segrete** (corrispondenza di parole chiave) cerca una parola chiave qualsiasi nel dizionario "Informazioni segrete".

Tabella 41-13 Regola di rilevamento Informazioni segrete (corrispondenza di parole chiave)

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave (DCM)	Informazioni segrete (corrispondenza di parole chiave): <ul style="list-style-type: none"> ■ Dizionario di parole chiave: "SEGRETO//" ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Eseguire la ricerca in busta, oggetto, corpo e allegati. ■ Distinzione maiuscole/minuscole. ■ Cercare la corrispondenza con parole intere o parziali.

La regola di rilevamento **Informazioni classificate o riservate** (corrispondenza di parole chiave) cerca una parola chiave qualsiasi nel dizionario "Informazioni classificate o riservate".

Tabella 41-14 Regola di rilevamento Informazioni classificate o riservate (corrispondenza di parole chiave)

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave (DCM)	Informazioni classificate o riservate (corrispondenza di parole chiave): <ul style="list-style-type: none"> ■ Dizionario di parole chiave: "CLASSIFICATO//,//RISERVATO//" ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Eseguire la ricerca in busta, oggetto, corpo e allegati. ■ Distinzione maiuscole/minuscole. ■ Cercare la corrispondenza con parole intere o parziali.

La regola di rilevamento **Altre informazioni sensibili** cerca una parola chiave qualsiasi nel dizionario "Altre informazioni sensibili".

Tabella 41-15 Regola di rilevamento Altre informazioni sensibili

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave (DCM)	Altre informazioni sensibili (corrispondenza di parole chiave): <ul style="list-style-type: none"> ■ Dizionario di parole chiave: SOLO PER USO UFFICIALE, RISERVATO MA NON CLASSIFICATO, INFORMAZIONI NUCLEARI CONTROLLATE NON CLASSIFICATE DOD ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Eseguire la ricerca in busta, oggetto, corpo e allegati. ■ Distinzione maiuscole/minuscole. ■ Cercare la corrispondenza solo con parole intere.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Documenti di progettazione

Questa politica rileva diversi tipi di documenti di progettazione, quali CAD/CAM, a rischio di divulgazione.

Regola IDM	<p>Documenti di progettazione, indicizzati</p> <p>Questa regola cerca il contenuto in documenti di progettazione specifici registrati come proprietari. Restituisce una corrispondenza se il motore individua l'80% o più del documento originale.</p>
Regola DCM	<p>Estensioni documenti di progettazione</p> <p>Questa regola cerca specifiche estensioni di file trovate nel dizionario "Estensioni documento di progettazione".</p>
Regola DCM	<p>Documenti di progettazione</p> <p>Questa regola cerca i seguenti tipi di file specificati:</p> <ul style="list-style-type: none"> ■ cad_draw ■ dwg

Nota: Per questa politica è necessario specificare il tipo e l'estensione del file poiché essa non individua il tipo di file effettivo per tutti i documenti richiesti.

Vedere ["Scelta di un profilo documento indicizzato"](#) a pagina 419.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Protezione dei dati dei dipendenti

Questa politica rileva i dati dei dipendenti a rischio di divulgazione.

Tabella 41-16 Regole EDM per protezione dei dati dei dipendenti

Nome	Tipo	Descrizione
Combinazioni nome utente/password	Regola EDM	<p>Questa regola cerca i nomi utenti e le password in combinazione a uno dei tre seguenti campi di informazione.</p> <ul style="list-style-type: none"> ■ Numero di previdenza sociale ■ Telefono ■ E-mail ■ Nome ■ Cognome ■ Numero di carta di credito ■ Numero di conto ■ Numero di routing ABA ■ Social Insurance Number (numero di previdenza sociale) canadese ■ Numero di previdenza sociale britannico ■ Data di nascita
Directory dipendenti	Regola EDM	Questa regola cerca il telefono o l'e-mail.

Tabella 41-17 Regole DCM per protezione dei dati dei dipendenti

Nome	Tipo	Descrizione
Formati Social Security Number (codice fiscale) statunitense	Regola DCM	<p>Questa regola ricerca una corrispondenza mediante l'identificatore dati Social Security Number (SSN) statunitense randomizzato e una parola chiave dal dizionario "Parole chiave SSN statunitense".</p> <p>Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218.</p>
Numeri di carta di credito, tutti	Regola DCM	<p>Questa regola ricerca una corrispondenza dal modello di sistema del numero di carta di credito e una parola chiave dal dizionario "Parole chiave Numero carta di credito".</p> <p>Vedere "Numero carta di credito" a pagina 993.</p>
Numeri di routing ABA	Regola DCM	<p>Questa regola ricerca una corrispondenza mediante l'identificatore dati del numero di routing ABA e una parola chiave dal dizionario "Parole chiave numero di routing ABA".</p> <p>Vedere "Numero di routing ABA" a pagina 918.</p>

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Dati crittografati

Questa politica rileva l'uso della crittografia mediante una serie di metodi, tra cui S/MIME, PGP, GPG e protezione con password.

Regola DCM	File protetti da password Questa regola cerca i seguenti tipi di file specificati: encrypted_zip, encrypted_doc, encrypted_xls, or encrypted_ppt.
Regola DCM	File PGP Questa regola cerca il seguente tipo di file: pgp.
Regola DCM	File GPG Questa regola cerca una parola chiave dal dizionario "Parole chiave Crittografia GPG".
Regola DCM	S/MIME Questa regola cerca una parola chiave dal dizionario "Parole chiave Crittografia S/MIME".
Regola DCM	Trasmissioni HushMail Questa regola cerca una corrispondenza in un elenco di URL di destinatari.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Export Administration Regulations (EAR)

La normativa Export Administration Regulations (EAR, normativa sulla gestione delle esportazioni) viene applicata dal Dipartimento del Commercio degli Stati Uniti. Questa normativa fa riferimento principalmente alle tecnologie e alle informazioni di natura tecnica che trovano applicazione in ambito commerciale e militare. Queste tecnologie sono note anche come tecnologie dual-use (ad esempio, sostanze chimiche, satelliti, software, computer e così via).

Questo modello di politica Export Administration Regulations (EAR) rileva le violazioni dei paesi regolamentati e delle tecnologie controllate.

La regola di rilevamento **Elementi della lista CCL dell'EAR indicizzati e destinatari** cerca un codice di paese per il destinatario nel dizionario "Codici di paese EAR" e uno "SKU" specifico

in un indice di un profilo di dati esatti (EDM). Entrambe le circostanze devono corrispondere per attivare un incidente.

Tabella 41-18 Regola di rilevamento Elementi della lista CCL dell'EAR indicizzati e destinatari

Metodo	Condizione	Configurazione
Regola composta	Contenuto corrispondente a dati esatti (EDM)	Vedere "Scelta di un profilo dati esatti" a pagina 417.
	Contenuto corrispondente a parola chiave (DCM)	Vedere "Configurazione della condizione Contenuto corrispondente a parola chiave" a pagina 779.

La regola di rilevamento **Lista CCL (Commerce Control List, lista di controllo del commercio) dell'EAR e destinatari** cerca un codice di paese per il destinatario nell'elenco "Codici di paese EAR" e una parola chiave nel dizionario "Parole chiave CCL EAR". Entrambe le circostanze devono corrispondere per attivare un incidente.

Tabella 41-19 Regola di rilevamento Lista CCL (Commerce Control List, lista di controllo del commercio) dell'EAR e destinatari

Metodo	Condizione	Configurazione
Regola composta	Destinatario corrispondente a criterio (DCM)	Lista CCL (Commerce Control List, lista di controllo del commercio) dell'EAR e destinatari (destinatario): <ul style="list-style-type: none"> ■ Cercare la corrispondenza con indirizzo e-mail O suffissi di dominio URL. ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Almeno 1 destinatario deve corrispondere. ■ Cercare la corrispondenza con l'intero messaggio.
	Contenuto corrispondente a parola chiave (DCM)	Lista CCL (Commerce Control List, lista di controllo del commercio) dell'EAR e destinatari (corrispondenza di parole chiave): <ul style="list-style-type: none"> ■ Cercare la corrispondenza con le parole chiave della lista CCL dell'EAR. ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica FACTA 2003 (regole Red Flag)

Questa politica contribuisce alla gestione delle sezioni 114 e 315 (o regole Red Flag) della normativa Fair and Accurate Credit Transactions Act (FACTA) of 2003. Nelle suddette regole viene specificato che un'istituzione finanziaria o un creditore che offrono o mantengono conti segreti devono sviluppare e implementare un programma di prevenzione dei furti di identità. Il programma FACTA ha il fine di rilevare, prevenire e limitare i furti di identità in relazione all'apertura di un conto segreto o a eventuali conti segreti esistenti.

La regola di rilevamento **Combinazioni nome utente/password** rileva la presenza sia di un nome utente che di una password in un indice di database con profilo.

Tabella 41-20 Regola di rilevamento Combinazioni nome utente/password

Metodo	Condizione	Configurazione
Regola semplice	Il contenuto corrisponde ai dati esatti (EDM)	Questa condizione rileva i dati esatti che contengono entrambi i seguenti elementi di dati: <ul style="list-style-type: none"> ■ Nome utente ■ Password Vedere "Scelta di un profilo dati esatti" a pagina 417.

La regola di rilevamento **SSN o CCN esatto** rileva la presenza di un codice fiscale o un numero di carta di credito in un database con profilo.

Tabella 41-21 Regola di rilevamento SSN o CCN esatto

Metodo	Condizione	Configurazione
Regola semplice	Il contenuto corrisponde ai dati esatti (EDM)	Questa condizione rileva i dati esatti che contengono una delle due colonne di dati che seguono: <ul style="list-style-type: none"> ■ Numero di codice fiscale (ID contribuente) ■ Numero di carta di credito Vedere "Scelta di un profilo dati esatti" a pagina 417.

La regola di rilevamento **Directory clienti** rileva la presenza di un indirizzo e-mail o di un numero di telefono in un database con profilo.

Tabella 41-22 Regola di rilevamento Directory clienti

Metodo	Condizione	Configurazione
Regola semplice	Il contenuto corrisponde ai dati esatti (EDM)	<p>Questa condizione rileva i dati esatti che contengono una delle due colonne di dati che seguono:</p> <ul style="list-style-type: none"> ■ Indirizzo e-mail ■ Numero di telefono <p>Vedere "Scelta di un profilo dati esatti" a pagina 417.</p>

La regola di rilevamento **Tre o più colonne di dati** rileva i dati esatti contenenti tre o più elementi di dati in un indice di database con profilo.

Tabella 41-23 Regola di rilevamento Tre o più colonne di dati

Metodo	Condizione	Configurazione
Regola semplice	Il contenuto corrisponde ai dati esatti (EDM)	<p>Rileva i dati esatti che contengono tre o più dei seguenti elementi di dati:</p> <ul style="list-style-type: none"> ■ Numero di routing ABA ■ Numero di conto ■ Numero di carta di credito ■ Data di nascita ■ Indirizzo e-mail ■ Nome ■ Cognome ■ Numero di assicurazione nazionale ■ Password ■ Numero di telefono ■ Numero di previdenza sociale ■ Numero di codice fiscale (ID contribuente) ■ Nome utente <hr/> <p>Tuttavia le seguenti combinazioni non rappresentano una corrispondenza:</p> <ul style="list-style-type: none"> ■ Numero di telefono, E-mail, Nome ■ Numero di telefono, Nome, Cognome <p>Vedere "Scelta di un profilo dati esatti" a pagina 417.</p>

La regola di rilevamento **Formati Social Security Number (codice fiscale) statunitense** implementa la versione a copertura limitata dell'identificatore dati di sistema Social Security Number (SSN) statunitense randomizzato.

Vedere ["Social Security Number \(SSN\) statunitense randomizzato"](#) a pagina 1218.

Questo identificatore dati rileva numeri a nove cifre con il criterio DDD-DD-DDDD separati da trattini o spazi o senza separatori. Il numero deve essere compreso negli intervalli numerici assegnati validi. Questa condizione elimina i numeri di prova comuni, quali 123456789 o quelli con tutte le cifre uguali. Richiede inoltre la presenza di una parola chiave associata all'SSN.

Tabella 41-24 Regola di rilevamento Formati Social Security Number (codice fiscale) statunitense

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a identificatore dati (DCM)	<ul style="list-style-type: none"> ■ Identificatore di dati: Social Security Number (SSN) statunitense randomizzato (copertura limitata) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo, allegati.

La regola di rilevamento **Numeri di carta di credito, tutti** implementa la versione a copertura limitata dell'identificatore dati di sistema Numero carta di credito.

Vedere ["Numero carta di credito"](#) a pagina 993.

Questo identificatore dati rileva i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori. Questa condizione esegue il controllo di convalida Luhn e include i formati per American Express, Diners Club, Discover, Japan Credit Bureau (JCB), MasterCard e Visa. Rimuove i numeri di prova comuni, compresi quelli riservati ai test eseguiti dagli emittenti di carte di credito. Richiede inoltre la presenza di una parola chiave associata alla carta di credito.

Tabella 41-25 Regola di rilevamento Numeri di carta di credito, tutti

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a identificatore dati (DCM)	<ul style="list-style-type: none"> ■ Identificatore dati: Numero di carta di credito, copertura limitata Vedere "Copertura limitata numero carta di credito" a pagina 997. ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo, allegati.

La regola di rilevamento **Numero di routing ABA** implementa la versione a copertura limitata dell'identificatore dati di sistema Numero di routing ABA.

Vedere ["Numero di routing ABA"](#) a pagina 918.

Questo identificatore dati rileva numeri a nove cifre. Convalida il numero utilizzando la cifra di controllo finale. Questa condizione elimina i numeri di prova più comuni, quali 123456789, gli intervalli numerici riservati per usi futuri e i numeri con tutte le cifre uguali. Richiede inoltre la presenza di una parola chiave ABA.

Tabella 41-26 Regola di rilevamento Numeri di routing ABA

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a identificatore dati (DCM)	<ul style="list-style-type: none"> ■ Identificatore dati: Numero di routing ABA, copertura limitata Vedere "Numero di routing ABA" a pagina 918. ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo, allegati.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Informazioni finanziarie

La politica di informazione finanziaria rileva informazioni e dati finanziari.

Regola IDM **Informazioni finanziarie, indicizzate**

Questa regola cerca il contenuto in un file di informazioni finanziarie specificato registrato come riservato e restituisce una corrispondenza se viene trovato almeno l'80% più del documento di origine.

Regola DCM **Informazioni finanziarie**

Questa regola cerca la combinazione di tipi di file specificati, parole chiave dal dizionario "Parole chiave finanziarie" e parole chiave dal dizionario "Parole confidenziali/private".

I tipi di file specificati sono i seguenti:

- excel_macro
- xls
- works_spread
- sylk
- quattro_pro
- mod
- csv
- applix_spread
- 123

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Siti Web non consentiti

Il modello della politica Siti Web non consentiti è stato realizzato per individuare l'accesso ai siti Web specificati.

Nota: Per elaborare correttamente le richieste GET HTTP, potrebbe essere necessario configurare il server Network Prevent for Web. Vedere ["Per consentire alla politica "Siti Web non consentiti" di elaborare correttamente le richieste"](#) a pagina 1341.

Tabella 41-27 Modello della politica Siti Web non consentiti

Regola parola chiave DCM	Descrizione
Siti Web non consentiti	Questa regola cerca tutte le parole chiave nel dizionario "Siti Web non consentiti" definite dall'utente.

Per consentire alla politica "Siti Web non consentiti" di elaborare correttamente le richieste

- 1 Configurare il server proxy Web in modo che inoltri le richieste GET al server Network Prevent for Web.
- 2 Impostare le impostazioni Advanced Server `L7.processGets` sul server Network Prevent for Web su "TRUE" (impostazione predefinita).
- 3 Ridurre l'impostazione Advanced Server `L7.minSizeofGetURL` nel server Network Prevent for Web a un valore inferiore a quello predefinito (100) fino a un numero di byte (caratteri) inferiore a quello della lunghezza del sito Web più corto specificato dalla politica.

Nota: La riduzione della dimensione minima dei comandi GET aumenta il numero di URL da elaborare e quindi il carico del traffico del server. Un'opzione è quella di calcolare il numero di caratteri dell'URL più breve specificato nell'elenco degli URL non consentiti e di impostare la lunghezza minima su quel numero. Un'altra opzione consiste nell'impostare la lunghezza minima dell'URL su 10 in modo che sia valido per tutti i casi.

- 4 Potrebbe essere necessario regolare l'impostazione "Ignora richieste inferiori a" nella configurazione ICAP del server Network Prevent (valore predefinito: 4096 byte). Questo valore interrompe l'elaborazione delle pagine Web in entrata che contengono un numero di byte inferiore a quello specificato. Se il numero di byte di una pagina di un URL di un sito Web non consentito fosse inferiore a quel numero, l'impostazione dovrà essere regolata di conseguenza.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello politica Gioco d'azzardo

Questa politica individua qualsiasi riferimento al gioco d'azzardo.

Tabella 41-28 Modello politica Gioco d'azzardo

Regola parola chiave DCM	Regola DCM
Parole chiave gioco d'azzardo sospetto	Questa regola cerca cinque istanze delle parole chiave dal dizionario "Parole chiave gioco d'azzardo, confermato".
Parole chiave gioco d'azzardo meno sospetto	Questa regola cerca dieci istanze delle parole chiave dal dizionario "Parole chiave gioco d'azzardo, sospetto".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Regolamento generale per la protezione dei dati (attività bancarie e finanza)

Questo modello è dedicato alle parole chiave del Regolamento generale per la protezione dei dati (GDPR) relative alle attività bancarie e finanziarie, oltre agli identificatori di dati e al profilo EDM con colonne connesse.

Il GDPR è un regolamento con cui la Commissione Europea vuole rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. Tratta inoltre dell'esportazione dei dati personali all'esterno dell'UE. Gli obiettivi principali del GDPR sono di restituire ai cittadini il controllo sui propri dati personali e di semplificare le norme per le aziende internazionali unificando i regolamenti all'interno dell'UE. Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Tabella 41-29 Regole di rilevamento regolamenti generali per la protezione dei dati (attività bancarie e finanza)

Nome	Tipo	Descrizione
Parole chiave relative ad attività bancarie e finanza nel GDPR	Corrispondenza parole chiave	<p>Definisce la corrispondenza di un elenco di parole chiave relative:</p> <p>account number, bank card number, driver license number, ID card number, Kontonummer, Bankkartennummer, Führerscheinnummer, Ausweisnummer, Numéro de compte, numéro carte bancaire, numéro de permis de conduire, numéro de carte d'identité, numero di conto, banca carta numero, carta d'identità numero, patente guida numero, Número cuenta, número tarjeta bancaria, número licencia conducir, número tarjeta de identificación, rekeningnummer, bank kaart aantal, rijbewijs nummer, ID-kaartnummer, bankkortnummer, körkort nummer, identitetskortnummer, førerkortnummer, ID-kortnummer, tilinúmero, pankkikortin numero, ajokortin numero, Henkilökortin numero, uimhir chuntais, uimhir chárta bainc, uimhir ceadúnas tiomána, Uimhir chárta aitheantais, Kontosnummer, Identifikatiounskaart, número de conta, número cartão bancário, número licença motorista, Número do cartão de identificação</p>
Numero carta di credito	Identificatori di dati	<p>Numero di conto necessario per l'elaborazione delle transazioni della carta di credito. Generalmente abbreviato con CCN. Noto anche come numero di conto principale (PAN).</p> <p>Vedere "Numero carta di credito" a pagina 993.</p>

Nome	Tipo	Descrizione
Numero di patente di guida britannica	Identificatori di dati	<p>Il numero di patente di guida britannica è il numero di identificazione della patente di guida individuale rilasciata dalla Driver and Vehicle Licensing Agency del Regno Unito.</p> <p>Vedere "Numero di patente di guida britannica" a pagina 1279.</p>
Numero di passaporto britannico	Identificatori di dati	<p>Il numero di passaporto britannico identifica un passaporto britannico utilizzando la specifica ufficiale corrente degli standard governativi dell'Ufficio del Gabinetto del Regno Unito.</p> <p>Vedere "Numero di passaporto britannico" a pagina 1287.</p>
Codice fiscale britannico	Identificatori di dati	<p>Il codice fiscale britannico è un numero di identificazione personale fornito dagli standard governativi dell'Ufficio del Gabinetto del Regno Unito.</p> <p>Vedere "Codice fiscale britannico" a pagina 1289.</p>
Dati banda magnetica per carte di credito	Identificatori di dati	<p>La banda magnetica di una carta di credito contiene informazioni sulla carta. L'archiviazione della versione completa di questi dati rappresenta una violazione dello standard Payment Card Industry (PCI) Data Security Standard (DSS).</p> <p>Vedere "Dati banda magnetica per carte di credito" a pagina 990.</p>

Nome	Tipo	Descrizione
Numero di passaporto francese	Identificatori di dati	<p>Il passaporto francese è un documento di identità rilasciato ai cittadini francesi. Oltre a consentire al portatore di viaggiare all'estero e servire come indicazione della cittadinanza francese, il passaporto assicura l'assistenza del consolato francese all'estero o, se necessario, di altri stati membri dell'Unione Europea, nel caso in cui il console francese non sia presente.</p> <p>Vedere "Numero di passaporto francese" a pagina 1051.</p>
Numero di identificazione nazionale belga	Identificatori di dati	<p>Tutti i cittadini del Belgio hanno un numero di identificazione nazionale. I belgi di età superiore ai 12 anni possiedono una carta d'identità belga.</p> <p>Vedere "Numero di identificazione nazionale belga" a pagina 942.</p>
Numero di identificazione personale ceco	Identificatori di dati	<p>A tutti i cittadini della repubblica Ceca viene assegnato un numero di identificazione personale univoco rilasciato dal Ministero dell'Interno.</p> <p>Vedere "Numero di identificazione personale ceco" a pagina 1004.</p>
Codice INSEE francese	Identificatori di dati	<p>In Francia il codice INSEE viene utilizzato come numero di previdenza sociale, un numero di identificazione nazionale, e a scopi fiscali e lavorativi.</p> <p>Vedere "Codice INSEE francese" a pagina 1049.</p>
Numero di previdenza sociale francese	Identificatori di dati	<p>Il numero di previdenza sociale francese (FSSN) è un numero univoco assegnato ai cittadini francesi o agli stranieri residenti nel paese. Funge da numero di identificazione nazionale.</p> <p>Vedere "Numero di previdenza sociale francese" a pagina 1052.</p>

Nome	Tipo	Descrizione
Codice fiscale greco (AFM)	Identificatori di dati	<p>L'Arithmo Forologiko Mitro (AFM) è un codice fiscale personale univoco assegnato a ogni persona residente o proprietaria di beni in Grecia.</p> <p>Vedere "Codice fiscale greco (AFM)" a pagina 1067.</p>
Numero di previdenza sociale ungherese	Identificatori di dati	<p>Il numero di previdenza sociale ungherese (TAJ) è un identificatore univoco rilasciato dal governo ungherese.</p> <p>Vedere "Numero di previdenza sociale ungherese" a pagina 1078.</p>
Numero di identificazione fiscale (TIN) ungherese	Identificatori di dati	<p>Il numero di identificazione fiscale ungherese è un numero di 10 cifre che comincia sempre con la cifra "8".</p> <p>Vedere "Numero di identificazione fiscale ungherese" a pagina 1080.</p>
Numero di partita IVA ungherese	Identificatori di dati	<p>Tutte le imprese ungheresi (incluse le organizzazioni non profit) registrate presso l'agenzia delle entrate nazionale hanno un numero di partita IVA.</p> <p>Vedere "Numero di partita IVA ungherese" a pagina 1082.</p>
Numero personale di servizio pubblico irlandese (PPS)	Identificatori di dati	<p>Il formato del numero è una stringa alfanumerica univoca di 8 caratteri che termina con una lettera, ad esempio 8765432A. Viene assegnato alla registrazione del neonato, è indicato sulla carta dei servizi sociali ed è univoco.</p> <p>Vedere "Numero personale di servizio pubblico irlandese" a pagina 1121.</p>

Nome	Tipo	Descrizione
Numero di identificazione lussemburghese (RNPP)	Identificatori di dati	<p>Il numero di identificazione lussemburghese è un numero di identificazione di 11 cifre rilasciato a tutti i cittadini del Lussemburgo all'età di 15 anni.</p> <p>Vedere "Numero di identificazione lussemburghese (RNPP)" a pagina 1153.</p>
Numero di carta di identità polacca	Identificatori di dati	<p>Ogni cittadino polacco che ha compiuto i 18 anni di età e che risiede in modo permanente in Polonia deve avere una carta di identità con un numero personale univoco. Tale numero viene utilizzato come strumento di identificazione in parecchi ambiti.</p> <p>Vedere "Numero di carta di identità polacca" a pagina 1197.</p>
Codice statistico polacco (REGON)	Identificatori di dati	<p>In Polonia ogni entità economica deve essere registrata nel Registro delle attività nazionali denominato REGON. È l'unico registro integrato del paese in cui sono elencate tutte le imprese nazionali. Ogni società ha un numero REGON univoco.</p> <p>Vedere "Codice statistico polacco (REGON)" a pagina 1199.</p>
Codice fiscale polacco (PESEL)	Identificatori di dati	<p>Il codice fiscale polacco (PESEL) è il numero di identificazione nazionale utilizzato in Polonia. Il numero PESEL è obbligatorio per tutte le persone residenti in modo permanente o temporaneo in Polonia. Esso identifica unicamente una persona e non può essere trasferito a un altro individuo.</p> <p>Vedere "Codice fiscale polacco (PESEL)" a pagina 1201.</p>

Nome	Tipo	Descrizione
Numero di identificazione fiscale polacco (NIP)	Identificatori di dati	<p>Il numero di identificazione fiscale polacco (NIP) è un numero che il governo assegna a ogni cittadino polacco che lavora o svolge un'attività commerciale in Polonia. Questo codice è denominato NIP.</p> <p>Vedere "Numero di identificazione fiscale polacco (NIP)" a pagina 1203.</p>
Numero di identificazione personale rumeno (CNP)	Identificatori di dati	<p>A ogni cittadino rumeno viene assegnato un numero di identificazione personale. Tale numero è utilizzato come strumento di riconoscimento da autorità, assistenza sanitaria, scuole, università, banche e compagnie di assicurazione.</p> <p>Vedere "Numero di identificazione personale rumeno (CNP)" a pagina 1223.</p>
Numero di DNI spagnolo	Identificatori di dati	<p>Il numero di DNI spagnolo è riportato sul Documento nacional de identidad (DNI) ed è rilasciato dall'Hacienda Publica spagnola a tutti i cittadini spagnoli. È il più importante identificatore univoco utilizzato in Spagna per l'apertura di conti, la firma di contratti, le tasse e le elezioni.</p> <p>Vedere "Numero di DNI spagnolo" a pagina 1245.</p>
Numero di previdenza sociale spagnolo	Identificatori di dati	<p>Il numero di previdenza sociale spagnolo è un numero a 12 cifre assegnato ai lavoratori spagnoli per consentire l'accesso al sistema sanitario spagnolo.</p> <p>Vedere "Numero di previdenza sociale spagnolo" a pagina 1249.</p>

Nome	Tipo	Descrizione
Numero di conto cliente spagnolo	Identificatori di dati	<p>Il numero di conto cliente spagnolo è il numero di conto bancario standard utilizzato in Spagna.</p> <p>Vedere "Numero di conto cliente spagnolo" a pagina 1243.</p>
Codice di identificazione fiscale spagnolo (CIF)	Identificatori di dati	<p>Il codice fiscale spagnolo (CIF) è equivalente alla partita IVA ed è necessario per svolgere un'attività lavorativa in Spagna. Esso è il numero identificativo di un'azienda per scopi fiscali ed è obbligatorio per qualsiasi transazione giuridica.</p> <p>Vedere "Codice fiscale spagnolo (CIF)" a pagina 1251.</p>
Numero di passaporto tedesco	Identificatori di dati	<p>Il numero di passaporto tedesco viene rilasciato alle persone di nazionalità tedesca, in genere per viaggiare all'estero. Un passaporto tedesco è un documento ufficialmente riconosciuto che le autorità tedesche accettano come prova dell'identità dai cittadini tedeschi.</p> <p>Vedere "Numero di passaporto tedesco" a pagina 1054.</p>
Numero di cittadinanza univoco bulgaro (EGN)	Identificatori di dati	<p>Il numero di cittadinanza univoco (EGN) è un numero univoco assegnato ai cittadini bulgari o agli stranieri residenti nel paese. Funge da numero di identificazione nazionale. L'EGN viene assegnato ai cittadini bulgari alla nascita o al momento del rilascio del certificato di nascita.</p> <p>Vedere "Numero di cittadinanza univoco bulgaro (EGN)" a pagina 967.</p>

Nome	Tipo	Descrizione
Numero di previdenza sociale austriaco	Identificatori di dati	<p>Il numero di previdenza sociale austriaco è assegnato ai cittadini austriaci che usufruiscono di prestazioni di assistenza sociale. È rilasciato da un'associazione ombrello dell'ente di previdenza sociale austriaco.</p> <p>Vedere "Numero di previdenza sociale austriaco" a pagina 939.</p>
Numero di passaporto spagnolo	Identificatori di dati	<p>I passaporti spagnoli sono rilasciati ai cittadini spagnoli per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto spagnolo" a pagina 1247.</p>
Numero di passaporto svedese	Identificatori di dati	<p>Il passaporto svedese viene rilasciato alle persone di nazionalità svedese per viaggiare all'estero. Oltre a servire quale prova della cittadinanza svedese, assicura l'assistenza del consolato svedese all'estero o, se necessario, di altri stati membri dell'Unione Europea, nel caso in cui sia il console svedese non sia presente.</p> <p>Vedere "Numero di passaporto svedese" a pagina 1260.</p>
Numero di identificazione personale tedesco	Identificatori di dati	<p>Il numero di identificazione personale tedesco è rilasciato a tutti i cittadini tedeschi.</p> <p>Vedere "Numero di identificazione personale tedesco" a pagina 1056.</p>

Nome	Tipo	Descrizione
IBAN paesi centrali	Identificatori di dati	<p>Il numero International Bank Account Number (IBAN) è uno standard internazionale per l'identificazione di conti bancari internazionali.</p> <p>L'IBAN paesi centrali rileva i numeri IBAN per Andorra, Austria, Belgio, Germania, Italia, Liechtenstein, Lussemburgo, Malta, Monaco, San Marino e Svizzera.</p> <p>Vedere "IBAN paesi centrali" a pagina 1084.</p>
IBAN paesi orientali	Identificatori di dati	<p>Il numero International Bank Account Number (IBAN) è uno standard internazionale per l'identificazione di conti bancari internazionali.</p> <p>L'identificatore di dati IBAN paesi orientali rileva numeri IBAN per Bosnia, Bulgaria, Croazia, Cipro, Estonia, Grecia, Israele, Lettonia, Lituania, Macedonia, Montenegro, Polonia, Repubblica Ceca, Romania, Serbia, Slovacchia, Slovenia, Turchia, Tunisia e Ungheria.</p> <p>Vedere "IBAN paesi orientali" a pagina 1088.</p>
IBAN paesi occidentali	Identificatori di dati	<p>Il numero International Bank Account Number (IBAN) è uno standard internazionale per l'identificazione di conti bancari internazionali.</p> <p>L'identificatore di dati IBAN paesi occidentali rileva i numeri IBAN per Danimarca, Fær Øer, Finlandia, Francia, Gibilterra, Groenlandia, Irlanda, Islanda, Norvegia, Paesi Bassi, Portogallo, Regno Unito, Spagna e Svezia.</p> <p>Vedere "IBAN paesi occidentali" a pagina 1094.</p>

Nome	Tipo	Descrizione
Burgerservicenummer	Identificatori di dati	<p>Nei Paesi Bassi, il Burgerservicenummer è utilizzato per identificare in modo univoco i cittadini ed è stampato su patenti di guida, passaporti e documenti d'identità internazionali sotto l'intestazione Numero personale.</p> <p>Vedere "Burgerservicenummer" a pagina 970.</p>
Codice Fiscale	Identificatori di dati	<p>Il codice fiscale identifica in modo univoco i cittadini italiani o gli stranieri con residenza permanente in Italia e viene rilasciato a livello centralizzato dal Ministero del Tesoro. In Italia il codice fiscale viene rilasciato a tutti i cittadini alla nascita.</p> <p>Vedere "Codice Fiscale" a pagina 979.</p>
Codice identificativo personale finlandese	Identificatori di dati	<p>Il numero di identificazione personale finlandese o il codice identificativo personale è un identificatore personale univoco utilizzato per l'identificazione dei cittadini all'interno del governo e di molte altre transazioni.</p> <p>Vedere "Codice identificativo personale finlandese" a pagina 1040.</p>
Numero di identificazione personale svedese	Identificatori di dati	<p>Il numero di identificazione personale svedese è l'identificazione nazionale univoca per ogni cittadino svedese. Tale numero è utilizzato come strumento di riconoscimento da autorità, assistenza sanitaria, scuole, università, banche e compagnie di assicurazione.</p> <p>Vedere "Numero di identificazione personale svedese" a pagina 1262.</p>

Nome	Tipo	Descrizione
Numero di passaporto austriaco	Identificatori di dati	<p>I passaporti austriaci sono documenti di viaggio rilasciati ai cittadini austriaci dalle autorità preposte in Austria e all'estero e consentono di effettuare viaggi internazionali.</p> <p>Vedere "Numero di passaporto austriaco" a pagina 933.</p>
Numero di identificazione fiscale austriaco	Identificatori di dati	<p>L'Austria rilascia numeri di identificazione fiscale agli individui in base alla loro area di residenza per identificare i contribuenti e agevolare le imposte nazionali.</p> <p>Vedere "Numero di identificazione fiscale austriaco" a pagina 935.</p>
Numero di passaporto belga	Identificatori di dati	<p>Il passaporto belga è rilasciato dallo stato belga ai suoi cittadini per consentire loro di viaggiare all'estero. Il Servizio pubblico federale degli Affari Esteri, in precedenza noto come Ministero degli Affari Esteri, è responsabile del rilascio e del rinnovo dei passaporti belgi.</p> <p>Vedere "Numero di passaporto belga" a pagina 947.</p>
Numero di identificazione fiscale belga	Identificatori di dati	<p>Il Belgio rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Belgio.</p> <p>Vedere "Numero di identificazione fiscale belga" a pagina 948.</p>
Numero di partita IVA belga	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Belgio, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA belga" a pagina 951.</p>

Nome	Tipo	Descrizione
Numero di patente di guida belga	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Belgio.</p> <p>Vedere "Numero di patente di guida belga" a pagina 945.</p>
Numero di identificazione personale danese	Identificatori di dati	<p>Ogni cittadino danese ha un numero di identificazione nazionale. Tale numero viene utilizzato come prova dell'identità di una persona in molti ambiti.</p> <p>Vedere "Numero di identificazione personale danese" a pagina 1007.</p>
Numero di patente di guida dei Paesi Bassi	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'ente governativo RDW nei Paesi Bassi.</p> <p>Vedere "Numero di patente di guida dei Paesi Bassi" a pagina 1183.</p>
Numero di passaporto dei Paesi Bassi	Identificatori di dati	<p>Il passaporto dei Paesi Bassi viene rilasciato ai cittadini dei Paesi Bassi per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto dei Paesi Bassi" a pagina 1184.</p>
Numero di partita IVA dei Paesi Bassi	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Nei Paesi Bassi, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA dei Paesi Bassi" a pagina 1189.</p>
Numero di patente di guida francese	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Francia.</p> <p>Vedere "Numero di patente di guida francese" a pagina 1042.</p>

Nome	Tipo	Descrizione
Numero di identificazione fiscale francese	Identificatori di dati	<p>La Francia rilascia un numero di identificazione fiscale a chiunque abbia l'obbligo di dichiarazione fiscale in Francia.</p> <p>Vedere "Numero di identificazione fiscale francese" a pagina 1045.</p>
Numero di patente di guida tedesca	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Germania.</p> <p>Vedere "Numero di patente di guida tedesca" a pagina 1059.</p>
Numero di passaporto italiano	Identificatori di dati	<p>Il passaporto italiano viene rilasciato ai cittadini italiani per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto italiano" a pagina 1129.</p>
Numero di partita IVA italiano	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Italia, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA italiano" a pagina 1131.</p>
Numero di patente di guida italiana	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Italia.</p> <p>Vedere "Numero di patente di guida italiana" a pagina 1126.</p>
Numero di identificazione fiscale dei Paesi Bassi	Identificatori di dati	<p>I Paesi Bassi emettono un numero di identificazione fiscale al momento della nascita o della registrazione presso l'anagrafe.</p> <p>Vedere "Numero di identificazione fiscale dei Paesi Bassi" a pagina 1185.</p>

Nome	Tipo	Descrizione
Numero di patente di guida spagnola	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Spagna.</p> <p>Vedere "Numero di patente di guida spagnola" a pagina 1238.</p>
Carta di identità ucraina	Identificatori di dati	<p>La carta di identità ucraina presenta un numero di 15 cifre rilasciato ai cittadini ucraini. È utilizzata come documento identificativo al posto del passaporto interno ucraino a partire dal 2016.</p> <p>Vedere "Carta di identità ucraina" a pagina 1296.</p>
Numero di passaporto interno ucraino	Identificatori di dati	<p>Un documento di identità rilasciato ai cittadini ucraini per l'uso nazionale. È stato sostituito dalla carta di identità ucraina a partire dal 2016, ma i passaporti esistenti sono ancora validi.</p> <p>Vedere "Passaporto ucraino (interno)" a pagina 1294.</p>
Numero di passaporto internazionale ucraino	Identificatori di dati	<p>Un documento utilizzato dai cittadini ucraini per viaggiare all'estero.</p> <p>Vedere "Passaporto ucraino (internazionale)" a pagina 1298.</p>
Numero di partita IVA della Germania	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Germania, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di patente di guida tedesca" a pagina 1059.</p>

Nome	Tipo	Descrizione
Numero di partita IVA della Francia	Identificatori di dati	<p>L'imposta sul valore aggiunto (IVA) è un'imposta applicata ai beni e servizi forniti in Francia e viene addebitata al cliente finale. Le aziende devono registrarsi nel registro per il commercio e le aziende in Francia per ottenere il numero di partita IVA.</p> <p>Vedere "Numero di partita IVA francese" a pagina 1047.</p>
Numero di partita IVA austriaco	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Austria, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA austriaco" a pagina 936.</p>
Numero di identificazione fiscale svedese	Identificatori di dati	<p>La Svezia utilizza i numeri di identificazione fiscale (TIN) per identificare i contribuenti e facilitare l'amministrazione delle questioni fiscali nazionali. I TIN sono anche utili per identificare i contribuenti che investono in altri paesi dell'UE e sono più affidabili di altri identificatori come il nome e l'indirizzo.</p> <p>Vedere "Numero di identificazione fiscale svedese" a pagina 1256.</p>
Numero di partita IVA svedese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.</p> <p>Vedere "Numero di partita IVA svedese" a pagina 1258.</p>

Nome	Tipo	Descrizione
Numero di partita IVA danese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Danimarca, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA danese" a pagina 1012.</p>
Numero di passaporto finlandese	Identificatori di dati	<p>Il passaporto finlandese viene rilasciato alle persone di nazionalità finlandese per viaggiare all'estero. Inoltre facilita le procedure di assistenza fornite dai funzionari consolari finlandesi all'estero.</p> <p>Vedere "Numero di passaporto finlandese" a pagina 1034.</p>
Numero di patente di guida finlandese	Identificatori di dati	<p>Numero di identificazione per la patente di guida personale emesso in uno stato membro dell'UE o del SEE per una patente finlandese.</p> <p>Vedere "Numero di patente di guida finlandese" a pagina 1029.</p>
Numero di partita IVA finlandese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.</p> <p>Vedere "Numero di partita IVA finlandese" a pagina 1038.</p>

Nome	Tipo	Descrizione
Numero di passaporto irlandese	Identificatori di dati	<p>Un passaporto irlandese è il passaporto rilasciato ai cittadini irlandesi. Un passaporto irlandese consente al portatore di viaggiare a livello internazionale e serve come prova della cittadinanza irlandese e della cittadinanza dell'Unione Europea. Facilita inoltre l'accesso all'assistenza consolare delle ambasciate irlandesi e di quelle di qualsiasi altro stato membro dell'Unione Europea all'estero.</p> <p>Vedere "Numero di passaporto irlandese" a pagina 1113.</p>
Numero di partita IVA irlandese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Per l'Irlanda, la partita IVA è emessa dall'autorità fiscale irlandese.</p> <p>Vedere "Numero di partita IVA irlandese" a pagina 1118.</p>
Numero di identificazione fiscale irlandese	Identificatori di dati	<p>Questo numero è rilasciato dal dipartimento della protezione sociale per le persone fisiche e dal commissario per le entrate per le persone giuridiche. Le persone giuridiche possono essere aziende, società di persone, trust ed enti non costituiti in società.</p> <p>Vedere "Numero di identificazione fiscale irlandese" a pagina 1114.</p>

Nome	Tipo	Descrizione
Numero di passaporto lussemburghese	Identificatori di dati	<p>Un passaporto lussemburghese è un documento di viaggio internazionale rilasciato ai cittadini del Granducato di Lussemburgo che può anche servire come prova della cittadinanza lussemburghese.</p> <p>Vedere "Numero di passaporto lussemburghese" a pagina 1155.</p>
Numero di partita IVA lussemburghese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.</p> <p>Vedere "Numero di partita IVA lussemburghese" a pagina 1161.</p>
Numero di identificazione nazionale portoghese	Identificatori di dati	<p>Il numero di identificazione nazionale è un numero di identificazione univoco solitamente presente in documenti come la carta del cittadino che il governo portoghese rilascia ai propri cittadini. Può essere utilizzato come documento di viaggio all'interno dell'UE e in altri paesi europei.</p> <p>Vedere "Numero di identificazione nazionale portoghese" a pagina 1208.</p>
Numero di passaporto portoghese	Identificatori di dati	<p>Il passaporto portoghese viene rilasciato ai cittadini portoghesi per viaggiare all'estero. Il passaporto, insieme alla carta di identità nazionale, dà diritto di movimento e residenza liberi in uno qualsiasi degli stati dell'Unione Europea e dello Spazio Economico Europeo.</p> <p>Vedere "Numero di passaporto portoghese" a pagina 1211.</p>

Nome	Tipo	Descrizione
Numero di identificazione fiscale portoghese	Identificatori di dati	<p>Un codice fiscale è un numero di identificazione fiscale rilasciato in Portogallo a chiunque desideri intraprendere qualsiasi attività ufficiale in Portogallo.</p> <p>Vedere "Numero di identificazione fiscale portoghese" a pagina 1212.</p>
Numero di partita IVA portoghese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.</p> <p>Vedere "Numero di partita IVA portoghese" a pagina 1215.</p>
Numero di patente di guida portoghese	Identificatori di dati	<p>L'Istituto per la mobilità e il trasporto terrestre (IMTT) rilascia le patenti di guida in Portogallo.</p> <p>Vedere "Numero di patente di guida portoghese" a pagina 1206.</p>
Numero di identificazione fiscale danese	Identificatori di dati	<p>La Danimarca rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Danimarca. Il numero di identificazione fiscale funge anche da numero di assicurazione sanitaria personale.</p> <p>Vedere "Numero di identificazione fiscale danese" a pagina 1009.</p>
Numero di identificazione fiscale finlandese	Identificatori di dati	<p>La Finlandia rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Finlandia.</p> <p>Vedere "Numero di identificazione fiscale finlandese" a pagina 1035.</p>

Nome	Tipo	Descrizione
Numero di identificazione fiscale lussemburghese	Identificatori di dati	<p>Questo numero è emesso dal dipartimento delle entrate interne lussemburghesi (Administration des contributions directes, ACD) e viene utilizzato a fini fiscali per le persone fisiche e giuridiche.</p> <p>Vedere "Numero di identificazione fiscale lussemburghese" a pagina 1157.</p>
Numero di identificazione fiscale tedesco	Identificatori di dati	<p>La Germania rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Germania.</p> <p>Vedere "Numero di identificazione fiscale tedesco" a pagina 1060.</p>
Numero di partita IVA britannico (VAT)	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Nel Regno Unito, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA britannico (VAT)" a pagina 1291.</p>
Numero di partita IVA spagnolo	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. L'IVA in Spagna è controllata dall'ente statale di amministrazione fiscale.</p> <p>Vedere "Numero di partita IVA spagnolo" a pagina 1240.</p>

Nome	Tipo	Descrizione
Coordinate bancarie di un numero di conto britannico	Identificatori di dati	<p>Le coordinate bancarie sono codici bancari utilizzati per instradare i trasferimenti di denaro tra banche all'interno dei rispettivi paesi attraverso le rispettive organizzazioni di liquidazione.</p> <p>Vedere "Coordinate bancarie di un numero di conto britannico" a pagina 1277.</p>
Codice fiscale della Grecia (AMKA)	Identificatori di dati	<p>Il codice fiscale AMKA è il numero identificativo di lavoro e di assicurazione di ogni lavoratore, pensionato e membro della famiglia protetto in Grecia.</p> <p>Vedere "Codice fiscale della Grecia (AMKA)" a pagina 1065.</p>
Numero di identificazione nazionale rumeno	Identificatori di dati	<p>A ogni cittadino rumeno viene assegnato un codice numerico personale (Cod Numeric Personal, CNP) come numero univoco di identificazione nazionale. Questo numero viene anche utilizzato come numero di identificazione fiscale per scopi finanziari.</p> <p>Vedere "Numero di identificazione nazionale rumeno" a pagina 1221.</p>
Numero di identificazione nazionale slovacco	Identificatori di dati	<p>In Slovacchia, le carte di identità sono rilasciate dalle autorità statali a ogni cittadino all'età di 15 anni. Questo numero viene utilizzato nella Repubblica Slovacca come principale identificatore univoco di ogni persona da istituzioni governative, banche e così via.</p> <p>Vedere "Numero di identificazione nazionale slovacco" a pagina 1230.</p>

Nome	Tipo	Descrizione
Numero identificativo cittadini della Slovenia	Identificatori di dati	<p>Il numero identificativo dei cittadini è un numero di identificazione univoco assegnato a tutti i cittadini sloveni alla nascita o acquisizione della cittadinanza.</p> <p>Vedere "Numero identificativo cittadini della Slovenia" a pagina 1233.</p>
Numero di identificazione personale lettone	Identificatori di dati	<p>Il numero di identificazione personale lettone viene utilizzato come numero di identificazione nazionale e codice fiscale per scopi finanziari. Viene emesso dall'ufficio per la cittadinanza e la migrazione del Ministero degli Interni.</p> <p>Vedere "Numero di identificazione personale lettone" a pagina 1151.</p>
Numero di patente di guida svedese	Identificatori di dati	<p>In Svezia, la patente di guida è necessaria quando si conduce un'auto, un motociclo o un ciclomotore su strade pubbliche. Le patenti di guida sono emesse dalle commissioni di sicurezza pubblica delle prefetture e sono supervisionate su base nazionale dall'ente nazionale di polizia.</p> <p>Vedere "Numero di patente di guida svedese" a pagina 1254.</p>

Regolamento generale per la protezione dei dati (identità digitale)

Questo modello è dedicato alle parole chiave del Regolamento generale per la protezione dei dati (GDPR) relative all'identità digitale, oltre agli identificatori di dati e al profilo EDM con colonne connesse.

Il GDPR è un regolamento con cui la Commissione Europea vuole rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. Tratta inoltre dell'esportazione dei dati personali all'esterno dell'UE. Gli obiettivi principali del GDPR sono di restituire ai cittadini il controllo sui propri dati personali e di semplificare le norme per le aziende internazionali unificando i regolamenti all'interno dell'UE. Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Tabella 41-30 Regola di rilevamento Regolamenti generali per la protezione dei dati (identità digitale)

Nome	Tipo	Descrizione
Numero IMEI	Identificatori di dati	<p>Il numero IMEI (International Mobile Equipment Identity) è un identificatore univoco per cellulari 3GPP (GSM, UMTS e LTE) e iDEN, nonché alcuni telefoni satellitari.</p> <p>Vedere "Numero IMEI" a pagina 1104.</p>

Regolamento generale per la protezione dei dati (identificazione governativa)

Questo modello è dedicato alle parole chiave del Regolamento generale per la protezione dei dati (GDPR) relative all'identificazione governativa, oltre agli identificatori di dati e al profilo EDM con colonne connesse.

Il GDPR è un regolamento con cui la Commissione Europea vuole rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. Tratta inoltre dell'esportazione dei dati personali all'esterno dell'UE. Gli obiettivi principali del GDPR sono di restituire ai cittadini il controllo sui propri dati personali e di semplificare le norme per le aziende internazionali unificando i regolamenti all'interno dell'UE. Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Tabella 41-31 Regole di rilevamento Regolamenti generali per la protezione dei dati (identificazione governativa)

Nome	Tipo	Descrizione
Parole chiave relative all'identificazione governativa nel GDPR	Corrispondenza parole chiave	<p>Definisce la corrispondenza di un elenco di parole chiave relative:</p> <p>patente di guida, numero carta d'identità, numero tessera elettorale numero, Führerscheinnnummer, ID-Kartenummer, Stimmzettel-Nummer, Numéro permis conduire, numéro carte d'identité, numéro du rôle électoral, numero patente guida, numero carta d'identità, numero elettorale rotolo, Número licencia conducir, número tarjeta de identificación, número boleta elettorale, rijbewijs nummer, ID-kaartnummer, kiezerslijst nummer, körkort nummer, identitetskort nummer, førerkortnummer, ID-kortnummer, ajokortin numero, numero Henkilökortin, numero vaaliluettelon, uimhir ceadúnas tiomána, Uimhir aitheantais chárta, uimhir rolla toghcháin, Identifikatiounskaart, número licença motorista, Número si cartão de identificação, número leitoral</p>
Numero di patente di guida britannica	Identificatori di dati	<p>Il numero di patente di guida britannica è il numero di identificazione della patente di guida individuale rilasciata dalla Driver and Vehicle Licensing Agency del Regno Unito.</p> <p>Vedere "Numero di patente di guida britannica" a pagina 1279.</p>

Nome	Tipo	Descrizione
Numero di tessera elettorale britannico	Identificatori di dati	<p>Il numero di tessera elettorale britannico è il numero di identificazione rilasciato ai cittadini per la registrazione elettorale. Il formato di questo numero è specificato dagli standard governativi dell'Ufficio del Gabinetto del Regno Unito.</p> <p>Vedere "Numero di tessera elettorale britannico" a pagina 1282.</p>
Numero NHS (National Health Service) del Regno Unito	Identificatori di dati	<p>Il numero NHS (National Health Service) del Regno Unito è il numero di identificazione personale rilasciato dal National Health Service (sistema sanitario nazionale) britannico per la gestione dell'assistenza medica.</p> <p>Vedere "Numero NHS (National Health Service) del Regno Unito" a pagina 1282.</p>
Numero di previdenza sociale britannico	Identificatori di dati	<p>Il numero di previdenza sociale britannico viene rilasciato dal Department for Work and Pensions (dipartimento per il lavoro e le pensioni) del Regno Unito ai fini dell'identificazione degli individui nell'ambito del programma di previdenza sociale nazionale. È noto anche come numero NI, NINO o NINo.</p> <p>Vedere "Numero di previdenza sociale britannico" a pagina 1285.</p>
Numero di passaporto britannico	Identificatori di dati	<p>Il numero di passaporto britannico identifica un passaporto britannico utilizzando la specifica ufficiale corrente degli standard governativi dell'Ufficio del Gabinetto del Regno Unito.</p> <p>Vedere "Numero di passaporto britannico" a pagina 1287.</p>

Nome	Tipo	Descrizione
Codice fiscale britannico	Identificatori di dati	<p>Il codice fiscale britannico è un numero di identificazione personale fornito dagli standard governativi dell'Ufficio del Gabinetto del Regno Unito.</p> <p>Vedere "Codice fiscale britannico" a pagina 1289.</p>
Numero di passaporto francese	Identificatori di dati	<p>Il passaporto francese è un documento di identità rilasciato ai cittadini francesi. Oltre a consentire al portatore di viaggiare all'estero e servire come indicazione della cittadinanza francese, il passaporto assicura l'assistenza del consolato francese all'estero o, se necessario, di altri stati membri dell'Unione Europea, nel caso in cui il console francese non sia presente.</p> <p>Vedere "Numero di passaporto francese" a pagina 1051.</p>
Numero di identificazione nazionale belga	Identificatori di dati	<p>Tutti i cittadini del Belgio hanno un numero di identificazione nazionale. I belgi di età superiore ai 12 anni possiedono una carta d'identità belga.</p> <p>Vedere "Numero di identificazione nazionale belga" a pagina 942.</p>
Numero di identificazione personale ceco	Identificatori di dati	<p>A tutti i cittadini della repubblica Ceca viene assegnato un numero di identificazione personale univoco rilasciato dal Ministero dell'Interno.</p> <p>Vedere "Numero di identificazione personale ceco" a pagina 1004.</p>

Nome	Tipo	Descrizione
Codice INSEE francese	Identificatori di dati	<p>In Francia il codice INSEE viene utilizzato come numero di previdenza sociale, un numero di identificazione nazionale, e a scopi fiscali e lavorativi.</p> <p>Vedere "Codice INSEE francese" a pagina 1049.</p>
Numero di previdenza sociale francese	Identificatori di dati	<p>Il numero di previdenza sociale francese (FSSN) è un numero univoco assegnato ai cittadini francesi o agli stranieri residenti nel paese. Funge da numero di identificazione nazionale.</p> <p>Vedere "Numero di previdenza sociale francese" a pagina 1052.</p>
Codice fiscale greco (AFM)	Identificatori di dati	<p>L'Arithmo Forologiko Mitro (AFM) è un codice fiscale personale univoco assegnato a ogni persona residente o proprietaria di beni in Grecia.</p> <p>Vedere "Codice fiscale greco (AFM)" a pagina 1067.</p>
Numero di previdenza sociale ungherese	Identificatori di dati	<p>Il numero di previdenza sociale ungherese (TAJ) è un identificatore univoco rilasciato dal governo ungherese.</p> <p>Vedere "Numero di previdenza sociale ungherese" a pagina 1078.</p>
Numero di identificazione fiscale (TIN) ungherese	Identificatori di dati	<p>Il numero di identificazione fiscale ungherese è un numero di 10 cifre che comincia sempre con la cifra "8".</p> <p>Vedere "Numero di identificazione fiscale ungherese" a pagina 1080.</p>

Nome	Tipo	Descrizione
Numero di partita IVA ungherese	Identificatori di dati	<p>Tutte le imprese ungheresi (incluse le organizzazioni non profit) registrate presso l'agenzia delle entrate nazionale hanno un numero di partita IVA.</p> <p>Vedere "Numero di partita IVA ungherese" a pagina 1082.</p>
Numero personale di servizio pubblico irlandese (PPS)	Identificatori di dati	<p>Il formato del numero è una stringa alfanumerica univoca di 8 caratteri che termina con una lettera, ad esempio 8765432A. Viene assegnato alla registrazione del neonato, è indicato sulla carta dei servizi sociali ed è univoco.</p> <p>Vedere "Numero personale di servizio pubblico irlandese" a pagina 1121.</p>
Numero di identificazione lussemburghese (RNPP)	Identificatori di dati	<p>Il numero di identificazione lussemburghese è un numero di identificazione di 11 cifre rilasciato a tutti i cittadini del Lussemburgo all'età di 15 anni.</p> <p>Vedere "Numero di identificazione lussemburghese (RNPP)" a pagina 1153.</p>
Numero di carta di identità polacca	Identificatori di dati	<p>Ogni cittadino polacco che ha compiuto i 18 anni di età e che risiede in modo permanente in Polonia deve avere una carta di identità con un numero personale univoco. Tale numero viene utilizzato come strumento di identificazione in parecchi ambiti.</p> <p>Vedere "Numero di carta di identità polacca" a pagina 1197.</p>

Nome	Tipo	Descrizione
Codice statistico polacco (REGON)	Identificatori di dati	<p>In Polonia ogni entità economica deve essere registrata nel Registro delle attività nazionali denominato REGON. È l'unico registro integrato del paese in cui sono elencate tutte le imprese nazionali. Ogni società ha un numero REGON univoco.</p> <p>Vedere "Codice statistico polacco (REGON)" a pagina 1199.</p>
Codice fiscale polacco (PESEL)	Identificatori di dati	<p>Il codice fiscale polacco (PESEL) è il numero di identificazione nazionale utilizzato in Polonia. Il numero PESEL è obbligatorio per tutte le persone residenti in modo permanente o temporaneo in Polonia. Esso identifica unicamente una persona e non può essere trasferito a un altro individuo.</p> <p>Vedere "Codice fiscale polacco (PESEL)" a pagina 1201.</p>
Numero di identificazione fiscale polacco (NIP)	Identificatori di dati	<p>Il numero di identificazione fiscale polacco (NIP) è un numero che il governo assegna a ogni cittadino polacco che lavora o svolge un'attività commerciale in Polonia. Questo codice è denominato NIP.</p> <p>Vedere "Numero di identificazione fiscale polacco (NIP)" a pagina 1203.</p>

Nome	Tipo	Descrizione
Numero di identificazione personale rumeno (CNP)	Identificatori di dati	<p>A ogni cittadino rumeno viene assegnato un numero di identificazione personale. Tale numero è utilizzato come strumento di riconoscimento da autorità, assistenza sanitaria, scuole, università, banche e compagnie di assicurazione.</p> <p>Vedere "Numero di identificazione personale rumeno (CNP)" a pagina 1223.</p>
Numero di DNI spagnolo	Identificatori di dati	<p>Il numero di DNI spagnolo è riportato sul Documento nacional de identidad (DNI) ed è rilasciato dall'Hacienda Publica spagnola a tutti i cittadini spagnoli. È il più importante identificatore univoco utilizzato in Spagna per l'apertura di conti, la firma di contratti, le tasse e le elezioni.</p> <p>Vedere "Numero di DNI spagnolo" a pagina 1245.</p>
Numero di previdenza sociale spagnolo	Identificatori di dati	<p>Il numero di previdenza sociale spagnolo è un numero a 12 cifre assegnato ai lavoratori spagnoli per consentire l'accesso al sistema sanitario spagnolo.</p> <p>Vedere "Numero di previdenza sociale spagnolo" a pagina 1249.</p>
Numero di conto cliente spagnolo	Identificatori di dati	<p>Il numero di conto cliente spagnolo è il numero di conto bancario standard utilizzato in Spagna.</p> <p>Vedere "Numero di conto cliente spagnolo" a pagina 1243.</p>

Nome	Tipo	Descrizione
Codice di identificazione fiscale spagnolo (CIF)	Identificatori di dati	<p>Il codice fiscale spagnolo (CIF) è equivalente alla partita IVA ed è necessario per svolgere un'attività lavorativa in Spagna. Esso è il numero identificativo di un'azienda per scopi fiscali ed è obbligatorio per qualsiasi transazione giuridica.</p> <p>Vedere "Codice fiscale spagnolo (CIF)" a pagina 1251.</p>
Numero di passaporto tedesco	Identificatori di dati	<p>Il numero di passaporto tedesco viene rilasciato alle persone di nazionalità tedesca, in genere per viaggiare all'estero. Un passaporto tedesco è un documento ufficialmente riconosciuto che le autorità tedesche accettano come prova dell'identità dai cittadini tedeschi.</p> <p>Vedere "Numero di passaporto tedesco" a pagina 1054.</p>
Numero di cittadinanza univoco bulgaro (EGN)	Identificatori di dati	<p>Il numero di cittadinanza univoco (EGN) è un numero univoco assegnato ai cittadini bulgari o agli stranieri residenti nel paese. Funge da numero di identificazione nazionale. L'EGN viene assegnato ai cittadini bulgari alla nascita o al momento del rilascio del certificato di nascita.</p> <p>Vedere "Numero di cittadinanza univoco bulgaro (EGN)" a pagina 967.</p>

Nome	Tipo	Descrizione
Numero di previdenza sociale austriaco	Identificatori di dati	<p>Il numero di previdenza sociale austriaco è assegnato ai cittadini austriaci che usufruiscono di prestazioni di assistenza sociale. È rilasciato da un'associazione ombrello dell'ente di previdenza sociale austriaco.</p> <p>Vedere "Numero di previdenza sociale austriaco" a pagina 939.</p>
Numero di passaporto spagnolo	Identificatori di dati	<p>I passaporti spagnoli sono rilasciati ai cittadini spagnoli per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto spagnolo" a pagina 1247.</p>
Numero di passaporto svedese	Identificatori di dati	<p>Il passaporto svedese viene rilasciato alle persone di nazionalità svedese per viaggiare all'estero. Oltre a servire quale prova della cittadinanza svedese, assicura l'assistenza del consolato svedese all'estero o, se necessario, di altri stati membri dell'Unione Europea, nel caso in cui sia il console svedese non sia presente.</p> <p>Vedere "Numero di passaporto svedese" a pagina 1260.</p>
Numero di identificazione personale tedesco	Identificatori di dati	<p>Il numero di identificazione personale tedesco è rilasciato a tutti i cittadini tedeschi.</p> <p>Vedere "Numero di identificazione personale tedesco" a pagina 1056.</p>

Nome	Tipo	Descrizione
Burgerservicenummer	Identificatori di dati	<p>Nei Paesi Bassi, il Burgerservicenummer è utilizzato per identificare in modo univoco i cittadini ed è stampato su patenti di guida, passaporti e documenti d'identità internazionali sotto l'intestazione Numero personale.</p> <p>Vedere "Burgerservicenummer" a pagina 970.</p>
Codice Fiscale	Identificatori di dati	<p>Il codice fiscale identifica in modo univoco i cittadini italiani o gli stranieri con residenza permanente in Italia e viene rilasciato a livello centralizzato dal Ministero del Tesoro. In Italia il codice fiscale viene rilasciato a tutti i cittadini alla nascita.</p> <p>Vedere "Codice Fiscale" a pagina 979.</p>
Codice identificativo personale finlandese	Identificatori di dati	<p>Il numero di identificazione personale finlandese o il codice identificativo personale è un identificatore personale univoco utilizzato per l'identificazione dei cittadini all'interno del governo e di molte altre transazioni.</p> <p>Vedere "Codice identificativo personale finlandese" a pagina 1040.</p>
Numero di identificazione personale svedese	Identificatori di dati	<p>Il numero di identificazione personale svedese è l'identificazione nazionale univoca per ogni cittadino svedese. Tale numero è utilizzato come strumento di riconoscimento da autorità, assistenza sanitaria, scuole, università, banche e compagnie di assicurazione.</p> <p>Vedere "Numero di identificazione personale svedese" a pagina 1262.</p>

Nome	Tipo	Descrizione
Numero di passaporto austriaco	Identificatori di dati	<p>I passaporti austriaci sono documenti di viaggio rilasciati ai cittadini austriaci dalle autorità preposte in Austria e all'estero e consentono di effettuare viaggi internazionali.</p> <p>Vedere "Numero di passaporto austriaco" a pagina 933.</p>
Numero di identificazione fiscale austriaco	Identificatori di dati	<p>L'Austria rilascia numeri di identificazione fiscale agli individui in base alla loro area di residenza per identificare i contribuenti e agevolare le imposte nazionali.</p> <p>Vedere "Numero di identificazione fiscale austriaco" a pagina 935.</p>
Numero di passaporto belga	Identificatori di dati	<p>Il passaporto belga è rilasciato dallo stato belga ai suoi cittadini per consentire loro di viaggiare all'estero. Il Servizio pubblico federale degli Affari Esteri, in precedenza noto come Ministero degli Affari Esteri, è responsabile del rilascio e del rinnovo dei passaporti belgi.</p> <p>Vedere "Numero di passaporto belga" a pagina 947.</p>
Numero di identificazione fiscale belga	Identificatori di dati	<p>Il Belgio rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Belgio.</p> <p>Vedere "Numero di identificazione fiscale belga" a pagina 948.</p>

Nome	Tipo	Descrizione
Numero di partita IVA belga	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Belgio, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA belga" a pagina 951.</p>
Numero di patente di guida belga	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Belgio.</p> <p>Vedere "Numero di patente di guida belga" a pagina 945.</p>
Numero di identificazione personale danese	Identificatori di dati	<p>Ogni cittadino danese ha un numero di identificazione nazionale. Tale numero viene utilizzato come prova dell'identità di una persona in molti ambiti.</p> <p>Vedere "Numero di identificazione personale danese" a pagina 1007.</p>
Numero di patente di guida dei Paesi Bassi	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'ente governativo RDW nei Paesi Bassi.</p> <p>Vedere "Numero di patente di guida dei Paesi Bassi" a pagina 1183.</p>
Numero di passaporto dei Paesi Bassi	Identificatori di dati	<p>Il passaporto dei Paesi Bassi viene rilasciato ai cittadini dei Paesi Bassi per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto dei Paesi Bassi" a pagina 1184.</p>

Nome	Tipo	Descrizione
Numero di partita IVA dei Paesi Bassi	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Nei Paesi Bassi, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA dei Paesi Bassi" a pagina 1189.</p>
Numero di patente di guida francese	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Francia.</p> <p>Vedere "Numero di patente di guida francese" a pagina 1042.</p>
Numero di previdenza sociale francese	Identificatori di dati	<p>La Carte Vitale è una tessera di previdenza sociale utilizzata in Francia che contiene le informazioni mediche del titolare. Ha un numero di serie univoco di 21 cifre.</p> <p>Vedere "Numero di previdenza sociale francese" a pagina 1044.</p>
Numero di identificazione fiscale francese	Identificatori di dati	<p>La Francia rilascia un numero di identificazione fiscale a chiunque abbia l'obbligo di dichiarazione fiscale in Francia.</p> <p>Vedere "Numero di identificazione fiscale francese" a pagina 1045.</p>
Numero di patente di guida tedesca	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Germania.</p> <p>Vedere "Numero di patente di guida tedesca" a pagina 1059.</p>

Nome	Tipo	Descrizione
Numero di passaporto italiano	Identificatori di dati	<p>Il passaporto italiano viene rilasciato ai cittadini italiani per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto italiano" a pagina 1129.</p>
Numero di partita IVA italiano	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Italia, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA italiano" a pagina 1131.</p>
Numero di patente di guida italiana	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Italia.</p> <p>Vedere "Numero di patente di guida italiana" a pagina 1126.</p>
Numero di identificazione fiscale dei Paesi Bassi	Identificatori di dati	<p>I Paesi Bassi emettono un numero di identificazione fiscale al momento della nascita o della registrazione presso l'anagrafe.</p> <p>Vedere "Numero di identificazione fiscale dei Paesi Bassi" a pagina 1185.</p>
Numero di patente di guida spagnola	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Spagna.</p> <p>Vedere "Numero di patente di guida spagnola" a pagina 1238.</p>

Nome	Tipo	Descrizione
Carta di identità ucraina	Identificatori di dati	<p>La carta di identità ucraina presenta un numero di 15 cifre rilasciato ai cittadini ucraini. È utilizzata come documento identificativo al posto del passaporto interno ucraino a partire dal 2016.</p> <p>Vedere "Carta di identità ucraina" a pagina 1296.</p>
Numero di passaporto interno ucraino	Identificatori di dati	<p>Un documento di identità rilasciato ai cittadini ucraini per l'uso nazionale. È stato sostituito dalla carta di identità ucraina a partire dal 2016, ma i passaporti esistenti sono ancora validi.</p> <p>Vedere "Passaporto ucraino (interno)" a pagina 1294.</p>
Numero di passaporto internazionale ucraino	Identificatori di dati	<p>Un documento utilizzato dai cittadini ucraini per viaggiare all'estero.</p> <p>Vedere "Passaporto ucraino (internazionale)" a pagina 1298.</p>
Numero di partita IVA della Germania	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Germania, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di patente di guida tedesca" a pagina 1059.</p>

Nome	Tipo	Descrizione
Numero di partita IVA della Francia	Identificatori di dati	<p>L'IVA è un'imposta applicata ai beni e servizi forniti in Francia e viene addebitata al cliente finale. Le aziende devono registrarsi nel registro per il commercio e le aziende in Francia per ottenere il numero di partita IVA.</p> <p>Vedere "Numero di partita IVA francese" a pagina 1047.</p>
Numero di passaporto irlandese	Identificatori di dati	<p>Un passaporto irlandese è il passaporto rilasciato ai cittadini irlandesi. Un passaporto irlandese consente al portatore di viaggiare a livello internazionale e serve come prova della cittadinanza irlandese e della cittadinanza dell'Unione Europea. Facilita inoltre l'accesso all'assistenza consolare delle ambasciate irlandesi e di quelle di qualsiasi altro stato membro dell'Unione Europea all'estero.</p> <p>Vedere "Numero di passaporto irlandese" a pagina 1113.</p>
Numero di passaporto lussemburghese	Identificatori di dati	<p>Un passaporto lussemburghese è un documento di viaggio internazionale rilasciato ai cittadini del Granducato di Lussemburgo che può anche servire come prova della cittadinanza lussemburghese.</p> <p>Vedere "Numero di passaporto lussemburghese" a pagina 1155.</p>

Nome	Tipo	Descrizione
Numero di passaporto portoghese	Identificatori di dati	<p>Il passaporto portoghese viene rilasciato ai cittadini portoghesi per viaggiare all'estero. Il passaporto, insieme alla carta di identità nazionale, dà diritto di movimento e residenza liberi in uno qualsiasi degli stati dell'Unione Europea e dello Spazio Economico Europeo.</p> <p>Vedere "Numero di passaporto portoghese" a pagina 1211.</p>
Numero di passaporto finlandese	Identificatori di dati	<p>Il passaporto finlandese viene rilasciato alle persone di nazionalità finlandese per viaggiare all'estero. Inoltre facilita le procedure di assistenza fornite dai funzionari consolari finlandesi all'estero.</p> <p>Vedere "Numero di passaporto finlandese" a pagina 1034.</p>
Numero di patente di guida finlandese	Identificatori di dati	<p>Numero di identificazione per la patente di guida personale emesso in uno stato membro dell'UE o del SEE per una patente finlandese.</p> <p>Vedere "Numero di patente di guida finlandese" a pagina 1029.</p>
Numero di partita IVA austriaco	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Austria, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA austriaco" a pagina 936.</p>

Nome	Tipo	Descrizione
Numero di identificazione fiscale svedese	Identificatori di dati	<p>La Svezia utilizza i numeri di identificazione fiscale (TIN) per identificare i contribuenti e facilitare l'amministrazione delle questioni fiscali nazionali. I TIN sono anche utili per identificare i contribuenti che investono in altri paesi dell'UE e sono più affidabili di altri identificatori come il nome e l'indirizzo.</p> <p>Vedere "Numero di identificazione fiscale svedese" a pagina 1256.</p>
Numero di partita IVA svedese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.</p> <p>Vedere "Numero di partita IVA svedese" a pagina 1258.</p>
Numero di partita IVA danese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. In Danimarca, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA danese" a pagina 1012.</p>
Numero di partita IVA finlandese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.</p> <p>Vedere "Numero di partita IVA finlandese" a pagina 1038.</p>

Nome	Tipo	Descrizione
Numero di partita IVA irlandese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Per l'Irlanda, la partita IVA è emessa dall'autorità fiscale irlandese.</p> <p>Vedere "Numero di partita IVA irlandese" a pagina 1118.</p>
Numero di identificazione fiscale irlandese	Identificatori di dati	<p>Questo numero è rilasciato dal dipartimento della protezione sociale per le persone fisiche e dal commissario per le entrate per le persone giuridiche. Le persone giuridiche possono essere aziende, società di persone, trust ed enti non costituiti in società.</p> <p>Vedere "Numero di identificazione fiscale irlandese" a pagina 1114.</p>
Numero di identificazione fiscale portoghese	Identificatori di dati	<p>Un codice fiscale è un numero di identificazione fiscale rilasciato in Portogallo a chiunque desideri intraprendere qualsiasi attività ufficiale in Portogallo.</p> <p>Vedere "Numero di identificazione fiscale portoghese" a pagina 1212.</p>
Numero di partita IVA portoghese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.</p> <p>Vedere "Numero di partita IVA portoghese" a pagina 1215.</p>

Nome	Tipo	Descrizione
Numero di partita IVA lussemburghese	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione.</p> <p>Vedere "Numero di partita IVA lussemburghese" a pagina 1161.</p>
Numero di identificazione nazionale portoghese	Identificatori di dati	<p>Il numero di identificazione nazionale è un numero di identificazione univoco solitamente presente in documenti come la carta del cittadino che il governo portoghese rilascia ai propri cittadini. Può essere utilizzato come documento di viaggio all'interno dell'UE e in altri paesi europei.</p> <p>Vedere "Numero di identificazione nazionale portoghese" a pagina 1208.</p>
Numero di patente di guida portoghese	Identificatori di dati	<p>L'Istituto per la mobilità e il trasporto terrestre (IMTT) rilascia le patenti di guida in Portogallo.</p> <p>Vedere "Numero di patente di guida portoghese" a pagina 1206.</p>
Numero di identificazione fiscale danese	Identificatori di dati	<p>La Danimarca rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Danimarca. Il numero di identificazione fiscale funge anche da numero di assicurazione sanitaria personale.</p> <p>Vedere "Numero di identificazione fiscale danese" a pagina 1009.</p>

Nome	Tipo	Descrizione
Numero di identificazione fiscale finlandese	Identificatori di dati	<p>La Finlandia rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Finlandia.</p> <p>Vedere "Numero di identificazione fiscale finlandese" a pagina 1035.</p>
Numero di identificazione fiscale lussemburghese	Identificatori di dati	<p>Questo numero è emesso dal dipartimento delle entrate interne lussemburghesi (Administration des contributions directes, ACD) e viene utilizzato a fini fiscali per le persone fisiche e giuridiche.</p> <p>Vedere "Numero di identificazione fiscale lussemburghese" a pagina 1157.</p>
Numero di identificazione fiscale tedesco	Identificatori di dati	<p>La Germania rilascia un numero di identificazione fiscale per individui che hanno l'obbligo di dichiarazione fiscale in Germania.</p> <p>Vedere "Numero di identificazione fiscale tedesco" a pagina 1060.</p>
Numero di partita IVA britannico (VAT)	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. Nel Regno Unito, la partita IVA è emessa dall'ufficio preposto per la regione in cui si stabilisce l'attività.</p> <p>Vedere "Numero di partita IVA britannico (VAT)" a pagina 1291.</p>

Nome	Tipo	Descrizione
Numero di partita IVA spagnolo	Identificatori di dati	<p>L'IVA è un'imposta di consumo a carico del consumatore finale. L'IVA è pagata per ogni transazione del processo di produzione e distribuzione. L'IVA in Spagna è controllata dall'ente statale di amministrazione fiscale.</p> <p>Vedere "Numero di partita IVA spagnolo" a pagina 1240.</p>
Coordinate bancarie di un numero di conto britannico	Identificatori di dati	<p>Le coordinate bancarie sono codici bancari utilizzati per instradare i trasferimenti di denaro tra banche all'interno dei rispettivi paesi attraverso le rispettive organizzazioni di liquidazione.</p> <p>Vedere "Coordinate bancarie di un numero di conto britannico" a pagina 1277.</p>
Codice fiscale della Grecia (AMKA)	Identificatori di dati	<p>Il codice fiscale AMKA è il numero identificativo di lavoro e di assicurazione di ogni lavoratore, pensionato e membro della famiglia protetto in Grecia.</p> <p>Vedere "Codice fiscale della Grecia (AMKA)" a pagina 1065.</p>
Numero di identificazione nazionale rumeno	Identificatori di dati	<p>A ogni cittadino rumeno viene assegnato un codice numerico personale (Cod Numeric Personal, CNP) come numero univoco di identificazione nazionale. Questo numero viene anche utilizzato come numero di identificazione fiscale per scopi finanziari.</p> <p>Vedere "Numero di identificazione nazionale rumeno" a pagina 1221.</p>

Nome	Tipo	Descrizione
Numero di identificazione nazionale slovacco	Identificatori di dati	<p>In Slovacchia, le carte di identità sono rilasciate dalle autorità statali a ogni cittadino all'età di 15 anni. Questo numero viene utilizzato nella Repubblica Slovacca come principale identificatore univoco di ogni persona da istituzioni governative, banche e così via.</p> <p>Vedere "Numero di identificazione nazionale slovacco" a pagina 1230.</p>
Numero identificativo cittadini della Slovenia	Identificatori di dati	<p>Il numero identificativo dei cittadini è un numero di identificazione univoco assegnato a tutti i cittadini sloveni alla nascita o acquisizione della cittadinanza.</p> <p>Vedere "Numero identificativo cittadini della Slovenia" a pagina 1233.</p>
Numero di identificazione personale lettone	Identificatori di dati	<p>Il numero di identificazione personale lettone viene utilizzato come numero di identificazione nazionale e codice fiscale per scopi finanziari. Viene emesso dall'ufficio per la cittadinanza e la migrazione del Ministero degli Interni.</p> <p>Vedere "Numero di identificazione personale lettone" a pagina 1151.</p>
Numero di previdenza sociale europea della Finlandia	Identificatori di dati	<p>L'identificatore numerico di 20 cifre univoco assegnato a ogni persona che utilizza i servizi sanitari in Finlandia.</p> <p>Vedere "Numero di previdenza sociale europea della Finlandia" a pagina 1032.</p>

Nome	Tipo	Descrizione
Numero di patente di guida svedese	Identificatori di dati	<p>In Svezia, la patente di guida è necessaria quando si conduce un'auto, un motociclo o un ciclomotore su strade pubbliche. Le patenti di guida sono emesse dalle commissioni di sicurezza pubblica delle prefetture e sono supervisionate su base nazionale dall'ente nazionale di polizia.</p> <p>Vedere "Numero di patente di guida svedese" a pagina 1254.</p>

Regolamento generale per la protezione dei dati (sanità e assicurazioni)

Questo modello è dedicato alle parole chiave del Regolamento generale per la protezione dei dati (GDPR) relative a sanità e assicurazioni, oltre agli identificatori di dati e al profilo EDM con colonne connesse.

Il GDPR è un regolamento con cui la Commissione Europea vuole rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. Tratta inoltre dell'esportazione dei dati personali all'esterno dell'UE. Gli obiettivi principali del GDPR sono di restituire ai cittadini il controllo sui propri dati personali e di semplificare le norme per le aziende internazionali unificando i regolamenti all'interno dell'UE. Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Tabella 41-32

Regole di rilevamento Regolamenti generali per la protezione dei dati (sanità e assicurazioni)

Nome	Tipo	Descrizione
Parole chiave relative a sanità e assicurazioni nel GDPR	Corrispondenza parole chiave	<p>Definisce la corrispondenza di un elenco di parole chiave relative:</p> <p>account number, bank card number,ID card number, medical record number,Kontonummer, Bankkartennummer, ID-Kartennummer, medizinische Datensatznummer, Numéro compte, banque carte nombre, numéro de carte d'identité, numéro d'enregistrement médical, numero conto, numero carta banca, numero carta d'identità, numero cartella clinica, número cuenta, Número cuenta bancaria, Numero de la tarjeta identificacion, número registro médico, rekeningnummer, bank kaartnummer, identiteitskaartnummer, medisch dossier nummer, bankkortnummer, identitetskortnummer, ID-kortnummer, tilinúmero, pankkikortin numero, Henkilökortin numero, lääketieteellisen ennätysnumero, uimhir chuntais, uimhir chárta bainc, Uimhir chárta aitheantais, uimhir taifead leighis, Kontosnummer, Identifikatiounskaart, medizinescher Dateschutznummer, número de conta, número cartão bancário, Número do cartão de identificação</p>

Nome	Tipo	Descrizione
Numero di patente di guida britannica	Identificatori di dati	<p>Il numero di patente di guida britannica è il numero di identificazione della patente di guida individuale rilasciata dalla Driver and Vehicle Licensing Agency del Regno Unito.</p> <p>Vedere "Numero di patente di guida britannica" a pagina 1279.</p>
Numero NHS (National Health Service) del Regno Unito	Identificatori di dati	<p>Il numero NHS (National Health Service) del Regno Unito è il numero di identificazione personale rilasciato dal National Health Service (sistema sanitario nazionale) britannico per la gestione dell'assistenza medica.</p> <p>Vedere "Numero NHS (National Health Service) del Regno Unito" a pagina 1282.</p>
Numero di previdenza sociale britannico	Identificatori di dati	<p>Il numero di previdenza sociale britannico viene rilasciato dal Department for Work and Pensions (dipartimento per il lavoro e le pensioni) del Regno Unito ai fini dell'identificazione degli individui nell'ambito del programma di previdenza sociale nazionale. È noto anche come numero NI, NINO o NINo.</p> <p>Vedere "Numero di previdenza sociale britannico" a pagina 1285.</p>
Numero di identificazione nazionale belga	Identificatori di dati	<p>Tutti i cittadini del Belgio hanno un numero di identificazione nazionale. I belgi di età superiore ai 12 anni possiedono una carta d'identità belga.</p> <p>Vedere "Numero di identificazione nazionale belga" a pagina 942.</p>

Nome	Tipo	Descrizione
Numero di identificazione personale ceco	Identificatori di dati	<p>A tutti i cittadini della repubblica Ceca viene assegnato un numero di identificazione personale univoco rilasciato dal Ministero dell'Interno.</p> <p>Vedere "Numero di identificazione personale ceco" a pagina 1004.</p>
Codice INSEE francese	Identificatori di dati	<p>In Francia il codice INSEE viene utilizzato come numero di previdenza sociale, un numero di identificazione nazionale, e a scopi fiscali e lavorativi.</p> <p>Vedere "Codice INSEE francese" a pagina 1049.</p>
Numero di previdenza sociale francese	Identificatori di dati	<p>Il numero di previdenza sociale francese (FSSN) è un numero univoco assegnato ai cittadini francesi o agli stranieri residenti nel paese. Funge da numero di identificazione nazionale.</p> <p>Vedere "Numero di previdenza sociale francese" a pagina 1052.</p>
Numero di previdenza sociale ungherese	Identificatori di dati	<p>Il numero di previdenza sociale ungherese (TAJ) è un identificatore univoco rilasciato dal governo ungherese.</p> <p>Vedere "Numero di previdenza sociale ungherese" a pagina 1078.</p>
Numero personale di servizio pubblico irlandese (PPS)	Identificatori di dati	<p>Il formato del numero è una stringa alfanumerica univoca di 8 caratteri che termina con una lettera, ad esempio 8765432A. Viene assegnato alla registrazione del neonato, è indicato sulla carta dei servizi sociali ed è univoco.</p> <p>Vedere "Numero personale di servizio pubblico irlandese" a pagina 1121.</p>

Nome	Tipo	Descrizione
Numero di identificazione lussemburghese (RNPP)	Identificatori di dati	<p>Il numero di identificazione lussemburghese è un numero di identificazione di 11 cifre rilasciato a tutti i cittadini del Lussemburgo all'età di 15 anni.</p> <p>Vedere "Numero di identificazione lussemburghese (RNPP)" a pagina 1153.</p>
Numero di carta di identità polacca	Identificatori di dati	<p>Ogni cittadino polacco che ha compiuto i 18 anni di età e che risiede in modo permanente in Polonia deve avere una carta di identità con un numero personale univoco. Tale numero viene utilizzato come strumento di identificazione in parecchi ambiti.</p> <p>Vedere "Numero di carta di identità polacca" a pagina 1197.</p>
Codice statistico polacco (REGON)	Identificatori di dati	<p>In Polonia ogni entità economica deve essere registrata nel Registro delle attività nazionali denominato REGON. È l'unico registro integrato del paese in cui sono elencate tutte le imprese nazionali. Ogni società ha un numero REGON univoco.</p> <p>Vedere "Codice statistico polacco (REGON)" a pagina 1199.</p>
Codice fiscale polacco (PESEL)	Identificatori di dati	<p>Il codice fiscale polacco (PESEL) è il numero di identificazione nazionale utilizzato in Polonia. Il numero PESEL è obbligatorio per tutte le persone residenti in modo permanente o temporaneo in Polonia. Esso identifica unicamente una persona e non può essere trasferito a un altro individuo.</p> <p>Vedere "Codice fiscale polacco (PESEL)" a pagina 1201.</p>

Nome	Tipo	Descrizione
Numero di identificazione personale rumeno (CNP)	Identificatori di dati	<p>A ogni cittadino rumeno viene assegnato un numero di identificazione personale. Tale numero è utilizzato come strumento di riconoscimento da autorità, assistenza sanitaria, scuole, università, banche e compagnie di assicurazione.</p> <p>Vedere "Numero di identificazione personale rumeno (CNP)" a pagina 1223.</p>
Numero di DNI spagnolo	Identificatori di dati	<p>Il numero di DNI spagnolo è riportato sul Documento nacional de identidad (DNI) ed è rilasciato dall'Hacienda Publica spagnola a tutti i cittadini spagnoli. È il più importante identificatore univoco utilizzato in Spagna per l'apertura di conti, la firma di contratti, le tasse e le elezioni.</p> <p>Vedere "Numero di DNI spagnolo" a pagina 1245.</p>
Numero di previdenza sociale spagnolo	Identificatori di dati	<p>Il numero di previdenza sociale spagnolo è un numero a 12 cifre assegnato ai lavoratori spagnoli per consentire l'accesso al sistema sanitario spagnolo.</p> <p>Vedere "Numero di previdenza sociale spagnolo" a pagina 1249.</p>

Nome	Tipo	Descrizione
Numero di cittadinanza univoco bulgaro (EGN)	Identificatori di dati	<p>Il numero di cittadinanza univoco (EGN) è un numero univoco assegnato ai cittadini bulgari o agli stranieri residenti nel paese. Funge da numero di identificazione nazionale. L'EGN viene assegnato ai cittadini bulgari alla nascita o al momento del rilascio del certificato di nascita.</p> <p>Vedere "Numero di cittadinanza univoco bulgaro (EGN)" a pagina 967.</p>
Numero di previdenza sociale austriaco	Identificatori di dati	<p>Il numero di previdenza sociale austriaco è assegnato ai cittadini austriaci che usufruiscono di prestazioni di assistenza sociale. È rilasciato da un'associazione ombrello dell'ente di previdenza sociale austriaco.</p> <p>Vedere "Numero di previdenza sociale austriaco" a pagina 939.</p>
Numero di identificazione personale tedesco	Identificatori di dati	<p>Il numero di identificazione personale tedesco è rilasciato a tutti i cittadini tedeschi.</p> <p>Vedere "Numero di identificazione personale tedesco" a pagina 1056.</p>
Burgerservicenummer	Identificatori di dati	<p>Nei Paesi Bassi, il Burgerservicenummer è utilizzato per identificare in modo univoco i cittadini ed è stampato su patenti di guida, passaporti e documenti d'identità internazionali sotto l'intestazione Numero personale.</p> <p>Vedere "Burgerservicenummer" a pagina 970.</p>

Nome	Tipo	Descrizione
Codice Fiscale	Identificatori di dati	<p>Il codice fiscale identifica in modo univoco i cittadini italiani o gli stranieri con residenza permanente in Italia e viene rilasciato a livello centralizzato dal Ministero del Tesoro. In Italia il codice fiscale viene rilasciato a tutti i cittadini alla nascita.</p> <p>Vedere "Codice Fiscale" a pagina 979.</p>
Codice identificativo personale finlandese	Identificatori di dati	<p>Il numero di identificazione personale finlandese o il codice identificativo personale è un identificatore personale univoco utilizzato per l'identificazione dei cittadini all'interno del governo e di molte altre transazioni.</p> <p>Vedere "Codice identificativo personale finlandese" a pagina 1040.</p>
Numero di identificazione personale svedese	Identificatori di dati	<p>Il numero di identificazione personale svedese è l'identificazione nazionale univoca per ogni cittadino svedese. Tale numero è utilizzato come strumento di riconoscimento da autorità, assistenza sanitaria, scuole, università, banche e compagnie di assicurazione.</p> <p>Vedere "Numero di identificazione personale svedese" a pagina 1262.</p>
Numero di patente di guida belga	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Belgio.</p> <p>Vedere "Numero di patente di guida belga" a pagina 945.</p>

Nome	Tipo	Descrizione
Numero di identificazione personale danese	Identificatori di dati	<p>Ogni cittadino danese ha un numero di identificazione nazionale. Tale numero viene utilizzato come prova dell'identità di una persona in molti ambiti.</p> <p>Vedere "Numero di identificazione personale danese" a pagina 1007.</p>
Numero di patente di guida dei Paesi Bassi	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'ente governativo RDW nei Paesi Bassi.</p> <p>Vedere "Numero di patente di guida dei Paesi Bassi" a pagina 1183.</p>
Numero di patente di guida francese	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Francia.</p> <p>Vedere "Numero di patente di guida francese" a pagina 1042.</p>
Numero di previdenza sociale francese	Identificatori di dati	<p>La Carte Vitale è una tessera di previdenza sociale utilizzata in Francia che contiene le informazioni mediche del titolare. Ha un numero di serie univoco di 21 cifre.</p> <p>Vedere "Numero di previdenza sociale francese" a pagina 1044.</p>
Numero di patente di guida tedesca	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Germania.</p> <p>Vedere "Numero di patente di guida tedesca" a pagina 1059.</p>

Nome	Tipo	Descrizione
Numero di previdenza sociale italiano	Identificatori di dati	<p>La tessera sanitaria italiana è rilasciata a tutti i cittadini italiani dal Ministero italiano dell'Economia e della Finanza, in collaborazione con l'agenzia italiana delle entrate. L'obiettivo della tessera è quello di migliorare i servizi di previdenza sociale tramite il controllo delle spese e delle prestazioni, e di ottimizzare l'utilizzo dei servizi sanitari per i cittadini.</p> <p>Vedere "Numero di previdenza sociale italiano" a pagina 1127.</p>
Numero di patente di guida italiana	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Italia.</p> <p>Vedere "Numero di patente di guida italiana" a pagina 1126.</p>
Numero di patente di guida spagnola	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Spagna.</p> <p>Vedere "Numero di patente di guida spagnola" a pagina 1238.</p>
Numero di patente di guida finlandese	Identificatori di dati	<p>Numero di identificazione per la patente di guida personale emesso in uno stato membro dell'UE o del SEE per una patente finlandese.</p> <p>Vedere "Numero di patente di guida finlandese" a pagina 1029.</p>

Nome	Tipo	Descrizione
Numero di identificazione nazionale portoghese	Identificatori di dati	<p>Il numero di identificazione nazionale è un numero di identificazione univoco solitamente presente in documenti come la carta del cittadino che il governo portoghese rilascia ai propri cittadini. Può essere utilizzato come documento di viaggio all'interno dell'UE e in altri paesi europei.</p> <p>Vedere "Numero di identificazione nazionale portoghese" a pagina 1208.</p>
Numero di patente di guida portoghese	Identificatori di dati	<p>L'Istituto per la mobilità e il trasporto terrestre (IMTT) rilascia le patenti di guida in Portogallo.</p> <p>Vedere "Numero di patente di guida portoghese" a pagina 1206.</p>
Codice fiscale della Grecia (AMKA)	Identificatori di dati	<p>Il codice fiscale AMKA è il numero identificativo di lavoro e di assicurazione di ogni lavoratore, pensionato e membro della famiglia protetto in Grecia.</p> <p>Vedere "Codice fiscale della Grecia (AMKA)" a pagina 1065.</p>
Numero di identificazione nazionale rumeno	Identificatori di dati	<p>A ogni cittadino rumeno viene assegnato un codice numerico personale (Cod Numeric Personal, CNP) come numero univoco di identificazione nazionale. Questo numero viene anche utilizzato come numero di identificazione fiscale per scopi finanziari.</p> <p>Vedere "Numero di identificazione nazionale rumeno" a pagina 1221.</p>

Nome	Tipo	Descrizione
Numero di identificazione nazionale slovacco	Identificatori di dati	<p>In Slovacchia, le carte di identità sono rilasciate dalle autorità statali a ogni cittadino all'età di 15 anni. Questo numero viene utilizzato nella Repubblica Slovacca come principale identificatore univoco di ogni persona da istituzioni governative, banche e così via.</p> <p>Vedere "Numero di identificazione nazionale slovacco" a pagina 1230.</p>
Numero identificativo cittadini della Slovenia	Identificatori di dati	<p>Il numero identificativo dei cittadini è un numero di identificazione univoco assegnato a tutti i cittadini sloveni alla nascita o acquisizione della cittadinanza.</p> <p>Vedere "Numero identificativo cittadini della Slovenia" a pagina 1233.</p>
Numero di identificazione personale lettone	Identificatori di dati	<p>Il numero di identificazione personale lettone viene utilizzato come numero di identificazione nazionale e codice fiscale per scopi finanziari. Viene emesso dall'ufficio per la cittadinanza e la migrazione del Ministero degli Interni.</p> <p>Vedere "Numero di identificazione personale lettone" a pagina 1151.</p>
Numero di previdenza sociale europea della Finlandia	Identificatori di dati	<p>L'identificatore numerico di 20 cifre univoco assegnato a ogni persona che utilizza i servizi sanitari in Finlandia.</p> <p>Vedere "Numero di previdenza sociale europea della Finlandia" a pagina 1032.</p>

Nome	Tipo	Descrizione
Numero di patente di guida svedese	Identificatori di dati	<p>In Svezia, la patente di guida è necessaria quando si conduce un'auto, un motociclo o un ciclomotore su strade pubbliche. Le patenti di guida sono emesse dalle commissioni di sicurezza pubblica delle prefetture e sono supervisionate su base nazionale dall'ente nazionale di polizia.</p> <p>Vedere "Numero di patente di guida svedese" a pagina 1254.</p>

Regolamento generale per la protezione dei dati (profilo personale)

Questo modello è dedicato alle parole chiave del Regolamento generale per la protezione dei dati (GDPR) relative al profilo personale, oltre agli identificatori di dati e al profilo EDM con colonne connesse.

Il GDPR è un regolamento con cui la Commissione Europea vuole rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. Tratta inoltre dell'esportazione dei dati personali all'esterno dell'UE. Gli obiettivi principali del GDPR sono di restituire ai cittadini il controllo sui propri dati personali e di semplificare le norme per le aziende internazionali unificando i regolamenti all'interno dell'UE. Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Tabella 41-33 Regola di rilevamento Regolamenti generali per la protezione dei dati (profilo personale)

Nome	Tipo	Descrizione
Parole chiave relative al profilo personale nel GDPR	Corrispondenza parole chiave	

Nome	Tipo	Descrizione
		<p>Definisce la corrispondenza di un elenco di parole chiave relative:</p> <p>titolo di studio, esperienze di lavoro, qualifiche professionali, riepilogo delle qualifiche, dati, dati biografici, CV, curriculum vitae, Akademische Details, Arbeitsgeschichte, Berufsqualifikation, Zusammenfassung der Qualifikationen, Bio-Daten, Lebenslauf, Bio Daten, Les données académiques, la qualification professionnelle, le résumé des qualifications, Bio données, le curriculum vitae, dettagli accademici, storia del lavoro, qualificazione professionale, sintesi delle qualifiche, i dati bio, bio-dati, Datos académicos, historial de trabajo, calificación profesional, resumen de calificaciones, datos bio, bio-datos, akademische informatie, werk geschiedenis, beroepskwalificatie, samenvatting van kwalificaties, bio gegevens, bio-gegevens, leerplan vitae, akademiska detaljer, Jobbhistorik, professionell kvalifikation, sammanfattning av kvalifikation, meritförteckning, akademiske detaljer, arbejdshistorie, professionel kvalifikation, Resumé af kvalifikation, Genoptag, akateemiset yksityiskohdat, työhistoria, ammattipätevyys, yhteenveto tutkinnoist, sonraí acadúla, stair oibre, cáilíocht ghairmiúil, achoimre ar cháilíochtaí,</p>

Nome	Tipo	Descrizione
		akademesch Detaller, Aarbechtsgeschicht, berufleeh Qualifikatioun, Zesummefaassung vu Qualifikatiounen, Liewenslaf, detalhes acadêmicos, histórico de trabalho, qualificação profissional, sumário de qualificações, Currículo

Regolamento generale per la protezione dei dati (viaggi)

Questo modello è dedicato alle parole chiave del Regolamento generale per la protezione dei dati (GDPR) relative ai viaggi, oltre agli identificatori di dati e al profilo EDM con colonne connesse.

Il GDPR è un regolamento con cui la Commissione Europea vuole rafforzare e unificare la protezione dei dati delle persone all'interno dell'UE. Tratta inoltre dell'esportazione dei dati personali all'esterno dell'UE. Gli obiettivi principali del GDPR sono di restituire ai cittadini il controllo sui propri dati personali e di semplificare le norme per le aziende internazionali unificando i regolamenti all'interno dell'UE. Il GDPR sostituisce le Direttive UE sulla protezione dei dati a partire dal 25 maggio 2018.

Tabella 41-34 Regole di rilevamento Regolamenti generali per la protezione dei dati (viaggi)

Nome	Tipo	Descrizione
Parole chiave relative a viaggi nel GDPR	Corrispondenza parole chiave	

Nome	Tipo	Descrizione
		<p>Definisce la corrispondenza di un elenco di parole chiave relative:</p> <p>account number, bank card number, driver license number, ID card number, passenger name, seat number, luggage details, journey details, purchase details, purchase invoice, travel ticket, travel invoice, passenger details, tourist details, Kontonummer, Bankkartennummer, Führerscheinnummer, Ausweisnummer, Passagiername, Sitzplatznummer, Einkaufsdetails, Kaufrechnungen, Passagierdetails, Touristendetails, Gepäckdetails, Fahrtdetails, ReiseFahrkarte, ReiseRechnung, numéro compte, numéro carte bancaire, numéro de permis de conduire, numéro de carte d'identité, passager nom, numéro du siège, bagage détails, détails voyage, l'achat détails, la facture d'achat, billet de voyage, la facture voyage, détails passager, détails touristiques, numero di conto, numero carta banca, numero patente di guida, numero carta d'identità, nome passeggero, numero del posto, dettagli dei bagagli, dettagli di viaggio, dettagli acquisto, fattura acquisto, biglietto viaggio, fattura viaggio, dati passeggeri, dettagli turistiche, Número cuenta, número tarjeta bancaria, número licencia de</p>

Nome	Tipo	Descrizione
		<p>conducir, número de tarjeta identificación, nombre pasajero, número asiento, detalles equipaje, detalles de viaje, detalles de compra, viaje factura, viaje billete, factura de viaje, pasajeros detalles, detalles turísticos, rekeningnummer, bankkaart nummer, rijbewijs nummer, ID-kaart nummer, naam passagier, stoelnummer, bagage-informatie, reis informatie, aankoopgegevens, aankoopfactuur, reizenreisbiljet, reizen factuur, passagiersgegevens, toeristische informatie, bankkortnummer, körkort nummer, identitetskortnummer, Passengerarens namn, sitsnummer, reseinformation, köp detaljer, inköpsfaktura, resa biljett, resefaktura, passagerare detaljer, førerkortnummer, ID-kortnummer, Passagernavn, sæde nummer, bagage detaljer, rejsedetaljer, købsoplysninger, købsfaktura, rejse billet, rejse faktura, passageroplysninger, turist detaljer, tilinúmero, pankkikortin numero, ajokortin numero, Henkilökortin numero, matkustajan nimi, istumapaikan numero, matkatavaran yksityiskohdat, matk yksityiskoh, ostotiedot, matkustaalippu, matkustajan yksityiskohdat, turisti yksityiskohdat, uimhir chuntais, uimhir chárta bainc, uimhir ceadúnas tiomána, Uimhir chárta aitheantais, ainm</p>

Nome	Tipo	Descrizione
		<p>phaisinéara, uimhir suíocháin, sonraí turas, sonraí cheannach, cheannach sonrasc, sonrasc taistil, sonraí paisinéirí, sonraí turasóireachta, Kontosnummer, Identifikatiounskaart, Numm Passagéier, Sitznummer, Gepäckdetailer, Rees Detailer, kaaft Detailer, Passagéierdetailer, número de conta, número cartão bancário, número licença motorista, Número do cartão de identificação, Nome do passageiro, Número do assento, Detalhes bagagem, detalhes viagem, detalhes da compra, nota fiscal de compra, bilhete de viagem, factura de viagem, Detalhes do passageiro, detalhes do turista</p>
Numero di patente di guida britannica	Identificatori di dati	<p>Il numero di patente di guida britannica è il numero di identificazione della patente di guida individuale rilasciata dalla Driver and Vehicle Licensing Agency del Regno Unito.</p> <p>Vedere "Numero di patente di guida britannica" a pagina 1279.</p>
Numero di passaporto britannico	Identificatori di dati	<p>Il numero di passaporto britannico identifica un passaporto britannico utilizzando la specifica ufficiale corrente degli standard governativi dell'Ufficio del Gabinetto del Regno Unito.</p> <p>Vedere "Numero di passaporto britannico" a pagina 1287.</p>

Nome	Tipo	Descrizione
Numero di passaporto francese	Identificatori di dati	<p>Il passaporto francese è un documento di identità rilasciato ai cittadini francesi. Oltre a consentire al portatore di viaggiare all'estero e servire come indicazione della cittadinanza francese, il passaporto assicura l'assistenza del consolato francese all'estero o, se necessario, di altri stati membri dell'Unione Europea, nel caso in cui il console francese non sia presente.</p> <p>Vedere "Numero di passaporto francese" a pagina 1051.</p>
Numero di passaporto tedesco	Identificatori di dati	<p>Il numero di passaporto tedesco viene rilasciato alle persone di nazionalità tedesca, in genere per viaggiare all'estero. Un passaporto tedesco è un documento ufficialmente riconosciuto che le autorità tedesche accettano come prova dell'identità dai cittadini tedeschi.</p> <p>Vedere "Numero di passaporto tedesco" a pagina 1054.</p>
Numero di passaporto spagnolo	Identificatori di dati	<p>I passaporti spagnoli sono rilasciati ai cittadini spagnoli per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto spagnolo" a pagina 1247.</p>

Nome	Tipo	Descrizione
Numero di passaporto svedese	Identificatori di dati	<p>Il passaporto svedese viene rilasciato alle persone di nazionalità svedese per viaggiare all'estero. Oltre a servire quale prova della cittadinanza svedese, assicura l'assistenza del consolato svedese all'estero o, se necessario, di altri stati membri dell'Unione Europea, nel caso in cui sia il console svedese non sia presente.</p> <p>Vedere "Numero di passaporto svedese" a pagina 1260.</p>
Numero di passaporto austriaco	Identificatori di dati	<p>I passaporti austriaci sono documenti di viaggio rilasciati ai cittadini austriaci dalle autorità preposte in Austria e all'estero e consentono di effettuare viaggi internazionali.</p> <p>Vedere "Numero di passaporto austriaco" a pagina 933.</p>
Numero di passaporto belga	Identificatori di dati	<p>Il passaporto belga è rilasciato dallo stato belga ai suoi cittadini per consentire loro di viaggiare all'estero. Il Servizio pubblico federale degli Affari Esteri, in precedenza noto come Ministero degli Affari Esteri, è responsabile del rilascio e del rinnovo dei passaporti belgi.</p> <p>Vedere "Numero di passaporto belga" a pagina 947.</p>
Numero di patente di guida belga	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Belgio.</p> <p>Vedere "Numero di patente di guida belga" a pagina 945.</p>

Nome	Tipo	Descrizione
Numero di patente di guida dei Paesi Bassi	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'ente governativo RDW nei Paesi Bassi.</p> <p>Vedere "Numero di patente di guida dei Paesi Bassi" a pagina 1183.</p>
Numero di passaporto dei Paesi Bassi	Identificatori di dati	<p>Il passaporto dei Paesi Bassi viene rilasciato ai cittadini dei Paesi Bassi per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto dei Paesi Bassi" a pagina 1184.</p>
Numero di patente di guida francese	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Francia.</p> <p>Vedere "Numero di patente di guida francese" a pagina 1042.</p>
Numero di patente di guida tedesca	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Germania.</p> <p>Vedere "Numero di patente di guida tedesca" a pagina 1059.</p>
Numero di passaporto italiano	Identificatori di dati	<p>Il passaporto italiano viene rilasciato ai cittadini italiani per viaggiare all'estero.</p> <p>Vedere "Numero di passaporto italiano" a pagina 1129.</p>
Numero di patente di guida italiana	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Italia.</p> <p>Vedere "Numero di patente di guida italiana" a pagina 1126.</p>

Nome	Tipo	Descrizione
Numero di patente di guida spagnola	Identificatori di dati	<p>Numero di identificazione per la patente di guida individuale rilasciata dall'autorità preposta in Spagna.</p> <p>Vedere "Numero di patente di guida spagnola" a pagina 1238.</p>
Numero di passaporto interno ucraino	Identificatori di dati	<p>Un documento di identità rilasciato ai cittadini ucraini per l'uso nazionale. È stato sostituito dalla carta di identità ucraina a partire dal 2016, ma i passaporti esistenti sono ancora validi.</p> <p>Vedere "Passaporto ucraino (interno)" a pagina 1294.</p>
Numero di passaporto internazionale ucraino	Identificatori di dati	<p>Un documento utilizzato dai cittadini ucraini per viaggiare all'estero.</p> <p>Vedere "Passaporto ucraino (internazionale)" a pagina 1298.</p>
Numero di passaporto irlandese	Identificatori di dati	<p>Un passaporto irlandese è il passaporto rilasciato ai cittadini irlandesi. Un passaporto irlandese consente al portatore di viaggiare a livello internazionale e serve come prova della cittadinanza irlandese e della cittadinanza dell'Unione Europea. Facilita inoltre l'accesso all'assistenza consolare delle ambasciate irlandesi e di quelle di qualsiasi altro stato membro dell'Unione Europea all'estero.</p> <p>Vedere "Numero di passaporto irlandese" a pagina 1113.</p>

Nome	Tipo	Descrizione
Numero di passaporto lussemburghese	Identificatori di dati	<p>Un passaporto lussemburghese è un documento di viaggio internazionale rilasciato ai cittadini del Granducato di Lussemburgo che può anche servire come prova della cittadinanza lussemburghese.</p> <p>Vedere "Numero di passaporto lussemburghese" a pagina 1155.</p>
Numero di passaporto portoghese	Identificatori di dati	<p>Il passaporto portoghese viene rilasciato ai cittadini portoghesi per viaggiare all'estero. Il passaporto, insieme alla carta di identità nazionale, dà diritto di movimento e residenza liberi in uno qualsiasi degli stati dell'Unione Europea e dello Spazio Economico Europeo.</p> <p>Vedere "Numero di passaporto portoghese" a pagina 1211.</p>
Numero di passaporto finlandese	Identificatori di dati	<p>Il passaporto finlandese viene rilasciato alle persone di nazionalità finlandese per viaggiare all'estero. Inoltre facilita le procedure di assistenza fornite dai funzionari consolari finlandesi all'estero.</p> <p>Vedere "Numero di passaporto finlandese" a pagina 1034.</p>
Numero di patente di guida finlandese	Identificatori di dati	<p>Numero di identificazione per la patente di guida personale emesso in uno stato membro dell'UE o del SEE per una patente finlandese.</p> <p>Vedere "Numero di patente di guida finlandese" a pagina 1029.</p>

Nome	Tipo	Descrizione
Numero di patente di guida portoghese	Identificatori di dati	L'Istituto per la mobilità e il trasporto terrestre (IMTT) rilascia le patenti di guida in Portogallo. Vedere "Numero di patente di guida portoghese" a pagina 1206.
Numero di patente di guida svedese	Identificatori di dati	In Svezia, la patente di guida è necessaria quando si conduce un'auto, un motociclo o un ciclomotore su strade pubbliche. Le patenti di guida sono emesse dalle commissioni di sicurezza pubblica delle prefetture e sono supervisionate su base nazionale dall'ente nazionale di polizia. Vedere "Numero di patente di guida svedese" a pagina 1254.

Modello di politica Gramm-Leach-Bliley

La normativa Gramm-Leach-Bliley (GLB) Act riconosce ai consumatori il diritto di limitare la condivisione delle proprie informazioni personali da parte delle istituzioni finanziarie.

Il modello di politica Gramm-Leach-Bliley rileva la trasmissione dei dati dei clienti.

Tabella 41-35 Condizioni del modello di politica Gramm-Leach-Bliley

Metodo di rilevamento	Tipo	Descrizione
Combinazioni nome utente/password	Regola semplice: EDM	Questa regola cerca le combinazioni di nomi utente e password. Vedere "Scelta di un profilo dati esatti" a pagina 417.
SSN o CCN esatto	Regola semplice: EDM	Questa regola cerca il numero di previdenza sociale o il numero di carta di credito.
Directory clienti	Regola semplice: EDM	Questa regola cerca il telefono o l'e-mail.

Metodo di rilevamento	Tipo	Descrizione
3 o più campi del cliente critici	Regola semplice: EDM	<p>Questa regola cerca una corrispondenza tra tre dei campi seguenti:</p> <ul style="list-style-type: none"> ■ Numero di conto ■ Numero di carta di credito ■ Indirizzo e-mail ■ Nome ■ Cognome ■ Numero PIN ■ Numero di telefono ■ Numero di codice fiscale ■ Numero di routing ABA ■ Social Insurance Number (numero di previdenza sociale) canadese ■ Numero di previdenza sociale britannico ■ Data di nascita <p>Tuttavia le combinazioni seguenti non sono una corrispondenza:</p> <ul style="list-style-type: none"> ■ Telefono, e-mail e nome ■ Telefono, e-mail e cognome ■ E-mail, nome e cognome ■ Telefono, nome e cognome
Numeri di routing ABA	Regola semplice: DCM (DI)	<p>Questa condizione rileva numeri a nove cifre. Convalida il numero utilizzando la cifra di controllo finale. Questa condizione elimina i numeri di prova comuni, quali 123456789, gli intervalli numerici riservati per usi futuri e i numeri con tutte le cifre uguali. Richiede inoltre la presenza di una parola chiave relativa ad ABA.</p> <p>Vedere "Numero di routing ABA" a pagina 918.</p>
Social Security Number statunitensi	Regola semplice: DCM (DI)	<p>Questa regola cerca i numeri di codice fiscale. Affinché questa regola corrisponda, deve esservi un numero che si adatta all'identificatore dati Social Security Number (SSN) statunitense randomizzato. Deve inoltre esservi una parola chiave o una frase chiave che indica la presenza di un numero di previdenza sociale statunitense con una parola chiave nel dizionario "Parole chiave SSN statunitense". La condizione di parola chiave viene inclusa per ridurre i falsi positivi con qualsiasi numero che corrisponda al formato di numero di previdenza sociale.</p> <p>Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218.</p>

Metodo di rilevamento	Tipo	Descrizione
Numeri di carta di credito	Regola semplice: DCM (DI)	<p>Questa condizione rileva i numeri di carta di credito validi con spazi, trattini o punti come separatori o senza separatori. Esegue il controllo di convalida Luhn e include i formati di carta di credito seguenti:</p> <ul style="list-style-type: none"> ■ American Express ■ Diner's Club ■ Discover ■ Japan Credit Bureau (JCB) ■ Mastercard ■ Visa <p>Questa regola elimina i numeri di prova comuni, compresi quelli riservati ai test eseguiti dagli emittenti di carte di credito, e richiede la presenza di una parola chiave correlata alla carta di credito.</p> <p>Vedere "Copertura limitata numero carta di credito" a pagina 997.</p>

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica HIPAA e HITECH (incluso PHI)

La politica **HIPAA e HITECH (incluso PHI)** applica rigorosamente l'Health Insurance Portability and Accountability Act (HIPAA - Legge sulla trasferibilità e gli obblighi di rendere conto in materia di copertura assicurativa) degli Stati Uniti. L'Health Information Technology for Economic and Clinical Health Act (HITECH) è la prima normativa nazionale a prevedere la notifica di violazione per le informazioni sanitarie protette (PHI).

Questo modello di politica rileva i dati relativi a medicinali con ricetta medica, malattie e cure unitamente a informazioni PHI. Le organizzazioni non soggette a HIPAA possono anche usare questa politica per controllare i dati PHI.

Il modello di politica HIPAA e HITECH (incluso PHI) è aggiornato con elenchi di parole chiave corrispondenti a medicinali, malattie e cure basate su informazioni della FDA (Federal Drug Administration) degli Stati Uniti e di altre fonti. Il modello di politica è inoltre aggiornato per usare l'identificatore SSN statunitense randomizzato che individua codici SSN sia tradizionali che randomizzati.

Vedere ["Aggiornamento degli elenchi di parole chiave per le politiche HIPAA e Caldicott."](#) a pagina 785.

Vedere ["Aggiornamento delle politiche per l'utilizzo dell'identificatore dati Social Security Number \(SSN\) statunitense randomizzato"](#) a pagina 747.

[Tabella 41-36](#) descrive l'eccezione TPO fornita dal modello. TPO (Treatment, Payment, Operation) sono provider di servizi degli enti sanitari e dispongono di una deroga alle restrizioni di informazioni HIPAA. Il modello richiede l'immissione degli indirizzi e-mail autorizzati. Se implementata, l'eccezione viene valutata prima delle regole di rilevamento e la politica non attiva un incidente se le informazioni protette sono inviate a uno dei partner autorizzati.

Tabella 41-36 Eccezione TPO

Nome	Tipo	Configurazione
Eccezione TPO	Contenuto corrispondente a parola chiave (DCM)	Eccezione semplice (corrispondenza con un'unica condizione). Cerca un indirizzo e-mail destinatario corrispondente a uno presente nel dizionario di keyword definito dall'utente "Indirizzi e-mail TPO".

[Tabella 41-37](#) è una regola che cerca una corrispondenza di dati esatta in tutte le colonne di un record Dati paziente con profilo.

Tabella 41-37 Regola di rilevamento Dati paziente

Nome	Tipo	Configurazione
Dati paziente	Il contenuto corrisponde ai dati esatti (EDM)	Corrispondenza con dati di qualsiasi campo singolo: <ul style="list-style-type: none"> ■ Cognome ■ ID contribuente (SSN) ■ Indirizzo e-mail ■ Numero di conto ■ Numero di carta d'identità ■ Numero di telefono Vedere "Scelta di un profilo dati esatti" a pagina 417.

[Tabella 41-38](#) è una regola di rilevamento composta che richiede una corrispondenza esatta con Dati paziente e una corrispondenza con l'identificatore dati Codice medicinale.

Tabella 41-38 Regola di rilevamento Dati paziente e codici medicinali

Nome	Tipi di condizione	Configurazione
Dati paziente e codici medicinali	Il contenuto corrisponde ai dati esatti (EDM) e Contenuto corrispondente a identificatore dati	Cerca una corrispondenza con qualsiasi colonna di un record del database con profilo Dati paziente e una corrispondenza con l'identificatore dati National Drug Code (NDC). Vedere Tabella 41-37 a pagina 1417. Vedere " National Drug Code (NDC, codici identificativi dei farmaci) " a pagina 1178.

[Tabella 41-39](#) è una regola di rilevamento composta che richiede una corrispondenza esatta con Dati paziente e una corrispondenza parola chiave con il dizionario "Nomi medicinale con ricetta".

Tabella 41-39 Regola di rilevamento Dati paziente e Nomi medicinale con ricetta

Nome	Tipo di condizione	Configurazione
Dati paziente e Nomi medicinale con ricetta	Il contenuto corrisponde ai dati esatti (EDM) e Contenuto corrispondente a parola chiave (DCM)	Cerca una corrispondenza con qualsiasi colonna di un record del database con profilo Dati paziente e una corrispondenza parola chiave dal dizionario Nomi medicinale con ricetta. Vedere Tabella 41-37 a pagina 1417. Vedere " Aggiornamento delle politiche dopo l'upgrade alla versione più recente " a pagina 459.

[Tabella 41-40](#) è una regola di rilevamento composta che richiede una corrispondenza esatta con Dati paziente e una corrispondenza parola chiave con il dizionario "Parole chiave cura".

Tabella 41-40 Regola di rilevamento Dati paziente e parole chiave trattamento

Nome	Tipo di condizione	Configurazione
Dati paziente e parole chiave trattamento	Il contenuto corrisponde ai dati esatti (EDM) e Contenuto corrispondente a parola chiave (DCM)	Cerca una corrispondenza con qualsiasi colonna di un record del database con profilo Dati paziente e una corrispondenza parola chiave dal dizionario Parole chiave trattamento medico. Vedere Tabella 41-37 a pagina 1417. Vedere " Aggiornamento delle politiche dopo l'upgrade alla versione più recente " a pagina 459.

Tabella 41-41 è una regola di rilevamento composta che richiede una corrispondenza esatta con Dati paziente e una corrispondenza parola chiave con il dizionario "Nomi malattia".

Tabella 41-41 Regola di rilevamento Dati paziente e parole chiave malattia

Nome	Tipo di condizione	Configurazione
Dati paziente e parole chiave malattia	Il contenuto corrisponde ai dati esatti (EDM) e Contenuto corrispondente a parola chiave (DCM)	Cerca una corrispondenza con qualsiasi colonna di un record del database con profilo Dati paziente e una corrispondenza parola chiave dal dizionario Nomi malattia. Vedere Tabella 41-37 a pagina 1417. Vedere "Aggiornamento delle politiche dopo l'upgrade alla versione più recente" a pagina 459.

Tabella 41-42 è una regola di rilevamento composta che ricerca codici SSN mediante l'identificatore dati SSN statunitense randomizzato e una parola chiave dal dizionario "Nomi medicinale con ricetta".

Tabella 41-42 Regola di rilevamento SSN e parole chiave medicinali

Nome	Tipo di condizione	Configurazione
SSN e parole chiave medicinali	Contenuto corrispondente a identificatore dati e Contenuto corrispondente a parola chiave	Identificatore dati Social Security Number (SSN) statunitense randomizzato (copertura limitata) Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218. Dizionario di parole chiave Nomi medicinale con ricetta Vedere "Aggiornamento delle politiche dopo l'upgrade alla versione più recente" a pagina 459.

Tabella 41-43 è una regola di rilevamento composta che ricerca codici SSN mediante l'identificatore dati SSN statunitense randomizzato e una corrispondenza con una parola chiave dal dizionario "Parole chiave trattamento medico".

Tabella 41-43 Regola di rilevamento SSN e parole chiave trattamento

Nome	Tipo di condizione	Configurazione
SSN e parole chiave trattamento	Contenuto corrispondente a identificatore dati e Contenuto corrispondente a parola chiave	Identificatore dati Social Security Number (SSN) statunitense randomizzato (copertura limitata) Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218. Dizionario Parole chiave trattamento medico. Vedere "Aggiornamento delle politiche dopo l'upgrade alla versione più recente" a pagina 459.

[Tabella 41-44](#) è una regola di rilevamento composta che ricerca codici SSN mediante l'identificatore dati SSN statunitense randomizzato e una corrispondenza con una parola chiave dal dizionario "Nomi malattia".

Tabella 41-44 Regola di rilevamento SSN e parole chiave malattia

Nome	Tipo di condizione	Configurazione
SSN e parole chiave malattia	Contenuto corrispondente a identificatore dati e Contenuto corrispondente a parola chiave	Identificatore dati Social Security Number (SSN) statunitense randomizzato (copertura limitata) Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218. Dizionario di parole chiave Nomi malattia Vedere "Aggiornamento delle politiche dopo l'upgrade alla versione più recente" a pagina 459.

[Tabella 41-45](#) è una regola di rilevamento composta che ricerca codici SSN mediante l'identificatore dati SSN statunitense randomizzato e un codice medicinale mediante l'identificatore dati Codice medicinale.

Tabella 41-45 Regola di rilevamento SSN e codice medicinale

Nome	Tipo di condizione	Configurazione
SSN e codice medicinale	Contenuto corrispondente a identificatore dati e Contenuto corrispondente a parola chiave	Identificatore dati Social Security Number (SSN) statunitense randomizzato (copertura limitata) Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218. Identificatore dati Codice medicinale (copertura limitata) Vedere "National Drug Code (NDC, codici identificativi dei farmaci)" a pagina 1178.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Human Rights Act (legge sui diritti umani) del 1998

La Human Rights Act (legge sui diritti umani) del 1998 consente ai cittadini britannici di asserire ai loro diritti secondo la Convenzione Europea sui diritti umani sotto la giurisdizione del Regno Unito. La legge afferma che "per quanto possibile, la legislazione deve essere letta e applicata secondo modalità conformi ai diritti di convenzione". La politica Human Rights Act (legge sui diritti umani) del 1998 applica l'articolo 8 garantendo che le vite private dei cittadini britannici restino private.

Regola EDM

Data Protection Act britannico, dati personali

Questa regola composta cerca due tipi di dati, il cognome e il numero di tessera elettorale insieme a una parola chiave dal dizionario "Parole chiave Dati personali britannici".

Regola DCM

Numeri di tessera elettorale britannici

Questa regola cerca una singola condizione composta da quattro parti:

- Una parola chiave singola del dizionario "Parole chiave Regno Unito"
- Un formato che corrisponde a quello dell'identificatore dati Numero di tessera elettorale britannico
- Una parola chiave singola del dizionario "Parole Numero di tessera elettorale britannico"
- Una parola chiave singola del dizionario "Parole chiave dati personali britannici"

Vedere ["Scelta di un profilo dati esatti"](#) a pagina 417.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Sostanze illegali

Questa politica rileva le conversazioni relative a sostanze illegali e sostanze controllate.

Regola DCM

Stupefacenti

Questa regola cerca cinque istanze delle parole chiave dal dizionario "Nomi stupefacenti".

Regola DCM

Sostanze controllate prodotte in serie

Questa regola cerca cinque istanze di parole chiave nel dizionario "Sostanze controllate prodotte".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Codici identificativi dei contribuenti (ITIN)

Il codice identificativo del contribuente (ITIN) è un numero di elaborazione delle imposte rilasciato dall'Internal Revenue Service (IRS) statunitense. L'IRS rilascia questi codici per registrare le persone non idonee ai Social Security Number (SSN).

Tabella 41-46 Condizioni del modello della politica ITIN

Regola parola chiave DCM	Descrizione
ITIN	Questa regola ricerca una corrispondenza mediante l'identificatore dati ITIN statunitense e una parola chiave dal dizionario "Parole chiave ITIN statunitense".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica International Traffic in Arms Regulations (ITAR)

La normativa International Traffic in Arms Regulations (ITAR, normativa sul traffico internazionale di armi) viene applicata dal Dipartimento di Stato degli Stati Uniti. Gli esportatori dei servizi di difesa o dei dati tecnici correlati sono tenuti a registrarsi presso il governo federale e potrebbero aver bisogno di una licenza di esportazione. Questa politica rileva le potenziali violazioni sulla base dei paesi e delle risorse controllate designate dall'ITAR.

La regola di rilevamento Munizioni ITAR indicizzate e destinatari cerca un codice di paese per il destinatario nel dizionario "Codici di paese ITAR" e uno "SKU" specifico in un file EDM indicizzato.

Tabella 41-47 Regola di rilevamento Munizioni ITAR indicizzate e destinatari

Metodo	Condizioni (devono corrispondere entrambe)	Configurazione
Regola composta	Destinatario corrispondente a criterio (DCM)	Cercare la corrispondenza dell'e-mail del destinatario o del dominio dell'URL nell'elenco dei codici di paese ITAR: <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Almeno 1 destinatario deve corrispondere.
	Contenuto corrispondente a dati esatti (EDM)	Vedere "Scelta di un profilo dati esatti" a pagina 417.

La regola di rilevamento Lista delle munizioni ITAR e destinatari cerca un codice di paese per il destinatario nel dizionario "Codici di paese ITAR" e una parola chiave nel dizionario "Nomi munizioni ITAR".

Tabella 41-48 Regola di rilevamento Lista delle munizioni ITAR e destinatari

Metodo	Condizioni (devono corrispondere entrambe)	Configurazione
Regola composta	Destinatario corrispondente a criterio (DCM)	Cercare la corrispondenza dell'e-mail del destinatario o del dominio dell'URL nell'elenco dei codici di paese ITAR: <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Almeno 1 criterio del destinatario deve corrispondere.
	Contenuto corrispondente a parola chiave (DCM)	Cercare la corrispondenza di qualsiasi parola chiave della Lista delle munizioni ITAR: <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Cercare la corrispondenza solo con parole intere. ■ Gravità: Alta.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica File multimediali

La politica dei file multimediali individua i vari tipi di file audio e video (mp3 compreso).

Regola DCM

File multimediali

Questa regola cerca i seguenti tipi di file multimediali:

- qt
- riff
- macromedia_dir
- midi
- mp3
- mpeg_movie
- quickdraw
- realaudio
- wav
- video_win
- vrml

Regola DCM

Estensioni file multimediali

Questa regola cerca le estensioni dei file dal dizionario "Estensioni file multimediali".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Medicare e Medicaid (incluso PHI)

Questa politica rileva le informazioni sanitarie protette (PHI) associate ai programmi Medicare e Medicaid degli Stati Uniti, compresi i numeri dei beneficiari di Medicare, i numeri delle richieste di rimborso dell'assicurazione sanitaria e i codici CPT (Current Procedural Terminology) correnti utilizzati dal sistema di codifica delle procedure di assistenza sanitaria più comuni (Healthcare Common Procedure Coding System).

Tabella 41-49 Regole di rilevamento Medicare e Medicaid (incluso PHI)

Nome	Tipo di condizione	Descrizione
Healthcare Common Procedure Coding System (codici CPT HCPCS)	Identificatori di dati e Parole chiave	<p>Queste tre regole soddisfano la copertura media dell'identificatore di dati Healthcare Common Procedure Coding System (codici HCPCS CPT).</p> <p>Corrispondono a tutte le occorrenze univoche in messaggio, oggetto, corpo o allegati. Alle corrispondenze viene assegnato un livello di gravità Alto.</p> <p>Vedere "Healthcare Common Procedure Coding System (codice CPT HCPCS)." a pagina 1069.</p> <p>Richiedono inoltre la presenza di parole chiave associate.</p>
Identificatore beneficiario di assistenza sanitaria	Identificatori di dati	<p>Questa regola soddisfa la copertura limitata dell'identificatore dati Identificatore beneficiario di assistenza sanitaria.</p> <p>Corrisponde a tutte le occorrenze univoche in messaggio, oggetto, corpo o allegati. Alle corrispondenze viene assegnato un livello di gravità Alto.</p> <p>Vedere "Identificatore beneficiario di assistenza sanitaria" a pagina 1167.</p>
Numero di assicurazione sanitaria	Identificatori di dati	<p>Questa regola soddisfa la copertura limitata dell'identificatore dati Numero di assicurazione sanitaria.</p> <p>Corrisponde a tutte le occorrenze univoche in messaggio, oggetto, corpo o allegati. Alle corrispondenze viene assegnato un livello di gravità Alto.</p> <p>Vedere "Numero di assicurazione sanitaria" a pagina 1072.</p>

Modello della politica Contratti di acquisizione e fusione

Il modello della politica Contratti di acquisizione e fusione rileva i contratti e la documentazione ufficiale relativa ad attività di acquisizione e fusione.

È possibile modificare il modello con parole chiave specifiche per l'azienda per rilevare determinate transazioni.

Il modello Contratti di acquisizione e fusione fornisce una singola regola di rilevamento composta. Tutte le condizioni contenute nella regola devono corrispondere affinché la regola attivi un incidente.

Tabella 41-50 Regola di rilevamento composta Contratti di acquisizione e fusione

Condizione	Configurazione
Parole chiave specifiche per il contratto (Corrispondenza parole chiave)	<ul style="list-style-type: none"> ■ Corrispondenza con qualsiasi parola chiave:fusione, contratto, accordo, lettera di intenti, term sheet, piano di riorganizzazione ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.
Parole chiave struttura aziendale acquisizione (Corrispondenza parole chiave)	<ul style="list-style-type: none"> ■ Corrispondenza con qualsiasi parola chiave:sussidiaria, sussidiarie, affiliata, acquirente, sub-fusione, stipulante, azienda acquisita, azienda acquirente, impresa superstite, azienda superstite ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.
Parole chiave considerazione fusione (Corrispondenza parole chiave)	<ul style="list-style-type: none"> ■ Corrispondenza con qualsiasi parola chiave:fusione magazzino, condivisioni fusione, azioni di scambio, capitale sociale, azioni di dissenso, struttura del capitale, fondo svincolato, conto fiduciario, agente depositario, fondi in sospenso, deposito di garanzia, importo del fondo, esame magazzino, imposta sulla rinuncia, avviamento ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

Condizione	Configurazione
Parole chiave contratto legale (Corrispondenza parole chiave)	<ul style="list-style-type: none"> ■ Corrispondenza con qualsiasi parola chiave: resoconti, in fede, legge applicabile, indennizzare, indennizzato, indennità, pagina di firma, migliori sforzi, negligenza grave, dolo, rappresentante autorizzato, separabilità, violazione sostanziale ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Regola NASD 2711 e regole NYSE 351 e 472

Questa politica protegge i nomi delle società coinvolte in un'offerta di azioni imminente, i nomi dei progetti interni per l'offerta e i simboli della teleborsa per le società offerenti.

La regola di rilevamento Documenti regola NASD 2711, indicizzati cerca il contenuto in specifici documenti registrati come riservati e conosciuti come Regola NASD 2711 e Regole NYSE 351 e 472. Questa regola restituisce una corrispondenza se viene trovato l'80% o più del documento di origine.

Tabella 41-51 Regola di rilevamento Documenti regola NASD 2711, indicizzati

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a firma documento (IDM)	<p>Documenti regola NASD 2711, indicizzati (IDM):</p> <ul style="list-style-type: none"> ■ Rilevare i documenti nel profilo di documento indicizzato selezionato. ■ Impostare una corrispondenza di contenuto pari ad almeno l'80%. ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Eseguire la ricerca in corpo e allegati. <p>Vedere "Scelta di un profilo documento indicizzato" a pagina 419.</p>

La regola di rilevamento Regola NASD 2711 e regole NYSE 351 e 472 è una regola composta che contiene una condizione di mittente e una condizione di parola chiave. La condizione di mittente si basa su un elenco, definito dall'utente, di indirizzi e-mail di analisti di ricerca presso la società dell'utente (dizionario "Indirizzi e-mail degli analisti"). La condizione di parola chiave

cerca le offerte di azioni imminenti, i nomi dei progetti interni per l'offerta e i simboli della teleborsa per le società offerenti (dizionario "Parole chiave NASD 2711"). Come la condizione di mittente, richiede la modifica da parte dell'utente.

Tabella 41-52 Regola di rilevamento Regola NASD 2711 e regole NYSE 351 e 472

Metodo	Condizione	Configurazione
Regola composta	Mittente/utente corrisponde a criterio (DCM)	Regola NASD 2711 e regole NYSE 351 e 472 (mittente): <ul style="list-style-type: none"> ■ Cercare la corrispondenza dei criteri di mittente: [analista_ricerca@società.com] (definito dall'utente). ■ Gravità: Alta. ■ Cercare la corrispondenza con l'intero messaggio.
	Contenuto corrispondente a parola chiave (DCM)	Regola NASD 2711 e regole NYSE 351 e 472 (corrispondenza di parola chiave): <ul style="list-style-type: none"> ■ Cercare la corrispondenza di "[simbolo azione società]", "[nome società offerente]", "[nome offerta (nome interno)]". ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Regola NASD 3010 e regola NYSE 342

Le regole NASD 3010 e NYSE 342 richiedono la supervisione delle comunicazioni tra gli addetti all'intermediazione finanziaria da parte degli operatori di borsa. Questa politica consente di monitorare le comunicazioni degli azionisti principali registrati che sono soggetti a queste regole.

La regola di rilevamento Raccomandazione titoli azionari cerca una parola chiave nei dizionari "Parole chiave titoli azionari NASD 3010" e "Parole chiave acquisto/vendita NASD 3010". Inoltre questa regola richiede la prova di una raccomandazione di titoli azionari in combinazione con un'operazione di acquisto o vendita.

Tabella 41-53 Regola di rilevamento Raccomandazione titoli azionari

Metodo	Condizioni (devono corrispondere tutte)	Configurazione
Regola composta	Contenuto corrispondente a parola chiave (DCM)	<p>Corrispondenza con parola chiave: "raccomandazione"</p> <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Cercare la corrispondenza solo con parole intere.
	Contenuto corrispondente a parola chiave (DCM)	<p>Corrispondenza con parola chiave: "acquisto" o "vendita"</p> <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Cercare la corrispondenza solo con parole intere.
	Contenuto corrispondente a parola chiave (DCM)	<p>Corrispondenza con parola chiave: "azione, azioni, titolo, titoli, borsa"</p> <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Cercare la corrispondenza solo con parole intere.

La regola di rilevamento Parole chiave regola NASD 3010 e regola NYSE 342 cerca le parole chiave nel dizionario "Parole chiave generali NASD 3010", che cercano eventuali attività di borsa generali e parole chiave relative alle azioni.

Tabella 41-54 Regola di rilevamento Parole chiave regola NASD 3010 e regola NYSE 342

Metodo	Condizioni (devono corrispondere entrambe)	Configurazione
Regola composta	Contenuto corrispondente a parola chiave (DCM)	Corrispondenza con parola chiave: "autorizzare", "discrezione", "garanzia", "opzioni" <ul style="list-style-type: none">■ Gravità: Alta.■ Verificare esistenza.■ Cerca in busta, oggetto, corpo, allegati.■ Senza distinzione maiuscole/minuscole.■ Cercare la corrispondenza solo con parole intere.
	Contenuto corrispondente a parola chiave (DCM)	Corrispondenza con parola chiave: "azione, azioni, titolo, titoli, borsa" <ul style="list-style-type: none">■ Gravità: Alta.■ Verificare esistenza.■ Cerca in busta, oggetto, corpo, allegati.■ Senza distinzione maiuscole/minuscole.■ Cercare la corrispondenza solo con parole intere.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Linee guida sulla sicurezza del NERC per le società elettriche

Le linee guida del NERC (North American Electric Reliability Council) relative alla tutela delle informazioni riservate spiegano come proteggere i dati relativi all'infrastruttura elettrica critica.

Questa politica rileva le informazioni contenute nelle linee guida sulla sicurezza del NERC per il settore dell'energia elettrica.

Tabella 41-55 Regola di rilevamento Personale di risposta chiave

Metodo di rilevamento	Condizione di corrispondenza	Configurazione
Regola semplice	Contenuto corrispondente a dati esatti (EDM)	<p>Cercare la corrispondenza con tre qualsiasi dei seguenti elementi di dati:</p> <ul style="list-style-type: none"> ■ Nome ■ Cognome ■ Telefono ■ E-mail <p>Vedere "Scelta di un profilo dati esatti" a pagina 417.</p>

Tabella 41-56 Regola di rilevamento Mappe dell'infrastruttura di rete

Metodo di rilevamento	Condizione di corrispondenza	Configurazione
Regola semplice	Contenuto corrispondente a documenti indicizzati (IDM)	<p>Questa regola richiede una corrispondenza binaria esatta.</p> <p>Vedere "Scelta di un profilo documento indicizzato" a pagina 419.</p>

Le regole di rilevamento Parole chiave riservate e Parole chiave sulla vulnerabilità cercano le corrispondenze di parole chiave nei dizionari "Parole chiave riservate" e "Parole chiave sulla vulnerabilità".

Tabella 41-57 Regole di rilevamento Parole chiave riservate e Parole chiave sulla vulnerabilità

Metodo di rilevamento	Condizioni di corrispondenza	Configurazione
Regola composta	Contenuto corrispondente a parola chiave (DCM)	<p>Cercare la corrispondenza con qualsiasi parola chiave riservata:</p> <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo e allegati. ■ Senza distinzione maiuscole/minuscole. ■ Cercare la corrispondenza solo con parole intere.
	Contenuto corrispondente a parola chiave (DCM)	<p>Cercare la corrispondenza con qualsiasi parola chiave sulla vulnerabilità:</p> <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo e allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Diagrammi di rete

La politica Diagrammi di rete rileva i diagrammi di rete dei computer a rischio di divulgazione.

Regola IDM	<p>Diagrammi di rete, indicizzati</p> <p>Questa regola cerca il contenuto in diagrammi di rete specifici registrati come riservati. Questa regola restituisce una corrispondenza se l'80% o più del documento originale viene rilevato.</p>
Regola DCM	<p>Diagrammi di rete con indirizzi IP</p> <p>Questa regola cerca il tipo di file Visio insieme a un identificatore di dati dell'indirizzo IP.</p>
Regola DCM	<p>Diagrammi di rete con parola chiave indirizzo IP</p> <p>Questa regola cerca il tipo di file Visio insieme alle variazioni della frase "Indirizzo IP" con un identificatore di dati.</p>

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Sicurezza di rete

La politica Sicurezza di rete rileva la prova di strumenti di hacking e piani di attacco.

Regola DCM	Attività GoToMyPC Questa regola cerca un formato di comando GoToMyPC con un identificatore di dati.
Regola DCM	Parole chiave hacker Questa regola cerca una parola chiave dal dizionario "Parole chiave hacker".
Regola DCM	Parole chiave KeyLogger Questa regola cerca una parola chiave dal dizionario "Parole chiave keylogger".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Linguaggio offensivo

La politica Linguaggio offensivo individua l'utilizzo di linguaggio offensivo.

Regola DCM	Linguaggio offensivo, esplicito Questa regola cerca qualsiasi parola chiave contenuta nel dizionario "Linguaggio offensivo, esplicito".
Regola DCM	Linguaggio offensivo, generale Questa regola cerca tre istanze delle parole chiave nel dizionario "Linguaggio offensivo, generale".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica OFAC (Ufficio per il Controllo dei Fondi Stranieri)

L'Ufficio per il Controllo dei Fondi Stranieri del Dipartimento del Tesoro degli Stati Uniti amministra e applica sanzioni economiche e commerciali nei confronti di determinati paesi,

individui e organizzazioni sulla base della politica estera statunitense e degli obiettivi in tema di sicurezza nazionale. La politica OFAC rileva le comunicazioni concernenti i suddetti gruppi di destinatari.

La politica OFAC comprende due parti principali. La prima si occupa dell'elenco Specially Designated Nationals (SDN) e la seconda delle restrizioni della politica OFAC.

L'elenco SDN fa riferimento a persone oppure organizzazioni specifiche, soggette a limitazioni commerciali. Il Dipartimento del Tesoro degli Stati Uniti fornisce file di testo con nomi specifici, gli ultimi indirizzi noti e gli alias noti per gli individui e le entità. Il Dipartimento del Tesoro stipula che gli indirizzi possono non essere corretti o correnti e che le posizioni diverse non modificano le restrizioni per persone e organizzazioni.

Nel modello di politica OFAC, Symantec Data Loss Prevention ha pulito l'elenco per renderlo più utilizzabile e pratico. È compresa l'estrazione di parole chiave e frasi chiave dall'elenco di nomi e alias, in quanto i nomi non sono sempre visualizzati nello stesso formato dell'elenco. Inoltre i nomi comuni sono stati rimossi per ridurre i falsi positivi. Ad esempio, un'organizzazione nell'elenco SDN è nota come "SARA". Se la si lascia nell'elenco, si genera un'incidenza di falsi positivi elevata. "Proprietà SARA" è un'altra voce dell'elenco. Viene utilizzata come frase chiave nel modello perché l'incidenza della frase è nettamente inferiore rispetto alla voce "SARA" da sola. L'elenco dei nomi e delle organizzazioni è considerato in combinazione con i paesi trovati comunemente nell'elenco di indirizzi SDN. Dopo che si sono rimossi altri paesi che occorrono più comunemente, vengono considerati i 12 paesi principali nell'elenco. Il modello cerca i destinatari con uno dei paesi elencati come codice di paese designato. L'elenco SDN riduce al minimo i falsi positivi mentre continua a rilevare transazioni o comunicazioni con parti con restrizioni note.

La politica OFAC fornisce inoltre indicazioni per le restrizioni che il Dipartimento del Tesoro degli Stati Uniti ha imposto al commercio generale con determinati paesi. È distinta dall'elenco SDN, in quanto gli individui e le organizzazioni non sono specificati. L'elenco delle sanzioni generali è disponibile all'indirizzo

<http://www.treasury.gov/offices/enforcement/ofac/programs/index.shtml>.

Il modello OFAC cerca i destinatari nei paesi elencati dall'Ufficio per il Controllo dei Fondi Stranieri in base al codice di paese designato.

La regola di rilevamento Specially Designated National List (SDN, lista nazionale specialmente designata) dell'OFAC e destinatari cerca un destinatario con un codice di paese che corrisponda alle voci nella specifica "Codici di paese SDN OFAC" in combinazione con una corrispondenza con una parola chiave nel dizionario "Specially Designated National List".

Tabella 41-58 Regola di rilevamento Specially Designated National List (SDN, lista nazionale specialmente designata) dell'OFAC e destinatari

Metodo	Condizione	Configurazione
Regola composta	Destinatario corrispondente a criterio (DCM)	<p>Specially Designated National List (SDN, lista nazionale specialmente designata) dell'OFAC e destinatari (destinatario):</p> <ul style="list-style-type: none"> ■ Cercare la corrispondenza dell'e-mail o del dominio URL in base al codice di paese SDN OFAC. ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Almeno 1 destinatario deve corrispondere. ■ Cercare la corrispondenza con l'intero messaggio.
	Contenuto corrispondente a parola chiave (DCM)	<p>Specially Designated National List (corrispondenza di parola chiave):</p> <ul style="list-style-type: none"> ■ Cercare la corrispondenza della parola chiave in base allo Specially Designated National List. ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Cercare la corrispondenza solo con parole intere.

La regola di rilevamento Comunicazioni ai paesi dell'OFAC cerca un destinatario con un codice di paese che corrisponde alle voci dell'elenco "Codici di paese OFAC".

Tabella 41-59 Regola di rilevamento Comunicazioni ai paesi dell'OFAC

Metodo	Condizione	Configurazione
Regola semplice	Destinatario corrispondente a criterio (DCM)	<p>Comunicazioni ai paesi dell'OFAC (destinatario):</p> <ul style="list-style-type: none"> ■ Cercare la corrispondenza dell'e-mail o del dominio URL in base al codice di paese OFAC. ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Almeno 1 destinatario deve corrispondere. ■ Cercare la corrispondenza con l'intero messaggio.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Memorandum OMB 06-16 e disposizioni FIPS 199

Questa politica rileva le informazioni classificate come riservate in conformità alle linee guida stabilite dalla pubblicazione 199 dei Federal Information Processing Standards (FIPS) da parte del National Institute of Standards and Technology (NIST). NIST è responsabile della definizione di standard e linee guida per la protezione dei dati in base alle disposizioni del Federal Information Security Management Act (FISMA).

Questo modello contiene tre regole di rilevamento semplici. Se una delle regole segnala una corrispondenza, la politica attiva un incidente.

La regola di rilevamento Indicatori livello di riservatezza elevato cerca le parole chiave nel dizionario "Livello di riservatezza elevato".

Tabella 41-60 Regola di rilevamento Indicatori livello di riservatezza elevato

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave	Indicatori livello di riservatezza elevato (Corrispondenza parole chiave): <ul style="list-style-type: none"> ■ Corrispondenza "(riservatezza, alta)", "(riservatezza,alta)" ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

La regola di rilevamento Indicatori livello di riservatezza moderato cerca le parole chiave nel dizionario "Livello di riservatezza moderato".

Tabella 41-61 Regola di rilevamento Indicatori livello di riservatezza moderato

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave	Indicatori livello di riservatezza moderato (Corrispondenza parole chiave): <ul style="list-style-type: none"> ■ Corrispondenza "(riservatezza, moderato)", "(riservatezza,moderato)" ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

La regola di rilevamento Indicatori livello di riservatezza basso cerca le parole chiave nel dizionario "Livello di riservatezza basso".

Tabella 41-62 Regola di rilevamento Indicatori livello di riservatezza basso

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave	Indicatori livello di riservatezza basso (Corrispondenza parole chiave): <ul style="list-style-type: none"> ■ Corrispondenza "(riservatezza, basso)", "(riservatezza,basso)" ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica File di password

La politica File di password rileva formati di file di password quali SAM, password e shadow.

Regola DCM **Nome file password**

Questa regola cerca i nomi file "passwd" or "shadow".

Regola DCM **Formato /etc/passwd**

Questa regola cerca un formato di espressione regolare con formato /etc/passwd.

Regola DCM **Formato /etc/shadow**

Questa regola cerca un formato di espressione regolare con formato /etc/shadow.

Regola DCM **Password SAM**

Questa regola cerca un formato di espressione regolare con formato SAM.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Payment Card Industry (PCI) Data Security Standard

Gli standard di sicurezza dei dati Payment Card Industry (PCI) sono definiti di comune accordo dai circuiti Visa o Mastercard per proteggere le informazioni che consentono l'identificazione dei titolari di carte. Il programma di sicurezza delle informazioni (CISP) dei titolari di carte Visa

e il programma Data Protection del sito dei titolari di carte Mastercard cooperano per l'applicazione di questi standard. La politica Payment Card Industry (PCI) Data Security Standards rileva i dati del numero di carta di credito dei circuiti Mastercard e Visa.

La regola di rilevamento Numeri di carta, Esatti individua i numeri di carta di credito esatti contenuti in un database o in un'origine dati diversa.

Tabella 41-63 Regola di rilevamento Numeri di carta di credito, esatti

Metodo	Condizione	Configurazione
Regola semplice	Il contenuto corrisponde ai dati esatti (EDM)	Questa regola rileva i numeri di carta di credito. Vedere "Scelta di un profilo dati esatti" a pagina 417.

La regola di rilevamento Numeri di carta di credito, tutti rileva i numeri di carta di credito mediante l'identificatore dati di sistema Numero carta di credito.

Tabella 41-64 Regola di rilevamento Numeri di carta di credito, tutti

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a identificatore dati (DCM)	Numeri di carta di credito, tutti (Identificatori dati): <ul style="list-style-type: none"> ■ Identificatore dati: Numero carta di credito (limitato) Vedere "Numero carta di credito" a pagina 993. ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati.

La regola di rilevamento Dati banda magnetica per carte di credito rileva i dati non elaborati della banda magnetica della carta di credito mediante l'identificatore dati del sistema della banda magnetica stessa.

Tabella 41-65 Regola di rilevamento Dati banda magnetica per carte di credito

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a identificatore dati (DCM)	Dati banda magnetica per carte di credito (identificatori dati): <ul style="list-style-type: none"> ■ Identificatore dati: banda magnetica carta di credito (media) Vedere "Numero carta di credito" a pagina 993. ■ Gravità dati: alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica PIPEDA

Il Personal Information Protection and Electronic Documents Act (PIPEDA, legge sulla tutela delle informazioni personali e sui documenti elettronici) canadese protegge le informazioni personali nelle mani delle aziende del settore privato. Questo documento fornisce le linee guida per la raccolta, l'utilizzo e la divulgazione di informazioni personali.

La politica PIPEDA rileva i dati del cliente protetti dai regolamenti PIPEDA.

La regola di rilevamento PIPEDA cerca una corrispondenza di due elementi di dati con determinate combinazioni di dati escluse dalla corrispondenza.

Tabella 41-66 Regola di rilevamento PIPEDA

Metodo di rilevazione	Descrizione	Combinazioni escluse
Regola EDM	<p>La regola di rilevamento PIPEDA cerca la corrispondenza con due dei seguenti elementi di dati:</p> <ul style="list-style-type: none"> ■ Cognome ■ Carta di credito ■ Codice fiscale ■ Cartella clinica ■ Numero agenzia ■ Numero di conto ■ PIN ■ Nome utente ■ Password ■ SIN ■ Numero di routing ABA ■ E-mail ■ Telefono ■ Il cognome da nubile della madre <p>Vedere "Scelta di un profilo dati esatti" a pagina 417.</p>	<p>Tuttavia, le seguenti combinazioni non creano una corrispondenza:</p> <ul style="list-style-type: none"> ■ Cognome, e-mail ■ Cognome, telefono ■ Cognome, numero di conto ■ Cognome, nome utente

La regola di rilevamento PIPEDA, informazioni di contatto cerca una corrispondenza di due elementi di dati con determinate combinazioni di dati escluse dalla corrispondenza.

Tabella 41-67 Regola di rilevamento PIPEDA, informazioni di contatto

Metodo di rilevazione	Descrizione
Regola EDM	<p>Questa regola cerca due delle seguenti colonne di dati:</p> <ul style="list-style-type: none"> ■ Cognome ■ Telefono ■ Numero di conto ■ Nome utente ■ E-mail <p>Vedere "Scelta di un profilo dati esatti" a pagina 417.</p>

Tabella 41-68 Regola di rilevamento Numeri di previdenza sociale (SIN) canadesi

Metodo di rilevazione	Descrizione
Regola DCM	<p>Questa regola implementa l'edizione a copertura limitata dell'identificatore di dati del Social Insurance Number (numero di previdenza sociale) canadese</p> <p>Vedere "Social Insurance Number (numero di previdenza sociale) canadese" a pagina 971.</p>

Tabella 41-69 Regola di rilevamento Numeri di routing ABA

Metodo di rilevazione	Descrizione
Regola DCM	<p>Questa regola implementa l'edizione a copertura limitata dell'identificatore di dati del numero di routing ABA.</p> <p>Vedere "Numero di routing ABA" a pagina 918.</p>

Tabella 41-70 Regola di rilevamento Numeri di carta di credito, tutti

Metodo di rilevazione	Descrizione
Regola DCM	<p>Questa regola implementa l'edizione a copertura limitata dell'identificatore di dati del numero carta di credito.</p> <p>Vedere "Copertura limitata numero carta di credito" a pagina 997.</p>

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Informazioni sui prezzi

La politica Informazioni sui prezzi rileva le informazioni su SKU e prezzi specifiche a rischio di divulgazione.

Regola EDM

Informazioni sui prezzi

Questa regola cerca la corrispondenza fra i numeri SKU specificati dall'utente e il prezzo per quel numero SKU.

Nota: Questo modello contiene una regola di rilevamento EDM. Se il profilo EDM non è configurato o si sta utilizzando lo Standard Symantec Data Loss Prevention, questo modello di politica è vuoto e non contiene regole da configurare.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Modello della politica Dati di progetto

La politica Dati di progetto rileva le discussioni relative ai progetti riservati.

Regola IDM

Documenti di progetto, indicizzati

Questa regola cerca il contenuto nei file dati di progetto specifici registrati come proprietari. Restituisce una corrispondenza se il motore individua l'80% o più del documento originale.

Regola DCM

Attività di progetto

Questa regola cerca tutte le parole chiave nel dizionario "Nomi codici progetti riservati" definite dall'utente.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica File multimediali proprietari

La politica File multimediali proprietari rileva diversi tipi di file audio e video che possono essere di proprietà intellettuale dell'azienda e a rischio di violazione.

Regola IDM **File multimediali, indicizzati**

Questa regola cerca il contenuto nei file multimediali specifici registrati come proprietari.

Regola DCM **File multimediali**

Questa regola cerca i seguenti tipi di file multimediali:

- qt
- riff
- macromedia_dir
- midi
- mp3
- mpeg_movie
- quickdraw
- realaudio
- wav
- video_win
- vrmf

Regola DCM **Estensioni file multimediali**

Questa regola cerca le estensioni dei file dal dizionario "Estensioni file multimediali".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Documenti di pubblicazione

La politica Documenti di pubblicazione rileva diversi tipi di documenti di pubblicazione, quali i file Adobe FrameMaker, a rischio di divulgazione.

Regola IDM **Documenti di pubblicazione, indicizzati**

Questa regola cerca il contenuto in documenti di pubblicazione specifici registrati come proprietari. Restituisce una corrispondenza se il motore individua l'80% o più del documento originale.

Regola DCM **Documenti di pubblicazione**

Questa regola cerca i tipi di file specificati:

- qxpress
- frame
- aldus_pagemaker
- publ

Regola DCM

Documenti di pubblicazione, estensioni

Questa regola cerca specifiche estensioni di file trovate nel dizionario "Estensioni documento di pubblicazione".

Nota: Per questa politica è necessario specificare il tipo e l'estensione del file poiché il motore di rilevazione non individua il tipo di file effettivo per tutti i documenti richiesti. Pertanto, l'estensione del file deve essere usata insieme al tipo di file.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello politica Linguaggio razzista

La politica Linguaggio razzista rileva l'utilizzo di linguaggio razzista.

Regola DCM

Linguaggio razzista

Questa regola cerca qualsiasi parola chiave contenuta nel dizionario "Linguaggio razzista".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica File con restrizioni

La politica File con restrizioni rileva tipi di file generalmente inadatti alla divulgazione al di fuori dell'azienda, quali file di Microsoft Access e file eseguibili.

Regola DCM

File Microsoft Access ed eseguibili

Questa regola cerca i seguenti tipi di file: access, exe, and exe_unix.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Destinatari con restrizioni

La politica Destinatari con restrizioni individua le comunicazioni con i destinatari specificati, ad esempio quelle dirette agli ex dipendenti.

Regole DCM

Destinatari con restrizioni

Questa regola cerca i messaggi diretti ai destinatari con indirizzi e-mail nel dizionario "Destinatari con restrizioni".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Curriculum

La politica Curriculum individua le ricerche di lavoro attive.

Regola EDM

Curriculum, Dipendente

Questa regola è una regola composta con due condizioni; entrambe devono corrispondere per attivare un incidente. Questa regola contiene una condizione EDM per il nome e il cognome dei dipendenti forniti dall'utente. Questa regola inoltre cerca un tipo di allegato specifico (.doc) che sia inferiore a 50 KB e che contenga almeno una parola chiave contenuta in ognuno dei seguenti dizionari:

- Parole chiave Ricerca di lavoro, Istruzione
- Parole chiave Ricerca di lavoro, Lavoro
- Parole chiave Ricerca di lavoro, Generale

Regola DCM

Curriculum, tutto

Questa regola cerca un tipo di file specifico (.doc) che sia inferiore a 50 KB e che corrisponda ad almeno una parola chiave contenuta in ognuno dei seguenti dizionari:

- Parole chiave Ricerca di lavoro, Istruzione
- Parole chiave Ricerca di lavoro, Lavoro
- Parole chiave Ricerca di lavoro, Generale

Regola DCM

Siti Web per la ricerca di lavoro

Questa regola cerca gli URL dei siti Web utilizzati nelle ricerche di lavoro.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Vedere ["Informazioni sul profilo dati esatti e sull'indice"](#) a pagina 478.

Modello della politica Sarbanes-Oxley

La normativa Sarbanes-Oxley Act (SOX) statunitense stabilisce i requisiti di contabilità, inclusa la conservazione dell'integrità dei dati e la capacità di creare un itinerario di controllo. La politica Sarbanes-Oxley rileva i dati finanziari riservati.

La regola di rilevamento Documenti Sarbanes-Oxley, indicizzati cerca il contenuto nei documenti specifici registrati conformi alla normativa Sarbanes-Oxley Act. Questa regola restituisce una corrispondenza se l'80% o più del documento originale viene trovato.

Tabella 41-71 Regola di rilevamento Documenti Sarbanes-Oxley, indicizzati

Metodo	Condizione	Configurazione
Regola semplice	Contenuti corrispondenti profilo documenti indicizzati	Vedere "Scelta di un profilo documento indicizzato" a pagina 419.

La regola composta di rilevamento Normativa sull'imparzialità della trasparenza SEC cerca le seguenti condizioni; tutte devono essere soddisfatte affinché la regola attivi un incidente:

- Le parole chiave Imparzialità della trasparenza SEC indicano la possibile divulgazione di informazioni finanziarie avanzate (dizionario "Parole chiave Imparzialità della trasparenza SEC").
- Un allegato o un tipo di file che sono documenti comunemente utilizzati o in formato foglio di calcolo. I tipi di file rilevati sono Microsoft Word, Excel Macro, Excel, Works Spreadsheet, SYLK Spreadsheet, Corel Quattro Pro, WordPerfect, Lotus 123, Applix Spreadsheets, CSV, Multiplan Spreadsheet e Adobe PDF.
- L'elenco delle parole chiave dell'azienda richiede la modifica da parte dell'utente. Può includere qualsiasi nome, un nome alternativo o un'abbreviazione che potrebbe indicare un riferimento alla società.

Tabella 41-72 Regola di rilevamento Normativa sull'imparzialità della trasparenza SEC

Metodo	Condizione	Configurazione
Regola composta	Contenuto corrispondente a parola chiave	<p>Normativa sull'imparzialità della trasparenza SEC (Corrispondenza parole chiave)</p> <ul style="list-style-type: none"> ■ Parola chiave corrispondenza: ricavi diluiti, orientamento ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere. ■ Corrispondenza sullo stesso componente. <p>La parola chiave deve essere contenuta nell'allegato o nel tipo di file rilevato dal quella condizione.</p>
	Corrispondenza allegato messaggio o tipo file	<p>Normativa sull'imparzialità della trasparenza SEC (Tipo di allegato/file)</p> <ul style="list-style-type: none"> ■ Tipo di file rilevato: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, wordperfect e pdf. ■ Gravità: Alta. ■ Corrispondenza in: allegati e stessi componenti.
	Contenuto corrispondente a parola chiave	<p>Normativa sull'imparzialità della trasparenza SEC (Corrispondenza parole chiave)</p> <ul style="list-style-type: none"> ■ Corrispondenza "[nome azienda]" ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere. ■ Corrispondenza sullo stesso componente. <p>La parola chiave deve essere contenuta nell'allegato o nel tipo di file rilevato dal quella condizione.</p>

La regola di rilevamento Informazioni finanziarie cerca un tipo di file specifico contenente una parola del dizionario "Parole chiave finanziarie" e una del dizionario "Parole confidenziali/private". I tipi di file foglio di calcolo rilevati sono Microsoft Excel Macro, Microsoft Excel, Microsoft Works Spreadsheet, SYLK Spreadsheet, Corel Quattro Pro e altri.

Tabella 41-73 Regola di rilevamento Informazioni finanziarie

Metodo	Condizione	Configurazione
Regola composta	Contenuti corrispondenti profilo documenti indicizzati	Informazioni finanziarie (Tipo di allegato/file): <ul style="list-style-type: none"> ■ Corrispondenza tipo file: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, Lotus 1-2-3 ■ Gravità: Alta. ■ Corrispondenza in: allegati e stessi componenti.
	Contenuto corrispondente a parola chiave	Informazioni finanziarie (corrispondenza parola chiave): <ul style="list-style-type: none"> ■ Corrispondenza Abbini "turnover crediti verso clienti", "margine lordo regolato", "spese di gestione regolate", "margine operativo regolato", "spese amministrative" e così via. ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere. ■ La parola chiave deve essere rilevata nell'allegato (stesso componente).
	Contenuto corrispondente a parola chiave	Informazioni finanziarie (corrispondenza parola chiave): <ul style="list-style-type: none"> ■ Corrispondenza "confidenziale", "solo uso interno", "riservato". ■ Gravità: Alta. ■ Verificare esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere. ■ La parola chiave deve essere rilevata nell'allegato (stesso componente).

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Normativa sull'imparzialità della trasparenza SEC

La normativa statunitense Selective Disclosure and Insider Trading Act di SEC vieta alle società ad azionariato diffuso di rivelare selettivamente informazioni materiali ad analisti e investitori istituzionali prima che vengano divulgate pubblicamente.

Il modello Normativa sull'imparzialità della trasparenza SEC rileva i dati indicanti la divulgazione di informazioni finanziarie materiali.

La regola di rilevamento Normativa sull'imparzialità della trasparenza SEC (IDM) cerca il contenuto in documenti specifici conformi alla normativa sull'imparzialità della trasparenza. Questa regola restituisce una corrispondenza se l'80% o più del contenuto del documento originale viene trovato.

Tabella 41-74 Regola di rilevamento Documenti della normativa sull'imparzialità della trasparenza SEC, indicizzati (IDM)

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a firma documento (IDM)	<p>Documenti della normativa sull'imparzialità della trasparenza SEC, indicizzati (IDM):</p> <ul style="list-style-type: none"> ■ Rilevare i documenti dal profilo documento indicizzato selezionato. Vedere "Scelta di un profilo documento indicizzato" a pagina 419. ■ Far corrispondere i documenti con almeno l'80% del contenuto. ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Cercare in corpo, allegati.

La regola di rilevamento Normativa sull'imparzialità della trasparenza SEC cerca la parola chiave corrispondente dal dizionario "Parole chiave imparzialità della trasparenza SEC", un allegato o un tipo di file che sono un documento o un foglio elettronico comunemente utilizzati e una parola chiave corrispondente dal dizionario "Parole chiave nome società".

Tutte e tre le condizioni devono essere soddisfatte affinché la regola attivi un incidente:

- Le parole chiave Imparzialità della trasparenza SEC indicano la possibile divulgazione di informazioni finanziarie avanzate.
- I tipi di file rilevati sono Microsoft Word, Excel Macro, Excel, Works Spreadsheet, SYLK Spreadsheet, Corel Quattro Pro, WordPerfect, Lotus 123, Applix Spreadsheets, CSV, Multiplan Spreadsheet e Adobe PDF.
- L'elenco delle parole chiave dell'azienda richiede la modifica da parte dell'utente. Può includere qualsiasi nome, un nome alternativo o un'abbreviazione che potrebbe indicare un riferimento alla società.

Tabella 41-75 Regola di rilevamento Normativa sull'imparzialità della trasparenza SEC

Metodo	Condizione	Configurazione
Regola composta	Contenuto corrispondente a parola chiave (DCM)	<p>Normativa sull'imparzialità della trasparenza SEC (Corrispondenza parole chiave):</p> <ul style="list-style-type: none"> ■ Corrispondenza "ricavi diluiti", "orientamento" ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Cerca in busta, oggetto, corpo, allegati. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.
	Corrispondenza allegato messaggio o tipo file (DCM)	<p>Normativa sull'imparzialità della trasparenza SEC (Tipo di allegato/file)</p> <ul style="list-style-type: none"> ■ Corrispondenza tipo file: excel_macro, xls, works_spread, sylk, quattro_pro, mod, csv, applix_spread, 123, doc, wordperfect, pdf ■ Gravità: Alta. ■ Corrispondenza negli allegati. ■ Richiede che il contenuto corrispondente si trovi nello stesso componente (allegato).
	Contenuto corrispondente a parola chiave (DCM)	<p>Normativa sull'imparzialità della trasparenza SEC (Corrispondenza parole chiave):</p> <ul style="list-style-type: none"> ■ Corrispondenza "[nome azienda]" (definito dall'utente) ■ Gravità: Alta. ■ Verificare l'esistenza. ■ Cercare in busta, oggetto, corpo, allegati e stesso componente. ■ Senza distinzione maiuscole/minuscole. ■ Crea corrispondenza solo con parole intere.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Linguaggio sessualmente esplicito

La politica Linguaggio sessualmente esplicito rileva contenuto dal linguaggio volgare, sessualmente esplicito e pornografico.

Regola DCM

Parole chiave sessualmente esplicite, confermate

Questa regola cerca una parola chiave contenuta nel dizionario "Parole chiave sessualmente esplicite, confermate".

Regola DCM **Parole chiave sessualmente esplicite, sospette**
Questa regola cerca tre istanze delle parole chiave nel dizionario "Parole sessualmente esplicite, sospette".

Regola DCM **Parole chiave sessualmente esplicite, possibili**
Questa regola cerca tre istanze delle parole chiave nel dizionario "Parole sessualmente esplicite, possibili".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Codice sorgente

Il modello della politica Codice sorgente fornisce i termini di corrispondenza per il rilevamento dei vari tipi di codici sorgente a rischio di divulgazione tra cui C, Java, Perl e Visual Basic (VB).

Tabella 41-76 Condizioni di corrispondenza modello di politica Codice sorgente

Nome	Tipo	Descrizione
Documenti Codice sorgente	IDM	Questa regola ricerca il codice sorgente fornito dall'utente in un Profilo documento . Questa regola restituisce una corrispondenza se rileva l'80% o più del documento sorgente. Questa regola non è disponibile se non si seleziona un profilo durante la creazione di una politica.
Estensioni codice sorgente	Corrispondenza nome file	Questa regola cerca la corrispondenza tra le estensioni dei nomi di file dal dizionario "Estensioni codice sorgente".
Codice sorgente Java	Espressioni regolari	Questa regola composta cerca le corrispondenze su due modelli diversi di espressione regolare: istruzioni di importazione di Java e file di classe di Java.
Codice sorgente C	Espressione regolare	Questa regola cerca le corrispondenze nel modello di espressione regolare Codice sorgente C.
Codice sorgente VB	Espressione regolare	Questa regola cerca le corrispondenze nel modello di espressione regolare Codice sorgente VB.
Codice sorgente Perl	Espressioni regolari	Questa regola composta cerca le corrispondenze su tre modelli differenti di espressioni regolari relativi a Perl.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di privacy dei dati relativi allo stato

Molti stati degli Stati Uniti hanno adottato statuti che richiedono la protezione dei dati e la divulgazione pubblica dei casi di violazione della sicurezza delle informazioni, che compromettono la riservatezza dei dati personali dei singoli. Il modello della politica Privacy dei dati relativi allo stato è pensato per questi tipi di violazioni dei dati confidenziali.

Il modello della politica **Privacy dei dati relativi allo stato** fornisce diverse regole di rilevamento e genera un incidente nel caso queste venissero violate. Questo modello della politica fornisce anche una condizione di eccezione configurabile che consente a uno o più destinatari e-mail autorizzati di ricevere altrimenti dati riservati.

[Tabella 41-77](#) descrive la condizione di utilizzo accettabile implementata dalla politica Privacy dei dati relativi allo stato. Per applicare l'eccezione, è necessario configurarla.

Tabella 41-77 Eccezione alla politica E-mail alle affiliate

Nome	Tipo	Descrizione	Dettagli di configurazione
E-mail alle affiliate (destinatario)	Identità descritta (DCM) Destinatario corrispondente a criterio	<p>E-mail alle affiliate è un'eccezione della politica che consente di inviare messaggi di posta elettronica alle affiliate autorizzate a ricevere le informazioni coperte dalle normative della privacy dei dati relativi allo stato.</p> <p>Le eccezioni della politica vengono valutate prima delle condizioni di corrispondenza del rilevamento. In caso di eccezione, come ad esempio un indirizzo e-mail dell'affiliata inserito dall'utente, l'intero messaggio viene ignorato e reso non disponibile per la valutazione tramite rilevamento.</p>	<ul style="list-style-type: none">■ Eccezione semplice (condizione singola)■ Corrispondenza del destinatario dell'e-mail: [affiliata1], [affiliata2].■ Modificare l'elenco "Domini affiliate" e inserire l'indirizzo e-mail di ogni destinatario idoneo all'utilizzo di dati riservati.■ Per attivare l'eccezione è necessario che almeno 1 destinatario corrisponda.■ Corrispondenze sull'intero messaggio.

Il modello Privacy dei dati relativi allo stato implementa Exact Data Matching ([Tabella 41-78](#)). Se non si seleziona un profilo **Dati esatti** durante la creazione di una politica basata su questo modello, non sarà possibile utilizzare lo stato EDM.

Vedere ["Scelta di un profilo dati esatti"](#) a pagina 417.

Tabella 41-78 Regola EDM Privacy dei dati relativi allo stato

Nome regola	Tipo condizione	Descrizione	Dettagli di configurazione
Privacy dei dati relativi allo stato, dati dei consumatori	Il contenuto corrisponde dati ai esatti (EDM)	<p>Questa regola ricerca la corrispondenza esatta di dati in tre dei seguenti elementi:</p> <ul style="list-style-type: none"> ■ Numero di routing ABA ■ Numero di conto ■ Numero di carta di credito ■ Data di nascita ■ Numero di patente di guida ■ Nome ■ Cognome ■ Password ■ Numero PIN ■ Numero di codice fiscale ■ Numero di carta d'identità <p>Condizioni di eccezione - Le seguenti combinazioni non corrispondono:</p> <ul style="list-style-type: none"> ■ Nome, Cognome, PIN ■ Nome, Cognome, Password 	<p>Durante la creazione del profilo EDM, è necessario convalidarlo rispetto al modello Privacy dei dati relativi allo stato per assicurarsi che l'indice risultante includa i campi previsti.</p> <ul style="list-style-type: none"> ■ Regola semplice (condizione della corrispondenza singola) ■ Gravità: Alta ■ Segnalare l'incidente nel caso di 1 corrispondenza ■ Cerca in busta, corpo e allegati

Tabella 41-79 elenca e descrive le regole di rilevamento DCM implementate dalla politica Privacy dei dati relativi stato. Se una qualsiasi di queste regole viene violata, la politica genera un incidente a meno che la condizione di eccezione non sia stata configurata e il destinatario del messaggio non sia un'affiliata autorizzata all'utilizzo.

Tabella 41-79 Regole di rilevamento Privacy dei dati relativi allo stato

Nome regola	Tipo condizione	Descrizione	Dettagli di configurazione
Formati Social Security Number (codice fiscale) statunitense	Contenuto corrispondente a identificatore dati (DCM)	<p>La regola Formati Social Security Number (codice fiscale) statunitense è pensata per individuare i numeri di previdenza sociale (SSN) degli Stati Uniti. Identificatore dati SSN degli Stati Uniti randomizzato individua i formati SSN, sia quelli tradizionali sia quelli pubblicati nel nuovo schema di sequenza casuale.</p> <p>Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218.</p>	<ul style="list-style-type: none"> ■ Regola semplice (condizione della corrispondenza singola) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati.

Nome regola	Tipo condizione	Descrizione	Dettagli di configurazione
Numeri di routing ABA	Contenuto corrispondente a identificatore dati (DCM)	<p>La regola Numeri di routing ABA è pensata per individuare i numeri routing ABA.</p> <p>L'identificatore di dati di numeri di routing di ABA individua i numeri di routing di ABA.</p> <p>Vedere "Numero di routing ABA" a pagina 918.</p>	<ul style="list-style-type: none"> ■ Regola semplice (condizione della corrispondenza singola) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati.
Numeri di carta di credito, tutti	Contenuto corrispondente a identificatore dati (DCM)	<p>La regola Numeri di carta di credito è pensata per cercare la corrispondenza con i numeri di carta di credito.</p> <p>Per individuare numeri di carta di credito, questa regola implementa la versione a copertura limitata dell'identificatore dati di sistema del numero di carta di credito.</p> <p>Vedere "Copertura limitata numero carta di credito" a pagina 997.</p>	<ul style="list-style-type: none"> ■ Regola semplice (condizione singola) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati
Numeri delle patenti di guida della California	Contenuto corrispondente a identificatore dati (DCM)	<p>La regola Numeri delle patenti di guida della California cerca la corrispondenza per il formato del numero di patenti di guida della California, la corrispondenza per l'identificatore dati per i termini correlati a "patenti di guida" e una parola chiave dal dizionario "Parole chiave della California".</p> <p>Vedere "Numero patente di guida - Stato della California" a pagina 1015.</p>	<ul style="list-style-type: none"> ■ Regola semplice (condizione singola) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati
Numeri delle patenti di guida dello Stato di New York	Contenuto corrispondente a identificatore dati (DCM)	<p>La regola Numeri delle patenti di guida dello Stato di New York cerca la corrispondenza per il formato del numero di patenti di guida dello Stato di New York, la corrispondenza per l'espressione regolare per i termini correlati a "patenti di guida" e una parola chiave dal dizionario "Parole chiave dello Stato di New York".</p> <p>Vedere "Numero patente di guida - Stato di New York" a pagina 1021.</p>	<ul style="list-style-type: none"> ■ Regola semplice (condizione singola) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati

Nome regola	Tipo condizione	Descrizione	Dettagli di configurazione
Numeri delle patenti di guida di Florida, Michigan e Minnesota	Contenuto corrispondente a identificatore dati (DCM)	<p>La regola Numeri delle patenti di guida di Florida, Michigan e Minnesota cerca la corrispondenza per il formato del numero di patenti di guida degli stati, la corrispondenza per l'espressione regolare per i termini correlati a "patenti di guida" e una parola chiave dal dizionario "Parole stato DLN lettere/12 num" (ossia, Florida, Minnesota e Michigan).</p> <p>Vedere "Numero di patente di guida - Stati della Florida, del Michigan e del Minnesota" a pagina 1016.</p>	<ul style="list-style-type: none"> ■ Regola semplice (condizione singola) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati
Numeri delle patenti di guida dell'Illinois	Contenuto corrispondente a identificatore dati (DCM)	<p>La regola di rilevamento Numeri delle patenti di guida dell'Illinois cerca la corrispondenza per il formato del numero di patenti di guida dell'Illinois, la corrispondenza per l'espressione regolare per i termini correlati a "patenti di guida" e una parola chiave dal dizionario "parole chiave dell'Illinois".</p> <p>Vedere "Numero patente di guida - Stato dell'Illinois" a pagina 1018.</p>	<ul style="list-style-type: none"> ■ Regola semplice (condizione singola) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati
Numeri delle patenti di guida del New Jersey	Contenuto corrispondente a identificatore dati (DCM)	<p>La regola Numeri delle patenti di guida del New Jersey cerca la corrispondenza per il formato del numero di patenti di guida del New Jersey, la corrispondenza per l'espressione regolare per i termini correlati a "patenti di guida" e una parola chiave dal dizionario "Parole chiave del New Jersey".</p> <p>Questa condizione implementa la versione a copertura media dell'identificatore dati di sistema del Numero patente di guida - Stato del New Jersey</p> <p>Vedere "Copertura media numero patente di guida - Stato del New Jersey" a pagina 1020.</p>	<ul style="list-style-type: none"> ■ Regola semplice (condizione singola) ■ Gravità: Alta. ■ Contare tutte le corrispondenze. ■ Cerca in busta, oggetto, corpo e allegati

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Codici SWIFT

La Society for Worldwide Interbank Financial Telecommunication (SWIFT - Società per le Telecomunicazioni Finanziarie Interbancarie Mondiali) è una società cooperativa con sede legale in Belgio di proprietà delle istituzioni finanziarie che ne fanno parte. Il codice SWIFT (detto anche codice BIC - Bank Identifier Code o ISO 9362) è in un formato standard e consente di identificare una banca, la sua posizione e la filiale interessata. Questi codici vengono utilizzati per i trasferimenti di denaro tra banche, specialmente nelle transazioni internazionali.

Regola DCM

Espressione regolare Codice SWIFT

Questa regola ricerca una corrispondenza con l'espressione regolare Codice SWIFT e una parola chiave dal dizionario "Parole chiave Codice SWIFT".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Compatibilità Symantec DLP e Prevenzione

La politica Compatibilità Symantec DLP e Prevenzione rileva le comunicazioni relative a sistemi di Symantec Data Loss Prevention o di prevenzione della perdita di dati e a un'eventuale prevenzione del rilevamento. La politica Compatibilità Symantec DLP e Prevenzione è particolarmente utile per le distribuzioni poco conosciute dagli utenti monitorati.

Regola DCM

Compatibilità Symantec DLP

Cerca la corrispondenza con una parola chiave nel dizionario "Compatibilità Symantec DLP".

Regola DCM

Prevenzione Symantec DLP

Questa regola è una regola composta con due condizioni; entrambe devono corrispondere per attivare un incidente. Questa regola cerca la corrispondenza con una parola chiave nel dizionario "Compatibilità Symantec DLP" e una parola chiave nel dizionario "Prevenzione Symantec DLP".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Numeri Patente di guida del Regno Unito

La politica Numeri Patente di guida del Regno Unito rileva i numeri delle patenti di guida britanniche utilizzando la specifica ufficiale degli standard governativi dell'Ufficio del Gabinetto del Regno Unito.

Regola DCM

Numeri Patente di guida del Regno Unito

Questa regola è una regola composta con le seguenti condizioni:

- Una parola chiave singola del dizionario "Parole chiave Regno Unito"
- Il modello corrispondente a quello dell'identificatore di dati della patente di guida del Regno Unito
- Combinazioni diverse della frase "patente di guida" tramite un identificatore di dati

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello politica Numeri di tessera elettorale britannici

La politica Numeri di tessera elettorale britannici rileva i numeri di tessera elettorale britannici utilizzando la specifica ufficiale degli standard governativi dell'Ufficio del Gabinetto del Regno Unito.

Regola DCM

Numeri di tessera elettorale britannici

Questa regola è una regola composta con le seguenti condizioni:

- Una parola chiave singola del dizionario "Parole chiave Regno Unito"
- Un formato che corrisponde all'identificatore dati Numero di tessera elettorale britannico
- Una parola chiave singola del dizionario "Parole Numero di tessera elettorale britannico"

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Numero NHS (National Health Service) britannico

La politica Numero NHS (National Health Service) britannico rileva il numero di identificazione personale rilasciato dal National Health Service (NHS, sistema sanitario nazionale) britannico per la gestione dell'assistenza medica.

Regola DCM

Numeri NHS britannici

Questa regola cerca una singola condizione composta da due parti: i numeri NHS nuovi o vecchi e una parola chiave dal dizionario "Parole chiave NHS britannici".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Numeri di previdenza sociale britannici

Il numero di previdenza sociale viene rilasciato dal Department for Work and Pensions and Inland Revenue (DWP/IR) del Regno Unito per l'amministrazione del sistema previdenziale nazionale. La politica Numeri di previdenza sociale britannici rileva questi numeri di previdenza della politica.

Regola DCM

Numeri di previdenza sociale britannici

Questa regola ricerca una corrispondenza con l'identificatore dati del numero previdenza sociale britannico e una parola chiave dal dizionario "Numeri di previdenza sociale britannici".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Numeri di passaporto britannici

La politica Numeri di passaporto britannici rileva i passaporti britannici validi utilizzando la specifica ufficiale degli standard governativi dell'Ufficio del Gabinetto del Regno Unito.

Regola DCM

Numeri di passaporto britannici (tipo vecchio)

Questa regola cerca una parola chiave dal dizionario "Parole chiave passaporti britannici" e un modello corrispondente con l'espressione regolare per i Numeri di passaporto britannici (tipo vecchio).

Regola DCM

Numeri di passaporto britannici (tipo nuovo)

Questa regola cerca una parola chiave dal dizionario "Parole chiave passaporti britannici" e un modello corrispondente con l'espressione regolare per i Numeri di passaporto britannici (tipo nuovo).

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Codici fiscali britannici

La politica Codici fiscali britannici rileva i Codici fiscali britannici utilizzando la specifica ufficiale degli standard governativi dell'Ufficio del Gabinetto del Regno Unito.

Regola DCM

Codici fiscali britannici

Questa regola ricerca una corrispondenza con l'identificatore dati del Codice fiscale britannico e una parola chiave dal dizionario "Parole chiave Codici fiscali britannici".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Marchi di controllo dei servizi di intelligence degli Stati Uniti (CAPCO) e modello della politica DCID 1/7

La politica Marchi di controllo dei servizi di intelligence degli Stati Uniti (CAPCO) e DCID 1/7 rileva i termini autorizzati per l'identificazione delle informazioni classificate all'interno della United States Intelligence Community, come definito nel registro dei marchi di controllo tenuto dal CAPCO (Controlled Access Program Coordination Office) del CMS (Community Management Staff). Il registro è stato redatto in risposta alla direttiva DCID (Director of Central Intelligence Directive) 1/7.

Questa regola cerca una corrispondenza con la parola chiave nella frase "TOP SECRET".

Tabella 41-80 Regola di rilevamento Informazioni top secret

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave (DCM)	Corrispondenza "TOP-SECRET//" <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare esistenza. ■ Eseguire la ricerca in busta, oggetto, corpo e allegati. ■ Distinzione maiuscole/minuscole. ■ Crea corrispondenza con parole intere o parziali.

Questa regola cerca una corrispondenza con la parola chiave nella frase "SECRET".

Tabella 41-81 Regola di rilevamento Informazioni segrete

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave (DCM)	Corrispondenza "SEGRETO//" <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare esistenza. ■ Eseguire la ricerca in busta, oggetto, corpo e allegati. ■ Distinzione maiuscole/minuscole. ■ Crea corrispondenza con parole intere o parziali.

Questa regola cerca una corrispondenza con la parola chiave nella frase "CLASSIFICATO" o "RISERVATO".

Tabella 41-82 Regola di rilevamento Informazioni classificate o riservate (Corrispondenza parole chiave)

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave (DCM)	Corrispondenza "CLASSIFICATO//, //RISERVATO//" <ul style="list-style-type: none"> ■ Gravità: Alta. ■ Verificare esistenza. ■ Eseguire la ricerca in busta, oggetto, corpo e allegati. ■ Distinzione maiuscole/minuscole. ■ Crea corrispondenza con parole intere o parziali.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Social Security Number statunitense

La politica Social Security Number statunitense rileva i formati indicanti i Social Security Number a rischio di divulgazione.

Tabella 41-83 Modello di politica Social Security Number statunitense

Nome regola	Tipo regola	Descrizione	Dettagli
Formati Social Security Number (codice fiscale) statunitense	Regola DCM	Questa regola ricerca una corrispondenza con l'espressione regolare Social Security Number e una parola chiave dal dizionario "Parole chiave SSN statunitensi".	Vedere "Social Security Number (SSN) statunitense randomizzato" a pagina 1218.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica Violenza e armi

La politica Violenza e armi rileva linguaggio violento e discussioni in merito alle armi.

Tabella 41-84 Modello della politica Violenza e armi

Nome	Tipo	Descrizione
Violenza e armi	Regola DCM	Questa regola è una regola composta con due condizioni; entrambe devono corrispondere per attivare un incidente. Questa regola cerca una parola chiave dal dizionario "Parole chiave violenza" e una parola chiave dal dizionario "Parole chiave armi".

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello della politica di Webmail

La politica di Webmail rileva l'utilizzo di vari servizi Webmail tra cui Yahoo, Google e Hotmail.

Tabella 41-85 Regole del modello della politica di Webmail

Nome	Tipo	Condizioni	Descrizione
Yahoo	Regola di rilevamento composta	Destinatario corrispondente a criterio (DCM)	Questa condizione cerca il dominio URL mail.yahoo.com .
		Contenuto corrispondente a parola chiave (DCM)	Questa condizione cerca la parola chiave ym/compose .
Hotmail	Regola di rilevamento composta	Destinatario corrispondente a criterio (DCM)	Questa condizione cerca il dominio URL hotmail.msn.com .
		Contenuto corrispondente a parola chiave (DCM)	Questa condizione cerca la parola chiave compose?&curmbox .
Vai	Regola di rilevamento composta	Destinatario corrispondente a criterio (DCM)	Questa condizione cerca l'URL gmailus.go.com .
		Contenuto corrispondente a parola chiave (DCM)	Questa condizione cerca la parola chiave compose .
AOL	Regola di rilevamento composta	Destinatario corrispondente a criterio (DCM)	Questa condizione cerca il dominio URL aol.com .
		Contenuto corrispondente a parola chiave (DCM)	Questa condizione cerca la parola chiave compose .
Gmail	Regola di rilevamento composta	Destinatario corrispondente a criterio (DCM)	Questa condizione cerca il dominio URL gmail.google.com .
		Contenuto corrispondente a parola chiave (DCM)	Questa condizione cerca la parola chiave gmail .

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Attività della bacheca messaggi di Yahoo

Il modello della politica Bacheca messaggi di Yahoo rileva l'attività della bacheca messaggi di Yahoo.

La regola di rilevamento della bacheca messaggi di Yahoo è un metodo composto che cerca i messaggi pubblicati sulla bacheca messaggi di Yahoo specificata.

[Tabella 41-86](#) descrive i relativi dettagli di configurazione.

Tabella 41-86 Regola di rilevamento della bacheca messaggi di Yahoo

Metodo	Condizione	Configurazione
Regola composta	Contenuto corrispondente a parola chiave (DCM)	Bacheca messaggi di Yahoo (Corrispondenza parole chiave): <ul style="list-style-type: none"> ■ Senza distinzione maiuscole/minuscole. ■ Corrispondenza con parola chiave: post.messages.yahoo.com/bbs. ■ Crea corrispondenza solo con parole intere. ■ Verifica esistenza (non contare le corrispondenze multiple). ■ Cerca in busta, oggetto, corpo e allegati. ■ La corrispondenza deve verificarsi nella stessa componente per entrambe le condizioni.
	AND	
	Contenuto corrispondente a parola chiave (DCM)	Bacheca messaggi di Yahoo (Corrispondenza parole chiave): <ul style="list-style-type: none"> ■ Senza distinzione maiuscole/minuscole. ■ Corrispondenza con parola chiave: bacheca=<inserire numero bacheca>. ■ Crea corrispondenza solo con parole intere. ■ Verifica esistenza (non contare le corrispondenze multiple). ■ Cerca in busta, oggetto, corpo e allegati. ■ La corrispondenza deve verificarsi nella stessa componente per entrambe le condizioni.

La regola di rilevamento URL bacheca messaggi finanza rileva i messaggi pubblicati sulla bacheca messaggi di Yahoo Finanza.

[Tabella 41-87](#) descrive la relativa configurazione.

Tabella 41-87 Regola di rilevamento URL bacheca messaggi finanza

Metodo	Condizione	Configurazione
Regola semplice	Contenuto corrispondente a parola chiave (DCM)	URL bacheca messaggi finanza (corrispondenza con parole chiave): <ul style="list-style-type: none"> ■ Senza distinzione maiuscole/minuscole. ■ Corrispondenza con parola chiave: messages.finance.yahoo.com. ■ Crea corrispondenza solo con parole intere. ■ Verifica esistenza (non contare le corrispondenze multiple). ■ Cerca in busta, oggetto, corpo e allegati.

La regola di rilevamento URL bacheca rileva i messaggi pubblicati sulla bacheca messaggi di Yahoo o Yahoo Finanza dall'URL di una di esse.

[Tabella 41-88](#) descrive i relativi dettagli di configurazione.

Tabella 41-88 Regola di rilevamento URL bacheca

Metodo	Condizione	Configurazione
Regola semplice	Destinatario corrispondente a criterio (DCM)	URL bacheca (destinatario): <ul style="list-style-type: none"> ■ URL destinatario:messages.yahoo.com,messages.finance.yahoo.com. ■ È necessario che almeno 1 destinatario corrisponda. ■ Corrispondenze sull'intero messaggio (non configurabile).

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Modello di politica Yahoo e MSN Messenger sulla porta 80

La politica Yahoo e MSN Messenger sulla porta 80 rileva l'attività di Yahoo e MSN Messenger sulla porta 80.

La regola di rilevamento di Yahoo IM cerca le corrispondenze di parole chiave sia su ymsg sia su shttp.msg.yahoo.com.

Tabella 41-89 Regola di rilevamento di Yahoo IM

Metodo	Condizione	Configurazione
Regola composta	Contenuto corrispondente a parola chiave (DCM)	<p>Yahoo IM (corrispondenza parole chiave):</p> <ul style="list-style-type: none"> ■ Senza distinzione maiuscole/minuscole. ■ Corrispondenza con parola chiave: ymsg. ■ Crea corrispondenza solo con parole intere. ■ Conta tutte le corrispondenze e segnala gli eventuali incidenti per ciascuna corrispondenza. ■ Cerca le corrispondenze in busta, oggetto, corpo e allegati. ■ La corrispondenza deve verificarsi nella stessa componente per entrambe le condizioni della regola.
	AND	
	Contenuto corrispondente a parola chiave (DCM)	<p>Yahoo IM (corrispondenza parole chiave):</p> <ul style="list-style-type: none"> ■ Senza distinzione maiuscole/minuscole. ■ Corrispondenza con parola chiave: shttp.msg.yahoo.com. ■ Crea corrispondenza solo con parole intere. ■ Conta tutte le corrispondenze e segnala gli eventuali incidenti per ciascuna corrispondenza. ■ Cerca le corrispondenze in busta, oggetto, corpo e allegati. ■ La corrispondenza deve verificarsi nella stessa componente per entrambe le condizioni della regola.

La regola di rilevamento MSN IM cerca le corrispondenze su tre parole chiave nello stesso componente del messaggio.

Tabella 41-90 Regola di rilevamento MSN IM

Metodo	Condizione	Configurazione
Regola composta	Contenuto corrispondente a parola chiave (DCM)	<p>MSN IM (corrispondenza con parole chiave):</p> <ul style="list-style-type: none"> ■ Senza distinzione maiuscole/minuscole. ■ Corrispondenza con parola chiave: msg. ■ Crea corrispondenza solo con parole intere. ■ Conta tutte le corrispondenze e segnala gli eventuali incidenti per ciascuna corrispondenza. ■ Cerca le corrispondenze in busta, oggetto, corpo e allegati. ■ La corrispondenza deve verificarsi nella stessa componente per tutte le condizioni della regola.
	AND	
	Contenuto corrispondente a parola chiave (DCM)	<p>MSN IM (corrispondenza con parole chiave):</p> <ul style="list-style-type: none"> ■ Senza distinzione maiuscole/minuscole. ■ Corrispondenza con parola chiave: x-msn. ■ Crea corrispondenza solo con parole intere. ■ Conta tutte le corrispondenze e segnala gli eventuali incidenti per ciascuna corrispondenza. ■ Cerca le corrispondenze in busta, oggetto, corpo e allegati. ■ La corrispondenza deve verificarsi nella stessa componente per tutte le condizioni della regola.
	AND	
	Contenuto corrispondente a parola chiave (DCM)	<p>MSN IM (corrispondenza con parole chiave):</p> <ul style="list-style-type: none"> ■ Senza distinzione maiuscole/minuscole. ■ Corrispondenza con parole chiave: charset=utf-8. ■ Crea corrispondenza solo con parole intere. ■ Conta tutte le corrispondenze e segnala gli eventuali incidenti per ciascuna corrispondenza. ■ Cerca le corrispondenze in busta, oggetto, corpo e allegati. ■ La corrispondenza deve verificarsi nella stessa componente per tutte le condizioni della regola.

Vedere ["Creazione di una politica a partire da un modello"](#) a pagina 405.

Vedere ["Esportazione del rilevamento di politiche come modello"](#) a pagina 454.

Regole delle regola di risposta di politica

- [Capitolo 42. Risposta alle violazioni di politica](#)
- [Capitolo 43. Configurazione e gestione delle regole di risposta](#)
- [Capitolo 44. Condizioni di regole di risposta](#)
- [Capitolo 45. Azioni di regole di risposta](#)

Risposta alle violazioni di politica

Il capitolo contiene i seguenti argomenti:

- Informazioni sulle regole di risposta
- Informazioni sulle azioni di regola di risposta
- Azioni delle regole di risposta per tutti i server di rilevamento
- Azioni delle regole di risposta per il rilevamento di endpoint
- Azioni delle regole di risposta per il rilevamento di Network Prevent
- Azioni delle regole di risposta per il rilevamento di Network Protect
- Azioni di regole di risposta per rilevamento archiviazione cloud
- Azioni di regole di risposta per rilevatori Applicazioni cloud e dispositivo API
- Informazioni sui tipi di esecuzione delle regole di risposta
- Informazioni sulle regole di risposta automatica
- Informazioni sulle regole di risposta smart
- Informazioni sulle condizioni delle regole di risposta
- Informazioni sulla priorità di esecuzione delle azioni di regola di risposta
- Informazioni sui privilegi di creazione di regole di risposta
- Implementazione di regole di risposta
- Best practice per le regole di risposta

Informazioni sulle regole di risposta

È possibile implementare una o più regole di risposta in una politica per rimediare, riassegnare, risolvere e ignorare gli incidenti quando si ha una violazione. Ad esempio, se una politica viene violata, una regola di risposta blocca la trasmissione di un file che contiene contenuto riservato.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Le regole di risposta vengono create, modificate e gestite separatamente dalle politiche che le dichiarano. Ciò consente l'aggiornamento delle regole di risposta e il riutilizzo delle stesse nelle politiche.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Il server di rilevamento esegue automaticamente le regole di risposta. Oppure, è possibile configurare regole di risposta smart per l'esecuzione manuale da parte di un addetto alla riparazione di incidenti.

Vedere ["Informazioni sui tipi di esecuzione delle regole di risposta"](#) a pagina 1478.

È possibile implementare delle condizioni per controllare come e quando le regole di risposta vengono eseguite.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

È possibile definire l'ordine di esecuzione delle regole di risposta dello stesso tipo.

Vedere ["Informazioni sulla priorità di esecuzione delle azioni di regola di risposta"](#) a pagina 1481.

È necessario disporre di privilegi di creazione di regole di risposta per creare e gestire le regole di risposta.

Vedere ["Informazioni sui privilegi di creazione di regole di risposta"](#) a pagina 1485.

Informazioni sulle azioni di regola di risposta

Le azioni di regola di risposta sono le componenti che generano un'azione quando viene violata una politica. Le azioni di regola di risposta sono componenti obbligatorie delle regole di risposta. Se si crea una regola di risposta, è necessario definire almeno un'azione affinché la regola di risposta sia valida.

Symantec Data Loss Prevention fornisce varie azioni di regola di risposta. Molte sono disponibili per tutti i tipi di server di rilevamento. Altre sono disponibili per specifici server di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Il server di rilevamento in cui una politica è distribuita esegue un'azione di regola di risposta ogni volta che viene violata una politica. Oppure, è possibile configurare una condizione di regola di risposta per stabilire quando l'azione della regola di risposta viene eseguita.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Ad esempio, ogni volta che una politica è violata, inviare un'e-mail all'utente che ha violato la politica e al responsabile. Oppure, se il livello di gravità della violazione di una politica è medio, visualizzare un avviso sul computer dell'utente. Oppure, se la gravità è alta, bloccare la copia di un file su un dispositivo esterno.

Tabella 42-1 Azioni delle regole di risposta per tipo di server

Tipo di server	Descrizione
Tutti i server di rilevamento	Vedere "Azioni delle regole di risposta per tutti i server di rilevamento" a pagina 1469.
Server di rilevamento di endpoint	Vedere "Azioni delle regole di risposta per il rilevamento di endpoint" a pagina 1470.
Server di rilevamento di Network Prevent	Vedere "Azioni delle regole di risposta per il rilevamento di Network Prevent" a pagina 1471.
Server di rilevamento di Network Protect	Vedere "Azioni delle regole di risposta per il rilevamento di Network Protect" a pagina 1472.
Server di rilevamento dell'archiviazione cloud e rilevatori	Vedere "Azioni di regole di risposta per rilevamento archiviazione cloud" a pagina 1473.
Rilevatori REST connettore servizio cloud e Dispositivo Rilevamento API per le app degli sviluppatori	Vedere "Azioni di regole di risposta per rilevatori Applicazioni cloud e dispositivo API" a pagina 1474.

Azioni delle regole di risposta per tutti i server di rilevamento

Symantec Data Loss Prevention fornisce diverse azioni di regola di risposta per Endpoint Prevent, Endpoint Discover, Network Prevent for Web, Network Prevent for Email e Network Protect.

Tabella 42-2 Azioni delle regole di risposta disponibili per tutti i server di rilevamento

Azione delle regole di risposta	Descrizione
Aggiungi nota	Aggiunge un campo al record dell'incidente che l'addetto alle riparazioni può annotare nella schermata Istantanea incidente . Vedere "Configurazione dell'azione Aggiungi nota" a pagina 1510.
Limita conservazione dati incidenti	Scarta o conserva i dati corrispondenti con il record dell'incidente. Vedere "Configurazione dell'azione Limita conservazione dati incidenti" a pagina 1510.

Azione delle regole di risposta	Descrizione
Registrazione a un server Syslog	Registra l'incidente in un server Syslog. Vedere "Configurazione del registro a un'azione del server Syslog" a pagina 1513.
Invia notifica e-mail	Inviare un'e-mail ai destinatari specificati. Vedere "Configurazione dell'azione Invia notifica e-mail" a pagina 1514.
FlexResponse server	Eseguire un'azione FlexResponse server personalizzata. Vedere "Configurazione dell'azione di FlexResponse server" a pagina 1516. Nota: Questa azione di regola di risposta è disponibile solo se si distribuiscono uno o più plug-in di FlexResponse server personalizzati a Symantec Data Loss Prevention. Vedere "Distribuzione di un plug-in di FlexResponse server" a pagina 1888.
Imposta attributo	Aggiunge un valore personalizzato al record dell'incidente. Vedere "Configurazione dell'azione Imposta attributo" a pagina 1517.
Imposta stato	Modifica lo stato dell'incidente e lo imposta sul valore specificato. Vedere "Configurazione dell'azione Imposta stato" a pagina 1518.

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Azioni delle regole di risposta per il rilevamento di endpoint

Symantec Data Loss Prevention fornisce varie azioni regola di risposta per Endpoint Prevent e Endpoint Discover.

Tabella 42-3 Azioni delle regole di risposta endpoint disponibili

Azione delle regole di risposta	Descrizione
Endpoint: FlexResponse	Azione personalizzata mediante l'API FlexResponse. Vedere "Configurazione dell'azione Endpoint: FlexResponse" a pagina 1544.
Endpoint Discover: metti file in quarantena	Mette in quarantena un file riservato rilevato. Vedere "Configurazione dell'azione Endpoint Discover: metti file in quarantena" a pagina 1545.

Azione delle regole di risposta	Descrizione
Endpoint Prevent: blocca	<p>Blocca il trasferimento dei dati che violano la politica.</p> <p>Ad esempio, blocca la copia di dati riservati da un endpoint a un'unità flash USB.</p> <p>Vedere "Configurazione dell'azione Endpoint Prevent: blocca" a pagina 1547.</p>
Endpoint Prevent: notifica	<p>Visualizza una notifica sullo schermo dell'utente dell'endpoint quando vengono trasferiti dati riservati.</p> <p>Vedere "Configurazione dell'azione Endpoint Prevent: notifica" a pagina 1554.</p>
Endpoint Prevent: operazione annullata dall'utente	<p>Consente all'utente di annullare il trasferimento di un file riservato. L'annullamento è limitato in termini di tempo.</p> <p>Vedere "Configurazione dell'azione Endpoint Prevent: operazione annullata dall'utente" a pagina 1557.</p>

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Vedere ["Funzionalità delle regole di risposta di Endpoint Prevent su Mac"](#) a pagina 2047.

Azioni delle regole di risposta per il rilevamento di Network Prevent

Symantec Data Loss Prevention fornisce varie azioni regola di risposta per Network Prevent for Web e Network Prevent for Email.

Tabella 42-4 Azioni delle regole di risposta della rete disponibili

Azione delle regole di risposta	Descrizione
Network Prevent: blocca richiesta FTP	<p>Blocca le trasmissioni FTP.</p> <p>Vedere "Configurazione dell'azione Network Prevent for Web: Blocca richiesta FTP" a pagina 1560.</p> <p>Nota: Disponibile solo con Network Prevent for Web.</p>
Network Prevent: blocca HTTP/HTTPS	<p>Blocca le pubblicazioni sul Web.</p> <p>Vedere "Configurazione dell'azione Network Prevent for Web: blocca HTTP/HTTPS" a pagina 1560.</p> <p>Nota: Disponibile solo con Network Prevent for Web.</p>

Azione delle regole di risposta	Descrizione
Network Prevent: blocca messaggio SMTP	<p>Blocca le e-mail che causano un incidente.</p> <p>Vedere "Configurazione dell'azione Network Prevent: blocca messaggio SMTP" a pagina 1562.</p>
Network Prevent: crittografia ICE	<p>Crittografare le e-mail e gli allegati o gli allegati.</p> <p>Vedere "Crittografia delle e-mail cloud con Symantec Information Centric Encryption" a pagina 2282.</p>
Network Prevent: modifica messaggio SMTP	<p>Modifica i messaggi e-mail riservati.</p> <p>Ad esempio, modificare l'oggetto dell'e-mail in modo da includere le informazioni sulla violazione.</p> <p>Vedere "Configurazione dell'azione Network Prevent: modifica messaggio SMTP" a pagina 1563.</p>
Network Prevent: rimuovi contenuto HTTP/HTTPS	<p>Rimuove il contenuto riservato dai post sul Web.</p> <p>Vedere "Configurazione dell'azione Network Prevent for Web: rimuovi contenuto HTTP/HTTPS" a pagina 1564.</p> <p>Nota: Disponibile solo con Network Prevent for Web.</p>

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Azioni delle regole di risposta per il rilevamento di Network Protect

Symantec Data Loss Prevention fornisce diverse azioni di regola di risposta per Network Protect (Discover).

Tabella 42-5 Azioni delle regole di risposta di Network Protect disponibili

Azione delle regole di risposta	Descrizione
Network Protect: copia file	<p>Copia i file riservati in un percorso specificato.</p> <p>Vedere "Configurazione dell'azione Network Protect: copia file" a pagina 1565.</p> <p>Nota: Disponibile solo con Network Protect.</p>

Azione delle regole di risposta	Descrizione
Network Protect: metti file in quarantena	<p>Mette in quarantena i file riservati.</p> <p>Vedere "Configurazione dell'azione Network Protect: metti file in quarantena" a pagina 1566.</p> <p>Nota: Disponibile solo con Network Protect.</p>
Network Protect: crittografa file	<p>Crittografare i file riservati utilizzando Symantec ICE.</p> <p>Vedere "Configurazione dell'azione Network Protect: crittografa file" a pagina 1567.</p> <p>Nota: Questa azione è disponibile solo se la licenza di Network Protect ICE è stata installata ed Enforce Server è stato configurato per connettersi al cloud Symantec ICE. Per informazioni su come Symantec Data Loss Prevention interagisce con Symantec ICE, fare riferimento al <i>Manuale di distribuzione di Symantec Information Centric Encryption</i> all'indirizzo http://www.symantec.com/docs/DOC9707..</p>

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Azioni di regole di risposta per rilevamento archiviazione cloud

Symantec Data Loss Prevention fornisce due azioni di regole di risposta per il rilevamento archiviazione cloud, dai server di rilevamento on-site o nei rilevatori di cloud.

Tabella 42-6 Azioni di regole di risposta archiviazione cloud disponibile

Azione delle regole di risposta	Descrizione
Archiviazione cloud: aggiungi tag visivo	<p>Aggiungere un tag di testo al contenuto di archiviazione cloud Box che viola una politica.</p> <p>Vedere "Configurazione dell'azione Archiviazione cloud: aggiungi tag visivo" a pagina 1523.</p>
Archiviazione cloud: quarantena	<p>Mettere in quarantena i file riservati da un account utente di archiviazione cloud in un account utente quarantena. Per la scansione Box on-site, è possibile utilizzare anche una posizione di quarantena on-site.</p> <p>Vedere "Configurazione dell'azione Archiviazione cloud: quarantena" a pagina 1523.</p>

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Azioni di regole di risposta per rilevatori Applicazioni cloud e dispositivo API

Il connettore servizio cloud di Symantec Data Loss Prevention consente di connettere Symantec Data Loss Prevention alla soluzione del broker di sicurezza per l'accesso al cloud (CASB). È possibile utilizzare l'API REST pubblica per inviare dati riservati dalla soluzione CASB a Symantec Data Loss Prevention per ispezione. Symantec Data Loss Prevention risponde con informazioni sulle violazioni della politica e consigli per l'azione di riparazione ove necessario.

Il dispositivo Rilevamento API per le app degli sviluppatori ti consente di connetterti con applicazioni on-site. È possibile utilizzare l'API REST per inviare dati dalle applicazioni a Symantec Data Loss Prevention per l'ispezione. Symantec Data Loss Prevention risponde con informazioni sulle violazioni della politica e consigli per l'azione di riparazione ove necessario.

Queste regole di risposta del dispositivo API e delle Applicazioni cloud consentono di configurare i messaggi sui consigli di riparazione inclusi da Symantec Data Loss Prevention nelle risposte di rilevamento inviate al client REST nei parametri `customResponsePayload` o `message`. Le regole di risposta automatica sono eseguite automaticamente sull'applicazione di destinazione.

Le regole di risposta per i dispositivi API e le applicazioni Cloud sono organizzate in due categorie, una per ogni tipo di dati in REST API: Dati a riposo (DAR) e Dati in movimento (DIM).

Tabella 42-7 Azioni di regole di risposta disponibili di applicazioni cloud e dispositivo API (dati a riposo)

Azione delle regole di risposta	Descrizione
Interrompi collegamenti nei dati a riposo	L'azione Interrompi collegamenti nei dati a riposo interrompe i collegamenti nei dati riservati. Vedere "Configurazione dell'azione Interrompi collegamenti nei dati a riposo" a pagina 1528.
Azione personalizzata su dati a riposo	L'azione Azione personalizzata su dati a riposo restituisce una raccomandazione per eseguire qualche azione personalizzata sui dati riservati con il risultato di rilevamento. Vedere "Configurazione dell'azione Azione personalizzata su dati a riposo" a pagina 1529.

Azione delle regole di risposta	Descrizione
Elimina dati a riposo	<p>L'azione Elimina dati a riposo elimina i dati riservati.</p> <p>Vedere "Configurazione dell'azione Elimina dati a riposo" a pagina 1530.</p>
Crittografa dati a riposo	<p>L'azione Crittografa dati a riposo crittografa i dati riservati.</p> <p>Vedere "Configurazione dell'azione Crittografa dati a riposo" a pagina 1531.</p>
Esegui DRM su dati a riposo	<p>L'azione Esegui DRM su dati a riposo applica Digital Rights Management (DRM) ai dati riservati.</p> <p>Vedere "Configurazione dell'azione Esegui DRM su dati a riposo" a pagina 1531.</p>
Metti in quarantena dati a riposo	<p>L'azione Metti in quarantena dati a riposo mette in quarantena i dati riservati.</p> <p>Vedere "Configurazione dell'azione Metti in quarantena dati a riposo" a pagina 1532.</p>
Marca dati a riposo	<p>L'azione Marca dati a riposo segna i dati riservati.</p> <p>Vedere "Configurazione dell'azione Marca dati a riposo" a pagina 1533.</p>

Tabella 42-8 Azioni di regole di risposta disponibili di applicazioni cloud e dispositivo API (azioni aggiuntive per dati a riposo)

Azione delle regole di risposta	Descrizione
Impedisci download, copia, stampa	<p>L'azione Impedire download, copia, stampa impedisce il download, la copia e le opzioni di stampa per i dati riservati.</p> <p>Vedere "Configurazione dell'azione Impedisci download, copia, stampa" a pagina 1534.</p>
Rimuovi accesso collaboratore	<p>L'azione Rimuovi accesso collaboratore rimuove i diritti di accesso ai dati riservati per tutti i collaboratori.</p> <p>Vedere "Configurazione dell'azione Rimuovi accesso collaboratore" a pagina 1534.</p>

Azione delle regole di risposta	Descrizione
Imposta accesso collaboratore in Modifica	<p>L'azione Imposta accesso collaboratore in Modifica consente ai collaboratori l'accesso e la modifica dei dati riservati.</p> <p>Vedere "Configurazione dell'azione Imposta accesso collaboratore in Modifica" a pagina 1535.</p>
Imposta accesso collaboratore in Anteprima	<p>L'azione Imposta accesso collaboratore in Anteprima concede ai collaboratori l'accesso in anteprima ai dati riservati.</p> <p>Vedere "Configurazione dell'azione Imposta accesso collaboratore in Anteprima" a pagina 1535.</p>
Imposta accesso collaboratore in Lettura	<p>L'azione Imposta accesso collaboratore in Lettura concede ai collaboratori l'accesso in lettura ai dati riservati.</p> <p>Vedere "Configurazione dell'azione Imposta accesso collaboratore in Lettura" a pagina 1536.</p>
Imposta accesso file in Lettura completa	<p>L'azione Imposta accesso file in Lettura completa consente l'accesso in lettura pubblica ai dati riservati.</p> <p>Vedere "Configurazione dell'azione Imposta accesso file in Lettura completa" a pagina 1537.</p>
Imposta accesso file in Modifica interna	<p>L'azione Imposta accesso file in Modifica interna autorizza tutti i membri dell'organizzazione a modificare i dati riservati.</p> <p>Vedere "Configurazione di Imposta accesso file in Modifica interna" a pagina 1537.</p>
Imposta accesso file in Lettura interna	<p>L'azione Imposta accesso file in Lettura interna concede a tutti i membri dell'organizzazione l'accesso in lettura ai dati riservati.</p> <p>Vedere "Configurazione dell'azione Imposta accesso file in Lettura interna" a pagina 1538.</p>

Tabella 42-9 Azioni di regole di risposta disponibili di applicazioni cloud e dispositivo API (dati in movimento)

Azione delle regole di risposta	Descrizione
Aggiungi autenticazione a due fattori	<p>L'azione Aggiungi autenticazione a due fattori aggiunge un'autenticazione a due fattori per i dati riservati.</p> <p>Vedere "Configurazione dell'azione Aggiungi autenticazione a due fattori" a pagina 1539.</p>
Blocca dati in movimento	<p>L'azione Blocca dati in movimento blocca i dati riservati.</p> <p>Vedere "Configurazione dell'azione Blocca dati in movimento" a pagina 1539.</p>
Azione personalizzata su dati in movimento	<p>L'azione Azione personalizzata su dati in movimento restituisce una raccomandazione per eseguire qualche azione personalizzata sui dati riservati con il risultato di rilevamento.</p> <p>Vedere "Configurazione dell'azione Azione personalizzata su dati in movimento" a pagina 1540.</p>
Crittografa dati in movimento	<p>L'azione Crittografa dati in movimento crittografa i dati riservati.</p> <p>Vedere "Configurazione dell'azione Crittografa dati in movimento" a pagina 1541.</p>
Esegui DRM su dati in movimento	<p>L'azione Esegui DRM su dati in movimento applica Digital Rights Management (DRM) ai dati riservati.</p> <p>Vedere "Configurazione dell'azione Esegui DRM su dati in movimento" a pagina 1541.</p>
Metti in quarantena dati in movimento	<p>L'azione Metti in quarantena dati in movimento mette in quarantena i dati riservati.</p> <p>Vedere "Configurazione dell'azione Metti in quarantena dati in movimento" a pagina 1542.</p>
Cancella dati in movimento	<p>L'azione Cancella dati in movimento cancella i dati riservati.</p> <p>Vedere "Configurazione dell'azione Cancella dati in movimento" a pagina 1543.</p>

Informazioni sui tipi di esecuzione delle regole di risposta

Symantec Data Loss Prevention fornisce due tipi di regole di risposta delle politiche: automatica e smart.

Il server di rilevamento che segnala una violazione della politica esegue le regole di risposta automatica. Gli utenti quali i risolutori di incidenti eseguono le regole di risposta smart su richiesta dalla console di amministrazione di Enforce Server.

Vedere ["Informazioni sui ruoli consigliati per l'organizzazione"](#) a pagina 111.

Tabella 42-10 Tipi di regole di risposta

Tipo di esecuzione delle regole di risposta	Descrizione
Regole di risposta automatica	Quando si ha una violazione della politica, il server di rilevamento esegue automaticamente azioni di regola di risposta. Vedere "Informazioni sulle regole di risposta automatica" a pagina 1478.
Regole di risposta smart	Quando si verifica una violazione della politica, un utente autorizzato attiva manualmente la regola di risposta. Vedere "Informazioni sulle regole di risposta smart" a pagina 1479.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Informazioni sulle regole di risposta automatica

Il sistema esegue le regole di risposta automatica quando il motore di rilevamento segnala una violazione della politica. Tuttavia, se si implementa una condizione di regola di risposta, la condizione deve essere soddisfatta perché il sistema esegua la regola di risposta. Le condizioni consentono di controllare l'esecuzione automatica delle azioni di regola di risposta.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Ad esempio, il sistema può bloccare automaticamente determinate azioni di violazione delle politiche, come il tentativo di trasferimento di dati di alto valore relativi a clienti o di documenti di progettazione riservati. Oppure, il sistema può riassegnare un incidente a un sistema di gestione del flusso di lavoro affinché venga gestito immediatamente. Oppure, per un incidente relativo a 1000 record di clienti, è possibile impostare un livello di gravità differente da quello per un incidente relativo a soltanto 10 record.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Informazioni sulle regole di risposta smart

Gli utenti eseguono le regole di risposta smart su richiesta, in risposta alle violazioni delle politiche, nella schermata **Istantanea incidente** della console di amministrazione di Enforce Server.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Le regole di risposta smart sono create per le situazioni che richiedono la riparazione da parte degli utenti. Ad esempio, è possibile creare una regola di risposta smart per ignorare gli incidenti falsi positivi. Un addetto alle riparazioni degli incidenti può esaminare l'incidente, identificare la corrispondenza come falso positivo e ignorarla.

Vedere ["Informazioni sulle regole di risposta smart"](#) a pagina 1492.

Soltanto alcune regole di risposta sono disponibili per l'esecuzione manuale.

Tabella 42-11 Regole di risposta smart disponibili per l'esecuzione manuale

Regola di risposta smart	Descrizione
Aggiungi nota	<p>Aggiunge un campo al record dell'incidente che l'addetto alle riparazioni può annotare nella schermata Istantanea incidente.</p> <p>Vedere "Configurazione dell'azione Aggiungi nota" a pagina 1510.</p>
Registrazione a un server Syslog	<p>Registra l'incidente a un server Syslog per la riparazione del flusso di lavoro.</p> <p>Vedere "Configurazione del registro a un'azione del server Syslog" a pagina 1513.</p>
Quarantena	Mette in quarantena i dati riservati nelle applicazioni del cloud.
Ripristina file	Ripristina un file di applicazione del cloud messo precedentemente in quarantena.
Invia notifica e-mail	<p>Inviare un'e-mail ai destinatari specificati.</p> <p>Vedere "Configurazione dell'azione Invia notifica e-mail" a pagina 1514.</p>
FlexResponse server	<p>Eseguire un'azione FlexResponse server personalizzata.</p> <p>Vedere "Configurazione dell'azione di FlexResponse server" a pagina 1516.</p> <p>Nota: Questa azione di regola di risposta è disponibile solo se si distribuiscono uno o più plug-in di FlexResponse server personalizzati a Symantec Data Loss Prevention.</p> <p>Vedere "Distribuzione di un plug-in di FlexResponse server" a pagina 1888.</p>
Imposta stato	<p>Impostare lo stato dell'incidente sul valore specificato.</p> <p>Vedere "Configurazione dell'azione Imposta stato" a pagina 1518.</p>

Regola di risposta smart	Descrizione
Quarantena SharePoint Network Protect	<p>Mettere in quarantena i dati riservati archiviati in un server Microsoft SharePoint.</p> <p>Vedere "Configurazione dell'azione di risposta smart alla Quarantena SharePoint" a pagina 1525.</p>

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Informazioni sulle condizioni delle regole di risposta

Le condizioni delle regole di risposta sono componenti delle regole di risposta opzionali. Definiscono come e quando il sistema attiva azioni delle regole di risposta. Offrono più modi di prioritizzare gli incidenti in entrata per concentrarsi sulla risoluzione e adottare la risposta appropriata.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Le condizioni delle regole di risposta attivano un'azione in base ai criteri di corrispondenza del rilevamento. Ad esempio è possibile configurare una condizione in modo da attivare un'azione per gli incidenti di gravità elevata, determinati tipi di incidenti o dopo un numero specificato di incidenti.

Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.

Le condizioni non sono obbligatorie. Se una regola di risposta non dichiara una condizione, l'azione della regola di risposta viene eseguita sempre ogni volta che si verifica un incidente. Se è dichiarata una condizione, questa deve essere soddisfatta affinché l'azione venga attivata. Se sono dichiarate più condizioni, queste devono essere soddisfatte tutte affinché il sistema intraprenda un'azione.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

Tabella 42-12 Condizioni delle regole di risposta disponibili

Tipo di condizione	Descrizione
Posizione endpoint	<p>Attiva un'azione di risposta quando l'endpoint è incluso o meno nella rete aziendale.</p> <p>Vedere "Configurazione dello condizione di risposta Posizione endpoint" a pagina 1499.</p>
Dispositivo endpoint	<p>Attiva un'azione di risposta quando si verifica un evento su un dispositivo endpoint configurato.</p> <p>Vedere "Configurazione della condizione di risposta del dispositivo endpoint" a pagina 1500.</p>

Tipo di condizione	Descrizione
Tipo di incidente	Attiva un'azione di risposta quando il tipo specificato di server di rilevamento segnala una corrispondenza. Vedere "Configurazione della condizione di risposta Tipo di incidente" a pagina 1501.
Numero corrispondenza incidenti	Attiva un'azione di risposta quando il numero di violazioni delle politiche supera una soglia o un intervallo. Vedere "Configurazione della condizione di risposta Numero corrispondenza incidenti" a pagina 1503.
Monitoraggio di endpoint o di protocollo	Attiva un'azione di risposta quando un incidente viene rilevato su un protocollo di comunicazione della rete specificato (quale HTTP) o su una destinazione endpoint (ad esempio, CD/DVD). Vedere "Configurazione della condizione di risposta Monitoraggio protocollo o endpoint" a pagina 1504.
Gravità	Attiva un'azione di risposta quando la violazione della politica è un determinato livello di gravità. Vedere "Configurazione della condizione di risposta Gravità" a pagina 1506.

Informazioni sulla priorità di esecuzione delle azioni di regola di risposta

Un server Symantec Data Loss Prevention esegue azioni di regola di risposta secondo una priorità definita dal sistema. Non è possibile modificare l'ordine di esecuzione delle regole di risposta di differenti tipi.

In tutti i casi, quando un server esegue due o più regole di risposta differenti per la stessa politica, l'azione di risposta con la priorità più alta ha la precedenza.

Considerare gli esempi seguenti:

- Una regola di risposta endpoint consente a un utente di annullare un tentativo di copia di file e un'altra regola blocca il tentativo.
Il server di rilevamento blocca la copia di file.
- Un'azione di regola di risposta di rete copia un file e un'altra azione la mette in quarantena.
Il server di rilevamento mette in quarantena il file.
- Un'azione di regola di risposta di rete modifica il contenuto di un messaggio di posta elettronica e un'altra azione blocca la trasmissione.
Il server di rilevamento blocca la trasmissione dell'e-mail.

Non è possibile modificare l'ordine di esecuzione per tipi di azione di regola di risposta differenti. È comunque possibile modificare l'ordine di esecuzione per azioni di regola di risposta dello stesso tipo con istruzioni in conflitto.

Vedere ["Modifica dell'ordinamento delle regole di risposta"](#) a pagina 1497.

Tabella 42-13 Priorità di esecuzione delle regole di risposta definita dal sistema

Priorità di esecuzione (dal più alto al più basso)	Descrizione
Endpoint Prevent: blocca	Vedere "Configurazione dell'azione Endpoint Prevent: blocca" a pagina 1547.
Endpoint Prevent: crittografa	Vedere "Configurazione dell'azione Endpoint Prevent: crittografa" a pagina 1550.
Endpoint Prevent: operazione annullata dall'utente	Vedere "Configurazione dell'azione Endpoint Prevent: operazione annullata dall'utente" a pagina 1557.
Endpoint: FlexResponse	Vedere "Configurazione dell'azione Endpoint: FlexResponse" a pagina 1544.
Endpoint Prevent: notifica	Vedere "Configurazione dell'azione Endpoint Prevent: notifica" a pagina 1554.
Endpoint Discover: metti file in quarantena	Vedere "Configurazione dell'azione Endpoint Discover: metti file in quarantena" a pagina 1545.
Tutto: limita conservazione dati incidenti	Vedere "Configurazione dell'azione Limita conservazione dati incidenti" a pagina 1510.
Network Prevent: blocca messaggio SMTP	Vedere "Configurazione dell'azione Network Prevent: blocca messaggio SMTP" a pagina 1562.
Network Prevent: modifica messaggio SMTP	Vedere "Configurazione dell'azione Network Prevent: modifica messaggio SMTP" a pagina 1563.
Network Prevent for Web: rimuovi contenuto HTTP/HTTPS	Vedere "Configurazione dell'azione Network Prevent for Web: rimuovi contenuto HTTP/HTTPS" a pagina 1564.
Network Prevent for Web: blocca HTTP/HTTPS	Vedere "Configurazione dell'azione Network Prevent for Web: blocca HTTP/HTTPS" a pagina 1560.
Network Prevent for Web: blocca richiesta FTP	Vedere "Configurazione dell'azione Network Prevent for Web: Blocca richiesta FTP" a pagina 1560.
Network Protect: metti file in quarantena	Vedere "Configurazione dell'azione Network Protect: metti file in quarantena" a pagina 1566.

Priorità di esecuzione (dal più alto al più basso)	Descrizione
Network Protect: crittografa file	Vedere "Configurazione dell'azione Network Protect: crittografa file" a pagina 1567.
Network Protect: copia file	Vedere "Configurazione dell'azione Network Protect: copia file" a pagina 1565.
Tutto: imposta stato	Vedere "Configurazione dell'azione Imposta stato" a pagina 1518.
Tutto: imposta attributo	Vedere "Configurazione dell'azione Imposta attributo" a pagina 1517.
Tutto: aggiungi nota	Vedere "Configurazione dell'azione Aggiungi nota" a pagina 1510.
Tutto: effettua registrazione a un server Syslog	Vedere "Configurazione del registro a un'azione del server Syslog" a pagina 1513.
Tutto: invia notifica e-mail	Vedere "Configurazione dell'azione Invia notifica e-mail" a pagina 1514.
Archiviazione cloud: aggiungi tag visivo	Vedere "Configurazione dell'azione Archiviazione cloud: aggiungi tag visivo" a pagina 1523.
Archiviazione cloud: quarantena	Vedere "Configurazione dell'azione Archiviazione cloud: quarantena" a pagina 1523.
FlexResponse server	Vedere "Configurazione dell'azione di FlexResponse server" a pagina 1516. Nota: Le azioni di FlexResponse server che fanno parte delle regole Risposta automatica sono eseguite su Enforce Server anziché sul server di rilevamento.
Applicazioni cloud e dispositivo API (dati in movimento): Blocca dati in movimento	Vedere "Configurazione dell'azione Blocca dati in movimento" a pagina 1539.
Applicazioni cloud e dispositivo API (dati in movimento): Cancella dati in movimento	Vedere "Configurazione dell'azione Cancella dati in movimento" a pagina 1543.
Applicazioni cloud e dispositivo API (dati in movimento): Crittografa dati in movimento	Vedere "Configurazione dell'azione Crittografa dati in movimento" a pagina 1541.
Applicazioni cloud e dispositivo API (dati in movimento): Metti in quarantena dati in movimento	Vedere "Configurazione dell'azione Metti in quarantena dati in movimento" a pagina 1542.

Priorità di esecuzione (dal più alto al più basso)	Descrizione
Applicazioni cloud e dispositivo API (dati in movimento): Esegui DRM su dati in movimento	Vedere "Configurazione dell'azione Esegui DRM su dati in movimento" a pagina 1541.
Applicazioni cloud e dispositivo API (dati in movimento): Azione personalizzata su dati in movimento	Vedere "Configurazione dell'azione Azione personalizzata su dati in movimento" a pagina 1540.
Applicazioni cloud e dispositivo API (dati a riposo): Crittografa dati a riposo	Vedere "Configurazione dell'azione Crittografa dati a riposo" a pagina 1531.
Applicazioni cloud e dispositivo API (dati a riposo): Elimina dati a riposo	Vedere "Configurazione dell'azione Elimina dati a riposo" a pagina 1530.
Applicazioni cloud e dispositivo API (dati a riposo): Metti in quarantena dati a riposo	Vedere "Configurazione dell'azione Metti in quarantena dati a riposo" a pagina 1532.
Applicazioni cloud e dispositivo API (dati a riposo): Marca dati a riposo	Vedere "Configurazione dell'azione Marca dati a riposo" a pagina 1533.
Applicazioni cloud e dispositivo API (dati a riposo): Esegui DRM su dati a riposo	Vedere "Configurazione dell'azione Esegui DRM su dati a riposo" a pagina 1531.
Applicazioni cloud e dispositivo API (dati a riposo): Interrompi collegamenti nei dati a riposo	Vedere "Configurazione dell'azione Interrompi collegamenti nei dati a riposo" a pagina 1528.
Applicazioni cloud e dispositivo API (dati a riposo): Azione personalizzata su dati a riposo	Vedere "Configurazione dell'azione Azione personalizzata su dati a riposo" a pagina 1529.
Applicazioni cloud e dispositivo API (azioni aggiuntive dati a riposo): Imposta accesso file in Lettura completa	Vedere "Configurazione dell'azione Imposta accesso file in Lettura completa" a pagina 1537.
Applicazioni cloud e dispositivo API (azioni aggiuntive dati a riposo): Impedisci download, copia, stampa	Vedere "Configurazione dell'azione Impedisci download, copia, stampa" a pagina 1534.
Applicazioni cloud e dispositivo API (azioni aggiuntive dati a riposo): Imposta accesso file in Lettura interna	Vedere "Configurazione dell'azione Imposta accesso file in Lettura interna" a pagina 1538.

Priorità di esecuzione (dal più alto al più basso)	Descrizione
Applicazioni cloud e dispositivo API (azioni aggiuntive dati a riposo): Imposta accesso file in Modifica interna	Vedere "Configurazione di Imposta accesso file in Modifica interna" a pagina 1537.
Applicazioni cloud e dispositivo API (azioni aggiuntive dati a riposo): Imposta accesso collaboratore in Lettura	Vedere "Configurazione dell'azione Imposta accesso collaboratore in Lettura" a pagina 1536.
Applicazioni cloud e dispositivo API (azioni aggiuntive dati a riposo): Imposta accesso collaboratore in Modifica	Vedere "Configurazione dell'azione Imposta accesso collaboratore in Modifica" a pagina 1535.
Applicazioni cloud e dispositivo API (azioni aggiuntive dati a riposo): Rimuovi accesso collaboratore	Vedere "Configurazione dell'azione Rimuovi accesso collaboratore" a pagina 1534.
Applicazioni cloud e dispositivo API (azioni aggiuntive dati a riposo): Imposta accesso collaboratore in Imposta accesso collaboratore in Anteprima	Vedere "Configurazione dell'azione Imposta accesso collaboratore in Anteprima" a pagina 1535.
Applicazioni cloud e dispositivo API (dati in movimento): Aggiungi autenticazione a due fattori	Vedere "Configurazione dell'azione Aggiungi autenticazione a due fattori" a pagina 1539.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Informazioni sui privilegi di creazione di regole di risposta

Per gestire e creare le regole di risposta, è necessario che l'utente sia assegnato a un ruolo con privilegi di creazione di regole di risposta. Per aggiungere una regola di risposta a una politica, è necessario disporre dei privilegi di creazione di politiche.

Vedere ["Privilegi di creazione politiche"](#) a pagina 380.

Per motivi commerciali si consiglia di concedere i privilegi di creazione di regole di risposta e politiche allo stesso ruolo. In alternativa si consiglia di mantenere questi ruoli separati.

Vedere ["Informazioni sui ruoli consigliati per l'organizzazione"](#) a pagina 111.

Se si accede al sistema come utente senza privilegi di creazione di regole di risposta, la schermata **Gestisci > Politiche > Regole di risposta** non è disponibile.

Vedere ["Informazioni sul controllo degli accessi basato sul ruolo"](#) a pagina 109.

Implementazione di regole di risposta

La configurazione delle regole di risposta è indipendente dalle politiche.

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

È necessario disporre di privilegi di creazione di regole di risposta per creare e gestire le regole di risposta.

Vedere ["Informazioni sui privilegi di creazione di regole di risposta"](#) a pagina 1485.

Tabella 42-14 Flusso di lavoro per l'implementazione di regole di risposta delle politiche

Passaggio	Azione	Descrizione
1	Esaminare le regole di risposta disponibili.	La schermata Gestisci > Politiche > Regole di risposta visualizza tutte le regole di risposta configurate. Vedere "Gestione di regole di risposta" a pagina 1489. Il pacchetto di soluzioni per il sistema in uso fornisce regole di risposta configurate. È possibile utilizzare queste regole di risposta nelle politiche così come sono oppure modificarle. Vedere "Pacchetti di soluzioni" a pagina 377.
2	Decidere il tipo di regola di risposta da implementare: smart, automatiche o entrambe.	Scegliere il tipo di regole di risposta in base ai requisiti aziendali. Vedere "Informazioni sui tipi di esecuzione delle regole di risposta" a pagina 1478.
3	Determinare il tipo di azioni che si intende implementare e tutte le condizioni di attivazione.	Vedere "Informazioni sulle condizioni delle regole di risposta" a pagina 1480. Vedere "Informazioni sulle azioni di regola di risposta" a pagina 1468.
4	Esaminare l'ordine di precedenza delle azioni di regola di risposta di differenti tipi e dello stesso tipo.	Vedere "Informazioni sulla priorità di esecuzione delle azioni di regola di risposta" a pagina 1481. Vedere "Modifica dell'ordinamento delle regole di risposta" a pagina 1497.

Passaggio	Azione	Descrizione
5	Integrare Enforce Server con un sistema esterno (se necessario per la regola di risposta).	<p>Alcune regole di risposta possono richiedere l'integrazione con sistemi esterni.</p> <p>Questi possono includere:</p> <ul style="list-style-type: none"> ■ Un sistema SIEM per la regola di risposta Registrazione a un server Syslog. ■ Un server di e-mail SMTP per la regola di risposta Invia notifica e-mail. ■ Un host di proxy Web per le regole di risposta di Network Prevent for Web. ■ Un agente MTA per le regole di risposta di Network Prevent for Email.
6	Aggiungere una nuova regola di risposta.	Vedere "Aggiunta di una nuova regola di risposta" a pagina 1490.
7	Configurare le regole di risposta.	Vedere "Configurazione di regole di risposta" a pagina 1491.
8	Configurare una o più regole di risposta (facoltativo).	Vedere "Configurazione delle condizioni della regola di risposta" a pagina 1492.
9	Configurare una o più azioni di regola di risposta (obbligatorio).	<p>È necessario definire almeno un'azione per una regola di risposta valida.</p> <p>Vedere "Configurazione delle azioni di regola di risposta" a pagina 1493.</p> <p>L'azione viene eseguita quando si segnala la violazione di una politica o in caso di corrispondenza con una condizione di regola di risposta.</p>
10	Aggiungere regole di risposta alle politiche.	<p>Per aggiungere regole di risposta alle politiche, è necessario disporre dei privilegi di creazione di politiche.</p> <p>Vedere "Aggiunta di una regola di risposta automatica a una politica" a pagina 455.</p>

Best practice per le regole di risposta

Quando si implementano le regole di risposta, considerare quanto riportato di seguito:

- Le regole di risposta non sono obbligatorie per l'esecuzione della politica. In generale è meglio implementare e ottimizzare le regole e le eccezioni della politica prima di implementare le regole di risposta. Dopo avere ottenuto i risultati desiderati per il rilevamento della politica, è possibile implementare e affinare le regole di risposta.

- Le regole di risposta richiedono almeno un'azione della regola. La condizione è opzionale. Se non si implementa una condizione, l'azione viene sempre eseguita quando viene segnalato un incidente. Se si configurano più condizioni per una regola di risposta, tutte le condizioni devono corrispondere affinché l'azione della regola di risposta venga attivata. Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.
- Le condizioni della regola di risposta derivano dalle regole della politica. È necessario comprendere il tipo di condizioni di regole ed eccezioni che la politica implementa quando si configurano le condizioni della regola di risposta. Il sistema valuta la condizione della regola di risposta in base a come la regola della politica conta le corrispondenze. Vedere ["Condizioni di corrispondenza di politiche"](#) a pagina 392.
- Il sistema visualizza solo il nome della regola di risposta che gli autori della politica devono selezionare quando aggiungono regole di risposta alle politiche. Assicurarsi di fornire un nome descrittivo che aiuti gli autori della politica a identificare lo scopo della regola di risposta. Vedere ["Configurazione di politiche"](#) a pagina 422.
- Non è possibile combinare un'azione della regola di risposta Endpoint Prevent: notifica o Endpoint Prevent: blocca con i metodi di rilevamento EDM, IDM o DGM. In caso contrario il sistema visualizza un avviso relativo alla regola configurata erroneamente. Vedere ["Gestione e aggiunta di politiche"](#) a pagina 444.
- Se si combinano più regole di risposta in un'unica politica, assicurarsi di comprendere l'ordine di precedenza tra tali regole. Vedere ["Informazioni sulla priorità di esecuzione delle azioni di regola di risposta"](#) a pagina 1481.
- Utilizzare le regole di risposta smart solo quando è richiesto l'intervento dell'utente. Vedere ["Informazioni sulle regole di risposta smart"](#) a pagina 1492.
- Quando i file riservati sono crittografati utilizzando Symantec Information Centric Encryption, il file originale è sostituito con un file HTML con lo stesso nome. È necessario aggiornare tutti i collegamenti e i riferimenti esistenti in modo che facciano riferimento al nuovo file HTML.
- Microsoft SharePoint consente agli utenti di caricare file HTML di dimensioni non superiori a 256 MB. Per assicurarsi che i file riservati in possano essere crittografati con successo in SharePoint, non caricare file con dimensioni di 256 MB o più. Vedere ["Configurazione dell'azione di FlexResponse server"](#) a pagina 1516.
- Se si configurano più azioni della regola di risposta di FlexResponse server per i target di scansione di Microsoft SharePoint, le azioni potrebbero essere eseguite in base alla loro priorità. Vedere ["Informazioni sulla priorità di esecuzione delle azioni di regola di risposta"](#) a pagina 1481.

Configurazione e gestione delle regole di risposta

Il capitolo contiene i seguenti argomenti:

- [Gestione di regole di risposta](#)
- [Aggiunta di una nuova regola di risposta](#)
- [Configurazione di regole di risposta](#)
- [Informazioni sulle regole di risposta smart](#)
- [Configurazione delle condizioni della regola di risposta](#)
- [Configurazione delle azioni di regola di risposta](#)
- [Modifica dell'ordinamento delle regole di risposta](#)
- [Informazioni sulla rimozione di regole di risposta](#)

Gestione di regole di risposta

La schermata **Gestisci > Politiche > Regole di risposta** consente di gestire le regole di risposta e di aggiungerne di nuove.

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

È necessario disporre di privilegi di creazione di regole di risposta per gestire e aggiungere le regole di risposta.

Vedere ["Informazioni sui privilegi di creazione di regole di risposta"](#) a pagina 1485.

Tabella 43-1 Azioni della schermata Regole di risposta

Azione	Descrizione
Aggiungere una regola di risposta	Fare clic su Aggiungi regola di risposta per definire una nuova regola di risposta. Vedere "Aggiunta di una nuova regola di risposta" a pagina 1490.
Modificare l'ordine delle regole di risposta	Fare clic su Modifica ordine regole di risposta per modificare l'ordine di priorità delle regole di risposta. Vedere "Modifica dell'ordinamento delle regole di risposta" a pagina 1497.
Modificare una regola di risposta	Fare clic sulla regola di risposta per modificarla. Vedere "Configurazione di regole di risposta" a pagina 1491.
Eliminare una regola di risposta	Fare clic sull'icona rossa X all'estrema destra della regola di risposta per eliminarla. È necessario confermare l'operazione per effettuare l'eliminazione. Vedere "Informazioni sulla rimozione di regole di risposta" a pagina 1498.
Aggiornare l'elenco	Fare clic sull'icona di aggiornamento in alto a destra nella schermata Regole di risposta per visualizzare lo stato corrente della regola.

Tabella 43-2 Visualizzazione della schermata Regole di risposta

Colonna visualizzata	Descrizione
Ordine	L' ordine di priorità quando sono configurate più regole di risposta. Vedere "Modifica dell'ordinamento delle regole di risposta" a pagina 1497.
Regola	Il nome della regola di risposta. Vedere "Configurazione di regole di risposta" a pagina 1491.
Azioni	Il tipo di azione che la regola di risposta può intraprendere per rispondere a un incidente (obbligatorio). Vedere "Configurazione delle azioni di regola di risposta" a pagina 1493.
Condizioni	La condizione che genera la regola di risposta (se presente). Vedere "Configurazione delle condizioni della regola di risposta" a pagina 1492.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Aggiunta di una nuova regola di risposta

È possibile aggiungere una nuova regola di risposta nella schermata **Gestisci > Politiche > Regole di risposta > Nuova regola di risposta**.

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Per aggiungere una nuova regola di risposta

- 1 Fare clic su **Aggiungi regola di risposta** nella schermata **Gestisci > Politiche > Regole di risposta**.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

- 2 Nella schermata **Nuova regola di risposta**, selezionare una delle opzioni seguenti:

- **Risposta automatica**

Il sistema esegue automaticamente l'azione di risposta mentre il server valuta gli incidenti (opzione predefinita).

Vedere ["Informazioni sulle regole di risposta automatica"](#) a pagina 1478.

- **Risposta smart**

Un utente autorizzato esegue l'azione di risposta dalla schermata **Istantanea incidente** nella console di amministrazione di Enforce Server.

Vedere ["Informazioni sulle regole di risposta smart"](#) a pagina 1479.

- 3 Fare clic su **Avanti** per configurare la regola di risposta.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione di regole di risposta

La configurazione delle regole di risposta viene eseguita nella schermata **Gestisci > Politiche > Regole di risposta > Configura regola di risposta**.

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Per configurare una regola di risposta

- 1 Aggiungere una nuova regola di risposta o modificarne una esistente.

Vedere ["Aggiunta di una nuova regola di risposta"](#) a pagina 1490.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

- 2 Immettere un nome nel campo **Nome regola** e una **Descrizione**.

- 3 Facoltativamente, definire una o più **Condizioni** per stabilire quando eseguire la regola di risposta.

Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.

Se non si specifica alcuna condizione, l'azione di regola di risposta viene sempre eseguita quando si ha una corrispondenza (purché l'impostazione della regola di rilevamento sia la stessa).

Ignorare questo passaggio se è stata selezionata l'opzione **Risposta smart**.

Vedere ["Informazioni sulle regole di risposta smart"](#) a pagina 1492.

- 4 Selezionare e configurare una o più **azioni**. È necessario definire almeno un'azione.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 5 Fare clic su **Salva** per salvare la definizione della regola di risposta.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Informazioni sulle regole di risposta smart

Quando si implementano le regole di risposta smart, considerare quanto segue:

- Le regole di risposta smart sono adatte agli incidenti che giustificano l'esame dell'utente per determinare se è necessaria un'azione di risposta.
Se non si desidera che l'utente sia coinvolto nell'attivazione di un'azione di regola di risposta, utilizzare le regole di risposta automatica.
- Non è possibile configurare alcuna condizione di attivazione con le regole di risposta smart. Gli utenti autorizzati decidono quando un incidente di rilevamento giustifica una risposta.
- L'utente è limitato nelle azioni che può eseguire con le regole di risposta smart (nota, registro, e-mail, stato).
Se è necessario bloccare o modificare un'azione, utilizzare le regole di risposta automatica.

Vedere ["Informazioni sulle regole di risposta smart"](#) a pagina 1479.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione delle condizioni della regola di risposta

È possibile aggiungere una o più condizioni a una regola di risposta. Un incidente deve rispettare tutte le condizioni della regola di risposta affinché il sistema esegua le azioni della regola di risposta.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Per configurare una condizione della regola di risposta

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Fare clic su **Aggiungi condizione** per aggiungere una nuova condizione.

Le condizioni sono facoltative e basate sulle corrispondenze delle regole di rilevamento. Ogni tipo di condizione della regola di risposta esegue una funzione differente.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

- 3 Scegliere il tipo di condizione dall'elenco **Condizioni**.

Vedere [Tabella 42-12](#) a pagina 1480.

Ad esempio, selezionare la condizione **Conteggio delle corrispondenze degli incidenti e È maggiore di** e inserire **15** nella casella di testo. Questa condizione avvia l'azione della regola di risposta dopo 15 corrispondenze di violazione della politica.

- 4 Per aggiungere un'altra condizione, fare clic su **Aggiungere condizione** e ripetere la procedura.

Se non c'è corrispondenza con nessuna delle condizioni, non viene eseguita alcuna azione.

- 5 Fare clic su **Salva** per salvare la condizione.

Fare clic su **Annulla** per non salvare la condizione e tornare alla schermata precedente.

Fare clic su l'icona della **X rossa** accanto alla condizione per eliminarla dalla regola di risposta.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione delle azioni di regola di risposta

È necessario configurare almeno un'azione perché la regola di risposta sia valida. È possibile configurare molteplici azioni di regola di risposta. Ogni azione è valutata indipendentemente.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Per definire un'azione di regola di risposta

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Scegliere un tipo di azione dall'elenco **Azioni** e fare clic su **Aggiungi azione**.

Ad esempio, aggiungere l'azione **Tutto: aggiungi nota** alla regola di risposta. Questa azione consente all'addetto alle riparazioni di aggiungere una nota relativa all'incidente.

- 3 Configurare il tipo di azione specificando i parametri previsti per il tipo di azione scelto.

Vedere [Tabella 43-3](#) a pagina 1494.

- 4 Ripetere questi passaggi per ogni azione che si desidera aggiungere.

Se si aggiungono ulteriori azioni, considerare l'ordine di esecuzione e la possibile modifica di tipi simili.

Vedere ["Modifica dell'ordinamento delle regole di risposta"](#) a pagina 1497.

- 5 Fare clic su **Salva** per salvare la regola di risposta.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 43-3 Configurazione di un'azione di regola di risposta

Tipo di incidente	Regola di risposta	Descrizione
Tutto	Aggiungi nota	Vedere "Configurazione dell'azione Aggiungi nota" a pagina 1510.
Tutto	Limita conservazione dati incidenti	Vedere "Configurazione dell'azione Limita conservazione dati incidenti" a pagina 1510.
Tutto	Registrazione a un server Syslog	Vedere "Configurazione del registro a un'azione del server Syslog" a pagina 1513.
Tutto	Invia notifica e-mail	Vedere "Configurazione dell'azione Invia notifica e-mail" a pagina 1514.
Tutto	FlexResponse server	Vedere "Configurazione dell'azione di FlexResponse server" a pagina 1516.
Tutto	Imposta attributo	Vedere "Configurazione dell'azione Imposta attributo" a pagina 1517.
Tutto	Imposta stato	Vedere "Configurazione dell'azione Imposta stato" a pagina 1518.
Archiviazione cloud	Aggiungi tag visivo	Vedere "Configurazione dell'azione Archiviazione cloud: aggiungi tag visivo" a pagina 1523.
Archiviazione cloud	Quarantena	Vedere "Configurazione dell'azione Archiviazione cloud: quarantena" a pagina 1523.

Tipo di incidente	Regola di risposta	Descrizione
Applicazioni: Dati a riposo (DAR)	Interrompi collegamenti nei dati a riposo	Vedere "Configurazione dell'azione Interrompi collegamenti nei dati a riposo" a pagina 1528.
Applicazioni: Dati a riposo (DAR)	Azione personalizzata su dati a riposo	Vedere "Configurazione dell'azione Azione personalizzata su dati a riposo" a pagina 1529.
Applicazioni: Dati a riposo (DAR)	Elimina dati a riposo	Vedere "Configurazione dell'azione Elimina dati a riposo" a pagina 1530.
Applicazioni: Dati a riposo (DAR)	Crittografa dati a riposo	Vedere "Configurazione dell'azione Crittografa dati a riposo" a pagina 1531.
Applicazioni: Dati a riposo (DAR)	Esegui DRM su dati a riposo	Vedere "Configurazione dell'azione Esegui DRM su dati a riposo" a pagina 1531.
Applicazioni: Dati a riposo (DAR)	Metti in quarantena dati a riposo	Vedere "Configurazione dell'azione Metti in quarantena dati a riposo" a pagina 1532.
Applicazioni: Dati a riposo (DAR)	Marca dati a riposo	Vedere "Configurazione dell'azione Marca dati a riposo" a pagina 1533.
Applicazioni: Dati in movimento	Aggiungi autenticazione a due fattori	Vedere "Configurazione dell'azione Aggiungi autenticazione a due fattori" a pagina 1539.
Applicazioni: Dati in movimento (DIM)	Blocca dati in movimento	Vedere "Configurazione dell'azione Blocca dati in movimento" a pagina 1539.
Applicazioni: Dati in movimento (DIM)	Azione personalizzata su dati in movimento	Vedere "Configurazione dell'azione Azione personalizzata su dati in movimento" a pagina 1540.
Applicazioni: Dati in movimento (DIM)	Crittografa dati in movimento	Vedere "Configurazione dell'azione Crittografa dati in movimento" a pagina 1541.
Applicazioni: Dati in movimento (DIM)	Esegui DRM su dati in movimento	Vedere "Configurazione dell'azione Esegui DRM su dati in movimento" a pagina 1541.
Applicazioni: Dati in movimento (DIM)	Metti in quarantena dati in movimento	Vedere "Configurazione dell'azione Metti in quarantena dati in movimento" a pagina 1542.
Applicazioni: Dati in movimento (DIM)	Cancella dati in movimento	Vedere "Configurazione dell'azione Cancella dati in movimento" a pagina 1543.

Tipo di incidente	Regola di risposta	Descrizione
Applicazioni: Dati a riposo (DAR)	Impedisci download, copia, stampa	Vedere "Configurazione dell'azione Impedisci download, copia, stampa" a pagina 1534.
Applicazioni: Dati a riposo (DAR)	Rimuovi accesso collaboratore	Vedere "Configurazione dell'azione Rimuovi accesso collaboratore" a pagina 1534.
Applicazioni: Dati a riposo (DAR)	Imposta accesso collaboratore in Modifica	Vedere "Configurazione dell'azione Imposta accesso collaboratore in Modifica" a pagina 1535.
Applicazioni: Dati a riposo (DAR)	Imposta accesso collaboratore in Anteprima	Vedere "Configurazione dell'azione Imposta accesso collaboratore in Anteprima" a pagina 1535.
Applicazioni: Dati a riposo (DAR)	Imposta accesso collaboratore in Lettura	Vedere "Configurazione dell'azione Imposta accesso collaboratore in Lettura" a pagina 1536.
Applicazioni: Dati a riposo (DAR)	Imposta accesso file in Lettura completa	Vedere "Configurazione dell'azione Imposta accesso file in Lettura completa" a pagina 1537.
Applicazioni: Dati a riposo (DAR)	Imposta accesso file in Modifica interna	Vedere "Configurazione di Imposta accesso file in Modifica interna" a pagina 1537.
Applicazioni: Dati a riposo (DAR)	Imposta accesso file in Lettura interna	Vedere "Configurazione dell'azione Imposta accesso file in Lettura interna" a pagina 1538.
Endpoint	FlexResponse	Vedere "Configurazione dell'azione Endpoint: FlexResponse" a pagina 1544.
Endpoint Discover	File in quarantena	Vedere "Configurazione dell'azione Endpoint Discover: metti file in quarantena" a pagina 1545.
Endpoint Prevent	Blocca	Vedere "Configurazione dell'azione Endpoint Prevent: blocca" a pagina 1547.
Endpoint Prevent	Crittografa	Vedere "Configurazione dell'azione Endpoint Prevent: crittografa" a pagina 1550.
Endpoint Prevent	Notifica	Vedere "Configurazione dell'azione Endpoint Prevent: notifica" a pagina 1554.
Endpoint Prevent	Operazione annullata dall'utente	Vedere "Configurazione dell'azione Endpoint Prevent: operazione annullata dall'utente" a pagina 1557.
Network Prevent for Web	Blocca richiesta FTP	Vedere "Configurazione dell'azione Network Prevent for Web: Blocca richiesta FTP" a pagina 1560.
Network Prevent for Web	Blocca HTTP/S	Vedere "Configurazione dell'azione Network Prevent for Web: blocca HTTP/HTTPS" a pagina 1560.

Tipo di incidente	Regola di risposta	Descrizione
Network Prevent for Email	Blocca messaggio SMTP	Vedere "Configurazione dell'azione Network Prevent: blocca messaggio SMTP" a pagina 1562.
Network Prevent for Email	Modifica messaggio SMTP	Vedere "Configurazione dell'azione Network Prevent: modifica messaggio SMTP" a pagina 1563.
Network Prevent for Web	Rimuovi contenuto HTTP/HTTPS	Vedere "Configurazione dell'azione Network Prevent for Web: rimuovi contenuto HTTP/HTTPS" a pagina 1564.
Network Protect	Copia file	Vedere "Configurazione dell'azione Network Protect: copia file" a pagina 1565.
Network Protect	File in quarantena	Vedere "Configurazione dell'azione Network Protect: metti file in quarantena" a pagina 1566.
Network Protect	Crittografa file	Vedere "Configurazione dell'azione Network Protect: crittografa file" a pagina 1567.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Modifica dell'ordinamento delle regole di risposta

Non è possibile modificare la priorità di esecuzione definita dal sistema per i differenti tipi di azioni di regola di risposta. È comunque possibile modificare l'ordine di esecuzione per le azioni di regola di risposta dello stesso tipo con istruzioni in conflitto.

Vedere ["Informazioni sulla priorità di esecuzione delle azioni di regola di risposta"](#) a pagina 1481.

Ad esempio, si consideri uno scenario che include due regole di risposta in una politica. Ogni regola di risposta implementa un'azione Limita conservazione dati incidenti. Un'azione ignora tutti gli allegati e l'altra ignora solo gli allegati che non sono violazioni. In questo caso, quando si verifica una violazione della politica, il server di rilevamento fa riferimento alla priorità di esecuzione delle regole di risposta per determinare quale azione deve essere eseguita per prima. Questo tipo di ordinamento è configurabile.

Per modificare l'ordinamento di un'azione di regola di risposta

- 1 Accedere alla pagina **Gestisci > Politiche > Regole di risposta**.
Vedere "[Gestione di regole di risposta](#)" a pagina 1489.
- 2 Notare la colonna **Ordine** e il numero accanto a ogni regola di risposta configurata.
Per impostazione predefinita, il sistema ordina l'elenco delle regole di risposta in base alla colonna **Ordine**, dalla priorità più alta (1) a quella più bassa. Inizialmente il sistema ordina le regole di risposta nell'ordine in cui sono create. È possibile modificare questo ordine.
- 3 Per attivare la modalità di modifica, fare clic su **Modifica ordine regole di risposta**.
La colonna **Ordine** ora visualizza un menu a discesa per ogni regola di risposta.
- 4 Per modificare l'ordinamento di una regola di risposta, selezionare la priorità desiderata dal menu a discesa.
Ad esempio, la priorità di una regola di risposta può essere modificata da 2 a 1 (priorità più alta).
La modifica della priorità sposta la regola di risposta nella nuova posizione nell'elenco e aggiorna tutte le altre regole di risposta.
- 5 Fare clic su **Salva** per salvare le modifiche all'ordinamento delle regole di risposta.
- 6 Ripetere questi passaggi come necessario per ottenere i risultati voluti.
Vedere "[Implementazione di regole di risposta](#)" a pagina 1486.

Informazioni sulla rimozione di regole di risposta

È possibile eliminare regole di risposta nella schermata **Gestisci > Politiche > Regole di risposta**.

Vedere "[Gestione di regole di risposta](#)" a pagina 1489.

Quando si eliminano regole di risposta, considerare quanto riportato di seguito:

- Un utente deve disporre di privilegi di creazione di regole di risposta per eliminare una regola di risposta.
- L'autore di regole di risposta non può eliminare una regola di risposta che un altro utente sta modificando.
- Un autore di regole di risposta non può eliminare una regola di risposta se una politica la dichiara. In questo caso è necessario rimuovere la regola di risposta da tutte le politiche che la dichiarano prima di poterla eliminare.

Condizioni di regole di risposta

Il capitolo contiene i seguenti argomenti:

- [Configurazione della condizione di risposta Posizione endpoint](#)
- [Configurazione della condizione di risposta del dispositivo endpoint](#)
- [Configurazione della condizione di risposta Tipo di incidente](#)
- [Configurazione della condizione di risposta Numero corrispondenza incidenti](#)
- [Configurazione della condizione di risposta Monitoraggio protocollo o endpoint](#)
- [Configurazione della condizione di risposta Gravità](#)

Configurazione della condizione di risposta Posizione endpoint

La condizione Posizione endpoint genera un'azione di regola di risposta basata sullo stato di connessione del DLP Agent quando una politica endpoint viene violata.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Nota: Questa condizione è specifica agli incidenti endpoint. Questa condizione non deve essere implementata per gli incidenti Rete o Discover. In caso contrario, l'azione di regola di risposta non viene eseguita.

Per configurare la condizione Posizione endpoint

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Selezionare la condizione **Posizione endpoint** dall'elenco **Condizioni**.
Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.
- 3 Selezionare i requisiti della posizione endpoint per generare azioni.
Vedere [Tabella 44-1](#) a pagina 1500.

Tabella 44-1 Opzioni della condizione Posizione endpoint

Qualificatore	Condizione	Descrizione
È uno qualsiasi dei seguenti valori	All'esterno della rete aziendale	Questa combinazione genera un'azione di regola di risposta se un incidente si verifica quando l'endpoint è all'esterno della rete aziendale.
Non è alcuno dei seguenti valori	All'esterno della rete aziendale	Questa combinazione non genera un'azione di regola di risposta se un incidente si verifica quando l'endpoint è all'esterno della rete aziendale.
È uno qualsiasi dei seguenti valori	All'interno della rete aziendale	Questa combinazione genera un'azione di regola di risposta se un incidente si verifica quando l'endpoint è all'interno della rete aziendale.
Non è alcuno dei seguenti valori	All'interno della rete aziendale	Questa combinazione non genera un'azione di regola di risposta se un incidente si verifica quando l'endpoint è all'interno della rete aziendale.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Configurazione della condizione di risposta del dispositivo endpoint

La condizione del dispositivo endpoint attiva l'azione della regola di risposta quando viene rilevato un incidente da uno o più dispositivi di endpoint configurati.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Configurare i dispositivi di endpoint nella schermata **Sistema > Agenti > Dispositivi endpoint**.

Vedere ["Informazioni sul rilevamento di dispositivi endpoint"](#) a pagina 826.

Nota: Questa condizione è specifica degli incidenti endpoint. Questa condizione non deve essere implementata per gli incidenti Rete o Discover. In caso contrario, l'azione di regola di risposta non viene eseguita.

Per configurare la condizione di risposta del dispositivo endpoint

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Selezionare la condizione **Dispositivo endpoint** dall'elenco **Condizioni**.
Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.
- 3 Selezionare per individuare o escludere dispositivi di endpoint specifici.
Vedere [Tabella 44-2](#) a pagina 1501.

Tabella 44-2 Parametri di condizione dei dispositivo endpoint

Qualificatore	Condizione	Descrizione
È uno qualsiasi dei seguenti valori	Dispositivo configurato	Avvia un'azione della regola di risposta quando si individua un incidente su un dispositivo di endpoint configurato.
Non è alcuno dei seguenti valori	Dispositivo configurato	Non avvia (esclude dall'esecuzione) un'azione della regola di risposta quando viene individuato un incidente su un dispositivo di endpoint configurato.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Configurazione della condizione di risposta Tipo di incidente

La condizione Tipo di incidente genera un'azione di regola di risposta basata sul tipo di server di rilevamento che segnala l'incidente.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Per configurare la condizione Tipo di incidente

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Scegliere la condizione **Tipo di incidente** dall'elenco **Condizioni**.
Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.
- 3 Selezionare uno o più tipi di incidente.
Utilizzare il tasto `Ctrl` per selezionare più tipi.
Vedere [Tabella 44-3](#) a pagina 1502.

Tabella 44-3 Parametri della condizione Tipo di incidente

Parametro	Server	Descrizione
È uno qualsiasi dei seguenti valori	Connettore servizio cloud o Dispositivo Rilevamento API per le app degli sviluppatori.	Attiva un'azione della regola di risposta per qualsiasi incidente rilevato dal Connettore servizio cloud o Dispositivo Rilevamento API per le app degli sviluppatori.
Non è alcuno dei seguenti valori		Non attiva un'azione della regola di risposta per qualsiasi incidente rilevato dal Connettore servizio cloud o Dispositivo Rilevamento API per le app degli sviluppatori.
È uno qualsiasi dei seguenti valori	Discover	Genera un'azione di regola di risposta per qualsiasi incidente rilevato da Network Discover.
Non è alcuno dei seguenti valori		Non genera un'azione di regola di risposta per qualsiasi incidente rilevato da Network Discover.
È uno qualsiasi dei seguenti valori	Endpoint	Genera un'azione di regola di risposta per qualsiasi incidente rilevato da Endpoint Prevent.
Non è alcuno dei seguenti valori		Non genera un'azione di regola di risposta per qualsiasi incidente rilevato da Endpoint Prevent.
È uno qualsiasi dei seguenti valori	Rete	Genera un'azione di regola di risposta per qualsiasi incidente rilevato da Network Prevent.
Non è alcuno dei seguenti valori		Non genera un'azione di regola di risposta per qualsiasi incidente rilevato da pn.NetworkPrevent;.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Configurazione della condizione di risposta Numero corrispondenza incidenti

La condizione Numero corrispondenza incidenti genera un'azione di regola di risposta basata sul numero di violazioni della politica segnalate.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Per configurare la condizione Numero corrispondenza incidenti

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Scegliere la condizione **Numero corrispondenza incidenti** dall'elenco **Condizioni**.
Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.
- 3 Nel campo di testo, immettere un valore numerico che indica la soglia a partire dalla quale si desidera attivare la regola di risposta.

Ad esempio, se si immette 15, la regola di risposta viene attivata dopo 15 violazioni della politica rilevate.

Vedere [Tabella 44-4](#) a pagina 1503.

Tabella 44-4 Opzioni della condizione Numero corrispondenza incidenti

Parametro	Input	Descrizione
È maggiore di	Numero definito dall'utente	Genera un'azione di regola di risposta se la soglia del numero di incidenti è superata.
È maggiore di o uguale a	Numero definito dall'utente	Genera un'azione di regola di risposta se il numero di incidenti è uguale o superiore alla soglia relativa.
È compreso tra	Coppia di numeri definita dall'utente	Genera un'azione di regola di risposta quando il numero degli incidenti è compreso tra l'intervallo di numeri specificati.
È minore di	Numero definito dall'utente	Genera un'azione di regola di risposta se il numero di incidenti è minore del numero specificato.
È minore o uguale a	Numero definito dall'utente	Genera un'azione di regola di risposta quando il numero di incidenti è uguale o minore al numero specificato.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Configurazione della condizione di risposta Monitoraggio protocollo o endpoint

La condizione Monitoraggio protocollo o endpoint genera un'azione in base alla destinazione endpoint, al protocollo, al dispositivo o all'applicazione dove si è verificata la violazione della politica.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Per configurare la condizione Monitoraggio protocollo o endpoint

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Scegliere la condizione **Monitoraggio protocollo o endpoint** dall'elenco **Condizioni**.
Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.
- 3 Usare il tasto **Ctrl** per selezionare molteplici elementi; usare il tasto **Shift** per selezionare un intervallo di elementi.
Vedere [Tabella 44-5](#) a pagina 1504.
Il sistema elenca tutti i protocolli di rete supplementari configurati nella schermata **Sistema > Impostazioni > Protocolli**.

Tabella 44-5 Opzioni della condizione Monitoraggio protocollo o endpoint

Qualificatore	Condizione	Descrizione
È uno qualsiasi dei seguenti valori	Accesso ai file di applicazione endpoint	Genera un'azione in caso di accesso a un file di applicazione endpoint.
Non è alcuno dei seguenti valori		Non genera un'azione in caso di accesso a un file di applicazione endpoint.
È uno qualsiasi dei seguenti valori	CD/DVD endpoint	Genera un'azione in caso di scrittura su un CD/DVD endpoint.
Non è alcuno dei seguenti valori		Non genera un'azione in caso di scrittura su un CD/DVD endpoint.
È uno qualsiasi dei seguenti valori	Appunti endpoint	Genera un'azione in caso di operazione di copia in o da Appunti endpoint.
Non è alcuno dei seguenti valori		Non genera un'azione in caso di operazione di copia in o da Appunti endpoint.

Qualificatore	Condizione	Descrizione
È uno qualsiasi dei seguenti valori	Copia endpoint in condivisione di rete	Genera un'azione se informazioni riservate sono copiate in o da una condivisione di rete.
Non è alcuno dei seguenti valori		Non genera un'azione se informazioni riservate sono copiate in o da una condivisione di rete.
È uno qualsiasi dei seguenti valori	Unità locale endpoint	Genera un'azione in caso di rilevamento di file riservati sull'unità locale.
Non è alcuno dei seguenti valori		Non genera un'azione in caso di rilevamento di file riservati sull'unità locale.
È uno qualsiasi dei seguenti valori	Stampante/fax endpoint	Genera un'azione in caso di invio a una stampante o fax endpoint.
Non è alcuno dei seguenti valori		Non genera un'azione in caso di invio a una stampante o fax endpoint.
È uno qualsiasi dei seguenti valori	Dispositivo di archiviazione rimovibile endpoint	Genera un'azione se dati riservati sono copiati su un dispositivo di archiviazione rimovibile.
Non è alcuno dei seguenti valori		Non genera un'azione se dati riservati sono copiati su un dispositivo di archiviazione rimovibile.
È uno qualsiasi dei seguenti valori	FTP	Genera un'azione se dati riservati sono copiati tramite FTP.
Non è alcuno dei seguenti valori		Non genera un'azione se dati riservati sono copiati tramite FTP.
È uno qualsiasi dei seguenti valori	HTTP	Genera un'azione se dati riservati sono inviati tramite HTTP.
Non è alcuno dei seguenti valori		Non genera un'azione se dati riservati sono inviati tramite HTTP.
È uno qualsiasi dei seguenti valori	HTTPS	Genera un'azione se dati riservati sono inviati tramite HTTPS.
Non è alcuno dei seguenti valori		Non genera un'azione se dati riservati sono inviati tramite HTTPS.
È uno qualsiasi dei seguenti valori	NNTP	Genera un'azione se dati riservati sono inviati tramite NNTP.
Non è alcuno dei seguenti valori		Non genera un'azione se dati riservati sono inviati tramite NNTP.

Qualificatore	Condizione	Descrizione
È uno qualsiasi dei seguenti valori	SMTP	Genera un'azione se dati riservati sono inviati tramite SMTP.
Non è alcuno dei seguenti valori		Non genera un'azione se dati riservati sono inviati tramite NNTP.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Configurazione della condizione di risposta Gravità

La condizione Gravità genera un'azione di regola di risposta basata sulla gravità della violazione della regola della politica.

Vedere ["Informazioni sulle condizioni delle regole di risposta"](#) a pagina 1480.

Per configurare la condizione Gravità

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Selezionare la condizione **Gravità** dall'elenco **Condizioni**.

Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.

- 3 Selezionare uno o più livelli di gravità.

Usare il tasto **CTRL** per selezionare molteplici condizioni; usare il tasto **MAIUSC** per selezionare un intervallo di condizioni.

Vedere [Tabella 44-6](#) a pagina 1506.

Tabella 44-6 Corrispondenze con la condizione Gravità

Parametro	Gravità	Descrizione
È uno qualsiasi dei seguenti valori	Alta	Genera un'azione di regola di risposta quando si ha la corrispondenza con una regola di rilevamento di gravità alta.
Non è alcuno dei seguenti valori	Alta	Non genera un'azione di regola di risposta quando si ha la corrispondenza con una regola di rilevamento di gravità alta.
È uno qualsiasi dei seguenti valori	Media	Genera un'azione di regola di risposta quando si ha la corrispondenza con una regola di rilevamento di gravità media.

Parametro	Gravità	Descrizione
Non è alcuno dei seguenti valori	Media	Non genera un'azione di regola di risposta quando si ha la corrispondenza con una regola di rilevamento di gravità media.
È uno qualsiasi dei seguenti valori	Bassa	Genera un'azione di regola di risposta quando si ha la corrispondenza con una regola di rilevamento di gravità bassa.
Non è alcuno dei seguenti valori	Bassa	Non genera un'azione di regola di risposta quando si ha la corrispondenza con una regola di rilevamento di gravità bassa.
È uno qualsiasi dei seguenti valori	Informazioni	Genera un'azione di regola di risposta quando si ha la corrispondenza con una regola di rilevamento di gravità informazioni.
Non è alcuno dei seguenti valori	Informazioni	Non genera un'azione di regola di risposta quando si ha la corrispondenza con una regola di rilevamento di gravità informazioni.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Azioni di regole di risposta

Il capitolo contiene i seguenti argomenti:

- Configurazione dell'azione Aggiungi nota
- Configurazione dell'azione Limita conservazione dati incidenti
- Configurazione del registro a un'azione del server Syslog
- Configurazione dell'azione Invia notifica e-mail
- Configurazione dell'azione di FlexResponse server
- Configurazione dell'azione Imposta attributo
- Configurazione dell'azione Imposta stato
- Configurazione dell'azione di risposta Classifica contenuto Enterprise Vault
- Configurazione dell'azione Archiviazione cloud: aggiungi tag visivo
- Configurazione dell'azione Archiviazione cloud: quarantena
- Configurazione dell'azione di risposta smart Quarantena
- Configurazione dell'azione di risposta smart alla Quarantena SharePoint
- Configurazione dell'azione di risposta smart Ripristina file
- Configurazione dell'azione Interrompi collegamenti nei dati a riposo
- Configurazione dell'azione Azione personalizzata su dati a riposo
- Configurazione dell'azione Elimina dati a riposo
- Configurazione dell'azione Crittografa dati a riposo
- Configurazione dell'azione Esegui DRM su dati a riposo

- Configurazione dell'azione Metti in quarantena dati a riposo
- Configurazione dell'azione Marca dati a riposo
- Configurazione dell'azione Impedisce download, copia, stampa
- Configurazione dell'azione Rimuovi accesso collaboratore
- Configurazione dell'azione Imposta accesso collaboratore in Modifica
- Configurazione dell'azione Imposta accesso collaboratore in Anteprima
- Configurazione dell'azione Imposta accesso collaboratore in Lettura
- Configurazione dell'azione Imposta accesso file in Lettura completa
- Configurazione di Imposta accesso file in Modifica interna
- Configurazione dell'azione Imposta accesso file in Lettura interna
- Configurazione dell'azione Aggiungi autenticazione a due fattori
- Configurazione dell'azione Blocca dati in movimento
- Configurazione dell'azione Azione personalizzata su dati in movimento
- Configurazione dell'azione Crittografia dati in movimento
- Configurazione dell'azione Esegui DRM su dati in movimento
- Configurazione dell'azione Metti in quarantena dati in movimento
- Configurazione dell'azione Cancella dati in movimento
- Configurazione dell'azione Endpoint: FlexResponse
- Configurazione dell'azione Endpoint Discover: metti file in quarantena
- Configurazione dell'azione Endpoint Prevent: blocca
- Configurazione dell'azione Endpoint Prevent: crittografia
- Configurazione dell'azione Endpoint Prevent: notifica
- Configurazione dell'azione Endpoint Prevent: operazione annullata dall'utente
- Configurazione dell'azione Network Prevent for Web: Blocca richiesta FTP
- Configurazione dell'azione Network Prevent for Web: blocca HTTP/HTTPS
- Configurazione dell'azione Network Prevent: blocca messaggio SMTP
- Configurazione dell'azione Network Prevent: modifica messaggio SMTP

- [Configurazione dell'azione Network Prevent for Web: rimuovi contenuto HTTP/HTTPS](#)
- [Configurazione dell'azione Network Protect: copia file](#)
- [Configurazione dell'azione Network Protect: metti file in quarantena](#)
- [Configurazione dell'azione Network Protect: crittografa file](#)

Configurazione dell'azione **Aggiungi nota**

L'azione di regola di risposta **Aggiungi nota** consente a un risponditore di incidenti di digitare una nota relativa a un particolare incidente.

Il limite per il campo **Aggiungi nota** è 4000 byte.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

L'azione di regola di risposta **Aggiungi nota** è disponibile per tutti i tipi di server di rilevamento.

Vedere ["Azioni delle regole di risposta per tutti i server di rilevamento"](#) a pagina 1469.

Per configurare l'azione **Aggiungi nota**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Aggiungere il tipo di azione **Tutto: aggiungi nota** dall'elenco **Azioni**.

Il sistema visualizza un campo **Nota**. In genere, si lascia il campo vuoto e si consente ai riparatori di aggiungere commenti quando valutano gli incidenti. È tuttavia possibile aggiungere commenti anche a questo livello della configurazione.

Il limite per il campo **Aggiungi nota** è 4000 byte.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Fare clic su **Salva** per salvare la configurazione.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione **Limita conservazione dati incidenti**

L'azione della regola di risposta **Limita conservazione dati incidenti** consente di modificare il comportamento predefinito relativo alla conservazione dei dati degli incidenti del server di rilevamento.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa regola di risposta è disponibile per tutti i tipi di server di rilevamento.

Vedere ["Azioni delle regole di risposta per tutti i server di rilevamento"](#) a pagina 1469.

Per configurare la conservazione dei dati degli incidenti

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Aggiungere il tipo di azione **Tutto: limita conservazione dati incidenti** dall'elenco **Azioni**.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Scegliere di conservare i dati degli incidenti degli endpoint selezionando questa opzione.

Per impostazione predefinita, l'agente elimina il messaggio originale e tutti gli allegati per gli incidenti endpoint.

Vedere ["Conservazione dei dati per gli incidenti degli endpoint"](#) a pagina 1511.

- 4 Scegliere di scartare i dati degli incidenti di rete selezionando questa opzione.

Per impostazione predefinita, il sistema conserva il messaggio originale e tutti gli allegati per gli incidenti di rete.

Vedere ["Eliminazione dei dati per gli incidenti di rete"](#) a pagina 1512.

- 5 Fare clic su **Salva** per salvare la configurazione della regola di risposta.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Conservazione dei dati per gli incidenti degli endpoint

Per impostazione predefinita, il sistema elimina i messaggi originali (inclusi file e allegati) relativi agli incidenti degli endpoint. È possibile implementare l'azione della regola di risposta Limita conservazione dati incidenti per ignorare questo comportamento predefinito e conservare gli allegati di e-mail originali per gli incidenti degli endpoint.

Nota: Limita conservazione dati incidenti non è valida per incidenti di stampa o degli Appunti degli endpoint.

Vedere ["Configurazione dell'azione Limita conservazione dati incidenti"](#) a pagina 1510.

Tabella 45-1 Conservazione dei dati per gli incidenti degli endpoint

Parametro	Descrizione
Tutti gli incidenti di endpoint (compresi gli incidenti di Endpoint Discover)	Selezionare questa opzione per conservare i file allegati originali per gli incidenti Endpoint Prevent e gli incidenti acquisiti da Endpoint Discover mediante un target endpoint.

Se si combina una regola di rilevamento lato server (EDM/IDM/DGM) con un'azione della regola di risposta Limita conservazione dati incidenti sull'endpoint, tenere presenti gli aspetti di utilizzo della larghezza di banda della rete. Quando un Endpoint Agent invia il contenuto a un Endpoint Server per l'analisi, invia testo o dati binari a seconda dei requisiti di rilevamento. Se possibile, i Symantec DLP Agent inviano testo per ridurre l'uso di larghezza di banda. Quando si conservano i messaggi originali degli incidenti endpoint, il sistema richiede sempre agli agenti di inviare dati binari a Endpoint Server. Pertanto verificare che la rete sia in grado di gestire l'incremento del traffico tra agenti di endpoint e Endpoint Server senza compromettere le prestazioni.

Vedere ["Rilevamento in due fasi per DLP Agent."](#) a pagina 403.

Tenere presente l'effetto sul sistema di qualsiasi politica che combina una regola di rilevamento lato agente (qualsiasi regola DCM, ad esempio una regola parola chiave). Se si implementa l'azione della regola di risposta Limita conservazione dati incidenti, l'incremento dell'utilizzo di larghezza di banda dipende dal numero di incidenti con i quali il motore di rilevamento rileva una corrispondenza. Per tali politiche, l'agente di endpoint non invia tutti i file originali a Endpoint Server, ma solo quelli associati a incidenti confermati. Se il numero di incidenti è piccolo, l'effetto è ridotto.

Eliminazione dei dati per gli incidenti di rete

Per impostazione predefinita, per gli incidenti di rete il server di rilevazione conserva il messaggio originale ed eventuali allegati che attivano un incidente.

È possibile implementare l'azione della regola di risposta Limita conservazione dati incidenti per ignorare il comportamento predefinito ed eliminare i messaggi originali e alcuni o tutti gli allegati.

Vedere ["Configurazione dell'azione Limita conservazione dati incidenti"](#) a pagina 1510.

Nota: il comportamento di conservazione dei dati predefinito per gli incidenti di rete si applica agli incidenti di Network Prevent for Web e Network Prevent for Email. Il comportamento predefinito non è applicabile agli incidenti di Network Discover. Per gli incidenti di Network Discover, il sistema fornisce un collegamento in **Istantanea incidente** che punta al file di errore nella posizione originale. La conservazione dei dati degli incidenti per Network Discover non è configurabile.

Tabella 45-2 Eliminazione dei dati degli incidenti di rete

Parametro	Descrizione
Ignora messaggio originale	Selezionare questa opzione per ignorare il messaggio originale. Utilizzare questa configurazione per liberare spazio su disco quando si è interessati solo ai dati statistici.
Ignora allegato	Selezionare Tutti per ignorare tutti gli allegati del messaggio. Selezionare Allegati senza violazioni per salvare solo gli allegati del messaggio pertinenti, ovvero quelli che attivano una violazione della politica. Nota: per questa opzione di azione è necessario selezionare qualcosa di diverso da Nessuno . Se si lascia Nessuno selezionato e non si seleziona la casella accanto a Ignora messaggio originale , l'azione non sortisce alcun effetto. Tale configurazione duplica il comportamento di conservazione dei dati degli incidenti predefinito per i server di rete.

Configurazione del registro a un'azione del server Syslog

L'azione della regola di risposta Registrazione a un server Syslog registra l'incidente su un server di syslog. Questi registri possono essere utili se si utilizza un sistema di informazioni di sicurezza e gestione di eventi (SIEM).

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione della regola di risposta è disponibile per tutti i tipi di server di rilevamento.

Vedere ["Azioni delle regole di risposta per tutti i server di rilevamento"](#) a pagina 1469.

Nota: Si usa questa regola di risposta insieme con un server Syslog. Vedere ["Attivazione di un server syslog"](#) a pagina 182.

Configurazione dell'azione della regola di risposta Registrazione a un server Syslog

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Registrazione a un server Syslog** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Inserire il nome **Host** del server Syslog.
- 4 Modificare la **Porta** del server Syslog, se necessario.
La porta predefinita è **514**.

- 5 Digitare il testo del **Messaggio** per registrarsi al server Syslog.
È possibile includere le variabili di azione di risposta nei messaggi del server Syslog.
Vedere ["Variabili azione di risposta"](#) a pagina 1576.
- 6 Selezionare il **Livello** da applicare al messaggio di registrazione dall'elenco a discesa.
Sono disponibili le seguenti opzioni:
 - 0 - Kernel Panic
 - 1 - Necessita di attenzione immediata
 - 2 - Condizione critica
 - 3 - Errore
 - 4 - Avviso
 - 5 - Potrebbe necessitare di attenzione
 - 6 - Informativo
 - 7 - Debug
- 7 **Salva** la regola di risposta.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Invia notifica e-mail

L'azione Invia notifica e-mail consente di comporre un'e-mail e inviarla ai destinatari specificati.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione della regola di risposta è disponibile per tutti i tipi di server di rilevamento.

Vedere ["Azioni delle regole di risposta per tutti i server di rilevamento"](#) a pagina 1469.

È necessario integrare l'Enforce Server con un server di e-mail SMTP per implementare l'azione di questa regola di risposta.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Per configurare l'azione della regola di risposta Invia notifica e-mail

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Tutto: invia notifica e-mail** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Configurare destinatari, mittente, formato, inclusione incidente e messaggi al giorno.
Vedere [Tabella 45-3](#) a pagina 1515.
- 4 Configurare il **Contenuto della notifica** dell'e-mail di notifica: lingua, oggetto, corpo.
Vedere [Tabella 45-4](#) a pagina 1515.
- 5 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-3 Informazioni sul destinatario e il mittente

Parametro	Descrizione
A: Mittente	Selezionare questa opzione per inviare la notifica e-mail al mittente dell'e-mail. Il destinatario si applica solo alle violazioni dei messaggi di e-mail.
A: Proprietario dati	Selezionare questa opzione per inviare la notifica e-mail al proprietario dei dati che il sistema identifica dall'indirizzo e-mail nell'incidente. Vedere "Istantanea incidente di Discover" a pagina 1615.
A: Altro indirizzo di e-mail	Questa opzione può includere gli attributi personalizzati designati come indirizzi e-mail (ad esempio "manager@email"). Ad esempio, se si definisce un attributo personalizzato che è un indirizzo e-mail o se ne recupera uno tramite un plug-in di ricerca, quell'indirizzo verrà visualizzato nel campo "A" per la selezione, a destra di "A: Mittente" e "A: Proprietario dati". Vedere "Configurazione di attributi personalizzati" a pagina 1709.
Personalizza a	Immettere uno o più indirizzi e-mail specifici separati da virgole.
CC	Immettere uno o più indirizzi e-mail specifici separati da virgole per le persone a cui inviare una copia della notifica.
Personalizza da	È possibile specificare il mittente del messaggio. Se questo campo è vuoto, il messaggio risulta inviato dall'indirizzo e-mail di sistema.
Formato notifica	Selezionare HTML o testo non formattato.
Includi messaggio originale	Selezionare questa opzione per includere il messaggio che ha generato l'incidente nella notifica e-mail.
Max per giorno	Immettere un numero per limitare il numero massimo di notifiche che il sistema invia in un giorno.

Tabella 45-4 Contenuto notifica

Parametro	Descrizione
Lingua	Selezionare la lingua per il messaggio dal menu a discesa.

Parametro	Descrizione
Aggiungi lingua	Fare clic sull'icona per aggiungere più lingue per il messaggio. Vedere "Informazioni sulle regole di risposta di Endpoint Prevent con impostazioni locali differenti" a pagina 2078.
Oggetto	Immettere l'oggetto del messaggio che indica il contenuto del messaggio.
Corpo	Immettere il corpo del messaggio.
Inserisci variabile	<p>È possibile aggiungere una o più variabili all'oggetto o al corpo del messaggio e-mail selezionando il valore desiderato dall'elenco Inserisci variabile.</p> <p>Le variabili possono essere utilizzate per includere nome del file, nome della politica, destinatari e mittente sia nell'oggetto che nel corpo del messaggio di e-mail. Ad esempio, se si desidera includere la politica e le regole violate, inserire le seguenti variabili:</p> <p>Un messaggio ha violato le seguenti regole in \$POLICY\$: \$RULES\$</p> <p>Vedere "Variabili azione di risposta" a pagina 1576.</p>

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione di FlexResponse server

L'azione **Tutto: FlexResponse server** consente di risolvere qualsiasi tipo di incidente con un plug-in di FlexResponse lato server personalizzato. È possibile configurare un'azione di risposta di FlexResponse server per le regole di risposta automatiche o le regole di risposta smart.

L'azione **Tutto: FlexResponse server** è disponibile solo se si è concesso in licenza Network Protect e si sono distribuiti uno o più plug-in di FlexResponse server a Symantec Data Loss Prevention.

Vedere ["Distribuzione di un plug-in di FlexResponse server"](#) a pagina 1888.

Per configurare un'azione di FlexResponse server

- 1 Accedere alla console di amministrazione di Enforce Server.
- 2 Creare una nuova regola di risposta per ciascun plug-in di FlexResponse server personalizzato.
Fare clic su **Gestisci > Politiche > Regole di risposta**.
- 3 Fare clic su **Aggiungi regola di risposta**.
- 4 Selezionare **Risposta automatica** o **Risposta smart**. Fare clic su **Avanti**.
- 5 Immettere un nome per la regola nel campo **Nome regola**. (Per le regole di risposta smart, questo nome viene visualizzato come etichetta del pulsante che i risponditori agli incidenti selezionano durante la risoluzione.)

- 6 Immettere una descrizione opzionale per la regola nel campo **Descrizione**.
- 7 Nel menu **Azioni (eseguite nell'ordine mostrato)** selezionare l'azione **Tutto: FlexResponse server**.
- 8 Fare clic su **Aggiungi azione**.
- 9 Nel menu **Plug-in FlexResponse** selezionare un plug-in di FlexResponse server distribuito da eseguire con questa azione della regola di risposta.

Il nome visualizzato in questo menu a discesa è il valore specificato nella proprietà `display-name` nel file delle proprietà di configurazione o nella classe di metadati del plug-in.

Vedere ["Distribuzione di un plug-in di FlexResponse server"](#) a pagina 1888.

Nota: Se la licenza di Network Protect ICE è installata ed Enforce Server è stato configurato per connettersi al cloud Symantec ICE, è possibile utilizzare l'azione di regola di risposta **SharePoint Encrypt** resa disponibile con un plug-in di FlexResponse server per la crittografia installato automaticamente con Symantec Data Loss Prevention. Non sono necessarie configurazioni o personalizzazioni aggiuntive per il plug-in di crittografia.

- 10 Fare clic su **Salva**.
- 11 Ripetere questa procedura aggiungendo una regola di risposta per eventuali plug-in di FlexResponse server aggiuntivi che si sono distribuiti.

Configurazione dell'azione Imposta attributo

L'azione della regola di risposta Imposta attributo imposta lo stato dell'incidente sul valore specificato.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione della regola di risposta è disponibile per tutti i server di rilevamento.

Vedere ["Azioni delle regole di risposta per tutti i server di rilevamento"](#) a pagina 1469.

L'azione Imposta attributo è basata sugli attributi personalizzati definiti nella schermata **Sistema > Dati incidente > Attributi**.

Vedere ["Informazioni sugli attributi personalizzati"](#) a pagina 1706.

Per configurare l'azione Imposta attributo

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
 - 2 Aggiungere il tipo di azione **Tutto: imposta attributo** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
 - 3 Selezionare **Attributo** dall'elenco a discesa (se sono definiti più attributi personalizzati).
 - 4 Immettere lo stato di incidente **Valore** per l'attributo personalizzato selezionato.
 - 5 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
- Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Imposta stato

L'azione di regola di risposta Imposta stato imposta lo stato dell'incidente sul valore specificato.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa regola di risposta è disponibile per tutti i server di rilevamento.

Vedere ["Azioni delle regole di risposta per tutti i server di rilevamento"](#) a pagina 1469.

Questa azione di regola di risposta è basata sui **valori di stato** dell'incidente configurati nella schermata **Sistema > Dati incidente > Attributi**.

Vedere ["Informazioni sugli attributi di stato incidente."](#) a pagina 1700.

Per configurare l'azione di regola di risposta Imposta stato

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Tutto: imposta stato** dall'elenco **Azioni**.
- 3 Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 4 Selezionare lo **stato** da assegnare all'incidente dall'elenco.
Di seguito sono elencati alcuni stati di incidente di esempio che è possibile configurare e selezionare:
 - Nuovo
 - Riassegnato
 - Analisi
 - Risolto

- Ignorato

5 Fare clic su **Salva** per salvare la configurazione.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione di risposta **Classifica contenuto Enterprise Vault**

La regola di risposta **Classificazione: classifica contenuto Enterprise Vault** definisce i tag del risultato della classificazione che un server di classificazione genera per un messaggio Exchange che corrisponde a una politica di rilevamento. Il server di classificazione consegna la categoria di conservazione e il tag di classificazione al filtro Data Classification for Enterprise Vault che ha consegnato il messaggio per il rilevamento. Il tag di classificazione corrisponde sempre al nome della politica che ha generato l'azione di regola di risposta.

Symantec Enterprise Vault for Microsoft Exchange può quindi usare la categoria di conservazione e il tag di classificazione per eseguire l'archiviazione, eliminare messaggi o contrassegnare il messaggio per le revisioni di conformità o le ricerche con e-discovery.

Per configurare l'azione di regola di risposta **Classifica contenuto Enterprise Vault**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta (Gestisci > Regole di risposta)**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Aggiungere il tipo di azione **Classificazione: classifica contenuto Enterprise Vault** dall'elenco **Azioni**.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Configurare i parametri per classificare il messaggio di Enterprise Vault.

Vedere [Tabella 45-5](#) a pagina 1519.

- 4 Fare clic su **Salva** per salvare la configurazione.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-5 Parametri di Classificazione: classifica contenuto Enterprise Vault

Parametro	Descrizione
Archivia e classifica messaggio	Selezionare questa opzione per indicare che Symantec Enterprise Vault deve archiviare il messaggio corrispondente alla regola di rilevamento. Se si seleziona questa opzione, usare anche il menu Assegna categoria di conservazione per specificare la categoria di conservazione che Enterprise Vault assegna.

Parametro	Descrizione
Assegna categoria di conservazione	<p>Il menu Assegna categoria di conservazione elenca tutte le categorie di conservazione configurate per l'uso con la soluzione Data Classification for Enterprise Vault. Se si configura la regola di risposta per archiviare un messaggio, selezionare anche la categoria di conservazione appropriata da questo menu.</p> <p>È necessario configurare i nomi delle categorie di conservazione in questo menu per la corrispondenza con le categorie disponibili nei server Enterprise Vault.</p> <p>Vedere "Configurazione delle categorie di conservazione disponibili per la classificazione" a pagina 1521.</p> <p>Se si seleziona Non sostituire categoria di conservazione, il server di classificazione comunica a Enterprise Vault che nessuna categoria di conservazione è stata assegnata. Enterprise Vault utilizza la categoria di conservazione già disponibile per il messaggio e la applica durante il processo di archiviazione.</p> <p>Quando si configura una regola di risposta, se non si seleziona il tipo di classificazione di tale regola, Enterprise Vault non può ricevere alcuna risposta dai servizi Symantec Enterprise Vault Data Classification. Enterprise Vault applica la categoria di conservazione già disponibile per il messaggio. Se la politica associata era eseguita in modalità di prova, l'incidente viene generato, ma Enterprise Vault non riceve alcuna risposta dal server di classificazione. Nemmeno i registri della modalità di prova di Enterprise Vault sono aggiornati.</p>
Revisione conformità	<p>Se si configura la regola di risposta per l'archiviazione del messaggio, è anche possibile selezionare Definisci priorità messaggio per revisione di conformità per definire la priorità del messaggio per la revisione. I prodotti Discovery Accelerator e Compliance Accelerator possono usare questo tag di classificazione per filtrare i messaggi durante le ricerche o i controlli.</p> <p>Quando si seleziona questa opzione, si hanno a disposizione due scelte supplementari:</p> <ul style="list-style-type: none"> ■ Includi nella revisione - Include il messaggio nelle ricerche e nei controlli successivi. ■ Escludi dalla revisione - Esclude il messaggio dalle ricerche e dai controlli successivi. <p>Consultare la documentazione di Discovery Accelerator e Compliance Accelerator per ulteriori informazioni sulla ricerca e sul controllo di messaggi in Enterprise Vault.</p>

Parametro	Descrizione
Non archiviare il messaggio	<p>Scegliere questa opzione per indicare che Symantec Enterprise Vault deve archiviare il messaggio corrispondente alla regola di rilevamento.</p> <p>Quando si seleziona questa opzione, vengono visualizzate le opzioni seguenti per specificare il modo in cui Enterprise Vault deve ignorare il messaggio:</p> <ul style="list-style-type: none"> ■ Elimina il messaggio subito e in modo permanente - Enterprise Vault deve eliminare immediatamente il messaggio. ■ Sposta il messaggio nella cartella della Posta eliminata - Enterprise Vault deve spostare il messaggio nella cartella della Posta eliminata. Il messaggio può essere eliminato in un secondo momento dopo che la cartella è stata svuotata. ■ Lascia messaggio nella cassetta postale - Enterprise Vault deve lasciare il messaggio nella cassetta postale e contrassegnarlo con "Do not archive". <p>Se si seleziona questa opzione ma in seguito si decide di eliminare la proprietà "Do not archive", è possibile farlo impostando i valori del registro ClearDoNotJournal e ClearDoNotArchive nel server Enterprise Vault. Per istruzioni, vedere il manuale relativo ai <i>valori del registro di Enterprise Vault</i>. Questi valori consentono alle attività di inserimento nel diario e alla cassetta postale di Exchange di archiviare i messaggi.</p> <p>Nota: Quando si controlla una cassetta postale diario, è possibile vedere i messaggi contrassegnati con "Do not archive" nella posta in arrivo del diario e nella cartella Posta eliminata. I messaggi contrassegnati con "Do not archive" non vengono spostati automaticamente. È possibile spostare manualmente i messaggi nella cartella della Posta eliminata.</p>

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione delle categorie di conservazione disponibili per la classificazione

La regola di risposta **Classificazione: classifica contenuto Enterprise Vault** definisce i tag del risultato della classificazione che un server di classificazione genera per un messaggio Exchange che corrisponde a una politica di rilevamento. Se si configura questa regola di risposta per eseguire l'azione **Archivia e classifica messaggio**, specificare anche la categoria di conservazione che Enterprise Vault deve applicare al messaggio archiviato. L'elenco di categorie di conservazione disponibili visualizzato nella console di amministrazione di Enforce Server viene definito con un file di configurazione, `RetentionCategories.config`.

Vedere ["Configurazione dell'azione di risposta Classifica contenuto Enterprise Vault"](#) a pagina 1519.

Quando si installa per la prima volta la soluzione dei servizi Data Classification, è necessario creare un file `RetentionCategories.config` per includere le categorie di conservazione disponibili nei server Enterprise Vault. Se si modificano le categorie di conservazione disponibili in una distribuzione Enterprise Vault, è inoltre necessario modificare manualmente le categorie disponibili definite in `RetentionCategories.config`.

Nota: il file `RetentionCategories.config` supporta la codifica dei caratteri UTF-8 senza contrassegno di ordine byte (BOM).

Per configurare le categorie di conservazione disponibili per la classificazione

- 1 Uno ogni server Enterprise Vault, eseguire l'utilità della riga di comando `ExportRetentionCategories.exe` installata nella cartella del programma Enterprise Vault. (Per visualizzare le istruzioni per l'uso, eseguire l'utilità senza fornire alcuna opzione della riga di comando.) È necessario aprire l'utilità della riga di comando di un utente con privilegi dell'amministratore.
- 2 Seguire le istruzioni visualizzate sullo schermo per generare un file che elenca le categorie di conversazione disponibili nel server Enterprise Vault. Le categorie di conservazione riportate di seguito vengono sempre escluse dal file:
 - Categorie di conservazione per le cartelle gestite
 - Per le distribuzioni inglesi, la categoria di conservazione con il nome **<Do not override retention category>** non applica una nuova categoria di conservazione. Durante il processo di archiviazione viene invece applicata una categoria di conservazione già disponibile per il messaggio.

Si tenga presente che le categorie di conservazione nascoste sono incluse nel file risultante.
- 3 Ripetere i passaggi 1 e 2 per ogni server Enterprise Vault nella distribuzione.
- 4 Se si sono generati file per più server Enterprise Vault, utilizzare un editor di testo per unire i contenuti di ciascun file in un singolo file.
- 5 Assegnare al file che contiene tutte le categorie di conservazione il nome `RetentionCategories.config`.
- 6 Accedere al computer di Enforce Server utilizzando i privilegi di amministratore o super utente.

- 7 Copiare il file `RetentionCategories.config` che si è creato nella sottodirectory `config` della directory di installazione del prodotto Symantec Data Loss Prevention. La directory predefinita è `c:\SymantecDLP\Protect\config`.
- 8 Riavviare Enforce Server per applicare le modifiche.
Vedere ["Controlli server"](#) a pagina 242.

Per informazioni sull'avvio e sull'arresto dei servizi di Symantec Data Loss Prevention consultare il *Manuale dell'amministratore di Symantec Data Loss Prevention*.

Configurazione dell'azione Archiviazione cloud: aggiungi tag visivo

L'azione della regola Aggiungi tag visivo consente a un risponditore incidenti di applicare tag visivi come metadati al contenuto sensibile archiviato nel target di archiviazione cloud Box. Il tag visivo aiuta gli utenti dell'archiviazione cloud Box a cercare e riparare autonomamente i dati sensibili. Ad esempio, si potrebbe desiderare che il tag legga "Questo contenuto è considerato confidenziale". È inoltre possibile ricordare loro delle ulteriori funzionalità di sicurezza di Box, come l'aggiunta della protezione con password a qualsiasi collegamento di download.

Per configurare l'azione Archiviazione cloud: aggiungi tag visivo

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Archiviazione cloud: aggiungi tag visivo** dall'elenco **Azioni**.
Il sistema mostra il campo **Aggiungi tag visivo**. Immettere il testo da visualizzare nel tag per gli utenti.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Archiviazione cloud: quarantena

L'azione della regola di risposta **Archiviazione cloud: quarantena** mette in quarantena il contenuto che il server di rilevamento identifica come riservato o protetto.

Per configurare l'azione Archiviazione cloud: quarantena

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Archiviazione cloud: quarantena** dall'elenco **Azioni**.
Il sistema visualizza il campo **Archiviazione cloud: quarantena**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare i parametri **Archiviazione cloud: quarantena**.
Vedere [Tabella 45-6](#) a pagina 1524.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-6 Parametri di configurazione di Archiviazione cloud: file in quarantena

Parametro	Descrizione
File marker	<p>Selezionare Lascia file marker al posto del file riparato per creare un file di testo marker al fine di sostituire il file originale. Questa azione informa l'utente in merito a quanto è accaduto al file invece di metterlo in quarantena o eliminarlo senza spiegazione.</p> <p>Nota: Il file marker è dello stesso tipo e ha lo stesso nome del file originale, purché sia un file di testo. Un esempio di questo tipo di file è Microsoft Word. Se il file originale è un PDF o un file di immagini, il sistema crea un file marker di testo semplice. Il sistema assegna poi al file lo stesso nome del file originale con .txt aggiunto alla fine. Ad esempio, se il nome del file originale è accounts.pdf, il nome del file marker è accounts.pdf.txt.</p>
Testo marker	<p>Specificare il testo che deve essere visualizzato nel file marker. Se è stata selezionata l'opzione per lasciare il file marker al posto del file riparato, è possibile utilizzare delle variabili nel testo del marker.</p> <p>Per specificare il testo del marker, selezionare la variabile dall'elenco Inserisci variabile.</p> <p>Ad esempio, per Testo marker è possibile immettere il seguente testo:</p> <p>Un messaggio ha violato le seguenti regole in \$POLICY\$: \$RULES</p> <p>In alternativa, è possibile immettere:</p> <p>\$FILE_NAME\$ è stato spostato in \$QUARANTINE_PARENT_PATH\$</p>
Aggiungi tag visivo al file marker	<p>Selezionare questa opzione per aggiungere un tag visivo al file marker. Il tag visivo aiuta gli utenti dell'archiviazione cloud Box a cercare file marker per dati riservati in quarantena</p>
Tag	<p>Immettere il testo del tag visivo in questo campo.</p>

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione di risposta smart Quarantena

L'azione di risposta smart **Quarantena** mette in quarantena i file nelle applicazioni cloud Salesforce, Box e OneDrive tramite il connettore servizio cloud. Il percorso di quarantena è relativo alla cartella principale dell'utente.

Per configurare l'azione di risposta smart Quarantena

- 1 Configurare una regola di risposta smart nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Quarantena** dall'elenco **Azioni**.
Il sistema visualizza il campo **Quarantena**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare i parametri di **Quarantena**.
Vedere [Tabella 45-7](#) a pagina 1525.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-7 Parametri di configurazione di Quarantena (risposta smart)

Parametro	Descrizione
Percorso file	Immettere il percorso file per la posizione di quarantena. Questo percorso file è relativo alla cartella principale dell'utente.
Utilizza file marker	Selezionare Utilizza file marker per creare un file di testo marker al fine di sostituire il file originale. Questa azione informa l'utente in merito a cosa è accaduto al file invece di mettere quest'ultimo in quarantena ed eliminarlo senza spiegazione.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione di risposta smart alla Quarantena SharePoint

L'azione di risposta smart Quarantena SharePoint mette in quarantena i file che vengono memorizzati negli archivi Microsoft SharePoint.

La funzionalità di quarantena è supportata nello stesso sito SharePoint del file sottoposto a scansione e anche in altre posizioni SharePoint, tra cui altri archivi SharePoint. Tuttavia, il

rilascio dalla quarantena è supportato solo all'interno dello stesso sito SharePoint del file in quarantena.

Note:

- Per mettere in quarantena file di SharePoint utilizzando Network Protect, gli utenti esistenti devono prima disinstallare il plug-in Symantec Data Loss Prevention SharePoint Quarantine FlexResponse.
- Per sbloccare file SharePoint riservati dalla quarantena, si deve proseguire con l'installazione della versione di SharePoint Symantec Data Loss Prevention dal plug-in Quarantine FlexResponse.
- Per informazioni sull'installazione e la disinstallazione dei plug-in FlexResponse, fare riferimento alla *Symantec Data Loss Prevention Guida all'implementazione del plug-in SharePoint Quarantine FlexResponse*

Per configurare l'azione di risposta smart Quarantena SharePoint

- 1 Configurare una regola di risposta smart nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Quarantena SharePoint Network Protect** dall'elenco **Azioni**.
Il sistema mostra il campo **Quarantena SharePoint Network Protect**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare i parametri di **Quarantena SharePoint Network Protect**.
Vedere [Tabella 45-8](#) a pagina 1526.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-8 Parametri di quarantena SharePoint Network Protect

Parametro	Descrizione
Origine	
Usa credenziali salvate	<p>Selezionare Usa credenziali salvate per scegliere una credenziale denominata dall'archivio credenziali nel menu a discesa Usa credenziali salvate se non si desidera immetterla manualmente.</p> <p>Per spostare i file per la quarantena durante la riparazione, l'account utente di SharePoint specificato deve avere accesso in scrittura alla posizione del file originale.</p>

Parametro	Descrizione
Usa queste credenziali	<p>Selezionare Usa queste credenziali per immettere manualmente le credenziali di accesso in scrittura per la posizione del file originale sottoposto a scansione. Quindi, immettere le seguenti informazioni: parametri</p> <ul style="list-style-type: none"> ■ Nome: il nome utente dell'account con accesso in scrittura alla posizione del file sottoposto a scansione. ■ Password: la password dell'account con accesso in scrittura alla posizione del file sottoposto a scansione. ■ Conferma Password: confermare la password dell'account con accesso in scrittura alla posizione del file sottoposto a scansione. <p>Per spostare i file per la quarantena durante la riparazione, l'account utente di SharePoint specificato deve avere accesso in scrittura alla posizione del file originale.</p>
Destinazione	
Percorso quarantena	Immettere il percorso di SharePoint in si devono mettere in quarantena i file riservati.
Usa credenziali salvate	<p>Selezionare Usa credenziali salvate per scegliere una credenziale con nome per la posizione di quarantena dall'archivio credenziali nel menu a discesa Usa credenziali salvate se non si desidera immetterla manualmente.</p> <p>Per spostare i file per la quarantena durante la riparazione, l'account utente di SharePoint specificato deve avere accesso in scrittura alla posizione della quarantena.</p>
Usa queste credenziali	<p>Selezionare Usa queste credenziali per immettere manualmente le credenziali di accesso in scrittura per la posizione di quarantena. Quindi, immettere le seguenti informazioni: parametri</p> <ul style="list-style-type: none"> ■ Nome: il nome utente dell'account con accesso in scrittura alla posizione di quarantena. ■ Password: la password dell'account con accesso in scrittura alla posizione di quarantena. ■ Conferma Password: confermare la password dell'account con accesso in scrittura alla posizione di quarantena. <p>Per spostare i file per la quarantena durante la riparazione, l'account utente di SharePoint specificato deve avere accesso in scrittura alla posizione della quarantena.</p>
File marker	
(Facoltativo) Lascia file marker al posto del file riparato	Selezionare Lascia file marker al posto del file riparato per creare un file di testo marker al fine di sostituire il file originale. Questa azione informa l'utente in merito a cosa è accaduto al file anziché spostarlo senza spiegazione.

Parametro	Descrizione
(Facoltativo) Testo marker	Specificare il testo che viene visualizzato nel file marker per informare gli utenti di quanto è accaduto al file che è stato messo in quarantena. Il testo del marker può contenere variabili sostitutive. Far clic all'interno della casella Testo marker per visualizzare un elenco di variabili di inserimento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione di risposta smart Ripristina file

L'azione di risposta smart **Ripristina file** ripristina un file in quarantena nelle applicazioni cloud Salesforce, Box e OneDrive tramite il connettore servizio cloud.

Per configurare l'azione di risposta smart **Ripristina file**

- 1 Configurare una regola di risposta smart nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Ripristina file** dall'elenco **Azioni**.
Il sistema visualizza il campo **Ripristina file**.
- 3 Fare clic su **Salva** per salvare la configurazione.
- 4 Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Interrompi collegamenti nei dati a riposo

L'azione **Interrompi collegamenti nei dati a riposo** interrompe i collegamenti ai dati riservati nelle seguenti applicazioni cloud attraverso il connettore servizio cloud:

- Salesforce
- Box
- Dropbox
- OneDrive
- SharePoint
- Google Drive

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione Interrompi collegamenti nei dati a riposo

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Interrompi collegamenti nei dati a riposo** dall'elenco **Azioni**.
Il sistema visualizza il campo **Interrompi collegamenti nei dati a riposo**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro **Interrompi collegamenti nei dati a riposo**.
Vedere [Tabella 45-9](#) a pagina 1529.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-9 Parametro di configurazione Interrompi collegamenti nei dati a riposo

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Interrompi collegamenti nei dati a riposo nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Azione personalizzata su dati a riposo

L'azione **Azione personalizzata su dati a riposo** restituisce una raccomandazione per eseguire qualche azione personalizzata sui dati riservati con il risultato di rilevamento.

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione Azione personalizzata su dati a riposo

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Azione personalizzata su dati a riposo** dall'elenco **Azioni**.
Il sistema visualizza il campo **Azione personalizzata su dati a riposo**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro **Azione personalizzata su dati a riposo**.
Vedere [Tabella 45-10](#) a pagina 1530.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-10 Parametro di configurazione Azione personalizzata su dati a riposo

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Azione personalizzata su dati a riposo nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Elimina dati a riposo

L'azione **Elimina dati a riposo** elimina i dati riservati nell'applicazione cloud Dropbox attraverso il connettore servizio cloud.

Per configurare l'azione Elimina dati a riposo

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
 - 2 Aggiungere il tipo di azione **Elimina dati a riposo** dall'elenco **Azioni**.
Il sistema visualizza il campo **Elimina dati a riposo**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
 - 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
- Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Crittografia dati a riposo

L'azione **Crittografia dati a riposo** crittografa i dati riservati nell'applicazione OneDrive attraverso il connettore servizio cloud.

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione Crittografia dati a riposo

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Crittografia dati a riposo** dall'elenco **Azioni**.
Il sistema visualizza il campo **Crittografia dati a riposo**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro .
Vedere [Tabella 45-11](#) a pagina 1531.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-11 Configurazione del parametro Crittografia dati a riposo

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Crittografia dati a riposo nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Esegui DRM su dati a riposo

L'azione **Esegui DRM su dati a riposo** applica Digital Rights Management (DRM) ai dati riservati nelle applicazioni attraverso il connettore servizio cloud o il dispositivo Rilevamento API per le app degli sviluppatori.

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione **Esegui DRM su dati a riposo**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Esegui DRM su dati a riposo** dall'elenco **Azioni**.
Il sistema visualizza il campo .
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro **Esegui DRM su dati a riposo**.
Vedere [Tabella 45-12](#) a pagina 1532.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-12 Parametro di configurazione Esegui DRM su dati a riposo

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Esegui DRM su dati a riposo nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Metti in quarantena dati a riposo

L'azione **Metti in quarantena dati a riposo** mette in quarantena i dati riservati nelle applicazioni cloud Salesforce, Box e OneDrive attraverso il connettore servizio cloud.

Per configurare l'azione **Metti in quarantena dati a riposo**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Metti in quarantena dati a riposo** dall'elenco **Azioni**.
Il sistema visualizza il campo **Metti in quarantena dati a riposo**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro **Metti in quarantena dati a riposo**.
Vedere [Tabella 45-13](#) a pagina 1533.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-13 Configurazione del parametro Metti in quarantena dati a riposo

Parametro	Descrizione
Percorso file	Immettere il percorso file per la posizione di quarantena. Questo percorso file è relativo alla cartella principale dell'utente.
Utilizza file marker	Selezionare Utilizza file marker per creare un file di testo marker al fine di sostituire il file originale. Questa azione informa l'utente in merito a cosa è accaduto al file invece di mettere quest'ultimo in quarantena ed eliminarlo senza spiegazione.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione **Marca dati a riposo**

L'azione **Marca dati a riposo** marca i dati riservati nelle applicazioni attraverso il connettore servizio cloud o il dispositivo Rilevamento API per le app degli sviluppatori.

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione **Marca dati a riposo**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Marca dati a riposo** dall'elenco **Azioni**.
Il sistema visualizza il campo **Marca dati a riposo**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro **Marca dati a riposo**.
Vedere [Tabella 45-14](#) a pagina 1533.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-14 Configurazione del parametro **Marca dati a riposo**

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Marca dati a riposo nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Impedisci download, copia, stampa

L'azione **Impedisci download, copia, stampa** impedisce il download, la copia o la stampa dei file di dati riservati dall'applicazione cloud Google Drive tramite il connettore servizio cloud.

Per configurare l'azione **Impedisci download, copia, stampa**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Impedisci download, copia, stampa** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Rimuovi accesso collaboratore

L'azione **Rimuovi accesso collaboratore** impedisce ai collaboratori di accedere ai file di dati riservati nelle seguenti applicazioni cloud attraverso il connettore servizio cloud:

- Salesforce
- Box
- Dropbox
- OneDrive
- SharePoint
- Google Drive

Per configurare l'azione **Rimuovi accesso collaboratore**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Rimuovi accesso collaboratore** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Imposta accesso collaboratore in Modifica

L'azione **Imposta accesso collaboratore in Modifica** concede ai collaboratori l'accesso in modifica ai file di dati riservati nelle seguenti applicazioni cloud attraverso il connettore servizio cloud:

- Salesforce
- Box
- Dropbox
- OneDrive
- SharePoint
- Google Drive

Per configurare l'azione **Imposta accesso collaboratore in Modifica**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Imposta accesso collaboratore in Modifica** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Imposta accesso collaboratore in Anteprima

L'azione **Imposta accesso collaboratore in Anteprima** concede ai collaboratori l'accesso in anteprima ai file di dati riservati nell'applicazione cloud Box attraverso il connettore servizio cloud.

Per configurare l'azione **Imposta accesso collaboratore in Anteprima**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Imposta accesso collaboratore in Anteprima** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Imposta accesso collaboratore in Lettura

L'azione **Imposta accesso collaboratore in Lettura** concede ai collaboratori l'accesso in lettura ai file di dati riservati nelle seguenti applicazioni cloud attraverso il connettore servizio cloud:

- Salesforce
- Box
- Dropbox
- OneDrive
- SharePoint
- Google Drive

Per configurare l'azione **Imposta accesso collaboratore in Lettura**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Imposta accesso collaboratore in Lettura** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Imposta accesso file in Lettura completa

L'azione **Imposta accesso file in Lettura completa** concede l'accesso in lettura pubblica ai file di dati riservati nelle applicazioni cloud OneDrive, SharePoint e Google Drive attraverso il connettore servizio cloud.

Per configurare l'azione **Imposta accesso file in Lettura completa**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Imposta accesso file in Lettura completa** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione di Imposta accesso file in Modifica interna

L'azione **Imposta accesso file in Modifica interna** concede a tutti i membri dell'organizzazione l'accesso in modifica ai file riservati nelle seguenti applicazioni cloud attraverso il connettore servizio cloud:

- Salesforce
- Box
- OneDrive
- SharePoint
- Google Drive

Per configurare l'azione Imposta accesso file in Modifica interna

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
 - 2 Aggiungere il tipo di azione **Imposta accesso file in Modifica interna** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
 - 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
- Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Imposta accesso file in Lettura interna

L'azione **Imposta accesso file in Lettura interna** concede a tutti i membri dell'organizzazione l'accesso in lettura ai file di dati riservati nelle seguenti applicazioni cloud attraverso il connettore servizio cloud:

- Salesforce
- Box
- OneDrive
- SharePoint
- Google Drive

Per configurare l'azione Imposta accesso file in Lettura interna

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
 - 2 Aggiungere il tipo di azione **Imposta accesso file in Lettura interna** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
 - 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
- Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione **Aggiungi autenticazione a due fattori**

L'azione **Aggiungi autenticazione a due fattori** aggiunge l'autenticazione a due fattori ai file di dati riservati nelle applicazioni tramite il connettore servizio cloud o il Rilevamento API per le app degli sviluppatori.

Per configurare l'azione **Aggiungi autenticazione a due fattori**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Aggiungi autenticazione a due fattori** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione **Blocca dati in movimento**

L'azione **Blocca dati in movimento** blocca i dati riservati nelle applicazioni tramite il connettore servizio cloud o il dispositivo rilevamento API per le app degli sviluppatori.

È possibile configurare un messaggio per gli utenti per informarli del motivo del blocco dei dati riservati. Il messaggio viene visualizzato nel parametro `message` della risposta di rilevamento.

Per configurare l'azione API REST dati in movimento (DIM)

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Blocca dati in movimento** dall'elenco **Azioni**.
Il sistema visualizza il campo **Blocca dati in movimento**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro **Blocca dati in movimento**.
Vedere [Tabella 45-15](#) a pagina 1540.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-15 Parametro di configurazione Blocca dati in movimento

Parametro	Descrizione
Messaggio	Immettere un messaggio per l'utente per l'azione Blocca dati in movimento nel campo message . Questi dettagli sono restituiti nel parametro <code>message</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Azione personalizzata su dati in movimento

L'azione **Azione personalizzata su dati in movimento** restituisce una raccomandazione per eseguire qualche azione personalizzata sui dati riservati con il risultato di rilevamento.

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione Azione personalizzata su dati in movimento

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Azione personalizzata su dati in movimento** dall'elenco **Azioni**.
Il sistema visualizza il campo **Azione personalizzata su dati in movimento**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro .
Vedere [Tabella 45-16](#) a pagina 1540.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-16 Parametro di configurazione Azione personalizzata su dati in movimento

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Azione personalizzata su dati in movimento nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Crittografia dati in movimento

L'azione **Crittografia dati in movimento** crittografa i dati riservati nell'applicazione cloud Box attraverso il connettore servizio cloud.

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione Crittografia dati in movimento

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Crittografia dati in movimento** dall'elenco **Azioni**.
Il sistema visualizza il campo **Crittografia dati in movimento**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro **Crittografia dati in movimento**.
Vedere [Tabella 45-17](#) a pagina 1541.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-17 Parametro di configurazione Crittografia dati in movimento

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Crittografia dati in movimento nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Esegui DRM su dati in movimento

L'azione **Esegui DRM su dati in movimento** applica Digital Rights Management (DRM) ai dati riservati nelle applicazioni cloud attraverso il connettore servizio cloud.

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione Esegui DRM su dati in movimento

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Esegui DRM su dati in movimento** dall'elenco **Azioni**.
Il sistema visualizza il campo **Esegui DRM su dati in movimento**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare il parametro **Esegui DRM su dati in movimento**.
Vedere [Tabella 45-18](#) a pagina 1542.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-18 Parametro di configurazione Esegui DRM su dati in movimento

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Esegui DRM su dati in movimento nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Metti in quarantena dati in movimento

L'azione **Metti in quarantena dati in movimento** mette in quarantena i dati riservati nelle applicazioni cloud Salesforce, Box e OneDrive attraverso il connettore servizio cloud.

È possibile configurare un payload personalizzato con dettagli aggiuntivi relativi a questa raccomandazione. Il payload personalizzato viene visualizzato nel parametro `customResponsePayload` della risposta di rilevamento.

Per configurare l'azione Metti in quarantena dati in movimento

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Metti in quarantena dati in movimento** dall'elenco **Azioni**.
Il sistema visualizza il campo **Metti in quarantena dati in movimento**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Configurare il parametro **Metti in quarantena dati in movimento**.

Vedere [Tabella 45-19](#) a pagina 1543.

- 4 Fare clic su **Salva** per salvare la configurazione.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-19 Parametro di configurazione Metti in quarantena dati in movimento

Parametro	Descrizione
Payload personalizzato	Immettere i dettagli sull'azione Metti in quarantena dati in movimento nel campo del payload personalizzato. Questi dettagli sono restituiti nel parametro <code>customResponsePayload</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione **Cancella dati in movimento**

L'azione **Cancella dati in movimento** cancella i dati riservati nelle applicazioni tramite il connettore servizio cloud o il dispositivo rilevamento API per le app degli sviluppatori.

È possibile configurare un messaggio per gli utenti per informarli del motivo della cancellazione dei dati riservati. Il messaggio viene visualizzato nel parametro `message` della risposta di rilevamento.

Per configurare l'azione **Cancella dati in movimento**

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Aggiungere il tipo di azione **Cancella dati in movimento** dall'elenco **Azioni**.

Il sistema visualizza il campo **Cancella dati in movimento**.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Configurare il parametro **Cancella dati in movimento**.

Vedere [Tabella 45-20](#) a pagina 1544.

- 4 Fare clic su **Salva** per salvare la configurazione.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-20 Parametro di configurazione Cancella dati in movimento

Parametro	Descrizione
Messaggio	Immettere un messaggio per l'utente per l'azione Cancella dati in movimento nel campo message . Questi dettagli sono restituiti nel parametro <code>message</code> del risultato di rilevamento.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Endpoint: FlexResponse

L'azione della regola di risposta Endpoint: FlexResponse consente di implementare una o più risposte personalizzate sviluppate utilizzando l'API FlexResponse.

Vedere ["Informazioni su Endpoint FlexResponse"](#) a pagina 2248.

Questa regola di risposta è disponibile per Endpoint Discover.

Nota: Questa funzionalità non è disponibile per gli agenti eseguiti su endpoint Mac.

Vedere ["Azioni delle regole di risposta per il rilevamento di endpoint"](#) a pagina 1470.

Per configurare l'azione di regola di risposta Endpoint: FlexResponse

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Endpoint: FlexResponse** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Immettere il **Nome** del plug-in FlexResponse e configurare i **Parametri**.
Vedere [Tabella 45-21](#) a pagina 1544.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-21 Parametri dell'azione della regola di risposta Endpoint: FlexResponse

Parametro	Descrizione
Plug-in Python FlexResponse	Inserire il nome del modulo di script con pacchetti separati da un punto (.).
Parametri del plug-in	Fare clic su Aggiungi parametro per aggiungere uno o più parametri allo script. Immettere la coppia Chiave/Valore per ogni parametro.

Parametro	Descrizione
Credenziali	<p>È possibile aggiungere credenziali per accedere al plug-in.</p> <p>È possibile aggiungere e immagazzinare le credenziali alla schermata di Sistema > Impostazioni > Credenziali.</p> <p>Vedere "Informazioni sull'archivio credenziali" a pagina 167.</p>

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Endpoint Discover: metti file in quarantena

L'azione di regola di risposta Endpoint Discover: metti file in quarantena sposta un file contenente informazioni riservate da una posizione non sicura in una sicura.

Vedere ["Informazioni sulla quarantena di endpoint"](#) a pagina 2088.

Questa azione di regola di risposta è specifica degli incidenti di Endpoint Discover. Questa regola di risposta non è applicabile ai metodi di rilevamento su due livelli che richiedono un profilo dati.

Vedere ["Impostazione e configurazione di Endpoint Discover"](#) a pagina 2089.

Se si utilizzano molteplici regole di risposta endpoint in una singola politica, assicurarsi di comprendere l'ordine di precedenza per tali regole.

Vedere ["Informazioni sulla priorità di esecuzione delle azioni di regola di risposta"](#) a pagina 1481.

Nota: Questa funzionalità non è disponibile per gli agenti eseguiti su endpoint Mac.

Per configurare l'azione Endpoint Discover: metti file in quarantena

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Endpoint Discover: metti file in quarantena** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Immettere il percorso in **Percorso quarantena** e le impostazioni di **File marker**.
Vedere [Tabella 45-22](#) a pagina 1546.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-22 Parametri dell'azione di regola di risposta Endpoint Discover: metti file in quarantena

Parametro	Descrizione
Percorso quarantena	Immettere il percorso alla posizione protetta dove si desidera spostare i file. La posizione protetta può essere sull'unità locale dell'endpoint o una condivisione file remota. Le cartelle EFS possono anche essere usate come posizione di quarantena.
Modalità accesso	<p>Se la posizione sicura è su una condivisione di file remota, è necessario selezionare il modo in cui Symantec DLP Agent vi accede.</p> <p>Selezionare uno dei seguenti tipi di accesso con credenziali:</p> <ul style="list-style-type: none"> ■ Accesso anonimo ■ Usa credenziali salvate <p>In modalità anonima, Symantec DLP Agent viene eseguito come utente LocalSystem per spostare i file riservati. È possibile utilizzare la modalità anonima per spostare file in una posizione sicura su un'unità locale o in una condivisione remota se l'accesso anonimo è consentito.</p> <p>Nota: Le cartelle EFS non accettano gli utenti anonimi.</p> <p>Una credenziale specificata consente a Symantec DLP Agent di impersonare l'utente specificato per accedere alla posizione sicura. Le credenziali devono essere nel formato seguente:</p> <p><code>dominio\utente</code></p> <p>È necessario immettere le credenziali che si desidera usare mediante la pagina delle credenziali di sistema.</p> <p>Vedere "Configurazione delle credenziali endpoint" a pagina 168.</p>
File marker	Selezionare la casella di controllo Lascia file marker al posto del file riparato per creare un file segnaposto che sostituisce il file riservato.
Testo marker	<p>Specificare il testo che deve essere visualizzato nel file marker. Se è stata selezionata l'opzione per lasciare il file marker al posto del file riparato, è possibile utilizzare delle variabili nel testo del marker.</p> <p>Per specificare il testo del marker, selezionare la variabile dall'elenco Inserisci variabile.</p> <p>Ad esempio, per Testo marker è possibile immettere il seguente testo:</p> <p>Un messaggio ha violato le seguenti regole in \$POLICY\$: \$RULES</p> <p>In alternativa, è possibile immettere:</p> <p>\$FILE_NAME\$ è stato spostato in \$QUARANTINE_PARENT_PATH\$</p>

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Vedere ["Azioni delle regole di risposta per il rilevamento di endpoint"](#) a pagina 1470.

Configurazione dell'azione Endpoint Prevent: blocca

L'azione di regola di risposta Endpoint Prevent: blocca impedisce il movimento di dati riservati sull'endpoint e se desiderato visualizza una notifica per l'utente dell'endpoint.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione di regola di risposta è specifica degli incidenti di Endpoint Prevent. Questa regola di risposta non è applicabile ai metodi di rilevamento su due livelli che richiedono un profilo dati.

Vedere ["Impostazione e configurazione di Endpoint Discover"](#) a pagina 2089.

Se si combinano molteplici regole di risposta endpoint in una singola politica, assicurarsi di comprendere l'ordine di precedenza per tali regole.

Vedere ["Informazioni sulla priorità di esecuzione delle azioni di regola di risposta"](#) a pagina 1481.

Nota: L'azione di blocco non è avviata in caso di copia di dati riservati su un'unità locale.

Per configurare l'azione di regola di risposta Endpoint Prevent: blocca

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Endpoint Prevent: blocca** dall'elenco **Azioni**.
- 3 Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 4 Immettere le impostazioni di **Contenuto della notifica di endpoint**.
Vedere [Tabella 45-23](#) a pagina 1547.
- 5 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-23 Parametri dell'azione di regola di risposta Endpoint Prevent: blocca

Parametro	Configurazione
Lingua	<p>Selezionare la lingua per l'esecuzione della regola di risposta. Fare clic su Aggiungi lingua se si desidera aggiungere più di una lingua.</p> <p>Vedere "Informazioni sulle regole di risposta di Endpoint Prevent con impostazioni locali differenti" a pagina 2078.</p> <p>Vedere "Configurazione delle regole di risposta di Endpoint Prevent per differenti impostazioni locali" a pagina 2079.</p>

Parametro	Configurazione
Visualizza finestra di avviso con questo messaggio	<p>Questo campo è facoltativo per le azioni Endpoint: blocca. Selezionare un'azione Endpoint: blocca per visualizzare una notifica per l'utente endpoint quando il sistema blocca un tentativo di copiare dati confidenziali.</p> <p>Immettere il messaggio di notifica nella casella di testo. È possibile aggiungere variabili al messaggio selezionando i valori appropriati nella casella Inserisci variabile.</p> <p>È eventualmente possibile configurare la notifica per includere le giustificazioni dell'utente predefinite come pure un'opzione per consentire agli utenti di immettere una loro giustificazione.</p> <p>È anche possibile aggiungere collegamenti ipertestuali a URL che contengono informazioni sulla sicurezza della società. Per aggiungere collegamenti ipertestuali, si utilizza la sintassi HTML standard, tag e URL. I tag fanno distinzione tra maiuscole e minuscole. È possibile includere il testo dei collegamenti ipertestuali tra il testo normale. Ad esempio, si potrebbe digitare:</p> <p>\$CONTENT_TYPE\$ "\$CONTENT_NAME\$" contiene informazioni riservate. Fare clic qui per informazioni. Contattare l'amministratore in caso di domande.</p>
Inserisci variabile	<p>Selezionare le variabili da includere nella notifica per l'endpoint quando il sistema blocca un tentativo di copiare dati confidenziali.</p> <p>È possibile selezionare variabili basate sui seguenti tipi:</p> <ul style="list-style-type: none"> ■ Applicazione ■ Nome contenuto ■ Tipo di contenuto ■ Tipo di dispositivo ■ Nomi di politica ■ Protocollo ■ Destinatario corrispondente

Parametro	Configurazione
Consenti all'utente di scegliere la spiegazione	<p>Selezionare questa opzione per visualizzare fino a quattro giustificazioni per l'utente nella notifica visualizzata. Quando la notifica compare sull'endpoint, l'utente è tenuto a scegliere una delle giustificazioni. Se si seleziona Consenti all'utente di immettere un testo esplicativo, l'utente può immettere una giustificazione. Symantec Data Loss Prevention fornisce quattro giustificazioni predefinite, che è possibile modificare o rimuovere come necessario.</p> <p>Giustificazione:</p> <ul style="list-style-type: none">■ Formazione utenti■ Processo di business interrotto■ Approvato dal manager■ Falso positivo <p>Ogni voce di giustificazione comprende le seguenti opzioni:</p> <ul style="list-style-type: none">■ Casella di controllo Questa opzione indica se includere la giustificazione associata nella notifica. Per rimuovere una giustificazione, deselezionare la casella di controllo accanto. Per includere una giustificazione, selezionare la casella di controllo accanto.■ Giustificazione L'etichetta di sistema per la giustificazione. Questo valore compare nei report (per scopi di ordinamento e filtro), ma l'utente non lo vede. È possibile selezionare l'opzione desiderata dall'elenco a discesa.■ Opzione presentata all'utente finale Il testo della giustificazione che il sistema visualizza nella notifica. Questo valore compare nei report con l'etichetta di giustificazione. È possibile modificare il testo predefinito come desiderato. <p>Per aggiungere una nuova giustificazione, selezionare Nuova giustificazione dall'elenco a discesa. Nella casella di testo Immettere una nuova giustificazione visualizzata, immettere il nome della giustificazione. Quando si salva la regola, Symantec Data Loss Prevention la include come opzione (in ordine alfabetico) in tutti gli elenchi a discesa di Giustificazione.</p> <p>Nota: È necessario essere selettivi quando si aggiungono nuove giustificazioni. La cancellazione di nuove giustificazioni non è attualmente supportata.</p>
Consenti all'utente di immettere un testo esplicativo	<p>Selezionare questa opzione per includere una casella di testo in cui gli utenti possono immettere la loro giustificazione.</p>

Vedere ["Azioni delle regole di risposta per il rilevamento di endpoint"](#) a pagina 1470.

Vedere ["Recupero dei file riservati negli endpoint Mac"](#) a pagina 2130.

Configurazione dell'azione Endpoint Prevent: crittografia

L'azione di regola di risposta Endpoint Prevent: crittografia visualizza una notifica temporanea quando l'utente tenta di trasferire un file riservato in un dispositivo esterno rimovibile.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Per informazioni sulle limitazioni dell'azione di regola di risposta Endpoint Prevent: crittografia, Vedere ["Best practice per le regole di risposta"](#) a pagina 1487.

Questa azione di regola di risposta è disponibile dopo aver applicato la licenza di Endpoint Prevent ICE.

Per utilizzare questa azione di risposta, assicurarsi di aver configurato le seguenti impostazioni. Se non si configurano le seguenti impostazioni, l'azione di risposta Crittografia blocca il file, anziché crittografarlo.

- La licenza di Endpoint Prevent ICE è applicata ed Enforce Server è configurato per connettersi al cloud Symantec Information Centric Encryption.
Per informazioni su come Symantec Data Loss Prevention interagisce con Symantec ICE, fare riferimento al *Manuale di distribuzione di Symantec Information Centric Encryption*.
Vedere ["Configurazione di Enforce Server per connettersi al cloud ICE Symantec"](#) a pagina 229.
- È necessario attivare le impostazioni di Information Centric Encryption per i DLP Agent nella pagina **Sistema > Agenti > Configurazione agente > Impostazioni**.
Vedere ["Impostazioni dell'agente"](#) a pagina 2126.
Vedere ["Impostazioni di Crittografia incentrata sulle informazioni per i DLP Agent"](#) a pagina 2133.

Nota: Attualmente l'azione Endpoint Prevent: crittografia sottopone automaticamente a crittografia solo i file riservati che vengono copiati o spostati su dispositivi di archiviazione USB 3.0 o nelle applicazioni di archiviazione cloud installate sugli endpoint. Le applicazioni di archiviazione cloud maggiormente utilizzate sono Box, Google Drive, Microsoft OneDrive e altre.

Quando viene rilevata una violazione, DLP Agent crittografa il file, il trasferimento di dati viene completato e viene generato un incidente. Se l'utente non prende una decisione entro il tempo consentito, il trasferimento di dati viene bloccato automaticamente e viene creato un incidente. È possibile fornire un motivo per la notifica come pure opzioni per consentire all'utente endpoint di immettere una giustificazione per l'azione. Questa azione di regola di risposta è disponibile per Endpoint Prevent negli endpoint Windows e Mac.

Vedere ["Come implementare Endpoint Prevent"](#) a pagina 2076.

Per configurare l'azione Endpoint Prevent: crittografia

- 1 Configurare una regola di risposta nella schermata Configura regola di risposta.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
Aggiungere il tipo di azione Endpoint Prevent: crittografia dall'elenco Azioni.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 2 Configurare i parametri di Endpoint Prevent: crittografia.
Vedere [Tabella 45-24](#) a pagina 1551.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-24 Parametri di Endpoint Prevent: crittografia

Parametro	Descrizione
Lingua	Selezionare la lingua per l'esecuzione della regola di risposta. Fare clic su Aggiungi lingua per aggiungere più di una lingua. Vedere "Informazioni sulle regole di risposta di Endpoint Prevent con impostazioni locali differenti" a pagina 2078. Vedere "Configurazione delle regole di risposta di Endpoint Prevent per differenti impostazioni locali" a pagina 2079.
Visualizza finestra di avviso di blocco con questo messaggio	Questo campo è obbligatorio per informare gli utenti che il trasferimento dei dati è stato bloccato. Immettere il messaggio di notifica nella casella di testo. È possibile aggiungere variabili al messaggio selezionando i valori appropriati dalla casella Inserisci variabile . È necessario fare clic su OK per confermare di aver visualizzato l'avviso e ignorare la finestra di dialogo pop-up.
Visualizza finestra di avviso di crittografia con questo messaggio:	Questo campo è obbligatorio per informare gli utenti che il file che hanno tentato di trasferire è stato crittografato. Immettere il messaggio di notifica nella casella di testo. È possibile aggiungere variabili al messaggio selezionando i valori appropriati dalla casella Inserisci variabile . È necessario fare clic su OK per confermare di aver visualizzato l'avviso e ignorare la finestra di dialogo pop-up.

Parametro	Descrizione
Inserisci variabile	<p>Selezionare le variabili che si desidera includere nella notifica visualizzata sullo schermo dell'utente endpoint.</p> <p>È possibile selezionare variabili basate sui seguenti tipi:</p> <ul style="list-style-type: none"> ■ Applicazione ■ Nome contenuto ■ Tipo di contenuto ■ Tipo di dispositivo ■ Nome politica ■ Protocollo ■ Contatore timeout <p>Nota: È necessario utilizzare Contatore timeout per visualizzare quanto tempo rimane prima del blocco del trasferimento di dati.</p>

Parametro	Descrizione
Consenti all'utente di scegliere la spiegazione.	<p>Selezionare questa opzione per visualizzare fino a quattro giustificazioni per l'utente nella notifica visualizzata. Quando la notifica compare sull'endpoint, l'utente è tenuto a scegliere una delle giustificazioni. Se si seleziona Consenti all'utente di immettere un testo esplicativo, l'utente può immettere una giustificazione. Symantec Data Loss Prevention fornisce quattro giustificazioni predefinite, che è possibile modificare o rimuovere in base alle esigenze.</p> <p>Giustificazioni disponibili:</p> <ul style="list-style-type: none"> ■ Processo di business interrotto ■ Falso positivo ■ Approvato dal manager ■ Formazione utenti ■ Personalizzato (nuova giustificazione) <p>Ogni voce di giustificazione comprende le seguenti opzioni:</p> <ul style="list-style-type: none"> ■ Casella di controllo Questa opzione indica se includere la giustificazione associata nella notifica. Per rimuovere una giustificazione, deselezionare la casella di controllo accanto. Per includere una giustificazione, selezionare la casella di controllo accanto. ■ Giustificazione L'etichetta di sistema per la giustificazione. Questo valore compare nei report (per scopi di ordinamento e filtro), ma l'utente non lo vede. È possibile selezionare l'opzione desiderata dall'elenco a discesa. ■ Opzione presentata all'utente finale Il testo della giustificazione visualizzato da Symantec Data Loss Prevention nella notifica. Questo valore compare nei report con l'etichetta di giustificazione. È possibile modificare il testo predefinito come desiderato. <p>Per aggiungere una nuova giustificazione, selezionare Nuova giustificazione dall'elenco a discesa appropriato. Nella casella di testo Immettere una nuova giustificazione visualizzata, digitare il nome della giustificazione. Quando si salva la regola, il sistema include la nuova giustificazione come opzione (in ordine alfabetico) in tutti gli elenchi a discesa di Giustificazione.</p> <p>Nota: È necessario essere selettivi quando si aggiungono nuove giustificazioni. La cancellazione di nuove giustificazioni non è attualmente supportata.</p>
Consenti all'utente di immettere un testo esplicativo	<p>Selezionare questa opzione per includere una casella di testo in cui gli utenti possono immettere la loro giustificazione.</p>

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Endpoint Prevent: notifica

L'azione di regola di risposta Endpoint Prevent: notifica mostra una notifica su schermo all'utente dell'endpoint quando si cerca di copiare o inviare un file contenente dati sensibili. È possibile fornire un motivo per la notifica come pure opzioni per consentire all'utente endpoint di fornire una giustificazione per l'azione.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione di regola di risposta è disponibile per Endpoint Prevent

Vedere ["Come implementare Endpoint Prevent"](#) a pagina 2076.

Nota: L'azione di notifica non è avviata in caso di copia di dati riservati su un'unità locale.

Per configurare l'azione Endpoint Prevent: notifica

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

Aggiungere il tipo di azione **Endpoint Prevent: notifica** dall'elenco **Azioni**.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 2 Configurare i parametri dell'azione.

Vedere [Tabella 45-25](#) a pagina 1554.

- 3 Fare clic su **Salva** per salvare la configurazione.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-25 Parametri dell'azione di regola di risposta Endpoint Prevent: Notifica

Parametro	Descrizione
Lingua	<p>Selezionare la lingua per l'esecuzione della regola di risposta.</p> <p>Fare clic su Aggiungi lingua se si desidera aggiungere più di una lingua.</p> <p>Vedere "Informazioni sulle regole di risposta di Endpoint Prevent con impostazioni locali differenti" a pagina 2078.</p> <p>Vedere "Configurazione delle regole di risposta di Endpoint Prevent per differenti impostazioni locali" a pagina 2079.</p>

Parametro	Descrizione
Visualizza finestra di avviso con questo messaggio	<p>Questo campo è obbligatorio per le azioni Endpoint: notifica Selezionare questa opzione per visualizzare una notifica sullo schermo dell'utente endpoint.</p> <p>Immettere il messaggio di notifica nella casella di testo. È possibile aggiungere variabili al messaggio selezionando i valori appropriati nella casella Inserisci variabile.</p> <p>È eventualmente possibile configurare la notifica per includere le giustificazioni per l'utente come pure un'opzione per consentire agli utenti di immettere la loro giustificazione.</p> <p>È anche possibile aggiungere collegamenti ipertestuali a URL che contengono informazioni sulla sicurezza della società. Per aggiungere collegamenti ipertestuali, si utilizza la sintassi HTML standard, tag e URL. I tag fanno distinzione tra maiuscole e minuscole. È possibile includere il testo di collegamenti ipertestuali tra testo normale. Ad esempio, si potrebbe digitare:</p> <p>\$CONTENT_TYPE\$ "\$CONTENT_NAME\$" contiene informazioni riservate. Fare clic qui per informazioni. Contattare l'amministratore in caso di domande.</p>
Inserisci variabile	<p>Selezionare le variabili che si desidera includere nella notifica visualizzata sullo schermo dell'utente endpoint.</p> <p>È possibile selezionare variabili basate sui seguenti tipi:</p> <ul style="list-style-type: none"> ■ Applicazione ■ Nome contenuto ■ Tipo di contenuto ■ Tipo di dispositivo ■ Nomi di politica ■ Protocollo

Parametro	Descrizione
Consenti all'utente di scegliere la spiegazione	<p>Selezionare questa opzione per visualizzare fino a quattro giustificazioni per l'utente nella notifica visualizzata. Quando la notifica compare sull'endpoint, l'utente è tenuto a scegliere una delle giustificazioni. Se si seleziona Consenti all'utente di immettere un testo esplicativo, l'utente può immettere una giustificazione. Symantec Data Loss Prevention fornisce quattro giustificazioni predefinite, che è possibile modificare o rimuovere come necessario.</p> <p>Giustificazioni disponibili:</p> <ul style="list-style-type: none"> ■ Processo di business interrotto ■ Falso positivo ■ Approvato dal manager ■ Formazione utenti ■ Personalizzato (nuova giustificazione) <p>Ogni voce di giustificazione comprende le seguenti opzioni:</p> <ul style="list-style-type: none"> ■ Casella di controllo Questa opzione indica se includere la giustificazione associata nella notifica. Per rimuovere una giustificazione, deselezionare la casella di controllo accanto. Per includere una giustificazione, selezionare la casella di controllo accanto. ■ Giustificazione L'etichetta di sistema per la giustificazione. Questo valore compare nei report (per scopi di ordinamento e filtro), ma l'utente non lo vede. È possibile selezionare l'opzione desiderata dall'elenco a discesa. ■ Opzione presentata all'utente finale Il testo della giustificazione di Symantec Data Loss Prevention viene visualizzato nella notifica. Questo valore compare nei report con l'etichetta di giustificazione. È possibile modificare il testo predefinito come desiderato. <p>Per aggiungere una nuova giustificazione, selezionare Nuova giustificazione dall'elenco a discesa appropriato. Nella casella di testo Immettere una nuova giustificazione visualizzata, digitare il nome della giustificazione. Quando si salva la regola, il sistema include la nuova giustificazione come opzione (in ordine alfabetico) in tutti gli elenchi a discesa di Giustificazione.</p> <p>Nota: È necessario essere selettivi quando si aggiungono nuove giustificazioni. La cancellazione di nuove giustificazioni non è attualmente supportata.</p>
Consenti all'utente di immettere un testo esplicativo	<p>Selezionare questa opzione per includere una casella di testo in cui gli utenti possono immettere la loro giustificazione.</p>

Vedere ["Azioni delle regole di risposta per il rilevamento di endpoint"](#) a pagina 1470.

Configurazione dell'azione Endpoint Prevent: operazione annullata dall'utente

L'azione di regola di risposta Endpoint Prevent: operazione annullata dall'utente visualizza una notifica per l'utente in caso di violazione di una politica.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Gli utenti hanno un tempo limitato per decidere se ignorare o meno la violazione. Se la violazione è ignorata, il trasferimento di dati viene completato e viene generato un incidente. Se la violazione non è ignorata, il trasferimento di dati viene interrotto e viene generato un incidente. Se l'utente non prende una decisione nel tempo consentito, il trasferimento di dati viene bloccato automaticamente e viene creato un incidente. È possibile fornire un motivo per la notifica come pure opzioni per consentire all'utente endpoint di immettere una giustificazione per l'azione.

Questa azione di regola di risposta è disponibile per Endpoint Prevent solo su endpoint Windows.

Vedere ["Come implementare Endpoint Prevent"](#) a pagina 2076.

Per configurare l'azione Endpoint Prevent: operazione annullata dall'utente

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

Aggiungere il tipo di azione **Endpoint Prevent: operazione annullata dall'utente** dall'elenco **Azioni**.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 2 Configurare i parametri di **Endpoint Prevent: operazione annullata dall'utente**.

Vedere [Tabella 45-26](#) a pagina 1557.

- 3 Fare clic su **Salva** per salvare la configurazione.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-26 Parametri di Endpoint Prevent: operazione annullata dall'utente

Parametro	Descrizione
Lingua	<p>Selezionare la lingua per l'esecuzione della regola di risposta.</p> <p>Fare clic su Aggiungi lingua per aggiungere più di una lingua.</p> <p>Vedere "Informazioni sulle regole di risposta di Endpoint Prevent con impostazioni locali differenti" a pagina 2078.</p> <p>Vedere "Configurazione delle regole di risposta di Endpoint Prevent per differenti impostazioni locali" a pagina 2079.</p>

Parametro	Descrizione
Avviso di pre-timeout	<p>Questo campo segnala agli utenti che hanno un tempo limitato per rispondere all'incidente.</p> <p>Immettere il messaggio di notifica nella casella di testo. È possibile aggiungere variabili al messaggio selezionando i valori appropriati nella casella Inserisci variabile.</p>
Messaggio di post-timeout	<p>Questo campo segnala agli utenti che il tempo disponibile per ignorare la politica è scaduto. Il trasferimento di dati è stato bloccato.</p> <p>Immettere il messaggio di notifica nella casella di testo. È possibile aggiungere variabili al messaggio selezionando i valori appropriati nella casella Inserisci variabile.</p>
Visualizza finestra di avviso con questo messaggio	<p>Questo campo è obbligatorio per le azioni Endpoint Prevent: operazione annullata dall'utente. Selezionare questa opzione per visualizzare una notifica sullo schermo dell'utente endpoint.</p> <p>Immettere il messaggio di notifica nella casella di testo. È possibile aggiungere variabili al messaggio selezionando i valori appropriati nella casella Inserisci variabile.</p> <p>È eventualmente possibile configurare la notifica per includere le giustificazioni per l'utente come pure un'opzione per consentire agli utenti di immettere la loro giustificazione.</p> <p>È anche possibile aggiungere collegamenti ipertestuali a URL che contengono informazioni sulla sicurezza della società. Per aggiungere collegamenti ipertestuali, si utilizza la sintassi HTML standard, tag e URL. I tag fanno distinzione tra maiuscole e minuscole. È possibile includere il testo di collegamenti ipertestuali tra testo normale. Ad esempio, si potrebbe digitare:</p> <p>\$CONTENT_TYPE\$ "\$CONTENT_NAME\$" contiene informazioni riservate. Fare clic qui per informazioni. Contattare l'amministratore in caso di domande.</p>
Inserisci variabile	<p>Selezionare le variabili che si desidera includere nella notifica visualizzata sullo schermo dell'utente endpoint.</p> <p>È possibile selezionare variabili basate sui seguenti tipi:</p> <ul style="list-style-type: none"> ■ Applicazione ■ Nome contenuto ■ Tipo di contenuto ■ Tipo di dispositivo ■ Nome politica ■ Protocollo ■ Contatore timeout <p>Nota: È necessario utilizzare Contatore timeout per visualizzare quanto tempo rimane prima del blocco del trasferimento di dati.</p>

Parametro	Descrizione
Consenti all'utente di scegliere la spiegazione.	<p>Selezionare questa opzione per visualizzare fino a quattro giustificazioni per l'utente nella notifica visualizzata. Quando la notifica compare sull'endpoint, l'utente è tenuto a scegliere una delle giustificazioni. Se si seleziona Consenti all'utente di immettere un testo esplicativo, l'utente può immettere una giustificazione. Symantec Data Loss Prevention fornisce quattro giustificazioni predefinite, che è possibile modificare o rimuovere come necessario.</p> <p>Giustificazioni disponibili:</p> <ul style="list-style-type: none"> ■ Processo di business interrotto ■ Falso positivo ■ Approvato dal manager ■ Formazione utenti ■ Personalizzato (nuova giustificazione) <p>Ogni voce di giustificazione comprende le seguenti opzioni:</p> <ul style="list-style-type: none"> ■ Casella di controllo Questa opzione indica se includere la giustificazione associata nella notifica. Per rimuovere una giustificazione, deselezionare la casella di controllo accanto. Per includere una giustificazione, selezionare la casella di controllo accanto. ■ Giustificazione L'etichetta di sistema per la giustificazione. Questo valore compare nei report (per scopi di ordinamento e filtro), ma l'utente non lo vede. È possibile selezionare l'opzione desiderata dall'elenco a discesa. ■ Opzione presentata all'utente finale Il testo della giustificazione di Symantec Data Loss Prevention viene visualizzato nella notifica. Questo valore compare nei report con l'etichetta di giustificazione. È possibile modificare il testo predefinito come desiderato. <p>Per aggiungere una nuova giustificazione, selezionare Nuova giustificazione dall'elenco a discesa appropriato. Nella casella di testo Immettere una nuova giustificazione visualizzata, digitare il nome della giustificazione. Quando si salva la regola, il sistema include la nuova giustificazione come opzione (in ordine alfabetico) in tutti gli elenchi a discesa di Giustificazione.</p> <p>Nota: È necessario essere selettivi quando si aggiungono nuove giustificazioni. La cancellazione di nuove giustificazioni non è attualmente supportata.</p>
Consenti all'utente di immettere un testo esplicativo	<p>Selezionare questa opzione per includere una casella di testo in cui gli utenti possono immettere la loro giustificazione.</p>

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Network Prevent for Web: Blocca richiesta FTP

L'azione regola di risposta Network Prevent for Web: blocca richiesta FTP blocca tutti i trasferimenti di file tramite FTP sulla rete o sul dispositivo mobile.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa regola di risposta è disponibile solo per Network Prevent for Web integrato con un server proxy.

Vedere ["Configurazione del server Network Prevent for Web"](#) a pagina 1807.

Per configurare l'azione regola di risposta Network Prevent for Web: blocca richiesta FTP

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Network Prevent for Web: blocca richiesta FTP** dall'elenco **Azioni**.

L'azione della regola di risposta Blocca richiesta FTP non richiede alcuna nuova configurazione. Una volta distribuita la regola di risposta a una politica, questa azione blocca qualsiasi tentativo FTP.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Network Prevent for Web: blocca HTTP/HTTPS

La regola di risposta Network Prevent for Web: blocca HTTP/HTTPS blocca la trasmissione del contenuto Web rilevato da Network Prevent for Web. Questa azione blocca anche gli allegati e i messaggi di posta elettronica basati su Web.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione di regola di risposta blocca la trasmissione di contenuto Web mediante il protocollo ICAP. Per implementare questa azione di regola di risposta è necessario integrare il server di rilevamento con il server proxy Web.

Vedere ["Configurazione del server Network Prevent for Web"](#) a pagina 1807.

Per configurare l'azione di regola di risposta Network Prevent: blocca HTTP/HTTPS

- 1 Integrare Network Prevent for Web con un proxy server e, se necessario, un server VPN.
Vedere ["Server Network Prevent for Web - Configurazione di base"](#) a pagina 251.
- 2 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 3 Aggiungere il tipo di azione **Network Prevent for Web: blocca HTTP/HTTPS** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 4 Modificare il **messaggio di rifiuto** come necessario.

Il sistema visualizza questo messaggio nel browser dell'utente quando l'azione blocca il contenuto.

Ad esempio, si potrebbe includere del testo HTML da visualizzare in un browser.

Nota: Se il client che genera la richiesta non prevede una risposta HTML, il messaggio di rifiuto potrebbe non essere visualizzato nel browser del client. Ad esempio, un client che prevede una risposta XML a un post Web può indicare solo un errore Javascript.

- 5 Fare clic su **Salva** per salvare la configurazione della regola di risposta.

Determinate applicazioni non possono fornire una risposta adeguata all'azione di risposta Network Prevent for Web: blocca HTTP/HTTPS. Questo comportamento è stato osservato con l'applicazione Yahoo! Mail quando un server di rilevamento blocca il caricamento di un file. Se un utente prova a caricare l'allegato di un'e-mail e l'allegato genera un'azione di risposta Network Prevent for Web: blocca HTTP/HTTPS, Yahoo! Mail non risponde o visualizza un messaggio di errore per indicare che il file è bloccato. Eppure, Yahoo! Mail sembra continuare il caricamento del file selezionato, ma il caricamento non viene completato. A un certo punto, l'utente deve annullare manualmente il caricamento premendo **Annulla**.

Anche altre applicazioni potrebbero mostrare questo comportamento, a seconda di come viene gestita la richiesta di blocco. In questi casi, viene creato un incidente del server di rilevamento e il caricamento del file viene bloccato anche se l'applicazione non fornisce alcuna indicazione.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Network Prevent: blocca messaggio SMTP

L'azione di regola di risposta Network Prevent: blocca messaggio SMTP blocca i messaggi e-mail SMTP che causano un incidente sul server di rilevamento di Network Prevent (Email).

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione di regola di risposta è disponibile solo con Network Prevent for Email.

Vedere ["Azioni delle regole di risposta per il rilevamento di Network Prevent"](#) a pagina 1471.

È necessario integrare il server di rilevamento di Network Prevent for Email con un agente MTA per implementare questa azione di regola di risposta. Per informazioni dettagliate, fare riferimento alla *Guida all'integrazione MTA di Symantec Data Loss Prevention per Network Prevent (Email)*.

Per configurare l'azione di regola di risposta Blocca messaggio SMTP

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Network Prevent: blocca messaggio SMTP** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare i parametri dell'azione Blocca messaggio SMTP
Vedere [Tabella 45-27](#) a pagina 1562.
- 4 Fare clic su **Salva** per salvare la regola di risposta.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-27 Parametri di Network Prevent: Blocca messaggio SMTP

Parametro	Descrizione
Restituisci messaggio al mittente	Immettere il testo da visualizzare nell'errore SMTP che Network Prevent (Email) invia all'agente MTA. Alcuni MTA visualizzano questo testo nel messaggio restituito al mittente. Se si lascia vuoto questo campo, il messaggio non viene restituito al mittente ma l'agente MTA invia un proprio messaggio.
Reindirizza messaggio a questo indirizzo	Se si desidera reindirizzare i messaggi bloccati a un determinato indirizzo (come l'amministratore di Symantec Data Loss Prevention), digitare l'indirizzo in questo campo. Se si lascia vuoto questo campo, il messaggio viene restituito solo al mittente.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Network Prevent: modifica messaggio SMTP

L'azione di regola di risposta Network Prevent: modifica messaggio SMTP consente di modificare un'e-mail riservata. Ad esempio, è possibile utilizzare questa azione per modificare l'oggetto di un'e-mail e includere informazioni sul tipo di violazione della politica.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Vedere ["Azioni delle regole di risposta per il rilevamento di Network Prevent"](#) a pagina 1471.

Per configurare l'azione Network Prevent: modifica messaggio SMTP

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Aggiungere il tipo di azione **Network Prevent: modifica messaggio SMTP** dall'elenco **Azioni**.

Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Configurare i parametri dell'azione.

Vedere [Tabella 45-28](#) a pagina 1563.

- 4 Fare clic su **Salva** per salvare la configurazione.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-28 Network Prevent: parametri di Modifica messaggio SMTP

Parametro	Descrizione
Oggetto	<p>Selezionare il tipo di modifica da apportare all'oggetto del messaggio selezionando una delle opzioni seguenti:</p> <ul style="list-style-type: none">■ Non modificare - Il testo non viene modificato nell'oggetto.■ Anteponi - Nuovo testo viene aggiunto all'inizio dell'oggetto.■ Aggiungi - Nuovo testo viene aggiunto alla fine dell'oggetto.■ Sostituisci con - Nuovo testo sostituisce completamente il testo dell'oggetto. <p>Se si modifica il testo dell'oggetto, specificare il nuovo testo.</p> <p>Ad esempio, se si desidera anteporre "VIOLAZIONE" all'oggetto del messaggio, selezionare Anteponi e immettere VIOLAZIONE nel campo di testo.</p>
Intestazioni	<p>Immettere un nome univoco e un valore per ogni intestazione che si desidera aggiungere al messaggio (fino a tre).</p>

Parametro	Descrizione
Abilita connessione quarantena e-mail (richiede Symantec Messaging Gateway)	<p>Selezionare questa opzione per consentire l'integrazione con Symantec Messaging Gateway. Quando questa opzione è attivata, Symantec Data Loss Prevention aggiunge al messaggio le intestazioni x preconfigurate che informano Symantec Messaging Gateway della necessità di mettere in quarantena il messaggio.</p> <p>Per maggiori informazioni, consultare la <i>Guida all'implementazione di plug-in di FlexResponse per connessione quarantena e-mail di Symantec Data Loss Prevention</i>.</p>

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Network Prevent for Web: rimuovi contenuto HTTP/HTTPS

L'azione di risposta Network Prevent for Web: rimuovi contenuto HTTP/HTTPS rimuove i dati riservati pubblicati su siti di posta Web (come Gmail), blog (come Blogspot) e altri siti. Questa azione rimuove inoltre i dati riservati inclusi in qualsiasi file che gli utenti caricano nei siti Web o allegano alla posta Web. Questa azione è utilizzabile solo con i comandi HTTP/S POST e non con i comandi GET.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione di regola di risposta è disponibile solo per Network Prevent for Web.

Vedere ["Azioni delle regole di risposta per il rilevamento di Network Prevent"](#) a pagina 1471.

Symantec Data Loss Prevention riconosce i campi di moduli Web per siti di posta Web, blog e social network selezionati. Se Network Prevent for Web non può rimuovere dati riservati per un sito Web che riconosce, crea un evento di sistema ed esegue un'opzione di fallback configurata.

Nota: Symantec Data Loss Prevention rimuove contenuto per caricamenti di file e, per Network Prevent, allegati di posta Web anche per quei siti che non riconosce per la rimozione di contenuto HTTP.

Per configurare l'azione Network Prevent for Web: rimuovi contenuto HTTP/HTTPS

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Network Prevent for Web: rimuovi contenuto HTTP/HTTPS** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.

- 3 Configurare i parametri dell'azione.
Vedere [Tabella 45-29](#) a pagina 1565.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-29 Parametri di Network Prevent for Web: rimuovi contenuto HTTP/HTTPS

Campo	Descrizione
Messaggio di rimozione	Il messaggio che compare nel contenuto (pubblicazioni Web, posta Web o file) da cui il sistema ha rimosso informazioni riservate. Soltanto il destinatario vede questo messaggio.
Opzione di fallback	L'azione da intraprendere se Network Prevent for Web non può rimuovere le informazioni riservate rilevate in un post HTTP o HTTPS. Le opzioni disponibili sono Blocca (impostazione predefinita) e Consenti . Nota: Symantec Data Loss Prevention rimuove i dati riservati nei caricamenti di dati e, per Network Prevent, negli allegati di posta Web, anche per i siti in cui non esegue la rimozione di contenuto. L' Opzione di fallback viene utilizzata solo nei casi in cui Symantec Data Loss Prevention individua contenuto riservato in un modulo Web riconosciuto, ma non può rimuovere il contenuto.
Messaggio di rifiuto	Il messaggio che Network Prevent for Web restituisce a un client quando blocca un post HTTP o HTTPS. L'applicazione Web client può visualizzare o meno il messaggio di rifiuto, a seconda della gestione dei messaggi di errore da parte dell'applicazione.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Network Protect: copia file

L'azione della regola di risposta Network Protect: copia file crea una copia di un file riservato nel file system locale.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione di regola di risposta è disponibile solo per Network Discover, configurato per Network Protect.

Vedere ["Azioni delle regole di risposta per il rilevamento di Network Prevent"](#) a pagina 1471.

Per configurare l'azione di regola di risposta Network Protect: copia file

- 1 Configurare una condivisione file in rete e specificare una posizione in cui copiare i file.
Vedere ["Configurazione di Network Protect per condivisioni file"](#) a pagina 1928.
- 2 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 3 Selezionare il tipo di azione **Network Protect: copia file** dall'elenco **Azioni**.
Questa azione non richiede di configurare nessun parametro.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.
Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Network Protect: metti file in quarantena

L'azione di regola di risposta Network Protect: metti file in quarantena mette in quarantena un file che il server di rilevamento identifica come sensibile o protetto.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Questa azione di regola di risposta è disponibile solo per Network Discover, configurato per Network Protect.

Vedere ["Azioni delle regole di risposta per il rilevamento di Network Prevent"](#) a pagina 1471.

Per configurare l'azione Network Protect: metti file in quarantena

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Network Protect: metti file in quarantena** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Configurare i parametri di **Network Protect: metti file in quarantena**.
Vedere [Tabella 45-30](#) a pagina 1567.
- 4 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Tabella 45-30 Parametri di configurazione di Network Protect: metti file in quarantena

Parametro	Descrizione
File marker	<p>Selezionare questa opzione per creare un file di testo marker al fine di sostituire il file originale. Questa azione informa l'utente in merito a quanto è accaduto al file invece di metterlo in quarantena o eliminarlo senza spiegazione.</p> <p>Nota: Il file marker è dello stesso tipo e ha lo stesso nome del file originale, purché sia un file di testo. Un esempio di questo tipo di file è Microsoft Word. Se il file originale è un PDF o un file di immagini, il sistema crea un file marker di testo semplice. Il sistema assegna poi al file lo stesso nome del file originale con .txt aggiunto alla fine. Ad esempio, se il nome del file originale è accounts.pdf, il nome del file marker è accounts.pdf.txt.</p>
Testo marker	<p>Specificare il testo che deve essere visualizzato nel file marker. Se è stata selezionata l'opzione per lasciare il file marker al posto del file riparato, è possibile utilizzare delle variabili nel testo del marker.</p> <p>Per specificare il testo del marker, selezionare la variabile dall'elenco Inserisci variabile.</p> <p>Ad esempio, per Testo marker è possibile immettere il seguente testo:</p> <p>Un messaggio ha violato le seguenti regole in \$POLICY\$: \$RULES</p> <p>In alternativa, è possibile immettere:</p> <p>\$FILE_NAME\$ è stato spostato in \$QUARANTINE_PARENT_PATH\$</p>

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Configurazione dell'azione Network Protect: crittografia file

L'azione di regola di risposta Network Protect: crittografia file crittografa un file che il server di rilevamento identifica come riservato o protetto. Questa funzionalità è disponibile solo se la licenza ICE di Network Discover è installata ed Enforce Server è stato configurato per connettersi al cloud Symantec ICE.

Vedere ["Configurazione di Enforce Server per connettersi al cloud ICE Symantec"](#) a pagina 229.

Per informazioni su come Symantec Data Loss Prevention interagisce con Symantec ICE, fare riferimento al *Manuale di distribuzione di Symantec Information Centric Encryption*.

Nota: Quando un file viene crittografato, la sua estensione diventa **.html**. È necessario aggiornare manualmente tutti i collegamenti che rimandano al file originale non crittografato.

Vedere ["Informazioni sulle azioni di regola di risposta"](#) a pagina 1468.

Per informazioni sulle limitazioni dell'azione di regola di risposta Network Protect: crittografia file, Vedere ["Best practice per le regole di risposta"](#) a pagina 1487.

Questa azione di regola di risposta è disponibile solo per Network Discover, configurato per Network Protect.

Vedere ["Azioni delle regole di risposta per il rilevamento di Network Prevent"](#) a pagina 1471.

Per configurare l'azione di regola di risposta Network Protect: crittografia file

- 1 Configurare una regola di risposta nella schermata **Configura regola di risposta**.
Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.
- 2 Aggiungere il tipo di azione **Network Protect: crittografia file** dall'elenco **Azioni**.
Vedere ["Configurazione delle azioni di regola di risposta"](#) a pagina 1493.
- 3 Fare clic su **Salva** per salvare la configurazione.
Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Vedere ["Implementazione di regole di risposta"](#) a pagina 1486.

Risoluzione e gestione degli incidenti

- [Capitolo 46. Risoluzione di incidenti](#)
- [Capitolo 47. Risoluzione di incidenti di rete](#)
- [Capitolo 48. Risoluzione di incidenti endpoint](#)
- [Capitolo 49. Risoluzione di incidenti di rilevazione](#)
- [Capitolo 50. Utilizzo di incidenti connettore cloud](#)
- [Capitolo 51. Gestione e report degli incidenti](#)
- [Capitolo 52. Come nascondere incidenti](#)
- [Capitolo 53. Utilizzo di dati di incidente](#)
- [Capitolo 54. Utilizzo del rischio dell'utente](#)
- [Capitolo 55. Implementazione dei plug-in di ricerca](#)

Risoluzione di incidenti

Il capitolo contiene i seguenti argomenti:

- [Informazioni sulla riparazione degli incidenti](#)
- [Risoluzione di incidenti](#)
- [Esecuzione di regole di risposta smart](#)
- [Comandi delle azioni di riparazione degli incidenti](#)
- [Variabili azione di risposta](#)

Informazioni sulla riparazione degli incidenti

In caso si verificassero errori nel sistema, gli addetti all'interno dell'organizzazione devono analizzare gli incidenti, determinarne la causa, identificarne le tendenze e risolvere i problemi.

Symantec Data Loss Prevention fornisce una ricca gamma di funzioni in grado di fornire un'efficiente procedura di riparazione dell'incidente. Una volta pronti, è possibile utilizzare una serie di comandi per l'incidente nelle pagine **Istantanea incidente** e **Elenco incidenti**.

Poiché la pagina **Istantanea incidente** visualizza i dettagli relativi a un incidente specifico, è possibile selezionare un comando per eseguire un'azione sull'incidente visualizzato.

Nella pagina **Elenco incidenti** è possibile eseguire un'azione su più incidenti contemporaneamente. È possibile selezionare più di un incidente dall'elenco e scegliere il comando desiderato.

[Tabella 46-1](#) descrive le opzioni coinvolte nella riparazione dell'incidente:

Tabella 46-1 Opzioni coinvolte nella riparazione dell'incidente

Opzioni di riparazione	Descrizione
Controllo degli accessi basato sul ruolo	<p>L'accesso alle informazioni relative all'incidente nel sistema Symantec Data Loss Prevention può essere ben controllato grazie al controllo degli accessi basato sul ruolo. I ruoli controllano quali incidenti possono essere riparati da uno specifico addetto alle riparazioni, nonché quali informazioni possono essere consultate per la riparazione. Ad esempio, è possibile utilizzare il controllo degli accessi per assicurarsi che un addetto alle riparazioni possa agire solo sugli incidenti verificatisi all'interno di una specifica unità operativa. Inoltre, può impedire al personale di quella unità di consultare gli incidenti più gravi indirizzandoli al dipartimento di sicurezza.</p> <p>Vedere "Informazioni sul controllo degli accessi basato sul ruolo" a pagina 109.</p>
Assegnazione del livello di gravità	<p>La gravità di incidente è la misura del rischio associato a un particolare incidente. Ad esempio, un messaggio di posta elettronica che contiene 50 record del cliente può essere considerato più grave di un messaggio che contiene 50 violazioni delle condizioni d'utilizzo. Symantec Data Loss Prevention consente di specificare cosa costituisce un incidente grave configurandolo al livello della regola della politica. Symantec Data Loss Prevention usa quindi la gravità dell'incidente per determinare le risposte successive all'incidente. Questo processo consente di dare la priorità agli incidenti e impiegare le risorse di riparazione manuale nelle aree dove sono più necessarie.</p>
Ricerca degli attributi personalizzati	<p>La ricerca degli attributi personalizzati è il processo di raccolta di ulteriori informazioni relative all'incidente provenienti dall'origine dei dati esterna a Enforce e all'incidente stesso. Ad esempio, è possibile consultare un server aziendale LDAP per ottenere ulteriori informazioni sul mittente del messaggio, come il nome del responsabile del mittente o dell'unità operativa.</p> <p>Vedere "Informazioni sull'uso di attributi personalizzati" a pagina 1708.</p> <p>Ad esempio, è possibile utilizzare gli attributi personalizzati come input alle risposte automatiche successive per informare automaticamente il responsabile del mittente della violazione della politica.</p> <p>Vedere "Impostazione manuale dei valori degli attributi personalizzati" a pagina 1710.</p>

Opzioni di riparazione	Descrizione
Risposte automatiche agli incidenti	<p>Una potente funzionalità dell'Enforce Server è la capacità di rispondere automaticamente agli incidenti non appena si verificano. Ad esempio, è possibile configurare il sistema per rispondere a un incidente grave, bloccando la comunicazione pericolosa. È possibile inviare un messaggio e-mail al responsabile del mittente. È possibile inviare un avviso al sistema di gestione degli eventi di sicurezza. È possibile eseguire l'escalation dell'incidente al dipartimento di sicurezza. Per contro, un incidente relativo all'autorizzazione all'utilizzo potrebbe essere distribuito inviando un'e-mail al mittente. È possibile quindi contrassegnare l'incidente come chiuso, senza la necessità di ulteriori azioni. Tra questi estremi, è possibile stabilire una politica che crittografa automaticamente le trasmissioni dei dati riservati a un partner commerciale. Tutti questi scenari possono essere gestiti automaticamente senza intervento dell'utente.</p> <p>Vedere "Configurazione delle azioni di regola di risposta" a pagina 1493.</p>
Risposta smart	<p>Nonostante la risposta automatica sia una parte importante del processo di riparazione, la funzionalità SmartResponse risulta necessaria alcune volte, specialmente nel caso di incidenti più gravi. Symantec Data Loss Prevention fornisce un'istantanea dettagliata dell'incidente contenente tutte le informazioni necessarie per determinare le fasi successive della riparazione. È possibile utilizzare Risposta smart per aggiornare manualmente la gravità degli incidenti, lo stato, gli attributi personalizzati e aggiungere commenti. È possibile spostare l'incidente all'interno del flusso di lavoro della riparazione per risolverlo.</p> <p>Vedere "Configurazione delle azioni di regola di risposta" a pagina 1493.</p> <p>Sono disponibili le seguenti azioni Risposta smart standard:</p> <ul style="list-style-type: none"> ■ Aggiungi nota ■ Registrazione a un server Syslog ■ Invia notifica e-mail ■ Imposta stato <p>Vedere "Configurazione dell'azione di FlexResponse server" a pagina 1516.</p>
Distribuzione dei report di incidenti aggregati	<p>È possibile creare e distribuire automaticamente report di incidenti aggregati ai proprietari di dati per la riparazione.</p>

Enforce Server gestisce tutti questi passaggi ad eccezione di Risposta smart. È possibile gestire gli incidenti in modalità completamente automatica. È possibile riservare l'intervento manuale (Risposta smart) solo agli incidenti più gravi.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Risoluzione di incidenti

Quando si ripara un incidente, è possibile eseguire le seguenti azioni:

- Impostare lo stato o la gravità dell'incidente.
- Applicare una regola di risposta smart all'incidente.
- Impostare gli attributi personalizzati dell'incidente.
- Aggiungere commenti al record di incidente.
- Riparare incidenti accedendo a un elenco di incidente o a un'istantanea di incidente e selezionando le azioni da eseguire su uno o più incidenti.
- Eseguire una combinazione di queste azioni.

Durante l'installazione è possibile importare un pacchetto di soluzioni. I pacchetti di soluzioni precompilano gli elenchi di incidenti e le istantanee di incidenti con numerose opzioni di riparazione e attributi personalizzati. Per descrizioni complete di tutti i pacchetti di soluzioni (incluse informazioni su tutte le opzioni di riparazione e gli attributi personalizzati che contengono), fare riferimento alla documentazione per ogni pacchetto di soluzioni nella directory dei pacchetti di soluzioni nella documentazione.

Per riparare incidenti

1 Accedere a un elenco di incidenti o a un'istantanea incidente.

Negli elenchi di incidenti, Symantec Data Loss Prevention visualizza le opzioni di riparazione disponibili nel menu a discesa **Azioni incidente**. Il menu diventa attivo quando si selezionano uno o più incidenti nell'elenco (con la casella di controllo). Nelle istantanee di incidente, Symantec Data Loss Prevention visualizza anche le opzioni di riparazione disponibili. È possibile impostare uno **Stato** o una **Gravità** dai menu a discesa.

Vedere ["Visualizzazione degli incidenti"](#) a pagina 1645.

È anche possibile modificare gli **Attributi** e fornire le informazioni correlate.

2 Eseguire una delle seguenti azioni

- Quando si visualizza un elenco di incidenti, selezionare gli incidenti da riparare (selezionare la casella). È possibile selezionare singoli incidenti o selezionare tutti gli incidenti nella schermata corrente. Selezionare l'azione desiderata dal menu a discesa **Azioni incidenti**. Selezionare ad esempio **Azioni incidente > Imposta stato > Riassegnato**.
 È possibile eseguire tutte le azioni necessarie.
- Quando si visualizza un'istantanea incidente, è possibile impostare lo **Stato** e la **Gravità** dai menu a discesa.

Se in precedenza è stata impostata una risposta smart, è possibile selezionare una regola di risposta smart nella barra di riparazione.

Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.

Ad esempio, se è stato installato uno dei pacchetti di soluzioni, è possibile selezionare **Ignora falso positivo** nella barra di riparazione. Quando viene visualizzata la schermata **Esegui regola di risposta**, fare clic su **OK**. Questa regola di risposta smart modifica lo stato dell'incidente da **Nuovo** a **Ignorato** e imposta l'attributo **Motivo rifiuto** su **Falso positivo**.

È possibile eseguire tutte le azioni di riparazione necessarie.

Esecuzione di regole di risposta smart

Quando si esegue una regola di risposta che invia un'e-mail, è possibile comporre manualmente il contenuto della notifica tramite e-mail.

Nota: L'invio di una notifica tramite e-mail al mittente è possibile solo con gli incidenti SMTP. Inoltre, gli indirizzi di notifica basati su attributi personalizzati (come "e-mail del responsabile") funzionano correttamente solo se popolati tramite il plug-in di ricerca di attributi.

Per comporre una risposta di notifica tramite e-mail

- 1 Immettere eventualmente indirizzi e-mail per le copie nel campo **CC**.
- 2 Selezionare la lingua.
- 3 Comporre o modificare l'oggetto e il corpo dell'e-mail.
- 4 Inserire variabili per i campi nell'incidente. Le variabili supportate sono visualizzate come collegamenti a destra dei campi modificabili.

Ad esempio, se si desidera includere la politica e le regole violate, si potrebbe immettere:

```
A message has violated the following rules in $POLICY$:
$RULES$
```

- 5 Fare clic su **OK** per inviare la notifica.

Vedere ["Aggiunta di una nuova regola di risposta"](#) a pagina 1490.

Vedere ["Informazioni sulla riparazione degli incidenti"](#) a pagina 1570.

Vedere ["Variabili azione di risposta"](#) a pagina 1576.

Comandi delle azioni di riparazione degli incidenti

In un elenco di incidenti, utilizzare il menu a discesa **Azioni incidente** per selezionare le azioni di riparazione.

Le seguenti azioni sono disponibili per un elenco di incidenti:

Aggiungi nota	<p>Aggiungere una breve nota agli incidenti selezionati. Il commento appare nella scheda Cronologia incidenti della pagina Istantanea incidente per ogni incidente selezionato.</p> <p>Il limite per il campo Aggiungi nota è 4000 byte.</p>
Elimina incidenti	<p>Eliminare gli incidenti selezionati dal sistema Symantec Data Loss Prevention.</p> <p>Procedere con attenzione quando si eliminano gli incidenti. Tutti i dati associati agli incidenti vengono rimossi. Questa operazione non può essere annullata.</p>
Esporta selezioni: CSV	Esportare gli incidenti selezionati in un file di dati (.csv) separati da virgole.
Esporta selezioni: XML	Esportare gli incidenti selezionati in un file XML.
Nascondi/Visualizza	<p>Selezionare una delle seguenti azioni per impostare lo stato nascosto per gli incidenti selezionati:</p> <ul style="list-style-type: none"> ■ Nascondi incidenti : contrassegna come archiviati gli incidenti selezionati. ■ Visualizza incidenti : ripristina la visualizzazione degli incidenti selezionati. ■ Non nascondere : impedisce che gli incidenti selezionati vengano nascosti. ■ Consenti nascondi : consente che gli incidenti selezionati vengano nascosti. <p>Vedere "Informazioni su come nascondere gli incidenti" a pagina 1696.</p>
Attributi di ricerca	Utilizzare i plug-in di ricerca configurati per cercare gli attributi configurati.
Imposta attributi	Visualizzare la pagina Imposta attributi in modo da poter immettere o modificare i valori di attributi per gli incidenti selezionati.
Imposta proprietario dati	<p>Impostare i seguenti attributi del proprietario dei dati:</p> <ul style="list-style-type: none"> ■ Nome ■ Indirizzo e-mail

Imposta gravità	Impostare la gravità stabilita per gli incidenti selezionati su una delle opzioni di Imposta gravità .
Imposta stato	<p>Impostare lo stato degli incidenti selezionati su una delle opzioni di Imposta stato. Un amministratore di sistema può personalizzare le opzioni che compaiono in questo elenco nella pagina Attributi incidente.</p> <p>Vedere "Informazioni sugli attributi di stato incidente." a pagina 1700.</p>
Esegui risposta smart	<p>Eseguire una delle risposte elencate sugli incidenti selezionati. Quando si fa clic su una regola di risposta, viene visualizzata la pagina Esegui regola di risposta.</p> <p>Queste regole di risposta manuali sono disponibili solo se si hanno le autorizzazioni di riparazione.</p>

Vedere "[Informazioni sulla riparazione degli incidenti](#)" a pagina 1570.

Variabili azione di risposta

Le variabili di azione di risposta possono essere utilizzate nelle regole di risposta.

Vedere "[Esecuzione di regole di risposta smart](#)" a pagina 1574.

Le variabili dell'azione di risposta variano in base al tipo di incidente.

Vedere "[Variabili generali di incidente](#)" a pagina 1576.

Vedere "[Variabili di incidente endpoint](#)" a pagina 1578.

Vedere "[Variabili di incidenti di Network Monitor e Network Prevent](#)" a pagina 1577.

Vedere "[Variabili di incidente di Discover](#)" a pagina 1578.

Variabili generali di incidente

Le seguenti variabili generali sono disponibili per tutti i tipi di incidente:

\$APPLICATION_NAME\$	Specifica il nome dell'applicazione associata all'incidente.
\$ATTACHMENT_FILENAME\$	Specifica il nome del file allegato.
\$BLOCKED\$	Indica se Symantec Data Loss Prevention ha bloccato il messaggio (sì o no).
\$DESTINATION_IP\$	Specifica l'indirizzo IP di destinazione.
\$INCIDENT_ID\$	L'identificatore univoco dell'incidente.

\$INCIDENT_SNAPSHOT\$	L'URL completo della pagina dell'istantanea incidente relativa all'incidente.
\$MATCH_COUNT\$	Il numero di corrispondenze incidenti.
\$OCCURED_ON\$	Specifica la data in cui si è verificato l'incidente. Questa data può essere differente da quella in cui si è verificato l'incidente.
\$POLICY\$	Il nome della politica che è stata violata.
\$POLICY_RULES\$	Elenco separato da virgole che include una o più regole di politica che sono state violate.
\$PROTOCOL\$	Il protocollo, il tipo di dispositivo e il tipo di target dell'incidente, dove applicabile.
\$RECIPIENTS\$	Un elenco separato da virgole che include un elenco di uno o più destinatari messaggio.
\$REPORTED_ON\$	Specifica la data in cui è stato segnalato l'incidente.
\$MONITOR_NAME\$	Specifica il server di rilevazione o il rivelatore di cloud che ha creato l'incidente.
\$SENDER\$	Il mittente del messaggio.
\$SEVERITY\$	La gravità assegnata all'incidente.
\$STATUS\$	Specifica lo stato di riparazione dell'incidente.
\$SUBJECT\$	L'oggetto del messaggio.
\$URL\$	Specifica il percorso o la posizione del file.

Variabili di incidenti di Network Monitor e Network Prevent

Sono disponibili le seguenti variabili di Network Monitor e Network Prevent:

\$DATAOWNER_NAME\$	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.
\$DATAOWNER_EMAIL\$	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca.

Variabili di incidente di Discover

Le seguenti variabili di incidente di Network Discover/Cloud Storage Discover e Network Protect sono disponibili:

\$DATAOWNER_NAME\$	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.
\$DATAOWNER_EMAIL\$	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca.
\$ENDPOINT_MACHINE\$	Nome del computer endpoint che ha generato la violazione.
\$PATH\$	Percorso completo del file in cui è stato rilevato l'incidente.
\$FILE_NAME\$	Il nome del file in cui è stato rilevato l'incidente.
\$PARENT_PATH\$	Il percorso della directory principale del file in cui è stato rilevato l'incidente.
\$QUARANTINE_PARENT_PATH\$	Il percorso della directory principale in cui il file è stato messo in quarantena.
\$SCAN_DATE\$	La data della scansione che ha rilevato l'incidente.
\$TARGET\$	Il nome del target in cui è stato rilevato l'incidente.

Variabili di incidente endpoint

Sono disponibili le seguenti variabili di incidente endpoint:

\$APPLICATION_USERS\$	Il nome dell'utente dell'applicazione.
\$DATAOWNER_NAME\$	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.
\$DATAOWNER_EMAIL\$	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo può essere impostato manualmente oppure con uno dei plug-in di ricerca.

\$ENDPOINT_LOCATION\$	La posizione del computer endpoint.
\$ENDPOINT_MACHINE\$	Nome del computer endpoint che ha generato la violazione.
\$ENDPOINT_USER_NAME\$	Il nome dell'utente di endpoint.
\$MACHINE_IP\$	L'indirizzo IP aziendale del computer endpoint.
\$USER_JUSTIFICATION\$	La giustificazione fornita dall'utente di endpoint.

Variabili di incidente dei connettori cloud

Sono disponibili le seguenti variabili di incidente dei connettori cloud:

\$DATAOWNER_NAME\$	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.
\$DATAOWNER_EMAIL\$	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente.

Risoluzione di incidenti di rete

Il capitolo contiene i seguenti argomenti:

- [Elenco degli incidenti di rete](#)
- [Elenco incidenti di rete - Azioni](#)
- [Elenco di incidenti di rete - Colonne](#)
- [Istantanea incidente di rete](#)
- [Istantanea incidente di rete - Intestazione e navigazione](#)
- [Istantanea incidente di rete—Informazioni generali](#)
- [Istantanea incidente di rete - Corrispondenze](#)
- [Istantanea incidente di rete - Attributi](#)
- [Report riepilogo rete](#)

Elenco degli incidenti di rete

Un elenco di incidenti di rete mostra molteplici record di incidenti con informazioni su ogni incidente quali gravità, politica associata, numero di corrispondenze e stato dell'incidente. Fare clic su una riga dell'elenco di incidenti per visualizzare ulteriori dettagli su uno specifico incidente. Selezionare incidenti specifici (o gruppi di incidenti) da modificare o riparare facendo clic sulle caselle di controllo a sinistra.

Quando gli indirizzi IPv6 sono visualizzati nei report, vengono applicate le seguenti regole:

- Gli indirizzi sono normalizzati nei campi **IP destinazione** e **IP origine**.

- Nei campi **Destinatario** (URL), gli indirizzi sono riportati come sono stati forniti, in genere un nome host che varia in base al protocollo.
- Nei campi **Mittente**, la rappresentazione degli indirizzi varia in base al protocollo.
- I campi normalizzati sono usati per il filtraggio in base all'IP.

Quando gli indirizzi IPv6 sono visualizzati nei filtri dell'elenco di incidenti, vengono applicate le seguenti regole:

- Gli indirizzi sono normalizzati nei campi **IP destinazione** e **IP origine**.
- Nel campo **Destinatario** (URL), gli indirizzi sono riportati come sono stati forniti nei campi **Destinatario** (URL), **Dominio** e **Mittente**.
- I campi normalizzati sono usati per il filtraggio in base all'IP.

Quando gli indirizzi IPv6 sono visualizzati nei dettagli degli incidenti, vengono applicate le seguenti regole:

- Gli indirizzi sono normalizzati nei campi **IP destinazione** e **IP origine**.
- Nel campo **Destinatario** (URL), gli indirizzi sono riportati come sono stati forniti.
- Nel campo **Mittente**, gli indirizzi sono riportati come sono stati forniti.
- I collegamenti agli elenchi filtrati si comportano come input degli utenti.

È possibile visualizzare indirizzi IPv6 normalizzati in un riepilogo degli incidenti:

- Gli indirizzi sono riepilogati in base ai campi **IP origine**, **IP destinazione**, **Mittente** e **Dominio**.
- La normalizzazione dei campi viene eseguita come quella dei dettagli degli incidenti.

È possibile visualizzare indirizzi IPv6 non normalizzati in un riepilogo degli incidenti:











- Gli indirizzi sono riepilogati in base ai campi **IP origine**, **IP destinazione**, **Mittente** e **Dominio**.
- La normalizzazione dei campi viene eseguita come quella dei dettagli degli incidenti.

Nota: Prestare attenzione quando si sceglie **Seleziona tutto**. Questa azione seleziona tutti gli incidenti nel report (non solo quelli nella pagina corrente). Qualsiasi comando applicato successivamente riguarda tutti gli incidenti. Per selezionare solo gli incidenti nella pagina corrente, selezionare la casella di controllo in alto a sinistra dell'elenco incidenti.

Le informazioni sugli incidenti sono suddivise in varie colonne. Fare clic sull'intestazione di una colonna per disporre le informazioni in ordine alfanumerico in base ai dati della colonna. Per utilizzare l'ordine inverso, fare di nuovo clic sull'intestazione della colonna. Per impostazione predefinita, Symantec Data Loss Prevention ordina gli incidenti per data.

La colonna **Tipo** mostra icone che indicano il tipo di incidente di rete. [Tabella 47-1](#) descrive le icone.

Tabella 47-1 Tipi di incidente di rete

Icona	Descrizione
	SMTP
	L'aggiunta della seconda icona indica un allegato del messaggio.
	HTTP Symantec Data Loss Prevention rileva anche il traffico di messaggistica istantanea (IM) Yahoo e MSN inoltrato tramite HTTP. L'aggiunta della seconda icona indica un allegato di un messaggio e-mail basato su Web.
	HTTPS
	FTP
	NNTP
	IM:MSN
	IM:AIM
	IM:Yahoo
	TCP: protocollo_personalizzato

Questa colonna indica inoltre se la comunicazione è stata bloccata o alterata. [Tabella 47-2](#) mostra i valori possibili.

Tabella 47-2 Stato di blocco o alterazione dell'incidente

Icona	Descrizione
Nessuna icona.	Vuoto se la comunicazione non è stata bloccata.

Icona	Descrizione
	Indica che Symantec Data Loss Prevention ha bloccato la comunicazione contenente il testo con corrispondenza.
	Indica che Symantec Data Loss Prevention ha rimosso dati riservati da post o messaggi e-mail Web. Questa icona può anche indicare che un file è stato caricato in un sito Web o allegato a un messaggio e-mail basato su Web.
	Indica che Symantec Data Loss Prevention ha aggiunto o modificato le intestazioni del messaggio che ha generato l'incidente.

Per ulteriori informazioni sulla pagina dell'elenco di incidenti di rete, utilizzare i seguenti collegamenti:

Per ulteriori informazioni su

Vedere la sezione

Colonne della tabella elenco incidenti

Vedere ["Elenco di incidenti di rete - Colonne"](#) a pagina 1585.

Azioni da eseguire su incidenti selezionati

Vedere ["Elenco incidenti di rete - Azioni"](#) a pagina 1583.

Dettagli di un incidente specifico

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Visualizzazione del riepilogo di tutti gli incidenti di rete

Vedere ["Report riepilogo rete"](#) a pagina 1591.

Caratteristiche comuni a tutti i report di Symantec Data Loss Prevention

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Elenco incidenti di rete - Azioni

È possibile selezionare uno o più incidenti e quindi ripararli utilizzando i comandi nell'elenco a discesa **Azioni incidente**. I comandi per gli incidenti sono i seguenti:

Azione	Descrizione
Aggiungi nota	Selezionare questa opzione per aprire una finestra di dialogo, digitare un commento e quindi fare clic su OK .
Nascondi/Visualizza	<p>Selezionare una delle seguenti azioni dell'archivio per impostare lo stato dell'archivio per gli incidenti selezionati:</p> <ul style="list-style-type: none"> ■ Nascondi incidenti : contrassegna come archiviati gli incidenti selezionati. ■ Visualizza incidenti : ripristina la visualizzazione degli incidenti selezionati. ■ Non nascondere : impedisce che gli incidenti selezionati vengano nascosti. ■ Consenti nascondi : consente che gli incidenti selezionati vengano nascosti. <p>Vedere "Informazioni su come nascondere gli incidenti" a pagina 1696.</p>
Elimina incidenti	Selezionare l'opzione per eliminare gli incidenti specificati.
Esporta selezioni: CSV Esporta selezioni: XML	Selezionare questa opzione per salvare gli incidenti specificati in un file di testo separato da virgole (.csv) o XML, visualizzabile in varie applicazioni comuni quali Microsoft Excel.
Attributi di ricerca	Utilizzare i plug-in di ricerca per cercare gli attributi personalizzati di un incidente.
Esegui risposta smart	Selezionare questa opzione per eseguire una regola di risposta smart configurata dall'utente o dall'amministratore. (Per configurare una regola di risposta smart, andare su Politica > Regole di risposta , fare clic su Aggiungere regola di risposta e selezionare Risposta smart).
Imposta attributi	Selezionare l'opzione per impostare attributi per gli incidenti selezionati.
Imposta proprietario dati	<p>Impostare il nome o l'indirizzo e-mail del proprietario dei dati. Il proprietario dei dati è la persona responsabile della riparazione dell'incidente.</p> <p>I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.</p>

Azione	Descrizione
Imposta gravità	Selezionare questa opzione per impostare la gravità.
Imposta stato	Selezionare questa opzione per impostare lo stato.

Vedere ["Informazioni sulla riparazione degli incidenti"](#) a pagina 1570.


Vedere ["Elenco degli incidenti di rete"](#) a pagina 1580.

Elenco di incidenti di rete - Colonne

Le informazioni sugli incidenti sono suddivise in varie colonne. Fare clic sull'intestazione di una colonna per disporre le informazioni in ordine alfanumerico in base ai dati della colonna. Per utilizzare l'ordine inverso, fare di nuovo clic sull'intestazione della colonna. Per impostazione predefinita Symantec Data Loss Prevention elenca gli incidenti in base alla data.

Il report include le colonne riportate di seguito:

- **Caselle di controllo** che consentono di selezionare gli incidenti da riparare.
 È possibile selezionare uno o più incidenti a cui applicare i comandi dal menu a discesa Incidente all'inizio dell'elenco. Fare clic sulla casella di controllo all'inizio della colonna per selezionare tutti gli incidenti nella pagina corrente (è possibile fare clic su Seleziona tutto all'estrema destra per selezionare tutti gli incidenti nel report).
- **Tipo**
 Il protocollo su cui è stata rilevata la corrispondenza.
 Vedere ["Elenco degli incidenti di rete"](#) a pagina 1580.
- **Oggetto/Mittente/Destinatari**
 Oggetto del messaggio, indirizzo e-mail o indirizzo IP del mittente, indirizzi e-mail del destinatario o URL.
- **Inviato**
 La data e l'ora in cui il messaggio è stato inviato.
- **ID/Politica**
 Il numero di identificazione dell'incidente di Symantec Data Loss Prevention e la politica in base alla quale l'incidente è stato registrato.
- **Corrispondenze**
 Il numero di corrispondenze nell'incidente.
- **Gravità**
 La gravità dell'incidente come determinato dall'impostazione della gravità della regola corrispondente.
 I valori possibili sono:

Icona	Descrizione
	Alta
	Media
	Bassa
	Solo per informazione

■ Stato

Lo stato corrente dell'incidente.

I valori possibili sono:

- **Nuovo**
- **In corso**
- **Riassegnato**
- **Falso positivo**
- **Errori di configurazione**
- **Risolto**

L'utente o l'amministratore può aggiungere nuove designazioni di stato nella pagina **Configurazione attributo**.

Vedere ["Elenco degli incidenti di rete"](#) a pagina 1580.

Istantanea incidente di rete

Un'istantanea incidente fornisce informazioni dettagliate riguardanti un incidente specifico. Visualizza le informazioni generali sull'incidente, le corrispondenze rilevate nel testo intercettato e gli attributi incidente. L'istantanea consente inoltre di eseguire tutte le regole di risposta smart configurate.

L'istantanea incidente è divisa in tre riquadri, con opzioni di navigazione e risposte smart. Fare clic su un collegamento per visualizzare altre informazioni sull'istantanea incidente:

Per ulteriori informazioni su

Navigazione e opzioni di risposta smart

Informazioni generali sull'incidente (riquadro a sinistra)

Vedere la sezione

Vedere ["Istantanea incidente di rete - Intestazione e navigazione"](#) a pagina 1587.

Vedere ["Istantanea incidente di rete—Informazioni generali"](#) a pagina 1587.

Per ulteriori informazioni su

Corrispondenze nell'incidente (riquadro al centro)

Attributi (riquadro a destra)

Vedere la sezione

Vedere ["Istantanea incidente di rete - Corrispondenze"](#) a pagina 1590.

Vedere ["Istantanea incidente di rete - Attributi"](#) a pagina 1591.

Istantanea incidente di rete - Intestazione e navigazione

I seguenti strumenti di navigazione sono visualizzati nella parte superiore dell'istantanea incidente:

Precedente

Visualizza l'incidente precedente nel report di origine.

Successivo

Visualizza l'incidente successivo nel report di origine.



Consente di ritornare al report di origine (dove si è fatto clic sul collegamento per accedere a questa schermata).



Aggiorna l'istantanea con i nuovi dati, come un nuovo commento nella sezione Cronologia o uno stato modificato.

Se è stata configurata una qualsiasi regola di risposta smart, Symantec Data Loss Prevention visualizza le opzioni di risposta per l'esecuzione delle regole nella parte superiore della pagina. In base al numero di regole di risposta smart, potrebbe visualizzarsi un menu a discesa.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Istantanea incidente di rete—Informazioni generali

La sezione sinistra dell'istantanea visualizza informazioni generali sull'incidente. È possibile fare clic su molti valori per visualizzare un elenco di incidenti filtrato in base al valore scelto. Un'icona può apparire accanto all'elenco a discesa **Stato** a indicare che la richiesta che ha generato l'incidente è stata bloccata o alterata.

Vedere [Tabella 47-2](#) a pagina 1582.

Lo stato corrente e la gravità dell'incidente sono visualizzati a destra dell'intestazione dell'istantanea. Per cambiare uno dei valori correnti, fare clic su di esso e scegliere un altro valore nell'elenco a discesa.

La parte restante del riquadro con le informazioni generali è suddivisa in quattro schede.

- Informazioni chiave
- Cronologia
- Note
- Correlazioni

Le informazioni in questa sezione sono suddivise nelle seguenti categorie (non tutte visualizzate per ogni tipo di incidente):

Tabella 47-3 Schede con informazioni generali sull'incidente

Nome scheda	Descrizione
Informazioni chiave	<p>La scheda Informazioni chiave mostra la politica che è stata violata nell'incidente. Inoltre mostra il numero totale di corrispondenze per la politica e le corrispondenze per regola della politica. Fare clic sul nome della politica per visualizzare un elenco di tutti gli incidenti che hanno violato la politica. Fare clic su visualizza politica per visualizzare una versione di sola lettura della politica.</p> <p>Questa sezione elenca anche altre politiche violate dallo stesso file. Per visualizzare l'istantanea di un incidente associato a una determinata politica, fare clic su Vai a incidente accanto al nome della politica. Per visualizzare un elenco di tutti gli incidenti creati dal file, fare clic su Mostra tutto.</p> <p>La scheda Informazioni chiave include inoltre le seguenti informazioni:</p> <ul style="list-style-type: none"> ■ Nome del server di rilevamento che ha registrato l'incidente. ■ Data e ora in cui il messaggio è stato inviato. ■ Indirizzo e-mail o IP del mittente ■ Indirizzo/i e-mail o IP del destinatario ■ Intestazione SMTP o intestazione oggetto NNTP ■ Il campo È nascosto visualizza lo stato archiviato dell'incidente, se l'incidente può essere nascosto, e consente di alternare il flag Non nascondere per l'incidente. ■ Nome o nomi dei file allegati Fare clic per aprire o salvare il file. Se una regola di risposta richiede a Symantec Data Loss Prevention di eliminare il messaggio originale, non è possibile visualizzare l'allegato. ■ La persona responsabile della risoluzione dell'incidente (Nome proprietario dati). Questo campo deve essere impostato manualmente, oppure con un plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione. Se si fa clic su un Nome proprietario dati con collegamento ipertestuale, viene visualizzato un elenco filtrato degli incidenti per nome di proprietario di dati. ■ L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente (Indirizzo e-mail proprietario dati). Questo campo deve essere impostato manualmente, oppure con un plug-in di ricerca. Se si fa clic su un Indirizzo e-mail proprietario dati con collegamento ipertestuale, viene visualizzato un elenco filtrato degli incidenti per indirizzo e-mail di proprietario di dati.

Nome scheda	Descrizione
Cronologia	<p>Visualizza le azioni eseguite sull'incidente. Per ogni azione, Symantec Data Loss Prevention visualizza la data e l'ora dell'azione, l'autore (utente o server) e l'azione o il commento.</p> <p>Vedere "Esecuzione di regole di risposta smart" a pagina 1574.</p> <p>Vedere "Gestione di regole di risposta" a pagina 1489.</p>
Note	<p>Visualizza tutte le note aggiunte dall'utente o da altri all'incidente. Fare clic su Aggiungi nota per aggiungere una nota.</p> <p>Vedere "Scheda note istantanea incidente" a pagina 1674.</p>
Correlazioni	<p>È possibile visualizzare un elenco degli incidenti che condividono attributi con l'incidente corrente. Ad esempio, è possibile visualizzare un elenco di tutti gli incidenti generati da un singolo account. La scheda Correlazioni mostra un elenco delle correlazioni che determinano la corrispondenza con i singoli attributi. Fare clic sui valori di attributo per visualizzare elenchi degli incidenti correlati a tali valori.</p> <p>Per cercare altri incidenti con gli stessi attributi, fare clic su Trova simile. Nella finestra di dialogo Trova incidenti simili visualizzata, selezionare gli attributi di ricerca desiderati. Quindi fare clic su Trova incidenti.</p> <p>Nota: L'elenco degli incidenti correlati non mostra gli incidenti correlati che sono stati nascosti.</p>

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Vedere ["Informazioni su come nascondere gli incidenti"](#) a pagina 1696.

Istantanea incidente di rete - Corrispondenze

Sotto le informazioni generali, Symantec Data Loss Prevention mostra il contenuto del messaggio (se applicabile) e le corrispondenze che hanno causato l'incidente. Symantec Data Loss Prevention visualizza i seguenti tipi di contenuti di messaggio, a seconda del tipo di protocollo:

Protocollo	Contenuto del messaggio
SMTP	Corpo messaggio
HTTP	Coppie di valori nome della richiesta HTTP
FTP	Nessuna indicazione
NNTP	Corpo messaggio

Protocollo	Contenuto del messaggio
IM (tutti i provider)	Conversazione IM
TCP	Dati che sono stati trasmessi mediante il protocollo personalizzato

Le corrispondenze sono evidenziate in giallo e organizzate per componente del messaggio (ad esempio intestazione, corpo o allegato) in cui sono state individuate. Symantec Data Loss Prevention visualizza le corrispondenze pertinenti totali per ogni componente del messaggio. Mostra le corrispondenze nell'ordine in cui compaiono nel testo originale. Per visualizzare la regola che ha attivato una corrispondenza, fare clic sulla corrispondenza evidenziata.

Vedere ["Informazioni sulla soglia di similarità e sul punteggio di somiglianza"](#) a pagina 632.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Istantanea incidente di rete - Attributi

Nota: Questa sezione appare solo se un amministratore di sistema ha configurato attributi personalizzati.

È possibile visualizzare un elenco di attributi personalizzati e dei relativi valori, se specificati. Fare clic sui valori di attributo per visualizzare un elenco di incidenti filtrato in base a tale valore. Per aggiungere nuovi valori o modificare quelli esistenti, fare clic su **Modifica**. Nella finestra di dialogo **Modifica attributi** visualizzata, digitare i nuovi valori e fare clic su **Salva**.

Vedere ["Impostazione manuale dei valori degli attributi personalizzati"](#) a pagina 1710.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Report riepilogo rete

Il report riepilogativo Rete fornisce informazioni di riepilogo sugli incidenti rilevati sulla rete. È possibile organizzare il report in base a uno o due criteri di riepilogo. Un report a riepilogo singolo è organizzato con un singolo criterio riepilogativo, quale la politica associata a ciascun incidente. Un report a riepilogo doppio è organizzato con due criteri, quali la politica e lo stato dell'incidente.

Per visualizzare i criteri di riepilogo primari e secondari disponibili per il report corrente, fare clic sulla barra **Filtri avanzati e riepilogo**. La barra si trova nella parte superiore del report. Le caselle di riepilogo **Riepiloga per** mostrano i criteri di riepilogo primari e secondari. In ogni casella di riepilogo Symantec Data Loss Prevention visualizza tutti i criteri creati al momento in ordine alfabetico, seguiti dai criteri personalizzati definiti dall'amministratore di sistema. I

report di riepilogo prendono il loro nome dal criterio di riepilogo primario (il valore della prima casella di riepilogo). Se si ripete l'esecuzione di un report con nuovi criteri, il nome del report cambia di conseguenza.

Le voci di riepilogo sono divise in varie colonne. Fare clic su qualsiasi intestazione di colonna per ordinare alfanumericamente in base ai dati di tale colonna. Per ordinare nell'ordine inverso, fare di nuovo clic sull'intestazione di colonna.

Tabella 47-4 Colonne del report riepilogativo

Nome colonna	Descrizione
<i>summary_criterion</i>	Questa colonna ha il nome del criterio di riepilogo primario. Elenca gli elementi di riepilogo primari e (per il riepilogo doppio) gli elementi di riepilogo secondari. In un Riepilogo politica, la colonna è denominata Politica ed elenca le politiche. Fare clic su un elemento di riepilogo per vedere un elenco degli incidenti associati a tale elemento.
Totale	Numero totale di incidenti associati all'elemento di riepilogo. In un Riepilogo politica, questa colonna restituisce il numero totale di incidenti associati a ciascuna politica.
Alta	Numero degli incidenti di gravità elevata associati all'elemento di riepilogo. La gravità dell'incidente è determinata dall'impostazione di gravità della regola attivata.
Media	Numero degli incidenti di gravità media associati all'elemento di riepilogo.
Bassa	Numero degli incidenti di gravità bassa associati all'elemento di riepilogo.
Informazioni	Numero degli incidenti di carattere informativo associati all'elemento di riepilogo.
Grafico a barre	Rappresentazione visiva del numero degli incidenti (di tutti i livelli di gravità) associati all'elemento di riepilogo. La barra è suddivisa in sezioni proporzionali e colorate che rappresentano le diverse gravità.
Corrispondenze	Numero totale di corrispondenze associate all'elemento di riepilogo.

Se una delle colonne della gravità contiene totali, è possibile farvi clic sopra per visualizzare un elenco degli incidenti con la gravità scelta.

Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.

Vedere ["Informazioni sui report dashboard e i riepiloghi executive"](#) a pagina 1637.

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Risoluzione di incidenti endpoint

Il capitolo contiene i seguenti argomenti:

- [Informazioni sugli elenchi di incidenti endpoint](#)
- [Istantanea ticket Endpoint](#)
- [Creazione di report su regole di risposta di Endpoint Prevent](#)
- [Informazioni specifiche al protocollo o alla destinazione degli incidenti Endpoint](#)
- [Report di riepilogo sugli incidenti endpoint](#)

Informazioni sugli elenchi di incidenti endpoint

Un elenco di incidenti endpoint mostra gli incidenti endpoint che contengono informazioni basilari quali protocollo o destinazione, gravità, politica associata, numero di corrispondenze e stato. Fare clic su un qualsiasi incidente per visualizzare un'istantanea contenente più dettagli sull'incidente. È possibile selezionare specifici incidenti (o gruppi di incidenti) da modificare o riparare.

Nota: I report endpoint mostrano solo gli incidenti rilevati da Endpoint Prevent. Gli incidenti rilevati da Endpoint Discover sono visualizzati nei report di Network Discover.














Le informazioni sugli incidenti sono suddivise in varie colonne. Fare clic su qualsiasi intestazione di colonna per ordinare alfanumericamente i dati in tale colonna. Per ordinare nell'ordine inverso, fare di nuovo clic sull'intestazione di colonna. Per impostazione predefinita, Symantec Data Loss Prevention elenca gli incidenti per data.

Il report include le seguenti colonne:

- Caselle di controllo che consentono di selezionare gli incidenti da risolvere

È possibile selezionare uno o più incidenti a cui applicare i comandi dal menu a discesa Incidente all'inizio dell'elenco. Fare clic sulla casella di controllo all'inizio della colonna per selezionare tutti gli incidenti nella pagina corrente (è possibile fare clic su **Seleziona tutto** all'estrema destra per selezionare tutti gli incidenti nel report).

Tabella 48-1 Tipo di incidente endpoint

Grafico	Tipo di incidente
	Masterizzatore CD/DVD (ad esempio, masterizzatore Windows Media)
	Supporti rimovibili (ad esempio, una chiavetta USB o scheda SD)
	Unità fissa (ad esempio, l'unità C:\)
	Copia endpoint in condivisione di rete
	E-mail/SMTP
	HTTP
	HTTPS
	FTP
	IM: MSN
	IM: Yahoo
	Stampa/Fax
	Appunti
	Accesso ai file di applicazione

Una colonna di risposta che indica se Symantec Data Loss Prevention ha bloccato un tentativo di violazione o ha informato l'utente finale della violazione dei dati riservati.

I valori possibili sono:

- Vuoto se Symantec Data Loss Prevention non ha bloccato la violazione o non ha informato l'utente finale
- Un'icona rossa indica che la violazione è stata bloccata da Symantec Data Loss Prevention, dall'utente o se il limite di tempo per l'opzione di annullamento da parte dell'utente è scaduto.
- Un'icona di notifica indica che Symantec Data Loss Prevention ha informato l'utente finale della violazione delle politiche relative ai dati riservati. L'icona di notifica viene inoltre visualizzata se l'utente ha consentito il trasferimento dei dati violati. L'icona inoltre viene visualizzata se il limite di tempo per l'opzione di annullamento da parte dell'utente è scaduto e l'azione predefinita è impostata per consentire i trasferimenti di dati.

Le altre colonne di questa sezione sono visualizzate come segue:

Tabella 48-2 Colonne di incidenti endpoint

Colonna	Definizione
Nome file/Computer/Utente/Oggetto/Destinatario	<p>Nome file, computer, utente endpoint (nome di dominio e di accesso), titolo dell'oggetto (se violazione e-mail/SMTP) e utente destinatario associato all'incidente.</p> <p>Quando i file temporanei generano incidenti negli agenti Mac, i nomi di tali file sono visualizzati nella colonna Nome file.</p>
Avvenuto il	<ul style="list-style-type: none"> ■ La data e l'ora dell'incidente ■ Segnalato il ■ La data e l'ora in cui l'incidente è stato segnalato. Se l'endpoint è disconnesso dalla rete aziendale, gli incidenti sono segnalati al ripristino della connessione.
ID/Politica	Il numero di identificazione dell'incidente di Symantec Data Loss Prevention e la politica in base alla quale l'incidente è stato registrato.
Corrisponde con	Il numero di corrispondenze nell'incidente.

Colonna	Definizione
Gravità	<p>La gravità dell'incidente come determinato dall'impostazione della gravità della regola corrispondente.</p> <p>I valori possibili sono:</p> <ul style="list-style-type: none"> ■ Alta ■ Media ■ Bassa ■ Solo per informazione
Stato	<p>Lo stato corrente dell'incidente.</p> <p>I valori possibili sono:</p> <ul style="list-style-type: none"> ■ Nuovo ■ In corso ■ Riassegnato ■ Falso positivo ■ Errori di configurazione ■ Risolto

È possibile aggiungere nuove designazioni di stato nella pagina Configurazione attributo.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Vedere ["Informazioni sulla riparazione degli incidenti"](#) a pagina 1570.

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Istantanea ticket Endpoint

Un'istantanea incidente fornisce informazioni dettagliate riguardanti un incidente Endpoint Prevent specifico. Visualizza le informazioni generali sull'incidente, le corrispondenze rilevate nel testo intercettato e dettagli sugli attributi, la cronologia incidente e la politica violata. È anche possibile cercare incidenti simili nell'area Correlazioni.

Nota: Gli incidenti Endpoint Discover vengono acquisiti nei report Network Discover.













Vedere ["Elenchi di incidenti di Discover"](#) a pagina 1611.


Lo stato attuale e la gravità vengono visualizzati sotto l'intestazione dell'istantanea. Per cambiare uno dei valori correnti, fare clic su di esso e scegliere un altro valore nell'elenco a discesa. Se è associata un'icona di azione, viene visualizzata qui.

Se le regole di risposta smart sono state configurate, Symantec Data Loss Prevention visualizza una barra di riparazione (sotto la barra di stato). La barra di riparazione include opzioni per eseguire le regole. In base al numero delle regole di risposta smart, potrebbe visualizzarsi un menu a discesa.

La sezione in alto a sinistra dell'istantanea visualizza informazioni generali sull'incidente. È possibile fare clic sulla maggior parte dei valori per visualizzare un elenco di incidenti filtrato in base al valore scelto. Le informazioni in questa sezione sono suddivise nelle seguenti categorie (non tutte visualizzate per ogni tipo di incidente):

Tabella 48-3 Tipo di incidente

Icona	Tipo di incidente
	Masterizzatori CD/DVD (ad esempio, masterizzatore Windows Media)
	Supporti rimovibili (ad esempio, una chiavetta USB o scheda SD)
	Unità locale
	Condivisione di rete
	E-mail/SMTP
	HTTP
	HTTPS/SSL
	FTP
	IM: MSN
	IM: Yahoo
	Stampa/Fax
	Appunti

Icona	Tipo di incidente
	Accesso ai file di applicazione

La seguente tabella contiene le altre sezioni informative:

Tabella 48-4 Sezioni dell'incidente

Sezione	Descrizione
Server	Nome dell'Endpoint Server che ha rilevato l'incidente per il rilevamento a due livelli oppure è il nome dell'Endpoint Server che ha ricevuto l'incidente da Symantec DLP Agent.
Risposta agente	<p>Azioni Endpoint Block, Endpoint: notifica, quarantena endpoint, quarantena endpoint, Endpoint FlexResponse, Azione crittografata, Azione crittografata bloccata o operazione annullata dall'utente, se presenti. I valori possibili sono:</p> <ul style="list-style-type: none"> ■ Vuoto o senza icona se Symantec Data Loss Prevention non ha bloccato la copia o non ha notificato l'utente finale. ■ Un cerchio rosso se Symantec Data Loss Prevention ha bloccato dati riservati. ■ Un'icona a forma di busta se Symantec Data Loss Prevention ha informato l'utente finale della riservatezza dei dati. ■ Un segno di spunta verde con una chiave indica che Symantec Data Loss Prevention ha bloccato l'azione dell'utente e ha crittografato il file o i file che l'utente stava cercando di copiare o spostare. ■ Un'icona X rossa con una chiave indica che Symantec Data Loss Prevention ha bloccato l'azione dell'utente, ma non ha crittografato il file o i file che l'utente stava cercando di copiare o spostare. <p>Vedi la sezione Reporting nelle regole di risposta di Endpoint Prevent.</p>
Incidente avvenuto il	Data e ora dell'incidente.
Incidente segnalato il	Data e ora in cui l'incidente è stato segnalato da Endpoint Server.

Sezione	Descrizione
È nascosto	Visualizza lo stato nascosto dell'incidente, se l'incidente può essere nascosto, e consente di alternare il flag Non nascondere per l'incidente. Vedere "Informazioni su come nascondere gli incidenti" a pagina 1696.
Utente	Nome utente Endpoint (ad esempio, MYDOMAIN\bsmith).
Giustificazione utente	L'etichetta di giustificazione precede il testo presentato all'utente finale nella notifica visualizzata sullo schermo (ad esempio, Approvato dal manager: "Il mio manager ha approvato il trasferimento di questi dati"). Symantec Data Loss Prevention utilizza l'etichetta per classificare e filtrare gli scopi all'interno dei report ma l'utente endpoint non può mai visualizzarli. Fare clic sull'etichetta per visualizzare un elenco di incidenti per i quali l'utente finale ha scelto questa giustificazione.
Nome computer	Il computer nel quale si è verificato l'errore.
IP computer (aziendale)	L'indirizzo IP del computer dal quale è stata avviata la violazione se il computer si trovava sulla rete aziendale.
Nome file	Nome del file che ha violato la politica. Il campo del nome del file viene visualizzato solo per gli incidenti che sono stati riparati dall'unità.
Risultato della quarantena	Se le regole di risposta Endpoint Discover: quarantena sono configurate, potrebbe verificarsi uno dei seguenti scenari: <ul style="list-style-type: none"> ■ File in quarantena ■ Quarantena non riuscita ■ Timeout risultato quarantena
Posizione quarantena	Visualizza il percorso della posizione di sicurezza in cui è stato spostato il file.

Sezione	Descrizione
Dettagli quarantena	<p>Consente di visualizzare il motivo per cui l'attività di quarantena non è riuscita a spostare il file riservato. Ad esempio, l'azione potrebbe non essere eseguita correttamente a causa della mancanza del file o le credenziali inserite per accedere alla posizione di sicurezza non sono valide.</p> <p>Il file Dettagli quarantena consente di visualizzare le informazioni anche se lo stato del file di quarantena è sconosciuto a causa di un evento Timeout risultato quarantena.</p>
Posizione endpoint	Indica se l'Endpoint era collegato alla rete aziendale al momento dell'incidente.
Nome applicazione	Il nome dell'applicazione che ha causato l'incidente.
Destinazione	Il percorso di destinazione o del file dei dati riservati a seconda del dispositivo o del protocollo.
IP di destinazione	<p>L'indirizzo IP di destinazione dei dati riservati.</p> <p>L'indirizzo IP di destinazione viene visualizzato solo per specifici incidenti della rete.</p>
Origine	Il file o i dati originali per la violazione. Per prima cosa, l'origine viene visualizzata negli incidenti avvenuti durante il trasferimento del file.
Mittente	Il mittente dei dati riservati per le violazioni della rete.
Destinatario	Il destinatario indicato dei dati riservati per le violazioni della rete.
Nome utente FTP	Il nome utente originale per la violazione dei trasferimenti FTP.
Allegati	I file associati o gli allegati inviati (per incidenti avvenuti sulla rete). Se l'amministratore ha configurato Symantec Data Loss Prevention in modo che conservi i dati degli incidenti endpoint, è possibile fare clic sul nome di un file per visualizzarne il contenuto.
Proprietario dati	Il proprietario specificato dei dati riservati.
Indirizzo e-mail proprietario dati	L'indirizzo e-mail del proprietario dei dati riservati.

Sezione	Descrizione
Informazioni di accesso	<p>Le informazioni ACL disponibili. Applicabile esclusivamente ai sistemi di monitoraggio dell'unità locale Endpoint Discover e Endpoint Prevent.</p> <p>Vedere "Sezione Informazioni accesso dell'istantanea incidente" a pagina 1676.</p>

Altre sezioni dell'istantanea dell'incidente sono comuni in tutti i prodotti Symantec Data Loss Prevention. Queste sezioni comuni includono:

- Corrispondenze istantanee incidenti
Vedere ["Sezione delle corrispondenze delle istantanee di incidenti"](#) a pagina 1675.
- Sezione politica istantanea incidente
Vedere ["Sezione Politica dell'istantanea incidente"](#) a pagina 1675.
- Sezione correlazioni istantanea incidente
Vedere ["Scheda Correlazioni dell'istantanea incidente"](#) a pagina 1674.
- Sezione attributi istantanea incidente Questa sezione appare solo se un amministratore di sistema ha configurato attributi personalizzati.
Vedere ["Sezione Politica dell'istantanea incidente"](#) a pagina 1675.
- Scheda della cronologia delle istantanee incidente
Vedere ["Scheda della cronologia delle istantanee incidente"](#) a pagina 1673.
- Scheda note istantanea incidente
Vedere ["Scheda note istantanea incidente"](#) a pagina 1674.

L'istantanea ticket Endpoint contiene anche due sezioni non comuni in tutte le linee di prodotti. Le sezioni sono:

- Destinazione o informazioni specifiche del protocollo
Vedere ["Informazioni specifiche al protocollo o alla destinazione degli incidenti Endpoint"](#) a pagina 1604.
- Reporting nelle regole di risposta di Endpoint Prevent.
Vedere ["Creazione di report su regole di risposta di Endpoint Prevent"](#) a pagina 1602.

Creazione di report su regole di risposta di Endpoint Prevent

Se l'attività dell'utente sull'endpoint attiva più di una regola di risposta, Symantec Data Loss Prevention determina quale politica applicare in base a un ordine di precedenza stabilito. Viene eseguita solo la regola di risposta associata alla politica prevalente. Symantec Data Loss

Prevention crea incidenti per tutte le politiche violate. Indica (nelle istantanee di incidente rilevanti) che le regole di risposta sono state sostituite.

Vedere "[Istantanea ticket Endpoint](#)" a pagina 1597.

Per impostazione predefinita, il seguente elenco è l'ordine principale di precedenza per gli incidenti di Endpoint Prevent:

- Blocca
- Operazione annullata dall'utente
- Endpoint FlexResponse
- Notifica

Nota: Per Endpoint Discover, gli incidenti di quarantena hanno sempre la precedenza rispetto agli incidenti di Endpoint FlexResponse.

In merito alla creazione di report sugli incidenti sostituiti, tenere in considerazione il seguente comportamento:

- L'istantanea di un incidente blocco endpoint o operazione annullata dall'utente visualizza ancora l'icona **Bloccato** perché Symantec Data Loss Prevention non ha bloccato il contenuto in questione. L'icona indica inoltre se il contenuto è stato bloccato perché l'utente ha scelto di bloccare il contenuto. In alternativa, l'icona indica che il limite temporale di annullamento dell'operazione da parte dell'utente è stato superato e il contenuto è stato bloccato.
- L'istantanea di un incidente di notifica endpoint **non** include l'icona **Notifica**. L'icona di notifica non è inclusa perché Symantec Data Loss Prevention non ha visualizzato una specifica notifica su schermo configurata nella politica.
- L'istantanea di un incidente di quarantena endpoint sostituito visualizza l'icona **Bloccato** perché i dati non sono stati spostati all'esterno dell'area protetta. L'icona indica inoltre se il contenuto è stato bloccato perché l'utente ha scelto di bloccare il contenuto. In alternativa, l'icona indica che il limite temporale di annullamento dell'operazione da parte dell'utente è stato superato e il contenuto è stato bloccato. La scheda Cronologia dell'istantanea incidente visualizza sempre informazioni che indicano se la regola di Endpoint FlexResponse era corretta.
- L'istantanea di un incidente di FlexResponse endpoint sostituito visualizza l'icona **Bloccato** perché i dati non sono stati spostati all'esterno dell'area protetta. L'icona indica inoltre se una regola di risposta di Endpoint Quarantena è stata attivata.

Se sono state configurate delle regole di risposta per visualizzare notifiche su schermo che spingono gli utenti a giustificare le loro azioni, le seguenti dichiarazioni sono vere:

- Symantec Data Loss Prevention visualizza la giustificazione utente nelle istantanee di tutti gli incidenti generate dalle politiche che includono la regola di risposta eseguita.
- Symantec Data Loss Prevention visualizza la giustificazione **Sostituito – Sì** nelle istantanee di tutti gli incidenti che non includono la regola di risposta eseguita.
- Se non è presente alcun utente per l'inserimento di una giustificazione, ad esempio se un utente accede a un computer remoto, la giustificazione indica N/A.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Vedere ["Configurazione delle condizioni della regola di risposta"](#) a pagina 1492.

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

Vedere ["Gestione di regole di risposta"](#) a pagina 1489.

Informazioni specifiche al protocollo o alla destinazione degli incidenti Endpoint

A seconda del tipo di incidente, vengono visualizzate ulteriori informazioni associate all'istantanea incidente.

Tabella 48-5 Informazioni specifiche al protocollo o alla destinazione

Destinazione o protocollo	Descrizione
URL	Per gli incidenti di rete, denota l'URL in cui l'incidente si è verificato.
Porta e IP di origine	Per gli incidenti di rete, denota l'indirizzo IP o la porta dell'endpoint che ha originato l'incidente. Questa informazione viene visualizzata solo se l'incidente viene creato su questo endpoint.
Porta e IP di destinazione	L'indirizzo IP dell'endpoint di destinazione associato all'incidente. Questa informazione viene visualizzata solo se l'incidente viene creato su questo endpoint.
Indirizzo e-mail di mittente/destinatario	Per gli incidenti e-mail/SMTP e IM, gli incidenti contengono anche gli indirizzi e-mail del mittente e del destinatario. Questi indirizzi sono indicati solo se relativi all'incidente.
Oggetto	Viene visualizzata la riga dell'oggetto del messaggio e-mail/SMTP.
Nome utente FTP alla destinazione FTP	Per gli incidenti FTP, viene indicato il nome utente alla destinazione FTP.

Destinazione o protocollo	Descrizione
IP del server	Per gli incidenti FTP, viene visualizzato l'indirizzo IP del server.
Nome e posizione del file	Per gli incidenti di fax/stampa, sono indicati il nome e la posizione del file sull'endpoint.
Nome del processo di stampa	Per gli incidenti di fax/stampa, il nome del processo di stampa è il nome di file del processo di stampa che ha generato l'incidente.
Nome/tipo di stampante	Per gli incidenti di fax/stampa, il nome e il tipo di stampante sono visualizzati solo se il file non può essere denominato a partire dal nome del processo di stampa. Oppure se il file è stato generato da un browser Internet.
Finestra dell'applicazione	Per gli incidenti relativi agli Appunti, la finestra dell'applicazione è il nome dell'applicazione da cui proviene il contenuto degli Appunti.
Applicazione di origine	Per gli incidenti relativi agli Appunti, il nome dell'applicazione da cui proviene il contenuto degli Appunti.
Titolo della finestra dell'applicazione di origine	Per gli incidenti relativi agli Appunti, il nome della finestra dell'applicazione da cui proviene il contenuto degli Appunti.
Barra del titolo	Per gli incidenti relativi agli Appunti, la barra del titolo è la finestra da cui i dati sono stati copiati.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Report di riepilogo sugli incidenti endpoint

I report di riepilogo sugli incidenti endpoint forniscono informazioni sugli incidenti di endpoint riassunti da criteri specifici. È possibile riepilogare gli incidenti in base a uno o più tipi di criteri. Un report a riepilogo singolo è organizzato con un singolo criterio riepilogativo, quale la politica associata a ciascun incidente. Un report a riepilogo doppio è organizzato con due o più criteri, quali la politica e lo stato dell'incidente.

Nota: I report endpoint mostrano solo gli incidenti rilevati da Endpoint Prevent. Gli incidenti da Endpoint Discover compaiono nei report di Network Discover.

Per osservare i criteri sommari primari e secondari disponibili per il report, andare sul collegamento di **Riepiloga per**. Fare clic su **Modifica**. Nei menu a discesa **Primario e Secondario**, Symantec Data Loss Prevention visualizza tutti i criteri in ordine alfabetico, seguiti dai criteri personalizzati definiti dall'amministratore di sistema. È possibile selezionare i criteri a partire dal menù a discesa di **Primario e Secondario** e poi fare clic su **Esegui ora** per creare una nuova relazione di sintesi. I report riepilogativi prendono il nome dal criterio di riepilogo principale. Se si ripete l'esecuzione di un report con nuovi criteri, il nome del report cambia di conseguenza.

Vedere ["Informazioni sui filtri e sulle opzioni di riepilogo per i report"](#) a pagina 1677.

Le voci di riepilogo sono divise in varie colonne. Fare clic su qualsiasi intestazione di colonna per ordinare alfanumericamente in base ai dati di tale colonna. Per utilizzare l'ordine inverso, fare di nuovo clic sull'intestazione della colonna.

Tabella 48-6 Dettagli dei report di riepilogo sugli incidenti endpoint

Campo	Descrizione
Criteri di riepilogo	Questa colonna contiene il nome dei criteri di riepilogo selezionati. Se si seleziona un criterio di riepilogo principale e uno secondario, viene visualizzato solo quello principale.
Totale	Numero totale di incidenti associati all'elemento di riepilogo. Ad esempio, in un Riepilogo politica, questa colonna restituisce il numero totale di incidenti associati a ciascuna politica.
Alta	Numero degli incidenti di gravità elevata associati all'elemento di riepilogo. Il livello dell'incidente è determinato dall'impostazione di gravità della regola attivata.
Media	Numero degli incidenti di gravità media associati all'elemento di riepilogo.
Bassa	Numero degli incidenti di gravità bassa associati all'elemento di riepilogo.
Informazioni	Numero degli incidenti di carattere informativo associati all'elemento di riepilogo.
Grafico a barre	Rappresentazione visiva del numero degli incidenti (di tutti i livelli di gravità) associati all'elemento di riepilogo. La barra è suddivisa in sezioni proporzionali e colorate che rappresentano le diverse gravità.

Campo	Descrizione
Corrispondenze	<p>Numero totale di corrispondenze associate all'elemento di riepilogo.</p> <p>Se una delle colonne della gravità contiene totali, è possibile farvi clic sopra per visualizzare un elenco degli incidenti con la gravità scelta.</p>

Risoluzione di incidenti di rilevazione

Il capitolo contiene i seguenti argomenti:

- [Informazioni sui report per Network Discover](#)
- [Informazioni sui report incidente per Network Discover/Cloud Storage Discover](#)
- [Report incidente di Discover](#)
- [Elenchi di incidenti di Discover](#)
- [Azioni relative a incidenti di Discover](#)
- [Voci sugli incidenti di Discover](#)
- [Istantanea incidente di Discover](#)
- [Report riepilogativi di Discover](#)

Informazioni sui report per Network Discover

Symantec Data Loss Prevention include report relativi a incidenti, target di Network Discover/Cloud Storage Discover, informazioni di scansione e cronologia delle scansioni.

I report incidente di Network Discover/Cloud Storage Discover contengono informazioni sui dati riservati esposti.

Vedere ["Informazioni sui report incidente per Network Discover/Cloud Storage Discover"](#) a pagina 1610.

Per informazioni sui target e sulla cronologia delle scansioni di Network Discover/Cloud Storage Discover, accedere a **Gestisci > Scansione Discover > Target di Discover**, quindi selezionare uno dei target di Discover dall'elenco. Per informazioni sui dettagli delle scansioni di Network

Discover/Cloud Storage Discover, accedere a **Gestisci > Scansione Discover > Cronologia scansione**, quindi selezionare una delle scansioni di Discover dall'elenco.

Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.

[Tabella 49-1](#) elenca i report di Network Discover/Cloud Storage Discover.

Tabella 49-1 Report di Network Discover/Cloud Storage Discover

Report	Navigazione
Target di Network Discover/Cloud Storage Discover	<p>Per visualizzare questo report, nella console di amministrazione di Enforce Server, accedere al menu Gestisci e selezionare Scansione Discover > Target di Discover.</p> <p>Vedere "Informazioni sull'elenco dei target di scansione di Network Discover/Cloud Storage Discover" a pagina 1854.</p>
Stato scansione	<p>Per visualizzare questo report, nella console di amministrazione di Enforce Server, accedere al menu Gestisci e selezionare Scansione Discover > Discover Server.</p> <p>Vedere "Visualizzazione dello stato dei server Network Discover/Cloud Storage Discover" a pagina 1864.</p>
Cronologia scansioni (singolo target)	<p>Per visualizzare questo report, nella console di amministrazione di Enforce Server, accedere al menu Gestisci e selezionare Scansione Discover > Target di Discover. Fare clic sul collegamento nella colonna Stato scansione per consultare la cronologia di un particolare target di scansione.</p> <p>Vedere "Informazioni sulle cronologie di scansione Discover e Endpoint Discover" a pagina 1857.</p>
Cronologia scansioni (tutti i target)	<p>Per visualizzare questo report, nella console di amministrazione di Enforce Server, accedere al menu Gestisci e selezionare Scansione Discover > Cronologia scansioni.</p> <p>Vedere "Informazioni sulle cronologie di scansione Discover e Endpoint Discover" a pagina 1857.</p>
Dettagli scansione	<p>Per visualizzare questo report, nella console di amministrazione di Enforce Server, accedere al menu Gestisci e selezionare Scansione Discover > Cronologia scansioni. Fare clic sul collegamento nella colonna Stato scansione per visualizzare i dettagli della scansione.</p> <p>Vedere "Informazioni sui dettagli di scansione di rilevamento" a pagina 1860.</p>

Informazioni sui report incidente per Network Discover/Cloud Storage Discover

Utilizzare i report degli incidenti per seguire e rispondere agli incidenti Network Discover/Cloud Storage Discover. È possibile salvare, inviare, esportare o pianificare i report di Symantec Data Loss Prevention.

Vedere ["Informazioni sui report Symantec Data Loss Prevention"](#) a pagina 1632.

Nella console di amministrazione di Enforce Server, nel menu **Incidenti**, fare clic su **Discover**. Questo report incidenti visualizza tutti gli incidenti di tutti i target di Discover. È possibile selezionare i report standard per tutti gli incidenti, nuovi incidenti, il riepilogo dei target, la politica per target, lo stato per target o le condivisioni a rischio.

I riepiloghi e le opzioni di filtro possono selezionare gli incidenti da visualizzare.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Vedere ["Informazioni sui filtri e sulle opzioni di riepilogo per i report"](#) a pagina 1677.

È possibile creare report personalizzati con combinazioni di filtri e riepiloghi per identificare gli incidenti da risolvere.

Ad esempio, è possibile creare i seguenti report:

- Un report riepilogativo del numero di incidenti in ogni categoria di riparazione. Selezionare il riepilogo **Stato della protezione**.
- Un report di tutti gli incidenti riparati con la copia o la quarantena. Selezionare il filtro **Stato della protezione** con i valori **File copiato** e **File in quarantena**.
- Un report degli incidenti di Network Discover mai rilevati prima (per identificare questi incidenti e notificare ai proprietari dei dati che devono essere riparati). Selezionare il filtro **Rilevato in precedenza**. Impostare **No**.
- Un report degli incidenti di Network Discover che sono ancora presenti (per conoscere quali incidenti devono essere riassegnati per la riparazione). Selezionare il filtro **Rilevato in precedenza**. Impostare **Sì**.
- Un report che utilizza i filtri riepilogativi, come i mesi dal primo rilevamento. Selezionare il riepilogo **Mesi trascorsi dal primo rilevamento**.

Report incidente di Discover

Utilizzare i report incidente di Network Discover/Cloud Storage Discover per monitorare e rispondere agli incidenti di Network Discover/Cloud Storage Discover. È possibile salvare, inviare, esportare o pianificare i report di Symantec Data Loss Prevention.

Nella console di amministrazione di Enforce Server, nel menu **Incidenti**, fare clic su **Discover**. Questo report incidenti visualizza tutti gli incidenti di tutti i target di Discover. È possibile selezionare i report standard per tutti gli incidenti, nuovi incidenti, il riepilogo dei target, la politica per target, lo stato per target o le condivisioni a rischio.

I riepiloghi e le opzioni di filtro possono selezionare gli incidenti da visualizzare.

Vedere ["Filtro report incidente e opzioni di riepilogo"](#) a pagina 1671.

È possibile creare report personalizzati con combinazioni di filtri e riepiloghi per identificare gli incidenti da risolvere.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Per Network Discover sono disponibili i seguenti tipi di report:

- Elenco incidenti
Vedere ["Elenchi di incidenti di Discover"](#) a pagina 1611.
- Istantanea incidente
Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.
- Riepilogo incidenti
Vedere ["Report riepilogativi di Discover"](#) a pagina 1618.

Elenchi di incidenti di Discover

Un elenco di incidenti di Discover mostra gli incidenti segnalati durante le scansioni di Discover (compresi gli incidenti di Endpoint Discover). Singoli record di incidente contengono informazioni quali gravità, politica associata, numero di corrispondenze e stato.

Vedere ["Voci sugli incidenti di Discover"](#) a pagina 1613.

È possibile selezionare specifici incidenti (o un gruppo di incidenti) da modificare o riparare.

Vedere ["Azioni relative a incidenti di Discover"](#) a pagina 1611.

È possibile fare clic su qualsiasi incidente per visualizzare un'istantanea contenente più dettagli.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Report incidente di Discover"](#) a pagina 1610.

Azioni relative a incidenti di Discover

È possibile selezionare uno o più incidenti e quindi ripararli utilizzando i comandi nell'elenco a discesa **Azioni incidente**.

I comandi per gli incidenti sono i seguenti:

- **Aggiungi nota**

Selezionare questa opzione per aprire una finestra di dialogo, digitare un commento e quindi fare clic su **OK**.

- **Elimina incidenti**

Selezionare l'opzione per eliminare gli incidenti specificati.

- **Esporta selezioni: CSV**

Selezionare questa opzione per salvare gli incidenti specificati in un file di testo separato da virgole (.csv), visualizzabile in varie applicazioni comuni quali Microsoft Excel.

- **Esporta selezioni: XML**

Selezionare questa opzione per salvare gli incidenti specificati in un file XML, visualizzabile in varie applicazioni comuni.

- **Nascondi/Visualizza**

Selezionare una delle seguenti azioni per impostare lo stato di visualizzazione per gli incidenti selezionati:

- **Nascondi incidenti** : contrassegna come nascosti gli incidenti selezionati.
- **Visualizza incidenti** : ripristina la visualizzazione degli incidenti selezionati.
- **Non nascondere** : impedisce che gli incidenti selezionati vengano nascosti.
- **Consenti nascondi** - Consente di nascondere gli incidenti selezionati.

Vedere ["Informazioni su come nascondere gli incidenti"](#) a pagina 1696.

- **Imposta attributi**

Selezionare l'opzione per impostare attributi per gli incidenti selezionati.

- **Imposta proprietario dati**

Impostare il nome o l'indirizzo e-mail del proprietario dei dati. Il proprietario dei dati è la persona responsabile della riparazione dell'incidente.

I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.

- **Imposta stato**

Selezionare questa opzione per impostare lo stato.

- **Imposta gravità**

Selezionare questa opzione per impostare la gravità.

- **Attributi di ricerca**

Utilizzare i plug-in di ricerca per cercare gli attributi personalizzati di un incidente.

- **Esegui risposta smart**

Selezionare questa opzione per eseguire una regola di risposta smart configurata dall'utente o dall'amministratore.

Vedere ["Elenchi di incidenti di Discover"](#) a pagina 1611.

Voci sugli incidenti di Discover

Le informazioni sugli incidenti sono suddivise in varie colonne. Fare clic su qualsiasi intestazione di colonna per ordinare alfanumericamente in base ai dati di tale colonna. Per utilizzare l'ordine inverso, fare di nuovo clic sull'intestazione della colonna.

Il report include le colonne riportate di seguito:

- Caselle di controllo che consentono di selezionare gli incidenti da riparare.
È possibile selezionare uno o più incidenti a cui applicare i comandi del menu a discesa **Azioni incidente**.
Fare clic sulla casella di controllo in cima alla colonna o fare clic su **Seleziona tutto** per selezionare tutti gli incidenti nella pagina corrente.

Nota: Prestare attenzione quando si utilizza **Seleziona tutto**. Questa opzione seleziona tutti gli incidenti nel report, non solo quelli nella pagina corrente. Qualsiasi comando applicato successivamente riguarda tutti gli incidenti. È possibile configurare la proprietà `maximum-incident-batch-size` per limitare il numero di incidenti elaborati contemporaneamente da un plug-in di FlexResponse server.

Vedere ["Aggiunta di un plug-in FlexResponse server al file delle proprietà dei plug-in"](#) a pagina 1889.




■ Tipo

Il tipo di target in cui è stata rilevata la corrispondenza.


Un'icona rappresenta ogni tipo di target.

Questa colonna visualizza anche un'icona di riparazione se è stata applicata una regola di risposta.

I valori possibili sono:

	Vuoto se non è stata applicata alcuna regola di risposta.
	Copiato
	In quarantena
	Errore di riparazione

Quando si utilizza un'azione di FlexResponse server per una regola di risposta smart o automatica, è possibile che sia visualizzata una delle seguenti icone:

	Questo incidente è stato riparato utilizzando un'azione di FlexResponse server.
---	---



L'azione di FlexResponse server è in corso.



L'azione di FlexResponse server presenta un errore.

Queste icone possono essere visualizzate anche per altri tipi di incidenti, per i quali è possibile eseguire le azioni di FlexResponse server.

Vedere ["Configurazione dell'azione di FlexResponse server"](#) a pagina 1516.

- **Posizione/Target/Scansione**

Posizione di file o archivi, nome del target e data e ora della scansione più recente.

- **Proprietario file**

Nome utente del proprietario del file (ad esempio, MIODOMINIO\Administratore).

- **ID/Politica**

Il numero dell'incidente Symantec Data Loss Prevention e la politica violata dall'incidente.

- **Corrispondenze**

Il numero di corrispondenze nell'incidente.

- **Gravità**

Gravità dell'incidente determinata dall'impostazione di gravità della regola corrispondente.

I valori possibili sono:



Alta



Media



Bassa



Solo per informazione

- **Stato**

Lo stato corrente dell'incidente.

I valori possibili sono:

- **Nuovo**

- **In corso**

- **Riassegnato**

- **Falso positivo**

- **Errori di configurazione**

- **Risolto**

L'icona seguente può essere visualizzata vicino allo stato se l'incidente si è già verificato in precedenza:



Questa icona viene visualizzata se esiste un incidente precedente correlato.

L'utente o l'amministratore può aggiungere nuove designazioni di stato nella pagina di configurazione degli attributi.

Vedere ["Configurazione di attributi personalizzati"](#) a pagina 1709.

Vedere ["Elenchi di incidenti di Discover"](#) a pagina 1611.

Istantanea incidente di Discover

Un'istantanea incidente fornisce informazioni dettagliate riguardanti un incidente specifico. Visualizza informazioni generali sull'incidente, le corrispondenze rilevate nel contenuto e dettagli relativi alla politica, agli attributi e alla cronologia degli incidenti. È inoltre possibile cercare incidenti simili nell'area **Correlazioni**.

Lo stato attuale e la gravità vengono visualizzati sotto l'intestazione dell'istantanea. Per modificare uno dei valori correnti, fare clic su di esso e scegliere un altro valore nell'elenco a discesa.

Utilizzare le icone nella parte superiore destra per stampare il report o inviarlo come e-mail. Per inviare i report, l'utente o l'amministratore deve innanzitutto attivare la distribuzione dei report nelle impostazioni del sistema.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Se sono configurate le regole di risposta smart, Symantec Data Loss Prevention visualizza una barra di riparazione che include alcuni pulsanti per l'esecuzione delle regole. A seconda del numero di regole di risposta smart può venire visualizzato anche un menu a discesa.

Vedere ["Informazioni sulla riparazione degli incidenti"](#) a pagina 1570.

I dati dell'incidente sono divisi nelle seguenti sezioni:

- **Scheda Informazioni chiave**

- **Corrispondenze politica**

Vedere ["Sezione Politica dell'istantanea incidente"](#) a pagina 1675.

- **Dettagli incidente**

Vengono visualizzati i seguenti dettagli:

Server	Nome del Discover Server che ha rilevato l'incidente.
Stato rilevamento riparazione	Ultimo stato di riparazione del file che ha generato l'incidente.

Target	Nome del target Network Discover.
Scansione	Data e ora della scansione che ha registrato l'incidente.
Data rilevamento	Data e ora in cui è stato rilevato l'incidente.
Stato della protezione	Per gli incidenti Box visualizza lo stato di riparazione del contenuto che ha generato l'incidente.
Rilevato in precedenza	No, se l'incidente non è stato rilevato in precedenza. Sì, se l'incidente è stato rilevato in precedenza.
Oggetto	Oggetto dell'e-mail per le scansioni integrate di Exchange.
Mittente	Mittente dell'e-mail per le scansioni integrate di Exchange.
Destinatario	Destinatario dell'e-mail per le scansioni integrate di Exchange.
Posizione file	<p>Posizione del file, dell'archivio o dell'elemento.</p> <p>Fare clic su vai a file per visualizzare l'elemento o il file o su vai a directory per visualizzare la directory. Se si visualizza un incidente di Endpoint Discover, non vengono visualizzati i collegamenti vai a file e vai a directory.</p>
È nascosto	Visualizza lo stato nascosto dell'incidente, se l'incidente può essere nascosto, e consente di alternare il flag Non nascondere per l'incidente. Vedere " Informazioni su come nascondere gli incidenti " a pagina 1696.
URL	Per SharePoint questo URL è l'elemento sul server SharePoint. Fare clic su questo URL per accedere all'elemento sul server SharePoint.
Nome documento	Nome del file o dell'elemento.
Proprietario file	<p>Autore del file o dell'elemento.</p> <p>Per le istantanee di incidenti di SharePoint e Exchange, il proprietario del file è elencato come sconosciuto perché non è applicabile a questi tipi di target.</p>
Data estrazione	<p>Data in cui è stato eseguito l'adattatore del target (nel browser Firefox, questi collegamenti non funzionano senza una configurazione aggiuntiva.</p> <p>Applicabile solo ai target personalizzati.)</p>
Computer sottoposto a scansione	<p>Nome host del computer sottoposto a scansione.</p> <p>Per SharePoint questo nome è il nome dell'applicazione Web.</p>
Database di Notes	Nome del database di IBM (Lotus) Notes (applicabile solo a IBM (Lotus) Notes.)

File creato	Data e ora in cui è stato creato il file o l'elemento.
Ultima modifica	Data e ora dell'ultima modifica apportata al file o all'elemento.
Ultimo accesso	Data e ora dell'ultimo accesso dell'utente al file o all'elemento. Per SharePoint questa data non è valida.
Creato da	Utente che ha creato il file.
Modificato da	Utente che ha modificato per ultimo il file.
Nome proprietario dati	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente o con un plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione. Se si fa clic sul nome del proprietario dei dati con collegamento ipertestuale, viene visualizzato un elenco degli incidenti filtrato in base al nome del proprietario dei dati.
Indirizzo e-mail proprietario dati	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente o con un plug-in di ricerca. Se si fa clic sull' indirizzo e-mail del proprietario dei dati con collegamento ipertestuale, viene visualizzato un elenco degli incidenti filtrato in base all'indirizzo e-mail del proprietario dei dati.

■ Informazioni accesso

Vedere ["Sezione Informazioni accesso dell'istantanea incidente"](#) a pagina 1676.

Per le istantanee di incidenti di SharePoint, i livelli di autorizzazione mostrano le autorizzazioni di SharePoint, ad esempio **Contribuisci** o **Design**. L'elenco nell'istantanea di incidente mostra solo le prime 50 voci. Tutte le voci ACL possono venire esportate in un file CSV. Le autorizzazioni sono separate da virgole. Gli utenti o i gruppi che dispongono di livelli di autorizzazione Accesso limitato non vengono registrati o visualizzati.

Nota: Se si esegue la scansione di un archivio SharePoint senza utilizzare la soluzione SharePoint, l'istantanea dell'incidente non mostra alcuna informazione sulle autorizzazioni SharePoint.

Le istantanee di incidenti Box visualizzano informazioni sulle cartelle collaborative, tra cui i collaboratori e i ruoli.

■ Informazioni collegamento condiviso

Le istantanee incidente di archiviazione cloud visualizzano informazioni sul collegamento condiviso, tra cui se un collegamento è condiviso, se è protetto tramite password, se può essere scaricato e la data di scadenza del collegamento.

- **Corpo messaggio**

Per un elemento dell'elenco SharePoint, il corpo del messaggio mostra le coppie di nome e valore nell'elenco.

- **Attributi**

Vedere ["Sezione attributi istantanea incidente"](#) a pagina 1674.

- **Scheda Cronologia**

Vedere ["Scheda della cronologia delle istantanee incidente"](#) a pagina 1673.

- **Scheda Note**

Vedere ["Scheda note istantanea incidente"](#) a pagina 1674.

- **Scheda Correlazioni**

Vedere ["Scheda Correlazioni dell'istantanea incidente"](#) a pagina 1674.

- **Corrispondenze** e contenuto del file

Vedere ["Sezione delle corrispondenze delle istantanee di incidenti"](#) a pagina 1675.

Vedere ["Report incidente di Discover"](#) a pagina 1610.

Report riepilogativi di Discover

I report riepilogativi di Discover forniscono informazioni di riepilogo sugli incidenti rilevati durante le scansioni di Discover.

Se Endpoint Discover è in esecuzione, i report riepilogativi di Discover comprendono anche gli incidenti di Endpoint Discover.

È possibile filtrare o riepilogare le opzioni nei report.

Vedere ["Filtro report incidente e opzioni di riepilogo"](#) a pagina 1671.

È possibile estrarre le informazioni dei report nei formati selezionati.

È possibile fare clic sugli elementi evidenziati, come le voci nella colonna **Totali**, per visualizzare i dettagli.

Le icone consentono di spostarsi nei report lunghi.

Vedere ["Navigazione della pagina dei report incidente"](#) a pagina 1670.

Vedere ["Report incidente di Discover"](#) a pagina 1610.

Utilizzo di incidenti connettore cloud

Il capitolo contiene i seguenti argomenti:

- [Informazioni sui report incidente delle applicazioni](#)
- [Elenco di incidenti applicazione](#)
- [Voci sugli incidenti delle applicazioni](#)
- [Azioni incidente delle applicazioni](#)
- [Istantanea incidente delle applicazioni](#)
- [Report riepilogativi delle applicazioni](#)

Informazioni sui report incidente delle applicazioni

Utilizzare i report incidente delle applicazione per monitorare e gestire gli incidenti da connettori di servizi Cloud e dispositivi di rilevamento API per le app degli sviluppatori. È possibile salvare, inviare, esportare o pianificare i report di Symantec Data Loss Prevention.

Nella console di amministrazione di Enforce Server, nel menu **Incidenti**, fare clic su **Applicazioni**. Questo report incidente visualizza tutti gli incidenti di tutti i connettori cloud.

È possibile filtrare preventivamente i report incidente delle applicazioni secondo i tipi Dati a riposo e Dati in movimento:

- **Incidenti > Applicazioni > Dati a riposo**
- **Incidenti > Applicazioni > Dati in movimento**

È possibile visualizzare i seguenti report standard per tutti gli incidenti:

- **Incidenti - Tutti**

Visualizza un elenco di tutti gli incidenti.

Vedere ["Elenco di incidenti applicazione"](#) a pagina 1621.

- **DIM - Incidenti - Tutti**

Visualizza un elenco di tutti gli incidenti Dati in movimento (DIM).

Vedere ["Elenco di incidenti applicazione"](#) a pagina 1621.

- **DIM - Incidenti - Nuovi**

Visualizza un elenco di tutti gli incidenti DIM con stato **Nuovo**.

Vedere ["Elenco di incidenti applicazione"](#) a pagina 1621.

- **DIM - Riepilogo politica**

Visualizza un riepilogo degli incidenti DIM per politica.

Vedere ["Report riepilogativi delle applicazioni"](#) a pagina 1628.

- **DIM - Stato per politica**

Visualizza un riepilogo degli incidenti DIM per politica e stato dell'incidente.

Vedere ["Report riepilogativi delle applicazioni"](#) a pagina 1628.

- **DIM - Utenti a rischio elevato - Ultimi 30 giorni**

Visualizza un riepilogo degli incidenti DIM associati ad utenti ad alto rischio negli ultimi 30 giorni.

Vedere ["Report riepilogativi delle applicazioni"](#) a pagina 1628.

- **DAR - Incidenti - Tutti**

Visualizza un elenco di tutti gli incidenti Dati a riposo (DAR).

Vedere ["Elenco di incidenti applicazione"](#) a pagina 1621.

- **DAR - Incidenti - Nuovi**

Visualizza un elenco di tutti gli incidenti DAR con stato **Nuovo**.

Vedere ["Elenco di incidenti applicazione"](#) a pagina 1621.

- **DAR - Riepilogo per applicazione**

Visualizza un riepilogo degli incidenti DAR per applicazione cloud.

Vedere ["Report riepilogativi delle applicazioni"](#) a pagina 1628.

- **DAR - Riepilogo politica**

Visualizza un riepilogo degli incidenti DAR per politica.

Vedere ["Report riepilogativi delle applicazioni"](#) a pagina 1628.

- **DAR - Stato per applicazione**

Visualizza un riepilogo degli incidenti DAR per stato e applicazione cloud.

Vedere ["Report riepilogativi delle applicazioni"](#) a pagina 1628.

- **DAR - Utenti a rischio elevato**

Visualizza un riepilogo degli incidenti DAR associati ad utenti ad alto rischio.

Vedere ["Report riepilogativi delle applicazioni"](#) a pagina 1628.

I riepiloghi e le opzioni di filtro possono selezionare gli incidenti da visualizzare.

Vedere ["Filtro report incidente e opzioni di riepilogo"](#) a pagina 1671.

È possibile creare report personalizzati con combinazioni di filtri e riepiloghi per monitorare gli incidenti.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Le applicazioni hanno i seguenti tipi di report:

- Elenco incidenti
Vedere ["Elenco di incidenti applicazione"](#) a pagina 1621.
- Istantanea incidente
Vedere ["Istantanea incidente delle applicazioni"](#) a pagina 1624.
- Riepilogo incidenti
Vedere ["Report riepilogativi delle applicazioni"](#) a pagina 1628.

Elenco di incidenti applicazione

Un elenco di incidenti applicazione mostra gli incidenti segnalati da un connettore servizio cloud un dispositivo di rilevamento API per le app degli sviluppatori. Singoli record di incidente contengono informazioni quali gravità, politica associata, numero di corrispondenze e stato.

Vedere ["Voci sugli incidenti delle applicazioni"](#) a pagina 1621.

È possibile selezionare specifici incidenti (o un gruppo di incidenti) da modificare o gestire.

Vedere ["Azioni incidente delle applicazioni"](#) a pagina 1623.

È possibile fare clic su qualsiasi incidente per visualizzare un'istantanea contenente più dettagli.

Vedere ["Istantanea incidente delle applicazioni"](#) a pagina 1624.

Vedere ["Informazioni sui report incidente delle applicazioni"](#) a pagina 1619.

Voci sugli incidenti delle applicazioni

Le informazioni sugli incidenti sono suddivise in varie colonne. Fare clic su qualsiasi intestazione di colonna per ordinare alfanumericamente i dati in tale colonna. Per utilizzare l'ordine inverso, fare di nuovo clic sull'intestazione della colonna.

Il report include le colonne riportate di seguito:

- Caselle di controllo che consentono di selezionare gli incidenti da gestire.
È possibile selezionare uno o più incidenti a cui applicare i comandi del menu a discesa **Azioni incidente**.

Fare clic sulla casella di controllo in cima alla colonna o fare clic su **Seleziona tutto** per selezionare tutti gli incidenti nella pagina corrente.

Nota: Prestare attenzione quando si utilizza **Seleziona tutto**. Questa opzione seleziona tutti gli incidenti nel report, non solo quelli nella pagina corrente. Qualsiasi comando applicato successivamente riguarda tutti gli incidenti.

- **Tipo di dati**

Specifica se l'incidente proviene da un **Connettore DAR** o un **Connettore DIM**.

- **Posizione/Applicazione/Data rilevamento**

La posizione dei dati riservati, l'applicazione a cui è associato l'incidente e la data in cui è stata rilevata la violazione della politica.

- **Utente**

Visualizza le informazioni dell'utente associato all'incidente, se applicabile.

- **ID/Politica**

Il numero dell'incidente Symantec Data Loss Prevention e la politica violata dall'incidente.

- **Corrispondenze**

Il numero di corrispondenze nell'incidente.

- **Gravità**

Gravità dell'incidente determinata dall'impostazione di gravità della regola corrispondente. I valori possibili sono:



Alta



Media



Bassa



Solo per informazione

- **Stato**

Lo stato corrente dell'incidente. I valori possibili sono:

- **Nuovo**

- **In corso**

- **Riassegnato**

- **Falso positivo**

- **Errori di configurazione**

- **Risolto**

Vedere ["Elenco di incidenti applicazione"](#) a pagina 1621.

Azioni incidente delle applicazioni

È possibile selezionare uno o più incidenti e poi gestirli mediante i comandi dell'elenco a discesa **Azioni incidente**.

I comandi per gli incidenti sono i seguenti:

- **Aggiungi nota**
Selezionare questa opzione per aprire una finestra di dialogo, digitare un commento e quindi fare clic su **OK**.
- **Elimina incidenti**
Selezionare l'opzione per eliminare gli incidenti specificati.
- **Esporta selezioni: CSV**
Selezionare questa opzione per salvare gli incidenti specificati in un file di testo separato da virgole (.csv), visualizzabile in varie applicazioni comuni quali Microsoft Excel.
- **Esporta selezioni: XML**
Selezionare questa opzione per salvare gli incidenti specificati in un file XML, visualizzabile in varie applicazioni comuni.
- **Segna come accettato**
Selezionare per impostare lo stato di riparazione su **Accettato**.
- **Esegui risposta smart**
Selezionare per eseguire le regole di risposta smart **Quarantena** o **Ripristina file**.
- **Nascondi/Visualizza**
Selezionare una delle seguenti azioni per impostare lo stato di visualizzazione per gli incidenti selezionati:
 - **Nascondi incidenti** : contrassegna come nascosti gli incidenti selezionati.
 - **Visualizza incidenti** : ripristina la visualizzazione degli incidenti selezionati.
 - **Non nascondere** : impedisce che gli incidenti selezionati vengano nascosti.
 - **Consenti nascondi** - Consente di nascondere gli incidenti selezionati.Vedere ["Informazioni su come nascondere gli incidenti"](#) a pagina 1696.
- **Imposta attributi**
Selezionare l'opzione per impostare attributi per gli incidenti selezionati.
- **Imposta proprietario dati**
Selezionare per impostare il proprietario dei dati per nome utente o per indirizzo e-mail.

- **Imposta gravità**

Selezionare questa opzione per impostare la gravità.

- **Imposta stato**

Selezionare questa opzione per impostare lo stato.

Vedere ["Elenco di incidenti applicazione"](#) a pagina 1621.

Istantanea incidente delle applicazioni

Un'istantanea incidente fornisce informazioni dettagliate riguardanti un incidente specifico. Visualizza informazioni generali sull'incidente, le corrispondenze rilevate nel contenuto e dettagli relativi alla politica, agli attributi e alla cronologia degli incidenti. È inoltre possibile cercare incidenti simili nell'area **Correlazioni**.

Lo stato attuale e la gravità vengono visualizzati sotto l'intestazione dell'istantanea. Per modificare uno dei valori correnti, fare clic su di esso e scegliere un altro valore nell'elenco a discesa.

È possibile utilizzare la casella di controllo **Accettato** per impostare lo stato di riparazione su **Accettato dall'utente**. Questo stato di riparazione indica che l'incidente è stato riparato dall'utente, dall'amministratore CASB o da un altro risponditore di incidenti.

Utilizzare le icone nella parte superiore destra per stampare il report o inviarlo come e-mail. Per inviare i report, l'utente o l'amministratore deve innanzitutto attivare la distribuzione dei report nelle impostazioni del sistema.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

I dati dell'incidente del connettore cloud sono suddivisi nelle seguenti sezioni:

- Scheda **Informazioni chiave** :

- **Corrispondenze politica**

Vedere ["Sezione Politica dell'istantanea incidente"](#) a pagina 1675.

- **Dettagli incidente**

I seguenti dettagli sono inclusi sia per gli incidenti DAR sia per gli incidenti DIM:

Tipo di dati Specifica il tipo di dati DAR o DIM.

Rilevatore Specifica il rivelatore di cloud che ha creato l'incidente.

È nascosto Visualizza lo stato nascosto dell'incidente, se l'incidente può essere nascosto, e consente di alternare il flag **Non nascondere** per l'incidente. Vedere ["Informazioni su come nascondere gli incidenti"](#) a pagina 1696.

Destinatario Per i caricamenti di dati, il destinatario è il sito in cui vengono caricati i dati.
Per i download di dati, il destinatario è l'utente che scarica i dati.

Data	La data in cui è stato creato l'incidente.
Oggetto	Il campo dell'oggetto dei dati riservati. Fare clic sul collegamento dell'oggetto per visualizzare tutti gli incidenti con lo stesso oggetto.
Nome proprietario dati	<p>La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente.</p> <p>I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.</p> <p>Fare clic su Nome proprietario dati per visualizzare un elenco filtrato degli incidenti per quel proprietario di dati.</p>
Indirizzo e-mail proprietario dati	<p>L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente.</p> <p>Fare clic su Indirizzo e-mail proprietario dati per visualizzare un elenco filtrato degli incidenti per quell'indirizzo e-mail del proprietario di dati.</p>
ID richiesta	L'identificatore univoco della richiesta di rilevamento dal connettore servizio cloud. È possibile utilizzare questo identificatore per tenere traccia di questo incidente in console cloud esterne, come Symantec CloudSOC.
Nome utente	Il nome dell'utente associato all'incidente.
Tipo attività utente	<p>Specifica il tipo di attività dell'utente sul file. Le attività possibili sono:</p> <ul style="list-style-type: none"> ■ Crea ■ Modifica ■ Rinomina ■ Elimina ■ Carica/scarica
ID transazione esterna	L'identificatore univoco della transazione fornito dall'applicazione cloud. È possibile utilizzare questo identificatore per tenere traccia di questo incidente in console cloud esterne, come Symantec CloudSOC.
<p>■ Dettagli sito/applicazione</p> <p>Specifica i seguenti dettagli sul sito Web o l'applicazione cloud associata all'incidente DAR o DIM:</p>	
Punteggio servizio	Il punteggio shadow IT fornito da Symantec CloudSOC.
Nome applicazione	Il nome dell'applicazione cloud associata all'incidente.
Punteggio di rischio sito	Il punteggio di rischio del sito fornito da Blue Coat WSS, in base alle informazioni di Global Intelligence Network.

URL HTTP L'URL HTTP cui ha acceduto l'utente.

■ **Dettagli utente**

Questa sezione fornisce i seguenti dettagli sull'utente associato all'incidente DAR o DIM:

Punteggio minaccia utente	Specifica il punteggio di minaccia dell'utente fornito da Symantec CloudSOC o Blue Coat WSS.
Totale documenti rivelato	Specifica il numero di documenti esposti per quell'utente. Fare clic su Ulteriori informazioni per visualizzare informazioni sull'esposizione del documento nella console cloud esterna.
Attività utente	Fornisce un collegamento ai dettagli dell'attività utente nella console cloud esterna.

■ **Dettagli rivelazione dati (solo DAR)**

Questa sezione fornisce i seguenti dettagli sull'esposizione dei dati sensibili:

Documento rivelato pubblicamente	Specifica se il documento è esposto in una posizione pubblicamente accessibile.
Documento condiviso internamente	Specifica se il documento è condiviso con i membri dell'organizzazione.
Documento rivelato	Specifica se il documento è esposto all'esterno dell'organizzazione.
Documento interno	Specifica se il documento è all'interno dell'organizzazione.
Totale attività documenti	Specifica il numero di accessi al documento.
ID autore documento	L'identificatore dell'autore del documento.
ID documento	L'identificatore del documento.
ID cartella principale documento	L'identificatore della cartella contenente il documento.

■ Informazioni file (solo DAR)

Questa sezione specifica le seguenti informazioni sul file contenente i dati riservati:

Cartella file	Specifica la cartella che contiene il file. Fare clic su Ulteriori informazioni per accedere alla finestra delle esposizioni per quel file.
Ultima modifica	Specifica la data e l'ora dell'ultima modifica del file.
URL di condivisione	Specifica l'URL in cui è stato condiviso il file.
Tipo documento	Specifica il tipo di documento del file.
Attività file	Fare clic su Ulteriori informazioni per visualizzare l'attività file nella console cloud esterna.
Avviso in CASB	Fare clic su Ulteriori informazioni per visualizzare informazioni sull'incidente nella console cloud esterna.

■ Trasferimento dei dati (solo DIM)

Specifica i seguenti dettagli sul dispositivo associato all'incidente DIM:

Direzione rete	Specifica la direzione del traffico di rete, upload o download.
Protocollo di origine connettore	Specifica il protocollo di rete del trasferimento dei dati, ad esempio <code>https</code> .
IP origine	Specifica l'indirizzo IP di origine del traffico di rete.
IP destinazione	Specifica l'indirizzo IP di destinazione del traffico di rete.
Dispositivo conforme	Specifica se il dispositivo è conforme agli standard dell'organizzazione.
Dispositivo non gestito	Specifica se il dispositivo non è gestito dall'organizzazione.
Dispositivo personale	Specifica se il dispositivo è di proprietà personale dell'utente.
Dispositivo attendibile	Specifica se il dispositivo è ritenuto attendibile dall'organizzazione.
Metodo HTTP	Specifica il metodo HTTP utilizzato durante la creazione dell'incidente.
Cookie HTTP	Elenco i cookie eventualmente associati all'incidente.

Sistema operativo dispositivo Specifica il sistema operativo del dispositivo.

Tipo di dispositivo Specifica il tipo di dispositivo.

- **Posizione (solo DIM)**

Specifica le seguenti informazioni sulla posizione del dispositivo:

Posizione Specifica la città e il paese in cui si trova il dispositivo.

Latitudine Specifica la coordinata della latitudine del dispositivo.

Longitudine Specifica la coordinata della longitudine del dispositivo.

- **Corpo messaggio**

Fornisce un collegamento al messaggio originale con formattazione JSON.

- **Cronologia**

Vedere ["Scheda della cronologia delle istantanee incidente"](#) a pagina 1673.

- **Note**

La scheda Note visualizza eventuali note disponibili per l'incidente.

- **Correlazioni**

Vedere ["Scheda Correlazioni dell'istantanea incidente"](#) a pagina 1674.

- **Corrispondenze**

Vedere ["Sezione delle corrispondenze delle istantanee di incidenti"](#) a pagina 1675.

Vedere ["Informazioni sui report incidente delle applicazioni"](#) a pagina 1619.

Report riepilogativi delle applicazioni

I report riepilogativi delle applicazioni forniscono informazioni riassuntive sugli incidenti delle applicazioni.

È possibile filtrare o riepilogare le opzioni nei report.

Vedere ["Filtro report incidente e opzioni di riepilogo"](#) a pagina 1671.

È possibile estrarre le informazioni dei report nei formati selezionati.

È possibile fare clic sugli elementi evidenziati, come le voci nella colonna **Totali**, per visualizzare informazioni dettagliate.

Le icone consentono di spostarsi nei report lunghi.

Vedere ["Navigazione della pagina dei report incidente"](#) a pagina 1670.

Vedere ["Informazioni sui report incidente delle applicazioni"](#) a pagina 1619.

Gestione e report degli incidenti

Il capitolo contiene i seguenti argomenti:

- Informazioni sui report Symantec Data Loss Prevention
- Informazioni sulle strategie per l'utilizzo di report
- Impostazione delle preferenze di report
- Informazioni sui report degli incidenti
- Informazioni sui report dashboard e i riepiloghi executive
- Visualizzazione di dashboard
- Creazione di report di dashboard
- Configurazione report della dashboard
- Scelta dei report da includere in un dashboard
- Informazioni sui report riepilogativi
- Visualizzazione di report riepilogativi
- Creazione di report riepilogativi
- Visualizzazione degli incidenti
- Informazioni su report e dashboard personalizzati
- Utilizzo di IT Analytics per la gestione di incidenti
- Report di filtraggio

- Salvataggio dei report di incidente personalizzati
- Pianificazione dei report di incidente personalizzati
- Opzioni di pianificazione di consegna per i report di incidente e di sistema
- Opzioni di pianificazione di consegna per i report del dashboard
- Utilizzo del widget della data per pianificare i report
- Modifica dei dashboard e dei report personalizzati
- Esportazione dei report di incidente
- Campi esportati per Network Monitor
- Campi esportati per Network Discover/Cloud Storage Discover
- Campi esportati per Endpoint Discover
- Eliminazione di incidenti
- Eliminazione dei dashboard e dei report personalizzati
- Caratteristiche report incidenti più comuni
- Navigazione della pagina dei report incidente
- Filtro report incidente e opzioni di riepilogo
- Invio dei report degli incidenti tramite e-mail
- Stampa di report di incidenti
- Scheda della cronologia delle istantanee incidente
- Scheda note istantanea incidente
- Sezione attributi istantanea incidente
- Scheda Correlazioni dell'istantanea incidente
- Sezione Politica dell'istantanea incidente
- Sezione delle corrispondenze delle istantanee di incidenti
- Sezione Informazioni accesso dell'istantanea incidente
- Personalizzazione della pagina dell'istantanea incidente
- Informazioni sui filtri e sulle opzioni di riepilogo per i report
- Filtri generali per i report

- [Opzioni di riepilogo per i report di incidente](#)
- [Opzioni di filtro avanzate per i report](#)

Informazioni sui report Symantec Data Loss Prevention

Utilizzare i report degli incidenti per seguire e rispondere agli incidenti. Symantec Data Loss Prevention segnala un incidente quando rileva dati che corrispondono ai parametri di rilevamento di una regola di politica.

Tali dati possono includere il contenuto di un file specifico, il mittente o il destinatario di un'e-mail, le proprietà di un allegato o molti altri tipi di informazioni.

Ogni dato corrispondente ai parametri di rilevamento viene denominato corrispondenza e un singolo incidente può includere un numero qualsiasi di corrispondenze.

È possibile impostare un flag nascosto su un incidente per indicare che l'incidente è stato nascosto. Per impostazione predefinita, gli incidenti nascosti non vengono visualizzati nei report incidenti, ma è possibile includerli nei report incidenti impostando **Filtri avanzati** sul report. Includere gli incidenti nascosti in un report potrebbe rallentare le attività di reporting. Vedere ["Informazioni su come nascondere gli incidenti"](#) a pagina 1696.

Symantec Data Loss Prevention traccia gli incidenti per tutti i server di rilevamento. Questi server includono Network Discover/Cloud Storage Discover Server, Network Monitor Server, Network Prevent for Email Server, Network Prevent for Web Server ed Endpoint Server.

È possibile specificare i report che Symantec Data Loss Prevention visualizza nel pannello di navigazione.

Vedere ["Impostazione delle preferenze di report"](#) a pagina 1634.

Symantec Data Loss Prevention fornisce i seguenti tipi di report di incidente:

- Gli elenchi di incidenti visualizzano i singoli record di incidente che contengono informazioni quali gravità, politica collegata, numero di corrispondenze e stato. È possibile fare clic su un incidente per visualizzare un'istantanea contenente più dettagli. Ed è possibile selezionare specifici incidenti (o gruppi di incidenti) da modificare o riparare. Symantec Data Loss Prevention fornisce report separati per gli incidenti selezionando **Rete, Endpoint, Discover o Utente**.
- I riepiloghi forniscono informazioni sugli incidenti nel sistema. Sono organizzati con uno o due criteri di riepilogo. Un report a riepilogo singolo è organizzato con un singolo criterio riepilogativo, come la politica associata a ciascun incidente. Un report a riepilogo doppio è organizzato con due criteri, quali la politica e lo stato dell'incidente. Per impostazione predefinita, gli incidenti nascosti non compaiono nei conteggi visualizzati nei report di

riepilogo, ma è possibile impostare i Filtri avanzati in modo da includere gli incidenti nascosti. (Vedere ["Informazioni su come nascondere gli incidenti"](#) a pagina 1696.)

- I dashboard riuniscono informazioni da diversi report. Includono grafici e totali di incidenti che rappresentano i contenuti dei diversi elenchi e riepiloghi degli incidenti. A volte, i grafici possono contenere elenchi di incidenti molto gravi o elenchi di gruppi di riepiloghi. È possibile fare clic su portlet di report (singoli riquadri che contengono dati di report) per accedere alle versioni dettagliate dei report.

I quadri generali sono simili ai dashboard. Includono informazioni simili, presentandole in modo intuitivo e di facile lettura. Non è possibile personalizzare un quadro generale. I quadri generali non includono portlet di report.

Symantec Data Loss Prevention viene fornito con quadri generali per incidenti **Rete**, **Endpoint** e **Discover**.

È possibile creare e salvare versioni personalizzate di tutti i report (tranne i quadri generali) per un uso continuato.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Symantec Data Loss Prevention visualizza i report in sezioni separate nella schermata **Incidente > Tutti i report** come segue:

- La sezione **Report salvati** contiene qualsiasi report condiviso associato al ruolo corrente. Questa sezione viene visualizzata solo se gli utenti del ruolo corrente hanno creato report salvati.
Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.
- La sezione **Rete** contiene elenchi di incidenti forniti da Symantec, riepiloghi e dashboard per incidenti di rete.
- La sezione **Endpoint** contiene elenchi di incidenti forniti da Symantec, riepiloghi e dashboard per incidenti endpoint. I report endpoint includono gli incidenti acquisiti da Endpoint, come incidenti Endpoint: blocca e Endpoint: notifica.
Incidenti acquisiti da Endpoint Discover vengono visualizzati nei report Discover.
- La sezione **Discover** contiene elenchi di incidenti forniti da Symantec, riepiloghi e dashboard per incidenti Network Discover/Cloud Storage Discover ed Endpoint Discover.
- La sezione **Applicazioni** contiene elenchi di incidenti forniti da Symantec e riepiloghi per incidenti dell'applicazione cloud.
- La sezione **Utenti** contiene l'elenco utenti e il riepilogo dei rischi utente, visualizzando utenti e relativi incidenti E-mail ed Endpoint.

Informazioni sulle strategie per l'utilizzo di report

Molte società configurano il reporting Symantec Data Loss Prevention in modo da soddisfare le seguenti regole principali:

- Un responsabile esecutivo per la riduzione complessiva dei rischi che monitora le tendenze dei rischi e sviluppa iniziative di livello elevato per rispondere a tali tendenze.
Il responsabile controlla i dashboard e i report riepilogativi (per ottenere un'immagine generale delle tendenze di perdita di dati nell'organizzazione). Il responsabile sviluppa inoltre i programmi e le iniziative per ridurre il rischio e comunica queste informazioni agli autori della politica e ai risponditori degli incidenti. Il responsabile controlla spesso i report tramite l'e-mail o altri formati di report esportati.
I dashboard e i report riepilogativi Symantec Data Loss Prevention consentono di verificare le tendenze di rischio nell'organizzazione. Questi report forniscono una panoramica di livello elevato degli incidenti. I responsabili e i manager possono valutare rapidamente le tendenze di rischio e informare gli autori delle politiche e i risponditori degli incidenti su come affrontare queste tendenze. È possibile visualizzare i dashboard e i report riepilogativi esistenti e creare le versioni personalizzate di questi report.
Vedere ["Informazioni sui report dashboard e i riepiloghi executive"](#) a pagina 1637.
Vedere ["Informazioni sui report riepilogativi"](#) a pagina 1643.
- Un risponditore di incidenti, come un analista InfoSec o un manager InfoSec, che monitora e risponde a particolari incidenti.
Il risponditore monitora le istantanee e i report dell'incidente per rispondere agli incidenti associati a un particolare gruppo di politica, dipartimento organizzativo o posizione geografica. Il risponditore potrebbe inoltre creare politiche per ridurre il rischio. Queste politiche possono essere originate alla direzione di un manager di riduzione dei rischi o basate sull'esperienza di rilevamento degli incidenti.
Vedere ["Informazioni sulla riparazione degli incidenti"](#) a pagina 1570.

Impostazione delle preferenze di report

È possibile specificare i report che Symantec Data Loss Prevention visualizza nel pannello di navigazione per ognuno dei tipi di report.

Per impostare le preferenze di reporting

- 1 Nella console di amministrazione di Enforce Server, nel menu **Incidenti**, fare clic su **Tutti i report**.
- 2 Nella schermata **Tutti i report**, fare clic su **Modifica preferenze**.

La schermata **Modifica preferenze report** elenca tutti i report salvati (per tutti i ruoli assegnati).

La schermata elenca anche i report di Rete, Endpoint e Discover.

- 3 Per visualizzare un report nell'elenco, selezionare la casella **Mostra report** per tale report. Per rimuovere un report dall'elenco, deselezionare **Mostra report** per tale report.

L'elenco dei report selezionato viene visualizzato in un pannello di navigazione sinistro per ogni tipo di report.

Ad esempio, per visualizzare l'elenco dei report di Rete, nel menu **Incidenti**, fare clic su **Rete**.

- 4 Dopo avere modificato le preferenze, fare clic su **Salva**.

Vedere "[Informazioni su report e dashboard personalizzati](#)" a pagina 1646.

Informazioni sui report degli incidenti

Utilizzare i report degli incidenti per seguire e rispondere agli incidenti sulla rete. Symantec Data Loss Prevention segnala un incidente quando rileva dati che corrispondono a una regola di rilevamento all'interno di una politica attiva. Tali dati possono includere il contenuto di un file specifico, il mittente o il destinatario di un'e-mail, le proprietà di un allegato o molti altri tipi di informazioni. Ogni dato corrispondente a una regola di rilevamento viene denominata corrispondenza e un singolo incidente può includere un numero qualsiasi di corrispondenze.

Nota: È possibile configurare quali report visualizzare nel pannello di navigazione. Per fare ciò, accedere a **Tutti i report** e fare clic su **Modifica preferenze**

Symantec Data Loss Prevention fornisce i seguenti tipi di report degli incidenti:

Elenchi di incidenti	Consente di visualizzare i singoli record di incidente che contengono informazioni quali gravità, politica collegata, numero di corrispondenze e stato. È possibile fare clic su un incidente per visualizzare un'istantanea contenente più dettagli. È possibile selezionare specifici incidenti o gruppi di incidenti da modificare o riparare.
Riepiloghi	Mostrano i totali degli incidenti organizzati per un attributo specifico di incidente come lo stato o una politica associata. Ad esempio, un Riepilogo politica include le righe di tutte le politiche che hanno associato gli incidenti. Ogni riga include un nome di politica, il numero totale di incidenti associati e i totali degli incidenti per gravità. È possibile fare clic su cliccare sopra qualsiasi punteggio di gravità totale per visualizzare l'elenco degli incidenti più importanti.
Riepiloghi doppi	Mostrano il numero totale di incidenti per due attributi di incidente. Ad esempio, un riepilogo di tendenza della politica mostra gli incidenti totali organizzati per politica e settimana. Simile al riepilogo della politica, ogni voce include un nome di politica, il numero totale di incidenti associati e i totali degli incidenti per gravità. Inoltre, ogni voce include una riga separata per ogni settimana, mostrando i totali degli incidenti della settimana e gli incidenti per gravità.

Dashboard e quadri generali	<p>Si tratta di dashboard di guida rapida che riuniscono informazioni da diversi report. Includono grafici e totali di incidenti che rappresentano i contenuti dei diversi elenchi incidenti, riepiloghi e riepiloghi doppi. A volte, i grafici si trovano a fianco di elenchi di incidenti molto gravi o elenchi di gruppi di riepiloghi. È possibile fare clic su nomi di report costitutivi per accedere ai report visualizzati sulla dashboard.</p> <p>Symantec Data Loss Prevention viene fornito con i riepiloghi generali per report relativi a Rete, Endpoint e Discover, opzioni non personalizzabili.</p> <p>È possibile creare le dashboard e personalizzarle secondo le proprie necessità.</p>
Personalizzato	Elenca i report condivisi associati al ruolo attuale. (Tali report vengono visualizzati solo se sono stati creati dall'utente in uso o da altri utenti con il ruolo attuale).
Rete	Elenca i report di incidente della rete.
Endpoint	<p>Elenca i report dei ticket Endpoint. I report Endpoint includono incidenti come Endpoint: blocca ed Endpoint: notifica.</p> <p>Gli incidenti ricevuti da Endpoint Discover vengono inclusi nei report Discover.</p>
Discover	<p>Elenca tutti i report degli incidenti di Network Discover/Cloud Storage Discover e Endpoint Discover.</p> <p>La cartella report dei rischi visualizza le cartelle di condivisione file ordinate per priorità del rischio. Il punteggio di rischio è basato sulle informazioni rilevanti degli incidenti di Symantec Data Loss Prevention e sulle informazioni del server di gestione VML.</p> <p>Vedere la <i>Guida all'implementazione di Symantec Data Loss Prevention Data Insight</i>.</p>
Utenti	Elenco utenti elenca gli utenti dei dati all'interno dell'organizzazione. Riepilogo rischi utente elenca tutti gli utenti e i relativi incidenti E-mail ed Endpoint associati.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Vedere ["Elenco degli incidenti di rete"](#) a pagina 1580.

Vedere ["Elenchi di incidenti di Discover"](#) a pagina 1611.

Vedere ["Informazioni sugli elenchi di incidenti endpoint"](#) a pagina 1594.

Informazioni sui report dashboard e i riepiloghi executive

I dashboard e i quadri generali sono le schermate di report di guida rapida che presentano informazioni riepilogative provenienti da diversi report di incidenti.

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

I dashboard presentano due colonne di report. La colonna sinistra mostra un grafico a torta o un diagramma e una barra di totali relativa agli incidenti. La colonna destra mostra gli stessi tipi di informazione della colonna sinistra. La colonna destra mostra inoltre un elenco degli incidenti più significativi o un elenco degli elementi riepilogativi con totali degli incidenti associati. Gli incidenti più significativi vengono classificati in base alla gravità e al numero delle corrispondenze. È possibile fare clic su un report per visualizzare il report completo che rappresenta.

Le dashboard sono composte da un massimo di sei portlet, ciascuna delle quali fornisce un rapido riepilogo di un report specificato.

È possibile creare dashboard personalizzate per gli utenti con responsabilità specifiche in termini di sicurezza. Se si sceglie di condividere una dashboard, questa sarà accessibile a tutti gli utenti nel ruolo con cui è stata creata. (Si noti che l'utente Amministratore non può condividere dashboard condivise.)

Le dashboard hanno due colonne di portlet di report (tasselli che contengono dati dei report). I portlet nella colonna sinistra mostrano un grafico a torta o un grafico e la barra dei totali. I portlet nella colonna destra mostrano lo stesso tipo di informazioni della colonna sinistra. Tuttavia, mostrano anche un elenco degli incidenti più significativi o dei criteri riepilogativi e degli incidenti a essi collegati. Gli incidenti vengono classificati in base alla gravità e al numero delle corrispondenze. I criteri riepilogativi evidenziano i totali degli incidenti ad alta gravità. È possibile scegliere fino a tre report da includere nella colonna sinistra e fino a tre report da includere in quella destra.

Per creare dashboard personalizzate, fare clic su **Report incidente** nella parte superiore del pannello di navigazione e, nella schermata **Report incidente** visualizzata, fare clic su **Crea dashboard**. L'amministratore può creare solo dashboard private, tuttavia altri utenti possono decidere se condividere una nuova dashboard o mantenerla privata.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Per modificare il contenuto di qualsiasi dashboard personalizzata, passare alla dashboard desiderata e fare clic su **Personalizza** vicino alla parte superiore dello schermo.

Vedere ["Configurazione report della dashboard"](#) a pagina 1641.

Per visualizzare una dashboard personalizzata all'accesso, specificarla come report di accesso predefinito.

Vedere ["Impostazione delle preferenze di report"](#) a pagina 1634.

Symantec Data Loss Prevention comprende tre quadri generali: **Quadro generale - Discover**, **Quadro generale - Endpoint**, e **Quadro generale - Rete**. A differenza dei dashboard, i quadri generali non possono essere creati o personalizzati.

I quadri generali includono i seguenti report:

Quadro generale - Discover

- **Distribuzione politiche nelle destinazioni** : Un grafico a torta che specifica la distribuzione delle politiche in vari target di scansione di rilevamento, con la percentuale e il numero di incidenti generati per ciascuna politica.
- **Prime 5 radici di contenuti** : Un grafico a barre che mostra le prime cinque radici di contenuti che hanno generato gli incidenti, comprese la gravità degli incidenti generati per ogni radice di contenuti.
- **Riepilogo primi 5 target** : Un grafico a barre che mostra i primi cinque target che hanno generato incidenti dall'ultima scansione di rilevamento completata, inclusa la gravità degli incidenti generati su ogni destinazione.
- **Stato per target** : Un grafico a torta che specifica lo stato dei vari target di scansione di rilevamento, inclusa la percentuale e il numero di incidenti generati per ciascuna politica.

Quadro generale - Endpoint

- **Riepilogo politica** : Un grafico a torta che specifica il numero e la percentuale di incidenti per ogni politica di Endpoint.
- **Primi 5 problemi principali** : Un grafico a barre che mostra i primi cinque endpoint che generano incidenti, inclusa la gravità degli incidenti associati a ciascun endpoint.
- **Riepilogo primi 5 tipi di incidente** : Un grafico a barre che mostra i primi cinque tipi di incidente, ad esempio Appunti o Unità locale.
- **Riepilogo giustificazione utente** : Un grafico a torta che mostra i tipi di giustificazioni per l'utente per gli incidenti endpoint, compresa la percentuale per ciascuna giustificazione.
- **Riepilogo posizione endpoint** : Un grafico a torta che mostra lo stato della connessione per gli endpoint che generano incidenti.
- **Riepilogo stato incidenti** : Un grafico a torta che mostra lo stato di tutti gli incidenti endpoint, con una percentuale per ogni categoria di stato.

Quadro generale - Rete

- **Riepilogo politica** : Un grafico a torta che specifica il numero e la percentuale di incidenti per ogni criterio di rete.
- **Primi 5 mittenti ad alto rischio** : Un grafico a barre che mostra i primi cinque mittenti ad alto rischio, inclusa la gravità degli incidenti associati a ogni mittente.
- **Riepilogo primi 5 protocolli** : Un grafico a barre che mostra i primi cinque protocolli di rete, inclusa la gravità degli incidenti associati a ogni protocollo.

- **Primi 5 domini destinatari** : Un grafico a barre che mostra i primi cinque domini destinatari che generano incidenti, inclusa la gravità degli incidenti associati a ogni dominio.
- **Stato per settimana** : Un grafico a barre che mostra gli incidenti degli ultimi 30 giorni, suddivisi per settimana, con il livello di gravità degli incidenti generati.
- **Riepilogo IP mittente** : Un grafico a torta che mostra gli indirizzi IP del mittente che generano incidenti, con il numero e la percentuale di incidenti per ciascun IP del mittente.

Visualizzazione di dashboard

Questa procedura mostra come visualizzare un dashboard.

Per visualizzare un dashboard

- 1 Nella console di amministrazione di Enforce Server, nel menu **Incidenti**, fare clic su **Report incidente**. Sotto **Report**, fare clic sul nome di un dashboard.

I dashboard sono composti da un massimo di sei portlet, ognuno dei quali fornisce un riepilogo di un determinato report.

- 2 Per consultare l'intero report per un portlet, fare clic sul portlet.

Symantec Data Loss Prevention visualizza l'elenco di incidenti o il report riepilogativo appropriato.

- 3 Esaminare l'elenco di incidenti o il report riepilogativo.

Vedere ["Visualizzazione degli incidenti"](#) a pagina 1645.

Vedere ["Informazioni sui report riepilogativi"](#) a pagina 1643.

Creazione di report di dashboard

È possibile creare dashboard e report personalizzati.

Se non si è connessi come amministratore, Symantec Data Loss Prevention consente di scegliere se condividere il dashboard o mantenerlo privato.

Per creare un dashboard

- 1 Nella console di amministrazione di Enforce Server, nel menu **Incidenti**, fare clic su **Report incidente**.
- 2 Nella schermata **Report incidente** visualizzata, fare clic su **Crea dashboard**.

Viene visualizzata la schermata **Configura dashboard**.

3 Scegliere se condividere il dashboard o mantenerlo privato.

Se si sceglie di condividere un dashboard, questo sarà accessibile a tutti gli utenti con il ruolo con cui è stato creato.

Se si è connessi come amministratore, questa scelta non è visualizzata.

Nota: Symantec Data Loss Prevention designa automaticamente tutti i dashboard che l'amministratore crea come privati.

Fare clic su **Avanti**.

4 Nella sezione **Generale**, nel campo **Nome**, digitare un nome per il dashboard.

5 In **Descrizione**, digitare una descrizione facoltativa per il dashboard.

6 Nella sezione **Pianifica consegna**, è possibile rigenerare e inviare il report del dashboard agli account e-mail specificati.

Se SMTP non è configurato su Enforce Server, la sezione **Pianifica consegna** non sarà disponibile.

Se il sistema è stato configurato per inviare avvisi e report, è possibile impostare un orario per rigenerare e inviare il report del dashboard agli account e-mail specificati.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Se Symantec Data Loss Prevention non è stato configurato per inviare report, andare al passaggio successivo.

Per impostare una pianificazione, individuare la sezione **Pianifica consegna** e selezionare un'opzione dall'elenco a discesa **Pianifica** (in alternativa, selezionare **Nessuna pianificazione**).

Ad esempio, selezionare **Invia settimanalmente ogni**.

Immettere i dati richiesti per la selezione **Pianifica**. Le informazioni richieste comprendono uno o più indirizzi e-mail (separati da virgole). Possono inoltre includere la data, l'ora, il giorno della settimana, il giorno del mese o l'ultima data valida per l'invio.

Vedere ["Opzioni di pianificazione di consegna per i report del dashboard"](#) a pagina 1654.

7 Per la **colonna sinistra**, è possibile scegliere cosa visualizzare in un grafico a torta o un grafico. Per la **colonna destra**, è possibile visualizzare anche una tabella delle informazioni.

Vedere ["Scelta dei report da includere in un dashboard"](#) a pagina 1642.

Selezionare un report fra i tre disponibili negli elenchi a discesa della colonna sinistra (solo grafico). Quindi, selezionare un report fra i tre disponibili negli elenchi a discesa della colonna destra (grafico e tabella).

8 Fare clic su **Salva**.

9 È possibile modificare il dashboard in un secondo momento dalla schermata **Modifica preferenze report**.

Per visualizzare un dashboard personalizzato all'accesso, specificarlo come report di accesso predefinito nella schermata **Modifica preferenze report**.

Vedere "[Modifica dei dashboard e dei report personalizzati](#)" a pagina 1656.

Configurazione report della dashboard

È possibile creare dashboard personalizzate per utenti con ruoli specifici.

Le dashboard sono composte da un massimo di sei portlet, ciascuna delle quali fornisce un rapido riepilogo di un report specificato.

Se si sceglie di condividere una dashboard, questa sarà accessibile a tutti gli utenti assegnati nel ruolo con cui è stata creata.

Nota: L'utente Amministratore non può creare dashboard condivise.

Configurazione di una dashboard personalizzata

- 1 Nella sezione **Generale**, nel **Nome**, digitare un nome per la dashboard.
- 2 In **Descrizione**, digitare una descrizione facoltativa per il dashboard.

- 3 Nella sezione **Pianifica consegna**, è possibile rigenerare e inviare il report del dashboard agli account e-mail specificati.

Se SMTP non è configurato su Enforce Server, la sezione **Pianifica consegna** non sarà disponibile.

Se il sistema è stato configurato per inviare avvisi e report, è possibile impostare un orario per rigenerare e inviare il report del dashboard agli account e-mail specificati.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Se Symantec Data Loss Prevention non è stato configurato per inviare report, andare al passaggio successivo.

Per impostare una pianificazione, individuare la sezione **Pianifica consegna** e selezionare un'opzione dall'elenco a discesa **Pianifica** (in alternativa, selezionare **Nessuna pianificazione**).

Ad esempio, selezionare **Invia settimanalmente ogni**.

Immettere i dati richiesti per la selezione **Pianifica**. Le informazioni richieste comprendono uno o più indirizzi e-mail (separati da virgole). Possono inoltre includere la data, l'ora, il giorno della settimana, il giorno del mese o l'ultima data valida per l'invio.

Vedere ["Opzioni di pianificazione di consegna per i report del dashboard"](#) a pagina 1654.

- 4 Per la **colonna sinistra**, è possibile scegliere cosa visualizzare in un grafico a torta o un grafico. Per la **colonna destra**, è possibile visualizzare anche una tabella delle informazioni.

Vedere ["Scelta dei report da includere in un dashboard"](#) a pagina 1642.

Selezionare un report fra i tre disponibili negli elenchi a discesa della colonna sinistra (solo grafico). Quindi, selezionare un report fra i tre disponibili negli elenchi a discesa della colonna destra (grafico e tabella).

- 5 Fare clic su **Salva**.
- 6 È possibile modificare il dashboard in un secondo momento dalla schermata **Modifica preferenze report**.

Per visualizzare un dashboard personalizzato all'accesso, specificarlo come report di accesso predefinito nella schermata **Modifica preferenze report**.

Vedere ["Modifica dei dashboard e dei report personalizzati"](#) a pagina 1656.

Scelta dei report da includere in un dashboard

I dashboard hanno due colonne di portlet di report.

I portlet nella colonna sinistra mostrano un grafico a torta o un grafico.

I portlet nella colonna destra mostrano le stesse informazioni della colonna sinistra. Visualizzano inoltre un elenco degli incidenti più significativi o un riepilogo. Gli incidenti sono classificati in base alla gravità e al numero di corrispondenze. È possibile visualizzare un elenco di criteri riepilogativi e incidenti associati che evidenziano i totali degli incidenti di gravità alta.

È possibile scegliere fino a tre report da includere nella colonna sinistra e fino a tre report da includere in quella destra.

Per scegliere i report da includere

- 1 Selezionare un report da tre elenchi a discesa della **colonna sinistra (solo grafico)**.
- 2 Selezionare un report dai tre elenchi a discesa della **colonna destra (grafico e tabella)**.
- 3 Dopo la configurazione del dashboard, fare clic su **Salva**.

Vedere ["Configurazione report della dashboard"](#) a pagina 1641.

Informazioni sui report riepilogativi

Symantec Data Loss Prevention fornisce due tipi di report riepilogativi: riepiloghi singoli e doppi.

I riepiloghi singoli mostrano i totali degli incidenti organizzati per un attributo specifico di incidente come lo stato o una politica associata. Ad esempio, un riepilogo della politica include una riga per ogni politica con incidenti associati. Ogni riga include un nome di politica, il numero totale di incidenti associati e i totali degli incidenti per gravità.

I riepiloghi doppi di incidente mostrano il numero totale di incidenti per due attributi di incidente. Ad esempio, un riassunto di tendenza della politica mostra gli incidenti totali organizzati con politica e settimana. Come in un riepilogo della politica, ogni voce include un nome di politica, il numero totale di incidenti associati e i totali degli incidenti per gravità. Inoltre, ogni voce include una riga separata per ogni settimana, mostrando i totali degli incidenti della settimana e gli incidenti per gravità.

Vedere ["Opzioni di riepilogo per i report di incidente"](#) a pagina 1682.

Da qualsiasi elenco di incidenti è possibile creare report riepilogativi personalizzati.

Visualizzazione di report riepilogativi

Questa procedura mostra come visualizzare un report riepilogativo.

Per visualizzare un report riepilogativo

- 1 Nella console di amministrazione di Enforce Server, nel menu **Incidenti**, selezionare uno dei tipi di report.

Ad esempio, selezionare **Rete**, quindi fare clic su **Riepilogo politica**.

Il report consiste di voci riepilogative (righe) che sono divise in varie colonne. La prima colonna è denominata per il criterio riepilogativo primario. Elenca gli elementi di riepilogo primari e (per riepiloghi doppi) secondari. Ad esempio, in un **Riepilogo politica** questa colonna è denominata **Politica** ed elenca le politiche. Ogni voce include una colonna per il numero totale di incidenti associati. Include inoltre le colonne che mostrano il numero di incidenti di gravità Alta, Media, Bassa e Informazioni. Include infine un grafico a barre che rappresenta il numero degli incidenti per gravità.

- 2 È possibile eventualmente ordinare il report in modo alfanumerico per i dati di una particolare colonna. A questo proposito, fare clic sull'intestazione della colonna desiderata. Per ordinare nell'ordine inverso, fare di nuovo clic sull'intestazione della colonna una seconda volta.
- 3 Per identificare le aree di rischio potenziale, fare clic sull'intestazione della colonna Alta per visualizzare le voci di riepilogo per numero di incidenti di gravità Alta.
- 4 Fare clic su una voce per visualizzare un elenco degli incidenti associati. In una qualsiasi delle colonne della gravità, è possibile fare clic sul totale per visualizzare un elenco degli incidenti con la gravità scelta.

Vedere ["Visualizzazione degli incidenti"](#) a pagina 1645.

Creazione di report riepilogativi

Questa procedura mostra come creare un report riepilogativo.

Per creare un report riepilogativo da un elenco di incidenti

- 1 Nella console di amministrazione di Enforce Server, nel menu **Incidenti**, selezionare uno dei tipi di report, quindi fare clic sull'elenco di incidenti.

Ad esempio, selezionare **Discover** e quindi il report **Incidenti - Tutte le scansioni**.

- 2 Fare clic sulla barra **Filtri avanzati e riepilogo** (vicino alla parte superiore del report).

Nel campo **Riepiloga per** delle caselle di riepilogo principale e secondaria, Symantec Data Loss Prevention visualizza tutti i criteri forniti da Symantec in ordine alfabetico. I criteri precedono tutti i criteri personalizzati che l'amministratore ha definito.

Vedere ["Opzioni di riepilogo per i report di incidente"](#) a pagina 1682.

- 3 Selezionare un criterio dalla casella di riepilogo principale e uno da quella secondaria. Ad esempio, selezionare **Gruppo di politiche** e quindi **Politica**. Da notare che le opzioni nella casella di riepilogo secondaria vengono visualizzate solo dopo che si è selezionata un'opzione nella casella di riepilogo principale.
- 4 Per creare il report riepilogativo, fare clic su **Applica**.
I report riepilogativi prendono il nome dal criterio di riepilogo principale. Se si ripete l'esecuzione di un report con nuovi criteri, il nome del report cambia di conseguenza.
- 5 Salvare il report.
Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Visualizzazione degli incidenti

Gli elenchi degli incidenti Symantec Data Loss Prevention visualizzano i singoli record di incidente con informazioni sugli incidenti. È possibile fare clic su un incidente per visualizzare un'istantanea contenente più dettagli. È possibile selezionare specifici incidenti o gruppi di incidenti da modificare o riparare.

Symantec Data Loss Prevention fornisce elenchi di incidenti per incidenti di rete, endpoint e di rilevazione.

Per visualizzare incidenti

- 1 Nella console di amministrazione Enforce Server, nel menu **Incidenti**, selezionare uno dei tipi di report.
Ad esempio, selezionare **Discover**. Nel riquadro di navigazione a sinistra, fare clic su **Incidenti - Tutte le scansioni**.
L'elenco di incidenti visualizza i singoli record di incidente che contengono informazioni quali gravità, politica collegata, il numero di corrispondenze e stato.
- 2 È anche possibile utilizzare filtri di report per restringere l'elenco di incidenti.
Vedere ["Report di filtraggio"](#) a pagina 1648.
- 3 Per visualizzare ulteriori dettagli su uno specifico incidente, fare clic sull'incidente.
Viene visualizzata l'istantanea incidente, che mostra informazioni generali sull'incidente, le corrispondenze rilevate nel testo intercettato e dettagli su politica, attributi e cronologia degli incidenti.
È anche possibile cercare incidenti simili tramite la scheda **Correlazioni**.
- 4 È anche possibile fare clic nell'istantanea incidente per visualizzare ulteriori informazioni sull'incidente.
Il seguente elenco descrive le modalità in cui è possibile accedere a ulteriori informazioni tramite l'istantanea:

- È possibile trovare informazioni sulla politica che ha rilevato l'incidente. Nella scheda **Informazioni chiave**, la sezione **Corrispondenze politica** visualizza il nome della politica. Fare clic sul nome di una politica per visualizzare un elenco di incidenti associati a tale politica. Fare clic su **visualizza politica** per visualizzare una versione di sola lettura della politica.

Questa sezione elenca inoltre altre politiche violate con lo stesso file o messaggio. Quando sono elencate più politiche, è possibile visualizzare l'istantanea di un incidente associato a una determinata politica. Fare clic su **vai a incidente** accanto al nome della politica. Per visualizzare un elenco di tutti gli incidenti creati dal file o dal messaggio, fare clic su **Mostra tutto**.

- È possibile visualizzare gli elenchi degli incidenti che condividono diversi attributi con l'incidente corrente. La scheda **Correlazioni** mostra un elenco di correlazioni che determinano la corrispondenza con i singoli attributi. Fare clic sui valori di attributo per visualizzare elenchi di incidenti correlati a tali valori.

Ad esempio, l'incidente della rete corrente è attivato da un messaggio proveniente da uno specifico account e-mail. È possibile visualizzare un elenco di tutti gli incidenti che ha creato questo account.

- Per la maggior parte degli incidenti di rete, è possibile accedere a tutti gli allegati associati al messaggio di rete. A tal fine, individuare il campo **Allegati** nella sezione **Dettagli incidente** dell'istantanea e fare clic sul nome file dell'allegato.

Per una descrizione dettagliata delle istantanee di incidente e delle azioni che è possibile eseguire tramite esse, consultare la guida in linea.

- 5 Al termine della consultazione degli incidenti, è possibile uscire dall'istantanea incidente o dall'elenco degli incidenti o scegliere uno o più incidenti da riparare.

Vedere ["Risoluzione di incidenti"](#) a pagina 1573.

Informazioni su report e dashboard personalizzati

È possibile filtrare e riepilogare i report e poi salvarli per uso continuativo. Quando si salva un report personalizzato, è possibile configurare Symantec Data Loss Prevention in modo che invii il report in base a una pianificazione specifica.

Symantec Data Loss Prevention mostra i titoli dei report personalizzati in **Incidenti > Tutti i report**.

La schermata **Tutti i report** mostra tutti i report creati al momento e personalizzati disponibili per il ruolo assegnato. L'elenco include report e dashboard personalizzati condivisi creati dall'utente o da chiunque altro nel ruolo creato corrente. Diversi report standard sono disponibili con Symantec Data Loss Prevention.

Symantec Data Loss Prevention mostra nome, prodotto associato e descrizione di ciascun report. Per i report personalizzati, Symantec Data Loss Prevention indica se il report è condiviso o privato e mostra la generazione del report e la pianificazione della consegna.

È possibile modificare i report esistenti e salvarli come report personalizzati, oltre a creare dashboard personalizzate. I report e le dashboard personalizzati vengono elencati nella sezione **Report salvati** del pannello di navigazione.

È possibile fare clic su qualsiasi report nell'elenco per eseguirlo nuovamente con i dati correnti.

È possibile visualizzare ed eseguire report personalizzati per i report creati da utenti con un ruolo qualsiasi assegnato all'utente. È possibile modificare o eliminare solo i report personalizzati associati al ruolo corrente. Gli unici report personalizzati visibili all'Amministratore sono i report creati dall'utente Amministratore.

Una serie di tabelle elenca tutte le opzioni disponibili per il report di filtraggio e riepilogo.

Vedere ["Informazioni sui report riepilogativi"](#) a pagina 1643.

Vedere ["Opzioni di riepilogo per i report di incidente"](#) a pagina 1682.

Vedere ["Filtri generali per i report"](#) a pagina 1679.

Vedere ["Opzioni di filtro avanzate per i report"](#) a pagina 1687.

Crea dashboard Consente di creare una dashboard personalizzata che mostra i dati di riepilogo provenienti da diversi report specificati dall'utente. Per gli utenti con un ruolo diverso dall'Amministratore, questa opzione porta alla schermata **Configura dashboard**, in cui è possibile specificare se la dashboard è privata o condivisa. Tutte le dashboard Amministratore sono private.

Vedere ["Creazione di report di dashboard"](#) a pagina 1639.

I report (personalizzati) associati al ruolo dell'utente vengono visualizzati vicino alla parte superiore dello schermo.

Le seguenti opzioni sono disponibili per i report personalizzati del ruolo corrente:



Fare clic sull'icona accanto a un report per visualizzare il report di salvataggio o configurare la schermata della dashboard. È possibile modificare il nome, la descrizione o la pianificazione, oppure (solo per le dashboard) modificare i report da includere.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Vedere ["Configurazione report della dashboard"](#) a pagina 1641.



Fare clic su questa icona accanto a un report per visualizzare la schermata e modificare la pianificazione di tale report. Se questa icona non viene visualizzata, il report non è attualmente pianificato.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.



Fare clic su questa icona accanto a un report per eliminare quel report. Una finestra di dialogo richiede di confermare l'eliminazione. Quando si elimina un report, non è possibile recuperarlo. Prima di eliminare il report, assicurarsi che non sia necessario per altri membri del ruolo.

Utilizzo di IT Analytics per la gestione di incidenti

IT Analytics Solution è un'applicazione di Business Intelligence (BI) che complementa e potenzia il reporting fornito da Symantec Data Loss Prevention. Offre analisi multidimensionale e robuste funzionalità di reporting grafico a Symantec Management Platform. Questa funzionalità consente di creare istantaneamente report ad hoc anche senza avere una conoscenza avanzata dei database o di strumenti di reporting di terzi. IT Analytics completa questa potente funzionalità di reporting ad hoc istantaneo con tabelle pivot, aggregazioni precompilate per una risposta rapida a query tipicamente molto lunghe e facili e modalità di esportazione in file di formato .PDF, Excel, .CSV e .TIF.

Per ulteriori informazioni, vedere la pagina di destinazione di IT Analytics nel Centro di supporto Symantec all'indirizzo https://support.symantec.com/en_US/dpl.56005.html.

Report di filtraggio

È possibile filtrare un elenco di incidenti o un report di riepilogo.

Per filtrare un elenco di incidenti

- 1 Nella console di amministrazione Enforce Server, nel menu **Incidenti**, selezionare uno dei tipi di report.
Ad esempio, selezionare **Rete**, quindi fare clic su **Riepilogo politica**.
- 2 Nell'area **Filtro**, vengono visualizzati i filtri correnti, nonché le opzioni per l'aggiunta e l'esecuzione di altri filtri.
- 3 Modificare i filtri predefiniti come desiderato. Ad esempio, dagli elenchi a discesa del filtro **Stato**, selezionare **È uguale a** e **Nuovo**.

Per i report **Rete** ed **Endpoint**, i filtri predefiniti sono **Data** e **Stato**. Per i report Discover, i filtri predefiniti sono **Stato**, **Esegui scansione** e **ID target**.

- 4 Per aggiungere un nuovo filtro, selezionare le opzioni di filtro dagli elenchi a discesa. Fare clic su **Filtri avanzati e riepilogo** per ulteriori opzioni. Fare clic su **Aggiungi filtro** a destra, per ulteriori opzioni di filtro.

Selezionare i parametri e il tipo di filtro da sinistra a destra come durante la scrittura di una frase. Ad esempio, nei filtri avanzati, opzioni **Aggiungi filtro**, selezionare **Politica** e **È uno qualsiasi dei seguenti valori**, quindi selezionare una o più politiche da visualizzare nel report. Tenere premuto Ctrl o Maiusc per selezionare più di un elemento nella casella di riepilogo.

- 5 Fare clic su **Applica** per aggiornare il report.
- 6 Salvare il report.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Salvataggio dei report di incidente personalizzati

Dopo aver riassunto o filtrato un report, è possibile salvarlo per un uso continuato. Quando si salva un report personalizzato, Symantec Data Loss Prevention visualizza il titolo del report in **Report salvati** nella sezione **Tutti i report**. Se l'utente sceglie di condividere il report, Symantec Data Loss Prevention visualizza il collegamento al report solo per gli utenti che appartengono allo stesso ruolo dell'utente che ha creato il report.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

È possibile modificare il report in seguito nella schermata **Modifica preferenze**.

Vedere ["Modifica dei dashboard e dei report personalizzati"](#) a pagina 1656.

Facoltativamente è possibile pianificare il report per l'esecuzione automatica regolare.

Vedere ["Pianificazione dei report di incidente personalizzati"](#) a pagina 1650.

Per salvare un report personalizzato

- 1 Impostare un filtro personalizzato o un report di riepilogo.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Fare clic su **Salva > Salva con nome**.

- 2 Immettere un nome di report univoco e descrivere il report. Il nome del report può includere fino a 50 caratteri.

- 3 Nella sezione **Condivisione**, tutti gli utenti all'infuori dell'amministratore possono condividere un report personalizzato.

Nota: Questa sezione non viene visualizzata per l'amministratore.

La sezione **Condivisione** consente di specificare se mantenere il report privato o di condividerlo con altri membri del ruolo. I membri del ruolo sono altri utenti assegnati allo stesso ruolo. Per condividere il report, selezionare **Condividi report**. Tutti i membri del ruolo ora hanno accesso a questo report e tutti possono modificare o eliminare il report. Se l'account viene eliminato dal sistema, i report condivisi rimangono nel sistema. I report condivisi vengono associati al ruolo, non a un account utente specifico. Se un report non viene condiviso l'utente che l'ha creato è il solo che può accedervi. Se l'account viene eliminato dal sistema, anche i report privati vengono eliminati. Se si accede con un altro ruolo, il report è visibile nella schermata **Tutti i report**, ma non accessibile.

- 4 Fare clic su **Salva**.

Pianificazione dei report di incidente personalizzati

Facoltativamente è possibile pianificare un report salvato per l'esecuzione automatica regolare.

È inoltre possibile pianificare il report in modo che venga inviato regolarmente via e-mail a indirizzi specificati o ai proprietari di dati.

Consultare la *Guida all'implementazione di Symantec Data Loss Prevention Data Insight*.

Per pianificare un report personalizzato

1 Fare clic su **Invia > Pianifica distribuzione**.

Se SMTP non è configurato su Enforce Server, non è possibile selezionare la voce di menu **Invia** per inviare il report.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

2 Specificare i **dettagli di consegna** :

A: Selezionare se il report viene inviato a indirizzi e-mail specificati o ai proprietari di dati.

Manuale - Invia a indirizzi e-mail specificati Immettere manualmente gli indirizzi e-mail specifici nella casella di testo.

Auto - Invia a proprietari dati incidenti Per inviare il report ai proprietari di dati, l'impostazione **Invia dati di report tramite e-mail** deve essere attivata affinché questa opzione venga visualizzata.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Se si configura l'invio del report ai proprietari di dati di incidenti, l'indirizzo e-mail nell'attributo dell'incidente **Indirizzo e-mail proprietario dati** è l'indirizzo a cui viene inviato il report.

L'opzione **Indirizzo e-mail proprietario dati** deve essere impostato manualmente o con un plug-in di ricerca.

Consultare la *Guida all'implementazione di Symantec Data Loss Prevention Data Insight*.

È possibile distribuire un massimo di 10.000 incidenti per proprietario di dati.

CC: Immettere manualmente gli indirizzi e-mail nella casella di testo.

Oggetto: Utilizzare l'oggetto predefinito o modificarlo.

Corpo: Immettere il corpo dell'e-mail.

È inoltre possibile inserire le variabili dell'azione di risposta nel corpo.

Vedere ["Variabili azione di risposta"](#) a pagina 1576.

- 3 Nella sezione **Pianifica consegna** specificare la pianificazione di consegna.
Vedere ["Opzioni di pianificazione di consegna per i report di incidente e di sistema"](#) a pagina 1652.
- 4 Nella sezione **Modifica stato/attributi incidente** è possibile implementare il flusso di lavoro.
L'opzione **Auto - Invia a proprietari dati incidenti** deve essere selezionata affinché questa sezione sia disponibile.
Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.
- 5 Dopo l'invio del report è possibile modificare lo stato di un incidente e impostare uno dei valori validi. Selezionare un valore di stato dall'elenco a discesa.
- 6 È inoltre possibile immettere nuovi valori per gli attributi personalizzati.
Questi attributi devono essere già configurati.
Vedere ["Informazioni sugli attributi di stato incidente."](#) a pagina 1700.
- 7 Selezionare uno degli attributi personalizzati dall'elenco a discesa.
- 8 Fare clic su **Aggiungi**.
- 9 Nella casella di testo immettere il nuovo valore per questo attributo personalizzato.
Dopo l'invio del report, gli attributi personalizzati selezionati impostano i nuovi valori per quegli incidenti inviati nel report.
- 10 Fare clic su **Avanti**.
- 11 Immettere il nome e la descrizione del report salvato.
- 12 Fare clic su **Salva**.

Opzioni di pianificazione di consegna per i report di incidente e di sistema

La sezione **Pianifica consegna** consente di configurare una pianificazione per il report.

Nota: Se Enforce Server non è configurato per inviare e-mail o se non si ha l'autorizzazione di inviare report, la sezione **Pianifica consegna** non viene visualizzata.

Quando si esegue una selezione dall'elenco, sono visualizzati campi supplementari.

Per rimuovere la pianificazione precedente di un report, fare clic sull'opzione **Rimuovi**.

La tabella seguente descrive i campi supplementari disponibili per ogni opzione nell'elenco.

Dettagli consegna Specificare i seguenti dettagli relativi alla consegna:

- **Invia a**
Selezionare **Manuale** per specificare gli indirizzi e-mail.
Selezionare **Automatico** per l'invio automatico ai proprietari dei dati.
- **A**
Immettere uno o più indirizzi e-mail. Separarli con virgole.
- **CC**
Immettere uno o più indirizzi e-mail. Separarli con virgole.
- **Oggetto**
Immettere un oggetto per l'e-mail.
- **Corpo**
Immettere il corpo dell'e-mail. Utilizzare le variabili per elementi quali il nome della politica.
Vedere "[Variabili azione di risposta](#)" a pagina 1576.

Una volta Selezionare **Una volta** per pianificare il report da eseguire una volta in futuro e quindi specificare i seguenti dettagli per quel report:

- **Orario**
Selezionare la data e l'ora alla quale si desidera generare il report.
- **Data di invio**
Immettere la data in cui si desidera generare il report, o fare clic sul widget data e selezionare una data.

Ogni giorno Selezionare **Ogni giorno** per pianificare l'esecuzione giornaliera del report e quindi specificare i seguenti dettagli per quel report:

- **Orario**
Selezionare la data e l'ora alla quale si desidera generare il report.
- **Fino a**
Immettere la data alla quale si intende arrestare la generazione di report quotidiani, fare clic sul widget data e selezionare una data o **Tempo indeterminato**.

Ogni settimana Selezionare **Ogni settimana** per pianificare l'esecuzione settimanale del report e quindi specificare i seguenti dettagli per quel report:

- **Orario**
Selezionare la data e l'ora alla quale si desidera generare il report.
- **Giorno della settimana**
Fare clic per selezionare una o più caselle di controllo corrispondenti ai giorni della settimana in cui si desidera generare il report.
- **Fino a**
Immettere la data alla quale si intende arrestare la generazione di report settimanali, fare clic sul widget data e selezionare una data o **Tempo indeterminato**.

- Ogni mese** Selezionare **Ogni mese** per pianificare l'esecuzione mensile del report e quindi specificare i seguenti dettagli per quel report:
- **Orario**
Selezionare la data e l'ora alla quale si desidera generare il report.
 - **Giorno del mese**
Immettere la data alla quale si desidera generare il report ogni mese.
 - **Fino a**
Immettere la data alla quale si intende arrestare la generazione di report mensili, fare clic sul widget data e selezionare una data o **Tempo indeterminato**.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Vedere [" Utilizzo dei report di sistema salvati"](#) a pagina 175.

Opzioni di pianificazione di consegna per i report del dashboard

La sezione **Pianifica consegna** consente di configurare una pianificazione per il report.

Nota: Se Enforce Server non è configurato per inviare e-mail o se non si ha l'autorizzazione di inviare report, la sezione **Pianifica consegna** non viene visualizzata.

Quando si esegue una selezione dall'elenco a discesa **Pianifica**, sono visualizzati campi supplementari.

La tabella seguente descrive i campi supplementari disponibili per ogni opzione nell'elenco.

- Nessuna pianificazione** Selezionare **Nessuna pianificazione** per salvare il report senza una pianificazione.
- Una volta** Selezionare **Una volta** per programmare il report essere fatto funzionare una volta a un tempo futuro e poi specificare i seguenti dettagli per quel report:
- **Il**
Immettere la data in cui si desidera generare il report, o fare clic sul widget data e selezionare una data.
 - **Alle**
Selezionare la data e l'ora alla quale si desidera generare il report.
 - **Invia a**
Immettere uno o più indirizzi e-mail. Separarli con virgole.

- Invia ogni giorno** Selezionare **Invia ogni giorno** per pianificare l'esecuzione giornaliera del report e quindi specificare i seguenti dettagli per quel report:
- Alle
- Selezionare la data e l'ora alla quale si desidera generare il report.
- Fino a
- Immettere la data alla quale si intende arrestare la generazione di report quotidiani, fare clic sul widget data e selezionare una data o **Tempo indeterminato**.
- Invia a
- Immettere uno o più indirizzi e-mail. Separarli con virgole.
- Invia settimanalmente ogni** Selezionare **Invia settimanalmente ogni** per pianificare l'esecuzione settimanale del report e quindi specificare i seguenti dettagli per quel report:
- Giorno
- Fare clic per selezionare una o più caselle di controllo corrispondenti ai giorni della settimana in cui si desidera generare il report.
- Alle
- Selezionare la data e l'ora alla quale si desidera generare il report.
- Fino a
- Immettere la data alla quale si intende arrestare la generazione di report settimanali, fare clic sul widget data e selezionare una data o **Tempo indeterminato**.
- Invia a
- Immettere uno o più indirizzi e-mail. Separarli con virgole.
- Invia mensilmente il** Selezionare **Inviare mensilmente** per programmare l'esecuzione del report ogni mese e poi specificare i seguenti dettagli per quel report:
- Giorno di ogni mese
- Immettere la data alla quale si desidera generare il report ogni mese.
- Alle
- Selezionare la data e l'ora alla quale si desidera generare il report.
- Fino a
- Immettere la data alla quale si intende arrestare la generazione di report mensili, fare clic sul widget data e selezionare una data o **Tempo indeterminato**.
- Invia a
- Immettere uno o più indirizzi e-mail. Separarli con virgole.

Vedere ["Configurazione report della dashboard"](#) a pagina 1641.

Utilizzo del widget della data per pianificare i report

Il widget della data specifica le date dei report.

Il widget della data inserisce automaticamente la data. È possibile fare clic su **Oggi** per inserire la data corrente.

Per utilizzare il widget della data

- 1 Fare clic sul widget della data.
- 2 Fare clic sulla freccia sinistra o destra ai lati del mese per cambiare il mese.
- 3 Fare clic sulla freccia sinistra o destra ai lati dell'anno per cambiare l'anno.
- 4 Fare clic sulla data desiderata del calendario.

Modifica dei dashboard e dei report personalizzati

È possibile modificare i dashboard o i report personalizzati creati.

Per modificare un dashboard o un report personalizzato

- 1 Nel menu **Incidenti** della console di amministrazione di Enforce Server selezionare **Report incidente**.

Viene visualizzato il dashboard **Report incidente** con **Report salvati** vicino alla parte superiore.

- 2 Fare clic sull'icona di modifica accanto al report o al dashboard da modificare.

Viene visualizzata la schermata **Salva report** o **Salva dashboard**. È possibile modificare il nome, la descrizione e la pianificazione di qualsiasi report o dashboard personalizzato, nonché selezionare diversi report di componente per un dashboard personalizzato.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

- 3 Al termine della modifica fare clic su **Salva**.

Esportazione dei report di incidente

Un report può essere esportato in un file di testo separato da virgole (.csv) o in un file XML.

È possibile configurare un delimitatore CSV diverso dalla virgola. È possibile specificare quali campi sono esportati in XML. Queste opzioni devono essere impostate nel profilo per poter esportare un report.

Vedere ["Modifica di un profilo utente"](#) a pagina 85.

Per esportare un report

- 1 Fare clic su **Incidenti** e selezionare un tipo di report.
- 2 Andare sul report che si desidera esportare. Filtrare o riepilogare gli incidenti nel report come desiderato.
Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.
- 3 Selezionare le caselle di controllo a sinistra degli incidenti per selezionare gli incidenti da esportare.
- 4 Nell'elenco a discesa **Esporta**, selezionare **Esporta tutto: CSV** o **Esporta tutto: XML**.

Nota: Vedere la versione corrente del *Manuale per sviluppatori dell'API di reporting e aggiornamento incidenti* per la posizione dei file di schema XML per i report esportati e per una descrizione dei singoli elementi XML.

- 5 Fare clic su **Apri** o **Salva**. Se è stato selezionato **Salva**, si apre una finestra di dialogo **Salva con nome** ed è possibile specificare la posizione e il nome del file.

Vedere ["Campi esportati per Network Monitor"](#) a pagina 1657.

Vedere ["Campi esportati per Endpoint Discover"](#) a pagina 1659.

Vedere ["Campi esportati per Network Discover/Cloud Storage Discover"](#) a pagina 1658.

Vedere ["Stampa di report di incidenti"](#) a pagina 1673.

Vedere ["Invio dei report degli incidenti tramite e-mail"](#) a pagina 1672.

Campi esportati per Network Monitor

I seguenti campi vengono esportati per Network Monitor:

Tipo	Tipo di incidente (ad esempio SMTP , HTTP o FTP).
Stato messaggio	Lo stato di questo messaggio di incidente.
Gravità	Gravità di questo incidente (Alta , Media o Bassa).
Inviato	La data e l'ora in cui il messaggio è stato inviato.
ID	Identificatore unico dell'incidente.
Politica	Nome della politica che ha generato l'incidente.
Corrispondenze	Il numero di volte in cui questo elemento corrisponde ai parametri di rilevamento di una regola della politica.

Argomento	Oggetto del messaggio.
Destinatari	Destinatari del messaggio.
Stato	Stato dell'incidente (Nuovo , È riassegnato , Ignorato o Chiuso).
Con allegato	Indica se questo messaggio ha un allegato.
Nome proprietario dati	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.
E-mail proprietario dati	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca.

Anche gli attributi personalizzati sono esportati.

Campi esportati per Network Discover/Cloud Storage Discover

I seguenti campi sono esportati per Network Discover/Cloud Storage Discover:

Tipo	Tipo di target (ad esempio file system, Lotus Notes o database SQL).
Stato messaggio	Lo stato di questo messaggio di incidente.
Gravità	La gravità dell'incidente (Alta , Media o Bassa).
Data rilevamento	La data in cui un incidente è stato rilevato.
Rilevato in precedenza	Questo incidente è stato rilevato in precedenza? Il valore è Sì o No .
Oggetto	Oggetto dell'e-mail per le scansioni integrate di Exchange.
Mittente	Mittente dell'e-mail per le scansioni integrate di Exchange.
Destinatario	Destinatario dell'e-mail per le scansioni integrate di Exchange.
ID	Identificatore unico dell'incidente.
Politica	Nome della politica che ha generato l'incidente.

Corrispondenze	Numero di volte che questo elemento corrisponde ai parametri di rilevamento di una regola della politica.
Posizione	Posizione (percorso) dell'elemento.
Stato	Stato dell'incidente (Nuovo , Riassegnato , Ignorato o Chiuso).
Target	Nome del target della scansione.
Scansione	Data e ora in cui il file è stato sottoposto a scansione.
Proprietario file	Proprietario del file.
Data ultima modifica	Data e ora dell'ultima modifica dell'elemento.
Data creazione file	Data e ora di creazione dell'elemento.
Data ultimo accesso	Data e ora dell'ultima modifica dell'elemento (non visualizzate per i target NFS).
Nome proprietario dati	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.
E-mail proprietario dati	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca.

Anche gli attributi personalizzati sono esportati.

Campi esportati per Endpoint Discover

I seguenti campi vengono esportati per Endpoint Discover:

Tipo	Tipo di target (ad esempio Archivi rimovibili).
Gravità	La gravità dell'incidente (Alta , Media o Bassa).
Avvenuto il	La data in cui un incidente è stato rilevato.
ID	L'identificatore univoco dell'incidente.
Politica	Il nome della politica che ha generato l'incidente.

Corrispondenze	Il numero di volte che questo elemento corrisponde ai parametri di rilevamento di una regola della politica.
Stato	Stato dell'incidente (Nuovo , È riassegnato , Ignorato o Chiuso).
Nome file	Il nome del file che ha violato la politica.
Percorso file	Il percorso del file. Nota: La posizione del file è visualizzata solo per gli incidenti relativi alle unità fisse.
Computer	Il computer nel quale si è verificato l'incidente.
Utente	Il nome dell'utente endpoint.
Stato prevenzione	Lo stato dell'endpoint (ad esempio Azione bloccata).
Oggetto	Oggetto del messaggio.
Destinatari	Il destinatario del messaggio.
Con allegato	Indica se questo messaggio ha un allegato.
Nome proprietario dati	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.
E-mail proprietario dati	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente oppure con uno dei plug-in di ricerca.

Anche gli attributi personalizzati sono esportati.

Eliminazione di incidenti

Le prestazioni di reporting di incidenti spesso peggiorano quando gli incidenti presenti nel sistema sono più di un milione (1.000.000). Symantec consiglia di mantenere il numero di incidenti al di sotto di tale soglia cancellando gli incidenti per non peggiorare le prestazioni del sistema.

L'eliminazione di un incidente è permanente: non è possibile recuperare gli incidenti che sono stati cancellati. Symantec Data Loss Prevention offre opzioni per l'eliminazione di soltanto determinate parti dei dati che hanno generato l'incidente.

Dopo aver contrassegnato gli incidenti per l'eliminazione, è possibile visualizzare, configurare, eseguire e risolvere i problemi del processo di eliminazione incidenti dalla console di

amministrazione di Enforce Server. È possibile contrassegnare gli incidenti da eliminare manualmente o automaticamente.

Vedere ["Informazioni su come contrassegnare automaticamente gli incidenti da eliminare"](#) a pagina 1665.

È anche possibile eliminare gli incidenti nascosti.

Vedere ["Eliminazione degli incidenti nascosti"](#) a pagina 1699.

Per eliminare un incidente

- 1 Nella schermata **Report incidente**, selezionare l'incidente o gli incidenti che si desidera eliminare, quindi fare clic su **Azioni incidente > Elimina incidenti**.
- 2 Nella schermata **Elimina incidenti**, selezionare una delle seguenti opzioni di eliminazione:

Elimina incidente completamente	Elimina in modo permanente gli incidenti e tutti i dati associati (ad esempio, eventuali e-mail e allegati). Si tenga presente che non è possibile recuperare gli incidenti che sono stati eliminati.
Mantieni incidente ma elimina dati messaggio	Mantiene gli incidenti effettivi, ma elimina la copia di Symantec Data Loss Prevention dei dati che hanno generato gli incidenti. È possibile eliminare solo determinate parti dei dati associati. Il resto dei dati viene conservato.
Elimina messaggio originale	Elimina il contenuto del messaggio (ad esempio, il messaggio e-mail o il post HTML). Questa opzione si applica solo agli incidenti di rete.
Elimina allegati/file	<p>Questa opzione fa riferimento ai file (per gli incidenti endpoint e di rilevazione) o agli allegati di e-mail o di post (per gli incidenti di rete). Le opzioni sono:</p> <ul style="list-style-type: none">■ Tutto, che elimina tutti gli allegati. Scegliere questa opzione per eliminare tutti i file (per gli incidenti endpoint e di rilevazione) o gli allegati di e-mail (per gli incidenti di rete). Gli allegati e i file sono aggiunti alla coda degli incidenti da eliminare dopo l'eliminazione degli incidenti associati.■ Allegati/file senza violazioni. Questa opzione elimina solo gli allegati in cui Symantec Data Loss Prevention non ha trovato alcuna corrispondenza. Scegliere questa opzione quando vi sono incidenti con singoli file estratti da un file compresso (incidenti endpoint e di rilevazione) o diversi allegati di e-mail (incidenti di rete).

- 3 Fare clic su **Annulla** o **Elimina**.

Elimina contrassegna l'incidente per l'eliminazione e lo aggiunge alla coda degli incidenti da eliminare. Non è possibile recuperare un incidente dopo che è stato contrassegnato per l'eliminazione. Symantec Data Loss Prevention elimina in modo permanente gli incidenti nella coda degli incidenti da cancellare quando esegue il processo di eliminazione.

Informazioni sul processo di eliminazione incidente

È possibile visualizzare, configurare, eseguire e risolvere i problemi del processo di eliminazione incidente nella schermata **Eliminazione incidente** della console di amministrazione di Enforce Server: **Sistema > Dati incidente > Eliminazione incidente**. La schermata mostra il numero di incidenti nella coda di eliminazione incidente, la pianificazione dell'eliminazione e una cronologia dei processi di eliminazione.

La coda di eliminazione incidente include tutti gli incidenti contrassegnati per l'eliminazione da tutti gli utenti di Symantec Data Loss Prevention. Oltre a visualizzare il numero degli incidenti contrassegnati per l'eliminazione, è possibile avviare e interrompere manualmente un processo di eliminazione dalla coda di eliminazione incidente.

È possibile visualizzare informazioni dettagliate sui processi di eliminazione nella sezione della cronologia processi di eliminazione. Sono disponibili il numero di incidenti e gli allegati o i file eliminati, l'ora di inizio e fine del processo, la durata del processo, un'indicazione del fatto che il processo sia stato o meno interrotto manualmente e lo stato del processo (**Completato**, **Non riuscito** o **In corso**). Nel caso di processi di eliminazione non riusciti, è possibile fare clic sul collegamento **Non riuscito** per visualizzare il messaggio di errore e la descrizione del problema. Queste informazioni possono essere utili all'amministratore del database Oracle nella risoluzione del problema associato all'interruzione del processo. Se le informazioni sono insufficienti a risolvere i problemi dei processi di eliminazione, è possibile esportare le informazioni da qualsiasi processo in un file CSV e inviarlo al Supporto Symantec Data Loss Prevention per ottenere ulteriore assistenza.

Per impostazione predefinita il processo di eliminazione incidenti viene eseguito ogni giorno alle 23.59 nella fascia oraria locale di Enforce Server. Quando viene eseguito, il processo crea anche un evento nella schermata **Sistema > Server e rilevatori > Eventi**. Questo evento viene creato indipendentemente dal fatto che uno o più incidenti vengano o meno eliminati.

Configurazione della pianificazione del processo di eliminazione incidenti

La pianificazione predefinita del processo di eliminazione incidenti è ogni giorno alle 23.59 nella fascia oraria locale di Enforce Server. È possibile configurare la pianificazione del processo di eliminazione in qualsiasi altro orario. Symantec suggerisce di eseguire l'eliminazione incidenti in un momento in cui il sistema è poco attivo.

Per configurare la pianificazione del processo di eliminazione incidenti

- 1 Fare clic sull'icona del calendario **Pianifica processo di eliminazione**.
- 2 Nella finestra di dialogo **Pianifica eliminazione incidente**, specificare una delle seguenti opzioni:
 - **Nessuna pianificazione regolare** : selezionare questa opzione per disattivare la pianificazione del processo di eliminazione.

- **Una volta** : specificare un giorno e un'ora per un singolo processo di eliminazione incidenti.
- **Ogni giorno** : specificare un orario per i processi di eliminazione incidenti quotidiani.
- **Ogni settimana** : specificare un giorno e un'ora per i processi di eliminazione incidenti.
- **Ogni mese** : specificare un giorno del mese e un orario per i processi di eliminazione incidenti. Per tenere conto delle differenze tra i mesi, il valore del giorno del mese deve essere compreso tra 1 e 28.

3 Fare clic su **Invia**.

Nota: La pianificazione del processo di eliminazione incidenti viene reimpostata sul valore predefinito durante il processo di aggiornamento. Se si sta utilizzando una pianificazione del processo di eliminazione incidenti personalizzata, riconfigurare la pianificazione una volta completato il processo di aggiornamento.

Avvio e arresto di processi di eliminazione incidenti

Se sono presenti incidenti in attesa di eliminazione, è possibile avviare manualmente un processo di eliminazione incidenti dalla coda di eliminazione incidenti. È inoltre possibile interrompere qualsiasi processo di eliminazione incidenti attualmente in esecuzione.

Per avviare e interrompere manualmente un processo di eliminazione incidenti

- 1 Fare clic su **Avvia eliminazione** per avviare manualmente un processo di eliminazione incidenti.
- 2 Quando un processo di eliminazione incidenti è in esecuzione, l'indicatore di stato mostra il numero di incidenti eliminati.
- 3 Per interrompere un processo di eliminazione incidenti, fare clic su **Interrompi eliminazione**.

L'indicatore di stato si aggiorna ogni 30 secondi per impostazione predefinita. Se si sta eliminando un numero di incidenti molto elevato (oltre 500.000), il processo di aggiornamento può ridurre le prestazioni del processo di eliminazione. È possibile regolare la frequenza di aggiornamento nel file `manager.properties`.

Per configurare la frequenza di aggiornamento della barra di stato

- 1 Aprire il file `manager.properties`:
 - **Sui sistemi Windows:** `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\manager.properties`

- Sui sistemi Linux: `/opt/Symantec/DataLossPrevention/EnforceServer/15.1/Protect/config/manager.properties`
 - 2 Impostare un nuovo valore in millisecondi per la proprietà `com.vontu.incident.deletion.progress.refreshRate`. Ad esempio, impostare la frequenza di aggiornamento su due minuti (120 secondi):

`com.vontu.incident.deletion.progress.refreshRate=120000`
 - 3 Salvare e chiudere il file `manager.properties`, quindi riavviare il servizio Symantec DLP Manager.
- Vedere ["Informazioni sui servizi Symantec Data Loss Prevention"](#) a pagina 101.

Uso della cronologia processi di eliminazione

La sezione della cronologia processi di eliminazione mostra i processi di eliminazione incidenti eseguiti in precedenza, tra cui:

- Numero di incidenti eliminati.
- Numero di allegati e file eliminati.
- Ora di inizio e fine del processo di eliminazione.
- Durata del processo di eliminazione.
- Se il processo di eliminazione è stato interrotto manualmente.
- Lo stato del processo di eliminazione.

Se un processo di eliminazione non riesce, nella colonna di stato viene visualizzato un collegamento. Fare clic sul collegamento per vedere il messaggio di errore e la descrizione del problema. Queste informazioni possono essere utili all'amministratore del database di Oracle per la risoluzione dei problemi di un processo di eliminazione non riuscito.

In caso di difficoltà con la risoluzione dei problemi associati a processi di eliminazione incidenti, è possibile esportare informazioni dettagliate sul processo di eliminazione e inviarle al Supporto Symantec Data Loss Prevention.

Per visualizzare ed esportare informazioni sul processo di eliminazione non riuscito

- 1 Nell'elenco **Cronologia processi di eliminazione** fare clic sul collegamento **Non riuscito** per il processo non riuscito da visualizzare.

Il messaggio di errore e la descrizione del problema visualizzati potrebbero risultare utili all'amministratore di database di Oracle per la risoluzione dei problemi di un processo di eliminazione incidenti non riuscito. Per ulteriori informazioni andare al passaggio 2.

- 2 Per esportare informazioni per un processo di eliminazione non riuscito, selezionare il processo nell'elenco **Cronologia processi di eliminazione**, quindi fare clic su **Esporta**.
- 3 Salvare il file ZIP da inviare al Supporto Symantec Data Loss Prevention per l'analisi. I dati contenuti nel file ZIP sono destinati all'uso esclusivo da parte del Supporto Symantec Data Loss Prevention e non risultano utili per operazioni di risoluzione dei problemi interne all'organizzazione.

Informazioni su come contrassegnare automaticamente gli incidenti da eliminare

È possibile contrassegnare automaticamente gli incidenti da eliminare sulla base di criteri definiti dall'utente. Ad esempio, è consigliabile contrassegnare automaticamente gli incidenti per l'eliminazione in base alla data. Contrassegnare automaticamente gli incidenti per l'eliminazione consente di risparmiare una notevole quantità di tempo e risorse, in particolare in caso di numero elevato di incidenti nel sistema.

Gli incidenti che vengono automaticamente contrassegnati per l'eliminazione vengono eliminati definitivamente dal sistema quando viene eseguito il processo di eliminazione incidenti successivo. A differenza degli incidenti selezionati manualmente, l'operazione di contrassegno automatico per l'eliminazione contrassegna per l'eliminazione l'intero incidente, inclusi dati dei messaggi e allegati.

Vedere ["Informazioni sul processo di eliminazione incidente"](#) a pagina 1662.

Per contrassegnare automaticamente gli incidenti per l'eliminazione, è necessario innanzitutto creare report di incidente personalizzati utilizzando i propri criteri, ad esempio l'età degli incidenti. È possibile avere un report attivo per categoria di incidente: **rete**, **endpoint**, **Discover** e **applicazioni**. Questi tipi di report dipendono dalle licenze: non è possibile creare o esaminare i report per i quali non si dispone di una licenza.

Vedere ["Informazioni sulla creazione dei report di incidente per contrassegnare automaticamente gli incidenti per l'eliminazione"](#) a pagina 1666.

Dopo aver creato i report di incidente personalizzati, configurare e gestire i processi di contrassegno degli incidenti da eliminare nella pagina **Sistema > Utilità di eliminazione degli incidenti > Contrassegna incidenti da eliminare**.

Vedere ["Configurazione del contrassegno automatico degli incidenti da eliminare"](#) a pagina 1667.

Vedere ["Gestione del processo di contrassegno automatico degli incidenti da eliminare"](#) a pagina 1668.

È necessario disporre dei privilegi di amministratore Symantec Data Loss Prevention per configurare il contrassegno automatico degli incidenti da eliminare.

Informazioni sulla creazione dei report di incidente per contrassegnare automaticamente gli incidenti per l'eliminazione

L'utente crea report personalizzati che includono i criteri per contrassegnare automaticamente gli incidenti da eliminare nella pagina **Incidenti** per ciascun tipo specifico di incidente. Symantec consiglia di utilizzare i report a riepilogo singolo solo per contrassegnare gli incidenti da eliminare.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

Il report di sistema più utile da cui iniziare quando si creano report di incidente personalizzati per contrassegnare gli incidenti da eliminare è il report **Incidenti > tipo di incidente > Incidenti-Tutti**. Questo report di sistema include tutti gli incidenti presenti nel sistema per un determinato tipo di incidente.

Di seguito è fornito un esempio della procedura da seguire per contrassegnare per l'eliminazione gli incidenti di rete creati tra 1° gennaio 2016 e il 1° gennaio 2017. Si tratta di una procedura semplice, basata esclusivamente sul filtraggio dell'elenco di tutti gli incidenti di rete per un intervallo di date. In questo esempio non vengono applicati filtri aggiuntivi o riepiloghi.

Per creare un report per filtrare gli incidenti di rete all'interno di un intervallo di date

- 1 Nella console di amministrazione di Enforce Server, accedere a **Incidenti > Rete > Incidenti-Tutti**.
- 2 Nella sezione **Filtro**, selezionare **Stato: È uguale a Tutti**.
- 3 Nella sezione **Data**, selezionare **Personalizza**, quindi immettere come data di inizio **1/1/16** e come data di fine **1/1/17**.
- 4 Fare clic su **Applica**.
- 5 Fare clic su **Salva > Salva con nome**.
- 6 Immettere un nome e una descrizione per il report nella finestra di dialogo **Salva report con nome**, quindi fare clic su **Salva**.

È ora possibile visualizzare il report personalizzato nella pagina **Incidenti > Tutti i report** e selezionarlo quando si configura il processo di contrassegno automatico degli incidenti da eliminare.

È possibile utilizzare **Filtri e riepilogo avanzati** per affinare ulteriormente i report.

Gli incidenti che sono stati nascosti dai report non verranno eliminati anche se soddisfano i criteri selezionati. È necessario rendere visibili gli incidenti che si desidera contrassegnare automaticamente per l'eliminazione.

Vedere ["Visualizzazione di incidenti nascosti"](#) a pagina 1697.

Vedere ["Report di filtraggio"](#) a pagina 1648.

Configurazione del contrassegno automatico degli incidenti da eliminare

È possibile configurare il contrassegno automatico degli incidenti da eliminare nella pagina **Sistema > Utilità di eliminazione degli incidenti > Contrassegna incidenti da eliminare**. Per configurare il contrassegno automatico degli incidenti da eliminare è necessario selezionare i report di incidente personalizzati e pianificare i processi di contrassegno degli incidenti da eliminare. È necessario disporre dei privilegi di amministratore Symantec Data Loss Prevention per configurare il contrassegno automatico degli incidenti da eliminare.

Vedere ["Informazioni sulla creazione dei report di incidente per contrassegnare automaticamente gli incidenti per l'eliminazione"](#) a pagina 1666.

Per configurare il contrassegno automatico degli incidenti da eliminare

- 1 Nella console di amministrazione di Enforce Server, accedere alla pagina **Sistema > Utilità di eliminazione degli incidenti > Contrassegna incidenti da eliminare**.
- 2 Fare clic su **Configura**.
- 3 Nella pagina di configurazione, selezionare il report o i report che includono gli incidenti che si desidera contrassegnare per l'eliminazione. È possibile selezionare un report per tipo di incidente. Non è possibile selezionare report di sistema per contrassegnare gli incidenti da eliminare.
- 4 Impostare una pianificazione per le operazioni di contrassegno degli incidenti da eliminare. È possibile pianificare le operazioni di contrassegno degli incidenti da eliminare in modo che vengano eseguite in un momento specifico una sola volta, ogni giorno, ogni settimana o ogni mese. È inoltre possibile selezionare **Nessuna pianificazione regolare** se si preferisce pianificare i processi di eliminazione degli incidenti manualmente.

In fase di pianificazione delle operazioni di contrassegno degli incidenti da eliminare è necessario tenere presenti due aspetti:

- Prima di poter eseguire le operazioni di eliminazione degli incidenti è necessario completare le operazioni di contrassegno degli incidenti da eliminare.
- Le operazioni di contrassegno degli incidenti da eliminare devono essere eseguite quando Symantec Data Loss Prevention non è in esecuzione in altri processi.

- 5 Fare clic su **Salva**.

Gestione del processo di contrassegno automatico degli incidenti da eliminare

È possibile gestire i processi di contrassegno automatico degli incidenti da eliminare nella pagina **Sistema > Utilità di eliminazione degli incidenti > Contrassegna incidenti da eliminare**. In questa pagina è possibile visualizzare i report personalizzati per contrassegnare gli incidenti da eliminare, la pianificazione del prossimo processo di contrassegno degli incidenti da eliminare e la cronologia dei processi di contrassegno degli incidenti da eliminare.

È possibile collegarsi direttamente al report dei processi di contrassegno degli incidenti da eliminare facendo clic sul nome del report nella sezione **Report selezionati per contrassegnare gli incidenti**.

È possibile visualizzare la cronologia dei processi di contrassegno degli incidenti da eliminare nella sezione **Cronologia processi contrassegno incidenti da eliminare**. Per la cronologia di ciascun processo, Symantec Data Loss Prevention visualizza le seguenti informazioni:

- **ID processo** : identificatore del processo di contrassegno degli incidenti da eliminare.
- **Processo avviato** : ora di inizio del processo di contrassegno degli incidenti da eliminare.
- **Nome report** : nome del report personalizzato utilizzato per contrassegnare gli incidenti da eliminare.
- **N. incidenti contrassegnati** : numero di incidenti contrassegnati per l'eliminazione mediante questo processo.
- **Stato** : stato del processo di contrassegno degli incidenti da eliminare.

È possibile annullare i processi di contrassegno degli incidenti da eliminare selezionando uno o più processi mediante le relative caselle di controllo e facendo clic su **Elimina**. Non viene visualizzato alcun messaggio di conferma dell'avvenuta eliminazione dei processi di contrassegno degli incidenti da eliminare, sebbene i processi eliminati vengono visualizzati nei registri Tomcat.

Risoluzione dei problemi relativi al contrassegno automatico degli incidenti da eliminare

Il contrassegno automatico degli incidenti da eliminare include due codici di evento utili per tenere traccia dei processi di contrassegno degli incidenti da eliminare. Inoltre, registra le informazioni sul processo nei registri Tomcat.

I codici di evento del sistema sono:

- 2318: Incident deletion flagging process started.
- 2319: Incident deletion flagging process ended.

I registri Tomcat includono le seguenti informazioni (interruzioni di riga aggiunte per migliorare la leggibilità):


```
Timestamp- Thread: 111 INFO  
[com.vontu.manager]  
User "Administrator" initiated incident action  
"Marked for Deletion" for 6 incident(s)
```

```
Timestamp- Thread: 111 INFO  
[com.vontu.manager]  
Incident deletion flagging process ended.
```

```
Timestamp- Thread: 119 INFO  
[com.vontu.manager.system.incident.deletion.IncidentFlagDeletionListController]  
The flagged incident deletion jobs have been deleted. Number of jobs deleted are: N
```

I processi di contrassegno degli incidenti da eliminare potrebbero avere esito negativo in quanto lo spazio disponibile è insufficiente per l'esecuzione delle azioni di annullamento/ripristino nel database Symantec Data Loss Prevention. Per informazioni dettagliate sulla gestione del database, consultare il *Manuale di manutenzione del sistema di Symantec Data Loss Prevention*.

Eliminazione dei dashboard e dei report personalizzati

È possibile eliminare i dashboard o i report personalizzati creati.

Per eliminare un dashboard o un report personalizzato

- 1 Nel menu **Incidenti** della console di amministrazione di Enforce Server selezionare **Report incidente**.
Viene visualizzato il dashboard **Report incidente** con **Report salvati** vicino alla parte superiore.
- 2 Fare clic sull'icona di eliminazione accanto al report o al dashboard da eliminare.
- 3 Fare clic su **Sì** per confermare.
- 4 Symantec Data Loss Prevention elimina il report e lo rimuove dalla schermata **Report incidente**.

Caratteristiche report incidenti più comuni

Le seguenti opzioni sono comuni negli elenchi dei report degli incidenti:





- Icone per eseguire le seguenti attività di un report:
 - **Salva**
È possibile salvare il report più aggiornato come report personalizzato.
Vedere "[Salvataggio dei report di incidente personalizzati](#)" a pagina 1649.

- **Invia**
 È possibile inviare il report tramite e-mail o pianificare la distribuzione del report.
 Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.
 - **Esporta**
 È possibile esportare il report corrente come CSV o XML.
 Vedere ["Esportazione dei report di incidente"](#) a pagina 1656.
 - **Elimina report**
 Se questo report non è un report salvato, l'opzione **Elimina report** non viene visualizzata.
 - Filtri report e opzioni di riepilogo
 Vedere ["Filtro report incidente e opzioni di riepilogo"](#) a pagina 1671.
 - Icone delle pagine di navigazione
 Vedere ["Navigazione della pagina dei report incidente"](#) a pagina 1670.
- I seguenti report dei riepiloghi sono disponibili per i tipi di incidente:
- Rete
 Vedere ["Report riepilogo rete"](#) a pagina 1591.
 - Endpoint
 Vedere ["Report di riepilogo sugli incidenti endpoint"](#) a pagina 1605.
 - Discover
 Vedere ["Report riepilogativi di Discover"](#) a pagina 1618.

Navigazione della pagina dei report incidente

Tutti i report, eccetto i quadri generali, comprendono opzioni di navigazione nella pagina. Symantec Data Loss Prevention mostra il numero di incidenti attualmente visibili sul totale degli incidenti riportati (ad esempio, 1-19 di 19 o 1-50 di 315).

I report con più di 50 incidenti hanno le seguenti opzioni:

- | | |
|---|--|
|  | Visualizza la prima pagina del report. |
|  | Visualizza la pagina precedente. |
|  | Visualizza la pagina successiva. |
|  | Visualizza l'ultima pagina. |

Mostra tutto	<p>Visualizza tutti gli oggetti su una singola pagina.</p> <p>Usare con prudenza il collegamento di Mostrare tutti su Lista incidenti quando il sistema contiene più di 500 incidenti. Le prestazioni del browser peggiorano drasticamente se sono visualizzati più di 500 incidenti alla pagina di Lista incidenti.</p>
Seleziona tutto	<p>Selezionare tutti gli incidenti su tutte le pagine, in modo da poterli aggiornare contemporaneamente. (Disponibile solo sulle liste di incidenti.) Fare clic su Deseleziona tutto per annullare.</p> <p>Nota: Prestare attenzione quando si sceglie Seleziona tutto. Questa opzione seleziona tutti gli incidenti nel report (non solo quelli nella pagina corrente). Qualsiasi comando incidente applicato successivamente riguarda tutti gli incidenti.</p> <p>Per selezionare solo gli incidenti nella pagina corrente, selezionare la casella di controllo in alto a sinistra dell'elenco incidenti.</p>

Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.

Filtro report incidente e opzioni di riepilogo

In genere, i filtri si dividono in filtri più utilizzati, filtri avanzati e riepiloghi.

I filtri più comuni includono le seguenti opzioni:

Stato	Selezionare È uguale a , È uno qualsiasi dei seguenti valori oppure Non è alcuno dei seguenti valori , quindi selezionare i valori dello stato. Tenere premuto Ctrl e fare clic per selezionare più valori di stato separati. Tenere premuto Maiusc e fare clic per selezionare un intervallo.
Data Report di rete ed Endpoint	Utilizzare il menu a discesa per selezionare un intervallo di date come Ultima settimana o Ultimo mese . Il valore predefinito è Tutte le date .
Gravità	Selezionare le caselle per scegliere i valori di gravità.
Scansione Report Discover	Per i report Discover, selezionare la scansione di cui creare il report. È possibile selezionare la scansione più recente, la scansione iniziale o una scansione in corso. Tutte le scansioni è il valore predefinito.
ID target	Per i report Discover, selezionare il nome del target di cui creare il report. Tutti i target è il valore impostato come predefinito.

Fare clic sulla barra **Filtri avanzati e riepilogo** per espandere la sezione con i filtri e le opzioni del riepilogo.

Fare clic su **Aggiungi filtro** per aggiungere un filtro avanzato.

Selezionare un'opzione primaria e secondaria facoltativa per il riepilogo. Un report a riepilogo singolo è organizzato con un singolo criterio riepilogativo, come la politica associata a ciascun incidente. Un report a riepilogo doppio è organizzato con due criteri, quali la politica e lo stato dell'incidente.

Nota: Se si seleziona una condizione nella quale si inserisce un contenuto da far corrispondere nel campo del testo, l'intera voce deve corrispondere esattamente. Ad esempio, se si inserisce "mele e arance", lo stesso identico testo deve essere visualizzato nel componente specificato affinché venga considerato corrispondente. La frase "Portami mele e arance" non è considerata una corrispondenza.

Per un elenco completo del filtro di report e le opzioni di riepilogo, vedere il *Manuale dell'amministratore di Symantec Data Loss Prevention*.

Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.

Invio dei report degli incidenti tramite e-mail

È possibile inviare una copia del report aggiornato a qualsiasi indirizzo e-mail.

Per inviare i report, l'amministratore di sistema deve configurare un server SMTP. L'amministratore deve specificare un'opzione di distribuzione del report alla pagina **Sistema > Impostazioni**. Inoltre, è necessario specificare un indirizzo e-mail per il proprio account utente.

Vedere ["Configurazione di Enforce Server per l'invio di avvisi tramite e-mail"](#) a pagina 183.

Per inviare un report

- 1 Fare clic su **Incidenti** e selezionare un tipo di report.
- 2 Andare sul report che si desidera esportare. Filtrare o riepilogare gli incidenti nel report come desiderato.

Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.

- 3 Fare clic su **Invia** nell'angolo in alto a destra.

In alternativa, è possibile utilizzare il menu **Invia** (sopra i filtri).

Vedere ["Salvataggio dei report di incidente personalizzati"](#) a pagina 1649.

4 Nella finestra di dialogo **Invia report**, specificare le seguenti opzioni:

A	Immettere uno o più indirizzi e-mail separati da virgole.
Oggetto	Immettere l'oggetto del messaggio.
Messaggio	Immettere il messaggio.

5 Fare clic su **Invio** o **Annulla**.

Vedere ["Stampa di report di incidenti"](#) a pagina 1673.

Vedere ["Esportazione dei report di incidente"](#) a pagina 1656.

Stampa di report di incidenti

È possibile stampare un report per ogni stampante disponibile.

Per stampare un report

- 1 Fare clic su **Incidenti** e selezionare un tipo di report.
- 2 Andare sul report che si desidera esportare. Filtrare o riepilogare gli incidenti nel report, come desiderato.
Vedere ["Caratteristiche report incidenti più comuni"](#) a pagina 1669.
- 3 Fare clic su **Stampa** nell'angolo in alto a destra.
- 4 Un'immagine del report compare in una finestra del browser.
- 5 Viene visualizzata la finestra di dialogo di selezione della stampante ed è possibile selezionare una stampante.

Vedere ["Invio dei report degli incidenti tramite e-mail"](#) a pagina 1672.

Vedere ["Esportazione dei report di incidente"](#) a pagina 1656.

Scheda della cronologia delle istantanee incidente

È possibile visualizzare le azioni effettuate sull'incidente. Per ogni azione, la scheda **Cronologia** visualizza la data e l'ora di azione, l'attore (un utente o un server) e l'azione o il commento.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Scheda note istantanea incidente

È possibile aggiungere una nota a un incidente o visualizzare le note esistenti per quell'incidente nella scheda **Note**. Per aggiungere una nota, fare clic su **Aggiungi nota**. Il limite per le note è 4000 byte.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Sezione attributi istantanea incidente

È possibile visualizzare un elenco di attributi personalizzati e dei relativi valori, se specificati. Fare clic sui valori di attributo per visualizzare un elenco di incidenti filtrato in base a tale valore. Per aggiungere nuovi valori o modificare i valori esistenti, fare clic su **Modifica**. Nella finestra di dialogo **Modifica attributi** visualizzata, digitare i nuovi valori e fare clic su **Salva**. Gli incidenti nascosti non sono visualizzati nell'elenco filtrato.

Nota: Questa sezione appare solo se un amministratore di sistema ha configurato attributi personalizzati.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Scheda Correlazioni dell'istantanea incidente

È possibile visualizzare elenchi di incidenti che condividono vari attributi dell'incidente corrente.

Ad esempio, se la copia di un file ha generato l'incidente corrente, è possibile visualizzare un elenco di tutti gli incidenti collegati alla copia di quel file. La scheda **Correlazioni** mostra un elenco delle correlazioni abbinate a singoli attributi. Fare clic sui valori di attributo per visualizzare elenchi degli incidenti correlati a tali valori.

Per cercare altri incidenti con gli stessi attributi, fare clic su **Trova simile**. Nella finestra di dialogo **Trova incidenti simili** visualizzata, selezionare gli attributi di ricerca desiderati. Quindi fare clic su **Trova incidenti**. Gli incidenti nascosti non sono visualizzati quando si cercano incidenti simili.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Sezione Politica dell'istantanea incidente

La sezione **Politica** mostra la politica che è stata violata nell'incidente e indica se questa ha bloccato uno spostamento o ha informato l'utente. Mostra inoltre il numero totale di corrispondenze per la politica e le corrispondenze per regola della politica. Fare clic sul nome della politica per visualizzare un elenco di tutti gli incidenti che hanno violato la politica. Fare clic su visualizza politica per visualizzare una versione di sola lettura della politica.

Sono visualizzate le icone che descrivono le seguenti informazioni:

- Symantec Data Loss Prevention ha bloccato una copia dei dati riservati.
- Symantec Data Loss Prevention ha informato l'utente della copia dei dati riservati.

Questa sezione elenca anche altre politiche violate dallo stesso file. Per visualizzare l'istantanea di un incidente associato a una determinata politica, fare clic sul collegamento **Vai a incidente** accanto al nome della politica. Per visualizzare un elenco di tutti gli incidenti relativi al file, fare clic su Mostra tutto.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Sezione delle corrispondenze delle istantanee di incidenti

Nella sezione **Corrispondenze**, Symantec Data Loss Prevention visualizza il contenuto (se applicabile) e le corrispondenze che hanno generato l'incidente.

Le corrispondenze sono evidenziate in giallo. Questa sezione mostra le corrispondenze totali nell'ordine in cui sono visualizzate nel contenuto originale. Per visualizzare la regola che ha attivato una corrispondenza, fare clic sulla corrispondenza evidenziata.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Vedere ["Informazioni sulla soglia di similarità e sul punteggio di somiglianza"](#) a pagina 632.

Sezione Informazioni accesso dell'istantanea incidente

La sezione **Informazioni accesso** di un'istantanea incidente mostra gli elenchi di controllo di accesso per quell'oggetto.

Gli elenchi di controllo di accesso (ACL) elencano le autorizzazioni associate a un oggetto o a un dato. L'elenco contiene informazioni su tutti gli utenti che hanno autorizzazioni di lettura e scrittura per il file. Utilizzare l'elenco per visualizzare quali utenti hanno accesso al file come pure le azioni che ogni utente può eseguire. Le autorizzazioni per ogni utente o gruppo non sono impostate tramite Symantec Data Loss Prevention. Gli amministratori impostano le autorizzazioni per ogni file utilizzando altri tipi di programmi sull'endpoint. Le autorizzazioni sono in genere impostate alla creazione del file.

Ad esempio, Utente 1 ha l'autorizzazione di accedere al file `Esempio1.doc`. Utente 1 può visualizzare e modificare il file. Anche Utente 2 ha accesso al file `Esempio1.doc`. Tuttavia, Utente 2 può soltanto visualizzare il file. Utente 2 non dispone dell'autorizzazione per modificare il file. Nell'ACL, sia Utente 1 che Utente 2 sono elencati con le autorizzazioni che sono state concesse loro.

[Tabella 51-1](#) mostra le combinazioni.

Tabella 51-1 Esempio di elenco di controllo di accesso

Nome	Autorizzazione
Utente 1	GRANT READ
Utente 1	GRANT WRITE
Utente 2	GRANT READ

L'ACL contiene una nuova riga per ogni autorizzazione concessa. L'ACL contiene solo una riga per Utente 2 in quanto questo utente ha una sola autorizzazione, quella per leggere il file. Utente 2 non può modificare il file. Utente 1 ha due voci in quanto tale utente ha due autorizzazioni: lettura e modifica del file.

È possibile visualizzare le informazioni ACL solo sulle istantanee incidente dell'unità locale dell'endpoint e di Discover. Non è possibile visualizzare le informazioni ACL su qualsiasi altro tipo di incidenti.

La sezione **Informazioni accesso** si trova nella scheda **Informazioni chiave** dell'istantanea incidente.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

Vedere ["Istantanea ticket Endpoint"](#) a pagina 1597.

Vedere ["Istantanea incidente di rete"](#) a pagina 1586.

Personalizzazione della pagina dell'istantanea incidente

È possibile personalizzare l'aspetto della pagina dell'istantanea incidente.

Per personalizzare l'aspetto della pagina dell'istantanea incidente

- 1 In un'istantanea incidente, fare clic su **Personalizza layout** (nell'angolo in alto a destra).
- 2 Selezionare le informazioni da visualizzare su ciascuna delle schede delle istantanee incidente.
- Scheda 1** contiene sempre le **informazioni chiave** e non può essere modificata.
- 3 Per ciascuna delle aree sulla schermata dell'istantanea incidente, selezionare le informazioni da visualizzare.
- 4 Fare clic su **Salva**.

Informazioni sui filtri e sulle opzioni di riepilogo per i report

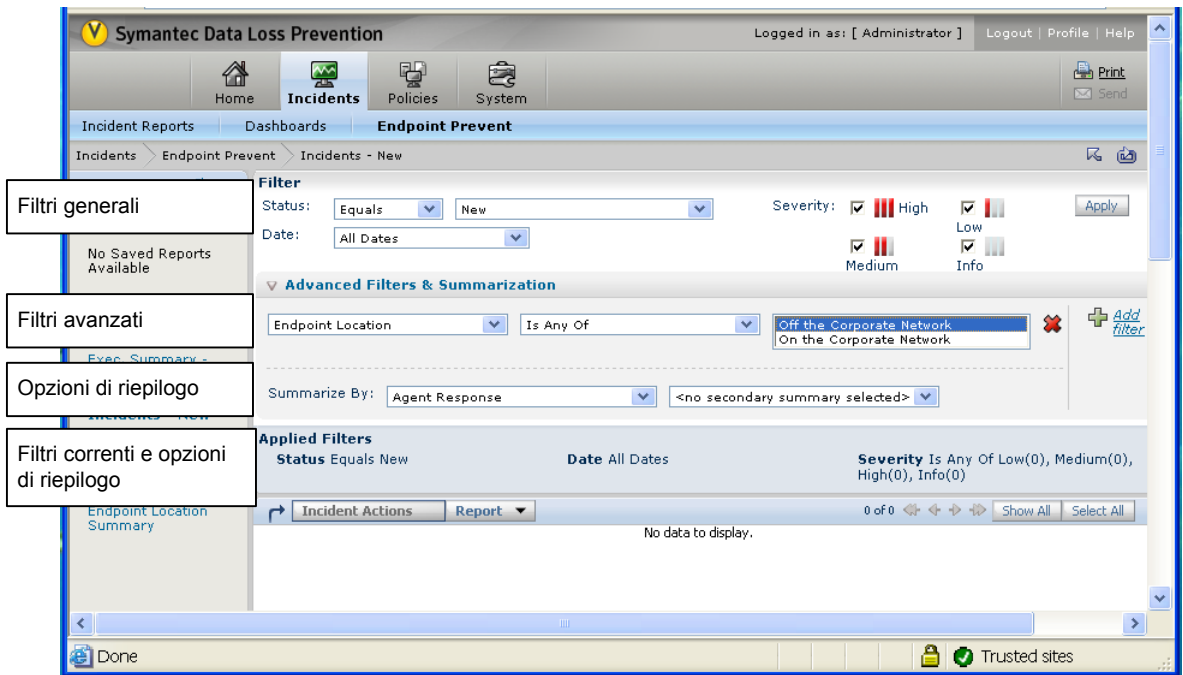
È possibile impostare una serie di filtri e di riepiloghi per i report incidenti di Symantec Data Loss Prevention.

Tali filtri consentono di visualizzare gli incidenti e i relativi dati in modi diversi.

Il set di filtri si applica separatamente agli eventi relativi a rete, endpoint e archiviazione.

[Figura 51-1](#) mostra le posizioni delle opzioni per filtrare e riepilogare i report.

Figura 51-1 Opzioni di riepilogo e di filtro



I filtri e le opzioni di riepilogo si trovano nelle seguenti sezioni:

Filtri generali

Le opzioni dei filtri generali sono quelle usate più comunemente. Sono sempre visibili nel report della lista di incidente.

Vedere ["Filtri generali per i report"](#) a pagina 1679.

Filtri avanzati

I opzioni dei filtri avanzati forniscono molte opzioni supplementari. È necessario fare clic sulla barra **Filtri avanzati e riepilogo** e poi su **Aggiungi filtro** per visualizzare queste opzioni del filtro.

Vedere ["Opzioni di filtro avanzate per i report"](#) a pagina 1687.

Opzioni di riepilogo

Le opzioni di riepilogo forniscono modi per riassumere gli incidenti nella lista. È necessario fare clic sulla barra **Filtri avanzati e riepilogo** per visualizzare queste opzioni di riepilogo.

Vedere ["Opzioni di riepilogo per i report di incidente"](#) a pagina 1682.

Symantec Data Loss Prevention contiene molti report standard. È inoltre possibile creare report personalizzati o salvare le opzioni di riepilogo e del filtro per riutilizzarle in futuro.

Vedere ["Informazioni sui report Symantec Data Loss Prevention"](#) a pagina 1632.

Filtri generali per i report

I filtri generali per i report comprendono un set di alcuni filtri comuni.

La maggior parte di questi filtri è applicabile a tutti i prodotti. Network Discover/Cloud Storage Discover contiene alcuni filtri generali relativi alle scansioni degli archivi. Ad esempio, è possibile filtrare gli incidenti in una particolare scansione. Questi filtri non sono applicabili a Network Prevent o Endpoint Prevent.

[Tabella 51-2](#) elenca le opzioni di filtro generali per i valori di stato dei report.

È anche possibile creare valori di stato personalizzati.

Vedere ["Informazioni sugli attributi di stato incidente."](#) a pagina 1700.

Questi filtri di stato sono disponibili per gli incidenti di Rete, Endpoint e Discover.

Tabella 51-2 Filtri generali per valori di stato

Nome	Descrizione
È uguale a	Lo stato è uguale al campo che è selezionato nell'elenco a discesa seguente.
È uno qualsiasi dei seguenti valori	Lo stato può essere uno qualsiasi dei campi selezionati nell'elenco a discesa seguente. Tenere premuto MAIUSC e fare clic per selezionare molteplici campi.
Non è alcuno dei seguenti valori	Lo stato non è nessuno dei campi selezionati nell'elenco a discesa seguente. Tenere premuto MAIUSC e fare clic per selezionare molteplici campi.

[Tabella 51-3](#) elenca le opzioni di filtro generali per data.

Questi filtri di data sono disponibili per gli incidenti di Rete ed Endpoint.

Tabella 51-3 Filtri generali per data

Nome	Descrizione
Tutte le date	Tutte le date che includono incidenti.
Mese corrente a data	Tutti gli incidenti che sono stati segnalati per il mese corrente fino alla data odierna.

Nome	Descrizione
Trimestre corrente a data	Tutti gli incidenti che sono stati segnalati per il trimestre corrente fino alla data odierna.
Settimana corrente a data	Tutti gli incidenti che sono stati segnalati per la settimana corrente.
Anno corrente a data	Tutti gli incidenti che sono stati segnalati per l'anno corrente fino alla data odierna.
Personalizzato	Un periodo di tempo personalizzato. Selezionare le date desiderate dal menu del calendario.
Ultimi 7 giorni	Tutti gli incidenti che sono stati segnalati negli ultimi 7 giorni.
Ultimi 30 giorni	Tutti gli incidenti che sono stati segnalati negli ultimi 30 giorni.
Ultimo mese	Tutti gli incidenti che sono stati segnalati nel mese di calendario precedente.
Ultima settimana	Tutti gli incidenti che sono stati segnalati nella settimana di calendario precedente.
Ultimo trimestre	Tutti gli incidenti che sono stati segnalati nel trimestre precedente.
Anno scorso	Tutti gli incidenti che sono stati segnalati nell'ultimo anno di calendario.
Oggi	Tutti gli incidenti che sono stati segnalati oggi.
Ieri	Tutti gli incidenti che sono stati segnalati ieri.

Tabella 51-4 elenca le opzioni di filtro per gravità. Spuntare la casella per selezionare i valori di gravità da includere nel filtro.

Questi filtri di gravità sono disponibili per gli incidenti di Rete, Endpoint e Discover.

Tabella 51-4 Filtri generali per valori di gravità

Nome	Descrizione
Alta	Elenca solo gli incidenti di gravità alta. Visualizza il numero di incidenti di gravità alta inclusi nell'elenco di incidenti.
Informazioni	Elenca solo gli incidenti di tipo informativo. Agli incidenti informativi non viene assegnato nessun altro valore di gravità. Visualizza il numero di incidenti informativi inclusi nell'elenco di incidenti.
Bassa	Elenca solo gli incidenti di gravità bassa. Visualizza il numero di incidenti di gravità bassa inclusi nell'elenco di incidenti.
Media	Elenca solo gli incidenti di gravità media. Visualizza il numero di incidenti di gravità media inclusi nell'elenco di incidenti.

[Tabella 51-5](#) elenca le opzioni di filtro generali per le scansioni di Network Discover. Questo filtro è disponibile solo per gli incidenti di Discover.

Tabella 51-5 Filtri generali per scansioni

Nome	Descrizione
Tutte le scansioni	Tutti gli incidenti che sono stati segnalati in tutte le scansioni eseguite.
Scansione iniziale	Tutti gli incidenti che sono stati segnalati nella scansione iniziale.
In corso	Tutti incidenti che sono stati segnalati nelle scansioni attualmente in corso.
Ultima scansione completata	Tutti incidenti che sono stati segnalati nell'ultima scansione completata.

È possibile filtrare gli incidenti di Discover mediante **ID target**. Questo filtro è disponibile solo per gli incidenti di Discover.

Selezionare il target oppure **Tutti i target**. Tenere premuto MAIUSC e fare clic per selezionare molteplici campi.

[Tabella 51-6](#) elenca le opzioni di filtro generali per data di rilevamento degli incidenti Discover.

Tabella 51-6 Filtri generali per data

Nome	Descrizione
Tutte le date	Tutte le date che includono incidenti.
Mese corrente a data	Tutti gli incidenti che sono stati segnalati per il mese corrente fino alla data odierna.
Trimestre corrente a data	Tutti gli incidenti che sono stati segnalati per il trimestre corrente fino alla data odierna.
Settimana corrente a data	Tutti gli incidenti che sono stati segnalati per la settimana corrente.
Anno corrente a data	Tutti gli incidenti che sono stati segnalati per l'anno corrente fino alla data odierna.
Personalizzato	Un periodo di tempo personalizzato. Selezionare le date desiderate dal menu del calendario.
Personalizza da	I Symantec DLP Agent che si sono collegati all'Endpoint Server a partire da una data specifica fino alla data corrente. Selezionare la data iniziale per il filtro.
Personalizza prima	I Symantec DLP Agent che si sono collegati a un Endpoint Server prima di una data specifica. Selezionare la data finale per il filtro.

Nome	Descrizione
Ultimi 7 giorni	Tutti gli incidenti che sono stati segnalati negli ultimi 7 giorni.
Ultimi 30 giorni	Tutti gli incidenti che sono stati segnalati negli ultimi 30 giorni.
Ultimo mese	Tutti gli incidenti che sono stati segnalati nel mese di calendario precedente.
Ultima settimana	Tutti gli incidenti che sono stati segnalati nella settimana di calendario precedente.
Ultimo trimestre	Tutti gli incidenti che sono stati segnalati nel trimestre precedente.
Anno scorso	Tutti gli incidenti che sono stati segnalati nell'ultimo anno di calendario.
Oggi	Tutti gli incidenti che sono stati segnalati oggi.
Ieri	Tutti gli incidenti che sono stati segnalati ieri.

Opzioni di riepilogo per i report di incidente

I riepiloghi dei report di incidenti forniscono opzioni per un riepilogo delle informazioni che sono contenute negli incidenti. Ad esempio, è possibile riassumere gli incidenti per stato o per politica.

Nota: Gli incidenti nascosti non sono inclusi in riassunti di report a meno che l'opzione Filtro avanzato per il filtro **È nascosto** sia impostata a **Mostra tutto**.

Vedere ["Informazioni su come nascondere gli incidenti"](#) a pagina 1696.

[Tabella 51-7](#) elenca le opzioni per i report di incidente.

Tabella 51-7 Filtri di riepilogo

Nome	Descrizione	Prodotti interessati
Configurazione agente	Riepiloga gli agenti e gli incidenti in base all'entità di configurazione agente associata. Se si hanno più entità di configurazione agente configurate, è possibile riassumerle o filtrarle mediante un menu a discesa. Se l'entità di configurazione agente predefinita è la sola entità configurata, il menu a discesa non è visualizzato.	Endpoint

Nome	Descrizione	Prodotti interessati
Risposta agente	Riepiloga gli incidenti in base alla risposta dell'agente all'incidente.	Endpoint
Radice di contenuti	Riepiloga gli incidenti in base al percorso della radice di contenuti.	Discover
Indirizzo e-mail proprietario dati	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente o con un plug-in di ricerca.	Rete Endpoint Discover
Nome proprietario dati	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente o con un plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.	Rete Endpoint Discover
IP destinazione	Riepiloga gli incidenti in base all'indirizzo IP di destinazione.	Rete Endpoint
Mese rilevamento	Riepiloga gli incidenti in base al mese in cui sono stati rilevati.	Discover
Trimestre rilevamento	Riepiloga gli incidenti in base al trimestre solare in cui sono stati rilevati.	Discover
Settimana rilevamento	Riepiloga gli incidenti in base alla settimana in cui sono stati rilevati.	Discover
Anno rilevamento	Riepiloga gli incidenti in base all'anno in cui sono stati rilevati.	Discover
ID istanza dispositivo	Riepiloga gli incidenti in base al dispositivo che ha creato la violazione.	Endpoint
Dominio	Riepiloga gli incidenti in base al nome di dominio.	Rete

Nome	Descrizione	Prodotti interessati
Posizione endpoint	Riepiloga gli incidenti in base alla posizione dell'endpoint. La posizione può essere una delle seguenti: <ul style="list-style-type: none"> ■ All'interno della rete aziendale ■ All'esterno della rete aziendale 	Endpoint
Nome file	Riepiloga gli incidenti in base al nome di file associato all'incidente.	Endpoint
Proprietario file	Riepiloga gli incidenti in base al proprietario del file.	Discover
Stato analisi	Riepiloga gli agenti in base allo stato corrente.	Endpoint Discover
Posizione	Riepiloga gli incidenti in base alla relativa posizione.	Discover
Livello registro	Riepiloga gli agenti in base ai livelli di registro configurati.	Endpoint
IP computer (aziendale)	Riepiloga gli incidenti in base all'indirizzo IP di un computer della rete aziendale.	Endpoint
Nome computer	Riepiloga gli incidenti in base al nome del computer in cui gli incidenti sono stati creati.	Endpoint
Mese	Riepiloga gli incidenti in base al mese in cui sono stati creati.	Rete Endpoint
Mesi trascorsi dal primo rilevamento	Riepiloga gli incidenti in base ai mesi trascorsi dal momento in cui l'incidente è stato rilevato per la prima volta.	Discover
Azione Network Prevent	Riepiloga gli incidenti in base all'azione di Network Prevent.	Rete
Nessun riepilogo primario selezionato	Selezione segnaposto per denotare che non è stato selezionato nessun riepilogo principale.	Rete Endpoint Discover

Nome	Descrizione	Prodotti interessati
Nessun riepilogo secondario selezionato	Selezione segnaposto per denotare che non è stato selezionato nessun riepilogo.	Rete Endpoint Discover
Politica	Riepiloga gli incidenti in base alla politica da cui sono stati creati.	Rete Endpoint Discover
Gruppo di politiche	Riepiloga gli incidenti in base al gruppo di politiche a cui appartengono.	Rete Discover
Stato della protezione	Riepiloga gli incidenti in base allo stato della rete degli incidenti.	Discover
Protocollo	Riepiloga gli incidenti in base al protocollo che ha generato l'incidente.	Rete
Destinazione endpoint o protocollo	Riepiloga gli incidenti in base alla destinazione endpoint o al protocollo in cui sono stati creati gli incidenti.	Endpoint
Stato rilevamento riparazione	Riepiloga gli incidenti in base al relativo stato di rilevamento della riparazione.	Discover
Motivo errore quarantena	Riepiloga gli incidenti in base al motivo per cui l'azione di risposta di quarantena non è riuscita.	Endpoint Discover
Trimestre	Riepiloga gli incidenti in base al trimestre in cui sono stati creati.	Rete Endpoint
Trimestri trascorsi dal primo rilevamento	Riepiloga gli incidenti in base ai trimestri trascorsi dal momento in cui l'incidente è stato rilevato per la prima volta.	Discover
Destinatario	Riepiloga gli incidenti in base al destinatario.	Discover
Scansione	Riepiloga gli incidenti in base alla scansione usata per trovare gli incidenti.	Discover
Computer sottoposto a scansione	Riepiloga gli incidenti in base ai computer sottoposti a scansione.	Discover

Nome	Descrizione	Prodotti interessati
Mittente	Riepiloga gli incidenti in base al mittente.	Rete Endpoint Discover
Server o rilevatore	Riepiloga gli incidenti in base al server in cui sono stati creati.	Rete Endpoint
IP origine	Riepiloga gli incidenti in base alla indirizzo IP di origine da cui sono stati creati.	Rete Endpoint
File di origine	Riepiloga gli incidenti in base al file di origine che ha violato la politica.	Endpoint
Stato	Riepiloga gli incidenti in base allo stato dell'incidente.	Rete Endpoint Discover
Argomento	Riepiloga gli incidenti in base all'argomento.	Discover
ID target	Riepiloga gli incidenti in base all>ID di scansione del target.	Discover
Tipo di target	Riepiloga gli incidenti dal tipo di target su cui l'incidente è stato generato.	Discover
Giustificazione utente	Riepiloga gli incidenti dalla giustificazione che è stata inserita dall'utente.	Endpoint
Nome utente	Riepiloga gli incidenti in base all'utente che ha generato l'incidente.	Endpoint
Settimana	Riepiloga gli incidenti in base alla settimana in cui sono stati creati.	Rete Endpoint
Settimane trascorse dal primo rilevamento	Riepiloga gli incidenti in base alle settimane trascorse dal momento in cui l'incidente è stato rilevato per la prima volta.	Discover
Anno	Riepiloga gli incidenti in base all'anno in cui sono stati creati.	Rete Endpoint

Nome	Descrizione	Prodotti interessati
Anni trascorsi dal primo rilevamento	Riepiloga gli incidenti in base agli anni trascorsi dal momento in cui l'incidente è stato rilevato per la prima volta.	Discover

Opzioni di filtro avanzate per i report

I filtri di report avanzati consentono di filtrare gli incidenti relativi a specifiche azioni o stringhe di testo. Ad esempio, è possibile filtrare gli incidenti relativi a una specifica parola chiave. Oppure, è possibile escludere gli incidenti relativi a una determinata azione. Questi filtri combinano un set di campi o caselle di testo per creare il filtro avanzato.

[Tabella 51-8](#), [Tabella 51-9](#) e [Tabella 51-10](#) elencano le opzioni di filtro avanzate per i report.

Tabella 51-8 Filtri avanzati, primo campo

Nome	Descrizione	Prodotti interessati
Configurazione agente	Riepiloga gli agenti e gli incidenti in base all'entità di configurazione agente associata. Se si hanno più entità di configurazione agente configurate, è possibile riassumerle o filtrarle mediante un menu a discesa. Se l'entità di configurazione agente predefinita è la sola entità configurata, il menu a discesa non è visualizzato.	Endpoint
Stato configurazione agente	Riepiloga gli agenti in base allo stato dell'entità di configurazione. <ul style="list-style-type: none">■ Configurazione corrente La configurazione sull'agente e quella su Endpoint Server sono uguali.■ Configurazione obsoleta La configurazione sull'agente è differente da quella su Endpoint Server.■ Configurazione sconosciuta/eliminata Gli agenti non possono indicare quale configurazione è installata oppure la configurazione sull'agente è stata eliminata da Endpoint Server.	Endpoint
Risposta agente	Filtra gli incidenti in base alla risposta dell'agente all'incidente.	Endpoint

Nome	Descrizione	Prodotti interessati
Nome applicazione	Filtra gli incidenti in base al nome dell'applicazione in cui l'incidente è stato generato.	Endpoint
Titolo finestra applicazione	Filtra gli incidenti in base a una stringa nel titolo della finestra in cui l'incidente è stato generato.	Endpoint
Nome file allegato	Filtra gli incidenti in base al nome di file dell'allegato associato all'incidente.	Rete
Dimensioni file allegato	Filtra gli incidenti in base alla dimensione dell'allegato associato all'incidente.	Rete
Box: collaboratore	Filtra gli incidenti in base ai collaboratori Box.	Discover
Box: ruolo collaboratore	Filtra gli incidenti in base al ruolo del collaboratore Box. I ruoli includono: <ul style="list-style-type: none"> ■ Comproprietario ■ Editor ■ Visualizzatore anteprima ■ Caricamento visualizzatore anteprima ■ Caricamento ■ Visualizzatore ■ Caricamento visualizzatore 	Discover
Box: collegamento condiviso	Filtra gli incidenti in base alla presenza o meno di un collegamento condiviso.	Discover
Box: download collegamento condiviso consentito	Filtra gli incidenti in base alla presenza o meno di un collegamento condiviso che consente i download.	Discover
Box: data di scadenza collegamento condiviso	Filtra gli incidenti in base alla data di scadenza di un collegamento condiviso.	Discover
Box: password collegamento condiviso protetta	Filtra gli incidenti in base alla presenza o meno di un collegamento condiviso protetto da password.	Discover
Radice di contenuti	Filtra gli incidenti in base al percorso della radice di contenuti.	Discover

Nome	Descrizione	Prodotti interessati
Indirizzo e-mail proprietario dati	L'indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente o con un plug-in di ricerca.	Rete Endpoint Discover
Nome proprietario dati	La persona responsabile della risoluzione dell'incidente. Questo campo deve essere impostato manualmente o con un plug-in di ricerca. I report possono essere inviati automaticamente al proprietario dei dati per la risoluzione.	Rete Endpoint Discover
IP di destinazione	Filtra gli incidenti in base all'indirizzo IP di destinazione per il messaggio che ha generato l'incidente.	Rete Endpoint
Data rilevamento	Filtra gli incidenti in base alla data in cui l'incidente è stato rilevato.	Discover
ID istanza dispositivo	Riepiloga gli incidenti in base al dispositivo che ha creato la violazione.	Endpoint
Nome documento	Filtra gli incidenti in base al nome del documento con la violazione.	Discover
Dominio	Filtra gli incidenti in base al nome di dominio associato all'incidente.	Rete
Posizione endpoint	Filtra gli incidenti in base alla posizione dell'endpoint. La posizione può essere una delle seguenti: <ul style="list-style-type: none"> ■ All'interno della rete aziendale ■ All'esterno della rete aziendale 	Endpoint
Data ultima modifica file	Filtra gli incidenti in base alla data dell'ultima modifica del file.	Endpoint Discover
Posizione file	Filtra gli incidenti in base alla posizione del file con la violazione.	Endpoint

Nome	Descrizione	Prodotti interessati
Nome file	Filtra gli incidenti in base al nome del file con la violazione. L'uso di caratteri jolly non è consentito, ma è possibile specificare una corrispondenza parziale, ad esempio <code>.pdf</code> .	Endpoint Discover
Proprietario file	Filtra gli incidenti in base al proprietario dei file con la violazione.	Discover
Dimensione del file	Filtra gli incidenti in base alla dimensione del file con la violazione.	Endpoint Discover
Emittente cronologia incidenti	Filtra gli incidenti in base all'utente responsabile dell'emissione della cronologia dell'incidente.	Rete Endpoint Discover
ID incidente	Filtra gli incidenti in base all'ID degli incidenti.	Rete Endpoint Discover
Numero corrispondenza incidenti	Filtra gli incidenti in base al numero di corrispondenze incidente.	Rete Endpoint Discover
Note incidente	Filtra gli incidenti in base a una stringa nelle note dell'incidente.	Rete Endpoint Discover
Incidente segnalato il	Filtra gli incidenti in base alla data in cui l'incidente è stato segnalato.	Endpoint
Stato analisi	Filtra gli agenti in base allo stato dell'analisi. È possibile selezionare una delle seguenti opzioni: <ul style="list-style-type: none"> ■ Analisi in corso ■ Nessuna analisi in corso 	Discover Endpoint

Nome	Descrizione	Prodotti interessati
È nascosto	<p>Filtra gli incidenti nascosti. È possibile selezionare una delle seguenti opzioni:</p> <ul style="list-style-type: none"> ■ Mostra tutto ■ Mostra elementi nascosti <p>Vedere "Informazioni su come nascondere gli incidenti" a pagina 1696.</p>	<p>Rete</p> <p>Endpoint</p> <p>Discover</p>
Può essere nascosto	<p>Filtra gli incidenti in base allo stato del flag Può essere nascosto. Selezionare l'operatore È uno qualsiasi dei seguenti valori nel secondo campo, quindi selezionare l'opzione Consenti nascondi o Non nascondere nel terzo campo.</p> <p>Vedere "Informazioni su come nascondere gli incidenti" a pagina 1696.</p>	<p>Rete</p> <p>Endpoint</p> <p>Discover</p>
Ora ultima connessione	Filtra gli agenti in base all'ultima connessione di ogni agente a Endpoint Server.	Endpoint
Posizione	Filtra gli incidenti in base alla relativa posizione. La posizione può includere il server in cui gli incidenti sono stati generati.	Discover
IP computer (aziendale)	Filtra gli incidenti in base all'indirizzo IP del computer in cui gli incidenti sono stati creati.	Endpoint
Nome computer	Filtra gli incidenti in base al nome del computer in cui gli incidenti sono stati creati.	Endpoint
Azione Network Prevent	Filtra gli incidenti in base all'azione di Network Prevent.	Rete
Politica	Filtra gli incidenti in base alla politica da cui sono stati creati.	<p>Rete</p> <p>Endpoint</p> <p>Discover</p>
Gruppo di politiche	Filtra gli incidenti in base al gruppo di politiche a cui appartengono.	<p>Rete</p> <p>Endpoint</p> <p>Discover</p>

Nome	Descrizione	Prodotti interessati
Regola politica	Filtra gli incidenti in base alla regola di politica che ha generato gli incidenti.	Rete Endpoint Discover
Stato della protezione	Filtra gli incidenti in base allo stato di Network Protect degli incidenti.	Discover
Protocollo	Filtra gli incidenti in base al protocollo a cui appartengono.	Rete
Destinazione endpoint o protocollo	Filtra gli incidenti in base alla destinazione endpoint o al protocollo che ha generato l'incidente.	Endpoint
Leggi ACL: file	Filtra gli incidenti in base all'elenco di controllo di accesso dei file.	Endpoint Discover
Leggi ACL: condivisione	Filtra gli incidenti in base all'elenco di controllo di accesso delle condivisioni.	Discover
Destinatario	Filtra gli incidenti in base al nome del destinatario del messaggio che ha generato l'incidente.	Rete Endpoint Discover
Stato rilevamento riparazione	Filtra gli incidenti in base allo stato di rilevamento riparazione.	Discover
Computer sottoposto a scansione	Filtra gli incidenti in base ai computer sottoposti a scansione.	Discover
Rilevato in precedenza	Filtra gli incidenti in base all'esistenza di un precedente incidente correlato.	Per Discover, ma non per gli incidenti Database SQL (dove Rilevato in precedenza è sempre falso)
Mittente	Filtra gli incidenti per mittente.	Rete Endpoint Discover

Nome	Descrizione	Prodotti interessati
Server o rilevatore	Filtra gli incidenti in base al server in cui sono stati creati.	Rete Endpoint Discover
SharePoint ACL: livello autorizzazione	Filtra gli incidenti in base al livello di autorizzazione dell'elenco di controllo di accesso SharePoint.	Discover
SharePoint ACL: utente/gruppo	Filtra gli incidenti in base all'utente o al gruppo nell'elenco di controllo di accesso SharePoint.	Discover
IP origine	Filtra gli incidenti in base all'indirizzo IP di origine da cui sono stati creati.	Rete
Oggetto	Filtra gli incidenti in base all'oggetto del messaggio che ha generato l'incidente.	Rete Discover
Sostituito	Filtra gli incidenti in base alle risposte agli incidenti sostituite da altre risposte.	Discover Endpoint
Tipo di target	Filtra gli incidenti in base al tipo di target associato agli incidenti.	Discover
Tempo trascorso dal primo rilevamento	Filtra gli incidenti in base al periodo di tempo trascorso dal momento in cui l'incidente è stato rilevato per la prima volta.	Per Discover, ma non per gli incidenti Database SQL
URL	Filtra gli incidenti in base all'URL in cui si sono verificate le violazioni.	Discover
Giustificazione utente	Filtra gli incidenti in base alla giustificazione specificata dall'utente.	Endpoint
Nome utente	Filtra gli incidenti in base all'utente che ha generato l'incidente.	Endpoint

Il secondo campo nei filtri avanzati consente di selezionare il tipo di corrispondenza nel filtro.

Tabella 51-9 Filtri avanzati, secondo campo

Nome	Descrizione
Contiene uno qualsiasi dei seguenti valori	Consente di modificare il filtro per includere una qualsiasi parola nella stringa di testo o di scegliere da un elenco nel terzo campo.

Nome	Descrizione
Contiene Ignora maiuscole/minuscole	Consente di modificare il filtro per ignorare una specifica stringa di testo.
Non contiene Ignora maiuscole/minuscole	Consente di modificare il filtro per escludere la stringa di testo ignorata.
Non corrisponde esattamente	Consente di modificare il filtro per la corrispondenza con qualsiasi combinazione della stringa di testo.
Termina con Ignora maiuscole/minuscole	Consente di modificare il filtro in modo da visualizzare solo gli incidenti che terminano con la stringa di testo ignorata.
È uno qualsiasi dei seguenti valori	Consente di modificare il filtro di modo che i risultati includano qualsiasi parola della stringa di testo o di scegliere da un elenco nel terzo campo.
È compreso tra	Consente di modificare il filtro di modo che i risultati numerici rientrino tra un intervallo di numeri specificati.
È maggiore di	Consente di modificare il filtro di modo che i risultati numerici siano maggiori di un numero specificato.
È minore di	Consente di modificare il filtro di modo che i risultati numerici siano minori di un numero specificato.
Non è alcuno dei seguenti valori	Consente di modificare il filtro di modo che i risultati non includano alcuna delle parole della stringa di testo o di scegliere da un elenco nel terzo campo.
Non assegnato	Consente di modificare il filtro per restituire incidenti il cui valore specificato nel primo campo è Non assegnato.
Corrisponde esattamente	Consente di modificare il filtro per una corrispondenza esatta con la stringa di testo.
Corrisponde esattamente a Ignora maiuscole/minuscole	Consente di modificare il filtro di modo che debba corrispondere esattamente con la stringa di testo ignorata.
Inizia con Ignora maiuscole/minuscole	Consente di modificare il filtro in modo da visualizzare solo gli incidenti che iniziano con la stringa di testo ignorata.

Il terzo campo nei filtri avanzati consente di selezionare da un elenco di elementi oppure fornisce una casella vuota in cui digitare una stringa.

Questo terzo campo varia a seconda delle selezioni nel primo e nel secondo campo.

Per un elenco di elementi, premere MAIUSC e fare clic per selezionare molteplici elementi.

Per le stringhe, i caratteri jolly non sono consentiti, ma è possibile immettere una stringa parziale.

Ad esempio, è possibile immettere `.pdf` per selezionare qualsiasi file PDF.

Se non si sa quale testo digitare, usare le opzioni di riepilogo per visualizzare l'elenco di possibili valori di testo. È inoltre possibile consultare un riepilogo del numero di incidenti in ogni categoria.

Vedere ["Opzioni di riepilogo per i report di incidente"](#) a pagina 1682.

[Tabella 51-10](#) elenca alcune delle opzioni nel terzo campo.

Tabella 51-10 Filtri avanzati, terzo campo

Nome	Descrizione
Bloccata	All'utente viene impedito di eseguire l'azione che ha causato l'incidente.
Azione crittografata	Un utente gestito ha cercato di copiare o spostare un file riservato tramite un canale supportato e il file è stato crittografato automaticamente.
Azione crittografata bloccata	L'azione di un utente è stata bloccata e un file è stato crittografato in quanto un utente non gestito ha tentato di copiarlo o spostarlo utilizzando un canale supportato, oppure perché un utente gestito ha cercato di copiare o spostare il file utilizzando un canale non supportato.
Contenuto rimosso	Il contenuto nella violazione è stato rimosso.
Nessuna riparazione	Per l'incidente in questione non è stata eseguita alcuna riparazione.
Nessuna	Nessuna azione è stata intrapresa in relazione alla violazione che ha causato l'incidente.
File di protezione copiato	Il file nella violazione è stato copiato in un'altra posizione.
File di protezione in quarantena	Il file nella violazione è stato messo in quarantena in un'altra posizione.
Utente notificato	L'utente è stato avvisato della violazione verificatasi.

Come nascondere incidenti

Il capitolo contiene i seguenti argomenti:

- [Informazioni su come nascondere gli incidenti](#)
- [Come nascondere gli incidenti](#)
- [Visualizzazione di incidenti nascosti](#)
- [Come impedire che gli incidenti vengano nascosti](#)
- [Eliminazione degli incidenti nascosti](#)

Informazioni su come nascondere gli incidenti

Se si nascondono gli incidenti, è possibile contrassegnare gli incidenti specificati come "nascosti". Poiché questi incidenti nascosti sono esclusi dal reporting di incidenti normale, per migliorare le prestazioni del reporting della distribuzione di Symantec Data Loss Prevention, è possibile nascondere eventuali incidenti che non sono più pertinenti. Gli incidenti nascosti rimangono nel database. Non vengono spostati in un'altra tabella, un altro database o un altro tipo di archiviazione non in linea.

È possibile impostare i filtri per i report di incidenti nella console di amministrazione di Enforce Server per visualizzare solo gli incidenti nascosti o per visualizzare gli incidenti nascosti e non nascosti. Con questi report è possibile contrassegnare uno o più incidenti come nascosti mediante le opzioni **Nascondi/Visualizza**, disponibili quando si selezionano uno o più incidenti, e fare clic sul pulsante **Azioni incidente**. Di seguito sono riportate le opzioni disponibili per **Nascondi/Visualizza** :

- **Nascondi incidenti** - Contrassegna gli incidenti selezionati come nascosti.
- **Visualizza incidenti** : ripristina la visualizzazione degli incidenti selezionati.
- **Non nascondere** : impedisce che gli incidenti selezionati vengano nascosti.
- **Consenti nascondi** - Consente di nascondere gli incidenti selezionati.

Lo stato nascosto di un incidente appare nella schermata dell'istantanea dell'incidente, nella console di amministrazione di Enforce Server. La scheda **Cronologia** dell'istantanea dell'incidente include una voce per ogni volta in cui i flag **Non nascondere** o **Consenti nascondi** vengono impostati per l'incidente.

Vedere ["Report di filtraggio"](#) a pagina 1648.

L'accesso alla funzionalità per nascondere è controllato dai ruoli. È possibile impostare i privilegi dell'utente seguenti affinché un ruolo controlli l'accesso:

- **Nascondi incidenti** - Concede l'autorizzazione a un utente di nascondere gli incidenti.
- **Visualizza incidenti** - Concede l'autorizzazione a un utente di visualizzare gli incidenti nascosti.
- **Ripara incidenti (stato, gravità, proprietario dati, commenti, regole di risposta, posizione riparazione, stato riparazione)** - Concede l'autorizzazione a un utente di impostare i flag **Non nascondere** o **Consenti nascondi**.

Vedere ["Informazioni sul controllo degli accessi basato sul ruolo"](#) a pagina 109.

Vedere ["Come nascondere gli incidenti"](#) a pagina 1697.

Vedere ["Visualizzazione di incidenti nascosti"](#) a pagina 1697.

Vedere ["Come impedire che gli incidenti vengano nascosti"](#) a pagina 1698.

Come nascondere gli incidenti

Per nascondere gli incidenti

- 1 Aprire la console di amministrazione di Enforce Server e selezionare il report di un incidente.
- 2 Selezionare gli incidenti che si desidera nascondere manualmente o impostando i filtri o i filtri avanzati per visualizzare il set di incidenti da nascondere.
- 3 Fare clic sul pulsante **Azioni incidente** e selezionare **Nascondi/Visualizza > Nascondi incidenti**.

Gli incidenti selezionati vengono nascosti.

Visualizzazione di incidenti nascosti

Per ripristinare gli incidenti nascosti

- 1 Aprire la console di amministrazione di Enforce Server e accedere a un report di incidente.
- 2 Selezionare il collegamento **Filtri avanzati e riepilogo**.
- 3 Fare clic sul pulsante **Aggiungi filtro**.

- 4 Selezionare **È nascosto** nel primo elenco a discesa.
- 5 Selezionare **Mostra elementi nascosti** nel secondo elenco a discesa.
- 6 Selezionare gli incidenti che si desidera tornare a visualizzare, manualmente o impostando filtri o filtri avanzati per restituire il set di incidenti da tornare a visualizzare.
Gli incidenti selezionati vengono nuovamente visualizzati.

Come impedire che gli incidenti vengano nascosti

È possibile impedire che gli incidenti vengano nascosti utilizzando un report di incidente o un'istantanea incidente.

Per impedire che gli incidenti vengano nascosti utilizzando un report di incidente

- 1 Aprire la console di amministrazione di Enforce Server e accedere a un report di incidente.
- 2 Selezionare gli incidenti che si desidera non vengano nascosti. È possibile selezionare gli incidenti manualmente o impostando filtri o filtri avanzati per restituire il set degli incidenti che si desidera non vengano nascosti.
- 3 Fare clic sul pulsante **Azioni incidente** e selezionare **Nascondi/Visualizza > Non nascondere**.

Gli incidenti selezionati non potranno essere nascosti.

Nota: È possibile tornare a consentire che tali incidenti vengano nascosti selezionando gli incidenti e scegliendo **Nascondi/Visualizza > Consenti nascosti** a partire dal pulsante **Azioni incidente**.

Per impedire che gli incidenti vengano nascosti utilizzando un'istantanea incidente

- 1 Aprire la console di amministrazione di Enforce Server e accedere a un report di incidente.
- 2 Fare clic su un incidente per aprire l'istantanea incidente.
- 3 Nella scheda **Informazioni chiave**, nella sezione **Dettagli incidente** fare clic su **Non nascondere**.

Nota: Per tornare a consentire che un incidente venga nascosto, aprire l'istantanea incidente e fare clic su **Consenti nascosti** nella sezione **Dettagli incidente**.

Eliminazione degli incidenti nascosti

Per eliminare gli incidenti nascosti

- 1 Aprire la console di amministrazione di Enforce Server e selezionare il report di un incidente.
- 2 Fare clic sul collegamento **Filtri avanzati e riepilogo**.
- 3 Fare clic su **Aggiungi filtro**.
- 4 Selezionare **È nascosto** dal primo elenco a discesa.
- 5 Selezionare **Mostra elementi nascosti** dal secondo elenco a discesa.
- 6 Selezionare gli incidenti che si desidera eliminare. È possibile selezionare gli incidenti manualmente o impostare filtri o filtri avanzati che restituiscono il set di incidenti da eliminare.
- 7 Fare clic sul pulsante **Azioni incidente** e selezionare **Elimina incidenti**.
- 8 Selezionare una delle opzioni di eliminazione riportate di seguito:

Elimina incidente completamente	Elimina in modo permanente gli incidenti e tutti i dati associati (ad esempio, eventuali e-mail e allegati). Si tenga presente che non è possibile recuperare gli incidenti che sono stati eliminati.
Mantieni incidente ma elimina dati messaggio	Mantiene gli incidenti effettivi, ma elimina la copia di Symantec Data Loss Prevention dei dati che hanno generato gli incidenti. È possibile eliminare solo determinate parti dei dati associati. Il resto dei dati viene conservato.
Elimina messaggio originale	Elimina il contenuto del messaggio (ad esempio, il messaggio e-mail o il post HTML). Questa opzione si applica solo agli incidenti di rete.
Elimina allegati/file	<p>Questa opzione fa riferimento ai file (per gli incidenti endpoint e di rilevazione) o agli allegati di e-mail o di post (per gli incidenti di rete). Le opzioni sono Tutti, che elimina tutti gli allegati, e Allegati senza violazioni. Ad esempio scegliere questa opzione per eliminare i file (per gli incidenti endpoint e di rilevazione) o gli allegati di e-mail (per gli incidenti di rete).</p> <p>Questa opzione elimina solo gli allegati in cui Symantec Data Loss Prevention non ha trovato alcuna corrispondenza. Ad esempio scegliere questa opzione quando vi sono incidenti con singoli file estratti da un file compresso (incidenti endpoint e di rilevazione) o diversi allegati di e-mail (incidenti di rete).</p>

- 9 Fare clic sul pulsante **Elimina**.

Utilizzo di dati di incidente

Il capitolo contiene i seguenti argomenti:

- Informazioni sugli attributi di stato incidente.
- Configurazione di attributi e valori di stato
- Configurazione di gruppi di stati
- Esporta archivio Web
- Esporta archivio Web - Crea archivio
- Esporta archivio Web - Tutti gli eventi recenti
- Informazioni sugli attributi personalizzati
- Informazioni sull'uso di attributi personalizzati
- Metodi di inserimento di attributi personalizzati
- Configurazione di attributi personalizzati
- Impostazione di attributi personalizzati
- Impostazione manuale dei valori degli attributi personalizzati

Informazioni sugli attributi di stato incidente.

Gli attributi di stato incidente sono specificati e configurati nella schermata **Attributi** (**Sistema** > **Dati incidente** > **Attributi**).

Qualsiasi attributo di stato elencato in questa schermata può essere assegnato a qualunque incidente selezionandolo dal menu a discesa **Stato** dell'istantanea incidente.

La pagina degli attributi di sistema contiene i seguenti attributi per la riparazione degli incidenti:

- **Valori stati**

La sezione **Valori stati** elenca gli attributi di stato incidente correnti assegnabili a un determinato incidente. Utilizzare questa sezione per creare nuovi attributi di stato, modificarli e cambiarne l'ordine di visualizzazione nei menu a discesa.

Vedere ["Configurazione di attributi e valori di stato"](#) a pagina 1702.

- **Gruppi stati**

La sezione **Gruppi stati** elenca i gruppi di stati incidente correnti e la relativa composizione. Utilizzare questa sezione per creare nuovi gruppi di stati, modificarli e cambiarne l'ordine di visualizzazione nei menu a discesa.

Vedere ["Configurazione di gruppi di stati"](#) a pagina 1703.

- **Attributi personalizzati nella scheda Attributi personalizzati**

La scheda **Attributi personalizzati** fornisce un elenco di tutti gli attributi incidente personalizzati attualmente definiti. Gli attributi personalizzati forniscono informazioni sull'incidente o associate all'incidente. Ad esempio, l'indirizzo e-mail della persona che ha causato l'incidente, il responsabile di quella persona, il motivo per cui l'incidente è stato ignorato e così via. Utilizzare questa scheda per aggiungere, configurare, eliminare e ordinare gli attributi incidente personalizzati.

Vedere ["Informazioni sugli attributi personalizzati"](#) a pagina 1706.

Il processo per la gestione degli incidenti comprende varie fasi dal rilevamento alla risoluzione. Ogni fase è identificata da un attributo di stato differente come "Nuovo", "Analisi", "Riassegnato" e "Risolto". Ciò consente di seguire l'avanzamento dell'incidente nel flusso di lavoro e di filtrare elenchi e report per stato incidente.

Il pacchetto di soluzioni installato insieme a Symantec Data Loss Prevention fornisce un set iniziale di attributi di stato e di gruppi di attributi di stato. È possibile creare nuovi attributi di stato o modificare quelli esistenti. I valori di attributi di stato e i gruppi di stati utilizzati devono essere basati sul flusso di lavoro che l'organizzazione utilizza per elaborare gli incidenti. Ad esempio, si potrebbe assegnare a tutti i nuovi incidenti lo stato "Nuovo". Successivamente, si potrebbe cambiare lo stato ad "Assegnato", "Analisi" o "Riassegnato". Alla fine, la maggior parte degli incidenti avranno lo stato "Risolto" o "Ignorato".

È anche possibile creare gruppi di stati per il filtraggio di elenchi e report.

In base alle preferenze dell'organizzazione e alla terminologia comunemente utilizzata nel settore in questione, è possibile:

- Personalizzare i nomi degli attributi di stato e aggiungere nuovi attributi di stato.
- Personalizzare i nomi dei gruppi di stati e aggiungere nuovi gruppi di stati.
- Impostare l'ordine in cui gli attributi di stato sono visualizzati nell'elenco a discesa **Stato** di un incidente.
- Specificare l'attributo di stato predefinito che viene assegnato automaticamente ai nuovi incidenti.

Vedere ["Configurazione di attributi e valori di stato"](#) a pagina 1702.

Vedere ["Informazioni sui report degli incidenti"](#) a pagina 1635.

Vedere ["Informazioni sulla riparazione degli incidenti"](#) a pagina 1570.

Vedere ["Informazioni sugli attributi personalizzati"](#) a pagina 1706.

Configurazione di attributi e valori di stato

Quando gli incidenti sono elaborati dal rilevamento alla risoluzione, ogni fase può essere contrassegnata con uno stato differente. Lo stato consente di seguire l'avanzamento dell'incidente nel flusso di lavoro. In base alle preferenze dell'organizzazione e alla terminologia comunemente utilizzata nel settore in questione, è possibile definire i differenti stati che si desidera utilizzare per tenere traccia del flusso di lavoro.

La sezione **Valori stati** elenca gli attributi di stato disponibili che possono essere assegnati a un incidente. L'ordine in cui gli attributi di stato sono visualizzati nell'elenco determina l'ordine in cui compaiono nei menu a discesa usati per impostare lo stato di un incidente. È possibile effettuare le seguenti azioni dalla sezione **Valori stati** :

Azione	Procedura
Creare un nuovo attributo di stato incidente.	Fare clic sul pulsante Aggiungi .
Eliminare un attributo di stato incidente.	Fare clic sulla X rossa dell'attributo e confermare la decisione.
Modificare un attributo di stato incidente.	Fare clic sull'attributo che si desidera modificare, immettere un nuovo nome e fare clic su Salva . Per modificare il nome di uno stato esistente, fare clic sull'icona con la matita di quello stato, immettere il nuovo nome e fare clic su Salva .
Impostare un attributo di stato incidente come predefinito.	Fare clic su [imposta come predefinito] accanto all'attributo per impostarlo come stato predefinito per tutti i nuovi incidenti.
Modificare l'ordine di un attributo di stato incidente nei menu a discesa.	<ul style="list-style-type: none"> ■ Fare clic su [su] per spostare un attributo verso l'alto. ■ Fare clic su [giù] per spostare un attributo verso il basso.

Per creare un nuovo attributo di stato incidente

- 1 Accedere alla schermata **Attributi** (**Sistema > Dati incidente > Attributi**).
Fare clic sulla scheda **Stato**.
- 2 Fare clic sul pulsante **Aggiungi** nella sezione **Valori stati**.
- 3 Inserire un nome per il nuovo attributo di stato.
- 4 Fare clic su **Salva**.

Vedere ["Configurazione di gruppi di stati"](#) a pagina 1703.

Vedere ["Informazioni sugli attributi di stato incidente."](#) a pagina 1700.

Configurazione di gruppi di stati

Gli attributi di stato relativi agli incidenti possono essere assegnati a gruppi di stati che corrispondono al flusso di lavoro dell'organizzazione. Ad esempio, un gruppo di stato **Apri** potrebbe includere gli attributi di stato **Nuovo**, **Analisi in corso** e **Riassegnato**. È quindi possibile filtrare i report e gli elenchi di incidenti in base al relativo gruppo di stati. Ad esempio, è possibile elencare tutti gli incidenti con gli attributi di stato che appartengono al gruppo di stati **Apri**.

Selezionare **Sistema > Dati incidente > Attributi** per accedere all'opzione **Gruppi stati**.

Per convenienza, è possibile raggruppare gli stati di incidente in base al flusso di lavoro della organizzazione. **Gruppi stati** consente di aggiungere o modificare il nome di un gruppo di stati e specificare quali valori includere nel gruppo.

La sezione **Gruppi stati** elenca i gruppi di stati di incidente disponibili per filtrare gli incidenti. Per ogni gruppo, sono elencati gli attributi di stato inclusi nel gruppo. È possibile effettuare le seguenti azioni dalla sezione **Valori stati** :

Azione	Procedura
Creare un nuovo gruppi di stati di incidente.	Fare clic sul pulsante Aggiungi gruppo stati .
Eliminare un gruppo di stati di incidente.	Fare clic sulla X rossa del gruppo e confermare la decisione.
Modificare gli attributi di stato di incidente o il nome di un gruppo.	Fare clic sul gruppo che si desidera modificare. Fare clic sull'icona a forma di matita. Modificare il nome, selezionare o deselezionare gli attributi e fare clic su Salva .
Cambiare l'ordine di un gruppo di stati nel menu a discesa.	<ul style="list-style-type: none">■ Fare clic su [su] per spostare un gruppo verso l'alto.■ Fare clic su [giù] per spostare un gruppo verso il basso.

Per definire un nuovo gruppo di stati

- 1 Accedere alla schermata **Attributi** (**Sistema > Dati incidente > Attributi**).
Fare clic sulla scheda **Stato**.
- 2 Fare clic sul pulsante **Aggiungi gruppo stati** nella sezione **Gruppi stati**.
- 3 Immettere un nome per il nuovo gruppo di stati.

- 4 Fare clic sulle caselle di controllo per gli attributi di stato che si desidera includere in questo gruppo.

Gli attributi di stato sono definiti con il pulsante **Aggiungi** nella sezione **Valori stati**.

Vedere ["Configurazione di attributi e valori di stato"](#) a pagina 1702.

- 5 Fare clic su **Salva**.

Vedere ["Configurazione di attributi e valori di stato"](#) a pagina 1702.

Vedere ["Informazioni sugli attributi di stato incidente."](#) a pagina 1700.

Esporta archivio Web

Utilizzare questa schermata per salvare un report Elenco incidenti come archivio di pagine HTML. Un archivio consente al personale senza accesso diretto a Symantec Data Loss Prevention di analizzare dati di incidenti, visualizzando le informazioni dettagliate necessarie su singoli incidenti.

Quando si esportano incidenti come un Archivio Web, l'archivio viene posizionato nella directory
\\Program Files\\Symantec\\Data Loss Prevention\\Enforce
Server\\15.1\\Protect\\archive\\webarchive.

Nota: Non è possibile archiviare report riepilogativi o dashboard.

Quando si esportano incidenti, considerare quanto segue:

- Un archivio non può essere riepilogato come un report normale.
- Un archivio non contiene filtri, può quindi essere difficile individuare uno specifico incidente in un archivio che contiene moltissimi incidenti.
- L'esportazione di un archivio di incidenti non rimuove gli incidenti dalla console di amministrazione.
- È possibile esportare un solo archivio alla volta.

Esporta archivio Web è un privilegio utente che deve essere assegnato a un ruolo. È possibile esportare archivi Web solo se il ruolo consente l'uso di questa funzionalità. Poiché l'accesso del ruolo determina anche quali informazioni sono contenute nei report incidente, si applica anche all'archiviazione di quei report incidente. Le informazioni contenute nell'archivio creato sono le stesse presenti nel report incidente originale.

Vedere ["Informazioni sulla configurazione di ruoli e utenti"](#) a pagina 110.

La schermata Esporta archivio Web include due sezioni:

Vedere ["Esporta archivio Web - Crea archivio"](#) a pagina 1705.

Vedere ["Esporta archivio Web - Tutti gli eventi recenti"](#) a pagina 1706.

Esporta archivio Web - Crea archivio

Nella sezione **Crea archivio**, completare le seguenti informazioni:

Campo	Descrizione
Nome archivio	Specificare un nome per l'archivio che si sta creando utilizzando le normali convenzioni di denominazione di Windows.
Report da esportare	<p>Dall'elenco a discesa, selezionare il report da archiviare. Tutti i report creati sono disponibili insieme alle opzioni per report predefinite.</p> <p>Le opzioni di Rete sono:</p> <ul style="list-style-type: none"> ■ Incidenti - Settimana corrente - Gli incidenti di rete nella settimana corrente. ■ Incidenti - Tutti - Tutti gli incidenti di rete. ■ Incidenti - Nuovo - Gli incidenti di rete con stato Nuovo. <p>Le opzioni di Endpoint sono:</p> <ul style="list-style-type: none"> ■ Incidenti - Settimana corrente - Gli incidenti Endpoint nella settimana corrente. ■ Incidenti - Tutti - Tutti gli incidenti endpoint. ■ Incidenti - Nuovo - Solo gli incidenti Endpoint con stato Nuovo. <p>Le opzioni di Discover sono:</p> <ul style="list-style-type: none"> ■ Incidenti - Ultima scansione - Gli incidenti di Discover nell'ultima scansione (gli incidenti di una scansione ancora attiva non sono inclusi). ■ Incidenti - Scansione in corso - Gli incidenti di Discover nella scansione corrente. ■ Incidenti - Tutte le scansioni - Tutti gli incidenti di Discover. ■ Incidenti - Nuovo - Gli incidenti di Discover con stato Nuovo.

Dopo avere completato i campi, fare clic su **Crea** per compilare l'archivio.

Vedere ["Esporta archivio Web"](#) a pagina 1704.

Esporta archivio Web - Tutti gli eventi recenti

La sezione **Tutti gli eventi recenti** visualizza un elenco degli eventi relativi a questo archivio. L'elenco compare solo dopo aver fatto clic su **Crea** per creare l'archivio. Le voci dell'evento mostrano le seguenti informazioni:

- Il tipo di evento (Errore, Avviso o Informazioni di sistema).
- La data e l'ora dell'evento
- Una breve descrizione dell'evento.

Per consultare i dettagli di ogni evento, fare clic sulla voce dell'evento nell'elenco. Per consultare l'intero report sugli eventi per questo archivio, fare clic su **Mostra tutto**.

Vedere "[Esporta archivio Web](#)" a pagina 1704.

Informazioni sugli attributi personalizzati

Gli attributi personalizzati sono campi di dati di incidente che forniscono un metodo per acquisire e archiviare informazioni supplementari sugli incidenti. I dati supplementari contenuti negli attributi personalizzati possono:

- Essere utilizzati per determinare il flusso di lavoro.
- Eseguire azioni di risposta agli incidenti
- Essere inclusi nelle metriche di reporting.
- Consentire ai team di risposta agli incidenti di agire più rapidamente.
- Consentire una maggiore automatizzazione di riparazioni e report.

Creare gli attributi personalizzati necessari a tali scopi. Gli attributi personalizzati forniscono informazioni su un incidente o associate a un incidente; ad esempio, l'indirizzo e-mail della persona che ha causato l'incidente, il responsabile di quella persona, il motivo per cui l'incidente è stato ignorato e così via.

La scheda **Attributi personalizzati** della schermata **Attributi** (**Sistema > Dati incidente > Attributi**) consente di gestire gli attributi personalizzati. La schermata **Attributi** include le seguenti schede:

- **Stato**. La scheda **Stato** fornisce un elenco di tutti gli attributi di stato incidente e di tutti i gruppi di attributi di stato correntemente definiti. Utilizzare questa scheda per aggiungere, configurare, eliminare e ordinare gli attributi e i gruppi di stato incidente.
Vedere "[Informazioni sugli attributi di stato incidente](#)." a pagina 1700.
- **Attributi personalizzati**. La scheda **Attributi personalizzati** fornisce un elenco di tutti gli attributi incidente personalizzati attualmente definiti. Utilizzare questa scheda per aggiungere, configurare, eliminare e ordinare gli attributi incidente personalizzati.

Il pacchetto di soluzioni installato insieme a Symantec Data Loss Prevention fornisce un set predefinito iniziale di attributi personalizzati. La scheda Attributi personalizzati fornisce un elenco di tutti gli attributi personalizzati attualmente definiti che possono essere applicati a qualsiasi incidente. Questa scheda consente di creare, modificare ed eliminare tutti gli attributi personalizzati per l'installazione. L'applicazione di uno qualsiasi di questi attributi personalizzati o valori di attributo a un singolo incidente si esegue nell'istantanea incidente o mediante un plug-in di ricerca.

Nella scheda **Attributi personalizzati**, è possibile eseguire le seguenti azioni:

Azione	Procedura
Creare un nuovo attributo personalizzato.	Fare clic sul pulsante Aggiungi .
Eliminare un attributo personalizzato.	Fare clic sulla X rossa dell'attributo e confermare la decisione. Tenere presente che non è possibile eliminare un attributo personalizzato attualmente assegnato a uno o più incidenti. È necessario assegnare un attributo differente agli incidenti in questione prima di poter eliminare l'attributo personalizzato.
Modificare nome, stato dell'e-mail e gruppo di attributi di un attributo.	Fare clic sull'attributo che si desidera modificare, modificarne i parametri e fare clic su Salva .
Cambiare l'ordine degli attributi nei menu a discesa.	1 Fare clic su [su] per spostare un attributo verso l'alto. 2 Fare clic su [giù] per spostare un attributo verso il basso.
Ricaricare i plug-in di ricerca	Fare clic su Ricarica plug-in di ricerca per ricaricare tutti i plug-in di ricerca di attributi personalizzati che sono stati scaricati dal sistema. Il ricaricamento del plug-in di ricerca riguarda tutti gli incidenti. È possibile che sia necessario ricaricare i plug-in di ricerca se una qualsiasi delle condizioni seguenti è vera: <ul style="list-style-type: none"> ■ Un plug-in presentava dei problemi e il sistema lo ha scaricato, ma ora il problema è risolto. ■ La rete non funzionava o era scollegata per lo stesso motivo, ma ora funziona correttamente. ■ Un plug-in archivia i dati in una cache e si desidera aggiornare la cache manualmente.

Vedere ["Informazioni sugli attributi di stato incidente."](#) a pagina 1700.

Vedere ["Configurazione di attributi personalizzati"](#) a pagina 1709.

Vedere ["Impostazione manuale dei valori degli attributi personalizzati"](#) a pagina 1710.

Informazioni sull'uso di attributi personalizzati

Quando si crea un incidente, Enforce Server recupera i dati relativi all'incidente. Alcuni di quei dati sono in forma di "attributi". Consultare il *Manuale dell'amministratore di Symantec Data Loss Prevention* per ulteriori informazioni sugli attributi di incidenti.

Gli attributi personalizzati sono utilizzati per acquisire e archiviare ulteriori dati. Tali dati sono relativi all'incidente, come il nome del responsabile o del reparto in questione. Creare solo gli attributi personalizzati necessari.

I dati supplementari contenuti negli attributi personalizzati possono essere utilizzati per:

- Iniziare un flusso di lavoro
- Eseguire azioni di risposta agli incidenti
- Essere inclusi nelle metriche di reporting
- Consentire ai team di risposta agli incidenti di agire più rapidamente
- Consentire una maggiore automatizzazione di riparazioni e report

Metodi di inserimento di attributi personalizzati

Per ogni incidente, è possibile inserire attributi personalizzati (i relativi valori possono essere impostati nei dati relativi all'incidente) nei seguenti modi:

- Automaticamente quando l'incidente viene rilevato mediante un plug-in di ricerca, come descritto in questa guida
- Automaticamente quando l'incidente viene rilevato mediante una regola di risposta automatica
- Automaticamente quando un utente esegue una regola di risposta smart
- Manualmente (mediante l'immissione di dati) da specifici utenti dopo il rilevamento

Gli attributi personalizzati possono essere anche reinseriti automaticamente facendo clic sull'opzione **Ricerca** nella sezione **Attributo** della schermata **Istantanea incidente**. Questa azione sostituisce i valori esistenti che vengono memorizzati nei campi degli attributi personalizzati con i valori restituiti dalla nuova ricerca.

Nota: Se la nuova ricerca restituisce valori null o vuoti per tutti i campi di attributo personalizzati, tali valori vuoti sovrascrivono i valori esistenti.

Configurazione di attributi personalizzati

Utilizzare la schermata **Configura attributo personalizzato** per aggiungere o modificare un attributo personalizzato.

Gli attributi personalizzati possono essere raggruppati in gruppi di attributi, come avviene per gli stati, allo scopo di organizzare le informazioni in modo utile. Esempi di gruppi di attributi comuni sono **Informazioni dipendente**, **Informazioni manager** e **Informazioni riparazione**. Tutti gli attributi personalizzati sono disponibili per tutti gli incidenti.

Per creare attributi personalizzati e aggiungerli a un gruppo

- 1 In Enforce Server, fare clic su **Sistema > Dati incidente > Attributi > Attributi personalizzati**. Tenere presente che un numero di attributi personalizzati sono stati definiti e caricati mediante il pacchetto di soluzioni selezionato durante l'installazione. Tutti gli attributi personalizzati esistenti sono elencati nella finestra **Attributi personalizzati**.
- 2 Per creare un nuovo attributo personalizzato, fare clic sull'opzione **Aggiungi**.
- 3 Digitare un nome per l'attributo personalizzato nella casella **Nome**. Se appropriato, selezionare la casella **È l'indirizzo e-mail**.

È possibile assegnare a un attributo personalizzato un nome qualsiasi. Ma la struttura dell'attributo personalizzato creato deve essere uguale a quella dell'origine dati esterna corrispondente. Ad esempio, si supponga che le informazioni su un reparto archiviate in un'origine esterna siano la posizione geografica e il nome del reparto. In questo caso, è necessario creare attributi personalizzati corrispondenti per la posizione e per il nome del reparto. Non è possibile creare un unico attributo personalizzato per l'ID del reparto che combina la posizione e il nome del reparto.

- 4 Selezionare un gruppo di attributi dall'elenco a discesa **Gruppo di attributi**. Se necessario, creare un nuovo gruppo di attributi. Selezionare **Crea nuovo gruppo di attributi** dall'elenco a discesa e digitare il nome del nuovo gruppo nella casella di testo visualizzata.
- 5 Fare clic su **Salva**.

Vedere ["Configurazione di attributi personalizzati"](#) a pagina 1709.

Vedere ["Informazioni sugli attributi di stato incidente."](#) a pagina 1700.

Vedere ["Configurazione di gruppi di stati"](#) a pagina 1703.

Vedere ["Configurazione di attributi e valori di stato"](#) a pagina 1702.

Impostazione di attributi personalizzati

Gli attributi personalizzati creati sono disponibili per ogni incidente. Ogni incidente riceve un set di attributi personalizzati (sebbene alcune coppie nome-valore possano essere vuote a

seconda delle circostanze). I valori degli attributi personalizzati per un incidente possono essere popolati e modificati indipendentemente da altri incidenti.

È possibile modificare i valori degli attributi personalizzati se il ruolo di cui si dispone include l'accesso in modifica per tali attributi. Se si desidera aggiornare un gruppo di incidenti, è possibile selezionare quegli incidenti nella pagina che elenca gli incidenti. Selezionare quindi il comando **Imposta attributi** nel menu **Azioni incidente**. È possibile selezionare **Attributi di ricerca** per cercare i valori degli attributi personalizzati. Tenere presente che il comando **Imposta attributi** e la sezione **Attributi** nella pagina **Istantanea incidente** sono disponibili solo se almeno un attributo personalizzato è definito.

Per impostare attributi personalizzati per gli incidenti

- 1 Nella pagina con l'elenco degli incidenti, selezionare l'incidente o gli incidenti per i quali si desidera impostare attributi personalizzati, quindi fare clic su **Azioni incidente > Imposta attributi**.

Viene visualizzata la pagina **Imposta attributi incidente**.

- 2 Selezionare gli attributi personalizzati che si desidera impostare per l'incidente o gli incidenti.
- 3 Fare clic su **Salva..**
- 4 Generare un nuovo incidente, o visualizzare un incidente esistente, e verificare che contenga il nuovo attributo personalizzato.

Vedere ["Configurazione di attributi personalizzati"](#) a pagina 1709.

Vedere ["Informazioni sugli attributi di stato incidente."](#) a pagina 1700.

Vedere ["Configurazione di attributi e valori di stato"](#) a pagina 1702.

Impostazione manuale dei valori degli attributi personalizzati

È possibile specificare manualmente lo stato di riparazione degli incidenti o l'avanzamento del flusso di lavoro con valori negli attributi personalizzati.

Nota: Per compilare automaticamente i valori degli attributi personalizzati, utilizzare uno o più plug-in di ricerca. Vedere ["Informazioni sui plug-in di ricerca"](#) a pagina 1727.

Per impostare il valore degli attributi personalizzati

- 1 Visualizzare l'istantanea di un incidente.
- 2 Fare clic sull'opzione **Modifica** nella sezione **Attributi** dell'istantanea incidente.

- 3 Per impostare un valore per un attributo personalizzato, immettere il valore nel campo appropriato degli attributi.
- 4 Una volta impostati i valori, fare clic su **Salva**.

Utilizzo del rischio dell'utente

Il capitolo contiene i seguenti argomenti:

- [Informazioni sui rischi utente](#)
- [Informazioni sulle origini dati dell'utente](#)
- [Informazioni sull'identificazione degli utenti in incidenti Web](#)
- [Visualizzazione dell'elenco utenti](#)
- [Visualizzazione dei dettagli dell'utente](#)
- [Utilizzo del riepilogo rischi utente](#)

Informazioni sui rischi utente

Il riepilogo rischi utente offre una visione del comportamento di singoli individui nell'organizzazione associando gli utenti a incidenti web, e-mail e di endpoint. Tali informazioni aiutano a concentrare gli sforzi di prevenzione della perdita di dati sugli utenti che comportano il rischio più elevato per la sicurezza dei dati.

La tabella [Tabella 54-1](#) fornisce una panoramica dei passaggi necessari per creare e gestire report di riepilogo dei rischi utente.

Tabella 54-1 Flusso di lavoro Riepilogo rischi utente

Passaggio	Azione	Descrizione
1	Creare attributi utente personalizzati	<p>È possibile creare attributi personalizzati per filtrare e gestire report di riepilogo dei rischi utente. Ad esempio, è possibile creare un attributo Stato lavorativo per seguire lo stato lavorativo di ciascun utente. È quindi possibile importare tali dati in un file che esportato dal sistema di pianificazione delle risorse aziendali, quale SAP.</p> <p>Vedere "Definizione di attributi personalizzati per i dati utente" a pagina 1715.</p>
2	Importazione dei dati utente	<p>È possibile importare i dati utente da un collegamento Active Directory o da un file CSV. Gli incidenti sono associati a utenti specifici mediante l'indirizzo e-mail e le credenziali di accesso. È anche possibile caricare file con gli attributi personalizzati, quali informazioni del sistema di pianificazione risorse dell'azienda. Symantec Data Loss Prevention fornisce un file modello CSV utilizzabile per formattare tutti i dati che si desidera caricare.</p> <p>Vedere "Importazione dei dati dell'utente" a pagina 1716.</p>
3	Configurare la risoluzione tra indirizzo IP e nome utente	<p>Symantec Data Loss Prevention è in grado di risolvere nomi utente dagli indirizzi IPv4 negli incidenti FTP e HTTP/S. L'agente del controller di dominio interroga gli eventi di Windows nel registro eventi di sicurezza di Microsoft Active Directory del controller di dominio. Symantec Data Loss Prevention associa tali eventi Windows ai dati utente del database.</p> <p>Vedere "Informazioni sull'identificazione degli utenti in incidenti Web" a pagina 1721.</p>
3	Visualizzare l' Elenco utenti .	<p>Elenco utenti è un elenco di tutti gli utenti del sistema, completo di indirizzi e-mail, dominio e nome di accesso.</p> <p>Vedere "Visualizzazione dell'elenco utenti" a pagina 1724.</p> <p>È possibile visualizzare i dettagli per utenti specifici nell'istantanea utente.</p> <p>Vedere "Visualizzazione dei dettagli dell'utente" a pagina 1724.</p>

Passaggio	Azione	Descrizione
4	Visualizzare Riepilogo rischi utente	<p>Riepilogo rischi utente visualizza gli utenti e i relativi incidenti di rete ed endpoint. Utilizzare Riepilogo rischi utente per eseguire il drill down nei dati incidente incentrati sull'utente e individuare gli utenti a maggior rischio. È possibile ordinare e filtrare questo elenco in base a politiche, attributi personalizzati, stato incidente, gravità dell'incidente, nome utente identificato dall'indirizzo IP, numero di incidenti, data, tipo di incidente e nome utente.</p> <p>Vedere "Utilizzo del riepilogo rischi utente" a pagina 1725.</p>
5	Esportare il riepilogo rischi utente o i dati di istantanea utente.	<p>È possibile esportare dati dal riepilogo rischi utente o dall'istantanea utente a un file CSV.</p> <p>Vedere "Utilizzo del riepilogo rischi utente" a pagina 1725.</p> <p>Vedere "Visualizzazione dei dettagli dell'utente" a pagina 1724.</p>

Mediante le informazioni fornite nel riepilogo rischi utente è possibile individuare gli utenti ad alto rischio e determinare le azioni da intraprendere. Tali azioni possono includere:

- Determinare se un utente rappresenta una minaccia attiva per la sicurezza dei dati.
- Applicare politiche supplementari per monitorare in maggior dettaglio lo stato di un utente.
- Applicare regole di risposta aggiuntive alle azioni di blocco o inviare avvisi.
- Segnalare lo stato di un utente al manager o a un altro responsabile.

Per lavorare con i dati dei rischi utente, un utente Symantec Data Loss Prevention deve disporre del privilegio **Reporting utente**. Tenere presente che gli utenti con questo privilegio possono visualizzare e accedere automaticamente a tutti gli incidenti e i tipi di incidente in Symantec Data Loss Prevention. Il riepilogo rischi utente è destinato a manager o responsabili della sicurezza delle informazioni di alto livello. Questo privilegio non fa parte di alcun ruolo predefinito.

Vedere ["Ruoli di configurazione"](#) a pagina 114.

Informazioni sulle origini dati dell'utente

È possibile importare i dati degli utenti in formato CSV o tramite una connessione di Active Directory.

I dati dell'utente sono informazioni sulle persone dell'organizzazione che possono avere accesso ai dati che si desidera proteggere. Per monitorare i rischi dell'utente, è necessario fornire il nome e il cognome dell'utente, l'indirizzo e-mail (per monitorare gli incidenti di rete) e le informazioni di accesso (per monitorare gli incidenti endpoint). È inoltre possibile fornire

altre informazioni sugli attributi di directory standard, ad esempio l'indirizzo e il numero di telefono dell'utente, nonché attributi personalizzati come lo stato di impiego dell'utente.

La [Tabella 54-2](#) elenca gli attributi dei dati dell'utente standard obbligatori e opzionali.

Tabella 54-2 Dati dell'utente standard

Attributo	Obbligatorio oppure opzionale	Descrizione
NOME	Obbligatorio	Nome dell'utente.
COGNOME	Obbligatorio	Cognome dell'utente.
E-MAIL	Obbligatorio se non sono incluse informazioni di accesso	Indirizzo e-mail dell'utente.
ACCESSO	Obbligatorio se non è incluso alcun indirizzo e-mail	Informazioni di accesso dell'utente nel formato DOMINIOACCESSO.
NUMERO DI TELEFONO	Opzionale	Numero di telefono dell'utente.
ID DIPENDENTE	Opzionale	Numero di identificazione del dipendente dell'utente.
TITOLO	Opzionale	Qualifica dell'utente.
REPARTO	Opzionale	Reparto in cui lavora l'utente.
INDIRIZZO	Opzionale	Indirizzo dell'utente.
PROVINCIA	Opzionale	Provincia in cui risiede l'utente.
PAESE	Opzionale	Paese in cui risiede l'utente.
CAP	Opzionale	CAP dell'indirizzo dell'utente.

Vedere ["Definizione di attributi personalizzati per i dati utente"](#) a pagina 1715.

Vedere ["Importazione dei dati dell'utente"](#) a pagina 1716.

Definizione di attributi personalizzati per i dati utente

È possibile creare attributi personalizzati per migliorare la rilevanza durante l'applicazione di filtri e la gestione di report di riepilogo dei rischi utente. Gli attributi personalizzati utili possono includere lo stato lavorativo, il nome del manager dell'utente, la mansione lavorativa e altre informazioni che potrebbero essere registrate nel sistema ERP o in un'altra origine dati.

È necessario creare attributi personalizzati prima di immettere i dati utente. A ogni attributo personalizzato è assegnato un numero di identificazione unico durante la creazione. È

necessario aggiungere questi numeri di identificazione attributo personalizzato al file di dati prima di importarlo in Symantec Data Loss Prevention.

Vedere ["Aggiunta di un'origine dati utente basata su file"](#) a pagina 1717.

Per definire attributi personalizzati per i dati utente

- 1 Nella console di amministrazione di Enforce Server accedere a **Sistema > Utenti > Attributi**.
- 2 Fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo **Attributo utente**.
- 3 Immettere l'attributo personalizzato nel campo **Nome**. L'attributo personalizzato può avere un massimo di 60 caratteri.
- 4 Fare clic su **Invia**.

Per visualizzare e modificare attributi personalizzati dell'utente

- 1 Nella console di amministrazione di Enforce Server accedere a **Sistema > Utenti > Attributi**.
- 2 Gli attributi personalizzati compaiono nell'elenco **Attributi personalizzati utente**. È possibile eseguire quanto segue:
 - Per filtrare l'elenco **Attributi personalizzati utente**, fare clic su **Filtri**, quindi usare i campi di testo **ID** o **Nome attributo** per immettere un valore di filtro.
 - Per modificare un attributo personalizzato, fare clic sul nome dell'attributo o sull'icona di modifica nella colonna **Azioni**, quindi modificare l'attributo nella finestra di dialogo **Attributo utente**.
 - Per eliminare un attributo personalizzato fare clic sull'icona di eliminazione nella colonna **Azioni**.

Importazione dei dati dell'utente

È possibile importare i dati dell'utente da un file o una connessione Active Directory.

Vedere ["Aggiunta di un'origine dati utente basata su file"](#) a pagina 1717.

Vedere ["Aggiunta di un'origine dati utente Active Directory"](#) a pagina 1718.

Dopo avere aggiunto le origini dati dell'utente, è possibile pianificare Symantec Data Loss Prevention per importare regolarmente i dati da quelle origini dati per garantire che i dati dell'utente siano sempre aggiornati. È inoltre possibile importare manualmente un'origine dati dell'utente.

Vedere ["Importazione dell'origine dati dell'utente"](#) a pagina 1720.

Aggiunta di un'origine dati utente basata su file

È possibile importare dati utente mediante un file `.csv`. Per praticità, Symantec Data Loss Prevention fornisce un modello `.csv` con annotazioni, che consente di verificare che i dati siano formattati correttamente. Il modello comprende tutti gli attributi utente standard oltre a esempi di formattazione e istruzioni per l'aggiunta di attributi personalizzati. Il modello include inoltre intestazioni per tutti gli attributi personalizzati definiti al momento del download.

Per creare un file di dati utente da un modello

- 1 Nella console di amministrazione di Enforce Server selezionare **Sistema > Utenti > Origini dati**.
- 2 Nella pagina **Origini dati**, fare clic su **Scarica modello CSV** sul lato destro della pagina.
- 3 Aprire il file modello e fornire informazioni per gli attributi standard dei dati utente.
Vedere ["Informazioni sulle origini dati dell'utente"](#) a pagina 1714.
- 4 Il file modello include intestazioni di colonna per gli attributi personalizzati eventualmente definiti.

Per aggiungere manualmente gli attributi personalizzati, creare una nuova colonna per ogni attributo, quindi popolare le righe nel modo desiderato.

È necessario immettere le intestazioni di colonna nel seguente formato: **ID[Nome attributo]**.
Ad esempio, **1[Condizione lavorativa]**.

Vedere ["Definizione di attributi personalizzati per i dati utente"](#) a pagina 1715.

- 5 Salvare il file (in formato `.csv`) in un percorso di Enforce Server.

Per aggiungere un'origine dati utente basata su file

- 1 Nella console di amministrazione di Enforce Server selezionare **Sistema > Utenti > Origini dati**.
- 2 Nella pagina **Gestione origine dati** fare clic su **Aggiungi > Origine utente CSV**. Viene visualizzata la finestra di dialogo **Aggiungi origine utente CSV**.
- 3 Nella finestra di dialogo **Aggiungi origine utente CSV** specificare le seguenti informazioni:
 - **Nome** : specificare un nome per l'origine dati.
 - **Percorso file** : specificare il percorso del file di dati dell'utente. Questo file deve trovarsi su Enforce Server.
 - **Delimitato da** : specifica il delimitatore per il file. I delimitatori validi sono virgola, carattere pipe, punto e virgola e carattere di tabulazione.
 - **Codificato da** : specifica il formato di codifica dei caratteri.
 - **Percentuale soglia errore** : specifica la percentuale di record utente non validi ammessi prima che il file venga rifiutato e il processo di importazione venga interrotto.

I record con indirizzi e-mail o accessi duplicati vengono conteggiati per la soglia di errore.

4 Fare clic su **Invia**.

Aggiunta di un'origine dati utente Active Directory

È possibile usare una connessione Active Directory esistente per importare dati utente. Per aggiungere attributi personalizzati per utenti aggiunti da un'origine Active Directory, creare e importare un file di dati utente che include il nome e cognome dell'utente, l'e-mail o le informazioni di accesso e gli attributi personalizzati che si desidera utilizzare. Symantec Data Loss Prevention associa automaticamente i dati utenti basati su file ai record utente esistenti importati dall'origine Active Directory.

Symantec Data Loss Prevention utilizza questo filtro Active Directory per recuperare dati utenti (interruzioni riga aggiunte per migliorare la leggibilità):

```
( &
  (objectClass=user)
  (objectCategory=person)
  (sAMAccountType=805306368)
  (!
    (|
      (&
        (sAMAccountType=805306368)
        (sAMAccountName=*)
      )
      (&
        (sAMAccountType=805306368)
        (sAMAccountName=_)
      )
    )
  )
)
```

Le credenziali Active Directory devono essere autorizzate ad accedere ai seguenti attributi utente:

```
FIRST_NAME givenName
LAST_NAME sn
EMAIL mail
LOGIN_NAME sAMAccountName
TELEPHONE telephoneNumber
TITLE title
```

```
COUNTRY co
DEPARTMENT department
EMPLOYEE_ID employeeId
STREET_ADDRESS streetAddress
LOCALITY_NAME l
POSTAL_CODE postalCode
STATE_OR_PROVINCE st
OBJECT_DISINGUISHED_NAME distinguishedName
```

Le credenziali Active Directory devono inoltre essere autorizzate ad accedere al record RootDSE. Symantec Data Loss Prevention legge questi attributi da RootDSE:

```
namingContexts
defaultNamingContext
rootDomainNamingContext
configurationNamingContext
schemaNamingContext
isGlobalCatalogReady
highestCommittedUSN
```

Vedere ["Configurazione delle connessioni a server di directory"](#) a pagina 162.

Vedere ["Definizione di attributi personalizzati per i dati utente"](#) a pagina 1715.

Vedere ["Aggiunta di un'origine dati utente basata su file"](#) a pagina 1717.

Per aggiungere un'origine dati utente Active Directory

- 1 Nella console di amministrazione di Enforce Server selezionare **Sistema > Utenti > Origini dati**.
- 2 Nella pagina **Gestione origine dati** fare clic su **Aggiungi > Aggiungi origine utente AD**. Viene visualizzata la finestra di dialogo **Aggiungi origine utente AD**.
- 3 Nella finestra di dialogo **Aggiungi origine utente AD** specificare le seguenti informazioni:
 - **Nome** : specificare un nome per l'origine dati.
 - **Connessione directory** : selezionare una connessione Active Directory esistente.
 - **Opzioni avanzate > Filtro personalizzato AD** : specifica un filtro opzionale per l'origine dati utente Active Directory, ad esempio un gruppo di lavoro. Ad esempio:

```
(&(region=North America)(!systemAccount=true))
```

- 4 Fare clic su **Invia**.

Nota: Una best practice è quella di fare riferimento agli oggetti connessione directory con baseDNs nella sezione utente della struttura directory. Ad esempio:

`ou=Users,dc=corp,dc=company,dc=com.`

Importazione dell'origine dati dell'utente

Dopo aver aggiunto l'origine dati dell'utente, è possibile pianificare Symantec Data Loss Prevention per importare regolarmente i dati da quell'origine dati per assicurarsi che i propri dati utente siano sempre aggiornati. È inoltre possibile importare manualmente un'origine dati dell'utente.

I record con accessi o indirizzi e-mail duplicati vengono esclusi dalle importazioni dell'origine dati dell'utente. Il numero dei record esclusi dall'importazione viene visualizzato al termine del processo di importazione mentre le informazioni duplicate vengono visualizzate nei registri.

Per visualizzare i dettagli di un'importazione dell'origine dati di un utente, fare clic sul collegamento **Stato**.

Pianificazione di un'importazione di un'origine dati dell'utente.

- 1 Nella console di amministrazione Enforce Server, accedere a **Sistema > Utenti > Origini dati**.
- 2 Nella pagina **Gestione origine dati**, fare clic sull'icona **Pianifica** per visualizzare l'origine dati desiderata.
- 3 Eseguire una selezione di queste opzioni per pianificare:
 - **Una volta:** consente di specificare un giorno e un'ora per l'importazione dei dati dell'utente.
 - **Giornaliera:** consente di specificare un orario specifico per l'importazione quotidiana dell'origine dati dell'utente.
 - **Giornaliera:** consente di specificare un giorno e un'ora per l'importazione settimanale dell'origine dati dell'utente.
 - **Mensile:** consente di specificare un giorno e un'ora per l'importazione mensile dell'origine dati dell'utente.
- 4 Fare clic su **Invia**.

Importazione manuale di un'origine dati

- 1 Nella console di amministrazione Enforce Server, accedere a **Sistema > Utenti > Origini dati**.
- 2 Nella pagina **Gestione origine dati**, selezionare l'origine dati che si desidera importare.
- 3 Fare clic su **Importa**.

Visualizzazione dei dettagli dell'importazione dell'origine dati

- 1 Nella console di amministrazione Enforce Server, accedere a **Sistema > Utenti > Origini dati**.
- 2 Nella pagina **Gestione origine dati**, fare clic sul collegamento **Stato** per visualizzare l'origine dati desiderata.

Viene visualizzata la finestra di dialogo **Dettagli importazione**.

- 3 La finestra di dialogo **Dettagli importazione** visualizza le seguenti informazioni per tutte le importazioni:

- **Nome** : il nome dell'origine dati importata.
- **Stato** : Fine, Operazione completata con errori, Non superato.
- **Inserita in coda alle** : l'orario in cui l'importazione dell'origine dati è stata inserita nella coda dell'importazione.
- **Avviata alle** : l'orario di avvio dell'importazione dell'origine dati.
- **Completata alle** : l'orario di fine dell'importazione dell'origine dati.

Per le importazioni riuscite e completate con errori, la finestra di dialogo **Dettagli importazione** consente di visualizzare la seguente ulteriore informazione:

- **Record aggiunti** : il numero dei record utente aggiunti.
- **Record aggiornati** : il numero dei record utente aggiornati.
- **Record con errori ignorati** : il numero di record ignorati a causa di errori nell'origine dati dell'utente.
- **Record duplicati ignorati** : il numero di record ignorati a causa di dati dell'utente duplicati.

Per le importazioni non riuscite, la finestra di dialogo **Dettagli importazione** consente di visualizzare le seguenti informazioni aggiuntive:

- **Ultima importazione riuscita** : la data e l'ora dell'ultima importazione dell'origine dati dell'utente riuscita.
- **Motivo dell'errore** : il motivo dell'errore dell'importazione.

Informazioni sull'identificazione degli utenti in incidenti Web

L'indirizzo IP in un incidente di Network Prevent for Web può essere utilizzato per determinare il nome utente associato a tale incidente. Tramite l'agente del controller di dominio, Symantec Data Loss Prevention raccoglie eventi Windows dal registro degli eventi di sicurezza sul server

del controller di dominio Microsoft Active Directory. Questi eventi vengono memorizzati nel database di Symantec Data Loss Prevention, dove un servizio di verifica può risolvere l'indirizzo IP nel relativo nome utente associato. Non è necessario eseguire un controllo incrociato degli incidenti con i registri del controller di dominio per determinare l'utente effettivo responsabile di ogni incidente. È possibile visualizzare nomi utente specifici associati agli incidenti (piuttosto che a indirizzi IP) nel report **Riepilogo rischi utente**. Vedere "[Utilizzo del riepilogo rischi utente](#)" a pagina 1725.

L'identificazione utente richiede un Enforce Server, Network Prevent for Web, server del controller di dominio e un controller di dominio di Active Directory. Vedere la sezione "Installazione dell'agente del controller di dominio" nel *Manuale di installazione di Symantec Data Loss Prevention* disponibile nel centro di supporto Symantec sul sito Web <http://www.symantec.com/doc/DOC9247> per istruzioni complete sull'installazione dell'agente del controller di dominio. Dopo avere installato tutti i componenti richiesti, è possibile attivare l'identificazione utente configurando una pianificazione del mapping alla pagina **Identificazione utente**.

Nota: Symantec Data Loss Prevention supporta l'uso di più controller di dominio.

Abilitare l'identificazione degli utenti e la configurazione della pianificazione di mapping.

L'agente del controller di dominio interroga gli eventi di Windows nel registro eventi di sicurezza di Microsoft Active Directory del controller di dominio. Symantec Data Loss Prevention associa tali eventi Windows ai dati utente del database. I dati dell'indirizzo IPv4 provenienti dal controller di dominio potrebbero non corrispondere precisamente a un dato utente. Se non si è sicuri che il nome utente risolto sia corretto, verificare che l'utente avesse eseguito l'accesso al momento dell'incidente prima di intraprendere qualsiasi azione di risposta agli incidenti.

Per impostazione predefinita, il processo di ricerca dell'identificazione utente in Enforce Server verifica la presenza nel database di nuovi eventi provenienti dal controller di dominio ogni giorno alle 4:00 AM.

Symantec Data Loss Prevention archivia i record degli utenti ricevuti dall'agente del controller di dominio nel database Symantec Data Loss Prevention. Per impostazione predefinita, i record degli utenti vengono eliminati ogni tre giorni.

Per impostare la Pianificazione mapping e attivare l'Identificazione utente

- 1 Fare clic su **Configura** dalla pagina **Sistema > Dati incidente > Identificazione utente**.
- 2 Fare clic su **Una volta**, **Giornaliera**, **Settimanale**, o **Mensile** per programmare un processo di mapping. Il valore predefinito è **Nessuna pianificazione regolare**. La Pianificazione deve essere configurata in modo da consentire il mapping.
- 3 Una volta terminato, fare clic su **Salva**.

Per configurare i parametri di conservazione dei dati

- 1 Accedere alla pagina **Sistema > Dati incidente > Identificazione utente > Configura**.
- 2 L'orario predefinito di conservazione degli eventi di accesso dell'utente è di 3 giorni. Se si desidera modificare questo valore, immetterne un altro nel **campo Conservazione dati utente**.
- 3 Una volta terminato, fare clic su **Salva**.

Per specificare la pianificazione di avviso del controller di dominio

- 1 Accedere alla pagina **Sistema > Dati incidente > Identificazione utente > Configura**.
- 2 Specificare l'avviso del controller di dominio in giorni. Si tratta del numero di giorni dall'ultimo collegamento a un controller di dominio. Il valore predefinito è 8 giorni.
- 3 Una volta terminato, fare clic su **Salva**.

Se si desidera interrompere l'utilizzo di Identificazione utente, è necessario interrompere il processo di mapping. Se non si arresta il processo di mapping, esso prosegue nell'esecuzione, anche se i controller di dominio hanno stato Sospeso.

Per arrestare un mapping pianificato

- 1 Accedere alla pagina **Sistema > Dati incidente > Identificazione utente > Configura**.
- 2 Selezionare la casella accanto ad **Arresta mapping**. La sospensione del mapping non arresta alcuni processi in corso.
- 3 Una volta terminato, fare clic su **Salva**.

Controllare dello stato dei controller di dominio

Dopo avere impostato un pianificazione del mapping, è possibile accedere alla pagina **Sistema > Dati incidente > Identificazione utente** e controllare lo stato dei controller di dominio. È possibile ordinare i controller per

- Stato: **Attivo** o **Sospeso**
- Nome controller di dominio
- Ora ultima connessione
- Giorni dall'ultima connessione
- Avvisi
- Timeout accesso

È possibile sospendere un controller di dominio facendo clic sul pulsante verde Attivo. È possibile attivare un controller di dominio sospeso facendo clic sul pulsante rosso Sospeso.

Visualizzazione dell'elenco utenti

L'elenco utenti visualizza tutti gli utenti inseriti in Symantec Data Loss Prevention. Nell'elenco utenti è possibile visualizzare i nomi, gli indirizzi e-mail, il dominio e le informazioni di accesso per ciascun utente. È possibile ordinare l'elenco per nome o cognome ed eseguire ricerche per nome, indirizzo e-mail, dominio o credenziali di accesso. Se si fa clic sul nome di un singolo utente appare la vista dei dettagli utente.

Vedere ["Visualizzazione dei dettagli dell'utente"](#) a pagina 1724.

L'elenco utenti non visualizza dati incidente, ma solo dati utente.

Per visualizzare l'elenco utenti

- 1 Nella console di amministrazione di Enforce Server accedere a **Incidenti > Utenti > Elenco utenti**.
- 2 Per ordinare l'elenco utenti per nome o cognome, fare clic su una delle icone di ordinamento nella colonna appropriata.
- 3 Per eseguire una ricerca nell'elenco utenti, immettere termine di ricerca nel campo di ricerca nell'angolo in alto a destra dell'elenco. È possibile eseguire la ricerca in base a nome, cognome, credenziali di accesso e indirizzo e-mail. Viene gestito un solo termine di ricerca alla volta.

Visualizzazione dei dettagli dell'utente

L'istantanea utente mostra tutte le informazioni e gli incidenti per un utente specifico. Per visualizzare l'istantanea utente fare clic su un nome utente nell'elenco utenti. È possibile esportare l'istantanea utente in un file CSV.

Vedere ["Visualizzazione dell'elenco utenti"](#) a pagina 1724.

Per visualizzare i dettagli utente

- 1 Nella console di amministrazione di Enforce Server accedere a **Incidenti > Utenti > Elenco utenti**.
- 2 Fare clic sul nome dell'utente di cui si desidera visualizzare i dettagli.
- 3 La pagina **Utente** visualizza l'elenco degli incidenti, nonché informazioni sull'utente, gli attributi standard e gli attributi personalizzati. Per gli utenti identificati dall'indirizzo IP sono inoltre disponibili dati sull'orario dell'ultima attività.
- 4 Per esportare l'istantanea utente in un file CSV, fare clic su **Esporta**.

Utilizzo del riepilogo rischi utente

Il riepilogo rischi utente visualizza tutti gli utenti ai quali sono associati incidenti. È possibile ordinare e filtrare il riepilogo per migliorare la comprensione dei rischi dell'utente nell'organizzazione. Ad esempio, è possibile visualizzare gli incidenti associati con politiche specifiche o con attributi personalizzati inseriti, quali la qualifica o lo stato lavorativo. Per tornare a una vista specifica del riepilogo rischi utente, è possibile salvare l'URL e associarlo a un segnalibro nel browser Web. È anche possibile esportare i dati dal riepilogo rischi utente in un file CSV.

Per visualizzare il riepilogo rischi utente

- 1 Nella console di amministrazione di Enforce Server accedere a **Incidenti > Utenti > Riepilogo rischi utente**.
- 2 Per ordinare l'elenco fare clic su una delle icone di ordinamento in una delle colonne.
- 3 Per filtrare l'elenco, selezionare i valori di filtro utilizzando le opzioni sopra l'elenco di riepilogo dei rischi utente:

Filtro	Valore predefinito	Descrizione
Politiche	Tutti	Selezionare una politica o le politiche espandendo il gruppo di politiche e selezionando la o le caselle appropriate.
Attributi	Nessuno (0)	Immettere fino a due attributi personalizzati per filtrare la lista. Selezionare l'attributo nell'elenco a discesa, quindi specificare una condizione di inclusione o esclusione e inserire i valori desiderati. Per aggiungere un secondo filtro attributi, fare clic su Aggiungi filtro attributi .
Stato	Tutti	Filtra l'elenco per stato incidente.
Data	Ultimi 7 giorni	Filtra l'elenco per data o dall'intervallo di date.
Tipo	Tutti	Filtra l'elenco per tipo incidente, quale E-mail/SMTP , Stampante/Fax o HTTP .
Includi	Tutti	È possibile filtrare l'elenco per gravità dell'incidente. È necessario selezionare almeno un livello di gravità. È anche possibile includere o escludere i nomi utente identificati mediante l'indirizzo IP.

- 4 Una volta selezionati i valori del filtro, fare clic su **Applica**.

- 5 Per salvare una configurazione di filtro specifica, fare clic su **Ottieni collegamento** e copiare l'URL fornito nei segnalibri del browser Web.
- 6 Per esportare dati dal riepilogo rischi utente a un file CSV, fare clic su **Esporta**. È possibile esportare la pagina corrente o tutte le pagine del riepilogo rischi utente.

Implementazione dei plug-in di ricerca

Il capitolo contiene i seguenti argomenti:

- [Informazioni sui plug-in di ricerca](#)
- [Implementazione e test dei plug-in di ricerca](#)
- [Configurazione del plug-in di ricerca CSV](#)
- [Configurazione dei plug-in di ricerca LDAP](#)
- [Configurazione dei plug-in di ricerca di script](#)
- [Configurazione dei plug-in di ricerca personalizzati \(precedenti\) migrati](#)

Informazioni sui plug-in di ricerca

Un plug-in di ricerca consente di collegare Enforce Server a un sistema esterno per recuperare dati aggiuntivi relativi a un incidente. I dati vengono memorizzati come attributi. I plug-in di ricerca consentono di aggiungere contesto agli incidenti per facilitare il flusso di lavoro di riparazione. Ad esempio, considerare un messaggio e-mail che attiva un incidente. Un plug-in di ricerca può essere utilizzato per recuperare e visualizzare il nome e l'indirizzo e-mail del responsabile del mittente da un server di directory, in base all'indirizzo e-mail del mittente.

I plug-in di ricerca utilizzano attributi di incidente e attributi personalizzati in coordinazione tra loro. Il sistema genera gli attributi incidente quando viene violata una regola della politica. È possibile definire attributi personalizzati per i dati incidente personalizzati. Per continuare con l'esempio, quando viene rilevato l'incidente, il sistema genera l'attributo di incidente "sender-email" e lo compila con l'indirizzo e-mail del mittente. Il plug-in di ricerca usa questa coppia chiave-valore per cercare i valori degli attributi personalizzati "Nome del responsabile"

e "E-mail del responsabile" in un server LDAP. Il plug-in compila gli attributi personalizzati e li visualizza in **Istantanea incidente**.

Vedere ["Informazioni sugli attributi personalizzati"](#) a pagina 1706.

Vedere ["Informazioni sull'uso di attributi personalizzati"](#) a pagina 1708.

Vedere ["Metodi di inserimento di attributi personalizzati"](#) a pagina 1708.

Tipi di plug-in di ricerca

Symantec Data Loss Prevention fornisce diversi tipi di plug-in di ricerca, tra cui CSV, LDAP, Script, Data Insight e personalizzato (precedente). Nella tabella seguente vengono descritti nei dettagli i tipi di plug-in di ricerca.

Vedere ["Informazioni sui plug-in di ricerca"](#) a pagina 1727.

Tabella 55-1 Tipi di plug-in di ricerca

Tipo	Descrizione
CSV	<p>Il plug-in di ricerca CSV consente di recuperare i dati dell'incidente da un file di valori separati da virgole (CSV) caricato su Enforce Server. È possibile configurare un plug-in di ricerca CSV per ogni istanza di Enforce Server.</p> <p>Vedere "Informazioni sul plug-in di ricerca CSV" a pagina 1729.</p>
LDAP	<p>Il plug-in di ricerca LDAP consente di recuperare i dati dell'incidente da un server di directory, ad esempio Microsoft Active Directory, Oracle Directory Server o IBM Tivoli. È possibile configurare più istanze del plug-in di ricerca LDAP.</p> <p>Vedere "Informazioni sui plug-in di ricerca LDAP" a pagina 1729.</p>
Script	<p>Il plug-in di ricerca Script consente di scrivere uno script per recuperare i dati dell'incidente da qualsiasi risorsa esterna. Ad esempio è possibile utilizzare un plug-in di ricerca Script per recuperare i dati dell'incidente da risorse esterne, quali file di registro proxy o sistemi DNS. È possibile configurare più istanze del plug-in di ricerca Script.</p> <p>Vedere "Informazioni sui plug-in di ricerca script" a pagina 1729.</p>
Data Insight	<p>Il plug-in di ricerca Data Insight consente di recuperare i dati dell'incidente da Symantec Data Insight in modo che sia possibile individuare e gestire i dati a rischio. È possibile configurare un plug-in di ricerca Data Insight per ogni istanza di Enforce Server.</p>
Personalizzato (precedente)	<p>Il plug-in di ricerca personalizzato (precedente) consente di utilizzare il codice Java per recuperare i dati dell'incidente da qualsiasi risorsa esterna.</p> <p>Vedere "Informazioni sui plug-in di ricerca (precedenti) personalizzati" a pagina 1730.</p> <p>Nota: come indica il nome, il plug-in di ricerca personalizzato (precedente) è riservato ai plug-in di ricerca Java precedenti. Per lo sviluppo di nuovi plug-in personalizzati è necessario utilizzare uno degli altri tipi di ricerca.</p>

Informazioni sul plug-in di ricerca CSV

Il plug-in di ricerca CSV estrae i dati da un file di valori separati da virgole (CSV) memorizzato in Enforce Server. Tali dati vengono quindi utilizzati per popolare gli attributi personalizzati per un incidente nel momento in cui l'incidente viene generato.

Il plug-in di ricerca CSV riceve un gruppo di parametri di ricerca che contengono i dati riguardanti un incidente da Enforce Server. Uno o più di quei parametri di ricerca nel gruppo vengono mappati alle intestazioni di colonna in un file CSV. Ad esempio, il parametro di ricerca `sender-email` potrebbe essere mappato alla colonna `Email` nel file CSV. Il valore nel parametro di ricerca viene utilizzato come una chiave per trovare un valore corrispondente nel relativo file CSV. Quando si ha una corrispondenza, la riga CSV che contiene il valore corrispondente fornisce i dati che sono restituiti a Enforce Server. Enforce Server utilizza i dati in quella riga per popolare gli attributi personalizzati per quell'incidente. Ad esempio, se il parametro di ricerca `sender-email` contiene il valore `mary.smith@mycompany.com`, il plug-in cerca nella colonna `Email` una riga che contenga `mary.smith@mycompany.com`. Quella riga è quindi utilizzata per fornire i dati con cui popolare gli attributi personalizzati per l'incidente.

Il plug-in di ricerca CSV utilizza un database residente in memoria per elaborare file di grandi dimensioni.

Vedere ["Configurazione del plug-in di ricerca CSV"](#) a pagina 1747.

Informazioni sui plug-in di ricerca LDAP

Il plug-in di ricerca LDAP estrae i dati da un sistema LDAP live (quale Microsoft Active Directory, Oracle Directory Server o IBM Tivoli). Tali dati vengono quindi utilizzati per popolare gli attributi personalizzati per un incidente nel momento in cui l'incidente viene generato.

Il plug-in di ricerca LDAP riceve un gruppo di parametri di ricerca che contengono i dati riguardanti un incidente da Enforce Server. Questi parametri di ricerca vengono quindi utilizzati nelle query LDAP per estrarre i dati da una directory LDAP esistente. Ad esempio, il valore del parametro di ricerca `sender-email` potrebbe essere confrontato ai valori nell'attributo `email` della directory. Se il parametro di ricerca `sender-email` contiene `mary.smith@mycompany.com`, è possibile costruire una query per cercare un record il cui attributo `email` contiene `mary.smith@mycompany.com`. I dati nel record restituiti dalla ricerca sono inseriti negli attributi personalizzati per l'incidente.

Vedere ["Configurazione dei plug-in di ricerca LDAP"](#) a pagina 1757.

Informazioni sui plug-in di ricerca script

È possibile scrivere uno o più plug-in di ricerca script per ricercare i valori attributo negli archivi dati. Ad esempio, è possibile scrivere uno script che ricerchi in un server DNS informazioni relative a un mittente coinvolto in un incidente. Un plug-in di ricerca script può utilizzare l'output di determinati script per popolare attributi personalizzati nei record degli incidenti.

A differenza dei plug-in di ricerca LDAP o CSV, il plug-in di ricerca script non utilizza mappe di attributi in linea per specificare come ricercare le chiavi di parametro. Al contrario, scrivere tale funzionalità in ciascuno script, come necessario.

Per implementare un plug-in di ricerca script, è possibile utilizzare qualsiasi linguaggio di script in grado di leggere l'input standard (`stdin`) e scrivere l'output standard (`stdout`). Gli esempi nell'interfaccia utente e nella presente documentazione utilizzano Python versione 2.6.

Vedere ["Configurazione di proprietà di plug-in avanzate"](#) a pagina 1745.

Informazioni sul plug-in di ricerca Data Insight

Il plug-in di ricerca Veritas Data Insight recupera i dati da un server di gestione Veritas Data Insight e li utilizza per popolare gli attributi per un incidente di Network Discover quando l'incidente è generato. Il plug-in di ricerca Data Insight si connette a Symantec Data Loss Prevention con Symantec Data Insight per recuperare i valori degli attributi. Data Insight può essere usato per fornire il contesto granulare per gli incidenti, comprese informazioni aggiornate sul proprietario dei dati. I valori per gli attributi incidente sono visualizzati e popolati nella schermata **Istantanea incidente**.

Il plug-in di ricerca Data Insight richiede una licenza Data Insight distinta da quella di Symantec Data Loss Prevention. Se il sistema non dispone della licenza per Data Insight, il plug-in di ricerca Data Insight non è disponibile. Se si dispone di una licenza per Data Insight, consultare la *Guida all'implementazione di Symantec Data Loss Prevention Data Insight* per informazioni dettagliate sull'integrazione con Data Insight.

Informazioni sui plug-in di ricerca (precedenti) personalizzati

È possibile utilizzare un plug-in di ricerca (precedente) personalizzato per migrare i plug-in di ricerca Java personalizzati precedenti alla console di amministrazione di Enforce Server. Poiché i Plug-in di ricerca Java personalizzati non sono più il modo preferito per creare nuovi plug-in, le informazioni presentate qui sono fornite per aiutare le organizzazioni che utilizzano plug-in precedenti ma devono effettuare l'upgrade a Data Loss Prevention versione 15.1. Come alternativa alla migrazione dei plug-in di ricerca Java personalizzati precedenti, considerare la possibilità di riscrivere tali plug-in utilizzando un plug-in di ricerca script o uno degli altri plug-in di ricerca supportati, come ad esempio CSV o LDAP.

Vedere ["Tipi di plug-in di ricerca"](#) a pagina 1728.

Nota: I plug-in di ricerca (precedenti) personalizzati devono essere usati solo per la migrazione di plug-in di ricerca precedenti implementati utilizzando l'API di ricerca Java. Il supporto per nuovi plug-in di ricerca Java personalizzati non è fornito.

Vedere ["Configurazione dei plug-in di ricerca personalizzati \(precedenti\) migrati"](#) a pagina 1773.

Informazioni sui parametri di ricerca

Quando viene creato un incidente, Enforce Server genera gli attributi dell'incidente e li popola con i dati acquisiti dall'incidente. Uno o più attributi dell'incidente sono utilizzati come chiavi dei parametri di ricerca per recuperare dati esterni e popolare attributi personalizzati con i valori recuperati dal sistema esterno. Scegliere i parametri di ricerca da utilizzare per i plug-in di ricerca nella schermata **Parametri di ricerca**. Almeno un parametro di ricerca deve essere presente nell'origine dati esterna affinché la ricerca venga eseguita.

Mentre alcuni attributi sono creati per tutti i tipi di incidenti, altri sono specifici del tipo di incidente. Ad esempio, l'attributo di incidente `sender-email` è specifico degli incidenti SMTP. Gli attributi degli incidenti Endpoint e Discover sono preceduti da un identificatore, ad esempio `discover-name` e `endpoint-machine-name`. Per convenienza amministrativa, i parametri di ricerca sono organizzati in gruppi. Un incidente espone tutti i parametri di ricerca in ogni gruppo di parametri di ricerca attivato. Nella ricerca, alcune delle coppie nome-valore in quel gruppo possono essere prive di valore a seconda del tipo di incidente. Ad esempio, il valore di attributo del parametro `sender-email` è null per gli incidenti di Discover (`sender-email=null`).

I plug-in di ricerca non modificano i valori definiti dal sistema dei parametri di ricerca. Il plug-in utilizza questi parametri solo come chiavi per eseguire la ricerca e popolare attributi personalizzati. Ad esempio, se un plug-in di ricerca utilizza il parametro di ricerca `subject`, il valore di questo attributo non viene sostituito da un valore per tale attributo nell'origine dati esterna; Enforce Server ignora il valore dopo l'esecuzione della ricerca. Ci sono tuttavia due eccezioni: `data-owner-name` e `data-owner-email`. Questi attributi di incidente definiti dal sistema funzionano come attributi personalizzati e sono popolati con valori recuperati.

Quando si esegue il mapping delle chiavi all'origine dati, il plug-in cerca le chiavi fino a che non trova il primo valore corrispondente. Quando un valore corrispondente viene trovato, il plug-in arresta la ricerca delle chiavi. Il plug-in utilizza i dati nella riga contenente il primo valore corrispondente per popolare gli attributi personalizzati pertinenti. Di conseguenza, i valori delle chiavi non vengono combinati, ma il primo valore trovato è la chiave. Poiché il plug-in interrompe la ricerca dopo aver trovato il primo valore corrispondente, l'ordine in cui le `chiavi` sono elencate nel mapping degli attributi è importante. Fare riferimento agli esempi e agli argomenti relativi al mapping di singoli attributi per informazioni dettagliate sulla sintassi utilizzata per il mapping degli attributi dei plug-in di ricerca.

Per eseguire una ricerca, è necessario mappare almeno una chiave parametro di ricerca a un campo nell'origine dati esterna. Ogni gruppo di parametri di ricerca che si attiva è una ricerca database separata che deve essere eseguita dall'Enforce Server. Tutte le query del database vengono eseguite per ciascun incidente prima della ricerca. Per evitare l'impatto sulle prestazioni di query del database inutili, è necessario attivare solo i gruppi di attributi richiesti dai plug-in di ricerca.

Poiché il plug-in interrompe la ricerca dopo avere trovato la prima coppia chiave di parametro di ricerca-valore corrispondente, l'ordine in cui si elencano le `chiavi` nella mappa di attributi

è importante. Fare riferimento agli esempi di mapping di attributi per il tipo specifico di plug-in che si sta implementando.

Vedere ["Selezione dei parametri di ricerca"](#) a pagina 1737.

Informazioni sulla distribuzione di plug-in

Un plug-in di ricerca viene distribuito mediante attivazione dello stesso nell'interfaccia utente. Ogni plug-in di ricerca deve essere attivato, anche se ne è presente uno solo. Se molteplici plug-in sono attivati, è necessario concatenarli e specificarne l'ordine dell'esecuzione.

Le chiavi dei parametri di ricerca selezionati si applicano globalmente a tutti i plug-in di ricerca distribuiti. Se i plug-in vengono ricaricati, lo stesso avviene per tutti i plug-in distribuiti.

È possibile distribuire soltanto un plug-in di ricerca CSV e un plug-in di ricerca Data Insight per istanza di Enforce Server.

Vedere ["Attivazione dei plug-in di ricerca"](#) a pagina 1742.

Informazioni sul concatenamento di plug-in

Quando si crea un plug-in di ricerca, si esegue il mapping delle chiavi dei parametri di ricerca e degli attributi personalizzati ai campi nell'origine dati esterna. Tutti i plug-in di ricerca distribuiti ricevono un riferimento alla stessa mappa attributi. Ciò consente il concatenamento e l'esecuzione in sequenza dei plug-in.

In una catena di plug-in di ricerca, il primo plug-in usa i parametri di ricerca ricevuti da Enforce Server per cercare i valori di attributi. Il secondo plug-in usa i dati ricevuti dal primo plug-in, ovvero i parametri di ricerca e tutte le variabili create mediante la ricerca precedente. Questo processo viene ripetuto in sequenza o per tutti i plug-in nella catena.

Una catena di plug-in è utile quando le informazioni devono essere estratte da origini differenti per popolare gli attributi personalizzati di un incidente. Una catena è inoltre utile quando ci sono differenze o dipendenze tra le "chiavi" necessarie per sbloccare i dati corretti.

Ad esempio, si consideri la seguente catena di plug-in:

1. Un plug-in di ricerca di script esegue una ricerca DNS utilizzando uno o più parametri.
2. Un plug-in di ricerca CSV usa il risultato della ricerca di script per recuperare i dati sugli incidenti da un file CSV che è un estratto di un sistema di gestione di cespiti.
3. Un plug-in di ricerca LDAP usa il risultato della ricerca CSV per ottenere i dati da una directory LDAP dell'azienda.

Vedere ["Concatenamento dei plug-in di ricerca"](#) a pagina 1742.

Vedere ["Concatenamento di più plug-in di ricerca script"](#) a pagina 1769.

Informazioni sull'aggiornamento dei plug-in di ricerca

Prima della versione 11.6 di Symantec Data Loss Prevention, i plug-in di ricerca venivano implementati manualmente utilizzando file di proprietà; non era disponibile un'interfaccia utente per la configurazione dei plug-in di ricerca. L'interfaccia utente dei plug-in di ricerca è stata introdotta nella versione 11.6.

Se si sta aggiornando alla versione 12.0 o successive, i plug-in di ricerca esistenti vengono aggiornati automaticamente alla nuova struttura e aggiunti all'interfaccia utente per la configurazione e la distribuzione. Inoltre lo stato del plug-in viene conservato dopo l'aggiornamento, ovvero se un plug-in era attivato prima dell'aggiornamento sarà attivato nell'interfaccia utente dopo l'aggiornamento.

Se l'aggiornamento di un plug-in di ricerca non riesce, il sistema visualizza il seguente messaggio di errore:

```
INFO: IN PROCESS: Errors detected in lookup plugin configuration.  
Your lookup plugins may require manual configuration after the upgrade.
```

In questo caso, controllare il plug-in nella schermata **Sistema > Plug-in di ricerca** e configurarlo manualmente con le istruzioni fornite nella presente documentazione. Consultare *Symantec Data Loss Prevention - Note sulla versione* per i problemi noti relativi all'aggiornamento dei plug-in di ricerca.

Implementazione e test dei plug-in di ricerca

Nella tabella seguente viene descritto il flusso di lavoro per implementare e testare i plug-in di ricerca. Nelle sezioni collegate sono illustrati nei dettagli questi passaggi.

Tabella 55-2 Implementazione e test dei plug-in di ricerca

Passaggio	Descrizione
1	Decidere quali dati esterni si desidera estrarre e caricare negli incidenti come attributi personalizzati. Vedere "Informazioni sull'uso di attributi personalizzati" a pagina 1708.
2	Identificare le origini da cui i dati degli attributi personalizzati devono essere ottenuti e il plug-in di ricerca appropriato per recuperare queste informazioni. Vedere "Tipi di plug-in di ricerca" a pagina 1728.
3	Creare un attributo personalizzato per ogni dato esterno che si desidera includere nelle istantanee e nei report degli incidenti. Vedere "Configurazione di attributi personalizzati" a pagina 1709.

Passaggio	Descrizione
4	<p>Determinare quali gruppi di parametri di ricerca includono i parametri di ricerca specifici di cui è necessario estrarre i dati pertinenti dalle origini esterne.</p> <p>Vedere "Informazioni sui parametri di ricerca" a pagina 1731.</p>
5	<p>Configurare il plug-in per estrarre i dati dall'origine dati esterna e inserire gli attributi personalizzati.</p> <p>Vedere "Configurazione del plug-in di ricerca CSV" a pagina 1747.</p> <p>Vedere "Configurazione dei plug-in di ricerca LDAP" a pagina 1757.</p> <p>Vedere "Configurazione dei plug-in di ricerca di script" a pagina 1762.</p> <p>Vedere "Configurazione dei plug-in di ricerca personalizzati (precedenti) migrati" a pagina 1773.</p>
6	<p>Attivare il plug-in su Enforce Server.</p> <p>Vedere "Attivazione dei plug-in di ricerca" a pagina 1742.</p>
7	<p>Impostare l'ordine di esecuzione per più plug-in.</p> <p>Vedere "Concatenamento dei plug-in di ricerca" a pagina 1742.</p>
8	<p>Verificare i privilegi. L'utente finale deve disporre dei privilegi degli attributi di ricerca per utilizzare un plug-in di ricerca per cercare i valori di attributo.</p> <p>Vedere "Ruoli di configurazione" a pagina 114.</p>
9	<p>Generare un incidente. L'incidente deve essere del tipo che espone uno o più attributi di incidente designati come chiavi di parametro.</p> <p>Vedere "Configurazione di politiche" a pagina 422.</p>
10	<p>Visualizzare i dettagli dell'incidente. Per l'incidente generato accedere alla schermata Istantanea incidente. Nella sezione Attributi si dovrebbero vedere gli attributi personalizzati creati. Si noti che non contengono alcun valore. Se gli attributi personalizzati non sono visualizzati, verificare i privilegi e assicurarsi che gli attributi personalizzati siano stati creati.</p>
11	<p>Se il plug-in di ricerca è stato implementato correttamente, il pulsante Ricerca è disponibile nella sezione Attributi della schermata Istantanea incidente. Dopo che si è fatto clic su Ricerca, viene inserito il valore per ciascun attributo personalizzato. Dopo la ricerca iniziale, la connessione viene mantenuta e per gli incidenti successivi il plug-in di ricerca inserisce gli attributi personalizzati. L'addetto alle risoluzioni non deve fare clic su Ricerca per gli incidenti successivi. Se necessario, è possibile ricaricare i plug-in.</p> <p>Vedere "Risoluzione dei problemi relativi ai plug-in di ricerca" a pagina 1743.</p> <p>Vedere "Ricaricamento dei plug-in di ricerca" a pagina 1743.</p>

Gestione e configurazione dei plug-in di ricerca

La schermata **Sistema > Dati incidente > Plug-in di ricerca** è la home page per la creazione, la configurazione e la gestione dei plug-in di ricerca. I plug-in di ricerca sono usati a scopi di riparazione, per recuperare dati associati a incidenti da un'origine dati esterna e popolare gli attributi incidente.

Vedere ["Informazioni sui plug-in di ricerca"](#) a pagina 1727.

I plug-in di ricerca vengono creati e configurati nella **Pagina elenco plug-in di ricerca**.

Tabella 55-3 Creazione e configurazione dei plug-in di ricerca

Azione	Descrizione
Nuovo plug-in	Selezionare questa opzione per creare un nuovo plug-in. Vedere "Creazione di nuovi plug-in di ricerca" a pagina 1736.
Modifica catena di plug-in	Selezionare questa opzione per attivare (distribuire) i plug-in e impostare l'ordine di ricerca per più plug-in. Vedere "Attivazione dei plug-in di ricerca" a pagina 1742.
Parametri di ricerca	Selezionare questa opzione per scegliere quali gruppi di parametri di ricerca utilizzare come chiavi per popolare i campi attributo da origini esterne. Vedere "Selezione dei parametri di ricerca" a pagina 1737.
Ricarica plug-in	Selezionare questa opzione per aggiornare il sistema dopo la modifica di plug-in attivati o se i dati esterni vengono aggiornati. Questa azione esegue automaticamente le ricerche consentite in ordine e popola gli incidenti mentre sono creati. Vedere "Ricaricamento dei plug-in di ricerca" a pagina 1743.

Per ogni plug-in di ricerca configurato, il sistema visualizza le seguenti informazioni nella **Pagina elenco plug-in di ricerca**. Queste informazioni consentono di gestire i plug-in di ricerca.

Tabella 55-4 Gestione dei plug-in di ricerca

Campo visualizzato	Descrizione
Sequenza di esecuzione	Questo campo visualizza l'ordine di esecuzione dei plug-in di ricerca nel sistema. Vedere "Attivazione dei plug-in di ricerca" a pagina 1742.
Nome	Questo campo visualizza il nome definito dall'utente di ciascun plug-in di ricerca. Fare clic sul collegamento Nome per modificare il plug-in corrispondente. Vedere "Creazione di nuovi plug-in di ricerca" a pagina 1736.

Campo visualizzato	Descrizione
Tipo	Il campo visualizza il tipo di plug-in di ricerca. È possibile configurare un plug-in di ricerca CSV e un plug-in di ricerca Data Insight per istanza di Enforce Server. È possibile configurare più istanze dei plug-in di ricerca LDAP, Script e Custom (legacy). Vedere "Tipi di plug-in di ricerca" a pagina 1728.
Descrizione	Questo campo visualizza la descrizione definita dall'utente di ciascun plug-in di ricerca. Vedere "Implementazione e test dei plug-in di ricerca" a pagina 1733.
Stato	Il campo visualizza lo stato di ciascun plug-in di ricerca, Attivato (verde) o Disattivato (rosso). Per modificare lo stato di un plug-in, fare clic su Modifica catena di plug-in . Vedere "Attivazione dei plug-in di ricerca" a pagina 1742.

Per ogni plug-in di ricerca configurato è possibile eseguire le seguenti funzioni di gestione nella **Pagina elenco plug-in di ricerca**.

Tabella 55-5 Ordinamento e raggruppamento dei plug-in di ricerca

Azione	Descrizione
Modifica	Fare clic sull'icona della matita nella colonna Azioni per modificare il plug-in.
Eliminazione	Fare clic sull'icona X nella colonna Azioni per eliminare il plug-in. È necessario confermare o annullare l'azione per eseguirla.
Ordinamento	Ordinare la colonna di visualizzazione selezionata in ordine crescente o decrescente.
Raggruppamento	Raggruppare i plug-in in base alla colonna di visualizzazione selezionata. Ad esempio, dove sono presenti più collegamenti, può risultare utile raggrupparli per Tipo o per Stato .

Creazione di nuovi plug-in di ricerca

Per creare e configurare i plug-in di ricerca è necessario disporre di privilegi Amministrazione server.

Vedere ["Ruoli di configurazione"](#) a pagina 114.

Per creare un nuovo plug-in di ricerca

- 1 Accedere a **Sistema > Dati incidente > Plug-in di ricerca** nella console di amministrazione dell'Enforce Server.
- 2 Fare clic su **Nuovo plug-in** nella **Pagina elenco plug-in di ricerca**.

- 3 Selezionare il tipo di plug-in di ricerca da creare e configurare:

CSV

Vedere ["Configurazione del plug-in di ricerca CSV"](#) a pagina 1747.

LDAP

Vedere ["Configurazione dei plug-in di ricerca LDAP"](#) a pagina 1757.

Script

Vedere ["Configurazione dei plug-in di ricerca di script"](#) a pagina 1762.

Data Insight

Personalizzato (precedente)

Vedere ["Configurazione dei plug-in di ricerca personalizzati \(precedenti\) migrati"](#) a pagina 1773.

- 4 Fare clic su **Salva** per applicare la configurazione del plug-in di ricerca.

Il sistema visualizza un messaggio operazione riuscita (verde) se il plug-in viene salvato correttamente o un messaggio di errore (rosso) se il plug-in non è configurato correttamente e non può essere salvato.

Vedere ["Risoluzione dei problemi relativi ai plug-in di ricerca"](#) a pagina 1743.

- 5 Fare clic su **Modifica catena di plug-in** e consentire il plug-in di ricerca e il concatenamento di più plug-in.

Vedere ["Attivazione dei plug-in di ricerca"](#) a pagina 1742.

Vedere ["Concatenamento dei plug-in di ricerca"](#) a pagina 1742.

Selezione dei parametri di ricerca

Nella pagina **Sistema > Plug-in di ricerca > Modifica parametri plug-in di ricerca** sono elencate le **chiavi dei parametri di ricerca** selezionate per attivare la ricerca dei valori di attributo. Le chiavi dei parametri di ricerca sono organizzate in gruppi di attributi. Le selezioni effettuate in questa schermata vengono applicate a tutti i plug-in di ricerca distribuiti su Enforce Server.

Per eseguire una ricerca, è necessario mappare almeno una chiave di un parametro di ricerca a un campo nell'origine dati esterna. Ogni gruppo di parametri di ricerca che si attiva è una ricerca database separata che deve essere eseguita dall'Enforce Server. Tutte le query del database vengono eseguite per ciascun incidente prima della ricerca. Per evitare l'impatto sulle prestazioni di query del database inutili, è necessario attivare solo i gruppi di attributi richiesti dai plug-in di ricerca.

Poiché il plug-in interrompe la ricerca dopo avere trovato la prima coppia chiave di parametro di ricerca-valore corrispondente, l'ordine in cui si elencano le `keys` nella mappa di attributi è importante. Per i dettagli fare riferimento agli esempi di mapping di attributi per il tipo specifico di plug-in che si sta implementando.

Vedere ["Informazioni sui parametri di ricerca"](#) a pagina 1731.

Per attivare una o più chiavi dei parametri di ricerca

- 1 Selezionare **Sistema > Plug-in di ricerca** nella console di amministrazione di Enforce Server.
- 2 Fare clic su **Parametri di ricerca** nella **Pagina elenco di plug-in di ricerca**.
- 3 Selezionare uno o più gruppi di attributi nella pagina **Modifica parametri plug-in di ricerca**.

Fare clic su **Visualizza proprietà** per visualizzare tutte le chiavi per il gruppo di attributi.

- Allegato [Tabella 55-6](#)
- Incidente [Tabella 55-7](#)
- Messaggio [Tabella 55-8](#)
- Politica [Tabella 55-9](#)
- Destinatario [Tabella 55-10](#)
- Mittente [Tabella 55-11](#)
- Server [Tabella 55-12](#)
- Monitoraggio [Tabella 55-13](#)
- Stato [Tabella 55-14](#)
- ACL [Tabella 55-15](#)

- 4 **Salvare** la configurazione.

Verificare il messaggio che indica che tutti i plug-in attivati sono stati ricaricati.

Tabella 55-6 Parametri di ricerca dell'allegato

Chiave di parametro di ricerca	Descrizione e commenti
<code>attachment-nameX</code>	Nome del file allegato, dove X è l'indice univoco per distinguere più allegati, ad esempio: <code>attachment-name1</code> , <code>attachment-size1</code> ; <code>attachment-name2</code> , <code>attachment-size2</code> ; e così via.
<code>attachment-sizeX</code>	Dimensione originale del file allegato, dove X è l'indice univoco per distinguere più allegati. Vedere l'esempio riportato sopra.

Tabella 55-7 Parametri di ricerca dell'incidente

Chiave di parametro di ricerca	Descrizione
date-detected	Data e ora in cui è stato rilevato l'incidente, ad esempio: date-detected=Tue May 15 15:08:23 PDT 2012.
incident-id	ID dell'incidente assegnato da Enforce Server. Lo stesso ID è riportato nel report dell'incidente. Ad esempio: incident-id=35.
protocol	Nome del protocollo di rete utilizzato per trasferire il messaggio di violazione, ad esempio SMTP e HTTP. Ad esempio: protocol=Email/SMTP.
data-owner-name	Persona responsabile della risoluzione dell'incidente. Questo attributo non viene inserito dal sistema. Viene invece impostato manualmente nella sezione Dettagli incidente della schermata Istantanea incidente o automaticamente con un plug-in di ricerca. I report basati su questo attributo possono venire automaticamente inviati al proprietario di dati per la risoluzione.
data-owner-email	Indirizzo e-mail della persona responsabile della risoluzione dell'incidente. Questo attributo non viene inserito dal sistema. Viene invece impostato manualmente nella sezione Dettagli incidente della schermata Istantanea incidente o automaticamente con un plug-in di ricerca.

Tabella 55-8 Parametri di ricerca del messaggio

Chiave di parametro di ricerca	Descrizione
date-sent	Data e ora in cui è stato inviato il messaggio se si tratta di un'e-mail. Ad esempio: date-sent=Mon Aug 15 11:46:55 PDT 2011.
subject	Oggetto del messaggio se si tratta di un incidente e-mail.
file-create-date	Data in cui il file è stato creato nella posizione corrente, indipendentemente dal fatto che sia stato originariamente creato qui o copiato da un'altra posizione. Recuperato dal sistema operativo.
file-access-date	Data in cui il file è stato esaminato.
file-created-by	Utente che ha sistemato il file sull'endpoint.
file-modified-by	Credenziale dell'utente qualificato per il computer su cui ha avuto luogo l'azione di copia all'origine della violazione.
file-owner	Nome dell'utente o del computer su cui è situato il file all'origine della violazione.
discover-content-root-path	Radice del percorso del file che ha causato un incidente di rilevazione.

Chiave di parametro di ricerca	Descrizione
discover-location	Percorso completo del file che ha causato un incidente di rilevazione.
discover-name	Nome del file all'origine della violazione.
discover-extraction-date	Data in cui un file secondario è stato estratto da un file incapsulato durante la scansione di rilevamento.
discover-server	Nome dell'archivio da sottoporre a scansione.
discover-notes-database	Attributo specifico per la scansione di rilevamento dell'archivio Lotus Notes.
discover-notes-url	Attributo specifico per la scansione di rilevamento dell'archivio Lotus Notes.
endpoint-volume-name	Nome dell'unità locale su cui si è verificato un incidente endpoint.
endpoint-dos-volume-name	Nome di Windows dell'unità locale su cui si è verificato un incidente endpoint.
endpoint-application-name	Nome dell'applicazione utilizzata più di recente per aprire (o creare) il file all'origine della violazione.
endpoint-application-path	Percorso dell'applicazione utilizzata per creare o aprire il file all'origine della violazione.
endpoint-file-name	Nome del file all'origine della violazione.
endpoint-file-path	Percorso in cui è stato copiato il file.

Tabella 55-9 Parametro di ricerca della politica

Chiave di parametro di ricerca	Descrizione e commenti
policy-name	Nome della politica che è stata violata, ad esempio: <code>policy-name=Keyword Policy</code> .

Tabella 55-10 Parametri di ricerca del destinatario

Chiave di parametro di ricerca	Descrizione
recipient-emailX	Indirizzo e-mail del destinatario, dove X è l'indice esclusivo per distinguere più destinatari, ad esempio: <code>recipient-email1</code> , <code>recipient-ip1</code> , <code>recipient-url1</code> ; <code>recipient-email2</code> , <code>recipient-ip2</code> , <code>recipient-url2</code> ; e così via.
recipient-ipX	Indirizzo IP del destinatario, dove X è l'indice esclusivo per distinguere più destinatari. Vedere l'esempio riportato sopra.
recipient-urlX	URL del destinatario, dove X è l'indice esclusivo per distinguere più destinatari. Vedere l'esempio riportato sopra.

Tabella 55-11 Parametri di ricerca del mittente

Chiave di parametro di ricerca	Descrizione
sender-email	Indirizzo e-mail del mittente per gli incidenti di Network Prevent for Email (SMTP).
sender-ip	Indirizzo IP del mittente per gli incidenti endpoint e di rete su protocolli diversi da SMTP.
sender-port	Porta del mittente per gli incidenti di rete su protocolli diversi da SMTP.
endpoint-user-name	Utente connesso sull'endpoint quando si è verificata la violazione.
endpoint-machine-name	Nome dell'endpoint su cui risiede il file all'origine della violazione.

Tabella 55-12 Parametro di ricerca del server

Chiave di parametro di ricerca	Descrizione e commenti
server-name	Nome del server di rilevamento che ha segnalato l'incidente. Questo nome è definito dall'utente e viene immesso quando viene distribuito il server di rilevamento. Ad esempio: server-name=My Network Monitor.

Tabella 55-13 Parametri di ricerca del monitoraggio

Chiave di parametro di ricerca	Descrizione
monitor-name	Nome del server di rilevamento che ha segnalato l'incidente. Questo nome è definito dall'utente e viene immesso quando viene distribuito il server di rilevamento. Ad esempio: server-name=My Network Monitor.
monitor-host	Indirizzo IP del server di rilevamento che ha segnalato l'incidente. Ad esempio: monitor-host=127.0.0.1
monitor-id	Identificatore numerico definito dal sistema del server di rilevamento. Ad esempio: monitor-id=1.

Tabella 55-14 Parametro di ricerca dello stato

Chiave di parametro di ricerca	Descrizione e commenti
incident-status	Stato corrente dell'incidente. Ad esempio: incident-status=incident.status.New.

Tabella 55-15 Parametri di ricerca dell'ACL

Chiave di parametro di ricerca	Descrizione
acl-principalX	Stringa che indica l'utente o il gruppo a cui si applica l'ACL.
acl-typeX	Stringa che indica se l'ACL si applica al file o alla condivisione.
acl-grant-or-denyX	Stringa che indica se l'ACL concede o rifiuta l'autorizzazione.
acl-permissionX	Stringa che indica se l'ACL denota l'accesso in lettura o scrittura.

Attivazione dei plug-in di ricerca

Per attivare un plug-in di ricerca, è necessario cambiarne lo stato da **Disattivato**, ovvero lo stato iniziale del plug-in dopo che è stato configurato, a **Attivato**. I plug-in di ricerca vengono attivati nella schermata **Sistema > Dati incidente > Plug-in di ricerca > Modifica catena di plug-in**.

Vedere ["Informazioni sulla distribuzione di plug-in"](#) a pagina 1732.

Per attivare un plug-in di ricerca

- 1 Accedere a **Sistema > Dati incidente > Plug-in di ricerca** nella console di amministrazione di Enforce Server.
- 2 Fare clic su **Modifica catena di plug-in** nella **Pagina elenco plug-in di ricerca**.
- 3 Nel campo **Azioni dedicate**, selezionare l'opzione **Attivato**.
- 4 Fare clic su **Salva** per applicare la configurazione.

Se il plug-in non può essere caricato, il sistema segnalerà un errore e lo stato del plug-in rimarrà **Disattivato**. In questo caso, verificare il file di registro Tomcat più recente per informazioni sull'errore.

Vedere ["Risoluzione dei problemi relativi ai plug-in di ricerca"](#) a pagina 1743.

Concatenamento dei plug-in di ricerca

In **Sistema > Dati incidente > Plug-in di ricerca > Modifica catena di esecuzione plug-in di ricerca** è possibile attivare i plug-in di ricerca e specificare l'ordine di esecuzione quando vengono distribuiti più plug-in di ricerca.

Vedere ["Attivazione dei plug-in di ricerca"](#) a pagina 1742.

Se si attivano più plug-in di ricerca, è necessario specificare l'ordine di esecuzione. Quando i plug-in sono concatenati, i plug-in di ricerca successivi utilizzano come attributi l'input di un plug-in precedente.

Vedere ["Informazioni sulla distribuzione di plug-in"](#) a pagina 1732.

Per concatenare più plug-in di ricerca

- 1 Accedere a **Sistema > Dati incidente > Plug-in di ricerca** nella console di amministrazione di Enforce Server.
- 2 Fare clic su **Modifica catena di plug-in** in **Pagina elenco plug-in di ricerca**.
- 3 Nel campo **Sequenza di esecuzione** selezionare l'ordine di esecuzione dal menu a discesa.
- 4 Fare clic su **Salva** per applicare la configurazione di concatenamento.

Ricaricamento dei plug-in di ricerca

Se si è modificata la configurazione di un plug-in di ricerca o i dati esterni sono cambiati, è necessario ricaricare i plug-in di ricerca. Il ricaricamento dei plug-in aggiorna il sistema, esegue automaticamente le ricerche attivate in ordine e inserisce gli attributi dell'incidente man mano che gli incidenti vengono rilevati.

Oltre a ricaricare i plug-in in caso di modifica, è possibile che sia necessario ricaricare i plug-in di ricerca se una delle condizioni seguenti è vera:

- Un plug-in presentava dei problemi e il sistema lo ha scaricato, ma ora il problema è risolto.
- La rete non funzionava o era scollegata per lo stesso motivo, ma ora funziona correttamente.
- Un plug-in archivia i dati in una cache e si desidera aggiornare la cache manualmente.

Per ricaricare i plug-in di ricerca

- 1 Accedere a **Sistema > Dati incidente > Plug-in di ricerca** nella console di amministrazione di Enforce Server.
- 2 Fare clic su **Ricarica plug-in** per ricaricare tutti i plug-in attivati.

Nota: gli amministratori possono inoltre ricaricare i plug-in di ricerca dalla scheda **Attributi personalizzati** nella schermata **Sistema > Dati incidente > Attributi**.

Risoluzione dei problemi relativi ai plug-in di ricerca

Symantec Data Loss Prevention restituisce messaggi di registrazione e di errore specifici dei plug-in di ricerca. Gli errori più comuni comprendono il mancato caricamento di un plug-in a causa di una o più configurazioni errate. Se un plug-in di ricerca non viene caricato, l'eccezione viene registrata come avviso nella schermata degli eventi del sistema e nel registro di Tomcat. Inoltre la catena di esecuzione dei plug-in e delle mappe di attributi viene registrata nel registro di Tomcat.

Per correggere gli errori relativi ai plug-in di ricerca

- 1 Accedere alla schermata **Sistema > Server e rilevatori > Panoramica** e cercare eventuali avvisi nella tabella **Recent Error and Warning Events** nella parte inferiore della pagina.
- 2 Sull'host di Enforce Server aprire il file di registro `c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\protect\Enforce\logs\tomcat\localhost.<date>.log` (Windows) o `/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/tomcat/localhost.<date>.log` (Linux).
- 3 Correggere gli errori visualizzati nel file di registro dell'host locale di Tomcat.
[Tabella 55-16](#)
- 4 Configurare la registrazione dettagliata per i plug-in di ricerca se il plug-in restituisce errori ma questi non vengono registrati.
Vedere ["Configurazione della registrazione dettagliata per i plug-in di ricerca"](#) a pagina 1744.
- 5 Per i plug-in specifici fare riferimento agli argomenti relativi alla risoluzione dei problemi.
Vedere ["Test e risoluzione dei problemi del plug-in di ricerca CSV"](#) a pagina 1753.
Vedere ["Test e risoluzione dei problemi dei plug-in di ricerca LDAP"](#) a pagina 1760.
Vedere ["Esercitazione del plug-in di ricerca Script"](#) a pagina 1770.

Tabella 55-16 Risoluzione dei problemi relativi ai plug-in di ricerca

Problema	Soluzione
Impossibile caricare il plug-in di ricerca	<p>Se il plug-in non viene caricato, cercare un messaggio nel file di registro simile al seguente:</p> <pre>SEVERE [com.vontu.enforce.workflow.attributes.AttributeLookupLoader] Error loading plugin [<Plugin_Name>]</pre> <p>Considerare la sezione Causa che segue questo tipo di messaggio di errore. Voci di questo tipo spiegano perché non è stato possibile caricare il plug-in.</p>
Impossibile inserire gli attributi in seguito alla ricerca	<p>Se il plug-in viene caricato, ma gli attributi non vengono inseriti, cercare la mappa degli attributi nel registro. Verificare che i valori vengano inseriti, compresi i parametri di ricerca attivati. A questo scopo cercare una chiave di parametro di ricerca attivata, ad esempio <code>sender-email</code>.</p>

Configurazione della registrazione dettagliata per i plug-in di ricerca

Il sistema fornisce una configurazione della registrazione dettagliata per i plug-in di ricerca. È possibile configurare i livelli di registrazione per i plug-in di ricerca nella tabella **Sistema >**

Registri > Configurazione. La configurazione dei registri per i plug-in di ricerca fornisce messaggi di registro più dettagliati nel registro localhost Tomcat.

Vedere ["Risoluzione dei problemi relativi ai plug-in di ricerca"](#) a pagina 1743.

Per configurare e raccogliere i registri per i plug-in di ricerca

- 1 Accedere alla schermata **Sistema > Server e rilevatori > Registri**.
- 2 Selezionare la tabella **Configurazione**.
- 3 In **Enforce Server**, selezionare la voce `Custom Attribute Lookup Logging` nel menu a discesa **Impostazione di registrazione diagnostica**.
- 4 Fare clic su **Configura registri**.
- 5 Nella scheda **Aggregazione** selezionare i registri di debug e traccia seguenti per Enforce Server.
- 6 Fare clic su **Raccogli registri**.
- 7 In fondo alla pagina, fare clic su **Scarica** per scaricare i registri. Utilizzare il pulsante **Aggiorna** per aggiornare la pagina. I registri vengono compressi in un file ZIP.
- 8 Aprire il file ZIP o salvarlo nel file system, quindi estrarlo.
- 9 Andare alla directory `c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs\tomcat` (**Windows**) o `/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/tomcat` (**Linux**).
- 10 Aprire il file `localhost.<date>.log` in un editor di testo. Aprire il file con la data più recente.
- 11 Cercare il nome del plug-in di ricerca. Verranno visualizzati vari messaggi.
- 12 Se necessario, verificare le proprietà di registrazione plug-in di ricerca nel file `ManagerLogging.properties` della directory `config`.

```
com.vontu.logging.ServletLogHandler.level=FINEST
com.vontu.enforce.workflow.attributes.CustomAttributeLookup.level=FINEST
com.vontu.lookup.level=FINEST
```

Configurazione di proprietà di plug-in avanzate

Il file `Plugins.properties` nella directory `config` (`\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config`) [**Windows**] o

`/opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config` [**Linux**])

contiene numerose proprietà avanzate per la configurazione dei plug-in di ricerca. Queste proprietà non devono essere modificate a meno che non sia necessario in base alle seguenti descrizioni.

Tabella 55-17 Proprietà avanzate per i plug-in di ricerca

Proprietà	Predefinito	Descrizione
AttributeLookup. output.parameters	<i>data-owner-name, data-owner-email</i>	<p>La proprietà dei parametri di output di ricerca attribuiti è un elenco separato da virgole che specifica quali parametri possono essere modificati tramite plug-in di ricerca. Solitamente, i valori per le chiavi dei parametri di ricerca vengono impostati dal sistema quando viene creato un incidente. Poiché questi parametri vengono utilizzati per cercare i valori di attributi personalizzati, non sono modificati dai valori ricercati sono diversi dai valori definiti dal sistema.</p> <p>Tuttavia, questa proprietà consente di modificare l'output degli attributi Nome proprietario dati e E-mail proprietario dati in base ai valori recuperati. Questi parametri vengono specificati nelle configurazioni e negli script dei plug-in di ricerca che utilizzano la stessa sintassi come attributi personalizzati. Entrambi gli attributi vengono attivati selezionando il gruppo di attributi Incidente.</p> <p>È possibile disattivare questa funzionalità rimuovendo una o entrambe le voci. Se rimosse, l'output per un parametro non viene modificato da un valore cercato.</p>
AttributeLookup.timeout	<i>60000</i>	<p>Per evitare un blocco di sistema a causa di problemi di ricerca imprevisti, l'Enforce Server limita il tempo assegnato a ogni plug-in di ricerca. Questo timeout è configurato nella <code>properties.com.vontu.api.incident.attributes.AttributeLookup.timeout</code> nel file <code>Plug-ins.properties</code>.</p> <p>Se una ricerca supera il timeout predefinito di 60 secondi, la struttura di attributi di incidenti scarica dalla memoria il plugin associato. Se è presente una ricerca in esecuzione, l'Enforce Server non può eseguire quella specifica ricerca per alcun incidente seguente. Se il plug-in supera il tempo impostato di frequente, è possibile estendere il timeout modificando il periodo (in millisecondi).</p> <p>Nota: Notare che se si aumenta questo valore è possibile che rallentino i tempi di elaborazione degli incidenti a causa di ricerche attributi più lente.</p>

Proprietà	Predefinito	Descrizione
<code>AttributeLookup.auto</code>	<i>true</i>	<p>La proprietà di ricerca automatica specifica se la ricerca deve essere avviata automaticamente quando viene rilevato un nuovo incidente. Questa proprietà popola automaticamente gli attributi di incidente tramite i plug-in di ricerca distribuiti dopo l'esecuzione della ricerca iniziale.</p> <p>Non è possibile disattivare il plug-in di ricerca automatica modificando il valore di proprietà in <i>false</i>. Se questa proprietà viene disattivata, i risolutori devono fare clic su Ricerca per ogni incidente.</p> <p>Dopo l'impostazione della <code>AttributeLookup.auto</code> proprietà su <i>false</i>, riavviare il servizio Symantec DLP Incident Persister. Se non si riavvia il servizio gli attributi personalizzati continueranno a essere popolati automaticamente.</p>
<code>AttributeLookup.reload</code>	<i>false</i>	<p>La proprietà di ricarica del plug-in automatico specifica se tutti i plug-in devono essere ricaricati automaticamente ogni giorno alle 3:00. Impostare la proprietà su <i>true</i> per attivarla.</p>

Configurazione del plug-in di ricerca CSV

È possibile configurare solo un plug-in di ricerca CSV per ogni istanza di Enforce Server.

Vedere ["Informazioni sul plug-in di ricerca CSV"](#) a pagina 1729.

Tabella 55-18 Configurazione del plug-in di ricerca CSV

Passaggio	Azione	Descrizione
1	Creare attributi personalizzati.	<p>Definire gli attributi personalizzati per le informazioni che si desidera cercare.</p> <p>Vedere "Impostazione manuale dei valori degli attributi personalizzati" a pagina 1710.</p>
2	Creare il file origine dati CSV.	<p>Questo file CSV contiene i dati da utilizzare per inserire gli attributi personalizzati per la risoluzione di un incidente.</p> <p>Vedere "Requisiti per la creazione del file CSV" a pagina 1748.</p>
3	Creare un nuovo plug-in CSV.	Vedere "Creazione di nuovi plug-in di ricerca" a pagina 1736.
4	Denominare e descrivere il plug-in.	La stringa del nome non può contenere più di 100 caratteri. Si consiglia di immettere una descrizione per il plug-in di ricerca.

Passaggio	Azione	Descrizione
5	Specificare il percorso del file.	Fornire il percorso del file CSV. Il file CSV deve essere locale su Enforce Server. Vedere "Definizione del percorso di file CSV" a pagina 1750.
6	Scegliere il delimitatore del file.	Specificare il delimitatore utilizzato nel file CSV. È consigliato il delimitatore barra verticale []. Vedere "Scelta del delimitatore di file CSV" a pagina 1750.
7	Scegliere la codifica dei file.	Esempio: UTF-8 Vedere "Selezione del set di caratteri per il file CSV" a pagina 1750.
8	Mappare gli attributi.	Mappare il sistema e gli attributi personalizzati alle intestazioni delle colonne del file CSV e definire le chiavi da utilizzare per estrarre i dati degli attributi personalizzati. Le chiavi vengono mappate alle intestazioni delle colonne, non agli attributi personalizzati. La sintassi è la seguente: <code>attr.attribute_name=column_head</code> <code>keys=column_head_first:column_head_next:column_head_3rd</code> Vedere "Mapping di attributi e chiavi di parametro a campi CSV" a pagina 1750.
9	Salvare il plug-in.	Assicurarsi che venga visualizzato il messaggio di salvataggio corretto per il plug-in.
9	Selezionare le chiavi dei parametri di ricerca.	Definire le chiavi utilizzate per estrarre i dati degli attributi personalizzati. Vedere "Selezione dei parametri di ricerca" a pagina 1737.
10	Attivare il plug-in di ricerca.	Il plug-in di ricerca CSV deve essere attivato su Enforce Server. Vedere "Attivazione dei plug-in di ricerca" a pagina 1742.
11	Risolvere i problemi relativi al plug-in.	Vedere "Test e risoluzione dei problemi del plug-in di ricerca CSV" a pagina 1753.
11	Testare il plug-in di ricerca.	

Requisiti per la creazione del file CSV

Il plug-in di ricerca CSV richiede un file CSV memorizzato in Enforce Server.

Durante la creazione di un file CSV, tenere presente i seguenti requisiti:

- La prima riga di dati del file CSV deve contenere le intestazioni di colonna.

- I campi dell'intestazione della colonna non possono essere vuoti.
- Assicurarsi che non vi sono spazi vuoti alla fine dei campi dell'intestazione delle colonne.
- Assicurarsi che tutte le righe abbiano lo stesso numero di colonne.
- Ogni riga del file deve trovarsi su una singola riga senza ritorni a capo.
- Una o più colonne nel file sono utilizzate come campi chiave per le ricerche di dati. Nel mapping degli attributi si specificano le intestazioni di colonna da utilizzare come campi chiave. Si specifica anche l'ordine di ricerca dei campi chiave. I campi chiave più comuni comprendono di solito indirizzo e-mail, Dominio\NomeUtente (per gli incidenti degli endpoint) e nome utente (per gli incidenti di archiviazione).
- I valori dei dati nelle colonne dei campi chiave devono essere univoci. Se più colonne sono utilizzate come campi chiave (ad esempio, `EMP_EMAIL` e `USER_NAME`), la combinazione di valori in ciascuna riga deve essere univoca.
- I campi nelle righe di dati (tranne la riga delle intestazioni di colonna) possono essere vuoti, ma almeno un campo chiave in ciascuna riga deve contenere dati.
- Lo stesso tipo di delimitatore deve essere utilizzato per tutti i valori nell'intestazione delle colonne e nelle righe di dati.
- Se il file CSV è di sola lettura, assicurarsi che contenga una nuova riga alla fine del file. Il sistema tenterà di aggiungere una nuova riga al file quando viene eseguito il plug-in, ma se il file è di sola lettura il sistema non può eseguire questa operazione e il plug-in non verrà caricato.
- Per gli incidenti della scansione di rilevamento, il parametro di ricerca `file-owner` non include un dominio. Per usare `file-owner` come chiave, la colonna del file CSV che corrisponde a `file-owner` deve essere nel formato `owner`. Il formato `DOMAIN\owner` non produce risultati della ricerca. Questa limitazione si applica solo agli incidenti di rilevazione, altri tipi di incidenti possono includere un dominio.
Ad esempio, la riga dell'intestazione delle colonne e la riga dei dati di un file CSV delimitato da barre verticali possono essere simili a queste:

```
email|first_name|last_name|domain_user_name|user_name|department|manager|manager_email  
jsmith@acme.com|John|Smith|CORP\jsmith1|jsmith1|Accounting|Mei Wong|mwong@acme.com
```

- Se più del 10% delle righe del file CSV violano uno dei requisiti, il plug-in non viene caricato.
- Per accuratezza nella ricerca, il file CSV deve essere tenuto aggiornato.

Vedere ["Informazioni sul plug-in di ricerca CSV"](#) a pagina 1729.

Definizione del percorso di file CSV

Per configurare il plug-in di ricerca CSV è necessario specificare la proprietà **Percorso file CSV** per la posizione del file CSV. Il file CSV deve essere memorizzato localmente in Enforce Server.

È possibile immettere un percorso di file assoluto oppure relativo. Ad esempio:

- `../../../../symantecDLP_csv_lookup_file/senders2.csv`
- `C:/SymantecDLP_csv_lookup_file/senders2.csv`

In Windows è possibile usare barre o barre rovesciate. Per esempio: `C:/Symantec/Data Loss Prevention/Enforce Server/15.1/Protect/plugins/employees.csv` o `C:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\plugins\employees.csv`. In Linux è possibile usare solo le barre.

Il sistema convalida il percorso di file quando si salva la configurazione. Se il sistema non può individuare il file, segnala un errore e non consente il salvataggio della configurazione. Assicurarsi che il file CSV non sia aperto e sia memorizzato localmente in Enforce Server.

Scelta del delimitatore di file CSV

Utilizzare la proprietà **Delimitatore** per specificare il delimitatore di file CSV.

I seguenti delimitatori sono supportati:

- Virgola
- Barra verticale
- Tabulazione
- Punto e virgola

Si consiglia di usare la barra verticale (“|”) come delimitatore. L'uso del delimitatore virgola non è consigliato perché le virgole fanno spesso parte dei dati inclusi nei campi di dati. Ad esempio, un indirizzo di recapito potrebbe contenere una virgola.

Selezione del set di caratteri per il file CSV

È necessario specificare il set di caratteri per il file CSV. L'impostazione predefinita è UTF-8.

Tutti i set di caratteri supportati sono elencati nel menu a discesa.

Mapping di attributi e chiavi di parametro a campi CSV

Per configurare il plug-in di ricerca CSV, immettere il codice di esecuzione nel campo **Mapping attributi**. Questo codice esegue il mapping degli attributi personalizzati e delle chiavi di parametro di ricerca alle intestazioni delle colonne nel file CSV. Una o più coppie

attributo=colonna sono usate per eseguire il mapping degli attributi di incidenti alle intestazioni delle colonne. La proprietà `keys` nella mappa di attributi identifica le colonne da usare per la ricerca.

Di seguito viene riportato un esempio di mapping degli attributi di file CSV:

```
attr.Store-ID=store-id
attr.Store\ Address=store_address
attr.incident-id=incident-id-key
attr.sender-email=sender-email-key
keys=sender-email-key:incident-id-key
```

Sulla base di questo esempio, aderire alle regole sintattiche esposte di seguito quando si esegue il mapping degli attributi ai dati di file CSV.

Tabella 55-19 Sintassi del mapping di attributi per file CSV

Esempio e sintassi	Descrizione
<pre>attr.Store-ID=store-id attr.attribute_name=column_head</pre>	<p>Gli attributi eseguono il mapping ai nomi delle intestazioni di colonna nelle coppie attributo-colonna.</p> <p>In questo esempio, Store-ID è un attributo personalizzato e store-id è il nome di un'intestazione di colonna nel file CSV.</p>
<pre>attr.Store\ Address=store_address attr.attribute\ name=column\ head</pre>	<p>Gli spazi sono consentiti prima e dopo il simbolo = (salvo per il plug-in di ricerca LDAP).</p> <p>Gli spazi vuoti nei nomi di colonne e attributi devono essere preceduti da una barra rovesciata.</p> <p>In questo esempio, l'attributo personalizzato è denominato Store Address.</p>
<pre>attr.Store-ID=store-id attr.Store\ Address=store_address attr.attribute_name=column_head attr.attribute_name=column_head</pre>	<p>Ogni coppia attributo-colonna è immesso su una riga distinta.</p>
<pre>attr.Store\ Address=STORE_ADDRESS</pre>	<p>Per tutta la sintassi è valida la distinzione tra maiuscole e minuscole.</p> <p>L'identificatore <code>attr.</code> deve essere minuscolo.</p> <p>Gli attributi di incidenti devono corrispondere esattamente alla stringa definita dal sistema.</p>

Esempio e sintassi	Descrizione
<pre>attr.incident-id=incident-id-key attr.sender-email=sender-email-key attr.attribute_name=column_head</pre>	Gli attributi di sistema vengono mappati ai nomi delle intestazioni di colonna. Il nome di colonna non deve corrispondere all'attributo di sistema e non richiede la parola "key".
<pre>keys=sender-email-key:incident-id-key keys=<primo_nome_colonna>:secondo_nome_colonna</pre>	Le chiavi mappano i nomi delle intestazioni di colonne alle chiavi degli attributi di incidenti che si intende usare per cercare i valori degli attributi. Le chiavi vengono mappate ai nomi delle intestazioni delle colonne, non ai nomi degli attributi di incidenti. L'ordine di visualizzazione determina la priorità. Dopo l'individuazione del primo incidente nel file CSV, gli altri attributi vengono popolati.

Esempio di mapping di attributi CSV

Ecco un altro esempio di mapping per il plug-in di ricerca CSV.

```
attr.sender-email = Email
attr.endpoint-user-name = Username
attr.file-owner = File-owner
attr.sender-ip = IP

attr.First\ Name = FIRST_NAME
attr.Last\ Name = LAST_NAME
attr.Business\ Unit = Org
attr.Manager\ Email = Mgr_email
attr.Employee\ ID = EMPLOYEE_NUMBER
attr.Phone\ Number = Phone
attr.Manager\ Last\ Name = Mgr_lastname
attr.Manager\ First\ Name = Mgr_firstname
attr.Employee\ Email = Emp_email

keys = Email:Username:File-owner:IP
```

Si noti quanto segue in questo esempio:

- Le prime quattro linee mappano i parametri di ricerca alle intestazioni di colonna.
- Le nove linee rimanenti mappano gli attributi personalizzati alle intestazioni di colonna.

- Una barra rovesciata precede ciascuna istanza di un carattere spazio in un nome attributo o colonna. In questo esempio `attr.Employee\ Email = Emp_email` mappa l'attributo personalizzato **Employee Email** all'intestazione colonna **emp_email**.
- La proprietà `keys` identifica e ordina le chiavi utilizzate per l'estrazione di dati attributo personalizzato. Le chiavi sono separate tramite due punti. L'ordine di elenco delle chiavi determina la sequenza di ricerca. In questo esempio (`keys = Email:Username:File-owner:IP`), il plug-in ricerca in primo luogo nella colonna `Email` un valore corrispondente al valore del parametro di ricerca di `sender-email` che è stato passato al plug-in stesso. Se non viene rilevato nessun valore corrispondente il plug-in ricerca nella colonna `Username` un valore corrispondente al valore di ricerca `endpoint-user-name`. Se non viene rilevato nessun valore corrispondente in tale colonna, il plug-in procede alla ricerca della chiave successiva (`File-owner`) e così via.
- Il plug-in interrompe la ricerca quando rileva la prima coppia chiave parametro-valore. Di conseguenza, l'ordine di elenco delle intestazioni colonna `keys` è importante.

Test e risoluzione dei problemi del plug-in di ricerca CSV

Se il plug-in non viene caricato o non riesce a compilare gli attributi personalizzati con i valori rilevati, eseguire la risoluzione dei problemi come segue:

Per testare e risolvere i problemi del plug-in di ricerca CSV

- 1 Verificare che il file CSV sia conforme ai requisiti. Se più del 10% delle righe del file CSV violano uno dei requisiti per i file CSV, il plug-in di ricerca non viene caricato.
Vedere ["Requisiti per la creazione del file CSV"](#) a pagina 1748.
- 2 Verificare che il delimitatore selezionato sia quello utilizzato nel file CSV. Tenere presente che l'impostazione predefinita del sistema è la virgola, mentre l'impostazione consigliata è il carattere pipe.
Vedere ["Scelta del delimitatore di file CSV"](#) a pagina 1750.
- 3 Verificare il mapping attributi. Il sistema non fornisce alcuna convalida per la mappa attributi. Verificare che la mappa attributi sia conforme alla sintassi.
Gli errori di sintassi comuni includono:
 - Ogni voce del campo di mapping attributo rileva la differenza tra maiuscole e minuscole.
 - Gli spazi nei nomi di colonna e di attributo devono essere identificati da una sbarra rovesciata.
 - Per ogni coppia attributo=colonna, i dati a destra del segno di uguale (=) devono essere un nome di intestazione colonna.
 - Le chiavi i nomi delle intestazioni colonna, non gli attributi dell'incidente.

4 Se il plug-in non si carica o non riesce a restituire i valori rilevati, controllare il file

```
c:\ProgramData\Symantec\Data Loss Prevention\Enforce
Server\Protect\logs\tomcat\localhost.<data_più_recente>.log (Windows) o
/var/log/Symantec/DataLossPrevention/Enforce
Server/15.1/tomcat/localhost.<data_più_recente>.log (Linux).
```

- Verificare che il database e la tabella siano stati creati e che il file CSV sia caricato nella tabella. Per verificare, cercare linee simili alle seguenti:

```
INFO [com.vontu.lookup.csv.CsvLookup]
creating database
create table using SQL
importing data from file into table LOOKUP having columns
```

Nota: Per l'elaborazione di file di grandi dimensioni, il plug-in di ricerca CSV utilizza un database residente in memoria (Apache Derby). In ogni Enforce Server può essere eseguita una sola istanza di Apache Derby. Se è in esecuzione un'istanza precedente, il plug-in di ricerca CSV non viene caricato. Se il database e la tabella non sono stati creati, riavviare il servizio Symantec DLP Manager e ricaricare il plug-in.

5 Se il plug-in non restituisce i valori ricercati, controllare il file

```
c:\ProgramData\Symantec\Data Loss Prevention\Enforce
Server\Protect\logs\tomcat\localhost.<data_più_recente>.log (Windows) o
/var/log/Symantec/DataLossPrevention/Enforce
Server/15.1/tomcat/localhost.<data_più_recente>.log (Linux).
```

Cercare un messaggio di avviso del tipo "La query SQL non ha restituito alcun risultato". In questo caso, assicurarsi che il mapping attributi corrisponda alle intestazioni colonna CSV e ricaricare il plug-in se sono state apportate modifiche.

Vedere ["Risoluzione dei problemi relativi ai plug-in di ricerca"](#) a pagina 1743.

Esercitazione del plug-in di ricerca CSV

Questa esercitazione fornisce le istruzioni per l'implementazione di un plug-in di ricerca CSV semplice. Lo scopo di questa esercitazione è quello di presentare la funzionalità del plug-in di ricerca secondo un approccio pratico. Se si ha esperienza nella generazione di incidenti, nella creazione di attributi personalizzati e nell'implementazione di plug-in di ricerca, questa esercitazione potrebbe essere troppo semplice.

Vedere ["Informazioni sul plug-in di ricerca CSV"](#) a pagina 1729.

Per implementare un plug-in di ricerca CSV semplice

- 1 Creare i seguenti attributi personalizzati in **Sistema > Attributi > Attributi personalizzati** :
 - **Manager**
 - **Reparto**
 - **Indirizzo e-mail**
- 2 Creare un file CSV delimitato da barre verticali che contenga i dati seguenti.

```
SENDER|MGR|DEPT|EMAIL  
emp@company.com|Merle Manager|Engineering|rmanager@company.com
```

- 3 Salvare il file CSV sulla stessa unità di volume su cui è installato Enforce Server.

Per esempio: C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\plugins\lookup\csv_lookup_file.csv.

- 4 Creare una politica di parole chiave di base.
Vedere ["Configurazione di politiche"](#) a pagina 422.
- 5 Generare un incidente e-mail.
Per avviare la ricerca per questo esempio, l'incidente deve essere un incidente SMTP in cui l'indirizzo del mittente dell'e-mail è emp@azienda.com. Cambiare il valore del mittente nel file CSV in modo che corrisponda al valore effettivo del mittente dell'e-mail.
- 6 Creare un nuovo plug-in di ricerca CSV in **Sistema > Dati incidente > Plug-in di ricerca > Nuovo plug-in**.
- 7 Configurare il plug-in di ricerca nel modo seguente:
 - Nome: *Plug-in di ricerca CSV*
 - Descrizione: *Cerca il manager del mittente dell'e-mail nel file CSV.*
 - Percorso file CSV: *C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\plugins\lookup\csv_lookup_file.csv*
 - Delimitatore: *Barra verticale [|]*
 - Codifica del file: *UTF-8*
 - Mapping attributi
Mappare gli attributi definiti dal sistema, gli attributi personalizzati e le chiavi di parametro di ricerca su righe separate nel modo seguente:

```
attr.sender-email=SENDER  
attr.Manager=MGR  
attr.Department=DEPT  
attr.Email\ Address=EMAIL  
keys=SENDER
```

<code>attr.sender-email = SENDER</code>	È una chiave di parametro di ricerca del gruppo Mittente . È mappata all'intestazione di colonna corrispondente nel file CSV.
<code>attr.Manager = MGR</code>	È un attributo personalizzato definito nel passaggio 1. È mappata all'intestazione di colonna corrispondente nel file CSV.
<code>attr.Department = DEPT</code>	È un attributo personalizzato definito nel passaggio 1. È mappata all'intestazione di colonna corrispondente nel file CSV.
<code>attr.Email\ Address = EMAIL</code>	È un attributo personalizzato delimitato da spazi definito nel passaggio 1. È mappato all'intestazione di colonna corrispondente nel file CSV.
<code>keys = SENDER</code>	Questa riga dichiara una chiave per eseguire la ricerca. La ricerca termina dopo che è stata individuata la prima chiave e vengono inseriti i valori di attributo.

- 8 Salvare la configurazione del plug-in.
- 9 Selezionare **Sistema > Plug-in di ricerca > Parametri di ricerca**, quindi selezionare il seguente gruppo di chiavi di parametro di ricerca:

Mittente	Questo gruppo contiene la chiave <code>sender-email</code> .
-----------------	--

- 10 Selezionare **Sistema > Plug-in di ricerca > Modifica catena di plug-in** e attivare il plug-in.
- 11 Aprire l' **istantanea dell'incidente** per l'incidente generato nel passaggio 4.
- 12 Verificare che gli attributi personalizzati non inseriti e creati nel passaggio 1 vengano visualizzati nel riquadro **Attributi** a destra della schermata.
In caso contrario completare il passaggio 1.
- 13 Verificare che il pulsante "Ricerca" venga visualizzato nel riquadro **Attributi** sopra gli attributi personalizzati.
In caso contrario verificare che il privilegio **Attributi di ricerca** venga concesso all'utente.
Fare clic su **Ricarica plug-in** dopo avere apportato eventuali modifiche.

14 Fare clic sul pulsante **Ricerca**.

Gli attributi personalizzati devono venire inseriti con i valori cercati e recuperati dal file CSV.

15 Risolvere i problemi relativi al plug-in in base alle esigenze.

Vedere ["Test e risoluzione dei problemi del plug-in di ricerca CSV"](#) a pagina 1753.

Configurazione dei plug-in di ricerca LDAP

Per configurare uno o più plug-in di ricerca LDAP, completare queste operazioni.

Tabella 55-20 Configurazione dei plug-in di ricerca LDAP

Passaggio	Azione	Descrizione
1	Creare attributi personalizzati.	Vedere "Configurazione di attributi personalizzati" a pagina 1709.
2	Configurare una connessione al server LDAP.	Deve essere disponibile una connessione funzionante a un server LDAP. Vedere "Requisiti per le connessioni del server LDAP" a pagina 1758. La connessione al server LDAP può essere configurata dal collegamento nel plug-in di ricerca LDAP. Vedere "Configurazione delle connessioni a server di directory" a pagina 162.
3	Creare un nuovo plug-in di ricerca LDAP.	Vedere "Creazione di nuovi plug-in di ricerca" a pagina 1736.
4	Mappare gli attributi.	Mappare gli attributi ai campi della directory LDAP corrispondenti. La sintassi è la seguente: <pre>attr.CustomAttributeName = search_base: (search_filter=\$variable\$): ldapAttribute</pre> Vedere "Mapping degli attributi ai dati LDAP" a pagina 1758. Vedere "Esempi di mapping attributi per LDAP" a pagina 1759.
5	Salvare e attivare il plug-in.	Il plug-in di ricerca LDAP deve essere attivato su Enforce Server. Vedere "Attivazione dei plug-in di ricerca" a pagina 1742.
6	Testare il plug-in di ricerca LDAP e risolvere i problemi a esso relativi.	Vedere "Risoluzione dei problemi relativi ai plug-in di ricerca" a pagina 1743.

Requisiti per le connessioni del server LDAP

Le seguenti condizioni devono essere soddisfatte affinché Symantec Data Loss Prevention stabilisca una connessione con una directory LDAP:

- La directory LDAP deve essere eseguita in un host che è accessibile a Enforce Server.
- Deve esistere un account LDAP che Symantec Data Loss Prevention può utilizzare. Questo account deve avere un accesso di sola lettura. È necessario conoscere il nome utente e la password dell'account.
- È necessario conoscere il nome di dominio completo del server LDAP (l'indirizzo IP non può essere usato).
- È necessario conoscere la porta del server LDAP che Enforce Server usa per comunicare con il server LDAP. La porta predefinita è 389.

È possibile utilizzare uno strumento di ricerca LDAP come Softerra LDAP Browser per verificare di disporre delle credenziali corrette per la connessione al server LDAP. Confermare inoltre di avere i campi appropriati definiti per popolare gli attributi personalizzati.

Vedere ["Informazioni sui plug-in di ricerca LDAP"](#) a pagina 1729.

Mapping degli attributi ai dati LDAP

Il mapping degli attributi di sistema e personalizzati ai dati LDAP viene eseguito nel campo **Mapping attributi**. Ogni mapping viene inserito su una riga distinta. L'ordine in cui queste voci di mapping vengono visualizzate non importa.

La sintassi del mapping degli attributi per i plug-in di ricerca LDAP è la seguente:

```
attr.CustomAttributeName = search_base:  
  (search_filter=$variable$):  
  ldapAttribute
```

La sintassi è descritta più dettagliatamente nella tabella seguente.

Tabella 55-21 Dettagli sulla sintassi del mapping LDAP

Elemento	Descrizione
<i>CustomAttributeName</i>	<p>Il nome dell'attributo personalizzato come definito in Enforce Server.</p> <p>Nota: Se il nome dell'attributo contiene spazi bianchi, è necessario anteporre a ogni istanza dello spazio bianco una barra rovesciata. Uno spazio bianco è uno spazio o un carattere di tabulazione. Ad esempio, è necessario immettere l'attributo personalizzato <code>Business Unit</code> come: <code>attr.Business\ Unit</code></p> <p>Vedere "Configurazione di attributi personalizzati" a pagina 1709.</p>

Elemento	Descrizione
<i>search_base</i>	Identifica la directory LDAP.
<i>search_filter</i>	Il nome dell'attributo LDAP (campo) che corrisponde al parametro di ricerca (o altra variabile) passato al plug-in da Enforce Server.
<i>variable</i>	<p>Il nome del parametro di ricerca che contiene il valore da usare come chiave per individuare i dati corretti nella directory LDAP.</p> <p>Nei casi in cui molteplici plug-in siano concatenati, il parametro potrebbe essere una variabile passata al plug-in di ricerca LDAP da un plug-in precedente.</p>
<i>ldapAttribute</i>	L'attributo LDAP il cui valore di dati viene restituito a Enforce Server. Questo valore viene utilizzato per compilare l'attributo personalizzato specificato nel primo elemento della voce.

Vedere ["Informazioni sui plug-in di ricerca LDAP"](#) a pagina 1729.

Esempi di mapping attributi per LDAP

I seguenti mapping forniscono esempi aggiuntivi di mapping attributi per i plug-in di ricerca LDAP.

Il seguente esempio di mapping attributi ricerca nella directory LDAP `hr.corp` un record con attributo `mail` il cui valore corrisponda al valore del parametro di ricerca `sender-email`. Restituisce a Enforce Server il valore dell'attributo `givenName` per tale record.

```
attr.First\ Name = dc=corp,dc=hr:(mail=$sender-email$):givenName
```

Nel seguente esempio di mapping attributi, viene inserita una riga separata per ogni attributo personalizzato che va compilato. Inoltre si noti l'uso della variabile temporanea `TempDeptCode`. Il codice reparto è necessario per ottenere il nome del reparto dalla gerarchia LDAP. Tuttavia è sufficiente archiviare come attributo personalizzato solo il nome del reparto. La variabile `TempDeptCode` viene creata a tale scopo.

```
attr.First\ Name = cn=users:(mail=$sender-email$):firstName
attr.Last\ Name = cn=users:(mail=$sender-email$):lastName
attr.TempDeptCode = cn=users:(mail=$sender-email$):deptCode
attr.Department = cn=departments:(deptCode=$TempDeptCode$):name
attr.Manager = cn=users:(mail=$sender-email$):manager
```

Test e risoluzione dei problemi dei plug-in di ricerca LDAP

Completare questi passaggi per risolvere i problemi relativi alle implementazioni dei plug-in di ricerca LDAP.

Vedere ["Informazioni sui plug-in di ricerca LDAP"](#) a pagina 1729.

Per risolvere i problemi relativi a un plug-in di ricerca LDAP

- 1 Se il plug-in non viene salvato correttamente, verificare la configurazione.

Prima di utilizzare il plug-in di ricerca LDAP, è necessario testare la connessione al server LDAP. È possibile utilizzare uno strumento di ricerca LDAP come Softerra LDAP Browser per verificare di aver definito i campi appropriati.

Vedere ["Configurazione delle connessioni a server di directory"](#) a pagina 162.
- 2 Assicurarsi che plug-in sia attivato
- 3 Assicurarsi di aver creato le definizioni degli attributi personalizzati.

In particolare, controllare il mapping degli attributi. I nomi di attributo devono essere identici.
- 4 Se sono state effettuate delle modifiche, o in caso di cambiamento delle chiavi dei parametri di ricerca, ricaricare il plug-in.

Vedere ["Ricaricamento dei plug-in di ricerca"](#) a pagina 1743.
- 5 Selezionare **Incidenti > Mostra tutti gli incidenti** per il server di rilevamento che si sta utilizzando per rilevare l'incidente.
- 6 Selezionare vari incidenti e quindi **Attributi di ricerca** dal menu a discesa **Azioni incidente**. Questa azione cerca i valori di attributo per tutti gli incidenti per quella forma di rilevamento.
- 7 Esaminare la schermata **Istantanea incidente** di un incidente. Verificare che gli attributi personalizzati **Ricerca** siano popolati con le voci recuperate dalla ricerca LDAP.
- 8 Se non sono visualizzati i valori corretti, o se per un attributo personalizzato definito non è specificato un valore, assicurarsi che non ci siano errori di connessione registrati nella scheda **Cronologia**.
- 9 Verificare il file di registro Tomcat.

Vedere ["Risoluzione dei problemi relativi ai plug-in di ricerca"](#) a pagina 1743.

Esercitazione del plug-in di ricerca LDAP

Questa esercitazione fornisce le istruzioni per l'implementazione di un plug-in di ricerca LDAP semplice.

Per implementare un plug-in di ricerca LDAP

- 1 Creare i seguenti attributi personalizzati in **Sistema > Attributi > Attributi personalizzati** :

LDAP givenName

LDAP telephoneNumber

- 2 Creare una connessione di directory per il server Active Directory in **Sistema > Impostazioni > Connessioni directory**.

Ad esempio:

- Nome host: **enforce.dlp.azienda.com**
- Porta: **389**
- DN di base: **dc=enforce,dc=dlp,dc=com**
- Crittografia: Nessuna
- Autenticazione: Autenticato
- Nome utente: **nome utente**
- Password: **password**

- 3 Provare la connessione. Il sistema indica se la connessione è stata stabilita.
- 4 Creare un nuovo plug-in LDAP in **Sistema > Plug-in di ricerca > Nuovo plug-in > LDAP**.

Nome: **Plug-in di ricerca LDAP**

Descrizione: **Descrizione del plug-in LDAP**.

- 5 Selezionare la connessione di directory creata al passaggio 2.
- 6 Mappare gli attributi ai metadati LDAP.

```
attr.LDAP\ givenName = cn=users:(|(givenName=$endpoint-user-name$)(mail=$sender-email$)(streetAddress=$discoverserver$)):givenName
attr.LDAP\ telephoneNumber = cn=users:(|(givenName=$endpoint-user-name$)(mail=$sender-email$)(streetAddress=$discoverserver$)):telephoneNumber
```

- 7 Salvare il plug-in. Assicurarsi che venga visualizzato il messaggio di salvataggio corretto per il plug-in.
- 8 Attivare le seguenti chiavi nella pagina **Sistema > Plug-in di ricerca > Parametri di ricerca**.
 - **Incidente**
 - **Messaggio**

■ Mittente

- 9 Creare un incidente che generi uno dei parametri di ricerca. Ad esempio, un incidente e-mail espone l'attributo sender-email. Nel server Active Directory devono esservi alcune informazioni corrispondenti.
- 10 Aprire **Istantanea incidente** per l'incidente.
- 11 Fare clic sul pulsante **Ricerca** e assicurarsi che gli attributi personalizzati creati al passaggio 1 vengano inseriti nel pannello corretto.

Configurazione dei plug-in di ricerca di script

Completare questi passaggi per implementare uno o più plug-in di ricerca di script per cercare informazioni esterne.

Vedere ["Scrittura di script per i plug-in di ricerca script"](#) a pagina 1763.

Tabella 55-22 Configurazione di un plug-in di ricerca di script

Passaggio	Azione	Descrizione
1	Creare attributi personalizzati.	Vedere "Configurazione di attributi personalizzati" a pagina 1709.
2	Creare lo script.	Vedere "Scrittura di script per i plug-in di ricerca script" a pagina 1763.
3	Definire le chiavi dei parametri di ricerca .	Selezionare le chiavi da utilizzare per estrarre i dati di attributo personalizzati. Vedere "Selezione dei parametri di ricerca" a pagina 1737.
4	Creare un nuovo plug-in di script.	Vedere "Creazione di nuovi plug-in di ricerca" a pagina 1736.
5	Immettere il comando script .	Questo valore è il percorso locale del motore di script eseguibile sull'host Enforce Server. Vedere "Definizione del comando script" a pagina 1764.
6	Specificare gli argomenti .	Questo valore è il percorso del file di script Python da utilizzare per la ricerca degli attributi ed eventuali argomenti della riga di comando. Iniziare il percorso dello script con l'argomento <code>-u</code> per migliorare le prestazioni della ricerca. Vedere "Definizione degli argomenti" a pagina 1765.
7	Attivare le opzioni stdin e stdout .	Attivare entrambe le opzioni per prevenire gli attacchi di iniezione dello script. Vedere "Attivazione delle opzioni stdin e stdout" a pagina 1765.

Passaggio	Azione	Descrizione
8	Facoltativamente attivare il filtro protocolli .	È possibile specificare i tipi di incidente in base al protocollo per passare i valori di attributo per eseguire una ricerca tra gli script. Vedere "Abilitazione del filtraggio del protocollo incidenti per gli script" a pagina 1766.
9	Facoltativamente attivare e crittografare le credenziali .	È possibile crittografare e passare le credenziali necessarie allo script per la connessione ai sistemi esterni. Vedere "Attivazione e crittografia delle credenziali script" a pagina 1767.
9	Salvare il plug-in.	Assicurarsi che venga visualizzato il messaggio di salvataggio corretto per il plug-in. Vedere "Creazione di nuovi plug-in di ricerca" a pagina 1736.
10	Attivare il plug-in di ricerca.	È possibile concatenare gli script insieme e con altri plug-in di ricerca.
11	Testare il plug-in di ricerca.	Testare il plug-in di ricerca. Vedere "Risoluzione dei problemi relativi ai plug-in di ricerca" a pagina 1743.

Scrittura di script per i plug-in di ricerca script

Se utilizzate il plug-in di ricerca script, è necessario scrivere uno script per estrarre dati e popolare gli attributi personalizzati per ciascun incidente. Il plug-in di ricerca script passa gli attributi agli script come coppie di valori chiave. In cambio, gli script devono produrre una serie di coppie di valori chiave per eseguire lo standard out (`stdout`). Il plug-in utilizza queste coppie di valori chiave per popolare gli attributi personalizzati.

Quando si scrivono script da utilizzare con il plug-in di ricerca script, seguire i requisiti di sintassi e le convenzioni di denominazione qui elencati, compreso il modo in cui il plug-in degli script passa gli argomenti agli script e il formato richiesto per l'output degli script.

Tabella 55-23 Convenzioni di denominazione dei plug-in degli script

Convenzione	Sintassi	Descrizione
Input	<code>attribute_name=attribute_value</code>	Il plug-in di ricerca script passa gli attributi agli script come parametri della riga di comando nella forma <code>key=value</code> .

Convenzione	Sintassi	Descrizione
Output	<code>stdout</code>	<p>Per lavorare con gli attributi del plug-in e di popolamento, gli script devono produrre una serie di coppie di valori chiave per eseguire lo standard out (<code>stdout</code>).</p> <p>I caratteri di nuova riga devono separare le coppie di valori chiave dell'output. Ad esempio:</p> <pre>host-name=mycomputer.company.corp username=DOMAIN\bsmith</pre>
codice di uscita	<code>0</code>	<p>Gli script devono uscire con un codice di uscita "0." Se gli script escono con qualunque altro codice, Enforce Server presuppone che si sia verificato un errore nell'esecuzione dello script e termina la ricerca degli attributi.</p>
gestione degli errori	<code>stderr</code> a un file	<p>Gli script non possono stampare informazioni relative a errori o debug. Reindirizzare <code>stderr</code> a un file. In Python sarebbe:</p> <pre>fsock=open("C:\error.log", "a") sys.stderr=fsock</pre>

Vedere ["Script di esempio"](#) a pagina 1771.

Definizione del comando script

Il campo **Comando script** specifica il percorso del motore di script per l'esecuzione dello script. Queste istruzioni sono specifiche di Python.

Per specificare il comando script

- 1 Se non si è già provveduto, scaricare e installare la versione 2.6 di Python sull'host di Enforce Server.
- 2 Immettere il percorso locale del file eseguibile `python.exe`.

Ad esempio:

- Windows: `c:\python26\python.exe`
- Linux: `/usr/local/bin/python`

- 3 Immettere gli **argomenti**.

Vedere ["Definizione degli argomenti"](#) a pagina 1765.

Definizione degli argomenti

Il campo **Argomenti** specifica il percorso dello script e gli eventuali argomenti aggiuntivi della riga di comando. Queste istruzioni sono specifiche per Python.

Per specificare gli argomenti

- 1 Dopo la creazione dello script, copiarlo nell'host Enforce Server o in una condivisione file accessibile da Enforce Server.
- 2 Verificare che le autorizzazioni siano impostate correttamente per la directory e lo script. Sia la directory che il file devono essere leggibili ed eseguibili dall'utente `protect`.
- 3 Inserire l'argomento `-u` nel campo **Argomento**.

Questo comando scarica completamente `stdin`, `stdout` e `stderr` dal buffer, con conseguente miglioramento delle prestazioni di ricerca.

- 4 Inserire il percorso completo del file script.

Ad esempio:

- Windows: `-u,c:\python26\scripts\ip-lookup.py`
- Linux: `-u,/opt/python26/scripts/ip-lookup.py`

Nota: Il sistema non convalida la posizione del file.

- 5 Salvare la configurazione del plug-in.

Attivazione delle opzioni `stdin` e `stdout`

Quando si configura un plug-in di ricerca Script, è possibile selezionare le opzioni **Attiva `stdin`** e **Attiva `stdout`**. Se queste opzioni sono attivate, il sistema controlla l'input e l'output dello script alla ricerca di caratteri non sicuri, quali delimitatori di comando e operatori logici che potrebbero venire sfruttati da uno shell UNIX o Windows.

Poiché si esegue lo script sull'host su cui è installato il server Enforcer, è necessario attivare entrambe le opzioni a meno che non si sia certi che lo script sia sicuro. Se attivati, i registri indicano i caratteri non validi e senza escape.

Vedere [Tabella 55-24](#) a pagina 1765.

Tabella 55-24 Caratteri non validi per i nomi di attributo

Carattere non valido	Descrizione
Stringa vuota	Le stringhe vuote non sono consentite.

Carattere non valido	Descrizione
@ . + = : / \) (- + -	Gli attributi che contengono questi caratteri vengono ignorati durante l'elaborazione se sono attivate le opzioni <code>stdin</code> e <code>stdout</code> .
\$ %	Gli attributi che contengono i caratteri \$ e % sono consentiti se questi ultimi sono preceduti da un carattere di escape barra rovesciata.

Abilitazione del filtraggio del protocollo incidenti per gli script

Se necessario, è possibile specificare i tipi di incidente (in base al protocollo) per passare i valori di attributo per eseguire una ricerca tra gli script. Se si abilita il filtraggio del protocollo, il plug-in di ricerca degli script verrà applicato a tutti gli incidenti.

Ad esempio, è possibile limitare il passaggio dei valori di attributo a quegli incidenti individuati tramite HTTP. Quando si filtra in base al protocollo, Enforce Server acquisisce comunque gli incidenti rilevati tramite altri protocolli. Tuttavia, non utilizza il plug-in di ricerca degli script per popolare tali incidenti con valori di attributo.

Per attivare il filtro protocolli

- 1 Dalla console di amministrazione di Enforce Server, accedere alla pagina **Sistema > Plug-in di ricerca > Modifica plug-in di ricerca script** nella console di amministrazione di Enforce Server.

Vedere ["Configurazione dei plug-in di ricerca di script"](#) a pagina 1762.

- 2 Nella schermata **Plug-in di ricerca script**, selezionare l'opzione **Attiva filtro protocolli**.

Questa azione visualizza tutti i protocolli disponibili per il filtraggio. Tenere presente che i protocolli sono specifici per ciascun server di rilevamento.

Nota: I protocolli di rete vengono configurati nella schermata **Sistema > Impostazioni > Protocolli**. I protocolli dell'endpoint vengono configurati nella schermata **Sistema > Agenti > Configurazione agente**. I protocolli Discover vengono configurati in **Politiche > Scansione Discover > Target di Discover**. E, una volta generato un incidente, il relativo valore di protocollo viene visualizzato nella parte superiore della schermata **Istantanea incidente**.

- 3 Specificare i protocolli che si desidera includere nella ricerca.

Se si abilita il filtro protocolli, è necessario selezionare almeno un protocollo da utilizzare come filtro.

- 4 Salvare la configurazione del plug-in.

Attivazione e crittografia delle credenziali script

Se lo script è connesso a un sistema esterno che richiede le credenziali, è possibile attivare le credenziali per lo script. Se vengono attivate le credenziali tramite l'opzione dell'interfaccia utente, è necessario sottoporle a crittografia. Symantec Data Loss Prevention fornisce l'utilità credenziale che consente di crittografare le credenziali di crittografia e utilizzarle per l'autenticazione in un'origine dati esterna.

Quando Enforce Server invoca il plug-in di ricerca script, il plug-in decrittografa qualsiasi credenziale al runtime e le passa allo script come attributi. Le credenziali sono quindi disponibili per l'utilizzo all'interno dello script. L'utilità credenziale utilizza le stesse chiavi di crittografia piattaforma utilizzate per proteggere gli account utente e le informazioni incidente all'interno del sistema Symantec Data Loss Prevention.

Vedere [Tabella 55-25](#) a pagina 1768.

Se si sceglie di utilizzare le credenziali in testo non crittografato, è necessario impostarle come hardcoded nello script. In questo caso, Enforce Server passa i valori esportati al file credenziale con testo non crittografato. Questi valori sono passati nel seguente formato: *chiave=valore*.

Tabella 55-25 Attivazione e crittografia delle credenziali

Passaggio	Azione	Descrizione
1	Creare un file testo che contiene le credenziali necessarie dallo script per accedere ai sistemi esterni appropriati.	Il formato di questo file è <i>key=value</i> , dove <i>chiave</i> è il nome della credenziale. Ad esempio: <code>username=msantos password=esperanza9</code>
2	Salvare questo file credenziale nel file system locale su Enforce Server.	Il file deve essere salvato in Enforce Server temporaneamente. Ad esempio: <code>C:\temp\MyCredentials.txt</code> .
3	Su Enforce Server, aprire una shell dei comandi o un prompt dei comandi e modificare le directory in <code>\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\bin</code> .	Questa directory su Enforce Server contiene l'utilità di generazione credenziale.
4	Pubblicare un comando per generare un file credenziali crittografato.	La sintassi di comando è la seguente: <code>CredentialGenerator.bat in-cleartext-filepathout-encrypted-filepath</code> Ad esempio, in Windows, pubblicare quanto segue: <code>CredentialGenerator.bat C:\temp\MyCredentials.txt C:\temp\MyCredentialsEncrypted.txt</code> È possibile aprire questo file in un editor di testo per verificarne la crittografia.
5	Selezionare Abilita credenziali .	Nella pagina Sistema > Plug-in di ricerca > Modifica plug-in di ricerca script , selezionare l'opzione Abilita credenziali .
6	Immettere il Percorso file di credenziali .	Immettere il percorso completo del file credenziali crittografato. Ad esempio: <code>C:\temp\MyCredentialsEncrypted.txt</code> .
7	Salvare il plug-in.	È ora possibile utilizzare le credenziali crittografate per l'autenticazione in un sistema esterno.

Passaggio	Azione	Descrizione
8	Proteggere il file credenziali con testo non crittografato.	Se si desidera salvare il file credenziali con testo non crittografato, spostarlo in una posizione sicura. Può essere utile per salvare il file se si desidera aggiornarlo e sottoporlo nuovamente a crittografia in seguito. Se non si desidera salvare il file, eliminarlo ora.
9	Ricaricare il plug-in di ricerca.	Vedere "Gestione e configurazione dei plug-in di ricerca" a pagina 1735.

Concatenamento di più plug-in di ricerca script

Tutti i plug-in di ricerca ricevono un riferimento alla stessa mappa attributi. Tale riferimento consente di concatenare i plug-in di ricerca. La necessità di concatenazione dei plug-in per la compilazione degli attributi personalizzati varia a seconda delle circostanze. Considerare i seguenti scenari di esempio.

L'ottenimento della chiave corretta per gli incidenti della posta elettronica di rete è in genere un'operazione semplice. L'indirizzo e-mail del mittente del messaggio viene acquisito automaticamente come parametro di ricerca `sender-email`. Tale parametro di ricerca può essere utilizzato come chiave per sbloccare le informazioni sul mittente archiviate in un'origine esterna. In questa istanza non è necessario concatenare più plug-in.

Per gli incidenti FTP o Web, può essere necessario un concatenamento di plug-in. Il parametro di ricerca acquisito per questo tipo di incidenti è l'indirizzo IP degli host di origine. Tuttavia gli indirizzi IP non sono in genere identificatori statici come gli indirizzi e-mail. Di conseguenza, può essere necessario eseguire più ricerche per ottenere un identificatore statico utilizzabile come chiave di informazioni.

È possibile creare uno script per passare il parametro di ricerca `sender-ip` a un server DNS al fine di ottenere il nome host. È quindi possibile creare un altro script per passare il nome host a un sistema di gestione risorse. Dal sistema di gestione risorse è possibile ottenere il nome utente o l'e-mail della persona che usa il computer. Tale nome utente e-mail può quindi essere usato come "chiave" per sbloccare il resto dei dati. Questa catena di plug-in avrebbe tre collegamenti:

1. Il plug-in di ricerca script che utilizza l'indirizzo IP per restituire il nome host.
2. Il plug-in di ricerca script che utilizza il nome host per restituire il nome o l'e-mail dell'utente.
3. Il plug-in di ricerca CSV che utilizza il nome o l'e-mail dell'utente per restituire gli altri dati attributo personalizzati.

In questo esempio, è necessario creare una nuova variabile temporanea `Host_Name` per archiviare le informazioni nome host. La variabile temporanea e il suo valore sono quindi disponibili al secondo script e ai plug-in successivi.

Esercitazione del plug-in di ricerca Script

Completare l'esercitazione seguente per implementare un plug-in di ricerca Script. In questa esercitazione si presuppone che l'utente abbia dimestichezza con l'implementazione di plug-in di ricerca. Per raggiungere questa familiarità, completare l'"Esercitazione del plug-in di ricerca CSV".

Vedere ["Esercitazione del plug-in di ricerca CSV"](#) a pagina 1754.

Per implementare un plug-in di ricerca Script

- 1 Scaricare e installare Python 2.6 sul sistema su cui è installato Enforce Server.
Ad esempio: `C:\python26`.
- 2 Copiare lo script di esempio fornito in questo capitolo in un file di testo e salvarlo in una directory sull'host di Enforce Server come `Script-Plug-In.py`.
Ad esempio: `C:\python26\scripts\Script-Plug-In.py`.
Vedere ["Script di esempio"](#) a pagina 1771.
- 3 Aprire questo script in un IDE Python, come l'IDE Wing (disponibile all'indirizzo <http://www.wingware.com/>).
- 4 Esaminare i commenti nello script ed eseguirlo.
 - Immettere un commento per la riga 18.
 - Eseguire lo script. Viene restituito "Script-attribute=script value".
 - Annullare il commento per la riga 18 in modo che non venga elaborata.
- 5 Creare l'attributo personalizzato seguente: `Script-attribute`.
- 6 Selezionare **Nuovo plug-in > Script** per creare un nuovo plug-in di ricerca Script.
Vedere ["Creazione di nuovi plug-in di ricerca"](#) a pagina 1736.
- 7 Configurare il plug-in di ricerca Script.
Utilizzare i parametri seguenti:
 - **Comando script** : `C:\python26\python.exe`
 - **Argomenti** : `-u,C:\python26\scripts\Script-Plugin.py`
- 8 Salvare il plug-in e assicurarsi che venga caricato correttamente come indicato dal messaggio di sistema.
- 9 Attivare i parametri di ricerca seguenti: **Incidente**, **Messaggio** e **Mittente**.
- 10 Generare un incidente che trasferisca l'attributo `date-sent`.
- 11 Accedere a Istantanea incidente per il nuovo incidente e fare clic su **Ricerca**.

- 12 Verificare che l'attributo personalizzato `Script-attribute` sia impostato sul valore `script value`.
- 13 Se l'attributo personalizzato non è popolato, controllare il file di registro
`c:\ProgramData\Symantec\Data Loss Prevention\Enforce
Server\Protect\logs\tomcat\localhost.<data_più_recente>.log` (Windows) o
`/var/log/Symantec/DataLossPrevention/Enforce
Server/15.1/tomcat/localhost.<data_più_recente>.log` (Linux).

Se `Script-attribute=null`, controllare lo script. Esaminare i commenti nello script fornito e assicurarsi che non vi siano spazi tra la coppia attributo=valore.

Vedere ["Risoluzione dei problemi relativi ai plug-in di ricerca"](#) a pagina 1743.
- 14 Esplorare attivando le proprietà opzionali per il plug-in di ricerca Script, tra cui `stdin/stdout`, il filtro del protocollo e le credenziali.

Vedere ["Attivazione delle opzioni `stdin` e `stdout`"](#) a pagina 1765.

Vedere ["Abilitazione del filtraggio del protocollo incidenti per gli script"](#) a pagina 1766.

Vedere ["Concatenamento di più plug-in di ricerca script"](#) a pagina 1769.

Script di esempio

Il seguente script è fornito come esempio del Plug-in di ricerca script. È scritto nel linguaggio Python 2.6 e ha lo scopo di fornire un esempio funzionale di base per la creazione di script in Python utilizzabili per Plug-in di ricerca script.

Lo script contiene la chiave parametro di ricerca `date-sent` e restituisce "script value" per l'attributo personalizzato `Script-attribute`.

Vedere ["Esercitazione del plug-in di ricerca Script"](#) a pagina 1770.

Nota: Poiché Python ha requisiti di ritorno a capo vincolanti, se si copia e incolla questo script di esempio potrebbe risultare necessario riformattarlo in modo che appaia esattamente come mostrato qui.

```
__name__ = "__main__"

import sys, os, traceback
import commands

# Switch this to 0 when in production mode.
debugMode = 1

def main(args):

    try:

        attributeMap = parseInput(args)

        # This is the lookup parameter key.
        # Comment-out this line for testing the script standalone.
        dateSent = attributeMap["date-sent"]

        # "Script-attribute" is the custom attribute.
        # "script value" is the return value.
        # You cannot have a space between the custom attribute and the
        # attribute value. For example, "Script-attribute = script value"
        # Does not work for Script Lookup Plugins.
        print "Script-attribute=script value"
        return

    except:
        error()
        print "something went wrong!"
        return "something went wrong!"

def parseInput(args):

    # Input data is a list of key value pairs seperated by carriage return
    # Create a python dictionary to create the attribute map
    attributeMap = {}
    delimiter = "="
    for item in args:
        if delimiter in item:
            tuple = item.split(delimiter)
            attributeMap[tuple[0]] = tuple[1]
    return attributeMap

def error():
    # "SCRIPT PROCESSING ERROR"
    if(debugMode):
```



```
#print "Script Processing Error"
    traceback.print_exc(file=sys.stdout)
    return ""

#-----
# DOS-style shells (for DOS, NT, OS/2):
#-----
def getstatusoutput(cmd):
    """ Return (status, output) of executing cmd in a
        shell."""

    pipe = os.popen(cmd + ' 2>&1', 'r')
    text = pipe.read()
    sts = pipe.close()
    if sts is None: sts = 0
    if text[-1:] == '\n': text = text[:-1]
    return sts, text

#-----
# Entry Point
#-----

if __name__ == "__main__":

    if(len(sys.argv) == 0):
        error()
    else:
        main(sys.argv)
```

Configurazione dei plug-in di ricerca personalizzati (precedenti) migrati

Questi passaggi presuppongono che siano presenti plug-in di ricerca Java personalizzati distribuiti in una versione precedente a 12.0 di Symantec Data Loss Prevention e di aver aggiornato il sistema a Symantec Data Loss Prevention versione 15.1. In questo caso un plug-in di ricerca Java personalizzato verrà migrato a un plug-in di ricerca personalizzato (precedente) e sarà visualizzato nell'interfaccia utente per la verifica e il test.

Vedere ["Informazioni sui plug-in di ricerca \(precedenti\) personalizzati"](#) a pagina 1730.

Tabella 55-26 Implementazione di plug-in di ricerca personalizzati (precedenti)

Passaggio	Azione	Descrizione
1	Creare attributi personalizzati.	Creare attributi personalizzati di cui il plug-in di ricerca personalizzato (precedente) recupererà i valori. Vedere "Informazioni sull'uso di attributi personalizzati" a pagina 1708.
2	Modificare il plug-in personalizzato (precedente).	Un upgrade riuscito deve importare il plug-in di ricerca personalizzato (precedente) nell'interfaccia utente in cui è possibile attivarlo. È possibile aggiornare il nome e la descrizione se necessario. Vedere "Creazione di nuovi plug-in di ricerca" a pagina 1736.
3	Verificare la classe di plug-in .	Dopo l'upgrade, il nome della classe deve essere popolato a partire dal file <code>Plugins.properties</code> .
4	Verificare i file JAR obbligatori .	Dopo l'upgrade, i file JAR precedentemente copiati in Enforce Server devono essere visualizzati in questo campo.
5	Attivare il plug-in.	Attivare il plug-in. Vedere "Attivazione dei plug-in di ricerca" a pagina 1742.
6	Attivare le chiavi di ricerca dei parametri.	Selezionare le chiavi per avviare la ricerca degli attributi. Vedere "Selezione dei parametri di ricerca" a pagina 1737.
7	Creare una politica e generare un incidente del tipo previsto dal plug-in.	Ad esempio, creare una politica con parola chiave e generare un incidente di rete SMTP che passa l'attributo <code>sender-name</code> .
8	Verificare che gli attributi personalizzati siano aggiornati.	Verificare gli attributi popolati in Istantanea incidente . Vedere "Risoluzione dei problemi relativi ai plug-in di ricerca" a pagina 1743.

Controllo e prevenzione di perdita di dati nella rete

- [Capitolo 56. Implementazione di Network Monitor](#)
- [Capitolo 57. Implementazione di Network Prevent for Email](#)
- [Capitolo 58. Implementazione di Network Prevent for Web](#)

Implementazione di Network Monitor

Il capitolo contiene i seguenti argomenti:

- [Implementazione di Network Monitor](#)
- [Informazioni sul supporto IP v6 per Network Monitor](#)
- [Scelta di un metodo di acquisizione dei pacchetti di rete](#)
- [Informazioni sull'installazione e sulla configurazione di software di acquisizione dei pacchetti](#)
- [Configurazione del server Network Monitor](#)
- [Attivazione dell'elaborazione GET con Network Monitor](#)
- [Creazione di una politica per Network Monitor](#)
- [Test di Network Monitor](#)

Implementazione di Network Monitor

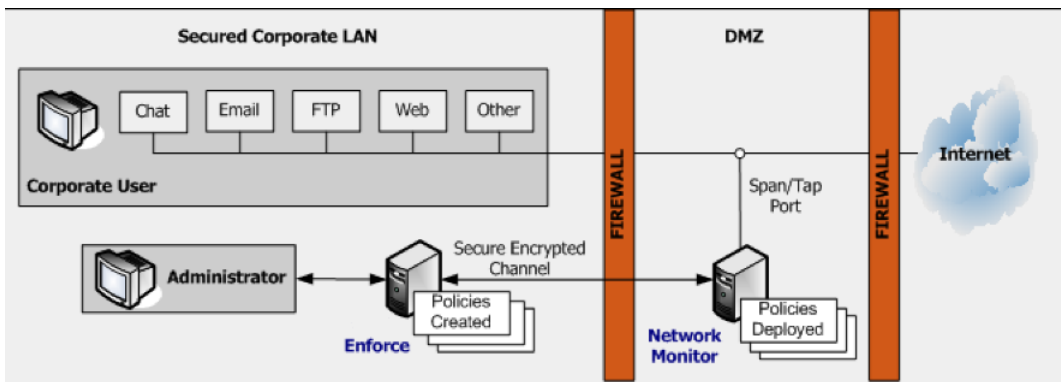
Network Monitor acquisisce e analizza il traffico nella rete, rilevando dati riservati e metadati di traffico significativi sui protocolli specificati. Ad esempio, SMTP, FTP, HTTP e diversi protocolli di messaggistica istantanea. È possibile configurare un Network Monitor Server per monitorare i protocolli personalizzati e utilizzare diversi filtri (per protocollo) per filtrare il traffico a basso rischio.

Per monitorare il traffico di rete, un Network Monitor Server necessita di:

- Uno Switch Port Analyzer di rete (SPAN) o un network tap per acquisire il traffico sulla rete target.

- Una scheda sull'host Network Monitor Server per acquisire il traffico di rete acquisito dallo SPAN o dal tap. È possibile utilizzare una scheda di interfaccia di rete (NIC) o la scheda di acquisizione pacchetti ad alta velocità (Endace o Napatech). (Notare che oltre a questa scheda di acquisizione del traffico è richiesto un NIC separato per la comunicazione tra il Network Monitor Server e Enforce Server. A questo fine è necessario utilizzare WinPcap).
- Software acquisizione pacchetti. Quando si utilizza un NIC per l'acquisizione di pacchetti, il software di acquisizione pacchetti deve essere installato sul Network Monitor Server. Quando si utilizza una scheda di acquisizione pacchetti ad alta velocità (Endace o Napatech), essa deve utilizzare il driver corretto.
Vedere ["Scelta di un metodo di acquisizione dei pacchetti di rete"](#) a pagina 1779.

Figura 56-1 Una configurazione di Network Monitor di base



Per implementare l'acquisizione pacchetti e configurare un Network Monitor, eseguire le seguenti operazioni di alto livello:

- 1 Installare e configurare il network tap o SPAN che acquisisce il traffico di rete.
- 2 Scegliere un metodo di acquisizione del traffico di rete.
Vedere ["Scelta di un metodo di acquisizione dei pacchetti di rete"](#) a pagina 1779.
- 3 Installare l'opportuno NIC o scheda di acquisizione pacchetti ad alta velocità (Endace o Napatech) sul Network Monitor come descritto nella documentazione della scheda. Utilizzare anche l'appropriato *Manuale di installazione di Symantec Data Loss Prevention* (Windows o Linux). Questo NIC o scheda di acquisizione pacchetti ad alta velocità (Endace o Napatech) deve funzionare in modalità promiscua affinché tutto il traffico in entrata e in uscita venga inoltrato tramite questa porta.

Per ulteriori informazioni sui NIC e sulle schede di acquisizione pacchetti ad alta velocità supportati, consultare la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*.

- 4 Su una piattaforma Windows, installare WinPcap se non è già installato.
Vedere ["Installazione di WinPcap su una piattaforma Windows"](#) a pagina 1781.
- 5 Se necessario, aggiornare il driver per la scheda di acquisizione pacchetti ad alta velocità.
Vedere ["Aggiornamento del driver delle schede Endace"](#) a pagina 1781.
- 6 Disattivare l'offload di checksum per il NIC utilizzato per monitorare il traffico di rete. Per le piattaforme Linux, utilizzare i seguenti comandi per disattivare l'offload di checksum per i dati ricevuti e trasmessi sull'interfaccia `eth0`:

```
ethtool -K eth0 tx off  
ethtool -K eth0 rx off
```

Per visualizzare lo stato corrente dell'offload del checksum, utilizzare il comando `ethtool -k eth0`.

Nota: Alcuni algoritmi di checksum funzionano modificando pacchetti di rete e aggiungendo checksum vuoti. A causa dei checksum vuoti alcuni driver di acquisizione di rete potrebbero eliminare i pacchetti e in tal caso essi non verrebbero valutati da Network Monitor.

- 7 Utilizzare un analizzatore di protocolli come Wireshark per convalidare il traffico sul tap o SPAN che viene indirizzato sul NIC o sulla scheda di acquisizione pacchetti ad alta velocità (Endace o Napatech).
- 8 Configurare il Network Monitor Server.
Vedere ["Configurazione del server Network Monitor"](#) a pagina 1787.
- 9 Creare e distribuire una politica di test per Network Monitor.
Vedere ["Creazione di una politica per Network Monitor"](#) a pagina 1789.
- 10 Verificare il sistema generando un incidente rispetto alla politica di test.
Vedere ["Test di Network Monitor"](#) a pagina 1790.

Informazioni sul supporto IP v6 per Network Monitor

Symantec Data Loss Prevention supporta il monitoraggio delle reti IPv4 pure, delle reti dual stack (IPv4 e IPv6) o delle reti IPv6 pure. La console di amministrazione di Enforce Server supporta gli ingressi e i reporting di entrambi gli indirizzi IPv4 e IPv6 per Network Monitor. Il supporto al monitoraggio delle reti Ipv6 si limita alle implementazioni di Network Monitor e non include supporto per gli altri prodotti Symantec Data Loss Prevention.

Di seguito è riportata una panoramica del supporto specifico per IPv6 in Symantec Data Loss Prevention:

- L'installazione di un server Network Monitor capace di monitorare le reti IPv6 o dual stack è uguale a quella utilizzata per un server Network Monitor che monitora una rete IPv4.
- I requisiti hardware e del sistema operativo sono gli stessi del Network Monitor IPv4. Per ulteriori informazioni sulla compatibilità con software e hardware di terzi, consultare la *Guida ai requisiti di sistema di Symantec Data Loss Prevention*.
- I tipi di dati dell'indirizzo IP possono supportare anche indirizzi IPv4 o IPv6.
- Gli incidenti sulla rete possono includere indirizzi IPv6.
- Le definizioni del protocollo di rete possono includere indirizzi IPv6.

Il supporto IPv6 Symantec Data Loss Prevention si limita al monitoraggio. La console di amministrazione di Enforce Server deve ancora essere distribuita su una rete IPv4; il supporto non è previsto per le funzionalità di comando e controllo sulla rete IPv6.

Questa versione non include supporto per:

- Distribuzione di Symantec Data Loss Prevention sulle reti IPv6
- Supporto degli altri server Symantec Data Loss Prevention sulle reti IPv6
- Utilizzo degli identificatori di dati definiti dal sistema IPv6
- Utilizzo della frammentazione IP sulla rete IPv6
- Configurazione o comunicazione con i server di rilevazione sulla rete IPv6
- Distribuzione degli endpoint IPv6
- Distribuzione di Symantec Encryption Server sulla rete IPv6
- Distribuzione del database di Oracle su connessione IPv6

Vedere *Configura protocollo* nella guida in linea per ulteriori informazioni sui dettagli di implementazione del supporto IPv6.

Scelta di un metodo di acquisizione dei pacchetti di rete

È possibile utilizzare tre metodi differenti per acquisire il traffico di rete che passa da uno SPAN o un tap:

- NIC su piattaforma Windows. Le piattaforme Windows che utilizzano un NIC per l'acquisizione di pacchetti necessitano di una libreria WinPcap sull'host di Network Monitor Server. Se WinPcap non è già presente sull'host di Network Monitor Server, è necessario installarlo. Per informazioni sulla versione supportata della libreria WinPcap, consultare la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*. Vedere "[Installazione di WinPcap su una piattaforma Windows](#)" a pagina 1781.

- NIC su una piattaforma Linux. Piattaforme Linux mediante un'acquisizione pacchetti Linux nativa che richiede il supporto PACKET_MMAP nel kernel. Il supporto per PACKET_MMAP è incluso per impostazione predefinita nei kernel Linux supportati.
- Scheda di acquisizione pacchetti ad alta velocità su piattaforme Windows o Linux. È possibile utilizzare una scheda di misurazione rete Endace DAG su piattaforme a 64 bit Linux per acquisire pacchetti di rete in ambienti ad alto traffico. In alternativa, per acquisire pacchetti di rete è possibile utilizzare una scheda di rete Napatech. Per ulteriori informazioni sulle schede di acquisizione pacchetti ad alta velocità supportati e sui driver, consultare la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*.

Tabella 56-1 Alternative per l'acquisizione di pacchetti

Tipo di acquisizione pacchetti	Piattaforma	Software
NIC	Windows	WinPcap
	Linux	Nativo
Schede di acquisizione pacchetti ad alta velocità	Windows a 64 bit	Napatech
	Linux a 64 bit	Endace Napatech

Informazioni sull'installazione e sulla configurazione di software di acquisizione dei pacchetti

Considerare i seguenti requisiti quando si installa e si configura software di acquisizione dei pacchetti:

- Sulle piattaforme Windows, l'acquisizione dei pacchetti richiede il software WinPcap che deve essere installato se non è già presente.
- Sulle piattaforme Linux, l'acquisizione dei pacchetti viene eseguita mediante `PACKET_MMAP`. `PACKET_MMAP` è un componente standard di Linux e non deve essere installato o modificato. Tuttavia, è anche necessario disporre di `apr-util`, `apr`, `expat` e altri pacchetti di terze parti per eseguire un server Network Monitor su Linux. Per ulteriori informazioni, consultare la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*.
- Se si utilizza una scheda di acquisizione pacchetti ad alta velocità (Endace o Napatech), è necessario installare o aggiornare il software del driver della scheda.

Vedere ["Installazione di WinPcap su una piattaforma Windows"](#) a pagina 1781.

Vedere ["Aggiornamento del driver delle schede Endace"](#) a pagina 1781.

Vedere ["Installazione e aggiornamento della scheda di rete e del software del driver Napatech"](#) a pagina 1781.

Installazione di WinPcap su una piattaforma Windows

Se il software WinPcap non è già presente su una piattaforma Windows, è necessario installarlo. Per informazioni sulla versione supportata della libreria WinPcap, consultare la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*. Ulteriori informazioni sono disponibili nella *Guida di installazione di Symantec Data Loss Prevention*.

Vedere ["Informazioni sulla gestione dei server Symantec Data Loss Prevention"](#) a pagina 241.

Per installare WinPcap sul server di rilevamento Network Monitor:

- 1 Individuare il software WinPcap all'URL seguente: <http://www.winpcap.org/>
- 2 Copiare i file di WinPcap in un'unità locale.
- 3 Avviare l'eseguibile di WinPcap e seguire le istruzioni di installazione.
- 4 Reimpostare le impostazioni del Registro di sistema di Windows eseguendo `pcapstart.reg` e seguire le istruzioni visualizzate.

Aggiornamento del driver delle schede Endace

Se si esegue l'upgrade di un server Network Monitor alla versione attuale, può essere necessario aggiornare il driver delle schede Endace. Per ulteriori informazioni sulle schede e i driver Endace supportati, consultare la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*.

Aggiornamento di un driver Endace

- 1 Installare il nuovo driver come descritto nella documentazione di Endace.
- 2 Riconfigurare Network Monitor per utilizzare il nuovo driver.

Vedere ["Configurazione del server Network Monitor"](#) a pagina 1787.

Installazione e aggiornamento della scheda di rete e del software del driver Napatech

Seguire le istruzioni riportate di seguito per installare scheda e driver di acquisizione del pacchetto ad alta velocità Napatech. Osservare i diversi prerequisiti e le procedure per Linux e Windows. Consultare la *guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention* a <http://www.symantec.com/docs/doc10602.html> per informazioni sulle versioni di scheda e driver Napatech supportate.

Prerequisiti del driver Napatech per Linux

- Intestazioni di sviluppo del kernel Linux
- Versione GCC 4.0 o successive
- GNU make
- Per utilizzare gli strumenti sono richieste le seguenti librerie:
 - `glibc` versione 2.5 o successiva
 - `ncurses` versione 5.0 o successiva; si applica solo a strumenti di monitoraggio e di profiling
- Per l'installazione e la compilazione del driver Linux e degli strumenti è necessario disporre dei privilegi di super utente.

Prerequisiti del driver Napatech per Windows

- Il server deve avere almeno 4 GB di memoria.
- Per installare Napatech è necessario disporre di privilegi di amministratore.
- Prima di installare il software Symantec Data Loss Prevention Network Monitor, è necessario installare la versione di WinPcap supportata da <https://www.winpcap.org/install/>. Per ulteriori informazioni, consultare il *Symantec Data Loss Prevention Manuale di installazione* in <http://www.symantec.com/docs/doc9257.html>.
- NTService, parte essenziale della suite software Napatech, può essere eseguito sia come servizio Windows che in modalità console (in primo piano). È necessario installarlo come servizio di avvio automatico.

Tabella 56-2 Installazione e aggiornamento della scheda di rete Napatech

Passaggio	Azione	Descrizione
1	Scaricare il pacchetto del prodotto dal Centro di supporto di Napatech.	Accedere a https://support.napatech.com .
2	Decomprimere o estrarre il pacchetto del prodotto.	<p>Per Linux:</p> <p>Decomprimere il pacchetto del prodotto mediante <code>-tar -xf/napatech/ntanl_package_3gd_linux_8.1.0.tar.gz</code>.</p> <p>Per Windows:</p> <p>Estrarre il programma di installazione dal pacchetto del prodotto <code>nt_suite_3gd_windows_x.y.z.zip</code>.</p>

Passaggio	Azione	Descrizione
3	Installare la scheda di acquisizione pacchetti ad alta velocità Napatech.	Consultare la <i>guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention</i> alla pagina http://www.symantec.com/docs/doc10602.html per le ultime versioni supportate di Napatech.
4	Installare il driver e gli strumenti Napatech.	<p>Per Linux:</p> <ol style="list-style-type: none"> 1 Installare il driver e gli strumenti con <code>./ntanl_package_3gd_linux_8.1.0/package_install_3gd.sh.</code> 2 Non installare la versione di libpcap con le estensioni Napatech. 3 Caricare il driver utilizzando: <code>/opt/napatech3/bin/ntload.sh.</code> 4 Avviare il servizio Napatech utilizzando <code>/opt/napatech3/bin/ststart.sh.</code> 5 Aggiungere le righe 3 e 4 a <code>/etc/rc.d/rc.local</code> per avviare automaticamente il servizio al riavvio del sistema. Alcune versioni Linux richiedono di impostare il bit di esecuzione nel file <code>rc.local</code>. <p>Per Windows:</p> <ol style="list-style-type: none"> 1 Eseguire <code>ntanl_package_3gd_windows_x.y.z.exe</code> per installare la suite di software. 2 Scegliere tutti i componenti eccetto WinPcap NT. La versione corretta di WinPcap è già stata installata come uno dei prerequisiti Windows. <p>Per ulteriori informazioni, vedere il <i>Manuale di installazione del software Napatech</i>.</p> <p>Per le versioni supportate dei driver Napatech, consultare la <i>Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention</i>.</p>

Passaggio	Azione	Descrizione
5	Verificare l'installazione Napatech.	<p>Per Linux</p> <ol style="list-style-type: none"> 1 Verificare che il driver Napatech sia stato compilato e installato correttamente. Lo script <code>./ntanl_package_3gd_linux_8.1.0/package_install_3gd.sh</code> compila il driver e installa il servizio. Se si riscontrano errori durante l'esecuzione di questo script, assicurarsi di avere installato tutti i prerequisiti necessari, tra cui i pacchetti di e gli strumenti di sviluppo del kernel. 2 Caricare il driver utilizzando: <code>/opt/napatech3/bin/ntload.sh</code>. 3 Avviare il servizio Napatech utilizzando <code>/opt/napatech3/bin/ntstart.sh</code>. 4 Quando si carica il driver (fase 2) e si avvia il servizio di Napatech (passaggio 3) si dovrebbe visualizzare un messaggio di operazione riuscita. Se il driver è stato compilato e installato correttamente, ma il caricamento del driver e del servizio genera un messaggio di errore, accedere a supporto Napatech all'indirizzo https://support.napatech.com. <p>Per Windows</p> <ol style="list-style-type: none"> 1 Utilizzare Gestione periferiche di Windows per verificare il corretto funzionamento dell'acceleratore di Napatech. Accedere a Classe della suite software Napatech > Stato del dispositivo nella scheda Generale. Si dovrebbe visualizzare il messaggio che indica che la periferica funziona correttamente. 2 Utilizzare i servizi di Windows per verificare che la Suite software Napatech a 64 bit sia in esecuzione e che il Tipo di avvio sia impostato su automatico. 3 Per risolvere i problemi, consultare il <i>Manuale di installazione del software Napatech</i> dal pacchetto software Napatech.
6	Configurare il server di rilevamento Network Monitor.	<p>Distribuire un server di rilevamento Network Monitor e configurare le impostazioni Advanced Server :</p> <ol style="list-style-type: none"> 1 Attivare l'acquisizione di pacchetti Napatech impostando il contrassegno <code>PacketCapture.IS_NAPATECH_ENABLED</code> su <code>true</code>. 2 Aggiornare il valore al percorso della directory degli strumenti driver Napatech inserendo il percorso nel campo della seguente voce: <code>PacketCapture.NAPATECH_TOOLS_PATH</code>. <ul style="list-style-type: none"> ■ Per Linux, <code>/opt/napatech3/bin</code> ■ Per Gestione periferiche di Windows, <code>C:\Programmi\Napatech3\bin</code> <p>Vedere "Impostazioni server avanzate" a pagina 279.</p>

File di configurazione acquisizione Napatech di esempio

Un file di configurazione acquisizione Napatech è incluso nel programma di installazione di Symantec Data Loss Prevention. Viene utilizzato per assegnare i flussi di acquisizione e configurare i filtri di acquisizione. Questo file di configurazione si trova nelle seguenti posizioni:

Nei sistemi Linux, in `/opt/Symantec/DataLossPrevention/Enforce
Server/15.1/Protect/config/napatech3gd.cfg`

Nei sistemi Windows, in `C:\Programmi\Symantec\Data Loss Prevention\Enforce
Server\15.1\Protect\config\napatech3gd.cfg`

Il seguente file di configurazione di esempio riflette le impostazioni predefinite consigliate da Symantec in grado di fornire prestazioni ottimali. Modificare il file per riflettere le impostazioni predefinite.

I flussi non sono assegnati a una porta fisica; il carico di payload viene bilanciato mediante l'impostazione di algoritmo HashMode. Per impostazione predefinita, i pacchetti UDP vengono filtrati in modo da ridurre il carico inutile su Symantec Data Loss Prevention.

Tabella 56-3 File d'esempio `napatech3gd.cfg`

```
# Napatech 3GD NTPL Configuration File #
# This file will be read by PacketCapture and fed to the Napatech Software Interface
  upon startup.
# PacketCapture will read all active streams from the Napatech system; delete all
  streams before opening new ones.
Delete = All
# Create streams. Edit this to customize stream assignment.
Assign[StreamId = (0..3)] = (Layer4Protocol != UDP)
# The recommended HashMode for splitting traffic for multithreaded processing. This
  should always be the last line.
HashMode = Hash2TupleSorted
```

È possibile abilitare il multithreading con l'impostazione

`PacketCapture.MultithreadingEnabled`. Per impostazione predefinita, è impostata su `true`. Per disattivare il multithreading, accedere alla pagina **Network Monitor Server Advanced Settings** (Impostazioni avanzate di Network Monitor Server) e impostare il valore su `false`. Se il file di configurazione `napatech3gd.cfg` viene modificato, è necessario riavviare il servizio di acquisizione del pacchetto di Data Loss Prevention per caricare la nuova configurazione. Fare riferimento alla documentazione Napatech per la sintassi aggiuntiva del filtro di acquisizione.

Aggiornamento di Napatech su Symantec Data Loss Prevention Network Monitor dalla versione 14.x alla versione 15

Aggiornamento del sistema Linux

- 1 Rimuovere l'installazione precedente: `rm -rf /opt/napatech/bin.`
- 2 Rimuovere la voce `/opt/napatech/bin/load_driver.sh` da `/etc/rc.d/rc.local.`
- 3 Compilare e installare i driver di terza generazione seguendo la procedura Linux in [Tabella 56-2.](#)
- 4 Accedere al *Manuale di aggiornamento di Symantec Data Loss Prevention* per eseguire l'upgrade di Enforce Server e dei server di rilevamento.
- 5 Modificare le impostazioni del server Network Monitor:
 - `PacketCapture.NAPATECH_TOOLS_PATH: /opt/napatech3/bin`
 - `PacketCapture.NUMBER_BUFFER_POOL_PACKETS: 1200000`
 - `PacketCapture.NUMBER_SMALL_POOL_PACKETS: 1000000`
- 6 Salvare le modifiche e riciclare Enforce Server.
- 7 Una volta riciclato il server, selezionare **Napatech 3GD Software Interface** dalla pagina **Configurazione di Network Monitor.**
- 8 Salvare la configurazione e riciclare nuovamente Enforce Server.

Aggiornamento del sistema Windows

- 1 Disinstallare il driver della periferica Napatech NT4E da **Gestione periferiche di Windows.**
- 2 Installare il driver di terza generazione seguendo la procedura Windows in [Tabella 56-2.](#)
- 3 Accedere al *Manuale di aggiornamento di Symantec Data Loss Prevention* per eseguire l'upgrade di Enforce Server e dei server di rilevamento.
- 4 Apportare le seguenti modifiche alle impostazioni di Network Monitor:
 - `PacketCapture.NAPATECH_TOOLS_PATH: C:\Program Files\Napatech3\bin`
 - `PacketCapture.NUMBER_BUFFER_POOL_PACKETS: 1200000`
 - `PacketCapture.NUMBER_SMALL_POOL_PACKETS: 1000000`
- 5 Salvare le modifiche e riciclare Enforce Server.
- 6 Una volta riciclato il server, selezionare **Napatech 3GD Software Interface** nella pagina **Configurazione di Network Monitor.**
- 7 Salvare la configurazione e riciclare nuovamente Enforce Server.

Nota: Durante l'aggiornamento, le interfacce Napatech preesistenti inutilizzate non vengono eliminate automaticamente dalla console di amministrazione di Enforce Server. È possibile ignorare o eliminare in modo permanente le interfacce dalla console di amministrazione di Enforce Server. Per rimuovere le interfacce, rimuovere e riaggiungere il server di monitoraggio. Se il server viene eliminato e aggiunto nuovamente, le impostazioni del server devono essere regolate in modo appropriato, come descritto nel passaggio 4; in caso contrario, il server viene eseguito con le impostazioni predefinite. Symantec consiglia di prendere nota delle impostazioni del server personalizzate prima di eliminare i server precedenti.

Configurazione del server Network Monitor

Configurare il server Network Monitor selezionando l'interfaccia di rete (scheda NIC, Napatech o Endace) da utilizzare per l'acquisizione del traffico. È inoltre necessario selezionare i protocolli da monitorare.

Per configurare un server Network Monitor

- 1 Nella console di amministrazione di Enforce Server selezionare **Sistema > Server e rilevatori > Panoramica** e fare clic sul server Network Monitor. Viene visualizzata la schermata **Dettagli server/rilevatore**.

Se non si utilizza una scheda di acquisizione di pacchetti ad alta velocità (Endace o Napatech) per l'acquisizione del traffico, andare al passaggio 6.
- 2 Se si utilizza una scheda di acquisizione di pacchetti ad alta velocità (Endace o Napatech), fare clic su **Impostazioni server**.
- 3 Per le schede Endace immettere i valori appropriati nei campi seguenti:

PacketCapture.ENDACE_BIN_PATH

Digitare il percorso della directory `\bin` di Endace.

Per impostazione predefinita, questa directory è situata in `endace_home\dag-version\bin`. Si tenga presente che non è possibile utilizzare variabili (ad esempio, `%ENDACE_HOME%`) in nessuno dei campi elencati qui.

PacketCapture.ENDACE_LIB_PATH

Digitare il percorso della directory `\lib` di Endace.

PacketCapture.ENDACE_XILINX_PATH

Digitare il percorso della directory `\xilinx` di Endace.

PacketCapture.IS_ENDACE_ENABLED

Impostare il valore su `true`.

- 4 Per le schede Napatech immettere i valori appropriati nei campi seguenti:

PacketCapture.IS_NAPATECH_ENABLED	Impostare il valore su true.
PacketCapture.NAPATECH_TOOLS_PATH	Digitare il percorso della directory <code>\tools</code> di Napatech.

- 5 Arrestare e riavviare il server Network Monitor. Symantec Data Loss Prevention visualizza la scheda Endace nel campo **Interfacce di rete** della schermata **Configura server** per il server Network Monitor.
- 6 Selezionare **Sistema > Server e rilevatori > Panoramica** e fare di nuovo clic sul server Network Monitor.
- 7 Nella schermata Dettagli server fare clic su **Configura**. È possibile verificare o modificare le impostazioni nella sezione generale nella parte superiore e nella scheda **Acquisizione del pacchetto** come descritto nei passaggi successivi.
- 8 Lasciare il campo **Sovrascrittura cartella di origine** vuoto per accettare la directory predefinita per il buffering dei flussi di rete prima che il server Network Monitor li elabori. Questa impostazione è l'impostazione consigliata. Per specificare una directory di buffer personalizzata, digitare il percorso completo della directory.
- 9 Selezionare una o più **interfacce di rete** (schede NIC, Napatech o Endace) attraverso cui il server Network Monitor deve acquisire il traffico.
- 10 Nella sezione **Protocollo** selezionare uno o più protocolli da monitorare. Ad esempio selezionare le caselle di controllo per SMTP, HTTP e FTP. Affinché un protocollo venga visualizzato in questa sezione, deve essere già configurato nella schermata globale Protocolli su Enforce Server.

Consultare la guida in linea associata alla schermata **Configura server**.

Symantec Data Loss Prevention ha impostazioni standard per ciascun protocollo dell'elenco. Per modificare le impostazioni di un protocollo, fare clic sull'icona a forma di **matita** accanto al protocollo appropriato. Per i dettagli della modifica delle impostazioni di protocollo, consultare la guida in linea.

- 11 Fare clic su **Salva**.
- 12 Arrestare e riavviare il server Network Monitor. Fare clic su **Ricicla** accanto alla voce **Stato** nella schermata Dettagli server.

Dopo la selezione di un'interfaccia di rete e la scelta dei protocolli, è possibile creare una politica di prova per testare la distribuzione.

Vedere ["Test di Network Monitor"](#) a pagina 1790.

Vedere ["Attivazione dell'elaborazione GET con Network Monitor"](#) a pagina 1789.

Vedere ["Creazione di una politica per Network Monitor"](#) a pagina 1789.

Attivazione dell'elaborazione GET con Network Monitor

Per impostazione predefinita, Network Monitor non elabora i comandi HTTP GET. L'elaborazione GET è disattivata in quanto comprende un volume di traffico elevato e si hanno raramente perdite di dati riservati con i comandi GET. Se si richiede l'elaborazione GET e il server Network Monitor può gestire il carico aumentato, seguire questa procedura per configurare Network Monitor affinché elabori i comandi GET.

Nota: Network Monitor ispeziona solo le richieste GET, ma non le risposte HTTP GET.

Per attivare l'elaborazione GET

- 1 Assicurarsi che l'impostazione server avanzata **L7.processGets** nel server Network Monitor sia impostata su **true** (impostazione predefinita).
- 2 Modificare l'impostazione server avanzata **PacketCapture.DISCARD_HTTP_GET** nel server Network Monitor da **true** (impostazione predefinita) a **false**.
- 3 Per l'impostazione server avanzata **L7.minSizeofGetURL** nel server Network Monitor, specificare un valore inferiore a quello predefinito (100). Ridurlo a un numero di byte inferiore alla lunghezza dell'URL più breve da cui si desidera elaborare i comandi GET. Una dimensione URL minima pari a 10 dovrebbe essere appropriata tutti i casi. Da notare, tuttavia, che la riduzione della dimensione minima dei comandi GET aumenta il numero di richieste da elaborare e quindi il carico del traffico del server.

Nota: Network Monitor ispeziona solo le richieste HTTP GET, ma non le risposte HTTP GET.

Vedere ["Attivazione dell'elaborazione GET per Network Prevent for Web"](#) a pagina 1812.

Creazione di una politica per Network Monitor

Per Network Monitor, è possibile creare le politiche che includono una qualsiasi delle regole di risposta standard. Per configurare un'azione della regola di risposta, accedere a **Gestisci > Politiche > Regole di risposta** e fare clic su **Aggiungi regola di risposta**.

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

Per creare una politica di test per Network Monitor

- 1 Nella console di amministrazione di Enforce Server, creare una regola di risposta che include una delle azioni applicata a Network Monitor. Ad esempio, creare una regola di risposta che include l'azione Tutto: imposta stato.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Creare una politica che comprenda la regola di risposta configurata nel passaggio precedente.

Ad esempio, creare una politica denominata Politica di test come descritto di seguito:

- Includere una regola di rilevamento **Contenuto corrispondente a parola chiave** che corrisponde alla parola chiave `test_dlp_secret_keyword`.
- Includere una regola di risposta **Tutto: imposta stato**.
- Associarla al gruppo di politiche Predefinito.

Vedere ["Aggiunta di una nuova politica o di un modello di politica"](#) a pagina 421.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Test di Network Monitor

È possibile testare Network Monitor inviando un'e-mail che viola la politica di test.

Per testare il sistema

- 1 Accedere a un account e-mail che invia i messaggi tramite l'MTA.
- 2 Inviare un'e-mail che contiene dati confidenziali. Ad esempio, inviare un'e-mail contenente la parola chiave `test_dlp_secret_keyword`.
- 3 Nella console di amministrazione di Enforce Server, accedere a **Incidenti > Rete** e fare clic su **Incidenti - Nuovi**. Individuare l'incidente risultante. Ad esempio, individuare una voce di incidente che include la marcatura orario e il nome della politica appropriati.
- 4 Fare clic sulla voce dell'incidente corrispondente per vedere l'istantanea completa dell'incidente.

Vedere ["Informazioni sui report Symantec Data Loss Prevention"](#) a pagina 1632.

Vedere ["Configurazione del server Network Monitor"](#) a pagina 1787.

Vedere ["Creazione di una politica per Network Monitor"](#) a pagina 1789.

Implementazione di Network Prevent for Email

Il capitolo contiene i seguenti argomenti:

- [Implementazione di Network Prevent for Email](#)
- [Informazioni sull'integrazione di Mail Transfer Agent \(MTA\)](#)
- [Configurazione di Network Prevent for Email Server per modalità di riflessione o inoltro](#)
- [Configurazione di uno o più MTA di upstream](#)
- [Creazione di una politica per Network Prevent for Email](#)
- [Informazioni sulle intestazioni dei dati relativi alle violazioni delle politiche](#)
- [Attivazione delle intestazioni dei dati sulle violazioni della politica](#)
- [Test di Network Prevent for Email](#)

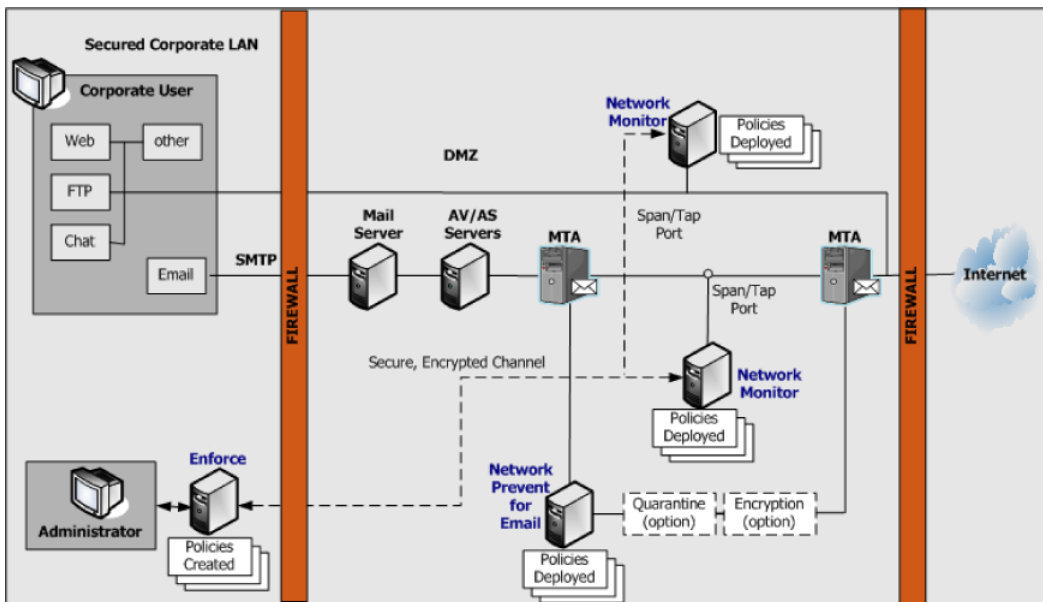
Implementazione di Network Prevent for Email

Network Prevent for Email monitora e analizza il traffico di e-mail in uscita in linea e (facoltativamente) blocca, ridirige o modifica messaggi e-mail come specificato nelle politiche. Network Prevent for Email si integra con Mail Transfer Agent (MTA) standard del settore e servizi e-mail ospitati per consentire di monitorare e arrestare incidenti di perdita dei dati su SMTP. Le politiche distribuite su Network Prevent for Email Server dirigono l'MTA con Prevent integrato o il server di posta ospitato. Il server di posta con Prevent integrato blocca, reindirizza e altera i messaggi di posta elettronica in base al contenuto specifico e ad altri attributi di messaggi.

Nota: Consultare *Guida all'integrazione di Symantec Data Loss Prevention MTA per Network Prevent for Email* per determinare l'architettura di integrazione preferita prima di continuare con l'implementazione.

Figura 57-1 mostra un'integrazione di Network Prevent for Email Server con un MTA dell'hop successivo che si gestisce nella rete. In alternativa, è possibile integrare Network Prevent for Email Server con un server di posta ospitato che si trova al di fuori del firewall.

Figura 57-1 Configurazione di Network Prevent for Email di base



In primo luogo, è necessario conoscere le fasi di alto livello richieste per l'implementazione di Network Prevent for Email. Per ulteriori dettagli è possibile verificare le sezioni relative a riferimenti incrociati.

Per implementare Network Prevent for Email

- 1 Scegliere un'architettura di integrazione e configurare il Mail Transfer Agent (MTA) per operare con il server Network Prevent for Email.
Vedere ["Informazioni sull'integrazione di Mail Transfer Agent \(MTA\)"](#) a pagina 1793.
- 2 Configurare il server Network Prevent for Email per operare all'interno dell'architettura di integrazione scelta.
Vedere ["Configurazione di Network Prevent for Email Server per modalità di riflessione o inoltrare"](#) a pagina 1793.

- 3 Se si prevede di crittografare o mettere in quarantena messaggi di posta elettronica, configurare i server di crittografia o archiviazione di terze parti necessari. Per dettagli, vedere la documentazione del prodotto.
- 4 Creare e distribuire una politica per Network Prevent for Email.
Vedere ["Creazione di una politica per Network Prevent for Email"](#) a pagina 1800.
- 5 Verificare il sistema generando un incidente rispetto alla politica di test.
Vedere ["Test di Network Prevent for Email"](#) a pagina 1803.

Informazioni sull'integrazione di Mail Transfer Agent (MTA)

Scegliere un'architettura di integrazione e configurare il Mail Transfer Agent (MTA) per operare con il server Network Prevent for Email.

Consultare la *Guida all'integrazione di Symantec Data Loss Prevention MTA per Network Prevent for Email*. Acquisire familiarità con le architetture di integrazione compatibili.

Il Network Prevent for Email Server può funzionare con MTA nelle modalità di riflessione o inoltro:

- Modalità di riflessione. Nel modalità di riflessione, il Network Prevent for Email Server riceve messaggi da un MTA. Esso li analizza e poi li restituisce allo stesso MTA (con le istruzioni per bloccare i messaggi o elaborarli downstream). In sostanza, il server restituisce i messaggi allo stesso indirizzo ip da cui sono stati inviati.
- Modalità di inoltro. Nella modalità di inoltro, il Network Prevent for Email Server riceve messaggi da un MTA upstream. Esso li analizza e li invia a un MTA downstream o a un provider di servizi e-mail ospitato. È possibile specificare un elenco di indirizzi IP o nomi di host per il server di posta dell'hop successivo nella configurazione di Network Prevent for Email Server.

È anche possibile configurare un singolo Network Prevent for Email Server per operare con più MTA.

Vedere ["Configurazione di uno o più MTA di upstream"](#) a pagina 1799.

Configurazione di Network Prevent for Email Server per modalità di riflessione o inoltro

Utilizzare le seguenti istruzioni per configurare Network Prevent for Email Server in modo che funzioni in modalità riflessione o inoltro.

Per configurare il server Network Prevent for Email

- 1 Accedere alla console di amministrazione di Enforce Server per il sistema Symantec Data Loss Prevention che si desidera configurare.
- 2 Per visualizzare l'elenco dei server configurati selezionare **Sistema > Server e rilevatori > Panoramica**.
- 3 Fare clic sul nome del server Network Prevent for Email che si desidera configurare.
- 4 Fare clic su **Configura**.
- 5 Deselezionare **Modalità di prova** per attivare il blocco di messaggi e-mail che sono stati identificati non conformi alle politiche di Symantec Data Loss Prevention.

6 Configurare la modalità di riflessione o di inoltro modificando i seguenti campi:

Campo	Descrizione
Configurazione hop successivo	<p>Selezionare Rifletti per eseguire il server Network Prevent for Email in modalità di riflessione. Selezionare Avanti per operare in modalità di inoltro.</p> <p>Nota: Se si seleziona Avanti è necessario selezionare anche Abilita ricerca MX o Disabilita ricerca MX per configurare il metodo impiegato per determinare l'MTA dell'hop successivo.</p>
Abilita ricerca MX	<p>Questa opzione si applica solo alle configurazioni della modalità di inoltro.</p> <p>Selezionare Abilita ricerca MX per eseguire una query DNS su un nome di dominio e ottenere i record di scambio di posta (MX) per il server. Il server Network Prevent for Email utilizza i record MX restituiti per selezionare l'indirizzo del server di posta dell'hop successivo.</p> <p>Se si seleziona Abilita ricerca MX, aggiungere anche uno o più nomi di dominio nella casella di testo Immetti domini. Ad esempio:</p> <p><code>companyname.com</code></p> <p>Il server Network Prevent for Email esegue query di record MX per i nomi di dominio specificati.</p> <p>Nota: È necessario includere almeno una voce valida nella casella di testo Immetti domini per configurare correttamente il comportamento delle modalità di inoltro.</p>

Campo

Disabilita ricerca MX

Descrizione

Questo campo si applica solo alle configurazioni della modalità di inoltro.

Selezionare **Disabilita ricerca MX** se si desidera specificare il nome host o l'indirizzo IP esatto di uno o più MTA dell'hop successivo. Il server Network Prevent for Email utilizza i nomi host o gli indirizzi specificati e non esegue una ricerca di record MX.

Se si seleziona **Disabilita ricerca MX**, aggiungere anche uno o più nomi di host o indirizzi IP per gli MTA degli hop successivi nella casella di testo **Immetti nomi host**. È possibile specificare più voci posizionando ognuna di esse su una linea separata. Ad esempio:

```
smtp1.companyname.com
smtp2.companyname.com
smtp3.companyname.com
```

Network Prevent for Email Server prova sempre a indirizzarsi verso il primo MTA che viene specificato nell'elenco. Se tale MTA non è disponibile, il server Network Prevent for Email prova la successiva voce disponibile nell'elenco.

Nota: È necessario includere almeno una voce valida nella casella di testo **Immetti nome host** per configurare correttamente il comportamento delle modalità di inoltro.

7 Fare clic su **Salva**.

- 8 Fare clic su **Impostazioni server** per verificare o configurare queste impostazioni avanzate:

Campo	Descrizione
RequestProcessor.ServerSocketPort	<p>Assicurarsi che questo valore corrisponda al numero di porta dell'SMTP Listener a cui l'MTA di upstream invia messaggi e-mail. Il valore predefinito è 10025.</p> <p>Nota: Molti sistemi Linux limitano le porte inferiori a 1024 all'accesso root. Network Prevent for Email non può eseguire il binding a queste porte con restrizioni. Se il computer riceve posta da sottoporre a ispezione su una porta con restrizioni (ad esempio, la porta 25), riconfigurare il computer in modo che diriga il traffico dalla porta con restrizioni alla porta di Network Prevent for Email senza restrizioni (per impostazione predefinita porta 10025).</p> <p>Vedere "Configurazione delle tabelle IP di Linux per reindirizzare il traffico da una porta con restrizioni" a pagina 1798.</p>
RequestProcessor.MTAResubmitPort	<p>Assicurarsi che questo valore corrisponda al numero di porta dell'SMTP Listener sull'MTA di upstream a cui il server Network Prevent for Email restituisce la posta. Il valore predefinito è 10026.</p>
RequestProcessor.AddDefaultHeader	<p>Per impostazione predefinita, Network Prevent for Email Server utilizza un'intestazione per identificare tutti i messaggi e-mail che ha elaborato. L'intestazione e il valore sono specificati nel campo RequestProcessor.DefaultPassHeader.</p> <p>Modificare il valore di questo campo su FALSE se non si desidera aggiungere un'intestazione a ogni messaggio.</p>

Campo	Descrizione
RequestProcessor.AddDefaultPassHeader	<p>Questo campo specifica l'intestazione e il valore che il server Network Prevent for Email aggiunge a ogni messaggio e-mail che elabora.</p> <p>L'intestazione e il valore predefiniti corrispondono a <code>X-Filter-Loop: Riflesso</code>. Modificare il valore di questo campo se si desidera aggiungere un'altra intestazione a ogni messaggio elaborato.</p> <p>Se non si desidera aggiungere un'intestazione a ogni messaggio e-mail, impostare il campo AddDefaultPassHeader su <code>FALSE</code>.</p>

Nota: Configurare sempre **RequestProcessor.ServerSocketPort** e **RequestProcessor.MTAResubmitPort**, sia che si implementi la modalità di riflessione sia che si implementi quella di inoltro. Con la modalità di inoltro **RequestProcessor.ServerSocketPort** specifica la porta dell'SMTP Listener sul server di rilevazione a cui l'MTA di upstream invia i messaggi e-mail. **RequestProcessor.ServerSocketPort** specifica la porta dell'SMTP Listener sull'MTA di downstream a cui il server di rilevazione invia i messaggi e-mail.

- 9 Fare clic su **Salva**.
- 10 Fare clic su **Fine**.
- 11 Se il sistema di consegna delle e-mail utilizza la comunicazione TLS in modalità di inoltro, ogni server di posta dell'hop successivo nella catena di proxy deve supportare TLS e autenticarsi all'hop precedente. Ciò significa che il server Network Prevent for Email deve autenticarsi nell'MTA di upstream e che l'MTA dell'hop successivo deve autenticarsi nel server Network Prevent for Email. L'autenticazione adeguata richiede che ogni server di posta archivi il certificato della chiave pubblica per server di posta dell'hop successivo nel relativo file di archivio chiavi locale.

Vedere ["Configurazione di uno o più MTA di upstream"](#) a pagina 1799.

Vedere ["Creazione di una politica per Network Prevent for Email"](#) a pagina 1800.

Vedere ["Test di Network Prevent for Email"](#) a pagina 1803.

Configurazione delle tabelle IP di Linux per reindirizzare il traffico da una porta con restrizioni

Molti sistemi Linux limitano le porte inferiori a 1024 all'accesso root. Network Prevent for Email non può eseguire il binding a queste porte con restrizioni.

Se il computer riceve la posta per ispezione su una porta con restrizioni (ad esempio, porta 25), utilizzare il comando `iptables` per dirigere quel traffico a una porta senza restrizioni, come la porta 10025, predefinita di Network Prevent for Email. Quindi assicurarsi che Network Prevent for Email ascolta la porta senza restrizioni per ispezionare l'e-mail.

Utilizzare le seguenti istruzioni per configurare un sistema Linux per indirizzare dalla porta 25 alla porta 10025. Se si utilizza una diversa porta con restrizioni o la porta di Network Prevent for Email, immettere i valori corretti nei comandi `iptables`.

Per configurare il traffico di routing dalla porta 25 alla porta 10025

- 1 Configurare Network Prevent for Email per usare la porta 10025 predefinita se necessario. Vedere ["Configurazione di Network Prevent for Email Server per modalità di riflessione o inoltra"](#) a pagina 1793.
- 2 In una finestra di terminale nel computer Network Prevent for Email, immettere i seguenti comandi per reindirizzare il traffico dalla porta 25 alla porta 10025:

```
iptables -N Vontu-INPUT
iptables -A Vontu-INPUT -s 0/0 -p tcp --dport 25 -j ACCEPT
iptables -I INPUT 1 -s 0/0 -p tcp -j Vontu-INPUT
iptables -t nat -I PREROUTING -p tcp --destination-port 25 -j REDIRECT --to-ports=10025
iptables-save > /etc/sysconfig/iptables
```

Nota: Se si desidera soltanto verificare il routing IP locale tra le porte con Telnet, utilizzare il comando: `iptables -t nat -I OUTPUT -o lo -p tcp --destination-port 25 -j REDIRECT --to-ports=10025`

Se successivamente si decide di eliminare la voce dalle tabelle IP, utilizzare il comando:

```
iptables -t nat -D OUTPUT -o lo -p tcp --destination-port 25 -j REDIRECT --to-ports=10025
```

Configurazione di uno o più MTA di upstream

Per impostazione predefinita, il server Network Prevent for Email può accettare connessioni alla porta del servizio ESMTP da qualsiasi sistema sulla rete. È possibile limitare la comunicazione ESMTP del server Network Prevent for Email a un set designato di MTA per motivi di sicurezza. Creare una "lista bianca" di sistemi autorizzati. Se uno o più sistemi sono aggiunti alla lista bianca, altri sistemi che non sono su tale lista non possono connettersi alla porta del servizio ESMTP del server Network Prevent for Email.

Da notare che una lista bianca di MTA potrebbe essere alterata dall'impostazione **RequestProcessor.BindAddress**. Per impostazione predefinita, l'impostazione

RequestProcessor.BindAddress è 0.0.0.0 e il listener esegue il binding a tutti gli indirizzi disponibili. Se **RequestProcessor.BindAddress** richiede al listener di eseguire il binding a un IP specifico, un MTA della lista bianca dovrà anche essere in grado di raggiungere l'indirizzo del listener.

Per creare una lista bianca di sistemi a cui è consentito di comunicare con il server **Network Prevent for Email**:

- 1 Accedere a **Sistema > Server e rilevatori > Panoramica** e fare clic sul server &pn.NetworkPreventEmail desiderato.
- 2 Nella schermata **Dettagli server/rilevatore** visualizzata, fare clic su **Impostazioni server**.
- 3 Scorrere in basso fino al campo **RequestProcessor.AllowHosts**.
Per impostazione predefinita, **RequestProcessor.AllowHosts** è impostato su *any*; ciò significa che tutti gli altri sistemi sulla rete possono comunicare con questo server Mobile Email Monitor.
- 4 È possibile limitare i sistemi ai quali è consentito connettersi con questo server **Network Prevent for Email**. Eliminare *any* e immettere gli indirizzi IP o i nomi di dominio completi (FQDN) dei sistemi che si desidera autorizzare. Separare gli indirizzi multipli con virgole. Ad esempio: "123.14.251.31, smtp_1.corp.mycompany.com, 123.14.223.111." Separare gli indirizzi solo con virgole; non includere spazi.
- 5 Fare clic su **Salva**.

La modifica a questa impostazione diventa effettiva dopo il riavvio del server.

Creazione di una politica per Network Prevent for Email

È possibile creare le politiche che includono una qualsiasi delle regole di risposta standard. Ad esempio, Aggiungi commento, Limita conservazione dati incidenti, Registrazione a un server Syslog, Invia notifica e-mail e Imposta stato.

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

È inoltre possibile incorporare le seguenti regole, specifiche per **Network Prevent for Email**:

■ Rete: Blocca messaggio SMTP

Blocca i messaggi di posta elettronica che contengono dati riservati o metadati significativi (come definito nelle politiche). È possibile configurare Symantec Data Loss Prevention per restituire il messaggio o reindirizzare il messaggio a un indirizzo specifico.

La funzionalità di reindirizzamento è tipicamente utilizzata per reindirizzare i messaggi all'indirizzo di una cassetta postale o mailing list. Gli amministratori e i responsabili usano la cassetta postale o l'elenco per esaminare e distribuire i messaggi. Tali cassette postali sono esterne al sistema Symantec Data Loss Prevention.

■ **Rete: Modifica messaggio SMTP**

Modifica i messaggi di posta elettronica che contengono dati riservati o metadati significativi (come definito nelle politiche). È possibile utilizzare questa azione per modificare l'oggetto del messaggio o aggiungere intestazioni messaggio RFC 5322 specifiche per attivare o disattivare ulteriormente il processo di downstream. Ad esempio, crittografia del messaggio, quarantena del messaggio o archiviazione del messaggio.

Per dettagli sulla configurazione di qualsiasi azione di regola di risposta, aprire la guida in linea. Accedere a **Gestisci > Politiche > Regole di risposta** e fare clic su **Aggiungi regola di risposta**.

Per dettagli sull'utilizzo dell'azione **Rete: Modifica messaggio SMTP** per attivare o disattivare il processo di downstream (come crittografia messaggio), consultare la *Guida all'integrazione di Symantec Data Loss Prevention MTA per Network Prevent*.

Anche se non vengono incorporate le regole di risposta nella politica, Network Prevent for Email acquisisce gli incidenti a condizione che le politiche contengano le regole di rilevamento. Questa caratteristica può essere utile se si desidera esaminare i tipi di incidenti acquisiti da Symantec Data Loss Prevention e quindi raffinare le politiche.

Per creare una politica di test per Network Prevent for Email

- 1 Nella console di amministrazione Enforce Server, creare una regola di risposta che comprenda una delle azioni specifiche di Network Prevent for Email. Ad esempio, creare una regola di risposta che comprenda l'azione **Rete: Blocca messaggio SMTP**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Creare una politica che comprenda la regola di risposta configurata nel passaggio precedente.

Ad esempio, creare una politica Test Policy nel modo seguente:

- Includere una regola di rilevamento **Contenuto corrispondente a parola chiave** che corrisponde alla parola chiave "secret".
- Comprendere una regola di risposta **Rete: Blocca messaggio SMTP**.
- Associarla al gruppo di politiche Predefinito.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Vedere ["Informazioni sulle intestazioni dei dati relativi alle violazioni delle politiche"](#) a pagina 1802.

Informazioni sulle intestazioni dei dati relativi alle violazioni delle politiche

Un messaggio potrebbe violare più di una politica. È possibile aggiungere intestazioni speciali ai messaggi in uscita che riportano il numero e la gravità delle politiche violate. Sono disponibili tre tipi differenti di intestazioni dei dati relativi alle violazioni:

- Numero di politiche violate: è possibile aggiungere un'intestazione che segnala il numero totale di politiche differenti che il messaggio viola.
- Gravità più alta: è possibile aggiungere un'intestazione che segnala il livello di gravità più elevato tra tutte le politiche che il messaggio viola (Alta, Media, Bassa o Informazioni).
- Punteggio di gravità cumulativo: è possibile aggiungere un'intestazione che segnala un punteggio di gravità totale che è la somma numerica di tutte le violazioni della politica. A questo scopo, ai livelli di gravità sono assegnati dei valori numerici: Alta=4, Media=3, Bassa=2 e Informazioni=1. Quindi, un messaggio che viola una politica di gravità Bassa (2) e una di gravità Media (3) ha un punteggio di gravità totale pari a 5.

È possibile usare le intestazioni per generare risposte basate sul numero di violazioni o sulla gravità delle violazioni. Ad esempio:

- I messaggi che violano una singola politica possono essere instradati a una cassetta postale di quarantena. I messaggi che violano molteplici politiche possono essere instradati a una seconda cassetta postale. I messaggi che violano un determinato numero di politiche possono essere instradati a una terza cassetta postale.
- I messaggi che violano molteplici politiche possono essere gestiti diversamente secondo il livello di gravità della violazione più grave.
- I messaggi che violano molteplici politiche possono essere gestiti diversamente secondo il punteggio di gravità totale del messaggio.

Vedere ["Attivazione delle intestazioni dei dati sulle violazioni della politica"](#) a pagina 1802.

Attivazione delle intestazioni dei dati sulle violazioni della politica

È possibile combinare tre intestazioni di più politiche.

Per attivare le intestazioni dei messaggi sulle violazioni della politica:

- 1 Accedere a **Sistema > Server e rilevatori > Panoramica** e fare clic sul server &pn.NetworkPreventEmail desiderato.
- 2 Nella schermata **Dettagli server/rilevatore** visualizzata, fare clic su **Impostazioni server**.

- 3 Scorrere verso il basso fino ad una delle tre seguenti impostazioni di **RequestProcessor**. Per impostazione predefinita, il valore di queste impostazioni è **false**.
- 4 Impostare il valore su **true**.
- 5 Fare clic su **Salva**.

Le modifiche a impostazioni sono effettive solo dopo il riavvio del server.

Tre impostazioni avanzate di **RequestProcessor** attivano tipi differenti di intestazioni di messaggi sulle violazioni di più politiche:

- RequestProcessor.TagPolicyCount.
Quando l'impostazione è true, Network Prevent aggiunge un'intestazione che segnala il numero totale di politiche che il messaggio viola. Ad esempio, se il messaggio viola 3 politiche viene aggiunta l'intestazione "X-DLP-Policy-Count: 3".
- RequestProcessor.TagHighestSeverity.
Quando l'impostazione è impostata su true, Network Prevent aggiunge un'intestazione che segnala la gravità più alta tra le politiche violate. Ad esempio, se un messaggio viola tre politiche, una con gravità "Media" e due con gravità "Bassa" viene aggiunta l'intestazione "X-DLP-Max-Severity: MEDIUM".
- RequestProcessor.TagScore.
Quando l'impostazione è impostata su true, Network Prevent aggiunge un'intestazione che segnala il punteggio cumulativo totale di tutte le politiche violate. I punteggi sono calcolati utilizzando la formula: Alta=4, Media=3, Bassa=2 e Informazioni=1. Ad esempio, se un messaggio viola tre politiche, una con gravità "Media" e due con gravità "Bassa" viene aggiunta l'intestazione: "X-DLP-Score: 7".

Impostando un valore su "true" provoca l'aggiunta automatica dell'intestazione corrispondente a ogni messaggio in uscita che viene elaborato. Ciò accade anche se il messaggio viola solo una singola politica.

Vedere ["Informazioni sulle intestazioni dei dati relativi alle violazioni delle politiche"](#) a pagina 1802.

Test di Network Prevent for Email

È possibile testare Network Prevent for Email inviando un'e-mail che viola la politica di test.

Per testare il sistema

- 1 Accedere a un indirizzo e-mail che invia i messaggi tramite un MTA integrato nel Server Network Prevent for Email.
- 2 Inviare un'e-mail che contiene dati confidenziali. Ad esempio, inviare un'e-mail contenente la parola *Segreto*.

- 3 Nella console di amministrazione di Enforce Server, passare a **Incidente > Rete** e fare clic su **Incidenti - Tutti**. Individuare l'incidente risultante. Ad esempio, individuare una voce di incidente che include la marcatura orario e il nome della politica appropriati.
- 4 Fare clic sulla voce dell'incidente corrispondente per vedere l'istantanea completa dell'incidente.

Vedere ["Informazioni sui report Symantec Data Loss Prevention"](#) a pagina 1632.

Implementazione di Network Prevent for Web

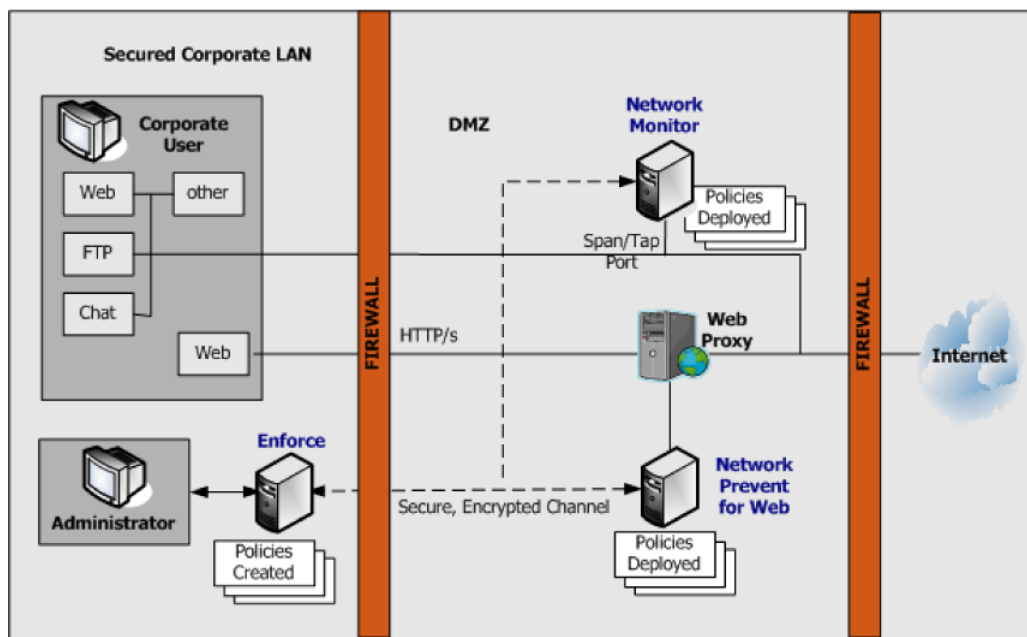
Il capitolo contiene i seguenti argomenti:

- [Implementazione di Network Prevent for Web](#)
- [Configurazione del server Network Prevent for Web](#)
- [Informazioni sulla configurazione di server proxy](#)
- [Configurazione di uno o più server proxy](#)
- [Attivazione dell'elaborazione GET per Network Prevent for Web](#)
- [Creazione di politiche per Network Prevent for Web](#)
- [Test di Network Prevent for Web](#)
- [Informazioni di risoluzione dei problemi per Network Prevent for Web Server](#)

Implementazione di Network Prevent for Web

Network Prevent for Web Server si integra con un server proxy HTTP, HTTPS o FTP tramite ICAP per la gestione di richieste Web attive in linea. Se rileva i dati riservati in contenuti Web, il proxy rifiuta le richieste o rimuove il contenuto HTML come specificato nelle politiche.

Figura 58-1 Una configurazione di Network Prevent for Web di base



In primo luogo, è necessario conoscere le fasi di alto livello richieste per l'implementazione di Network Prevent for Web. Per ulteriori dettagli è possibile verificare le sezioni relative a riferimenti incrociati.

Per implementare Network Prevent for Web

- 1 Assicurarsi che il Network Prevent for Web Server sia configurato per comunicare con il server del proxy HTTP. È anche possibile configurare il server di rilevazione per filtrare il traffico come desiderato.

Vedere ["Configurazione del server Network Prevent for Web"](#) a pagina 1807.

- 2 Configurare il server del proxy HTTP per fare in modo che operi con il Network Prevent for Web Server.

Vedere ["Informazioni sulla configurazione di server proxy"](#) a pagina 1810.

- 3 Creare e distribuire una politica per Network Prevent for Web.

Vedere ["Creazione di politiche per Network Prevent for Web"](#) a pagina 1813.

- 4 Verificare il sistema generando un incidente rispetto alla politica di test.
Vedere ["Test di Network Prevent for Web"](#) a pagina 1815.
- 5 Se richiesto, risolvere il problema relativo all'implementazione.
Vedere ["Informazioni di risoluzione dei problemi per Network Prevent for Web Server"](#) a pagina 1815.

Configurazione del server Network Prevent for Web

È possibile usare una serie di opzioni di configurazione per il server Network Prevent for Web. Ad esempio è possibile configurare il server in modo che:

- ignori le richieste o le risposte HTTP di piccole dimensioni
- ignori le richieste o le risposte da un host o un dominio specifico (quale il dominio di una filiale)
- ignori le query del motore di ricerca dell'utente

Per modificare la configurazione del server Network Prevent for Web

- 1 Selezionare **Sistema > Server e rilevatori > Panoramica** e fare clic sul server Network Prevent for Web.
- 2 Nella schermata **Dettagli server/rilevatore** visualizzata fare clic su **Configura**.
È possibile verificare o modificare le impostazioni nella scheda **ICAP** come descritto nei passaggi successivi. La scheda è divisa in diverse sezioni: **Filtraggio richieste**, **Filtraggio risposte** e **Connessione**.
- 3 Verificare o modificare l'impostazione **Modalità di prova**. **Modalità di prova** consente di verificare la prevenzione senza bloccare le richieste in tempo reale. Se si seleziona **Modalità di prova**, Symantec Data Loss Prevention rileva gli incidenti e indica che ha bloccato una comunicazione HTTP, ma non blocca la comunicazione.

- 4 Verificare o modificare le opzioni di filtraggio per le richieste dei client HTTP (agenti utente). Le opzioni della sezione **Filtraggio richieste** sono le seguenti:

Ignora richieste inferiori a

Specifica la dimensione minima del corpo delle richieste HTTP per l'ispezione (l'impostazione predefinita è 4096 byte). Ad esempio, le stringhe di ricerca digitate in motori di ricerca quali Yahoo o Google sono in genere brevi. È possibile regolare questo valore per escludere tali ricerche dall'ispezione.

Ignora richieste senza allegati

Fa sì che il server ispezioni solo le richieste che contengono allegati. Questa opzione può essere utile se una delle preoccupazioni principali è rappresentata dalle richieste associate alla pubblicazione di file riservati.

Ignora richieste a host o domini

Fa sì che il server ignori le richieste agli host o ai domini specificati. Questa opzione può essere utile se si prevede molto traffico HTTP tra i domini della sede aziendale e delle filiali. È possibile digitare uno o più nomi host o di dominio (ad esempio `www.azienda.com`), ciascuno su una riga distinta.

Ignora richieste da agenti utente

Fa sì che il server ignori le richieste dagli agenti utente (client HTTP) specificati. Questa opzione può essere utile se l'organizzazione usa un programma o una lingua (quale Java) che fa frequenti richieste HTTP. È possibile digitare uno o più valori dell'agente utente, ciascuno su una riga distinta.

- 5 Verificare o modificare le opzioni di filtro per le risposte dei server Web. Le opzioni della sezione **Filtraggio risposte** sono le seguenti:

Ignora risposte inferiori a

Specifica la dimensione minima del corpo delle risposte HTTP ispezionate da questo server (l'impostazione predefinita è 4096 byte).

Ispeziona tipo di contenuto

Specifica i tipi di contenuti MIME che Symantec Data Loss Prevention deve controllare nelle risposte. Per impostazione predefinita, questo campo contiene valori di tipo contenuto per i formati Microsoft Office, PDF e testo semplice. Per aggiungerne altri, digitare un tipo di contenuto MIME per riga. Ad esempio digitare `application/word2013` affinché Symantec Data Loss Prevention analizzi i file Microsoft Word 2013.

Si tenga presente che in genere è più efficiente specificare i tipi di contenuto MIME a livello del proxy Web.

Ignora risposte da host o domini

Fa sì che il server ignori le risposte dagli host o dai domini specificati. È possibile digitare uno o più nomi host o di dominio (ad esempio `www.azienda.com`), ciascuno su una riga distinta.

Ignora risposte da agenti utente

Fa sì che il server ignori le risposte agli agenti utente (client HTTP) specificati. È possibile digitare uno o più valori dell'agente utente, ciascuno su una riga distinta.

- 6 Verificare o modificare le impostazioni per la connessione ICAP tra il server proxy HTTP e il server Web Prevent. Le opzioni della sezione **Connessione** sono le seguenti:

Porta TCP	Specifica il numero della porta TCP sulla quale il server riceve le richieste ICAP. Questo numero deve corrispondere al valore configurato sul proxy HTTP che invia le richieste ICAP a questo server. Il valore consigliato è 1344.
Numero massimo di richieste	Specifica il numero massimo di connessioni di richiesta ICAP simultanee dal proxy HTTP. Il valore predefinito è 25.
Numero massimo di risposte	Specifica il numero massimo di connessioni di risposta ICAP simultanee dal proxy HTTP. Il valore predefinito è 25.
Backlog connessione	Specifica il numero di connessioni in attesa consentite. Una connessione in attesa è un utente che attende una risposta HTTP dal browser. Il valore minimo è 1. Se il proxy HTTP riceve un numero eccessivo di richieste (o risposte), le gestisce in base alla configurazione del proxy. È possibile configurare il proxy HTTP in modo che blocchi eventuali richieste (o risposte) oltre il numero limite.

- 7 Fare clic su **Salva** per chiudere la schermata **Configura server**, quindi fare clic su **Fine** per chiudere la schermata **Dettagli server**.

Informazioni sulla configurazione di server proxy

È necessario configurare almeno un server proxy HTTP per inoltrare richieste o risposte Web a Network Prevent for Web Server. Il proxy HTTP funziona come client ICAP per Network Prevent for Web Server. Symantec Data Loss Prevention supporta modalità di ICAP sia di modifica richiesta (REQMOD) sia di modifica risposta (RESPMOD). Se si desidera analizzare le richieste come risposte, utilizzare un Network Prevent for Web Server per analizzare le richieste. Utilizzare un secondo Network Prevent for Web Server per analizzare le risposte.

Notare che la maggior dei proxy server forniscono i metodi per il filtraggio di ciò che viene inoltrato al venNetwork Prevent for Web Server sia in modalità REQMOD sia in modalità RESPMOD. Per informazioni dettagliate consultare la documentazione del server proxy.

Vedere ["Configurazione di uno o più server proxy"](#) a pagina 1812.

Vedere ["Configurazione di servizi in modalità di richiesta e risposta"](#) a pagina 1811.

Configurazione di servizi in modalità di richiesta e risposta

Per i dettagli della configurazione del server proxy, consultare la documentazione del server proxy o contattare l'amministratore del server.

Per configurare un server proxy

- 1 **REQMOD.** Sul server proxy creare un servizio REQMOD ICAP che inoltri le richieste al server Network Prevent for Web. Se il server proxy supporta diversi protocolli, configurarlo in modo che gestisca i protocolli desiderati.

Per la modalità REQMOD, un servizio ICAP del server proxy deve avere il seguente aspetto:

```
icap://ip_address|FQDN[:port]/reqmod
```

- 2 **RESPMOD.** Sul server proxy, creare un servizio REQMOD ICAP che inoltri le risposte al server Network Prevent for Web. Se il server proxy supporta diversi protocolli, configurarlo in modo che gestisca i protocolli desiderati.

Per la modalità RESPMOD, un servizio ICAP del server proxy deve avere il seguente aspetto:

```
icap://ip_address|FQND[:port]/respmod
```

Dove:

- *ip_address|FQDN* identifica il server &pn.NetworkPreventWeb con un indirizzo IP o un nome di dominio completo.
- *Port* è il numero di porta su cui ascolta il server &pn.NetworkPreventWeb. La definizione del numero di porta è opzionale quando viene utilizzata la porta ICAP predefinita (1344).
- */reqmod* è obbligatorio per il funzionamento corretto nella modalità REQMOD.
- */respmod* è obbligatorio per il funzionamento corretto in modalità RESPMOD.

Esempi:

```
icap://10.66.194.45/reqmod
icap://10.66.194.45:1344/reqmod
icap://netmonitor1.company.com/reqmod
icap://10.66.194.45/respmod
icap://10.66.194.45:1344/respmod
icap://netmonitor1.company.com/respmod
```

La porta specificata nella definizione del servizio ICAP sul proxy deve corrispondere alla porta su cui ascolta il server Network Prevent for Web.

Vedere ["Informazioni sulla configurazione di server proxy"](#) a pagina 1810.

Configurazione di uno o più server proxy

Per impostazione predefinita, il server Network Prevent for Web può accettare connessioni alla porta di servizio ICAP da qualsiasi sistema sulla rete. Per motivi di sicurezza è possibile limitare le connessioni ICAP solo ai sistemi designati (o inseriti nella lista bianca). Dopo avere inserito nella lista bianca uno o più sistemi, i sistemi che non sono inclusi nella lista non possono connettersi alla porta del servizio ICAP del server Network Prevent for Web.

Si tenga presente che una lista bianca di server proxy può essere influenzata dall'impostazione **Icap.BindAddress**. Per impostazione predefinita, l'impostazione **Icap.BindAddress** è 0.0.0.0 e il listener esegue il binding a tutti gli indirizzi disponibili. Se **Icap.BindAddress** richiede al listener il binding a un IP specifico, un proxy della lista bianca deve anche essere in grado di raggiungere l'indirizzo del listener.

Per creare una lista bianca dei sistemi autorizzati a creare una connessione alla porta del servizio ICAP del server Mobile Email Monitor:

- 1 Selezionare **Sistema > Server e rilevatori > Panoramica** e fare clic sul server Network Prevent for Web desiderato.
- 2 Nella schermata **Dettagli server/rilevatore** visualizzata fare clic su **Impostazioni server**.
- 3 Scorrere verso il basso fino all'impostazione **Icap.AllowHosts**.

Per impostazione predefinita, **Icap.AllowHosts** è impostato su *any*. Ciò significa che tutti gli altri sistemi sulla rete possono comunicare con questo server Mobile Email Monitor.

- 4 È possibile limitare i sistemi autorizzati a connettersi con questo server Network Prevent for Web. Eliminare *any* e immettere gli indirizzi IP o i nomi di dominio completi (FQDN) dei sistemi che si desidera autorizzare.

Separare più indirizzi con le virgole. Ad esempio:

123.14.251.31,cacheweb.org.azienda.com,123.14.223.111. Utilizzare le virgole solo per separare più voci. Non includere spazi.

- 5 Fare clic su **Salva**.

La modifica a questa impostazione diventa effettiva dopo il riavvio del server.

Vedere ["Informazioni sulla configurazione di server proxy"](#) a pagina 1810.

Attivazione dell'elaborazione GET per Network Prevent for Web

Per impostazione predefinita, Network Prevent for Web non elabora i comandi HTTP GET a causa dell'elevato volume di traffico. Per consentire al server di elaborare i comandi GET, attenersi alla seguente procedura.

Per attivare l'elaborazione GET con Network Prevent for Web

- 1 Configurare il server Web in modo che inoltri le richieste GET al server Network Prevent for Web, come descritto nella documentazione del server proxy.
- 2 Assicurarsi che l'impostazione server avanzata **L7.processGets** nel server Network Prevent for Web sia true (impostazione predefinita).
- 3 Ridurre il valore dell'impostazione server avanzata **L7.minSizeofGetURL** nel server Network Prevent for Web. Ridurre dall'impostazione predefinita (100) a un numero di byte inferiore alla lunghezza dell'URL del sito Web più breve da cui si desidera elaborare i comandi GET. Una dimensione URL minima pari a 10 dovrebbe essere appropriata tutti i casi. Si noti tuttavia che la riduzione della dimensione minima dei comandi GET aumenta il numero di richieste da elaborare e quindi il carico del traffico del server.
- 4 Regolare l'impostazione **Ignora richieste inferiori a** nella sezione ICAP della pagina **Dettagli server** di Network Prevent for Web. Ridurla dall'impostazione predefinita di 4096 byte a un valore inferiore che autorizzi la richiesta per l'ispezione DLP. Tenere tuttavia presente che una riduzione del valore incrementa il carico di traffico del server.

Vedere ["Attivazione dell'elaborazione GET con Network Monitor"](#) a pagina 1789.

Creazione di politiche per Network Prevent for Web

È possibile creare le politiche che includono una qualsiasi delle regole di risposta standard. Ad esempio, Aggiungi commento, Limita conservazione dati incidenti, Registrazione a un server Syslog, Invia notifica e-mail e Imposta stato.

Vedere ["Informazioni sui report Symantec Data Loss Prevention"](#) a pagina 1632.

È inoltre possibile incorporare le regole specifiche in Network Prevent for Web Server, come di seguito:

■ Network Prevent: blocca HTTP/HTTPS

Blocca le pubblicazioni che contengono dati riservati (come definito nelle politiche). Questo include pubblicazioni sul Web, messaggi e-mail basati sul Web e file caricati su siti Web o messaggi e-mail basati su Web allegati.

Nota: Alcune applicazioni potrebbero non fornire una risposta adeguata all'azione di risposta **Network Prevent: blocca HTTP/HTTPS**. Questo comportamento è stato osservato con l'applicazione Yahoo! Mail quando un server di rilevazione blocca un caricamento di file. Se un utente prova a caricare un allegato di e-mail e l'allegato attiva un'azione di risposta **Network Prevent: blocca HTTP/HTTPS**, Yahoo! Mail non risponde o visualizza un messaggio di errore per indicare che il file è bloccato. Eppure, Yahoo! Mail sembra continuare il caricamento del file selezionato, ma il caricamento non viene completato. A un certo punto, l'utente deve annullare manualmente il caricamento premendo **Annulla**.

Anche altre applicazioni potrebbero mostrare questo comportamento, a seconda di come viene gestita la richiesta di blocco. In questi casi, viene creato un incidente del server di rilevazione e il caricamento del file viene bloccato anche se l'applicazione non fornisce alcuna indicazione.

■ **Network Prevent: rimuovi contenuto HTTP/HTTPS**

Rimuove i dati riservati dalle pubblicazioni che contengono dati riservati (come definito nelle politiche). Questo include messaggi e-mail basati sul Web e file caricati su siti Web o messaggi e-mail basati su Web allegati. Tenere presente che l'azione Rimuovi contenuto HTTP/HTTPS funzioni solo su richieste.

■ **Network Prevent: blocca richiesta FTP**

Blocca trasferimenti FTP che contengono dati riservati (come definito nelle politiche).

Per dettagli sulla configurazione di qualsiasi azione di regola di risposta, aprire la guida in linea. Accedere a **Gestisci > Politiche > Regole di risposta** e fare clic su **Aggiungi regola di risposta**.

Anche se non vengono incorporate le regole di risposta nella politica, Network Prevent for Web acquisisce gli incidenti a condizione che le politiche contengano le regole di rilevamento. È possibile configurare tali politiche affinché monitorino l'attività Web e FTP sulla rete prima di implementare le politiche che bloccano o rimuovono il contenuto.

Se il proxy è configurato per l'inoltro di risposte e richieste HTTP/HTTPS, le politiche lavorano su entrambe. Ad esempio, le politiche vengono applicate al caricamento su un sito Web e al download da un sito Web.

Per creare una politica di test per Network Prevent for Web

- 1 Nella console di amministrazione Enforce Server, creare una regola di risposta che comprenda una delle azioni specifiche di Network Prevent for Web. Ad esempio, creare una regola di risposta che comprenda l'azione **Network Prevent: blocca HTTP/HTTPS**.

Vedere "[Configurazione di regole di risposta](#)" a pagina 1491.

- 2 Creare una politica che comprenda la regola di risposta configurata nel passaggio precedente.

Ad esempio, creare una politica Test Policy nel modo seguente:

- Includere una regola di rilevamento **Contenuto corrispondente a parola chiave** che corrisponde alla parola chiave "secret".
- Includere una regola di risposta **Network Prevent: blocca HTTP/HTTPS**.
- Associarla al gruppo di politiche Predefinito.

Vedere ["Configurazione di politiche"](#) a pagina 422.

Test di Network Prevent for Web

È possibile testare Network Prevent for Web inviando un'e-mail Web che viola la politica di test.

Per testare il sistema

- 1 Aprire un browser con accesso a Internet tramite il server proxy HTTP.
- 2 Nel browser, accedere a un account e-mail Web di prova e inviare un'e-mail con un allegato contenente dati riservati. Ad esempio, accedere a un account Hotmail e inviare un'e-mail con un allegato contenente la parola *secret* e altri paragrafi di testo.
- 3 Nella console di amministrazione di Enforce Server, accedere a **Incidenti > Rete** e fare clic su **Incidenti - Tutti**. Individuare l'incidente risultante. Ad esempio, individuare una voce di incidente che include la marcatura orario e il nome della politica appropriati.
- 4 Fare clic sulla voce dell'incidente corrispondente per vedere l'istantanea completa dell'incidente.

Vedere ["Informazioni sulle strategie per l'utilizzo di report"](#) a pagina 1633.

Informazioni di risoluzione dei problemi per Network Prevent for Web Server

La seguente tabella descrive un problema comune durante l'utilizzo di Network Prevent for Web Server e suggerisce una possibile soluzione.

Tabella 58-1 Risoluzione dei problemi

Problema	Possibile soluzione
<p>Gli incidenti vengono visualizzati nei report Rete, ma Symantec Data Loss Prevention non esegue l'azione specificata nella regola di risposta relativa.</p>	<p>Si tratta del comportamento previsto quando Network Prevent for Web Server è in esecuzione in modalità di prova (impostazione predefinita). Se non si desidera l'esecuzione in modalità di prova, modificare l'impostazione.</p> <p>Vedere "Configurazione del server Network Prevent for Web" a pagina 1807.</p>

Individuazione della posizione di archiviazione dei dati riservati

- [Capitolo 59. Informazioni su Network Discover](#)
- [Capitolo 60. Impostazione e configurazione di Network Discover](#)
- [Capitolo 61. Opzioni di configurazione target di scansione Network Discover](#)
- [Capitolo 62. Gestione delle scansioni target di Network Discover](#)
- [Capitolo 63. Utilizzo dei plug-in FlexResponse server per riparare gli incidenti](#)
- [Capitolo 64. Configurazione delle scansioni dell'archiviazione cloud Box utilizzando un server di rilevamento on-site](#)
- [Capitolo 65. Impostazione di scansioni di condivisioni file](#)
- [Capitolo 66. Impostazione delle scansioni di database Lotus Notes](#)
- [Capitolo 67. Impostazione delle scansioni di database SQL](#)
- [Capitolo 68. Impostazione delle scansioni di server SharePoint](#)
- [Capitolo 69. Impostazione delle scansioni di server Exchange](#)

- [Capitolo 70. Informazioni sui rilevatori Network Discover](#)
- [Capitolo 71. Impostazione della scansione di file system](#)
- [Capitolo 72. Impostazione della scansione di server Web](#)
- [Capitolo 73. Impostazione della scansione di archivi Documentum](#)
- [Capitolo 74. Impostazione della scansione di archivi Livelink](#)
- [Capitolo 75. Impostazione dei servizi Web per target di scansione personalizzati](#)

Informazioni su Network Discover

Il capitolo contiene i seguenti argomenti:

- [Informazioni su Network Discover/Cloud Storage Discover](#)
- [Funzionamento di Network Discover/Cloud Storage Discover](#)

Informazioni su Network Discover/Cloud Storage Discover

Network Discover individua i dati riservati esposti sottoponendo a scansione un'ampia gamma di archivi di dati aziendali. Questi archivi di dati includono archiviazione cloud Box, file server, database, Microsoft SharePoint, IBM (Lotus) Notes, Documentum, OpenText (Livelink), Microsoft Exchange, server Web e altri.

Network Discover/Cloud Storage Discover può eseguire la scansione delle seguenti origini dati:

- Archiviazione cloud Box
Vedere ["Configurazione delle scansioni dei target di archiviazione cloud Box utilizzando un server di rilevazione on-site"](#) a pagina 1899.
- Condivisioni file di rete (CIFS, NFS o DFS)
Vedere ["Impostazione delle scansioni di file system"](#) a pagina 1906.
- File system locali su computer portatili e desktop Windows
File system locali su server Windows, Linux, AIX e Solaris
Vedere ["Impostazione della scansione remota di file system"](#) a pagina 1986.
- Database IBM (Lotus) Notes

Vedere ["Impostazione delle scansioni del server di database di IBM \(Lotus\) Notes"](#) a pagina 1931.

- Database SQL

Vedere ["Impostazione delle scansioni del server di database SQL"](#) a pagina 1938.

- Server Microsoft SharePoint

Vedere ["Impostazione delle scansioni di server SharePoint"](#) a pagina 1946.

- Server Microsoft Exchange

Vedere ["Impostazione della scansione di server di repository Exchange"](#) a pagina 1965.

- Documentum

Vedere ["Configurazione della scansione remota degli archivi Documentum"](#) a pagina 2009.

- OpenText (Livelink)

Vedere ["Configurazione della scansione remota degli archivi OpenText \(Livelink\)"](#) a pagina 2018.

- Server Web (siti Web e applicazioni basate su Web)

Vedere ["Configurazione di una scansione remota di Web Server"](#) a pagina 1998.

- Personalizzato

I servizi Web espongono un punto di integrazione personalizzato. È possibile scrivere un codice personalizzato per eseguire la scansione di qualsiasi archivio. Il codice personalizzato effettua una ricerca per indicizzazione all'interno dell'archivio e inserisce il contenuto in un Network Discover/Cloud Storage Discover Server per la scansione. È possibile eseguire le scansioni di applicazioni personalizzate e archivi con i servizi Web.

Vedere ["Configurazione dei servizi Web per target di scansione personalizzati"](#) a pagina 2026.

È possibile utilizzare Veritas Data Insight assieme a Network Discover per aggiungere ricche funzionalità alla propria distribuzione di Symantec Data Loss Prevention. Con Veritas Data Insight è possibile monitorare l'accesso ai file per identificare automaticamente l'utente dati di un file in base alla cronologia degli accessi. Le informazioni di utilizzo vengono quindi inserite automaticamente nei dettagli di incidente di file che violano le politiche Symantec Data Loss Prevention. Ciò consente di identificare dati sensibili assieme agli utenti responsabili per consentire una riparazione e una gestione dei dati più efficienti.

Vedere la *Guida all'implementazione di Symantec Data Loss Prevention Data Insight*.

La piattaforma FlexResponse estende ulteriormente le funzionalità di Network Discover. La piattaforma FlexResponse consente la creazione di azioni di riparazione personalizzate complete per i file rilevati tramite Symantec Data Loss Prevention Network Discover. FlexResponse supporta Symantec e soluzioni di protezione di file di terze parti inclusi Enterprise Digital Rights Management e crittografia. FlexResponse è un'estensione del prodotto Network Protect e il prodotto Network Protect è necessario per la funzionalità FlexResponse.

Durante la riparazione di un incidente, è possibile utilizzare i plug-in installati di FlexResponse per riparare incidenti.

Consultare il *Manuale per sviluppatori della piattaforma FlexResponse di Symantec Data Loss Prevention* o contattare il supporto di Symantec Data Loss Prevention per un elenco dei plug-in disponibili.

Vedere ["Utilizzo dei plug-in personalizzati di FlexResponse server per riparare gli incidenti"](#) a pagina 1887.

Funzionamento di Network Discover/Cloud Storage Discover

Il server Network Discover/Cloud Storage Discover individua una vasta gamma di dati riservati esposti. Comunica con Enforce Server per ottenere informazioni sulle politiche e sui target di scansione. Invia le informazioni sui dati riservati esposti che trova a Enforce Server per il reporting e la riparazione.

[Figura 59-1](#) mostra il server Network Discover in una posizione sicura nella LAN aziendale.

Il server Network Discover/Cloud Storage Discover è connesso a Enforce Server e ogni server esegue le attività relative all'individuazione dei dati riservati esposti.

È possibile configurare molteplici server `&pn.NetworkDiscoverFull` per distribuire le attività.

Vedere ["Aggiunta di un server di rilevazione"](#) a pagina 268.

Vedere ["Informazioni sulla scansione della griglia"](#) a pagina 1874.

Il server Network Discover/Cloud Storage Discover esegue la scansione dei target selezionati, legge i file o gli archivi e rileva la presenza di informazioni riservate.

Enforce Server contiene l'interfaccia utente in cui vengono svolte le seguenti attività:

- Configurazione delle scansioni dei target.
- Selezione degli archivi target.
- Definizione dei filtri per le scansioni.
- Pianificazione delle scansioni.

Vedere ["Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover"](#) a pagina 1826.

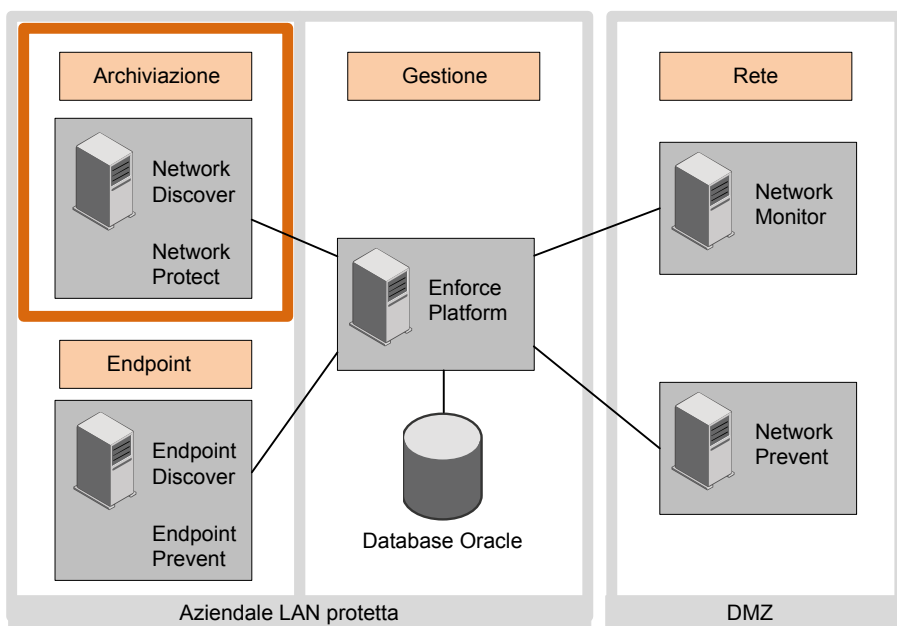
Enforce Server inoltre gestisce le scansioni eseguite sui server Network Discover/Cloud Storage Discover e visualizza lo stato delle scansioni nell'interfaccia utente.

Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.

Dopo il completamento di una scansione, è possibile visualizzare i report dei dati riservati esposti su Enforce Server.

Vedere ["Informazioni sui report per Network Discover"](#) a pagina 1608.

Figura 59-1 Network Discover



Impostazione e configurazione di Network Discover

Il capitolo contiene i seguenti argomenti:

- [Impostazione e configurazione di Network Discover/Cloud Storage Discover](#)
- [Modifica della configurazione del server Network Discover/Cloud Storage Discover](#)
- [Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover](#)
- [Modifica di un target di Network Discover/Cloud Storage Discover esistente](#)

Impostazione e configurazione di Network Discover/Cloud Storage Discover

La configurazione di un target di scansione di Network Discover/Cloud Storage Discover comporta vari passaggi. Ognuno di questi passaggi è necessario per implementare la scansione di target di Network Discover/Cloud Storage Discover.

Tabella 60-1 Impostazione e configurazione di Network Discover

Passaggio	Azione	Dettagli
1	Modificare la configurazione del server Network Discover/Cloud Storage Discover, se necessario.	Vedere "Modifica della configurazione del server Network Discover/Cloud Storage Discover" a pagina 1824.

Passaggio	Azione	Dettagli
2	Creare un gruppo di politiche.	<p>Accedere a Sistema > Server e rilevatori > Gruppi di politiche.</p> <p>Nella schermata Elenco gruppo di politiche visualizzata, fare clic su Aggiungi.</p> <p>Vedere "Creazione e modifica di gruppi di politiche" a pagina 447.</p>
3	Creare una politica.	<p>Accedere a Gestisci > Politiche > Elenco politiche su Enforce Server.</p> <p>Selezionare Aggiungere una politica vuota.</p> <p>Aggiungere una regola alla politica.</p> <p>Vedere "Configurazione di politiche" a pagina 422.</p>
4	Prima di utilizzare Network Protect per un target di Discover di condivisione file, creare una regola di risposta. L'utilizzo di Network Protect è facoltativo.	<p>Vedere "Informazioni sulle regole di risposta" a pagina 1468.</p>
5	Creare un target di Network Discover/Cloud Storage Discover.	<p>Accedere a Gestisci > Scansione Discover > Target di Discover su Enforce Server.</p> <p>Fare clic su Nuovo target e utilizzare il menu a discesa per selezionare il tipo di target specifico.</p> <p>Vedere "Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover" a pagina 1826.</p>
6	Impostare le opzioni per il target.	<p>Vedere "Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover" a pagina 1830.</p>
7	Configurare i report.	<p>Vedere "Informazioni sui report Symantec Data Loss Prevention" a pagina 1632.</p>

Modifica della configurazione del server Network Discover/Cloud Storage Discover

Dopo l'installazione dei server Network Discover/Cloud Storage Discover e la registrazione degli stessi con Enforce Server, è possibile modificare la configurazione del server Network Discover/Cloud Storage Discover.

Il server Network Discover/Cloud Storage Discover può essere installato su un computer virtuale. Per i tipi di computer virtuali supportati, vedere la *Guida alla compatibilità e requisiti di sistema di Symantec Data Loss Prevention*.

Se è stata configurata una scansione incrementale, l'indice relativo viene automaticamente distribuito a tutti i Discover Server, inclusi quelli nuovi.

Vedere ["Informazioni sulle scansioni incrementali"](#) a pagina 1869.

Per modificare la configurazione di un server Network Discover/Cloud Storage Discover

- 1 Nella console di amministrazione di Enforce Server, accedere a **Sistema > Server e rilevatori > Panoramica**. Quindi fare clic sul server da modificare.

Viene visualizzata la schermata **Dettagli server/rilevatore** appropriata in cui sono riportate informazioni generali sul server, informazioni sulla configurazione, gli indici distribuiti e gli eventi recenti del server.

- 2 Fare clic su **Configura**.

Viene visualizzata la schermata **Configura server** con opzioni di configurazione per il tipo di server.

- 3 Modificare la configurazione del server.

Le seguenti opzioni di configurazione si trovano nella scheda **Generale** :

- **Nome**
Il nome del server di rilevazione (utilizzato per le visualizzazioni nella console di amministrazione di Enforce Server). La modifica di questa impostazione per un server di rilevazione esistente ha effetto sulle opzioni di filtro nei report di Symantec Data Loss Prevention. I server Network Discover/Cloud Storage Discover sono server di rilevazione.
- **Host**
Il nome host o l'indirizzo IP del server di rilevazione su cui il server di rilevazione ascolta le connessioni a Enforce Server. È possibile che sia necessario modificare questa impostazione quando si sostituisce un computer host del server Network Discover/Cloud Storage Discover.
- **Porta**
Il server di rilevazione utilizza il numero di porta per accettare le connessioni da Enforce Server. Questo valore deve essere maggiore di 1024. Deve anche corrispondere al valore della proprietà `listenPort` nel file `Communication.properties` del server di rilevamento. Questo file si trova in `\Programmi\Symantec\Data Loss Prevention\Detection Server\15.1\Protect\config` in Windows o in `opt/Symantec/DataLossPrevention/Detection Server/15.1/Protect/config` su Linux. Se si modifica questa impostazione, riavviare il server di rilevamento dopo

la modifica del valore di `listenPort` nel file `Communication.properties`. Non dovrebbe essere necessario modificare questa impostazione dopo un'installazione riuscita. Vedere ["Controlli server"](#) a pagina 242.

- 4 La configurazione per le scansioni parallele viene eseguita nella scheda **Discover**. Immettere il numero di scansioni parallele da eseguire su questo server Network Discover/Cloud Storage Discover. Il valore predefinito è 1.

Il numero massimo può essere aumentato in qualunque momento. Dopo l'aumento, tutte le scansioni in coda eseguibili sul server Network Discover/Cloud Storage Discover vengono avviate.

Il numero può essere diminuito solo se nel server Network Discover/Cloud Storage Discover non sono in esecuzione scansioni. Prima di ridurre il numero, sospendere o arrestare tutte le scansioni in esecuzione nel server Network Discover/Cloud Storage Discover.

Le scansioni parallele dei tipi di target di server e rilevatori sono supportate.

Vedere ["Configurazione delle scansioni parallele di target di Network Discover/Cloud Storage Discover"](#) a pagina 1873.
- 5 Dopo la modifica della configurazione di un server, fare clic su **Salva** per uscire dalla schermata **Configura server** e quindi fare clic su **Fine** per uscire dalla schermata **Dettagli server**.
- 6 Per visualizzare le scansioni attive sul server Network Discover/Cloud Storage Discover, accedere a **Politiche > Scansione Discover > Discover Server**.

Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.

Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover

Prima di aggiungere un target di Network Discover/Cloud Storage Discover, è necessario completare la configurazione del server Network Discover/Cloud Storage Discover.

Vedere ["Impostazione e configurazione di Network Discover/Cloud Storage Discover"](#) a pagina 1823.

Per aggiungere un target di Network Discover/Cloud Storage Discover

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su **Nuovo target** e utilizzare il menu a discesa per selezionare il tipo di target specifico.

- 3 Nella scheda **Generale**, digitare il nome di questo target di Network Discover/Cloud Storage Discover. Questo nome viene visualizzato per la gestione delle scansioni.
 Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.
 - 4 Immettere gli altri parametri richiesti. Immettere il gruppo di politiche. Immettere il server Network Discover/Cloud Storage Discover.
 Vedere ["Configurazione dei campi obbligatori per i target di Network Discover"](#) a pagina 1832.
 - 5 Continuare l'aggiunta di un nuovo target con le voci specifiche di quel tipo di target.
- | | |
|--|---|
| Archiviazione cloud Box | Vedere "Configurazione delle scansioni dei target di archiviazione cloud Box utilizzando un server di rilevazione on-site" a pagina 1899. |
| File server e condivisioni di rete (CIFS, NFS, DFS) | Vedere "Impostazione delle scansioni di file system" a pagina 1906. |
| Database IBM (Lotus) Notes | Vedere "Impostazione delle scansioni del server di database di IBM (Lotus) Notes" a pagina 1931. |
| Database SQL | Vedere "Impostazione delle scansioni del server di database SQL" a pagina 1938. |
| File system locali su computer portatili e desktop Windows | Vedere "Impostazione della scansione remota di file system" a pagina 1986. |
| File system locali su server Windows, Linux, AIX e Solaris | |
| Microsoft Exchange | Vedere "Impostazione della scansione di server di repository Exchange" a pagina 1965. |
| Microsoft SharePoint | Vedere "Impostazione delle scansioni di server SharePoint" a pagina 1946. |
| Documentum | Vedere "Configurazione della scansione remota degli archivi Documentum" a pagina 2009. |
| OpenText (Livelink) | Vedere "Configurazione della scansione remota degli archivi OpenText (Livelink)" a pagina 2018. |
| Server Web (siti Web e applicazioni basate su Web) | Vedere "Configurazione di una scansione remota di Web Server" a pagina 1998. |
- 6 Configurare parametri opzionali per i target di Network Discover/Cloud Storage Discover.
 Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Modifica di un target di Network Discover/Cloud Storage Discover esistente

Per impostare varie opzioni di configurazione, modificare la configurazione di un target di Network Discover/Cloud Storage Discover.

Durante tale operazione, è anche possibile aggiungere un nuovo target di Network Discover/Cloud Storage Discover e impostare opzioni.

Vedere ["Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover"](#) a pagina 1826.

Per modificare un target di Network Discover/Cloud Storage Discover

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su uno dei target di scansione nell'elenco per aprire il target da modificare.
- 3 Modificare l'opzione desiderata.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Opzioni di configurazione target di scansione Network Discover

Il capitolo contiene i seguenti argomenti:

- Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover
- Configurazione dei campi obbligatori per i target di Network Discover
- Pianificazione delle scansioni di Network Discover/Cloud Storage Discover
- Autenticazione tramite password per il contenuto sottoposto a scansione Network Discover
- Gestione delle autorizzazioni di archiviazione cloud
- Password crittografate nei file di configurazione
- Impostazione di Network Discover/Cloud Storage Discover filtri per includere o escludere oggetti dalla scansione
- Filtraggio dei target di Discover per dimensione dell'oggetto
- Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica
- Ottimizzazione delle risorse con le opzioni di limitazione delle scansioni di Network Discover/Cloud Storage Discover
- Creazione di un inventario delle posizioni di dati riservati non protetti

Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover

Utilizzare le schede **Generale**, **Autorizzazione**, **Contenuto sottoposto a scansione**, **Filtri** e **Avanzate** per configurare un target di scansione di Network Discover/Cloud Storage Discover.

La scheda **Generale** è disponibile per tutti i tipi di target.

Le schede **Autorizzazione**, **Contenuto sottoposto a scansione**, **Filtri** e **Avanzate** sono disponibili solo per alcuni tipi di target.

Vedere ["Modifica di un target di Network Discover/Cloud Storage Discover esistente"](#) a pagina 1828.

Per informazioni di configurazione supplementari specifiche a un tipo di obiettivo, fare riferimento alla sezione per quel tipo di target.

Tenere presente che tutti i filtri sono combinati con "and" se viene fornito un valore. Considerare tutti i valori di filtro quando si aggiungono o modificano filtri di scansione, per evitare di includere o escludere involontariamente tutto dalla scansione.

Per l'aggiunta o la modifica di un target, utilizzare le seguenti opzioni di configurazione:

Attività opzionali	Scheda nel target di scansione	Descrizione dell'attività
Configurare campi obbligatori. Questi campi obbligatori devono essere impostati quando si aggiunge un nuovo target.	Generale	Vedere "Configurazione dei campi obbligatori per i target di Network Discover" a pagina 1832.
Pianificare scansioni di Network Discover/Cloud Storage Discover.	Generale	Vedere "Pianificazione delle scansioni di Network Discover/Cloud Storage Discover" a pagina 1833.
Configurare scansioni incrementali.	Generale	Vedere "Scansione di elementi nuovi o modificati con scansioni incrementali" a pagina 1870.
Assegnare i server di rilevamento per la scansione.	Destinazione	Selezionare il server di rilevamento in cui eseguire la scansione. Per le scansioni di File System, è possibile scegliere di eseguire una scansione della griglia utilizzando più server di rilevamento Vedere "Informazioni sulla scansione della griglia" a pagina 1874.

Attività opzionali	Scheda nel target di scansione	Descrizione dell'attività
Fornire l'autenticazione per l'archiviazione cloud Box.	Autorizzazione	Vedere "Fornitura delle credenziali di autorizzazione dell'archiviazione cloud Box" a pagina 1837.
Fornire l'autenticazione e configurare le credenziali.	Contenuto sottoposto a scansione	Vedere "Autenticazione tramite password per il contenuto sottoposto a scansione Network Discover" a pagina 1835.
Includere o escludere archivi da una scansione.	Filtri	Vedere " Impostazione di Network Discover/Cloud Storage Discover filtri per includere o escludere oggetti dalla scansione" a pagina 1840.
Filtrare target per dimensione di file.	Filtri	Vedere "Filtraggio dei target di Discover per dimensione dell'oggetto" a pagina 1843.
Filtrare target in base alla data dell'ultimo accesso o modifica.	Filtri	Vedere "Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica" a pagina 1844.
Ottimizzare le risorse con la limitazione della scansione.	Avanzate	Vedere "Ottimizzazione delle risorse con le opzioni di limitazione delle scansioni di Network Discover/Cloud Storage Discover" a pagina 1847.
Creare un inventario delle posizioni dei dati riservati non protetti.	Avanzate	Vedere "Creazione di un inventario delle posizioni di dati riservati non protetti" a pagina 1849.
Specificare le opzioni per il rilevamento automatico dello stato di riparazione degli incidenti relativi ai file system di rete.	Avanzate	Vedere "Configurazione delle scansioni del file system" a pagina 1922.
Spostare, mettere in quarantena o crittografare i file presenti nelle condivisioni di file in rete con Network Protect.	Proteggi	Vedere "Configurazione di Network Protect per condivisioni file" a pagina 1928.
Mettere in quarantena o applicare un tag visivo al contenuto dell'archiviazione cloud Box.	Proteggi	Vedere "Configurazione delle opzioni di riparazione per target di archiviazione cloud Box" a pagina 1904.
Mettere in quarantena file nel repository di SharePoint con Network Protect	Proteggi	Vedere "Configurazione Network Protect per i server SharePoint" a pagina 1956.

Configurazione dei campi obbligatori per i target di Network Discover

Per un nuovo target, immettere il nome del target, il gruppo di politiche e il Discover Server in cui possono essere eseguite le scansioni.

Questi campi obbligatori devono essere impostati quando si aggiunge un nuovo target.

Per configurare i campi obbligatori per un target

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.

- 2 Fare clic su **Nuovo target** e utilizzare il menu a discesa per selezionare il tipo di target specifico.

- 3 Nella scheda **Generale**, immettere il **nome** del target di Discover.

Digitare un nome univoco per il target, che non deve contenere più di 255 caratteri.

- 4 Selezionare **Gruppo di politiche**.

Se nessun altro gruppo di politiche è stato selezionato, viene utilizzato il gruppo di politiche predefinito. Per applicare un gruppo di politiche, selezionare il gruppo di politiche da utilizzare per il target. È possibile assegnare più gruppi di politiche a un target.

L'amministratore definisce i gruppi di politiche nella pagina **Elenco gruppo di politiche**. Se il gruppo di politiche che si desidera utilizzare non appare nell'elenco, contattare l'amministratore Symantec Data Loss Prevention.

- 5 Nella scheda **Destinazione**, selezionare il Discover Server (o più Discover Server) in cui si desidera consentire l'esecuzione della scansione.

Se si seleziona più di un server senza specificare una scansione della griglia, Symantec Data Loss Prevention seleziona automaticamente uno dei server all'avvio della scansione.

La funzionalità di scansione della griglia per i target di scansione del file system fornisce un'opzione aggiuntiva che consente di distribuire il carico di lavoro della scansione su tutti i server selezionati, a condizione che si selezionino almeno due server.

Vedere ["Informazioni sulla scansione della griglia"](#) a pagina 1874.

Soltanto i server di rilevamento configurati come Discover Server sono visualizzati nell'elenco. Se è presente solo un Discover Server nella rete, il nome di quel server viene automaticamente specificato. Prima di configurare i target, è necessario configurare i Discover Server. È necessario specificare almeno un server prima di poter eseguire una scansione del target.

- 6 Nella scheda **Contenuto sottoposto a scansione**, è necessario indicare l'elemento da sottoporre a scansione. Fare riferimento alla documentazione relativa a ogni tipo di target per informazioni supplementari su questa voce.

Vedere ["Informazioni su Network Discover/Cloud Storage Discover"](#) a pagina 1819.

- 7 È possibile configurare altre opzioni per questo target.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Pianificazione delle scansioni di Network Discover/Cloud Storage Discover

È possibile pianificare le scansioni di Network Discover/Cloud Storage Discover affinché siano eseguite regolarmente, ad esempio durante la notte o nei fine settimana. È anche possibile pianificare la sospensione delle scansioni durante determinati periodi di tempo, ad esempio quando le risorse sono normalmente utilizzate per altre attività.

Per l'archiviazione cloud, le condivisioni di file, Lotus Notes o i database SQL, la pianificazione delle scansioni può essere specificata completamente con i parametri **Pianificazione scansioni**.

Per i target di rilevatore (quali SharePoint o Exchange), la scansione deve anche essere pianificata dal computer in cui il rilevatore è installato. È necessario gestire manualmente la pianificazione della scansione tra il target di Discover e l'applicazione del rilevatore. I rilevatori sono installati, configurati ed eseguiti esternamente a Enforce Server e al server Network Discover/Cloud Storage Discover. Ad esempio, il rilevatore può essere pianificato per un'esecuzione automatica utilizzando la pianificazione nativa dell'host. È possibile creare un cron job UNIX o aggiungere il rilevatore alla Utilità di pianificazione di Microsoft Windows. Il rilevatore deve essere pianificato per un'esecuzione prima della scansione di Network Discover/Cloud Storage Discover affinché la scansione di Network Discover/Cloud Storage Discover disponga di informazioni da utilizzare.

Se si seleziona una determinata ora per avviare o sospendere una scansione, viene utilizzata la fascia oraria di Enforce Server.

È possibile configurare altre opzioni per questo target.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Per configurare la pianificazione di una scansione

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul nome della scansione che si desidera pianificare.

3 Fare clic sulla scheda **Generale**.

4 Selezionare l'elemento **Avvia processo di scansione come pianificato**.

Quando si seleziona questa casella di controllo per configurare una pianificazione per la scansione del target specificato, l'elenco a discesa Pianifica diventa disponibile. Dopo avere selezionato un'opzione a partire dal elenco a discesa Pianifica, vengono visualizzati dei campi supplementari.

5 Selezionare uno dei seguenti campi supplementari:

Nessuna pianificazione regolare	Salva il target senza una pianificazione.
Esegui scansione una volta	Esegue la scansione una volta, all'ora e alla data specificate.
Esegui scansione ogni giorno	Esegue la scansione del target ogni giorno, all'ora specificata. Selezionare Fino a per arrestare la scansione giornaliera dopo una determinata data.
Esegui scansione ogni settimana	Esegue la scansione del target ogni settimana. Selezionare Fino a per arrestare la scansione settimanale dopo una determinata data.
Esegui scansione ogni mese	Esegue la scansione del target ogni mese. Selezionare Fino a per arrestare la scansione mensile dopo una determinata data.

6 Fare clic su **Salva**.

Per sospendere una scansione durante determinati periodi di tempo

1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.

2 Fare clic sul nome della scansione che si desidera sospendere nei periodi di tempo specificati.

3 Fare clic sulla scheda **Generale**.

4 Selezionare l'elemento **Sospendi scansione in questo periodo**.

5 Selezionare le opzioni di sospensione.

Questa opzione sospende automaticamente le scansioni durante l'intervallo di tempo specificato. È possibile ignorare la sospensione della scansione di un target passando alla schermata Target di Discover e facendo clic sull'icona di avvio per la voce del target. Il periodo di sospensione rimane inalterato e tutte le scansioni future che vengono eseguite in base alla finestra di scansione vengono sospese come specificato. È inoltre possibile riavviare una scansione sospesa facendo clic sull'icona Continua relativa alla voce del target.

Nota: Se la configurazione del target viene modificata durante la sospensione, la configurazione modificata non viene applicata agli elementi già sottoposti a scansione. Quando una scansione viene sospesa e riavviata, la scansione ricomincia da un checkpoint creato quando la scansione è stata sospesa. La configurazione modificata viene utilizzata per gli elementi sottoposti a scansione a partire da quel checkpoint.

6 Fare clic su **Salva**.

Autenticazione tramite password per il contenuto sottoposto a scansione Network Discover

Nella scheda **Contenuto sottoposto a scansione**, inserire le opzioni di configurazione per l'autenticazione.

Evitare i caratteri speciali nelle credenziali di autenticazione. Le credenziali di autenticazione non devono contenere i seguenti caratteri o la scansione non andrà a buon fine:

- Barra verticale (|)
- E commerciale (&)
- Virgolette (singole ' o doppie ")

Per fornire l'autenticazione tramite password per il contenuto sottoposto a scansione

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul nome di una scansione per fornire l'autenticazione della password.
- 3 Fare clic sulla scheda **Contenuto sottoposto a scansione**.
- 4 È possibile fornire le informazioni di autenticazione in vari modi:
 - Usare credenziali archiviate.
Se le credenziali archiviate sono disponibili, selezionare le credenziali nominate a partire menu a discesa in **Usa credenziali salvate**.

- Le credenziali di scansione globali possono essere fornite per tutte le condivisioni in questo target.
 Digitare il nome utente e la password in **Usa queste credenziali**.
 - Credenziali separate dell'autenticazione possono essere fornite per ogni condivisione in un elenco.
 Le credenziali separate sovrascrivono le credenziali di scansione globali, se fornite.
 Fare clic su **Aggiungi** o **Modifica** per fornire le credenziali per ogni condivisione in un elenco.
 Nella sezione **Aggiungi**, inserire condivisione e credenziali con la seguente sintassi:
percorso[, [nome utente, password][, [profondità][, riparazione-nome utente, riparazione-password]]]
 Per gli oggetti omessi, fornire una voce nulla con virgole consecutive.
- 5 Il formato delle credenziali dipende dal tipo di scansione. Per il formato e gli esempi specifici delle credenziali per ogni tipo di target, vedere l'argomento per quel tipo di target.
 Vedere ["Informazioni su Network Discover/Cloud Storage Discover"](#) a pagina 1819.
- 6 È possibile impostare altre opzioni nella scheda **Contenuti scansionati**.
 Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.
 Le credenziali di riparazione possono essere impostate sulla scheda **Proteggi**.
 Vedere ["Configurazione di Network Protect per condivisioni file"](#) a pagina 1928.

Gestione delle autorizzazioni di archiviazione cloud

Prima di poter eseguire scansioni di Discover sui target di archiviazione cloud Box, è necessario autorizzare Symantec Data Loss Prevention ad accedere e a modificare il contenuto dell'utente su tali target. È possibile creare e gestire le autorizzazioni per i target di archiviazione cloud Box nella pagina **Sistema > Impostazioni > Autorizzazione cloud**.

Vedere ["Fornitura delle credenziali di autorizzazione dell'archiviazione cloud Box"](#) a pagina 1837.

È possibile effettuare le seguenti azioni nella pagina **Autorizzazione cloud** :

Tabella 61-1 Azioni della pagina Autorizzazione cloud

Azione	Descrizione
Creare una nuova autorizzazione cloud	<p>È possibile creare una nuova autorizzazione cloud per i target di archiviazione cloud Box.</p> <p>Vedere "Fornitura delle credenziali di autorizzazione dell'archiviazione cloud Box" a pagina 1837.</p> <p>È possibile avere una sola autorizzazione cloud per i target di archiviazione cloud Box.</p>
Modificare un'autorizzazione cloud esistente	<p>Per modificare un'autorizzazione cloud esistente, fare clic sull'icona di modifica.</p> <p>Vedere "Per modificare un'autorizzazione di archiviazione cloud esistente" a pagina 1837.</p>
Eliminare un'autorizzazione cloud	<p>Per eliminare un'autorizzazione cloud, fare clic sull'icona di eliminazione.</p> <p>Non è possibile eliminare un'autorizzazione cloud che è in uso da un target di scansione di Discover.</p>

Modifica delle autorizzazioni di archiviazione cloud esistenti

È possibile modificare le autorizzazioni di archiviazione cloud esistenti nella pagina **Sistema > Impostazioni > Autorizzazione cloud > Modifica autorizzazione di archiviazione cloud**. Utilizzare questa pagina per modificare la maggior parte delle impostazioni esistenti, come **Nome**, **ID client**, **Chiave privata client** e così via.

Per modificare un'autorizzazione di archiviazione cloud esistente

- 1 Nella console di amministrazione di Enforce Server, accedere a **Sistema > Impostazioni > Autorizzazione cloud**.
- 2 Fare clic sull'icona di modifica per l'autorizzazione dell'archiviazione cloud che si desidera modificare nell'elenco **Autorizzazioni di archiviazione cloud**.
- 3 Immettere le modifiche nella schermata **Modifica autorizzazione di archiviazione cloud**.
- 4 Fare clic su **Salva**.

Fornitura delle credenziali di autorizzazione dell'archiviazione cloud Box

L'autorizzazione delle scansioni dell'archiviazione cloud Box richiede tre azioni:

- Creare un'applicazione Box nell'account Box. Questa applicazione dà accesso all'API Box appropriata.

- Creare un'autorizzazione cloud nella console di amministrazione di Enforce Server.
- Autorizzare il target di scansione Discover.

Creazione di un'applicazione Box nell'account Box

La pagina app.box.com/developers/services consente di creare un'applicazione nel proprio account Box.

Per creare un'applicazione Box nell'account Box

- 1 Accedere al proprio account Box come utente amministrativo.
- 2 Passare a app.box.com/developers/services.
- 3 Fare clic su **Introduzione**.
Viene visualizzata la pagina **Crea un'applicazione Box**.
- 4 Inserire un nome per l'applicazione, ad esempio **"Symantec Data Loss Prevention"**, quindi fare clic su **Crea applicazione**.
Viene visualizzata la pagina di modifica per l'applicazione.
- 5 Nella sezione **Informazioni generali**, accertarsi che **Solo accesso a API contenuto** sia selezionato.
- 6 Nella sezione **Parametri OAuth2**, accertarsi che **Autenticazione standard (OAuth2.0 a tre fasi)** sia selezionato.
- 7 Selezionare i seguenti ambiti:
 - **Leggi e scrivi tutti i file e le cartelle**
 - **Gestisci azienda**
 - **Gestisci gruppi**
 - **Gestisci proprietà aziendali**
 - **Gestisci criteri di conservazione**
- 8 Immettere l'URI di Enforce Server nel campo **redirect_uri**.
- 9 Fare clic su **Salva applicazione**.

Dopo aver creato l'applicazione Box, contattare Box per attivare le seguenti impostazioni aggiuntive:

- **Come utente**
- **L'amministratore può fare chiamate per conto degli utenti**
- **L'amministratore o co-amministratore può fare chiamate per chiunque**
- **Può eliminare le notifiche e-mail dalle chiamate API**

Creazione di un'autorizzazione cloud per Box

Dopo aver creato l'applicazione Box, creare l'autorizzazione cloud di Box nella console di amministrazione di Enforce server.

Per creare un'autorizzazione cloud per Box

- 1 Nella console di amministrazione di Enforce Server, accedere a **Sistema > Impostazioni > Autorizzazione cloud**.
- 2 Fare clic su **Nuova autorizzazione di archiviazione cloud**.
Viene visualizzata la schermata **Aggiungi autorizzazione di archiviazione cloud**.
- 3 Nella sezione **Autorizzazione di archiviazione cloud**, compilare **Nome** e **Descrizione** per la nuova autorizzazione.
- 4 Nella sezione **Configurazione client**, immettere l' **ID client** per l'applicazione Box.
L'ID client dell'applicazione Box è il **client_id** che si trova nella pagina di informazioni dell'applicazione Box.
- 5 Immettere la **Chiave privata client** per l'applicazione Box.
La chiave privata client per l'applicazione Box è il **client_secret** che si trova nella pagina di informazioni dell'applicazione Box.
- 6 Immettere di nuovo la chiave privata client.
- 7 Fare clic su **Salva**.

Autorizzazione di una scansione dell'archiviazione cloud Box

Dopo aver creato un'autorizzazione cloud per l'archiviazione cloud Box, è possibile autorizzare una scansione dell'archiviazione cloud Box.

Per autorizzare le scansioni dell'archiviazione cloud Box

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul nome di una scansione per fornire l'autenticazione della password.
- 3 Fare clic sulla scheda **Autorizzazione**.
- 4 Fare clic su **Autorizza**.
Viene visualizzata la finestra di dialogo **Accedere per concedere l'accesso a Box**.
- 5 Immettere le credenziali di autorizzazione Box per questa scansione. È necessario usare le credenziali con i privilegi di amministratore o co-amministratore Box per il contenuto che si desidera sottoporre a scansione. È inoltre necessario disporre delle autorizzazioni necessarie per scaricare i file da sottoporre a scansione.

Password crittografate nei file di configurazione

Crittografare le password nei file di configurazione con l'utilità `EncryptPassword.exe`.

Per crittografare password nei file di configurazione

- 1 Accedere alla directory `bin` dell'installazione rilevatore sul computer rilevatore.

Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.

- 2 Eseguire l'utilità `EncryptPassword.exe`.

Questa utilità esegue la crittografia della password fornita nei file di configurazione rilevatore.

- 3 Quando l'utilità richiede l'immissione di una password, immetterla.

- 4 Fare clic sull'opzione di crittografia.

- 5 Inserire la password crittografata nell'impostazione Password= nel file

`Vontuscanner_typeScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori Web Server"](#) a pagina 2003.

Vedere ["Opzioni di configurazione per i rilevatori Documentum"](#) a pagina 2014.

Vedere ["Opzioni di configurazione per rilevatori Livelink"](#) a pagina 2024.

Impostazione di Network Discover/Cloud Storage Discover filtri per includere o escludere oggetti dalla scansione

I filtri di inclusione ed esclusione consentono di ridurre il numero di elementi e archivi da sottoporre a scansione.

Utilizzare il campo **Filtri di inclusione** per specificare gli elementi che Symantec Data Loss Prevention dovrà elaborare. Se si lascia vuoto il campo **Filtri di inclusione**, Symantec Data Loss Prevention ricerca la corrispondenza con tutti gli oggetti del target selezionato. Se si immette qualsiasi valore nel campo, Symantec Data Loss Prevention analizza solo gli elementi corrispondenti al filtro specificato.

Utilizzare il campo **Filtri di esclusione** per specificare gli elementi che Symantec Data Loss Prevention non deve elaborare. Se si lascia vuoto il campo **Filtri di esclusione**, Symantec Data Loss Prevention analizza tutti gli elementi nel target selezionato. Se si immette qualsiasi valore nel campo, Symantec Data Loss Prevention analizza solo gli elementi non corrispondenti al filtro specificato.

Per ottimizzare la scansione, è possibile suddividere le scansioni che utilizzano filtri di inclusione ed esclusione. Ad esempio è possibile escludere gli elementi binari. È poco probabile che gli elementi binari contengano violazioni di politiche.

Vedere ["Informazioni sull'ottimizzazione delle scansioni di Network Discover/Cloud Storage Discover"](#) a pagina 1865.

Tenere presente che tutti i filtri sono combinati con “and” se viene fornito un valore. Considerare tutti i valori di filtro (ad esempio dimensione e data) quando si aggiungono o modificano i filtri di scansione. Fare attenzione a non includere o escludere tutto involontariamente dalla scansione.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Per configurare i filtri di inclusione o i filtri di esclusione:

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul nome della scansione alla quale si desidera aggiungere i filtri di inclusione o esclusione.
- 3 Fare clic sulla scheda **Filtri**.
- 4 Inserire nomi file o percorsi nei filtri di inclusione ed esclusione per selezionare un sottoinsieme di elementi che Symantec Data Loss Prevention dovrà elaborare. Delimitare le voci mediante virgole, senza spazi. Il filtro del percorso fa distinzione tra maiuscole e minuscole.

Quando vengono utilizzati sia i filtri di inclusione sia i filtri di esclusione, i filtri di esclusione hanno la precedenza.

I nomi di file dei filtri di inclusione e di esclusione sono relativi alla radice del file system. Specificare i percorsi completi o le sottodirectory, come necessario. È consentito l'uso di alcuni caratteri jolly.

La [Tabella 61-2](#) mostra la sintassi per i filtri.

Se la voce del filtro di esclusione supera il limite di 1024 caratteri, è possibile creare un file di esclusione con i nomi dei file da escludere.

- 5 Fare clic su **Salva**.

Per creare un file di esclusione:

- 1 Creare una directory denominata `excludeFiles` nella directory di configurazione Symantec Data Loss Prevention, ad esempio `\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\excludeFiles\`.

Per una configurazione con più server Discovery, una copia della directory e del file deve essere presente in ciascun server Discovery.

- 2 Nella directory creare un file di testo per ciascun set di elementi da escludere.

Ad esempio, è possibile creare un file per ciascun sistema Unix da sottoporre a scansione. Assegnare ai file il nome `nomehost.txt`, dove `nomehost` è il nome del sistema da sottoporre a scansione, fornito nella configurazione target. Il nome host in questo file di testo deve corrispondere esattamente al nome presente nel target Network Discover/Cloud Storage Discover.

- 3 In ciascun file, elencare i percorsi (ognuno su una linea separata) che si desidera escludere dalla ricerca.

I percorsi possono essere file, directory, collegamenti simbolici o directory montate. Ogni percorso deve iniziare con il delimitatore “/” o “\” seguito dal nome di condivisione, dal nome directory e dal nome file. Ad esempio, un percorso valido è
`\condivisioneesclusione\directory esclusione\fileesclusione`.

La [Tabella 61-2](#) mostra la sintassi per i filtri.

Tabella 61-2 Sintassi per filtri di inclusione ed esclusione

Carattere jolly	Descrizione
* (asterisco)	Questo carattere sostitutivo corrisponde a qualsiasi sequenza di caratteri, incluso null.
? (punto interrogativo)	Utilizzare questo carattere sostitutivo per la corrispondenza con un solo carattere nella posizione in cui si trova.
, (virgola)	Corrisponde a un OR logico. Delimitare le voci con una virgola, ma non utilizzare spazi.
Caratteri barra (/) e barra rovesciata (\)	Questi caratteri sono equivalenti. Rappresentano in genere separatori di directory, anche se in Linux la barra rovesciata è un carattere valido in un nome file.
Spazio vuoto all'inizio e alla fine del criterio	Lo spazio vuoto all'inizio e alla fine del criterio viene ignorato. Non utilizzare spazi prima o dopo i virgole che delimitano le voci.

Carattere jolly	Descrizione
Caratteri escape	Il processo di corrispondenza non supporta i caratteri escape, quindi non è possibile stabilire una corrispondenza esplicita con un punto interrogativo, una virgola o un asterisco. In genere i caratteri speciali non sono supportati negli elementi filtro.

La [Tabella 61-3](#) mostra i filtri di esempio.

Tabella 61-3 Filtri di esempio con caratteri jolly

Filtro di esempio	Descrizione
<code>*.txt,*.doc</code>	Questo esempio di filtro di inclusione rileva solo la corrispondenza con file o documenti con le estensioni <code>.txt</code> o <code>.doc</code> e ignora tutto il resto.
<code>*.?</code>	Questo esempio di filtro di inclusione rileva solo la corrispondenza con file o documenti con un'estensione costituita da una sola lettera. Ad esempio, rileva la corrispondenza con i file <code>hello.1</code> e <code>hello.2</code> , ma non con i file <code>hello.doc</code> o <code>hello.html</code> .
<code>*/documentation/*,*/specs/*</code>	Questo esempio di filtro di inclusione rileva solo la corrispondenza con sottodirectory specifiche di una condivisione di file o di un'unità locale, con nome <code>documentation</code> e <code>specs</code> .

La sintassi e gli esempi di scansione dei database SQL sono disponibili nella sezione Database SQL.

Vedere ["Configurazione ed esecuzione di scansioni database SQL"](#) a pagina 1940.

La sintassi e gli esempi di scansione SharePoint sono disponibili nella sezione SharePoint.

Vedere ["Configurazione ed esecuzione delle scansioni dei server SharePoint"](#) a pagina 1950.

Filtraggio dei target di Discover per dimensione dell'oggetto

Utilizzare i filtri di dimensione per escludere elementi dal processo di corrispondenza in base alla relativa dimensione.

I filtri di dimensione sono disponibili solo per i file presenti nell'archiviazione cloud Box, le condivisioni file, i documenti di Lotus Notes, gli elementi di SharePoint e gli elementi di Exchange.

È possibile configurare altre opzioni per il target.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Per escludere elementi in base alla relativa dimensione

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul nome della scansione che si desidera filtrare in base alla dimensione degli elementi.
- 3 Fare clic sulla scheda **Filtri**.
- 4 Immettere valori facoltativi sotto i filtri di dimensione degli elementi.

Symantec Data Loss Prevention include solo gli elementi che corrispondono ai filtri di dimensione specificati. Se si lascia vuoto questo campo, Symantec Data Loss Prevention cerca la corrispondenza con gli elementi di tutte le dimensioni.

Tenere presente che tutti i filtri sono combinati con "and" se viene fornito un valore. Considerare tutti i valori di filtro (ad esempio inclusione, esclusione e data) quando si aggiungono o modificano i filtri di scansione. Fare attenzione a non includere o escludere tutto involontariamente dalla scansione.

- 5 Per escludere elementi più piccoli di una determinata dimensione, immettere un numero nel campo accanto a **Ignora documenti di dimensioni inferiori a**. Selezionare quindi l'unità di misura appropriata (byte, KB o MB) dall'elenco a discesa accanto.
- 6 Per escludere elementi più grandi di una determinata dimensione, immettere un numero nel campo accanto a **Ignora documenti di dimensioni superiori a**. Selezionare quindi l'unità di misura appropriata (byte, KB o MB) dall'elenco a discesa accanto.
- 7 Fare clic su **Salva** per salvare tutti gli aggiornamenti al target.

Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica

Specificare i filtri di data per escludere elementi dal processo di corrispondenza in base alle relative date. Soltanto gli elementi che corrispondono ai filtri di data specificati sono inclusi.

I filtri di data sono disponibili per file nell'archiviazione cloud Box, condivisioni di file, documenti di Lotus Notes e documenti di Microsoft SharePoint e Exchange.

Le scansioni incrementali e differenziali sono disponibili per alcuni tipi di target di Network Discover/Cloud Storage Discover.

Vedere ["Scansione di elementi nuovi o modificati con scansioni incrementali"](#) a pagina 1870.

Vedere ["Scansione di elementi nuovi o modificati con scansioni differenziali"](#) a pagina 1872.

È possibile configurare altre opzioni per il target.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Tenere presente che tutti i filtri sono combinati con "and" se viene fornito un valore. Considerare tutti i valori di filtro (ad esempio inclusione, esclusione e dimensione) quando si aggiungono o modificano filtri di scansione. Fare attenzione a non includere o escludere tutto involontariamente dalla scansione.

Per escludere elementi in base alla data dell'ultimo accesso o modifica

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sulla scheda **Filtri**.
- 3 Immettere valori facoltativi in **Filtri data file**.

4 Selezionare **Esegui scansione solo di file aggiunti o modificati dopo l'ultima scansione completa** per una scansione differenziale.

Vedere ["Scansione di elementi nuovi o modificati con scansioni differenziali"](#) a pagina 1872.

Questa opzione esegue la scansione soltanto degli elementi aggiunti o modificati (a seconda di quali sono più recenti) dopo l'ultima scansione completa.

Se non si seleziona questa opzione, Symantec Data Loss Prevention non utilizza filtri di data. Cerca la corrispondenza con elementi di qualsiasi data nel target specificato.

La prima scansione deve essere una scansione completa. Una scansione completa si verifica se si seleziona questa opzione prima che Symantec Data Loss Prevention esegua una scansione di questo target per la prima volta.

Quando si seleziona questa opzione, è anche possibile selezionare l'opzione **Esegui prossima scansione come completa**. Quando si seleziona questa opzione, i filtri di data per **Esegui scansione solo di file aggiunti o modificati** e per **Esegui scansione solo di ultimi file utilizzati** sono disattivati. La scansione seguente è una scansione completa (se nessuna scansione completa precedente è stata completata). Le scansioni successive esaminano solo gli elementi aggiunti o modificati dopo l'ultima scansione completa. Dopo che Symantec Data Loss Prevention esegue la scansione completa, questa casella di controllo viene automaticamente deselezionata.

Questa opzione non è disponibile per i target di un file system (condivisione di file). Per quei target, utilizzare la scansione incrementale.

Vedere ["Informazioni sulle scansioni incremental"](#) a pagina 1869.

Vedere ["Informazioni sulla differenza tra scansioni incremental e scansioni differenziali"](#) a pagina 1868.

5 Selezionare **Esegui scansione solo di file aggiunti o modificati** per includere i file in base alla data dell'aggiunta o della modifica.

Symantec Data Loss Prevention esegue la scansione degli elementi soltanto dopo la data specificata in **Dopo**, prima della data specificata in **Prima** o tra le date specificate.

Tenere presente che se la data in **Dopo** è successiva alla data in **Prima**, nessun elemento viene sottoposto a scansione. Se la data in **Prima** e la data in **Dopo** sono uguali, nessun elemento viene sottoposto a scansione. Questo perché l'ora del parametro **Prima** è zero e quella di **Dopo** è 24.

Quando si seleziona questa opzione, è possibile selezionare anche le opzioni seguenti:

- **Dopo**
 Per includere gli elementi creati o modificati (a seconda di quali sono più recenti) dopo una data particolare, digitare la data. È anche possibile fare clic sul widget data e selezionare una data.
- **Prima**

Per includere gli elementi creati o modificati (a seconda di quali sono più recenti) prima di una data particolare, digitare la data. È anche possibile fare clic sul widget data e selezionare una data.

- 6 Selezionare **Esegui scansione solo di ultimi file utilizzati** per includere i file in base alla data dell'ultimo accesso.

Symantec Data Loss Prevention esegue la scansione degli elementi soltanto dopo la data specificata in **Dopo**, prima della data specificata in **Prima** o tra le date specificate.

La funzionalità relativa all'ultimo accesso è supportata solo per la scansione di condivisioni CIFS con Network Discover per Windows.

Tenere presente che se la data in **Dopo** è successiva alla data in **Prima**, nessun elemento viene sottoposto a scansione. Se la data in **Prima** e la data in **Dopo** sono uguali, nessun elemento viene sottoposto a scansione. Questo perché l'ora del parametro **Prima** è zero e quella di **Dopo** è 24.

Quando si seleziona questa opzione, è possibile selezionare anche le opzioni seguenti:

- **Dopo**

Per includere gli elementi a cui si ha accesso dopo una data particolare, digitare la data. È anche possibile fare clic sul widget data e selezionare una data.

- **Prima**

Per includere gli elementi a cui si ha accesso prima di una data particolare, digitare la data. È anche possibile fare clic sul widget data e selezionare una data.

Nota: Il processo di montaggio predefinito utilizza il client CIFS. Se il montaggio predefinito non funziona, l'attività di montaggio può utilizzare il client JCIFS impostando `filesystemcrawler.use.jcifs=true` nel file delle proprietà `Crawler.properties`.

- 7 Fare clic su **Salva** per salvare tutti gli aggiornamenti al target.

Ottimizzazione delle risorse con le opzioni di limitazione delle scansioni di Network Discover/Cloud Storage Discover

È possibile impostare opzioni di limitazione nella scheda **Avanzate** del target per i seguenti target:

- Archiviazione cloud Box
- Condivisioni di file

- File endpoint
- Documenti di Lotus Notes
- Database SQL

Per i rilevatori, la limitazione deve essere impostata modificando il file di configurazione sul computer rilevatore.

Nota: L'utilizzo della limitazione riduce la velocità di scansione originale di almeno la metà.

È anche possibile impostare altre opzioni per ottimizzare le scansioni.

Vedere ["Informazioni sull'ottimizzazione delle scansioni di Network Discover/Cloud Storage Discover"](#) a pagina 1865.

Per impostare la limitazione per l'archiviazione cloud Box, documenti di Lotus Notes o database SQL

- 1 Nella console di amministrazione di Enforce Server, selezionare **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul nome del target da sottoporre a scansione per aprire il target e modificarlo.
- 3 Nella scheda **Avanzate**, impostare le opzioni di limitazione.
- 4 Immettere il numero massimo di file o righe oppure di byte da elaborare al minuto per ciascun server di rilevamento.

Se si selezionano entrambe le opzioni, la velocità di scansione è inferiore rispetto a entrambe le opzioni.

Numero massimo di file analizzati al minuto per server di rilevamento	Specificare il numero massimo di file, documenti (in Lotus Notes) o righe (in database SQL) da elaborare al minuto per ciascun server.
Dimensione massima analizzata al minuto per server di rilevamento	Specificare il numero massimo di byte da elaborare al minuto per ciascun server. Specificare l'unità di misura dall'elenco a discesa. Le opzioni sono byte, KB (kilobyte) o MB (megabyte).

Per impostare la limitazione per i rilevatori

- 1 Individuare il file di configurazione del rilevatore (*scanner-type.cfg*) sul computer in cui il rilevatore è stato installato.
- 2 Nel file di configurazione del rilevatore, modificare il parametro *ImportPoliteness* e il parametro *BatchSize*.

Quando si imposta la limitazione, il rilevatore recupera il numero di elementi indicato in *BatchSize* nell'archiviazione locale e quindi attende per il numero di millisecondi indicato in *ImportPoliteness* tra l'elaborazione di ogni elemento recuperato.

La limitazione di byte non è supportata per i rilevatori.

- 3 Per realizzare la limitazione di elementi dall'archivio, impostare un valore basso per il parametro *BatchSize*. Il valore *ImportPoliteness* ha quindi maggiore effetto. L'impostazione *BatchSize=1* consente di ottenere la limitazione massima nel recupero di documenti.

Ad esempio, se si imposta *BatchSize=25* e *ImportPoliteness=5000* (5 secondi), il rilevatore scarica i 25 documenti e quindi fa una pausa di 5 secondi tra l'elaborazione di ogni documento.

Creazione di un inventario delle posizioni di dati riservati non protetti

Per verificare se esistono dati confidenziali in un target, senza sottoporli tutti a scansione, utilizzare la modalità inventario per la scansione. La modalità inventario è utile quando l'esistenza di incidenti è più importante del numero di incidenti in ogni posizione.

L'esecuzione di una scansione in modalità inventario può anche migliorare le prestazioni quando si esegue la scansione di un gran numero di computer o di grandi quantità di dati. L'impostazione di soglie di incidenti può migliorare le prestazioni della scansione poiché, quando viene raggiunta una soglia, viene eseguita la scansione della radice di contenuti successiva anziché di tutti gli elementi. Una radice di contenuti è una condivisione di file, un server Domino o un database SQL specificato nella scheda **Contenuto sottoposto a scansione**.

È possibile impostare un numero massimo di incidenti per ogni elemento da sottoporre a scansione. L'elemento può essere una condivisione di file o un computer fisico.

Quando la soglia di incidenti viene raggiunta, la scansione della radice di contenuti corrente viene interrotta e inizia quella dalla radice di contenuti successiva. Poiché il processo è asincrono, è possibile che venga creato qualche incidente in più di quelli specificati dalla soglia.

La scansione in modalità inventario è supportata per i seguenti target di scansione basati su server e cloud:

- Archiviazione cloud

Per i target di archiviazione cloud Box, è possibile specificare la soglia di incidenti per ciascun utente.

- Condivisioni di file

Per le condivisioni di file, è anche possibile specificare se conteggiare gli incidenti per radice di contenuti o per computer. La radice di contenuti è una condivisione di file nell'elenco della scheda **Contenuto sottoposto a scansione**. La selezione è specificata nel campo *Conteggia incidenti per*.

- Database Lotus Notes

La soglia di incidenti viene conteggiata per radice di contenuti (server Domino nell'elenco della scheda **Contenuto sottoposto a scansione**).

- Database SQL

La soglia di incidenti viene conteggiata per radice di contenuti (database SQL nell'elenco della scheda **Contenuto sottoposto a scansione**).

La modalità inventario può essere impostata con il parametro della soglia di incidenti. È possibile impostarla quando si aggiunge un nuovo target o quando si modifica un target esistente.

Dopo aver individuato i dati riservati, è possibile impostare altre opzioni per eseguire le scansioni complete di quelle posizioni.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Per creare un inventario di dati riservati

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul nome del target da sottoporre a scansione per aprire il target e modificarlo.
- 3 Nella scheda **Avanzate**, è possibile ottimizzare la scansione con la modalità inventario.
- 4 Impostare la **soglia di incidenti**.

Immettere il numero di incidenti da generare prima di passare all'utente o alla radice di contenuto successiva (specificata nella scheda **Contenuto sottoposto a scansione**).

- 5 Impostare l'opzione **Conteggia incidenti per**.

Per le condivisioni di file è anche possibile scegliere i seguenti metodi per conteggiare gli incidenti:

- **Radice di contenuti** (impostazione predefinita)

La radice di contenuti è una condivisione di file nell'elenco della scheda **Contenuto sottoposto a scansione**.

Quando viene raggiunta la soglia di incidenti, la scansione passa alla condivisione di file successiva.

- **Computer**

Selezionare questa opzione per eseguire il conteggio per computer (le condivisioni specificate di un computer).

Quando viene raggiunta la soglia di incidenti, la scansione passa alla radice di contenuti successiva nell'elenco di elementi da sottoporre a scansione. Se quella radice di contenuti si trova sullo stesso computer fisico dell'elemento precedente, viene ignorata.

Tenere presente che il nome di computer deve essere letteralmente lo stesso affinché la radice di contenuti sia ignorata. Ad esempio, `\\localhost\myfiles` e

`\\127.0.0.1\myfiles` vengono considerati computer diversi, anche se sono logicamente uguali.

Gestione delle scansioni target di Network Discover

Il capitolo contiene i seguenti argomenti:

- Gestione delle scansioni target di Network Discover/Cloud Storage Discover
- Gestione di target Network Discover/Cloud Storage Discover
- Gestione delle cronologie di scansione di Network Discover/Cloud Storage Discover
- Gestione di server Network Discover/Cloud Storage Discover
- Informazioni sull'ottimizzazione delle scansioni di Network Discover/Cloud Storage Discover
- Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali
- Informazioni sulle scansioni incrementali
- Scansione di elementi nuovi o modificati con scansioni incrementali
- Informazioni sulla gestione delle scansioni incrementali
- Scansione di elementi nuovi o modificati con scansioni differenziali
- Configurazione delle scansioni parallele di target di Network Discover/Cloud Storage Discover
- Informazioni sulla scansione della griglia
- Configurazione della scansione della griglia
- Rinnovo dei certificati di comunicazione griglia per i server di rilevamento Discover
- Migrazione di una scansione di rilevamento da un server singolo a una griglia
- Linee guida per le prestazioni della scansione della griglia

- [Risoluzione dei problemi delle scansioni di griglia](#)

Gestione delle scansioni target di Network Discover/Cloud Storage Discover

Le attività di gestione delle scansioni target di Network Discover/Cloud Storage Discover rientrano in quattro categorie generiche: gestione di target Network Discover/Cloud Storage Discover, gestione delle cronologie di scansione di Network Discover/Cloud Storage Discover, gestione dei server Network Discover/Cloud Storage Discover e ottimizzazione delle scansioni.

Vedere ["Gestione di target Network Discover/Cloud Storage Discover"](#) a pagina 1853.

Vedere ["Gestione delle cronologie di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1856.

Vedere ["Gestione di server Network Discover/Cloud Storage Discover"](#) a pagina 1864.

Vedere ["Informazioni sull'ottimizzazione delle scansioni di Network Discover/Cloud Storage Discover"](#) a pagina 1865.

Gestione di target Network Discover/Cloud Storage Discover

Per gestire i target di Scansione Discover è possibile:

- Avviare, interrompere e sospendere le scansioni sui target.
- Monitorare lo stato durante l'esecuzione di una scansione target.
- Selezionare target per visualizzarne i dettagli.
- Modificare o eliminare i target.
- Gestire più target.
- Ordinare e filtrare target per semplificare la gestione.
- Specificare il numero dei target da visualizzare.

Vedere ["Informazioni sull'elenco dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1854.

Vedere ["Utilizzo dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1855.

Vedere ["Rimozione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1856.

Informazioni sull'elenco dei target di scansione di Network Discover/Cloud Storage Discover

È possibile gestire i target di scansione di Network Discover/Cloud Storage Discover nella schermata **Target di Discover**. La barra degli strumenti sopra l'elenco di target include un menu a discesa per la creazione di nuovi target di scansione, pulsanti per l'avvio, l'arresto e la messa in pausa delle scansioni e un'icona per filtrare gli elementi dell'elenco. È possibile applicare le azioni a più target.

È possibile fare clic sulla maggior parte delle intestazioni della colonna per ordinare l'elenco in base ai dati nella colonna.

È possibile selezionare il numero di voci da visualizzare nell'elenco **Target di Discover** utilizzando il menu a discesa sopra la colonna **Azioni**.

Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.

La [Tabella 62-1](#) elenca le colonne per ogni scansione di target.

Tabella 62-1 Target di Discover

Informazioni target	Descrizione
Nome target	Nome della scansione del target.
Tipo di target	Tipo di target per la scansione (ad esempio File system o SharePoint).
Gruppi di politiche	Elenca i gruppi di politiche a cui è assegnato il target.
Server	<p>Elenca i server assegnati a questo target.</p> <p>Nota: Se una scansione di griglia è configurata per un particolare target di scansione, all'elenco dei server viene aggiunto il prefisso "Grid". Attualmente la scansione di griglia è disponibile solo per target di scansione di SharePoint e File System (condivisione file).</p> <p>Vedere "Informazioni sulla scansione della griglia" a pagina 1874.</p>
Ultima modifica	Specifica la data e l'ora dell'ultima modifica del target.
Stato scansione	Visualizza lo stato della scansione. Fare clic sul collegamento in questa colonna per visualizzare una pagina della cronologia delle scansioni filtrata per questo target.
Scansione successiva	Visualizza la scansione pianificata successiva per il target, se applicabile.

Informazioni target	Descrizione
Azioni	<p>Fare clic sull'icona Modifica target per modificare la definizione del target.</p> <p>Fare clic sull'icona Elimina per eliminare l'obiettivo.</p>

Per filtrare l'elenco Target di Discover

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su **Filtro**. In ogni intestazione di colonna nell'elenco **Target di Discover** viene visualizzato un campo di testo o un elenco a discesa.
- 3 Applicare uno di questi filtri all'elenco:
 - **Nome target** : digitare il nome del target nel campo di testo.
 - **Tipo di target** : selezionare il tipo di target dall'elenco a discesa.
 - **Gruppi di politiche** : immettere il nome del gruppo di politiche nel campo di testo.
 - **Server** : immettere il nome del server nel campo di testo.
 - **Ultima modifica** : selezionare un intervallo dall'elenco a discesa.
 - **Stato scansione** : selezionare uno stato di scansione dall'elenco a discesa.
 - **Scansione successiva** : selezionare un intervallo dall'elenco a discesa.
- 4 Per annullare un filtro, cancellare il valore dal campo di testo o dall'elenco a discesa relativo, o fare clic su **Filtro**.

Utilizzo dei target di scansione di Network Discover/Cloud Storage Discover

È possibile eseguire le seguenti attività con i target di scansione:

Per avviare, arrestare e sospendere le scansioni di Network Discover/Cloud Storage Discover

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Selezionare i target di scansione che si desidera avviare, arrestare o sospendere.
- 3 Fare clic su **Avvia scansione**, **Arresta scansione** o **Sospendi scansione** nella barra degli strumenti dell'elenco di target.

Per modificare un target di scansione di Network Discover/Cloud Storage Discover

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul pulsante **Modifica target** per il target che si desidera modificare.
- 3 Apportare le modifiche desiderate nella pagina **Modifica target**.

Vedere "[Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover](#)" a pagina 1830.

Rimozione dei target di scansione di Network Discover/Cloud Storage Discover

Verificare le scansioni in esecuzione o in coda prima di rimuovere la destinazione di una scansione.

Vedere "[Gestione delle scansioni target di Network Discover/Cloud Storage Discover](#)" a pagina 1853.

Per rimuovere i target di scansione, eseguite queste operazioni:

- Rimuovere il target di scansione dall'Enforce Server.
- Disinstallare lo scanner dal computer in cui è installato, se applicabile.

Per rimuovere un target di scansione

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su **Elimina** per il target che si desidera rimuovere.

Gestione delle cronologie di scansione di Network Discover/Cloud Storage Discover

Per gestire le cronologie di scansione di Network Discover/Cloud Storage Discover è possibile:

- Visualizzare statistiche sulle scansioni in esecuzione o completate.
- Scaricare informazioni sulla cronologia scansioni in formato valori separati da virgola (CSV).
- Visualizzare i dettagli scansione.
- Visualizzare report degli incidenti.
- Eliminare cronologie di ricerca.
- Gestire più cronologie di ricerca.
- Ordinare e filtrare cronologie di ricerca per semplificare la gestione.

- Specificare il numero di cronologie di ricerca da visualizzare.

Vedere ["Informazioni sulle cronologie di scansione Discover e Endpoint Discover"](#) a pagina 1857.

Vedere ["Gestione delle cronologie scansioni di Network Discover/Cloud Storage Discover"](#) a pagina 1859.

Vedere ["Eliminazione delle scansioni di Network Discover/Cloud Storage Discover"](#) a pagina 1859.

Vedere ["Informazioni sui dettagli di scansione di rilevamento"](#) a pagina 1860.

Vedere ["Uso dei dettagli scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1864.

Informazioni sulle cronologie di scansione Discover e Endpoint Discover

È possibile gestire le cronologie scansioni di Discover e Endpoint Discover nella schermata **Cronologia scansioni**. Per visualizzare un elenco di cronologie scansioni per tutti i target di Discover, nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Cronologia scansioni**.

Fare clic su qualsiasi intestazione di colonna per ordinare l'elenco alfanumericamente in base ai dati di tale colonna.

È possibile selezionare il numero di voci da visualizzare nell'elenco **Target di Discover** utilizzando il menu a discesa sopra la colonna **Azioni**.

Per maggiori informazioni su una scansione, fare clic sul collegamento nella colonna **Stato scansione** per visualizzare la schermata **Dettagli scansione**.

Vedere ["Informazioni sui dettagli di scansione di rilevamento"](#) a pagina 1860.

Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.

[Tabella 62-2](#) elenca i campi visualizzati per ogni scansione.

Tabella 62-2 Cronologia scansioni

Cronologia scansioni	Descrizione
Nome target	Nome della scansione del target.
Tipo di target	Tipo di target per la scansione (ad esempio File system o SharePoint).
Scansione avviata	Data e ora di inizio della scansione.
Stato scansione	Stato attuale della scansione: In esecuzione, Sospesa, Completata, Arrestata.

Cronologia scansioni	Descrizione
Numero di server nella griglia	<p>Numero di server di rilevamento selezionati per eseguire una scansione della griglia.</p> <p>Nota: Attualmente la scansione di griglia è disponibile solo per target di scansione di SharePoint e File System (condivisione file). Per le scansioni non eseguite nella griglia viene visualizzato il valore N/D in questa colonna.</p> <p>Vedere "Informazioni sulla scansione della griglia" a pagina 1874.</p>
Tipo di scansione	Tipo di scansione: Incrementale, Differenziale o Completa.
Incidenti generati	Numero di incidenti generati dalla scansione.
Tempo di esecuzione	Durata della scansione nel formato gg:hh:mm:ss.
Byte/Elementi sottoposti a scansione	Numero di byte ed elementi sottoposti a scansione nel target.
Errori	Numero di errori durante la scansione.
Azioni	<p>Fare clic sull'icona Visualizza incidenti per visualizzare un report di riepilogo degli incidenti per la scansione.</p> <p>Vedere "Informazioni sui report incidente per Network Discover/Cloud Storage Discover" a pagina 1610.</p> <p>Vedere "Report incidente di Discover" a pagina 1610.</p> <p>Fare clic sull'icona Elimina per eliminare la scansione. Assicurarsi di eliminare le scansioni differenziali prima di eliminare la scansione di base.</p> <p>Vedere "Eliminazione delle scansioni di Network Discover/Cloud Storage Discover" a pagina 1859.</p>

Per filtrare l'elenco Cronologia scansioni

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Cronologia scansioni**.
- 2 Fare clic su **Filtro**. Un campo di testo o un elenco a discesa appare nell'intestazione della colonna nell'elenco **Cronologia scansioni**.
- 3 Applicare uno di questi filtri all'elenco:
 - **Nome target** : digitare il nome del target nel campo di testo.
 - **Tipo di target** : selezionare il tipo di target dall'elenco a discesa.

- **Scansione avviata** : selezionare un intervallo dall'elenco a discesa.
 - **Stato scansione** : selezionare uno stato di scansione dall'elenco a discesa.
 - **Tipo di scansione** : selezionare un tipo di scansione dall'elenco a discesa.
- 4 Per annullare un filtro, cancellare il valore dal campo di testo o dall'elenco a discesa relativo, o fare clic su **Filtro**.

Vedere ["Gestione delle scansioni target Endpoint Discover"](#) a pagina 2105.

Gestione delle cronologie scansioni di Network Discover/Cloud Storage Discover

È possibile eseguire le seguenti attività con le cronologie scansioni:

Per esportare cronologie scansioni Network Discover/Cloud Storage Discover

- 1 Nella console di amministrazione di Enforce Server accedere a **Gestisci > Scansione Discover > Cronologia scansioni**.
- 2 Selezionare la o le scansioni che si desidera esportare.
- 3 Fare clic su **Esporta**. Viene visualizzata la finestra di dialogo di scaricamento del file.
- 4 Fare clic su **Apri** per visualizzare i dati esportati o su **Salva** per salvare il file.
- 5 Per annullare l'operazione di esportazione, fare clic su **Annulla**.

Per visualizzare gli incidenti per una scansione specifica

- 1 Nella console di amministrazione di Enforce Server accedere a **Gestisci > Scansione Discover > Cronologia scansioni**.
- 2 Fare clic sull'icona **Visualizza incidenti** per la scansione che si desidera visualizzare. Viene visualizzata la schermata **Incidenti di rilevazione**.

Eliminazione delle scansioni di Network Discover/Cloud Storage Discover

È possibile eliminare scansioni specifiche dalla cronologia delle scansioni.

Per eliminare una scansione

- 1 Nella console di amministrazione di Enforce Server selezionare **Gestisci > Scansione Discover > Cronologia scansioni**.
- 2 Eliminare eventuali scansioni differenziali prima di eliminare la scansione completa di base per il target.
 Questo passaggio non è necessario per le scansioni incrementali.
- 3 Selezionare la scansione da eliminare, quindi fare clic sull'icona di eliminazione nella colonna **Azioni**.

Per eliminare più scansioni, selezionare le caselle di controllo relative alle scansioni che si desidera eliminare, quindi fare clic su **Elimina** sulla barra degli strumenti.

Informazioni sui dettagli di scansione di rilevamento

È possibile visualizzare informazioni dettagliate di ogni scansione di rilevamento, incluse informazioni generali, statistiche, errori recenti e attività. È anche possibile scaricare report in formato CSV per le statistiche, gli errori recenti e l'attività, ove disponibile.

Per visualizzare informazioni dettagliate su una scansione, selezionare **Gestisci > Scansione Discover > Cronologia scansioni**. Selezionare la scansione, quindi fare clic sul collegamento nella colonna **Stato**.

Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.

Vedere ["Gestione delle scansioni target Endpoint Discover"](#) a pagina 2105.

Nota: Le informazioni visualizzate nella schermata **Dettagli scansione** sono specifiche per il tipo di scansione completato. Le seguenti tabelle elencano tutti i possibili campi visualizzati.

Tabella 62-3 mostra la sezione **Generale**, in cui sono visualizzate informazioni su una scansione.

Tabella 62-3 Informazioni generali su una scansione

Informazioni generali su una scansione	Descrizione
Tipo di target	Il tipo e l'icona del target che è stato sottoposto a scansione.
Nome target	Il nome del target.

Informazioni generali su una scansione	Descrizione
Stato	Lo stato della scansione. Se la scansione è in esecuzione, viene visualizzato il nome del server Network Discover/Cloud Storage Discover in cui viene eseguita.
Tipo di scansione	Il tipo di scansione, come incrementale o completa.
Ora di inizio	La data e l'ora di inizio della scansione.
Ora di fine	La data e l'ora in cui la scansione è stata completata.

Tabella 62-4 mostra la sezione **Statistiche scansione**, che fornisce informazioni dettagliate su una scansione.

Tabella 62-4 Statistiche scansione

Statistiche scansione	Descrizione
Elaborato	Il numero di radici di contenuti (utenti, condivisioni o siti) sottoposte a scansione. Se la scansione è ancora in corso, questo campo fornisce un'idea dell'avanzamento della scansione.
Tempo di esecuzione (Giorni:Ore:Minuti:Secondi)	La durata della scansione. Se la scansione è ancora in corso, il contatore continua ad avanzare. Il totale non include i periodi di tempo durante i quali la scansione è stata sospesa.
Elementi sottoposti a scansione	Il numero di elementi sottoposti a scansione.
Byte sottoposti a scansione	Il numero di byte sottoposti a scansione.
Elementi filtrati	Numero di elementi filtrati.
Byte filtrati	Numero di byte filtrati.
Errori	Il numero di errori durante la scansione. Un elenco degli errori è disponibile nella sezione Errori di scansione recenti .
Elemento non elaborabile	Numero di elementi che non sono stati elaborati durante la scansione.
Numero corrente di incidenti	Il numero di incidenti rilevati durante la scansione corrente, meno gli incidenti eventualmente eliminati. È possibile fare clic su questo numero per visualizzare un elenco di incidenti per questa scansione.

La sezione **Stato griglia recente** è un elenco dei server che sono stati assegnati al target di scansione per eseguire una scansione della griglia. Attualmente la scansione della griglia è disponibile solo per target di scansione di SharePoint e File System (condivisione file).

Per impostazione predefinita, la sezione di **Stato griglia recente** è compressa quando si apre la schermata **Dettagli scansione**.

Tabella 62-5 Stato griglia recente

Dettagli stato griglia recente	Descrizione
Elemento principale griglia	Il nome del server di rilevamento a cui è stato assegnato il ruolo Elemento principale griglia durante la scansione. È possibile fare clic sul nome di ciascun server per accedere alla schermata Dettagli server/rilevatore di quel server.
Server di rilevamento partecipanti	I nomi dei server di rilevamento nella griglia che hanno eseguito la scansione. È possibile fare clic sul nome di ciascun server per accedere alla schermata Dettagli server/rilevatore di quel server.
Server di rilevamento non partecipanti	I nomi dei server di rilevamento nella griglia che non sono stati in grado di eseguire la scansione. Viene visualizzato un messaggio di errore accanto a ogni nome del server per descrivere il motivo dell'impossibilità a partecipare alla scansione. È possibile fare clic sul nome di ciascun server per accedere alla schermata Dettagli server/rilevatore di quel server.

La sezione **Errori di scansione recenti** elenca gli errori verificatisi durante la scansione.

Se una scansione ha molti errori, non potranno essere visualizzati tutti nella schermata **Dettagli scansione**. Per visualizzare un elenco completo degli errori verificatisi durante la scansione, fare clic su **Scarica report errori completo**.

[Tabella 62-6](#) mostra informazioni su ogni errore visualizzate nel report Errori di scansione recenti.

Tabella 62-6 Errori di scansione recenti

Dettagli su errori di scansione recenti	Descrizione
Data	La data e l'ora dell'errore durante la scansione.
Percorso	Il percorso di directory alla posizione del file con l'errore durante la scansione.

Dettagli su errori di scansione recenti	Descrizione
Errore	Il messaggio di errore.

Attività di scansione recente visualizza le voci di registro più recenti degli eventi importanti verificatisi durante la scansione.

Se una scansione ha molti messaggi, non saranno visualizzati tutti nella schermata **Dettagli scansione**. Per visualizzare un elenco completo dei messaggi della scansione, fare clic su **Scarica report attività completo**.

[Tabella 62-7](#) mostra il report Attività di scansione recente, che fornisce informazioni su ogni attività.

Tabella 62-7 Attività di scansione recente

Dettagli sull'attività di scansione recente	Descrizione
Data/ora	La data e l'ora in cui si è verificato l'evento registrato.
Livello	La gravità dell'evento.
Messaggio	Il messaggio registrato relativo all'evento.

[Tabella 62-8](#) spiega le opzioni della schermata **Dettagli scansione**.

Tabella 62-8 Opzioni della schermata Dettagli scansione

Opzioni di Dettagli scansione	Descrizione
Scarica report statistico completo	Scarica un report con tutte le statistiche sulla scansione in formato CSV.
Scarica report errori completo	Scarica un report con tutti gli errori di scansione in formato CSV.
Scarica report attività completo	Scarica un report con tutte le attività della scansione in formato CSV.

Uso dei dettagli scansione di Network Discover/Cloud Storage Discover

È possibile eseguire le seguenti attività con i dettagli scansione:

Per visualizzare i dettagli scansione

- 1 Nella console di amministrazione di Enforce Server, fare clic su **Gestisci > Scansione Discover > Cronologia scansioni**.
- 2 Nella pagina **Cronologia scansioni** fare clic sul collegamento nella colonna **Stato scansione** corrispondente alla scansione di cui si desidera visualizzare i dettagli.

Per esportare i dettagli scansione in un file CSV

- 1 Nella console di amministrazione di Enforce Server accedere a **Gestisci > Scansione Discover > Cronologia scansioni**.
- 2 Nella pagina **Cronologia scansioni** fare clic sul collegamento nella colonna **Stato scansione** corrispondente alla scansione di cui si desidera visualizzare i dettagli.
- 3 Nella pagina **Dettagli scansione** fare clic su uno delle seguenti pulsanti:
 - Scarica report statistico completo
 - Scarica report errori completo
 - Scarica report attività completo

Gestione di server Network Discover/Cloud Storage Discover

È possibile visualizzare lo stato e i dettagli delle scansioni Network Discover/Cloud Storage Discover per ciascun server Discover.

Vedere ["Visualizzazione dello stato dei server Network Discover/Cloud Storage Discover"](#) a pagina 1864.

Visualizzazione dello stato dei server Network Discover/Cloud Storage Discover

La schermata **Discover Server** elenca i server di rilevamento per Network Discover/Cloud Storage Discover o Endpoint Discover configurati sulla rete. Questa schermata mostra i dettagli sulle scansioni in ogni server di rilevamento.

Per visualizzare i Discover Server nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Discover Server**.

Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.

[Tabella 62-9](#) elenca le informazioni per ogni server.

Tabella 62-9 Discover Server

Informazioni sul server	Descrizione
Nome server	Il nome del server. Tra parentesi è indicato il tipo di server di rilevamento, Discover o Endpoint.
Scansioni in esecuzione	Un elenco delle scansioni attualmente in esecuzione su questo server.
Scansioni in coda	Un elenco delle scansioni in coda per l'esecuzione su questo server.
Scansioni pianificate	Un elenco delle scansioni di cui è stata pianificata l'esecuzione su questo server.
Scansioni sospese	Un elenco delle scansioni sospese su questo server.

Per visualizzare i dettagli delle scansioni da un server Network Discover/Cloud Storage Discover

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Discover Server**.
- 2 Nella pagina **Discover Server**, fare clic sul nome della scansione per cui si desidera visualizzare i dettagli.

Vedere ["Informazioni sui dettagli di scansione di rilevamento"](#) a pagina 1860.

Informazioni sull'ottimizzazione delle scansioni di Network Discover/Cloud Storage Discover

Le scansioni di target di Network Discover/Cloud Storage Discover possono durare varie ore o giorni, a seconda del tipo di scansione e della quantità e del formato dei dati da sottoporre a scansione, come pure la velocità della rete e dell'hardware. Per ottimizzare le scansioni di grandi quantità di informazioni, seguire i suggerimenti in questa sezione.

Per ottimizzare le scansioni di Network Discover/Cloud Storage Discover, considerare l'uso di alcuni dei seguenti metodi:

- Iniziare sottoponendo a scansione solo gli archivi o le condivisioni di file più accessibili e disponibili (ad esempio, accesso guest o pubblico). Iniziare con una piccola quantità di informazioni e confermare l'accuratezza delle scansioni prima di aumentare il volume delle informazioni da sottoporre a scansione. Dopo aver raggiunto prestazioni soddisfacenti con

le scansioni iniziali, eseguire anche la scansione delle unità aziendali che gestiscono i dati riservati.

- Installare più server Network Discover/Cloud Storage Discover sulla rete.
- Per le scansioni File System (condivisione file) e SharePoint, utilizzare la scansione di griglia per assegnare due o più server Network Discover/Cloud Storage Discover per eseguire la scansione di archivi di dati molto grandi.
 Vedere ["Informazioni sulla scansione della griglia"](#) a pagina 1874.
 Vedere ["Configurazione della scansione della griglia"](#) a pagina 1876.
- Suddividere le scansioni di grandi dimensioni in più scansioni di dimensioni minori. Creare target di scansione separati e utilizzare i filtri per suddividere il set da sottoporre a scansione. È possibile suddividere le scansioni con i filtri di inclusione, esclusione, dimensione e data.
 Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.
 Vedere ["Filtraggio dei target di Discover per dimensione dell'oggetto"](#) a pagina 1843.
 Vedere ["Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica"](#) a pagina 1844.
- Eseguire dapprima la scansione di file non binari. È poco probabile che i file binari contengano violazioni di politiche.
 Ad esempio, è possibile applicare il filtro di esclusione all'elenco seguente per eseguire la scansione di file non binari:

```
*.exe, *.lib, *.bin, *.dll, *.cab, *.dat
```

```
*.au, *.avi, *.mid, *.mov, *.mp, *.mp3, *.mp4, *.mpeg, *.wav, *.wma
```

Per sottoporre a scansione il resto dei file, utilizzare questo filtro come filtro di inclusione di un altro target di scansione.

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

- Per i target di archiviazione cloud, è possibile configurare una scansione incrementale con una finestra di scansione limitata (sette giorni massimo) e una scansione completa una tantum per l'intero set di dati. La scansione incrementale troverà rapidamente i dati riservati recenti a rischio, mentre la scansione completa funziona analizza la massa dei dati. Poiché i repository cloud possono contenere i terabyte o petabyte di dati, è possibile che l'esecuzione della scansione completa richieda diversi giorni.
 Vedere ["Scansione di elementi nuovi o modificati con scansioni incrementali"](#) a pagina 1870.
 Vedere ["Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali"](#) a pagina 1868.
- Per i target di file system e SharePoint, è possibile configurare scansioni incrementali per verificare soltanto i file che non sono ancora stati sottoposti a scansione.
 Vedere ["Scansione di elementi nuovi o modificati con scansioni incrementali"](#) a pagina 1870.

Vedere ["Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali"](#) a pagina 1868.

- Eseguire la scansione di elementi nuovi o modificati di recente in un obiettivo di scansione e la scansione di quelli meno recenti in un secondo obiettivo di scansione. Utilizzare il filtro di data per suddividere le scansioni per valori di dati, file più vecchi o file più nuovi.

Vedere ["Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica"](#) a pagina 1844.

- Dopo la scansione iniziale, eseguire scansioni differenziali per verificare solo gli elementi aggiunti o modificati dopo l'ultima scansione completata.

Vedere ["Scansione di elementi nuovi o modificati con scansioni differenziali"](#) a pagina 1872.

Vedere ["Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali"](#) a pagina 1868.

- Eseguire la scansione di file di piccole dimensioni in un target di scansione e quella di file di grandi dimensioni in un altro target. La scansione di molti file di piccole dimensioni comporta un maggior sovraccarico di quella di pochi file di grandi dimensioni. Utilizzare il filtro di dimensione per suddividere le scansioni per dimensione.

Vedere ["Filtraggio dei target di Discover per dimensione dell'oggetto"](#) a pagina 1843.

- Eseguire la scansione di file compressi in un target di scansione distinto. Utilizzare il filtro di inclusione per eseguire la scansione di file compressi. Ad esempio, utilizzare l'elenco seguente:

```
*.zip,*.gzip
```

Per sottoporre a scansione il resto dei file, utilizzare questo filtro come filtro di esclusione di un altro target di scansione.

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

- Eseguire la scansione di file di database o di fogli di calcolo in un target di scansione distinto.

Utilizzare il target Database SQL per eseguire la scansione di file di database.

Vedere ["Configurazione ed esecuzione di scansioni database SQL"](#) a pagina 1940.

Utilizzare il filtro di inclusione per eseguire la scansione di fogli di calcolo.

```
*.xls
```

Configurare un target di scansione distinto e utilizzare il filtro di esclusione per eseguire la scansione di tutti gli altri elementi.

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

- Escludere le cartelle nelle applicazioni. Ad esempio, nella scansione di una condivisione DFS, escludere la cartella `DfsrPrivate` interna. Nella scansione di una condivisione su un file NetApp, escludere la cartella `.snapshot`.
 Vedere ["Esclusione delle cartelle DFS interne"](#) a pagina 1920.
 Vedere ["Configurazione delle scansioni del file system"](#) a pagina 1922.
- Utilizzare la scansione Modalità inventario per spostarsi all'elemento successivo se viene raggiunta una soglia di incidenti. La scansione Modalità inventario consente di determinare dove si trovano i dati riservati, senza eseguirne la scansione completa.
 Vedere ["Creazione di un inventario delle posizioni di dati riservati non protetti"](#) a pagina 1849.
- Utilizzare tutto l'hardware disponibile per le scansioni. Ad esempio, sospendere o chiudere qualsiasi altro programma eseguito sul server.
- Utilizzare Sospensione in corso per sospendere automaticamente la scansione durante l'orario di lavoro.
- Eseguire le scansioni in parallelo.
 Vedere ["Configurazione delle scansioni parallele di target di Network Discover/Cloud Storage Discover"](#) a pagina 1873.
- Utilizzare la limitazione per ridurre il carico di rete.
 Vedere ["Ottimizzazione delle risorse con le opzioni di limitazione delle scansioni di Network Discover/Cloud Storage Discover"](#) a pagina 1847.
- Aggiornare l'hardware del server.
 È possibile usare fino a 12 GB di memoria, CPU quad, unità disco rigido ultra veloci e schede di rete per risolvere colli di bottiglia nell'hardware.

Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali

Le scansioni incrementali e differenziali consentono di ottimizzare le prestazioni di scansione esaminando solo elementi nuovi o modificati. Le scansioni incrementali vengono riprese dal punto in cui sono terminate, anche se la prima scansione non era una scansione completa. Le scansioni differenziali eseguono la scansione soltanto degli elementi aggiunti o modificati dopo l'ultima scansione completa: è necessario eseguire almeno una scansione completa del target di scansione prima di poter usare la scansione differenziale.

Vedere ["Informazioni sulle scansioni incrementali"](#) a pagina 1869.

Vedere ["Scansione di elementi nuovi o modificati con scansioni incrementali"](#) a pagina 1870.

Vedere ["Scansione di elementi nuovi o modificati con scansioni differenziali"](#) a pagina 1872.

[Tabella 62-10](#) confronta le scansioni incrementali e quelle differenziali.

Tabella 62-10 Differenze tra le scansioni incrementali e quelle differenziali

Scansioni incrementali	Scansioni differenziali
<p>Le scansioni incrementali sono supportate per i target seguenti:</p> <ul style="list-style-type: none"> ■ Cloud > Box (server di rilevamento on-site) ■ Server > File system ■ Server > SharePoint 	<p>Le scansioni differenziali sono supportate per i target seguenti:</p> <ul style="list-style-type: none"> ■ Server > IBM (Lotus) Notes ■ Server > Exchange ■ Endpoint > File system
<p>Le scansioni parziali conservano le informazioni sugli elementi sottoposti a scansione.</p> <p>Se file, condivisioni o altri elementi non sono sottoposti a scansione in quanto inaccessibili, lo saranno automaticamente con la scansione incrementale successiva.</p>	<p>Le scansioni differenziali iniziano con una scansione completa del target di Discover. Questa scansione completa è denominata scansione di base.</p> <p>Le scansioni parziali non possono essere usate come scansione di base.</p>
<p>Le esecuzioni successive eseguono la scansione di tutti gli elementi non esaminati in precedenza, inclusi gli elementi nuovi o modificati.</p>	<p>Le esecuzioni successive eseguono la scansione di tutti gli elementi che sono stati aggiunti o modificati a partire dalla data dell'ultima scansione (di base) completa ultimata.</p> <p>Il sistema considera la data di inizio della scansione di base per la scansione differenziale.</p>
<p>Un indice di scansioni incrementali tiene traccia degli elementi già sottoposti a scansione.</p>	<p>La scansione di base completa più recente viene utilizzata per stabilire quali elementi devono essere sottoposti a scansione, in base alla data della scansione di base.</p>

Informazioni sulle scansioni incrementali

Le scansioni incrementali consentono di ottimizzare le prestazioni di scansione esaminando solo elementi nuovi o modificati. Le scansioni incrementali vengono riprese dal punto in cui sono terminate, anche se la prima scansione non era una scansione completa.

Vedere ["Informazioni sull'ottimizzazione delle scansioni di Network Discover/Cloud Storage Discover"](#) a pagina 1865.

La scansione incrementale è disponibile solo per alcuni tipi di target.

Vedere ["Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali"](#) a pagina 1868.

Le scansioni incrementali conservano le informazioni sugli elementi sottoposti a scansione.

Alcuni file possono essere ignorati durante una scansione, ad esempio, perché protetti o in uso. Una scansione può non essere completata a causa di dati inaccessibili, ad esempio quando un server o un dispositivo non è in linea. Questi file mancanti vengono esaminati nelle scansioni successive del target.

Un indice di scansioni incrementali tiene traccia degli elementi già sottoposti a scansione. Questo indice viene sincronizzato tra molteplici Discover Server.

A partire da Symantec Data Loss Prevention versione 15.0, quando si configura una scansione incrementale nei server del file system, è possibile selezionare uno o più target di scansione esistenti i cui indici incrementali verranno riutilizzati nella nuova scansione. Il riutilizzo degli indici incrementali consente di risparmiare tempo di indicizzazione degli elementi sottoposti a scansione nel nuovo target di scansione. Inoltre, questa funzionalità consente di consolidare e suddividere i target di scansione del server del file system, aumentando la gestibilità del target di scansione.

Per informazioni sui requisiti per la dimensione dell'indice di scansioni incrementali, vedere la *Guida alla compatibilità e ai requisiti di sistema di Symantec Data Loss Prevention*.

Scansione di elementi nuovi o modificati con scansioni incrementali

Una scansione incrementale consente di riprendere una scansione di Network Discover/Cloud Storage Discover a partire dal primo elemento non sottoposto a scansione. Una scansione incrementale esegue la scansione solo degli elementi di cui non è stata eseguita la scansione in precedenza.

Vedere ["Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali"](#) a pagina 1868.

Per configurare una scansione incrementale

- 1 Accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sull'elenco a discesa **Nuovo target** e selezionare il tipo di target **Cloud > Box (server di rilevamento on-site)**, **File system** o **SharePoint**, oppure selezionare uno dei target di scansione archiviazione cloud, file system o SharePoint nell'elenco per modificarlo.
- 3 Fare clic sulla scheda **Generale**.

- 4 In **Tipo di scansione**, selezionare **Esegui scansione solo di elementi nuovi o modificati (scansione incrementale)**. Questa opzione è il valore predefinito per i nuovi target. Per i target di archiviazione cloud, questa opzione è **Esegue la scansione solo degli elementi aggiunti o modificati nella finestra specificata (scansione incrementale)**.

In caso di modifica della politica o di altre definizioni in una scansione esistente, è possibile configurare la scansione successiva in modo che sia una scansione completa per essere certi di includere tutte le politiche. Selezionare la seguente opzione:

Se si desidera eseguire sempre la scansione di tutti gli elementi in questo target, selezionare la seguente opzione:

Esegui sempre scansione di tutti gli elementi (scansione completa). Per i target di archiviazione cloud, questa opzione è **Esegue la scansione di tutti i file aggiunti o modificati nella finestra specificata (scansione completa)**.

- 5 Eseguire le altre operazioni per configurare o modificare un target di Discovery ed eseguire la scansione.

Vedere ["Configurazione dei campi obbligatori per i target di Network Discover"](#) a pagina 1832.

Vedere ["Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1830.

Vedere ["Impostazione delle scansioni di file system"](#) a pagina 1906.

- 6 Per gestire la scansione incrementale e diagnosticare i problemi, consultare il seguente argomento:

Vedere ["Informazioni sulla gestione delle scansioni incremental"](#) a pagina 1871.

Informazioni sulla gestione delle scansioni incremental

Quando si eseguono scansioni incremental, tenere presente quanto segue:

- Se l'installazione include più Discover Server, l'indice della scansione incrementale viene sincronizzato automaticamente su tutti gli altri Discover Server per il target.
- Quando si modifica l'impostazione di scansione incrementale da **Esegui scansione solo di elementi nuovi o modificati (scansione incrementale)** a **Esegui scansione di tutti gli elementi alla scansione successiva**. Le scansioni successive saranno incremental, quindi l'indice di scansione incrementale per il target verrà azzerato prima dell'avvio della scansione. Le scansioni successive saranno incremental.

Nota: Facoltativamente, quando si seleziona l'opzione **Esegui scansione solo di elementi nuovi o modificati (scansione incrementale)**, è possibile selezionare uno o più target di scansione server del file system esistenti i cui indici incrementali verranno riutilizzati nella nuova scansione. Il riutilizzo degli indici incrementali consente di risparmiare tempo di indicizzazione degli elementi sottoposti a scansione nel nuovo target di scansione. Questa funzionalità è disponibile solo quando si crea un nuovo target di scansione o se ne modifica uno esistente prima di eseguire una scansione per la prima volta.

- Per eseguire la scansione di tutti gli elementi, impostare **Esegui sempre scansione di tutti gli elementi (scansione completa)** per il target del server di rilevamento Discover.
- Se l'impostazione **Esegui sempre scansione di tutti gli elementi (scansione completa)** è selezionata, tutte le voci di indice precedenti per il target vengono rimosse prima dell'avvio della scansione. L'indice non viene ricompilato durante la scansione.
 Per eseguire la scansione di tutti gli elementi e quindi procedere con la scansione incrementale, selezionare l'opzione **Esegui scansione di tutti gli elementi alla scansione successiva. Le scansioni successive saranno incrementali**. Questa non è un'opzione per i target dell'archiviazione cloud.
- Quando un target Discover viene eliminato, l'indice della scansione incrementale non viene rimosso automaticamente.

Scansione di elementi nuovi o modificati con scansioni differenziali

Per risparmiare risorse, le ricerche differenziali eseguono la scansione soltanto degli elementi aggiunti o modificati dopo l'ultima scansione completa.

Per informazioni sull'upgrade di un target configurato per la scansione differenziale durante l'aggiornamento di una versione, vedere il *Manuale di aggiornamento di Symantec Data Loss Prevention*.

Vedere ["Informazioni sulla differenza tra scansioni incrementali e scansioni differenziali"](#) a pagina 1868.

Per configurare una scansione differenziale

- 1 Accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sull'elenco a discesa **Nuovo target** e selezionare un tipo di target, oppure selezionare uno dei target nell'elenco per modificarlo.
- 3 Fare clic sulla scheda **Filtri**.

- 4 Selezionare l'opzione relativa alla data per una scansione differenziale.
Vedere ["Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica"](#) a pagina 1844.
- 5 Eseguire una scansione completa. La scansione iniziale deve essere una scansione completa.
- 6 Al termine della scansione iniziale, la scansione seguente esamina solo gli elementi aggiunti o modificati dopo l'ultima scansione completa.

Configurazione delle scansioni parallele di target di Network Discover/Cloud Storage Discover

Molteplici scansioni di differenti target possono essere eseguite contemporaneamente sullo stesso server Network Discover/Cloud Storage Discover.

Le scansioni parallele dei tipi di target di server e rilevatori sono supportate. La scansione parallela dello stesso server o condivisione CIFS con differenti credenziali e dallo stesso server Network Discover/Cloud Storage Discover non è supportata.

La scansione può essere controllata (sospesa, ripresa o arrestata) indipendentemente da altre scansioni nel server Network Discover/Cloud Storage Discover. Lo stato di ogni scansione viene mantenuto e segnalato separatamente.

Quando si avvia una scansione e sono selezionati molteplici server Network Discover/Cloud Storage Discover, uno di questi viene selezionato per questa scansione. La scansione è assegnata per l'esecuzione sul server con il minor numero di scansioni in esecuzione. Il server viene scelto dal gruppo di server specificato nel target.

Per determinati target di scansione, è possibile scegliere due o più server per eseguire una scansione della griglia. Il carico di lavoro della scansione viene quindi distribuito sui server nella griglia. Attualmente, è possibile configurare le scansioni della griglia per le condivisioni di file e gli archivi di Microsoft SharePoint.

Dopo l'avvio, una scansione viene eseguita sullo stesso server fino a che non viene completata, arrestata o sospesa. Alla ripresa, l'esecuzione della scansione può essere assegnata a un server differente. Per le scansioni della griglia, il ruolo di Elemento principale griglia è assegnato a uno dei server nella griglia in base alla disponibilità dei server.

Il bilanciamento del carico automatizzato non è supportato. Se un server Network Discover/Cloud Storage Discover completa l'esecuzione di tutte le scansioni, quelle da altri server non vengono migrate al server scaricato. Tuttavia, una scansione può essere migrata manualmente, sospendendo e riavviando la scansione.

Per eseguire molteplici target di rilevatore sullo stesso server Network Discover/Cloud Storage Discover, è necessario configurare porte distinte per ogni rilevatore. La porta predefinita per un nuovo rilevatore è un valore non ancora usato da qualsiasi target della scansione.

Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.

Per configurare la scansione parallela

- 1 Nella console di amministrazione di Enforce Server, accedere a **Sistema > Server e rilevatori > Panoramica**.
- 2 Selezionare un server Network Discover/Cloud Storage Discover da configurare e fare clic sul nome del server.
- 3 Fare clic sull'opzione **Configura** nella parte superiore.
- 4 Selezionare la scheda **Discover**.
- 5 Impostare il numero massimo di scansioni parallele da eseguire su quel server Network Discover/Cloud Storage Discover.

Il valore predefinito per **Numero massimo di scansioni parallele** è 1. Il numero massimo può essere aumentato in qualunque momento. Dopo l'aumento, tutte le scansioni in coda eseguibili nel server Network Discover/Cloud Storage Discover vengono avviate. Il numero può essere diminuito solo se sul server Network Discover/Cloud Storage Discover non sono eseguite scansioni. Prima di ridurre il numero, sospendere o arrestare tutte le scansioni in esecuzione sul server Network Discover/Cloud Storage Discover.

Nota: Se si prevede di utilizzare la funzionalità di scansione di griglia per distribuire il carico di lavoro di scansione tra più server di rilevamento, mantenere il valore predefinito (1).

- 6 Fare clic su **Salva**.
- 7 Fare clic su **Fine**.
- 8 È possibile osservare le scansioni in esecuzione, in coda, programmate o sospese in ogni server Network Discover/Cloud Storage Discover. Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Discover Server**.

Vedere ["Gestione delle scansioni target di Network Discover/Cloud Storage Discover"](#) a pagina 1853.

Informazioni sulla scansione della griglia

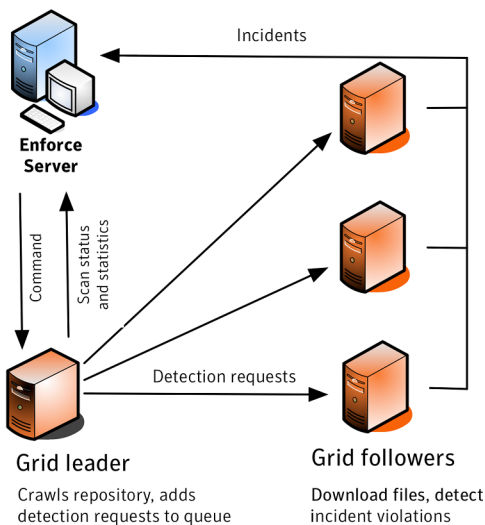
È possibile assegnare un insieme o una "griglia" di server di rilevamento Network Discover/Cloud Storage Discover a un unico target di scansione di grandi dimensioni. La scansione della griglia può migliorare significativamente la velocità di scansione per gli archivi di dati di grandi dimensioni.

Network Discover/Cloud Storage Discover supporta le scansioni della griglia sui seguenti tipi di target di scansione:

- Condivisioni file
- Server Microsoft SharePoint

Quando si assegnano server di rilevamento Network Discover/Cloud Storage Discover a una griglia, un server di rilevamento assume il ruolo di elemento principale della griglia, mentre i server di rilevamento rimanenti assumono il ruolo di elementi secondari. L'elemento principale della griglia analizza l'archivio dei dati, aggiunge le richieste di rilevamento alla coda delle richieste di rilevamento e segnala statistiche di scansione e stato a Enforce Server. Distribuisce le richieste di rilevamento provenienti dalla coda delle richieste di rilevamento agli elementi secondari della griglia. Dopodiché, gli elementi secondari della griglia scaricano ed eseguono il rilevamento sui dati richiesti, restituendo gli incidenti generati a Enforce Server. L'elemento principale della griglia gestisce automaticamente la distribuzione del carico agli elementi secondari della griglia al fine di assicurare un utilizzo ottimale delle risorse.

Figura 62-1 Panoramica dell'architettura di scansione della griglia



Quando si assegnano server di rilevamento Network Discover/Cloud Storage Discover a una griglia, Symantec Data Loss Prevention designa il primo server di rilevamento alfanumerico come elemento principale della griglia. Se il server di rilevamento non è disponibile per la scansione, Symantec Data Loss Prevention designa il server successivo nell'elenco alfanumerico come elemento principale della griglia. Ad esempio, se i server di rilevamento sono denominati:

- server-rilevamento-1A
- server-rilevamento-2B

- server-rilevamento-3C

Symantec Data Loss Prevention designa prima server-rilevamento-1A come elemento principale della griglia. Se quest'ultimo non è disponibile, Symantec Data Loss Prevention designa server-rilevamento-2B come elemento principale della griglia e così via. Non è possibile selezionare manualmente l'elemento principale della griglia. Inoltre, non è possibile aggiungere o rimuovere server a o da una griglia durante l'esecuzione di una scansione.

Vedere ["Configurazione della scansione della griglia"](#) a pagina 1876.

Vedere ["Migrazione di una scansione di rilevamento da un server singolo a una griglia"](#) a pagina 1880.

Vedere ["Linee guida per le prestazioni della scansione della griglia"](#) a pagina 1881.

Vedere ["Risoluzione dei problemi delle scansioni di griglia"](#) a pagina 1882.

La funzionalità di scansione della griglia utilizza i certificati SSL per l'autenticazione dei server di rilevamento. Quando si configura un nuovo server di rilevamento, un archivio chiavi e un archivio Attendibilità sono generati per il server di rilevamento. L'archivio chiavi e l'archivio Attendibilità contengono ciascuno un certificato di comunicazione griglia che consente al server di comunicare con l'elemento principale griglia durante una scansione della griglia. I certificati hanno un periodo di validità di cinque anni.

Quando i certificati dell'archivio chiavi e dell'archivio Attendibilità di un server di rilevamento scadono, quel server di rilevamento non potrà partecipare a una scansione della griglia fino al rinnovo dei certificati.

Vedere ["Rinnovo dei certificati di comunicazione griglia per i server di rilevamento Discover"](#) a pagina 1878.

Configurazione della scansione della griglia

Per configurare la scansione della griglia, seguire questi passaggi:

Tabella 62-11 Elenco di attività per configurare la scansione della griglia

Passaggio	Operazione	Descrizione
1	Configurare le impostazioni per ogni server di rilevamento Discover nella griglia.	Symantec suggerisce di configurare nello stesso modo tutti i server di rilevamento in una griglia. È possibile trovare informazioni utili e un foglio di lavoro sulla scalabilità nel seguente articolo del centro di supporto Symantec: http://www.symantec.com/docs/TECH247513 .

Passo	Operazione	Descrizione
2	La porta di comunicazione della griglia nel file <code>ScanManager.properties</code> sull'Enforce Server è impostata su 61616 per impostazione predefinita. È possibile cambiare questo numero di porta.	<p>La proprietà <code>com.vontu.filescan.scanmanager.ScanManager.leader_port</code> nel file <code>ScanManager.properties</code> specifica la porta utilizzata dall'elemento principale della griglia per comunicare con gli altri membri della griglia. Questa porta deve essere aperta su tutti i server di rilevamento nella griglia.</p> <p>Vedere "Per impostare la porta di comunicazione della griglia" a pagina 1878.</p>
3	Confermare la dimensione della coda e i valori moltiplicatori della dimensione della coda. I valori predefiniti per la dimensione della coda e per i moltiplicatori della dimensione della coda si impostano nel file <code>Crawler.properties</code> in ogni server di rilevamento.	<p>Queste proprietà specificano la dimensione della coda e il numero di handle di file per ogni server di rilevamento nella griglia. È possibile adattare questo parametro per ottimizzare la gestione della richiesta di rilevamento da parte degli elementi secondari della griglia. È possibile trovare l'impostazione ottimale per l'ambiente in questione aumentando i valori nel proprio ambiente di test e osservando i risultati.</p> <p>Questa impostazione è applicabile solo all'elemento principale della griglia operativo, ma deve essere impostata su ogni server di rilevamento nella griglia.</p> <p>Vedere "Per impostare la dimensione della coda e il moltiplicatore della dimensione della coda" a pagina 1878.</p>
4	Assicurarsi che il valore Numero massimo di scansioni parallele su ogni server di rilevamento sia 1 .	<p>Ogni server di rilevamento nella griglia è dedicato a una singola scansione e deve quindi eseguire una singola scansione.</p> <p>Vedere "Per impostare il numero massimo di scansioni parallele" a pagina 1878.</p>
5	Configurare il target di scansione.	<p>Configurare il target di scansione sulla pagina Gestisci > Scansione Discover > Target di Discover.</p> <p>Vedere "Configurazione delle scansioni del file system" a pagina 1922.</p> <p>Vedere "Configurazione ed esecuzione delle scansioni dei server SharePoint" a pagina 1950.</p>

Per impostare la porta di comunicazione della griglia

- 1 Su Enforce Server, aprire il file `ScanManager.properties` in un editor di testo.
- 2 Impostare il valore desiderato per la proprietà `com.vontu.filescan.scanmanager.ScanManager.leader_port`. La porta predefinita è 61616.
- 3 Salvare e chiudere il file.
- 4 Riavviare il servizio `SymantecDLPDetectionServerController`.

Per impostare la dimensione della coda e il moltiplicatore della dimensione della coda

- 1 Su ogni server di rilevamento Network Discover nella griglia, aprire il file `Crawler.properties` in un editor di testo.
- 2 Impostare il valore desiderato per la proprietà `crawler.grid.queue.size.multiplier`. Il valore predefinito è 60.
- 3 Impostare il valore desiderato per la proprietà `crawler.grid.follower.queue.size`. Il valore predefinito è 30.
- 4 Salvare e chiudere il file.
- 5 Riavviare il servizio `SymantecDLPDetectionServer` su ogni server di rilevamento.

Per ulteriori informazioni sulle impostazioni del server di rilevamento per le scansioni della griglia, vedere <http://www.symantec.com/docs/TECH247513>.

Per impostare il numero massimo di scansioni parallele

- 1 Accedere alla pagina **Sistema > Server e rilevatori > Panoramica > Configura server** per ogni server di rilevamento nella griglia.
- 2 Nel campo **Numero massimo di scansioni parallele** della sezione **Discover**, inserire 1.
- 3 Fare clic su **Salva**.

Rinnovo dei certificati di comunicazione griglia per i server di rilevamento Discover

La funzionalità di scansione di griglia utilizza i certificati SSL per autenticare i server di rilevamento Discover che fanno parte di una griglia affinché possano comunicare con l'elemento principale della griglia. Quando si configura un nuovo server di rilevamento, un archivio chiavi e un archivio Attendibilità sono generati per quel server. Quando il certificato di comunicazione griglia di un server scade, quel server non può più partecipare alle scansioni di griglia fino al rinnovo del certificato.

Prima di rinnovare il certificato di comunicazione griglia di un server di rilevamento, è necessario identificare i file dell'archivio chiavi e dell'archivio Attendibilità che ne contengono i certificati.

Per identificare il file dell'archivio chiavi per un server di rilevamento

- 1 Nella console di amministrazione di Enforce Server, accedere a **Sistema > Server e rilevatori > Eventi**.
- 2 Nell'area **Filtro**, espandere la sezione **Filtri avanzati e riepilogo**.
- 3 Fare clic su **Aggiungi filtro** e procedere come segue:
 - Nella prima casella di riepilogo, selezionare **Server o rilevatore**.
 - Nella seconda casella di riepilogo, selezionare **È uno qualsiasi dei seguenti valori**.
 - Nella terza casella di riepilogo, selezionare il server di rilevamento con il certificato di comunicazione griglia scaduto.
- 4 Fare clic di nuovo su **Aggiungi filtro** e procedere come segue:
 - Nella prima casella di riepilogo, selezionare **Codice evento**.
 - Nella seconda casella di riepilogo, selezionare **È uno qualsiasi dei seguenti valori**.
 - Nella terza casella di riepilogo, digitare **2136**.
- 5 Fare clic su **Applica**.
- 6 Quando il filtro diventa effettivo, aprire il record creato dell'evento 2136 creato più di recente.
- 7 Nella schermata **Dettagli evento**, prendere nota del nome del file dell'archivio chiavi che viene visualizzato nel campo **Dettaglio**.

Ad esempio, `monitor11_keystore_v1.jks`.

Per identificare il file dell'archivio Attendibilità per un server di rilevamento

- 1 Nella console di Enforce Server, accedere a **Sistema > Server e rilevatori > Eventi**.
- 2 Nell'area **Filtro**, espandere la sezione **Filtri avanzati e riepilogo**.
- 3 Fare clic su **Aggiungi filtro** e procedere come segue:
 - Nella prima casella di riepilogo, selezionare **Server o rilevatore**.
 - Nella seconda casella di riepilogo, selezionare **È uno qualsiasi dei seguenti valori**.
 - Nella terza casella di riepilogo, selezionare il server di rilevamento con il certificato di comunicazione griglia scaduto.
- 4 Fare clic di nuovo su **Aggiungi filtro** e procedere come segue:
 - Nella prima casella di riepilogo, selezionare **Codice evento**.
 - Nella seconda casella di riepilogo, selezionare **È uno qualsiasi dei seguenti valori**.

- Nella terza casella di riepilogo, digitare **2138**.
- 5 Fare clic su **Applica**.
- 6 Quando il filtro diventa effettivo, aprire il record creato dell'evento 2136 creato più di recente.
- 7 Nella schermata **Dettagli evento**, prendere nota del nome del file dell'archivio chiavi che viene visualizzato nel campo **Dettaglio**.
 Ad esempio, `monitor11_truststore_v1.jks`.

Per rinnovare il certificato di comunicazione griglia per un server di rilevamento

- 1 Nel sistema di Enforce Server, accedere alla directory `X:\Programmi\Symantec\Data Loss Prevention\Enforce Server\Protect\keystore`, dove **X** è la lettera dell'unità in cui Enforce Server è installato.
 - 2 Eliminare i file identificati dell'archivio Attendibilità e dell'archivio chiavi.
 - 3 Riavviare il server di rilevamento.
- Quando rileva il server di rilevamento riavviato, Enforce Server genera i nuovi file dell'archivio Attendibilità e dell'archivio chiavi che contengono i nuovi certificati validi per altri cinque anni.

Migrazione di una scansione di rilevamento da un server singolo a una griglia

È possibile eseguire la migrazione delle scansioni da server singolo esistenti alla scansione di una griglia. Le best practice per la migrazione di una scansione sono:

- Scegliere i server di rilevamento più vicini ai target di scansione per la scansione della griglia. La scelta dei server di rilevamento più vicini al target consente di massimizzare le prestazioni per la griglia.
- Unire i target di scansione delle scansioni da server singolo alla scansione di una griglia in prossimità. Se un target viene suddiviso tra più scansioni di un singolo server, unendo tali target alla scansione singola della griglia più vicina si ottiene un miglioramento delle prestazioni.

Se è stata configurata l'indicizzazione incrementale per gli esistenti target di scansione delle condivisioni file su server singolo, è possibile incorporare gli indici incrementali nella nuova scansione della griglia.

Vedere ["Informazioni sulle scansioni incrementali"](#) a pagina 1869.

Nota: Attualmente, è possibile configurare le scansioni della griglia solo per le condivisioni di file e gli archivi Microsoft SharePoint.

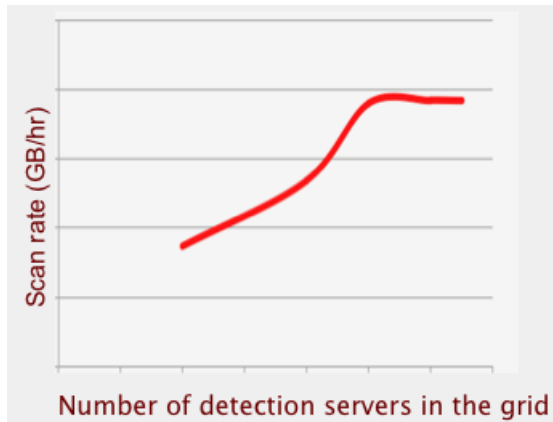
Linee guida per le prestazioni della scansione della griglia

Le prestazioni relative alla scansione di una griglia dipendono da diversi fattori:

- Complessità della politica di rilevamento
- Specifiche dei server di rilevamento
- Dimensioni medie dei file nel set di dati
- Latenze I/O di rete e file
- Numero di richieste simultanee consentite sui server del target di scansione
- Il tempo di risposta del file system e dei server SharePoint di destinazione

Tenendo presenti queste considerazioni, occorre osservare che la scansione della griglia non offre una scalabilità lineare. Le prestazioni seguono piuttosto un andamento curvilineo simile a quello illustrato in [Figura 62-2](#).

Figura 62-2 Modello di prestazioni di scansione della griglia



Sebbene Symantec non possa fornire valori specifici per gli assi di questo grafico, la curva indica che verrà raggiunto un punto in cui l'aggiunta di più server di rilevamento alla scansione della griglia non comporterà un aumento della velocità di scansione.

Per informazioni sulle impostazioni consigliate per ciascun server per ottenere prestazioni ottimali, consultare l'articolo del centro di supporto Symantec all'indirizzo:

<http://www.symantec.com/docs/TECH247513>.

Determinare il numero corretto di server di rilevamento per la griglia

In un ambiente di test, è possibile valutare qual è il numero ottimale di server di rilevamento da assegnare a una scansione della griglia. L'obiettivo del test è determinare il numero di server richiesti per il download e la scansione di tutte le richieste di rilevamento provenienti dall'elemento principale della griglia. Dopo avere assegnato un numero di server sufficiente per la gestione di tutte le richieste di rilevamento provenienti dall'elemento principale della griglia, la scansione verrà eseguita a un livello di prestazioni ottimale. L'aggiunta di altri server alla griglia in questa fase non comporterà un aumento della velocità di scansione.

Non vi è una stretta correlazione tra dimensione media dei file nel target di scansione e numero ottimale di server di rilevamento nella griglia. File di dimensioni medie ridotte offrono in genere prestazioni migliori con un numero inferiore di server di rilevamento nella griglia, mentre file di dimensioni medie più elevate richiedono più server.

Visualizzare il registro delle prestazioni della griglia per semplificare l'individuazione del numero corretto di server, al fine di ottimizzare le prestazioni di scansione della griglia. Il registro delle prestazioni della griglia registra i valori delle prestazioni a intervalli di 15 minuti durante tutta la scansione della griglia.

Utilizzo del registro delle prestazioni della griglia per valutare le prestazioni di scansione

- 1 Quando la scansione è completa, aprire il file `c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\logs\GridPerformance-TargetName.log` (Windows) o `/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/GridPerformance-TargetName.log` (Linux) in un editor di testo.
- 2 Individuare il `CrawlerWaitTime` per l'elemento principale della griglia negli ultimi 15 minuti della scansione. Per garantire prestazioni ottimali, il tempo di attesa crawler deve essere 0. Regolare il numero di elementi secondari della griglia in base alle esigenze di ottimizzazione della griglia. Potrebbe essere necessario ripetere e registrare diverse scansioni per raggiungere questo risultato.

Aumento del carico sui server target della scansione

Si tenga presente che una scansione della griglia potrebbe comportare un carico maggiore sui server target della scansione rispetto alla scansione di rilevamento su server singolo. Potrebbe essere necessario aumentare il numero di richieste simultanee consentite dai server del file system e SharePoint nonché migliorarne i tempi di risposta al fine di massimizzare le prestazioni di scansione.

Risoluzione dei problemi delle scansioni di griglia

La sezione **Stato griglia recente** di **Dettagli scansione** visualizza un messaggio di errore quando uno o più server di rilevamento non sono stati in grado di partecipare alla scansione

di griglia. È possibile visualizzare i registri operativi e di debug per ogni server di rilevamento non partecipante per determinare la causa del problema e la soluzione appropriata.

Vedere ["Raccolta dei registri e dei file di configurazione del server"](#) a pagina 351.

Nota: Le scansioni della griglia sono supportate attualmente solo nei target di scansione dei server File System e SharePoint. Vedere ["Configurazione delle scansioni del file system"](#) a pagina 1922. e Vedere ["Configurazione ed esecuzione delle scansioni dei server SharePoint"](#) a pagina 1950.

Certificato di comunicazione griglia scaduto

Quando si accede al file del registro operativo per un server di rilevamento, il messaggio di errore **Certificato di comunicazione griglia scaduto o non ancora valido** indica che è necessario rinnovare i certificati SSL del server di rilevamento.

Nota: Quando il certificato di comunicazione griglia dell'elemento principale della griglia scade, anche la sezione **Errori di scansione** della schermata **Dettagli scansione** visualizza il messaggio di errore **Certificato di comunicazione griglia scaduto o non ancora valido**. È quindi necessario rinnovare il certificato di comunicazione griglia per l'elemento principale della griglia. Vedere ["Rinnovo dei certificati di comunicazione griglia per i server di rilevamento Discover"](#) a pagina 1878.

Messaggi di errore di timeout di scansione

Se la sezione **Errori di scansione recenti** della schermata **Dettagli scansione** visualizza il messaggio di errore **Timeout durante l'attesa di una risposta dai server di rilevamento**. **Verifica lo stato dei server di rilevamento nella griglia**, verificare che i server di rilevamento interessati siano in esecuzione e assicurarsi che ci sia connettività tra i server di rilevamento e l'elemento principale della griglia.

Disconnessione da Enforce Server

Se la sezione **Errori di scansione recenti** della schermata **Dettagli scansione** visualizza il messaggio di errore **Disconnesso da Enforce**, verificare lo stato della connettività di rete in tutti i membri della griglia.

Esecuzione di scansioni della griglia consecutive sullo stesso target di scansione

Dopo avere completato una scansione della griglia, i membri della griglia potrebbero rimanere occupati con attività di post-scansione per un breve periodo di tempo. Se si tenta di inizializzare un'altra scansione della griglia sullo stesso target di scansione durante questo periodo, alcuni dei server di rilevamento potrebbero non partecipare alla scansione.

Se la sezione **Stato griglia recente** dello schermo **Dettagli scansione** mostra il messaggio di errore **Esecuzione istanza precedente della scansione corrente** accanto ai nomi di uno o più server di rilevamento, mettere in pausa la scansione della griglia e riprenderla dopo dieci minuti.

Membri della griglia occupati con altre scansioni

Quando si inizializza una scansione della griglia, alcuni dei membri della griglia potrebbero ancora essere occupati con altre scansioni e non parteciperanno alla nuova scansione della griglia.

Se la sezione **Stato griglia recente** dello schermo **Dettagli scansione** mostra il messaggio di errore **Esecuzione scansione Nome target di scansione** accanto ai nomi di uno o più server di rilevamento, mettere in pausa la scansione della griglia e riprenderla quando sono disponibili tutti i membri della griglia.

Tempi di scansione più lunghi alla fine della scansione

I tempi di scansione potrebbero aumentare quando la scansione si avvicina al completamento. Ciò può essere dovuto al ravvio degli elementi secondari della griglia, a errori di rilevamento o al timeout dei processi di download o rilevamento.

L'elemento principale della griglia attende la risposta di ogni elemento secondario della griglia per 30 minuti. Se l'elemento principale non riceve una risposta entro 30 minuti, contrassegnerà tali richieste come non riuscite.

Utilizzo dei plug-in FlexResponse server per riparare gli incidenti

Il capitolo contiene i seguenti argomenti:

- [Informazioni sulla piattaforma FlexResponse server](#)
- [Utilizzo dei plug-in personalizzati di FlexResponse server per riparare gli incidenti](#)
- [Distribuzione di un plug-in di FlexResponse server](#)
- [Individuazione di incidenti per la riparazione manuale](#)
- [Utilizzo dell'azione di un plug-in di FlexResponse server per riparare un incidente manualmente](#)
- [Verifica dei risultati di un'azione di risposta agli incidenti](#)
- [Risoluzione dei problemi relativi a un plug-in di FlexResponse server](#)

Informazioni sulla piattaforma FlexResponse server

L'API FlexResponse server fornisce una piattaforma flessibile per la riparazione degli incidenti. Consente agli utenti di Symantec Data Loss Prevention di proteggere i dati richiamando automaticamente o manualmente azioni di FlexResponse server personalizzate.

Symantec fornisce un set di plug-in di FlexResponse server che eseguono varie riparazioni come la quarantena di dati riservati, la copia di file e la protezione o la crittografia di diritti digitali. Gli sviluppatori indipendenti possono anche scrivere plug-in di FlexResponse server per eseguire la riparazione personalizzata degli incidenti utilizzando questa API e il linguaggio di programmazione Java. L'API FlexResponse server consente agli sviluppatori di generare

un plug-in che può essere utilizzato per implementare risposte agli incidenti da utilizzare nelle regole di risposta automatiche e smart.

Di seguito sono riportati alcuni esempi di azioni di Network Protect che è possibile implementare sviluppando un plug-in di FlexResponse server:

- Modificare gli elenchi ACL nei file. Ad esempio, è possibile rimuovere l'accesso di tipo guest ai file selezionati.
- Applicare il componente DRM. Ad esempio, è possibile applicare diritti digitali ai documenti in modo da limitare l'accesso delle entità esterne a materiale riservato. Questi diritti digitali possono includere "non inoltrare" o "non stampare".
- Crittografare i file.
- Migrare file a SharePoint. L'azione di protezione personalizzata può spostare i file da condivisioni in un archivio SharePoint e quindi applicare DRM e ACL.
- Eseguire il flusso di lavoro e l'automazione delle risposte di riparazione.
- Utilizzare il flusso di lavoro di automazione del processo aziendale Symantec Workflow.

I seguenti passaggi sono inclusi nella costruzione, nella distribuzione e nell'utilizzo di un plug-in di FlexResponse server:

- Sviluppo di un plug-in utilizzando l'API Java. Questa fase comprende la progettazione e la scrittura del codice del plug-in e dell'azione di riparazione.
- Configurazione dei parametri del plug-in mediante la creazione del file delle proprietà di configurazione per il plug-in.
Vedere ["Creazione di un file di proprietà per configurare un plug-in di FlexResponse server"](#) a pagina 1891.
- Aggiunta dei plug-in al file delle proprietà di configurazione dei plug-in.
Vedere ["Aggiunta di un plug-in FlexResponse server al file delle proprietà dei plug-in"](#) a pagina 1889.
- Distribuzione del plug-in personalizzato su Enforce Server.
Vedere ["Distribuzione di un plug-in di FlexResponse server"](#) a pagina 1888.
- Caricamento del plug-in, inclusi i metadati del plug-in.
- Creazione di regole di risposta per le azioni di risposta smart per incidenti.
- Utilizzo dell'azione del plug-in per riparare un incidente.
Vedere ["Utilizzo dell'azione di un plug-in di FlexResponse server per riparare un incidente manualmente"](#) a pagina 1895.
- Verifica dei risultati dell'azione del plug-in di FlexResponse server.
Vedere ["Verifica dei risultati di un'azione di risposta agli incidenti"](#) a pagina 1896.

Nota: I plug-in di FlexResponse server che sono stati creati per le versioni 12.x e 14.x di Symantec Data Loss Prevention sono compatibili con Symantec Data Loss Prevention 15.x.

Le sezioni che seguono descrivono come distribuire e configurare i plug-in di FlexResponse predefiniti, nonché come utilizzare le azioni dei plug-in personalizzati nella politiche di Symantec Data Loss Prevention. È possibile ottenere alcuni plug-in di FlexResponse server direttamente da Symantec. È anche possibile sviluppare i propri plug-in personalizzati utilizzando l'API FlexResponse server. Per informazioni sullo sviluppo di plug-in utilizzando l'API Java, vedere la *Guida degli sviluppatori della piattaforma FlexResponse server di Symantec Data Loss Prevention*.

Utilizzo dei plug-in personalizzati di FlexResponse server per riparare gli incidenti

È possibile utilizzare le azioni dei plug-in di FlexResponse server per riparare automaticamente o manualmente gli incidenti di Network Discover.

Per sviluppare un'azione di riparazione personalizzata, vedere la *Guida degli sviluppatori della piattaforma FlexResponse server di Symantec Data Loss Prevention*.

Per riparare automaticamente o manualmente gli incidenti con un plug-in personalizzato di FlexResponse server, è necessario completare i seguenti passaggi:

Tabella 63-1

Passaggio	Azione	Descrizione
1	Distribuire un plug-in di FlexResponse server al computer Enforce Server.	Ogni plug-in di FlexResponse server deve essere distribuito al computer Enforce Server prima di poter utilizzare le azioni dei plug-in nelle politiche di Symantec Data Loss Prevention. Vedere " Distribuzione di un plug-in di FlexResponse server " a pagina 1888.
2	Creare una regola di risposta che utilizza un'azione di risposta agli incidenti personalizzata di FlexResponse server.	Vedere " Configurazione dell'azione di FlexResponse server " a pagina 1516.

Passaggio	Azione	Descrizione
3	(Facoltativo) Utilizzare il plug-in di FlexResponse server per riparare manualmente gli incidenti.	<p>Se si sta utilizzando un'azione del plug-in di FlexResponse server in una regola di risposta smart, è necessario individuare manualmente un incidente ed eseguire l'azione di FlexResponse.</p> <p>Vedere "Individuazione di incidenti per la riparazione manuale" a pagina 1894.</p> <p>Vedere "Utilizzo dell'azione di un plug-in di FlexResponse server per riparare un incidente manualmente" a pagina 1895.</p> <p>Questo passaggio non è necessario se si configura una regola di risposta automatica per eseguire un'azione di FlexResponse server. Con le regole di risposta automatiche, la creazione di un incidente che genera la regola di risposta automatica esegue anche l'azione di FlexResponse configurata.</p>
4	Verificare i risultati.	Vedere "Verifica dei risultati di un'azione di risposta agli incidenti" a pagina 1896.

Distribuzione di un plug-in di FlexResponse server

Attivare un plug-in per l'API FlexResponse server.

Per distribuire un plug-in di FlexResponse server

- 1 Copiare il file JAR completato del plug-in di FlexResponse server nella directory dei plug-in:

```
\Program Files\Symantec\Data Loss Prevention\Enforce
Server\15.1\Protect\plugins\.
```

- 2 Configurare il plug-in con un file di proprietà.

Vedere ["Creazione di un file di proprietà per configurare un plug-in di FlexResponse server"](#) a pagina 1891.

- 3 Copiare il file di proprietà per ogni plug-in nella directory in cui si trova il file JAR:

```
\Program Files\Symantec\Data Loss Prevention\Enforce
Server\15.1\Protect\plugins\
```

- 4 Nel file `\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config\Plugins.properties`, aggiungere il plug-in all'elenco e immettere le proprietà per il plug-in.

Vedere ["Aggiunta di un plug-in FlexResponse server al file delle proprietà dei plug-in"](#) a pagina 1889.

- 5 Assicurarsi che l'utente Proteggi di Symantec Data Loss Prevention abbia eseguito l'accesso al file JAR del plug-in e al file di proprietà del plug-in.
- 6 Per caricare il plug-in, arrestare i servizi Symantec DLP Incident Persister e Symantec DLP Manager, quindi riavviarli.

Aggiunta di un plug-in FlexResponse server al file delle proprietà dei plug-in

La seguente procedura fornisce istruzioni dettagliate su come aggiungere il plug-in di FlexResponse server al file `Plugins.properties`.

Nota: Symantec Data Loss Prevention 15.1 include plug-in di FlexResponse preinstallati per **SharePoint Encrypt** e **Quarantena SharePoint**. I plug-in **SharePoint Encrypt** e **Quarantena SharePoint** funzionano solo se ci si connette alla distribuzione di SharePoint utilizzando la soluzione Symantec SharePoint. Il plug-in FlexResponse di **SharePoint Encrypt** richiede inoltre una connessione al cloud Symantec ICE. Vedere ["Installazione della soluzione SharePoint su front end Web in un gruppo"](#) a pagina 1958. Vedere ["Configurazione di Enforce Server per connettersi al cloud ICE Symantec"](#) a pagina 229.

Aggiungere un plug-in FlexResponse server al file delle proprietà

- 1 Modificare il file `Plugins.properties`.

Questo file contiene valori generali per tutti i plug-in, oltre a un elenco di tutti i plug-in implementati.

Vedere [Tabella 63-2](#) a pagina 1890.

Questo file si trova nella directory `\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config`.

- 2 Individuare la seguente riga nel file, che specifica i file JAR dei plug-in da generare al caricamento:

```
# Incident Response Action configuration parameters.
```

```
com.symantec.dlp.flexresponse.Plugin.plugins =  
    plugin1.jar,plugin2.jar
```

Rimuovere il commento dall'inizio della riga, se necessario, e sostituire `plugin1.jar,plugin2.jar` con i nomi dei file JAR dei plug-in che si desidera distribuire. Separare i file JAR con una virgola.

- 3 Se desiderato, modificare altri parametri in questo file.

[Tabella 63-2](#) descrive le proprietà supplementari dell'API di FlexResponse server nel file `Plugins.properties`.

- 4 Arrestare i servizi Symantec DLP Incident Persister e Symantec DLP Manager e riavviarli. Questo consente il caricamento del nuovo plug-in e degli altri parametri di questo file.

Se successivamente si modifica il file `Plugins.properties`, è necessario riavviare i servizi Symantec DLP Incident Persister e Symantec DLP Manager per applicare la modifica.

Nella [Tabella 63-2](#) *plugin-id* è un identificatore unico del plug-in all'interno di questo file di proprietà, ad esempio `test1`.

Tabella 63-2 Parametri nel file `Plugins.properties`

Nome proprietà	Descrizione
protect.plugins.directory	La directory nella quale sono installati tutti i plug-in di Symantec Data Loss Prevention.
com.symantec.dlp.flexresponse.Plugin.plugins	<p>L'elenco separato da virgole dei file JAR (o titoli JAR) da caricare nel contenitore dei plug-in di FlexResponse server.</p> <p>Ogni plug-in in questo elenco corrisponde a un'azione della regola di risposta nella console di amministrazione di Enforce Server.</p> <p>Il contenitore in cui i file JAR vengono distribuiti include tutte le classi pubbliche JRE fornite dalla JVM installata con Symantec Data Loss Prevention. Il contenitore include anche tutte le classi dell'API FlexResponse descritte in questo documento (classi nella gerarchia dei pacchetti <code>com.symantec.dlp</code>). Il codice del plug-in FlexResponse potrebbe contenere parti che dipendono da altri file JAR non disponibili nel contenitore dei plug-in. Collocare i file JAR esterni richiesti nella directory <code>\plugins</code> di Enforce Server in cui è stato distribuito il plug-in. Quindi fare riferimento al JAR in questa proprietà.</p>
com.vontu.enforce.incidentresponseaction.IncidentResponseActionInvocationService.maximum-incident-batch-size	<p>Il numero massimo di incidenti che possono essere selezionati dal report dell'elenco di incidenti per ogni invocazione della regola di risposta di FlexResponse server.</p> <p>L'impostazione predefinita è 100.</p> <p>In questa versione, il valore massimo di questo parametro non può superare 1000.</p>

Nome proprietà	Descrizione
com.vontu.enforce.incidentresponseaction. IncidentResponseActionInvocationService. keep-alive-time	Non cambiare il valore del parametro. Questo parametro è riservato per lo sviluppo e il debug. Utilizzare la proprietà <code>timeout</code> nel file delle proprietà dei singoli plug-in per impostare il timeout dei thread di esecuzione del plug-in.
com.vontu.enforce.incidentresponseaction. IncidentResponseActionInvocationService. serial-timeout	Il timeout dei thread di esecuzione per l'esecutore dei thread seriali (globale). Per dettagli, consultare la proprietà <code>is-serialized</code> nel file delle proprietà dei singoli plug-in.

Creazione di un file di proprietà per configurare un plug-in di FlexResponse server

Informazioni e parametri specifici per ogni plug-in di FlexResponse server sono inclusi nel file `nome plug-in.properties`.

Ogni plug-in deve avere un file di proprietà distinto.

Un singolo file di proprietà di plug-in non è necessario se il plug-in soddisfa le seguenti condizioni:

- Non necessita di proprietà personalizzate.
- Fornisce il nome visualizzato e l'identificatore del plug-in nell'implementazione della classe di metadati del plug-in.
- Non necessita di una credenziale archiviata.

Per configurare un plug-in di FlexResponse server

- 1 Creare un file di testo che contiene le proprietà per ogni plug-in di FlexResponse server.

Ogni file JAR ha un file di proprietà associato opzionale con lo stesso nome base del file JAR. Questi file sono situati nella directory `\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\plugins`.

Ad esempio, se si ha un file `plugin1.jar`, è necessario creare un file `plugin1.properties`.

- 2 In questo file, immettere le chiavi e i valori di tutti i parametri per il plug-in:

```
display-name=plugin 1
plugin-identifier=IncidentResponseAction1
```

Per aggiornare le proprietà, è necessario arrestare i servizi Symantec DLP Manager e Symantec DLP Incident Persister, quindi riavviarli per caricare i nuovi valori.

Vedere [Tabella 63-3](#) a pagina 1892.

- 3 Assicurarsi che l'utente di Symantec Data Loss Prevention abbia eseguito l'accesso al file di proprietà del plug-in.

[Tabella 63-3](#) descrive le proprietà nel file `nome plug-in.properties`.

Tabella 63-3 Parametri nel file di proprietà del plug-in personalizzato

Nome proprietà	Descrizione
display-name	<p>Il nome di questo plug-in.</p> <p>Questo nome viene visualizzato nel menu a discesa per la scelta del plug-in quando si seleziona un'azione Tutto: FlexResponse server in una regola di risposta smart o in una regola di risposta automatica.</p> <p>Una best practice consiste nel definire questa proprietà nel file di proprietà del plug-in.</p> <p>Se si modifica il valore di questo nome nel file di proprietà dopo che il plug-in è stato caricato, è necessario riavviare i servizi Symantec DLP Incident Persister e Symantec DLP Manager per caricare il nuovo nome.</p> <p>In alternativa, questo valore può essere specificato nella classe di metadati.</p> <p>Questo valore è obbligatorio e deve essere specificato almeno nel file di proprietà di configurazione o nella classe di metadati del plug-in.</p> <p>Per gli ambienti internazionali, questo nome visualizzato può essere nella lingua locale.</p>
plugin-identifier	<p>L'identificatore di questo plug-in. Questo identificatore deve essere univoco per tutti i plug-in di FlexResponse server su questo Enforce Server.</p> <p>Una best practice consiste nel definire questa proprietà nel file di proprietà del plug-in.</p> <p>In alternativa, questo valore può essere specificato nella classe di metadati.</p> <p>Questo valore è obbligatorio e deve essere specificato almeno nel file di proprietà di configurazione o nella classe di metadati del plug-in.</p> <p>Se una qualsiasi regola di risposta è assegnata a questo plug-in di FlexResponse server, non modificare questo identificatore nel file di proprietà.</p>

Nome proprietà	Descrizione
<i>referimento-credenziale.credential</i>	<p>Specifica un riferimento a una credenziale con nome per autenticare l'accesso, ad esempio a un database di inventario. Il valore di questa proprietà deve fare riferimento a una credenziale con nome definita su Enforce Server. Il testo <i>referimento-credenziale</i> nel nome della proprietà fornisce un metodo per differenziare molteplici credenziali nel file di proprietà.</p> <pre>inventory-credential.credential= InventoryDB1</pre>
<p>custom name</p> <p>Esempio:</p> <p>test1.value.1</p> <p>test1.value.2</p>	<p>Questi parametri personalizzati opzionali sono richiesti per trasmettere informazioni al plug-in. Questi parametri sono passati a ogni chiamata del plug-in e possono eventualmente risultare disponibili al momento della costruzione del plug-in.</p>
timeout	<p>Parametro opzionale con il timeout in millisecondi per l'esecuzione dei thread per questo plug-in.</p> <p>Il valore predefinito è 60000 (un minuto).</p> <p>Se il valore di timeout viene raggiunto, nell'interfaccia utente lo stato del plug-in di FlexResponse server è non riuscito e la cronologia incidenti viene aggiornata con un messaggio di timeout.</p> <p>Se si modifica il valore di questa proprietà nel file di proprietà dopo che il plug-in è stato caricato, è necessario arrestare e quindi riavviare i servizi Symantec DLP Incident Persister e Symantec DLP Manager.</p>
maximum-thread-count	<p>Parametro opzionale con il numero di thread paralleli disponibili per l'esecuzione di questo plug-in. Questo parametro viene ignorato se <i>is-serialized</i> è impostato.</p> <p>Il valore predefinito è 2.</p> <p>Se si modifica il valore di questa proprietà nel file di proprietà dopo che il plug-in è stato caricato, è necessario arrestare e quindi riavviare i servizi Symantec DLP Incident Persister e Symantec DLP Manager.</p>

Nome proprietà	Descrizione
is-serialized	<p>Il valore di questo parametro può essere true o false. Impostare questo parametro opzionale su true se l'esecuzione di questo plug-in deve essere serializzata (un thread alla volta). Tutti i collegamenti serializzati condividono un singolo thread di esecuzione. Se questo parametro è impostato, <code>timeout</code> e <code>maximum-thread-count</code> vengono ignorati.</p> <p>L'impostazione predefinita è false.</p> <p>Se si modifica il valore di questa proprietà nel file di proprietà dopo che il plug-in è stato caricato, è necessario arrestare e quindi riavviare i servizi Symantec DLP Incident Persister e Symantec DLP Manager.</p>

Individuazione di incidenti per la riparazione manuale

Per eseguire manualmente l'azione del plug-in configurata in una regola di risposta smart, usare i report su Enforce Server per selezionare gli incidenti da riparare.

Per individuare gli incidenti per la riparazione manuale

- 1 Accedere alla console di amministrazione di Enforce Server.
- 2 Fare clic su **Incidenti > Discover**.
- 3 Selezionare un incidente (o molteplici) da riparare. È possibile utilizzare i report o i filtri di report standard per limitare l'elenco di incidenti.
- 4 È possibile selezionare un gruppo di incidenti, oppure un incidente per la riparazione:
 - Nell'elenco degli incidenti, selezionare la casella a sinistra di ogni incidente per selezionare l'incidente corrispondente. È possibile selezionare molteplici incidenti.
 - Nell'elenco degli incidenti, selezionare tutti gli incidenti in questa pagina facendo clic sulla casella di controllo a sinistra dell'intestazione del report.
 - Nell'elenco degli incidenti, selezionare tutti gli incidenti nel report facendo clic sull'opzione **Seleziona tutto** nella parte superiore destra del report.
 - Fare clic su un incidente per visualizzare **dettagli sull'incidente** e selezionare quell'incidente per una possibile riparazione.

Dopo aver selezionato gli incidenti, è possibile ripararli manualmente.

Vedere ["Utilizzo dell'azione di un plug-in di FlexResponse server per riparare un incidente manualmente"](#) a pagina 1895.

Utilizzo dell'azione di un plug-in di FlexResponse server per riparare un incidente manualmente

Dopo aver selezionato un incidente o un gruppo di incidenti da riparare, è possibile richiamare l'azione di una regola di risposta smart. Questa azione utilizza il plug-in di FlexResponse server personalizzato per riparare gli incidenti manualmente.

Per riparare un singolo incidente

- 1 Informarsi sulle regole di risposta disponibili per la riparazione manuale di un incidente.
Fare clic su **Gestisci > Politiche > Regole di risposta**.
La colonna **Condizioni** indica quali regole possono essere eseguite manualmente.
- 2 Selezionare un singolo incidente e fare clic su **Dettagli incidente** per visualizzare le informazioni relative.
Vedere ["Individuazione di incidenti per la riparazione manuale"](#) a pagina 1894.
- 3 Nella schermata **Dettagli incidente**, le opzioni di riparazione sono visualizzate sopra il numero di incidente. Queste opzioni mostrano i nomi delle regole di risposta.
- 4 Fare clic su un plug-in di FlexResponse server per eseguire l'azione di riparazione.
- 5 Visualizzare l'azione di riparazione. Fare clic su **OK**.
- 6 Verificare il completamento della riparazione. Alcune azioni di riparazione, ad esempio la crittografia di un file di grandi dimensioni, possono richiedere molto tempo. Per visualizzare gli aggiornamenti dell'interfaccia utente, fare clic su l'icona di aggiornamento nell'angolo superiore destro del report. Aggiornare la pagina fino a che non è visualizzata l'icona verde (operazione completata) o rossa (operazione non riuscita) della riparazione nei dettagli sull'incidente.
Vedere ["Verifica dei risultati di un'azione di risposta agli incidenti"](#) a pagina 1896.

Per riparare un gruppo di incidenti selezionato

- 1 Selezionare gli incidenti a partire da un report Elenco incidenti. Selezionare la casella di controllo a sinistra degli incidenti selezionati.
Alternativamente, è possibile selezionare tutti gli incidenti in una pagina o in un report.
Vedere ["Individuazione di incidenti per la riparazione manuale"](#) a pagina 1894.
- 2 **Azioni incidente** diventa un menu a discesa.
- 3 Dal menu a discesa **Azioni incidente**, selezionare **Esegui risposta smart** e quindi il plug-in FlexResponse server personalizzato.

- 4 Visualizzare l'azione di riparazione. Fare clic su **OK**.
- 5 Verificare il completamento della riparazione. Alcune azioni di riparazione possono richiedere molto tempo, soprattutto se sono stati selezionati vari incidenti. Per visualizzare gli aggiornamenti dell'interfaccia utente, fare clic su l'icona di aggiornamento nell'angolo superiore destro del report. Aggiornare la pagina fino a che non è visualizzata l'icona verde (operazione completata) o rossa (operazione non riuscita) della riparazione nei dettagli sull'incidente.

Vedere ["Verifica dei risultati di un'azione di risposta agli incidenti"](#) a pagina 1896.

Verifica dei risultati di un'azione di risposta agli incidenti

È possibile verificare il completamento di un'azione di riparazione utilizzando la scheda **Cronologia** di un incidente.

Per verificare i risultati di un'azione di risposta agli incidenti per un singolo incidente

- 1 Accedere alla console di amministrazione di Enforce Server.
- 2 Fare clic su **Incidenti > Discover**.
Cercare l'icona verde (operazione completata) o rossa (operazione non riuscita) nel report incidente.
- 3 Per informazioni supplementari sui risultati, fare clic su un incidente per visualizzare **Dettagli incidente**.
- 4 Fare clic sulla scheda **Cronologia**.
- 5 Visualizzare i messaggi sulla riparazione dal plug-in. Un messaggio indicante che il plug-in è stato richiamato e un altro che informa della riuscita o meno dell'operazione dovrebbero essere visualizzati. È possibile che siano visualizzati altri messaggi relativi allo stato e al risultato della riparazione.

Per verificare i risultati di un'azione di risposta agli incidenti per un gruppo di incidenti

- 1 Accedere alla console di amministrazione di Enforce Server.
- 2 Fare clic su **Incidenti > Discover**.
- 3 Utilizzare filtri di report e riepiloghi per visualizzare lo stato di protezione o prevenzione degli incidenti.

Vedere ["Visualizzazione degli incidenti"](#) a pagina 1645.

È anche possibile creare report personalizzati per visualizzare lo stato di protezione o prevenzione o i valori degli attributi personalizzati.

Vedere ["Informazioni su report e dashboard personalizzati"](#) a pagina 1646.

Risoluzione dei problemi relativi a un plug-in di FlexResponse server

Tabella 63-4 elenca i problemi relativi a FlexResponse server e i suggerimenti per risolverli.

Tabella 63-4 Suggerimenti per la risoluzione dei problemi

Problema	Suggerimenti
Durante la creazione di una regola di risposta smart, il menu a discesa non visualizza l'azione Tutto: FlexResponse server .	Questa problema si verifica perché il plug-in non è stato caricato. Alla fine del file <code>Plug-ins.properties</code> , immettere il nome del file JAR del plug-in nell'elenco di plug-in. Assicurarsi che questa riga non sia commentata.
Durante la creazione di una regola di risposta automatizzata, il menu a discesa non visualizza l'azione Tutto: FlexResponse server .	Riavviare i servizi Symantec DLP Incident Persister e Symantec DLP Manager per caricare il plug-in.
Se si dispone di molteplici plug-in, il nome di plug-in non viene visualizzato nel menu a discesa Tutto: FlexResponse server .	Il file di proprietà e il codice del plug-in potrebbero non corrispondere. Esaminare gli errori nel registro Tomcat. Il file di registro è <code>localhost.date.log</code> . Questo file di registro si trova in <code>c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs\tomcat (Windows)</code> o <code>/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/tomcat (Linux)</code> . Per verificare che il plug-in sia caricato, cercare l'evento di sistema di Enforce (2122). Questo evento elenca tutti i plug-in caricati.

Problema	Suggerimenti
<p>Il plug-in in uso non viene eseguito correttamente.</p>	<p>Verificare la cronologia dell'istantanea incidente per i messaggi del plug-in e del relativo framework.</p> <p>Per le risposte smart, esaminare gli errori nel registro Tomcat. Questo registro si trova in <code>c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs\tomcat (Windows)</code> o <code>/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/tomcat (Linux)</code>. Il file di registro è <code>localhost.date.log</code>.</p> <p>Per le risposte automatiche, consultare il file di registro di debug in <code>c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\logs\debug\IncidentPersister.log (Windows)</code> o <code>/var/log/Symantec/DataLossPrevention/Enforce Server/15.1/IncidentPersister.log</code>.</p>

Configurazione delle scansioni dell'archiviazione cloud Box utilizzando un server di rilevamento on-site

Il capitolo contiene i seguenti argomenti:

- [Configurazione delle scansioni dei target di archiviazione cloud Box utilizzando un server di rilevazione on-site](#)
- [Configurazione delle scansioni dei target di archiviazione cloud Box](#)
- [Ottimizzazione della scansione dell'archiviazione cloud di Box](#)
- [Configurazione delle opzioni di riparazione per target di archiviazione cloud Box](#)

Configurazione delle scansioni dei target di archiviazione cloud Box utilizzando un server di rilevazione on-site

Per individuare i dati riservati, è possibile eseguire la scansione dei target di archiviazione cloud Box con Cloud Storage Discover. È possibile eseguire la scansione di file e cartelle dell'utente, cartelle di collaborazione e file o cartelle con collegamenti comuni. È possibile

configurare le regole di risposta automatica per mettere in quarantena e/o applicare tag visivi ai file riservati individuati nei target dell'archiviazione cloud Box.

Per configurare la scansione dei target di archiviazione cloud Box, completare la seguente procedura:

Tabella 64-1 Configurazione di una scansione dell'archiviazione cloud Box utilizzando un server di rilevazione on-site

Passaggio	Azione	Descrizione
1	Accedere a Gestisci > Scansione Discover > Target di Discover per creare un nuovo target e configurare la scansione dell'archiviazione cloud Box.	Vedere " Configurazione delle scansioni dei target di archiviazione cloud Box " a pagina 1900.
2	Impostare eventuali altre opzioni di configurazione per la scansione dei target.	Vedere " Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover " a pagina 1830.
3	Per applicare un tag visivo a file riservati, o mettere in quarantena file riservati nel cloud o on-site, configurare Network Protect.	Vedere " Configurazione delle opzioni di riparazione per target di archiviazione cloud Box " a pagina 1904.
4	Avviare la scansione dell'archiviazione cloud Box. Accedere a Gestisci > Scansione Discover > Target di Discover .	Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona di avvio.
5	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere " Informazioni sull'elenco dei target di scansione di Network Discover/Cloud Storage Discover " a pagina 1854.

Configurazione delle scansioni dei target di archiviazione cloud Box

Prima di eseguire una scansione, è necessario configurare un target utilizzando la seguente procedura.

Per configurare un nuovo target per l'archiviazione cloud Box

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su **Nuovo target** e utilizzare il menu a discesa per selezionare il tipo di target **Box (server di rilevamento on-site)**.
- 3 Nella scheda **Generale**, digitare il **Nome** del target Box.
Immettere un nome univoco per il target, con un massimo di 255 caratteri.
- 4 Selezionare **Gruppo di politiche**.
Se nessun altro gruppo di politiche è stato selezionato, viene utilizzato il gruppo di politiche predefinito. Per applicare un gruppo di politiche, selezionare il gruppo di politiche da utilizzare per il target. È possibile assegnare più gruppi di politiche a un target.
È possibile definire i gruppi di politiche nella pagina **Elenco gruppo di politiche**.
- 5 Specificare le opzioni di pianificazione.
Scegliere **Avvia processo di scansione come pianificato** per configurare una pianificazione per la scansione del target specificato. Selezionare un'opzione a partire dall'elenco a discesa di pianificazione per visualizzare ulteriori campi. Selezionare **Sospendi scansione in questo periodo** per sospendere automaticamente le scansioni durante l'intervallo di tempo specificato. È possibile sovrascrivere la finestra di pausa di un target di scansione passando alla schermata Target di Discover e facendo clic sull'icona di avvio per la voce del target. La finestra di pausa rimane intatta e tutte le scansioni future che vengono eseguite in base a tale finestra possono essere interrotte come specificato. È inoltre possibile riavviare una scansione interrotta facendo clic sull'icona Continua relativa alla voce del target.
- 6 Nella scheda **Destinazione**, selezionare il Discover Server (o più Discover Server) in cui si desidera eseguire la scansione.
Se si seleziona più di un server, Symantec Data Loss Prevention seleziona automaticamente uno dei server all'avvio della scansione.
Soltanto i server di rilevamento configurati come Discover Server sono visualizzati nell'elenco. Se è presente solo un Discover Server nella rete, il nome di quel server viene automaticamente specificato. Prima di configurare i target, è necessario configurare i Discover Server. È necessario specificare almeno un server prima di poter eseguire una scansione del target.
- 7 In **Tipo di scansione**, selezionare **Esegui scansione solo di elementi nuovi o modificati (scansione incrementale)**. Questa opzione è il valore predefinito per i nuovi target.
 - Se sono state modificate la politica o altre definizioni in una scansione esistente, è possibile configurare la scansione successiva in modo che sia una scansione completa. Selezionare la seguente opzione:

Esegui scansione di tutti gli elementi alla scansione successiva. Le scansioni successive saranno incrementali.

- Se si desidera eseguire sempre la scansione di tutti gli elementi in questo target, selezionare la seguente opzione:

Esegui sempre scansione di tutti gli elementi (scansione completa)

- 8 Sulla scheda **Autorizzazione**, fare clic su **Autorizza**.

Viene visualizzata la finestra di dialogo **Accedere per concedere l'accesso a Box**.

- 9 Immettere le credenziali di autorizzazione Box per questa scansione. È necessario usare le credenziali con i privilegi di amministratore o co-amministratore Box per il contenuto che si desidera sottoporre a scansione. È inoltre necessario disporre delle autorizzazioni necessarie per scaricare i file da sottoporre a scansione.

- 10 Fare clic su **Concedi** per concedere a Symantec Data Loss Prevention l'accesso agli account di archiviazione cloud Box.

- 11 Fare clic su **OK**.

- 12 Nella scheda **Filtri**, specificare i filtri per **Utenti/gruppi**, **Collaborazione cartelle**, **Collegamenti condivisi**, **Includi ed Escludi tipo file**, **Dimensione del file** e **Data file**.

- **Utenti/gruppi** : selezionare **Esegui scansione di tutti gli elementi** per eseguire la scansione di tutti gli utenti e i gruppi per questo target. Selezionare **Esegui scansione della selezione** per eseguire la scansione solo di utenti e gruppi selezionati. Caricare un file CSV o un file di testo (separati da virgola o da una nuova linea) per gli utenti e i gruppi che si desidera sottoporre a scansione.
- **Collaborazione cartelle** : selezionare un'opzione per eseguire la scansione di cartelle collaborative dall'elenco a discesa in questa sezione:
 - **Esegui scansione di tutti gli elementi** : selezionare questa opzione per sottoporre a scansione tutte le cartelle per questo target.
 - **Esegui scansione solo di cartelle private** : selezionare questa opzione per sottoporre a scansione solo le cartelle private e non collaborative.
 - **Esegui scansione solo di cartelle collaborative (interne o esterne)** : selezionare questa opzione per sottoporre a scansione tutte le cartelle collaborative per questo target.
 - **Esegui scansione solo di cartelle collaborative** : selezionare questa opzione per sottoporre a scansione solo le cartelle collaborative esterne per questo target.
- **Collegamenti condivisi** : selezionare **Esegui scansione solo di collegamenti condivisi** per eseguire una scansione solo su file o cartelle con collegamenti condivisi. È possibile scegliere tra queste opzioni aggiuntive:
 - **Non protetto da password** Selezionare questa opzione per sottoporre a scansione solo file e cartelle con collegamenti condivisi non protetti da password.

- **Senza data di scadenza** : selezionare questa opzione per sottoporre a scansione solo file e cartelle con collegamenti condivisi senza data di scadenza.
 - **Con autorizzazioni di download** : selezionare questa opzione per sottoporre a scansione solo file e cartelle con collegamenti condivisi e autorizzazioni di download.
 - **Tipo file**: immettere l'estensione per i tipi di file che si desidera includere o escludere dalla scansione, ad esempio *.dwg o *.csv.
 - **Filtri dimensioni file** : immettere i limiti di dimensione superiore e inferiore che desidera ignorare nella scansione, in byte, kilobyte o megabyte.
 - **Filtri data file** : immettere un intervallo di date per i file e cartelle aggiunti o modificati che si desidera sottoporre a scansione.
- 13 Nella scheda **Avanzate**, selezionare le opzioni per ottimizzare la scansione.
Vedere ["Ottimizzazione della scansione dell'archiviazione cloud di Box"](#) a pagina 1903.
- 14 Nella scheda **Proteggi**, attivare le opzioni di riparazione di Network Protect per questo target.
Vedere ["Configurazione delle opzioni di riparazione per target di archiviazione cloud Box"](#) a pagina 1904.

Ottimizzazione della scansione dell'archiviazione cloud di Box

Per ottimizzare scansioni del target di archiviazione cloud di Box, è possibile configurare opzioni di limitazione o impostare una soglia di incidenti per la scansione (**Scansione inventario**).

Per limitare un scansione di un target di archiviazione cloud Box

- 1 Accedere alla scheda **Avanzate** della definizione del target.
- 2 Nel campo **Numero massimo di file al minuto** immettere il numero massimo di file da elaborare al minuto.
- 3 Nel campo **Dimensione massima sottoposta a scansione al minuto** immettere la quantità massima di dati da elaborare al minuto. Selezionare i byte, i kilobyte (KB) o i megabyte (MB) dall'elenco a discesa.

Per impostare una soglia di incidenti

- 1 Accedere alla scheda **Avanzate** della definizione del target.
- 2 Nel campo **Soglia incidenti** immettere il numero massimo di incidenti da creare per utente.

Configurazione delle opzioni di riparazione per target di archiviazione cloud Box

È possibile applicare tag visivi come metadati al contenuto riservato memorizzato nel target di archiviazione cloud Box. Il tag visivo aiuta gli utenti dell'archiviazione cloud Box a cercare e riparare autonomamente i dati sensibili. Ad esempio, si potrebbe desiderare che il tag legga "Questo contenuto è considerato confidenziale". È inoltre possibile ricordare loro delle ulteriori funzionalità di sicurezza di Box, come l'aggiunta della protezione con password a qualsiasi collegamento di download.

È inoltre possibile mettere in quarantena il contenuto riservato memorizzato nel target di archiviazione cloud Box. È possibile mettere in quarantena il contenuto riservato in Box o in una condivisione file on-site. È possibile scegliere facoltativamente di lasciare un file marker al posto del contenuto messo in quarantena.

Per riparare gli incidenti di archiviazione cloud Box, è necessario aver configurato una politica e una regola di risposta nella console di amministrazione Enforce Server.

Per configurare la riparazione per l'archiviazione cloud Box

- 1 Creare una politica con una regola di risposta. Accedere a **Gestisci > Politiche > Regole di risposta** e fare clic su **Aggiungi regola di risposta**.
Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.
- 2 Selezionare **Risposta automatica**.
- 3 Fare clic su **Avanti**.
- 4 Per **Azione**, selezionare una o entrambe le seguenti opzioni:
 - **Archiviazione cloud: aggiungi tag visivo**
Il sistema mostra il campo **Aggiungi tag visivo**. Immettere il testo da visualizzare nel tag per gli utenti.
Vedere ["Configurazione dell'azione Archiviazione cloud: aggiungi tag visivo"](#) a pagina 1523.
 - **Archiviazione cloud: quarantena**
Il sistema visualizza il campo **Archiviazione cloud: quarantena**. Se si desidera lasciare un file marker al posto del file messo in quarantena, selezionare **Lascia file marker al posto del file riparato** e immettere il testo per il file marker nella casella **Testo marker**. È inoltre possibile applicare un tag visivo al file marker.
Vedere ["Configurazione dell'azione Archiviazione cloud: quarantena"](#) a pagina 1523.
- 5 Fare clic su **Salva**.
- 6 Aggiungere una nuova politica o modificare una politica esistente.
Vedere ["Configurazione di politiche"](#) a pagina 422.

- 7 Fare clic sulla scheda **Risposta**.
- 8 Nel menu a discesa, selezionare una delle regole di risposta create in precedenza.
- 9 Fare clic su **Aggiungi regola di risposta**.

La regola di risposta selezionata specifica la risposta automatica quando la politica genera un incidente.

Possono esistere diverse regole di risposta con diverse condizioni per una politica.
- 10 Creare una nuovo target Network Discover di archiviazione cloud Box o modificare un target esistente.

Vedere "[Configurazione delle scansioni dei target di archiviazione cloud Box](#)" a pagina 1900.
- 11 Fare clic sulla scheda **Proteggi** nella pagina del target **Box**.
- 12 In **Riparazione protezione consentita**, selezionare **Quarantena** e/o **Attiva tutte le regole di risposta con tag durante la scansione**, come necessario.
- 13 In **Dettagli quarantena**, selezionare una delle seguenti opzioni:
 - **Quarantena nel cloud**

Facoltativo: per mettere in quarantena il contenuto riservato nel cloud, immettere **Utente Box** e **Sottocartella quarantena** nei campi appropriati. L'account **Utente Box** può essere l'account di scansione o un account di utente non amministrativo.

Se viene selezionato **Quarantena nel cloud** e lasciati tali campi vuoti, Symantec Data Loss Prevention utilizza l'account di scansione come account di quarantena.

Specificare una sottocartella nell'account di quarantena Box immettendola nel campo **Sottocartella quarantena**.
 - **Quarantena on-site**

Per mettere in quarantena il contenuto riservato su una condivisione file on-site, immettere il percorso e le credenziali utente per la condivisione file.
- 14 Fare clic su **Salva**.

Impostazione di scansioni di condivisioni file

Il capitolo contiene i seguenti argomenti:

- [Impostazione delle scansioni di file system](#)
- [Target del file system supportati](#)
- [Rilevamento automatico di server e condivisioni prima di configurare un target File system](#)
- [Rilevamento automatico di condivisioni file aperte](#)
- [Informazioni sul rilevamento automatico dello stato di riparazione incidente](#)
- [Esclusione delle cartelle DFS interne](#)
- [Configurazione delle scansioni delle cartelle personali di Microsoft Outlook \(file .pst\)](#)
- [Configurazione delle scansioni del file system](#)
- [Ottimizzazione della scansione del target del file system](#)
- [Configurazione di Network Protect per condivisioni file](#)

Impostazione delle scansioni di file system

Network Discover esegue la scansione dei server di file in rete e le risorse condivise ("condivisioni") quali le unità disco o le directory per rilevare dati confidenziali. Network Discover supporta i file server conformi a CIFS e le condivisioni file che utilizzano CIFS, NFS, DFS o qualunque altro client. Network Discover può inoltre eseguire la scansione delle cartelle personali di Microsoft Outlook (file .pst) su condivisioni di file in rete.

Per configurare la scansione dei file system, completare i seguenti processi:

Tabella 65-1 Impostazione di una scansione del file system in rete

Passaggio	Azione	Descrizione
1	Verificare che il file system in rete si trovi nell'elenco dei target supportati.	Vedere "Target del file system supportati" a pagina 1907.
2	Facoltativo: eseguire una scansione Enumerazione radici contenuti per rilevare automaticamente le root di contenuto del file system all'interno del dominio.	Vedere "Rilevamento automatico di server e condivisioni prima di configurare un target File system" a pagina 1908.
3	Accedere a Gestisci > Scansione Discover > Target di Discover per creare un nuovo target per il file system e per configurare la scansione del file system.	Vedere "Configurazione delle scansioni del file system" a pagina 1922.
4	Impostare eventuali altre opzioni di configurazione per la scansione dei target. Per la scansione delle cartelle personali di Microsoft Outlook, verificare che l'opzione sia impostata.	Vedere "Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover" a pagina 1830. Vedere "Configurazione delle scansioni delle cartelle personali di Microsoft Outlook (file .pst)" a pagina 1921.
5	Per spostare, mettere in quarantena o crittografare automaticamente i file, configurare Network Protect. Nota: La funzionalità di crittografia è disponibile solo dopo aver configurato Enforce Server per connettersi a Symantec ICE.	Vedere "Configurazione di Network Protect per condivisioni file" a pagina 1928.
6	Avviare la scansione del file system. Accedere a Gestisci > Scansione Discover > Target di Discover .	Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.
7	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Informazioni sull'elenco dei target di scansione di Network Discover/Cloud Storage Discover" a pagina 1854.

Target del file system supportati

Il target del file system supporta la scansione dei seguenti file system di rete.

File server supportati:

- Solo server CIFS

Condivisioni file supportate:

- CIFS su Windows Server 2008 R2, 2012, 2012 R2 e 2016
- NFS su Red Hat Enterprise Linux 6.x, e 7.x
- Scansione DFS su Windows 2008 R2, 2012, 2012 R2 e 2016.

Nota: DFS non è supportato con Network Protect.

Inoltre, il target del file system supporta la scansione dei seguenti tipi di file:

- Cartelle personali di Microsoft Outlook (file .pst) create con Outlook 2007, 2010, 2013 e 2016.

Nota: Outlook 2007 è obsoleto in Symantec Data Loss Prevention 15.1.

Il server Network Discover che esegue la scansione di questo target deve avere un sistema operativo Windows e Outlook 2007 o versione successiva deve essere installato nel sistema. Vedere "[Configurazione delle scansioni delle cartelle personali di Microsoft Outlook \(file .pst\)](#)" a pagina 1921.

- File system sui sistemi Unix, anche se non sono mostrati come condivisioni NFS o CIFS. Utilizzare il protocollo SFTP per fornire un metodo simile alle scansioni delle condivisioni di file.
È inoltre possibile eseguire la scansione del file system locale su un server Network Discover Linux elencandone il nome del percorso nella radice del contenuto. Ad esempio, è possibile immettere `/home/myfiles`.

Rilevamento automatico di server e condivisioni prima di configurare un target File system

Il rilevamento automatico di server e condivisioni (Enumerazione radici contenuti) consente di individuare server e condivisioni in un dominio e di filtrarli in base all'intervallo IP o al nome server. La scoperta delle condivisioni funziona solo per i file server conformi a CIFS, inclusi quelli con condivisioni file DFS. Le scansioni Enumerazione radici contenuti producono un elenco dei server e delle parti utilizzabili direttamente nei target File system per la Scansione Discover o per l'esportazione in un file CSV. Una scansione Enumerazione radici contenuti non esplora il contenuto dei server e delle condivisioni che rileva, ma consente di trovare i server e le condivisioni nel dominio e di configurarne la scansione automatizzata.

Le scansioni Enumerazione radici contenuti richiedono un collegamento al server di directory LDAP. Inoltre Enforce Server deve avere accesso a tutti i server e alle condivisioni che si desidera sottoporre a scansione.

Vedere ["Configurazione delle connessioni a server di directory"](#) a pagina 162.

Vedere ["Configurazione delle scansioni del file system"](#) a pagina 1922.

Utilizzo delle scansioni di enumerazione di radici di contenuti

Per creare, avviare e interrompere le scansioni di enumerazione di radici di contenuti e visualizzare le radici di contenuti rilevate, seguire le procedure descritte.

Per creare una scansione di enumerazione di radici di contenuti

- 1 Configurare la connessione del server di directory LDAP. Assicurarsi che le credenziali della directory includano i privilegi di lettura ed elenco per tutti gli oggetti del computer che si desidera sottoporre a scansione.
Vedere ["Configurazione delle connessioni a server di directory"](#) a pagina 162.
- 2 Nella console di amministrazione di Enforce Server selezionare **Gestisci > Scansione Discover > Enumerazione radici contenuti**.
- 3 Fare clic su **Aggiungi scansione**. Viene visualizzata la pagina **Configurazione scansione di enumerazione radici contenuto**.
- 4 Nella sezione **Generale** immettere un nome per la scansione nel campo **Nome**.
- 5 Selezionare una connessione alla directory.
- 6 Specificare la preferenza **Enumerare le condivisioni?** :
 - Per elencare i server e le condivisioni di file, fare clic su **Si**.
 - Per elencare solo i server, fare clic su **No, solo i server**.
- 7 Nella sezione **Filtri** selezionare almeno un filtro per la scansione:
 - **Intervallo IP** : specificare un intervallo IP per la scansione di radici di contenuti.
 - **Nomi server** : specificare uno o più filtri per i nomi dei server. Per affinare il filtro, utilizzare il menu a discesa.
- 8 Fare clic su **Salva**.

Per avviare o interrompere una scansione di enumerazione di radici di contenuti

- 1 Nella console di amministrazione di Enforce Server selezionare **Gestisci > Scansione Discover > Enumerazione radici contenuti**.
- 2 Selezionare le scansioni da avviare o interrompere.
- 3 Effettuare una delle seguenti operazioni:
 - Per avviare una ricerca, fare clic su **Avvia**.
 - Per interrompere una scansione in corso, fare clic su **Interrompi**.

Per visualizzare le radici di contenuti rilevate

- 1 Nella console di amministrazione di Enforce Server selezionare **Gestisci > Scansione Discover > Enumerazione radici contenuti**.
- 2 Fare clic sul collegamento nella colonna **Radici di contenuti** della scansione desiderata per visualizzare un elenco delle radici di contenuti.
- 3 Per esportare l'elenco delle radici di contenuti in formato `.csv`, fare clic su **Esporta in CSV** nella finestra di dialogo **Radici di contenuti**.

È possibile utilizzare il file `.csv` esportato per inserire le informazioni in un target del file system Discover.

Vedere ["Configurazione delle scansioni del file system"](#) a pagina 1922.

Opzioni di configurazione per le scansioni di enumerazione radici contenuto

È possibile trovare le opzioni di configurazione per le scansioni di enumerazione radici contenuto nel file `Manager.properties` nella directory di configurazione:

`\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (piattaforme Microsoft Windows) o `opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/config` (piattaforme Linux). Queste impostazioni predefinite danno risultati ottimali nella maggior parte dei casi.

Tabella 65-2

Proprietà di configurazione	Valore predefinito	Descrizione
content_root_enumeration.scanResultThreshold	10000	Numero massimo delle radici contenuto rilevabili in una scansione di enumerazione radici contenuto. Se il numero delle radici contenuto nella scansione supera la soglia di risultati, Symantec Data Loss Prevention visualizza un errore. Tale soglia impedisce alle scansioni di enumerazione radici contenuto di restituire un numero eccessivo di radici contenuto da utilizzare in un target Discover File System.

Proprietà di configurazione	Valore predefinito	Descrizione
<code>content_root_enumeration.maximumParallelScanCount</code>	5	Numero massimo di scansioni di enumerazione radici contenuto che Symantec Data Loss Prevention può eseguire in parallelo. Se viene raggiunto il numero massimo di scansioni eseguibili in parallelo, le rimanenti scansioni vengono inserite in coda.
<code>content_root_enumeration.scan_log.location</code>	Windows: <code>c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs</code> Linux: <code>/var/logs/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/</code>	Posizione dei file registro dettagli della scansione di enumerazione radici contenuto.
<code>content_root_enumeration.scan_log.limit</code>	5000000	Dimensione massima in byte di ogni file registro dettagli della scansione.

Proprietà di configurazione	Valore predefinito	Descrizione
<code>content_root_enumeration.scan_log.count</code>	15	Numero massimo di file registro dettagli della scansione in uso in qualsiasi momento.
<code>content_root_enumeration.scan_log.append</code>	true	Valore booleano che specifica se Symantec Data Loss Prevention aggiunge i risultati del registro alla fine di ciascun file registro dettagli della scansione.
<code>content_root_enumeration.scan_log.encoding</code>	UTF-8	Set di caratteri utilizzato da Symantec Data Loss Prevention per creare il file di registro dettagli della scansione.

Risoluzione dei problemi relativi alle scansioni di enumerazione di radici di contenuti

È possibile visualizzare sia gli avvisi di scansione sia i file di registro per le scansioni di enumerazione di radici di contenuti. Gli avvisi e i registri possono essere utili per la risoluzione dei problemi relativi alle scansioni di enumerazione di radici di contenuti.

Gli avvisi relativi alle scansioni di enumerazioni di radici di contenuti sono errori che non riguardano il terminale, ad esempio timeout di connessione o problemi DNS, e che si verificano durante la scansione. Se tali errori si verificano durante una scansione di enumerazione di

radici di contenuti, viene visualizzato un collegamento nella colonna **Avvisi** nella pagina **Gestisci > Scansione Discover > Enumerazione radici contenuti** per la scansione. Per visualizzare questi avvisi, seguire la procedura descritta:

Per visualizzare gli avvisi relativi alla scansione di enumerazione di radici di contenuti

- 1 Nella console di amministrazione di Enforce Server selezionare **Gestisci > Scansione Discover > Enumerazione radici contenuti**.
- 2 Fare clic sul collegamento nella colonna **Avvisi** per gli avvisi di scansione che si desidera visualizzare. Viene visualizzata la finestra di dialogo **Avvisi di scansione**.
- 3 Per esportare l'elenco degli avvisi di scansione in un file .csv, fare clic su **Esporta in CSV** nella finestra di dialogo **Avvisi di scansione**.

I file di registro sono disponibili nella directory dei registri: c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs nelle piattaforme Microsoft Windows e /var/logs/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/ nelle piattaforme Linux. I registri dell'enumerazione di radici di contenuti sono denominati secondo questo formato: ContentRootEnumerationScanDetail-*nome scansione*0.log. I file di registro dell'enumerazione di radici di contenuti elencano ogni radice contenuto rilevata, nonché tutti gli avvisi e gli errori che si verificano durante la scansione.

Rilevamento automatico di condivisioni file aperte

Symantec Data Loss Prevention può rilevare automaticamente le condivisioni aperte su un server CIFS specificato. Specificare il percorso UNC o l'URL SMB: Symantec Data Loss Prevention trova ed esegue automaticamente la scansione delle condivisioni di file aperte su tale server.

Vedere ["Per configurare un nuovo target del file system"](#) a pagina 1922.

È possibile scoprire automaticamente condivisioni amministrative che corrispondono a unità logiche, quali C\$ o D\$.

Per scoprire automaticamente le condivisioni amministrative

- 1 Nella console di amministrazione di Enforce Server selezionare **Gestisci > Scansione Discover > Target di Discover**.
- 2 Creare o selezionare una destinazione File System Server.
- 3 Nella scheda **Avanzate** della pagina **Modifica file system destinazione**, selezionare **Esegui scansione di condivisioni amministrative**.

Informazioni sul rilevamento automatico dello stato di riparazione incidente

È possibile configurare Network Discover per seguire automaticamente lo stato di riparazione degli incidenti di target di file system.

Durante la prima scansione Network Discover per un target di file system dato, i metadati dell'incidente (nome risorsa, politiche violate e così via) vengono aggiunti al catalogo di monitoraggio della riparazione incidenti di Discover. Se durante una successiva scansione un incidente archiviato nel catalogo non appare nei risultati di scansione, Network Discover contrassegna l'incidente come riparato con uno dei seguenti indicatori di stato:

- **Elemento modificato.** L'elemento è stato modificato e non viola più una politica. Se sia l'elemento che la politica sono stati modificati, l'incidente viene contrassegnato come riparato con lo stato **Elemento modificato**. Questa opzione è disattivata per impostazione predefinita.
- **Politica modificata.** La politica violata dall'incidente è stata modificata. Se sia l'elemento che la politica sono stati modificati, l'incidente viene contrassegnato come riparato con lo stato **Elemento modificato**. Questa opzione è disattivata per impostazione predefinita.
- **L'elemento non esiste più.** L'elemento è stato spostato, eliminato o rinominato. Questa opzione è attivata per impostazione predefinita.

Per impedire la riparazione automatica accidentale ed errata degli incidenti, Network Discover non contrassegna come riparato un incidente se l'incidente è escluso da una scansione a causa di:

- Scansione incrementale
- Filtraggio in base alla data
- Filtraggio in base alla dimensione
- Filtri di inclusione o esclusione

Il catalogo di riparazione incidenti è incluso in un database Apache Derby eseguito sotto il processo `BoxMonitor`. Il catalogo master è archiviato in Enforce Server e ciascun server di rilevamento dispone di una versione locale del catalogo stesso. I cataloghi sono sincronizzati per garantire che Enforce Server e tutti i server di rilevamento Network Discover rilevino correttamente lo stato di riparazione degli incidenti.

È possibile impostare le preferenze per il rilevamento dello stato di riparazione degli incidenti nella scheda Avanzate del target di file system.

Vedere ["Configurazione delle scansioni del file system"](#) a pagina 1922.

È possibile configurare opzioni per la riparazione automatizzata di incidenti, quali la posizione dei file di catalogo, la scadenza dei file temporanei e così via.

Vedere ["Opzioni di configurazione per il rilevamento automatico della risoluzione degli incidenti"](#) a pagina 1917.

È possibile visualizzare lo stato di riparazione più recente di un incidente nell'istantanea incidente.

Vedere ["Istantanea incidente di Discover"](#) a pagina 1615.

È anche possibile filtrare e riepilogare i report Network Discover in base allo stato di riparazione degli incidenti.

Vedere ["Informazioni sui filtri e sulle opzioni di riepilogo per i report "](#) a pagina 1677.

Risoluzione dei problemi di rilevamento della riparazione automatizzata degli incidenti

Il rilevamento della riparazione automatizzata degli incidenti non funziona se è stato attivato un sistema di soglie incidenti. Se il rilevamento della riparazione automatizzata degli incidenti è stato attivato per un file system target ma non appaiono le informazioni di rilevamento, verificare di avere disattivato le soglie di incidenti.

Vedere ["Creazione di un inventario delle posizioni di dati riservati non protetti"](#) a pagina 1849.

È possibile visualizzare un file di log per il catalogo di riparazione degli incidenti sul server di rilevamento nei seguenti percorsi:

- **Windows:** `c:\ProgramData\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\logs\debug\DetectionServerDatabase%g`
- **Linux:** `var/log/Symantec/DataLossPrevention/Enforce Server/15.1/debug/DetectionServerDatabase%g`

In entrambi i casi, %g è un numero intero che inizia da 0. I log degli incidenti rilevati con questa funzionalità sono inviati a `FileReader%.log` e `IncidentPersister%.log`.

È possibile impostare il livello di registrazione del catalogo di riparazione degli incidenti nel file `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\config\DetectionServerDatabaseLogging.properties` (Windows) o `opt/Symantec/DataLossPrevention/Enforce Server/15.1/config/DetectionServerDatabaseLogging.properties` (Linux):

Tabella 65-3 Opzioni di registrazione nel database di rilevamento delle riparazioni

Livello registro	Descrizione
POCO RILEV.	Gli heartbeat del database del server di rilevazione vengono registrati con il livello POCO RILEV.

Livello registro	Descrizione
INFO	I messaggi di avvio e arresto del database vengono registrati con il livello INFO.
GRAVE	Tutti i funzionamenti imprevisti del database generano un'eccezione e appaiono nel registro al livello GRAVE.

Opzioni di configurazione per il rilevamento automatico della risoluzione degli incidenti

È possibile impostare le opzioni di configurazione seguenti per il rilevamento automatico della risoluzione degli incidenti nel file `c:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\config\protect.properties` (Windows) o `opt/Symantec/DataLossPrevention/Enforce Server/15.1/config/protect.properties` (Linux). Se si dispone di un'installazione multi-tier, vi sono file separati per Enforce Server e Network Discover Server.

Tabella 65-4

Proprietà	Valore predefinito	Descrizione
<code>com.vontu.discover.detectionserver.remediation.detection.comm.maxfiles</code>	15000	È il numero massimo di file archiviati nella directory del catalogo per il rilevamento della risoluzione di Network Discover Server prima della sincronizzazione con il catalogo master su Enforce Server. Se il numero di file di catalogo supera questo limite, Network Discover non crea nuove voci di catalogo fino a quando non è sincronizzato almeno un file.

Proprietà	Valore predefinito	Descrizione
com.vontu.discover.enforce. remediation.detection. comm.maxfiles	15000	È il numero massimo di file archiviati nella directory del catalogo per il rilevamento della risoluzione di Enforce Server prima della sincronizzazione con il catalogo locale su Network Discover Server. Se il numero di file di catalogo supera questo limite, Network Discover non crea nuove voci del catalogo master fino a quando non è sincronizzato almeno un file.
com.vontu.discover.detectionserver. remediation.detection. catalogfolder.checkperiod	10000	È la frequenza, in millisecondi, con cui Network Discover Server controlla la directory del catalogo per il rilevamento della risoluzione per il numero di file di catalogo in coda per la sincronizzazione con il catalogo master su Enforce Server.
com.vontu.discover.enforce. remediation.detection. catalogfolder.checkperiod	10000	È la frequenza, in millisecondi, con cui Enforce Server controlla la directory del catalogo master per il rilevamento della risoluzione per il numero di file di catalogo in coda per la sincronizzazione con il catalogo su Network Discover Server.

Proprietà	Valore predefinito	Descrizione
com.vontu.discover.detectionserver. remediation.detection. catalog.tempfile.expirationhours	24	È il periodo di scadenza, in ore, dei file temporanei nella directory del catalogo per il rilevamento della risoluzione.
com.vontu.discover.enforce. remediation.detection. catalog.tempfile.expirationhours	24	È il periodo di scadenza, in ore, dei file temporanei nella directory del catalogo master per il rilevamento della risoluzione.
com.vontu.discover.detectionserver. remediation.detection. catalog.folder	C:\Programmi\Symantec\Data Loss Prevention\Detection Server\15.1\Protect\scan\catalog (Windows) /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/scan (Linux)	È la directory che contiene i file del catalogo per il rilevamento della risoluzione di Network Discover Server.
com.vontu.discover.enforce. remediation.detection. catalog.folder	C:\Programmi\Symantec\Data Loss Prevention\Detection Server\15.1\Protect\scan\catalog (Windows) /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/scan (Linux)	È la directory che contiene i file del catalogo master per il rilevamento della risoluzione di Enforce Server.
com.vontu.discover.detectionserver. remediation.detection. threadpoolsize	5	È la dimensione del pool di thread utilizzato per il rilevamento automatico della risoluzione degli incidenti su Network Discover Server.

Proprietà	Valore predefinito	Descrizione
com.vontu.discover.enforce. remediation.detection. threadpoolsize	5	È la dimensione del pool di thread utilizzato per il rilevamento automatico della risoluzione degli incidenti su Enforce Server.
com.vontu.detectionserver. database.home	C:\Programmi\Symantec\Data Loss Prevention\Detection Server\15.1\Protect\scan\catalog (Windows) /opt/Symantec/DataLossPrevention/Detection Server/15.1/Protect/scan (Linux)	È la directory che contiene il database di rilevamento della risoluzione di Network Discover Server.
com.vontu.detectionserver. database.port	1527	È la porta utilizzata dal database di rilevamento della risoluzione di Network Discover Server.
com.vontu.manager.incidents.dir	\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\incidents (Windows) /opt/Symantec/DataLossPrevention/Enforce Server/15.1/Protect/incidents (Linux)	È la directory che contiene gli incidenti non in linea su Enforce Server.

Esclusione delle cartelle DFS interne

Per impostazione predefinita, le scansioni della condivisione file DFS includono le cartelle DFS interne dinamiche. Poiché queste cartelle non contengono dati riservati dell'organizzazione è possibile escluderle senza problemi dalle ricerche.

Per escludere le cartelle interne DFS

- 1 Nella console di amministrazione di Enforce Server selezionare **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic sul nome della ricerca alla quale si desidera aggiungere il filtro di esclusione per le cartelle interne DFS.

- 3 Fare clic sulla scheda **Contenuto sottoposto a scansione**.
- 4 Nel campo **Filtri di esclusione** digitare `/DfsrPrivate/*`.
- 5 Fare clic su **Salva**.

Configurazione delle scansioni delle cartelle personali di Microsoft Outlook (file .pst)

È possibile eseguire la scansione delle cartelle personali di Microsoft Outlook (file .pst) su condivisioni di file. La scansione supporta le cartelle personali di Microsoft Outlook (file .pst) create con Outlook 2007, 2010, 2013 e 2016.

Vedere ["Configurazione delle scansioni del file system"](#) a pagina 1922.

Le seguenti note riguardano la scansione di file .pst:

- Il server Network Discover che esegue la scansione di questo target deve avere un sistema operativo Windows a 64 bit e dei client Outlook 2007, 2010, 2013 o 2016 a 64 bit installati.
- Outlook deve essere il client di posta predefinito nel server Network Discover utilizzato per la scansione.
- Network Protect non è supportato per i file .pst, anche se i file si trovano su condivisioni CIFS.
- Dopo la scansione di base iniziale, la scansione incrementale esamina l'intero file .pst se la data dell'ultima modifica cambia.
- Il filtro di data e il filtro di dimensione sono applicati all'intero file .pst e non alle singole e-mail o ad altri elementi all'interno del file.
- Non è possibile eseguire la scansione parallela dei file .pst. Se le scansioni eseguite in parallelo iniziano la scansione dei file .pst, le scansioni vengono serializzate.

Per configurare la scansione delle cartelle personali di Microsoft Outlook

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Configurare la scansione della condivisione di file contenente le cartelle personali di Microsoft Outlook.

Vedere ["Configurazione delle scansioni del file system"](#) a pagina 1922.

- 3 Nella scheda **Avanzate**, selezionare la casella **Esegui scansione di file PST** (per impostazione predefinita, la casella è selezionata).

Configurazione delle scansioni del file system

Prima di eseguire una scansione, è necessario configurare un target utilizzando la seguente procedura.

Per configurare un nuovo target del file system

- 1 Nella console di amministrazione di Enforce Server accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su **Nuovo target** e utilizzare il menu a discesa per selezionare il tipo di target specifico.
- 3 Nella scheda **Generale**, digitare il **Nome** del target Discover.
Digitare un nome univoco per il target, con un massimo di 255 caratteri.
- 4 Selezionare **Gruppo di politiche**.
Se nessun altro gruppo di politiche è stato selezionato, viene utilizzato il gruppo di politiche predefinito. Per applicare un gruppo di politiche, selezionare il gruppo di politiche da utilizzare per il target. È possibile assegnare più gruppi di politiche a un target.
È possibile definire i gruppi di politiche nella pagina **Elenco gruppo di politiche**.
- 5 In **Esecuzione scansione**, selezionare **Esegui scansione solo di elementi nuovi o modificati (scansione incrementale)**. Questa opzione è il valore predefinito per i nuovi target.
 - Se sono state modificate la politica o altre definizioni in una scansione esistente, è possibile configurare la scansione successiva in modo che sia una scansione completa. Selezionare la seguente opzione:
Esegui scansione di tutti gli elementi alla scansione successiva. Le scansioni successive saranno incrementali.
 - Se si desidera eseguire sempre la scansione di tutti gli elementi in questo target, selezionare la seguente opzione:
Esegui sempre scansione di tutti gli elementi (scansione completa)
- 6 Facoltativamente, se è stata selezionata l'opzione **Esegui scansione solo di elementi nuovi o modificati (scansione incrementale)**, è possibile selezionare uno o più target di scansione esistenti i cui indici incrementali verranno riutilizzati nella nuova scansione. Il riutilizzo degli indici incrementali consente di risparmiare tempo di indicizzazione degli elementi sottoposti a scansione nel nuovo target di scansione.
 - Per riutilizzare gli indici incrementali esistenti, selezionare il target di scansione desiderato nell'elenco **Destinazioni di Discover disponibili** e fare clic su **Aggiungi >>**. Il target di scansione selezionato passa nell'elenco **Destinazioni di Discover selezionate** e il relativo indice incrementale diventa disponibile per il nuovo target di scansione quando nel nuovo target viene eseguita la scansione per la prima volta.

- Per smettere di riutilizzare l'indice incrementale esistente, selezionare il target di scansione desiderato nell'elenco **Destinazioni di Discover selezionate** e fare clic su << **Rimuovi**. Il target di scansione selezionato torna nell'elenco **Destinazioni di Discover disponibili** e il relativo indice incrementale non è più disponibile per il nuovo target di scansione.

Nota: È possibile aggiungere e rimuovere gli indici incrementali riutilizzabili solo mentre si configura un nuovo target di scansione e prima di eseguire per la prima volta la scansione in questo target.

7 Specificare le opzioni di pianificazione.

Scegliere **Avvia processo di scansione come pianificato** per configurare una pianificazione per la scansione del target specificato. Selezionare un'opzione a partire dall'elenco a discesa di pianificazione per visualizzare ulteriori campi. Selezionare **Sospendi scansione in questo periodo** per sospendere automaticamente le scansioni durante l'intervallo di tempo specificato. È possibile sovrascrivere la finestra di pausa di un target di scansione passando alla schermata Target di Discover e facendo clic sull'icona di avvio per la voce del target. La finestra di pausa rimane intatta e tutte le scansioni future che vengono eseguite in base a tale finestra possono essere interrotte come specificato. È inoltre possibile riavviare una scansione interrotta facendo clic sull'icona Continua relativa alla voce del target.

8 Nella scheda **Destinazione**, in **Server di scansione ed endpoint di destinazione**, selezionare il Discover Server (o più Discover Server) in cui si desidera eseguire la scansione.

Soltanto i server di rilevamento configurati come Discover Server sono visualizzati nell'elenco. Se è presente solo un Discover Server nella rete, il nome di quel server viene automaticamente specificato. Prima di configurare i target, è necessario configurare i Discover Server. È necessario specificare almeno un server prima di poter eseguire una scansione del target.

9 Per l'opzione **Modalità di scansione**, selezionare una delle opzioni seguenti:

- Selezionare **Utilizza server singolo per la scansione** per eseguire le scansioni utilizzando solo un server. Se nel passaggio precedente è stato selezionato più di un server, Symantec Data Loss Prevention seleziona automaticamente uno dei server all'avvio della scansione.
- Selezionare **Utilizza tutti i server selezionati per la scansione in una griglia** per attivare la funzionalità di scansione della griglia che distribuisce il carico di lavoro della scansione su più server. Quando si inizializza una scansione, a uno dei server è assegnato il ruolo di Elemento principale griglia che coordina le azioni degli altri server.

Nota: È necessario selezionare almeno due server affinché il target della scansione possa eseguire una scansione della griglia. Symantec consiglia di applicare la stessa configurazione hardware e software a tutti i server di rilevamento che si intende utilizzare per le scansioni della griglia. Prima di eseguire per la prima volta una scansione della griglia, assicurarsi che la porta di comunicazione della griglia configurata nel file `ScanManager.properties` sia aperta su tutti i server nella griglia.

Vedere ["Configurazione della scansione della griglia"](#) a pagina 1876.

10 Nella scheda **Contenuto sottoposto a scansione**, selezionare o immettere le credenziali.

Le credenziali che si forniscono devono disporre sia dell'autorizzazione di lettura sia di quella di scrittura attribuiti nel target di scansione. L'autorizzazione di scrittura attribuiti è necessaria per aggiornare la data di ultimo accesso.

È possibile specificare un nome utente predefinito da usare per accedere a tutti i file system.

La password non deve contenere il carattere virgolette. Se le password contengono un carattere virgolette, tali file system non vengono montati per la scansione.

Se è necessario utilizzare i caratteri virgolette nelle password, è possibile usare JCIFS. Il processo di montaggio predefinito utilizza il client CIFS. Se il montaggio predefinito non funziona, l'attività di montaggio può utilizzare il client CIFS basato su Java impostando `filesystemcrawler.use.jcifs=true` nel file delle proprietà `Crawler.properties`.

11 In **Radici di contenuti**, immettere l'elemento da sottoporre a scansione.

Selezionare uno dei metodi seguenti di immissione dei file system:

■ **Esegui scansione delle radici di contenuti da un file caricato**

Creare e salvare un file di testo (`.txt` o `.csv`) che elenca i server che si desidera sottoporre a scansione. Quindi fare clic su **Sfoglia** per individuare l'elenco e su **Carica file** per importarlo. Creare un file utilizzando un editor di testo ASCII e digitare un file server o condividere in base alla riga. Non includere nome utente e password. Per impostazione predefinita, Symantec Data Loss Prevention li interpreta come percorsi Server Message Block (SMB). Se si desidera specificare i percorsi NFS, includere `nfs` nei percorsi.

```
\\server\marketing  
nfs:\\share\marketing  
//server/engineering/documentation  
/home/protect/mnt/server/share/marketing  
c:\share\engineering
```

■ **Specifica radici di contenuti**

- Selezionare **Aggiungi radici di contenuti > Per immissione diretta** per utilizzare un editor di riga per specificare i server o le condivisioni da sottoporre a scansione. Le informazioni immesse qui hanno la precedenza sui valori predefiniti e si applicano solo al percorso specificato.

```
\\server\share  
\\server.company.com  
smb://server.company.com  
\\10.66.23.34
```

Nota: Se si sceglie di attivare la scansione incrementale per questo target di scansione e se è stato selezionato uno o più target di scansione esistenti i cui indici incrementali verranno riutilizzati, è possibile unire i target di scansione esistenti specificando un percorso di directory di livello più elevato. In alternativa, è possibile specificare un percorso di directory più granulare per dividere un target di scansione esistente più grande in vari target di scansione più piccoli.

- Selezionare **Aggiungi radici di contenuti > Da una scansione di enumerazione radici contenuti** per importare le radici di contenuti da una scansione di enumerazione radici contenuti. Seleziona la scansione da importare nella finestra di dialogo **Importa risultati scansione di enumerazione radici contenuti**.

Se l'elenco delle radici di contenuti include molti elementi, è possibile filtrarlo in modo da includere solo le radici di contenuti pertinenti alla scansione della destinazione di Discover. Nella sezione **Radici di contenuti**, fare clic su **Filtri**, quindi digitare il testo del filtro. Ad esempio, per visualizzare solo le parti su un server denominato `my_company`, immettere `\\my_company` nel campo di testo **Filtri**.

Per eliminare le radici dei contenuti dal target, selezionare le radici dei contenuti dall'elenco e fare clic su **Elimina**.

12 Nella scheda **Filtri**, specificare i filtri di inclusione, di esclusione, di dimensione e di data.

- Utilizzare i **Filtri di inclusione** e i **Filtri di esclusione** per specificare i file che Symantec Data Loss Prevention deve elaborare o ignorare. È necessario specificare i percorsi assoluti. Se si lascia vuoto il campo, Symantec Data Loss Prevention ricerca la corrispondenza in tutti i file nella condivisione file. Se si immette un qualsiasi valore nel campo **Filtri di inclusione**, Symantec Data Loss Prevention sottopone a scansione solo i file e i documenti corrispondenti al filtro specificato. Delimitare le voci mediante virgole, ma senza utilizzare spazi. Quando vengono utilizzati sia i **Filtri di inclusione** sia i **Filtri di esclusione**, i **Filtri di esclusione** hanno la precedenza.

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

Durante la scansione delle condivisioni DFS, escludere la cartella DFS interna.

Vedere ["Esclusione delle cartelle DFS interne"](#) a pagina 1920.

Durante la scansione di condivisioni su un filer NetApp con l'applicazione Snapshot, escludere la cartella `.snapshot`. Questa cartella è solitamente alla base del file system o della condivisione di rete, ad esempio `\\myshare\.snapshot`.

- Specificare i filtri di dimensione.
 I filtri di dimensione consentono di escludere file dal processo di corrispondenza in base alla loro dimensione. Symantec Data Loss Prevention include solo i file che corrispondono ai filtri di dimensione specificati. Se si lasciano vuoti questi campi, Symantec Data Loss Prevention ricerca la corrispondenza per file o documenti di tutte le dimensioni.
- Specificare filtri di data.
 I filtri di data consentono di includere file dal processo di corrispondenza in base alle loro date. Vengono sottoposti a scansione tutti i file che corrispondono ai filtri di data specificati.

13 Nella scheda **Avanzate**, specificare le preferenze di rilevamento riparazione per rilevare automaticamente lo stato di riparazione dell'incidente:

- **Elemento modificato** : consente di rilevare automaticamente se un incidente è stato riparato tramite la modifica del file pericoloso.
- **Politica modificata** : rileva automaticamente se un incidente è stato riparato tramite una modifica della politica.
- **L'elemento non esiste più** : consente di individuare automaticamente se un incidente è stato riparato tramite eliminazione o rimozione.

Vedere ["Informazioni sul rilevamento automatico dello stato di riparazione incidente"](#) a pagina 1915.

14 Nella scheda **Avanzate**, selezionare le opzioni per ottimizzare la scansione.

Vedere ["Ottimizzazione della scansione del target del file system"](#) a pagina 1926.

15 Nella scheda **Proteggi**, specificare le preferenze di riparazione per i file che contengono informazioni riservate.

Vedere ["Configurazione di Network Protect per condivisioni file"](#) a pagina 1928.

Ottimizzazione della scansione del target del file system

Per ottimizzare la scansioni del target di scansione del **file system**, è possibile configurare le opzioni di limitazione, impostare una soglia di incidenti per la scansione (**Scansione inventario**), omettere o selezionare i file `.pst` di Outlook e attivare o disattivare le scansioni delle condivisioni amministrative.

Per limitare una scansione del target del file system

- 1 Accedere alla scheda **Avanzate** della definizione del target.
- 2 Nel campo **Numero massimo di file analizzati al minuto per server di rilevamento**, digitare il numero massimo di file da elaborare al minuto per server di rilevamento.
- 3 Nel campo **Dimensione massima analizzata al minuto per server di rilevamento**, digitare la quantità massima di dati da elaborare al minuto per server di rilevamento. Selezionare i byte, i kilobyte (KB) o i megabyte (MB) dall'elenco a discesa.

Per impostare una soglia di incidenti

- 1 Accedere alla scheda **Avanzate** della definizione del target.
- 2 Nel campo **Soglia incidenti** immettere il numero massimo di incidenti da creare da una singola condivisione di file (**Radice di contenuti**) o server (**Computer**).
- 3 Selezionare **Conteggia incidenti per: Radice di contenuti o Computer**.

Radice di contenuti è una condivisione di file nell'elenco della scheda Contenuto sottoposto a scansione. Quando viene raggiunta la soglia di incidenti, la scansione passa alla condivisione di file successiva.

Computer è un computer fisico. Quando viene raggiunta la soglia di incidenti, la scansione passa all'elemento successivo nell'elenco da sottoporre a scansione. Se l'elemento si trova sullo stesso computer fisico dell'elemento precedente, viene ignorato. Il nome del computer fisico deve essere esattamente identico nell'elenco degli elementi da sottoporre a scansione affinché Network Discover riconosca che è lo stesso computer. Ad esempio, `\\localhost\myfiles` e `\\127.0.0.1\myfiles` vengono considerati computer diversi, anche se sono logicamente uguali.

Se si utilizza il servizio di individuazione automatica per eseguire la scansione di condivisioni aperte su un file server specificato, la radice di contenuti e il computer coincidono.

Per eseguire la scansione di condivisioni amministrative

- 1 Accedere alla scheda **Avanzate** della definizione del target.
- 2 Nella sezione **Scansione di condivisioni amministrative** selezionare **Esegui scansione di condivisioni amministrative**.

È inoltre possibile configurare la scansione dei file `.pst` di Outlook.

Vedere ["Configurazione delle scansioni delle cartelle personali di Microsoft Outlook \(file .pst\)"](#) a pagina 1921.

Configurazione di Network Protect per condivisioni file

Utilizzare Network Protect per copiare o mettere in quarantena automaticamente in una posizione protetta i file riservati trovati su condivisioni pubbliche. In alternativa, è possibile crittografare i file riservati.

Network Protect è disponibile solo per una scansione basata su server di condivisioni CIFS. Network Protect non è supportato per file .pst.

Con Network Protect attivato, viene visualizzata una scheda nella pagina **Aggiungi target file system** che contiene le opzioni di riparazione di Network Protect. Per utilizzare Network Protect, è necessario possedere una politica e una regola di risposta configurate nella console di amministrazione Enforce Server. Inoltre, le credenziali di scansione (nome utente e password) devono essere presenti nella scheda **Aggiungi destinazione file system** per questo target.

Per configurare Network Protect per condivisioni file

- 1 Creare una politica con una regola di risposta. Accedere a **Gestisci > Politiche > Regole di risposta** e fare clic su **Aggiungi regola di risposta**.
Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.
- 2 Selezionare **Risposta automatica**.
- 3 Fare clic su **Avanti**.

- 4 Per **Azione**, selezionare **Network Protect: copia file**, **Network Protect: metti file in quarantena** o **Network Protect: crittografia file**.

Per l'azione **File in quarantena**, se necessario, è possibile inserire un file marker al posto del file che è stato rimosso selezionando la casella di controllo **File marker**. Inserire il testo del marker nella casella **Testo marker**. Il file di marker è un file di testo. Il testo del marker può contenere variabili sostitutive. Far clic all'interno della casella **Testo marker** per visualizzare un elenco di variabili di inserimento.

Se il file originale era di un altro tipo, il file originale viene spostato nell'area di quarantena. Il nome del file marker è il nome di file originale più un'estensione `.txt`. Le estensioni di file predefinite conservate sono elencate nel file di proprietà

`ProtectRemediation.properties`. Le estensioni di file conservate includono `txt`, `doc`, `xls`, `ppt`, `java`, `c`, `cpp`, `h` e `js`. Ad esempio, un file denominato `myfile.pdf` avrebbe un nome di file del marker `myfile.pdf.txt`.

È possibile creare una nuova sottodirectory per i file messi in quarantena da ogni scansione (il valore predefinito). È possibile modificare il valore predefinito e aggiungere le informazioni di scansione al nome del file (versione) in una directory di quarantena. Modificare il file di proprietà `ProtectRemediation.properties` per modificare il valore predefinito.

Nota: La funzionalità di crittografia è disponibile solo se la licenza di Network Protect ICE è stata installata ed Enforce Server è stato configurato per connettersi al cloud Symantec ICE.

- 5 Fare clic su **Salva**.
- 6 Aggiungere una nuova politica o modificare una politica esistente.
Vedere ["Configurazione di politiche"](#) a pagina 422.
- 7 Fare clic sulla scheda **Risposta**.
- 8 Nel menu a discesa, selezionare una delle regole di risposta create in precedenza.
- 9 Fare clic su **Aggiungi regola di risposta**.
Tale regola di risposta specifica quindi la risposta automatica quando la politica attiva un incidente durante la scansione di un file.
Possono esistere diverse regole di risposta con diverse condizioni per una politica.
- 10 Creare un nuovo target di file system Network Discover o modificare un target esistente.
Vedere ["Configurazione delle scansioni del file system"](#) a pagina 1922.

- 11 Con Network Protect attivato nella licenza, una scheda **Proteggi** viene visualizzata nella pagina target **File system** che contiene le opzioni di riparazione Network Protect.

In **Riparazione protezione consentita**, scegliere se il file deve essere copiato, messo in quarantena (spostato) o crittografato per proteggere le informazioni.

Questa selezione deve corrispondere alla selezione **Azione** dalla regola di risposta.

Inoltre, una regola di risposta con tale azione (copia o messa in quarantena) deve esistere all'interno di una delle politiche selezionate per questo target del file system.

- 12 Se si è scelto di copiare o mettere in quarantena i file riservati, in **Condivisione Copia/Quarantena**, specificare la condivisione in cui i file sono stati messi in quarantena o copiati.

Se necessario, è possibile selezionare una credenziale denominata dall'archivio credenziali nel menu a discesa **Usa credenziali salvate**.

- 13 Se si è scelto di copiare o mettere in quarantena i file riservati, in **Credenziale di protezione**, specificare la credenziale di accesso scrittura per la posizione del file di cui è stata eseguita la scansione.

Per spostare i file per la quarantena durante la riparazione, la definizione del target di Network Discover deve avere accesso in scrittura sia per la posizione di quarantena sia per la posizione del file originale. Specificare il percorso (posizione) in cui i file vengono copiati o messi in quarantena. Digitare il nome utente e la password di accesso scrittura per tale posizione.

Solitamente, le condivisioni sottoposte a scansione richiedono solo credenziali di accesso in lettura (ad esempio, se l'opzione **Copia** è stata selezionata).

Specificare la credenziale di accesso in scrittura della condivisione, se diversa da quella di accesso in lettura.

Se necessario, è possibile selezionare una credenziale denominata dall'archivio credenziali nel menu a discesa **Usa credenziali salvate**.

Vedere ["Configurazione di Enforce Server per connettersi al cloud ICE Symantec"](#) a pagina 229.

Impostazione delle scansioni di database Lotus Notes

Il capitolo contiene i seguenti argomenti:

- [Impostazione delle scansioni del server di database di IBM \(Lotus\) Notes](#)
- [Target di IBM \(Lotus\) Notes supportati](#)
- [Configurazione ed esecuzione di scansioni IBM \(Lotus\) Notes](#)
- [Configurazione delle opzioni di scansione della configurazione della modalità IBM \(Lotus\) Notes DIIOP](#)


Impostazione delle scansioni del server di database di IBM (Lotus) Notes

È possibile configurare scansioni di archivi IBM (Lotus) Notes. Symantec Data Loss Prevention supporta solo scansioni in modalità DIIOP.

Vedere ["Configurazione ed esecuzione di scansioni IBM \(Lotus\) Notes"](#) a pagina 1932.

Per configurare la scansione dei database di Lotus Notes, completare i seguenti processi:

Tabella 66-1 Configurazione di una scansione di database di Lotus Notes

 Pagina	Azione	Descrizione
1	Verificare che il database di IBM (Lotus) Notes sia presente nell'elenco dei target supportati.	Vedere "Target di IBM (Lotus) Notes supportati" a pagina 1932.

Passo	Azione	Descrizione
2	Configurare la scansione per la modalità DIIOP di IBM (Lotus) Notes.	Vedere " Configurazione delle opzioni di scansione della configurazione della modalità IBM (Lotus) Notes DIIOP " a pagina 1936.
3	Fare clic su Gestisci > Scansione Discover > Target di Discover per creare un target di Lotus Notes e configurare le scansioni dei database di Lotus Notes.	Vedere " Configurazione ed esecuzione di scansioni IBM (Lotus) Notes " a pagina 1932.
4	Configurare tutte le opzioni di scansione aggiuntive per il target di IBM (Lotus) Notes.	Vedere " Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover " a pagina 1830.
5	Avviare la scansione del database di IBM (Lotus) Notes. Fare clic su Gestisci > Scansione Discover > Target di Discover .	Selezionare il target di scansione dall'elenco dei target, quindi fare clic sull'icona di avvio.
6	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere " Gestione delle scansioni target di Network Discover/Cloud Storage Discover " a pagina 1853.

Target di IBM (Lotus) Notes supportati

Il target di IBM Notes (precedentemente denominato Lotus Notes) supporta la scansione delle versioni seguenti:

- Lotus Notes 8.5.x
- IBM Notes 9.0.x

I file `Notes.jar` e `NCSO.jar` si trovano nella directory di installazione del client di Lotus Notes. Il numero di versione manifesto di questi file dipende dalla versione del server Domino.

- La versione 8 ha una versione manifesto nel file JAR di 1.5.0
- La versione 9 ha una versione manifesto nel file JAR di 1.6.0

Configurazione ed esecuzione di scansioni IBM (Lotus) Notes

Prima di eseguire una scansione, è necessario configurare un target.

Per configurare un nuovo target per la scansione di database IBM (Lotus) Notes

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su **Nuovo target** e utilizzare il menu a discesa per selezionare il tipo di target **Lotus Notes**.
- 3 Nella scheda **Generale**, digitare il **Nome** del target Discover.
 Digitare un nome univoco per il target, con un massimo di 255 caratteri.
- 4 Selezionare **Gruppo di politiche**.
 Se nessun altro gruppo di politiche è stato selezionato, viene utilizzato il gruppo di politiche predefinito. Per applicare un gruppo di politiche, selezionare il gruppo di politiche da utilizzare per il target. È possibile assegnare più gruppi di politiche a un target.
 È possibile definire i gruppi di politiche nella pagina **Elenco gruppo di politiche**.
- 5 Specificare le opzioni di pianificazione.
 Scegliere **Avvia processo di scansione come pianificato** per configurare una pianificazione per la scansione del target specificato. Selezionare un'opzione a partire dall'elenco a discesa di pianificazione per visualizzare ulteriori campi. Selezionare **Sospendi scansione in questo periodo** per sospendere automaticamente le scansioni durante l'intervallo di tempo specificato. È possibile sovrascrivere la finestra di pausa di un target di scansione passando alla schermata Target di Discover e facendo clic sull'icona di avvio per la voce del target. La finestra di pausa rimane intatta e tutte le scansioni future che vengono eseguite in base a tale finestra possono essere interrotte come specificato. È inoltre possibile riavviare una scansione interrotta facendo clic sull'icona Continua relativa alla voce del target.
- 6 Nella scheda **Destinazione**, in **Server di scansione ed endpoint di destinazione**, selezionare il Discover Server (o più Discover Server) in cui si desidera eseguire la scansione.
 Soltanto i server di rilevamento configurati come Discover Server sono visualizzati nell'elenco. Se è presente solo un Discover Server nella rete, il nome di quel server viene automaticamente specificato. Prima di configurare i target, è necessario configurare i Discover Server. È necessario specificare almeno un server prima di poter eseguire una scansione del target.
- 7 Nella scheda **Contenuto sottoposto a scansione**, selezionare o immettere le credenziali.
 È possibile specificare un nome utente predefinito e una password per accedere a tutti i server Domino specificati nel target. Le credenziali possono essere sovrascritte per un server modificando una singola voce nell'elenco dei server Domino. Le credenziali per una singola voce sono possibili solo se l'elenco è creato con nomi server immessi singolarmente. Le credenziali per una singola voce non sono possibili in un file di testo caricato che contiene l'elenco dei server.

- 8 Nella scheda **Contenuto sottoposto a scansione**, specificare la radice contenuto per una scansione Lotus Notes come server Domino o elenco di server Domino.

Specificare i database per eseguire la scansione come segue:

- **Specifica server Domino**

Fare clic su **Aggiungi radici di contenuti > Per immissione diretta** per specificare i server da sottoporre a scansione. Le informazioni relative alle credenziali del server immesse qui hanno la precedenza sui valori predefiniti e si applicano solo al server specificato.

```
[hostname,username,password]
```

Per una configurazione di modalità nativa, è possibile utilizzare il nome "locale" nell'elenco dei server Domino. Specificare "locale" include i database locali visibili per il client da sottoporre a scansione. Ad esempio, invece dell'URI immettere il testo seguente:

```
local
```

- **Usa server Domino da un file caricato**

Creare e salvare un file di testo (.txt) con i server che si desidera sottoporre a scansione. Non è possibile specificare le credenziali server in questo file di testo. Vengono utilizzati il nome utente e la password specificati nella scheda **Contenuto sottoposto a scansione** della pagina **Aggiungi target Lotus Notes**.

Esempio dei primi server Domino nell'elenco:

```
dominoserver1.company.com  
dominoserver2.company.com  
dominoserver3.company.com
```

Fare clic su **Carica file** per caricare l'elenco dei server Domino.

9 Nella scheda **Filtri**, selezionare i filtri di percorso.

Utilizzare il campo Filtri di inclusione e Filtri di esclusione per specificare i nomi di database Lotus Notes che Symantec Data Loss Prevention dovrà puntare. I filtri corrispondono al percorso completo dell'URI database. Se il campo è vuoto, Symantec Data Loss Prevention esegue la scansione di tutti i database in tutti i server Domino specificati. Delimitare le voci con virgole. Se un URI database corrisponde a un filtro di esclusione e inclusione, il filtro di esclusione ha la precedenza e il database non viene sottoposto a scansione.

Se un filtro di inclusione non rileva una corrispondenza nel database delle radici dei contenuti, il database non viene sottoposto a scansione. Ad esempio, se si desidera rilevare una corrispondenza con il file

`notes://notes.example.com/ABC/2_databases/1.nsf/91A`, il filtro di inclusione ***91A*** non la rileverà, poiché il database delle radici dei contenuti non è incluso nel filtro. Il filtro di inclusione ***1.nsf*** esegue la scansione dell'intera radice dei contenuti. Il filtro di inclusione **/ABC/2_databases/1.nsf/91A** esegue la scansione solo del file specificato. Il database delle radici dei contenuti inizia con il carattere **/**.

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

10 Nella scheda **Filtri**, selezionare **Filtri dimensioni documenti**.

È possibile specificare i documenti da ignorare al sotto e/o al di sopra di una dimensione specificata.

11 Nella scheda **Filtri**, selezionare una scansione differenziale (opzionale).

Selezionare **Esegui scansione solo di file aggiunti o modificati dopo l'ultima scansione completa** in modo che Symantec Data Loss Prevention esegua la scansione solo degli elementi o dei documenti che sono stati aggiunti o modificati dall'ultima scansione completa. La prima scansione deve essere una scansione completa (base iniziale). Una scansione completa si verifica se si seleziona questa opzione prima che Symantec Data Loss Prevention esegua una scansione di questo target per la prima volta.

12 Nella scheda **Filtri**, selezionare **Filtri data documenti**.

Specificare i filtri di data per escludere i documenti Lotus Notes dalla scansione in base alle relative date. Soltanto i documenti che corrispondono ai filtri di data specificati sono inclusi.

13 Selezionare la scheda **Avanzate** per le opzioni di ottimizzazione della scansione. Nella scheda **Avanzate**, è possibile configurare le opzioni di limitazione o la modalità inventario per la scansione.

- **Opzioni di limitazione**

Immettere il numero massimo di documenti oppure di byte da elaborare al minuto per ciascun server di rilevamento. Per i byte, specificare l'unità di misura dall'elenco a discesa. Le opzioni sono byte, KB (kilobyte) o MB (megabyte).

- Scansione inventario

Immettere il numero di incidenti da generare prima di passare al server Domino successivo (specificato nella scheda **Contenuto sottoposto a scansione**). Per verificare se esistono dati confidenziali in un target, senza sottoporli tutti a scansione, configurare la modalità inventario per la scansione. L'impostazione di soglie per gli incidenti può migliorare le prestazioni della scansione ignorando il server successivo da sottoporre a scansione, invece di sottoporre a scansione tutto.

Vedere ["Creazione di un inventario delle posizioni di dati riservati non protetti"](#) a pagina 1849.

Configurazione delle opzioni di scansione della configurazione della modalità IBM (Lotus) Notes DIIOP

Nel file `Crawler.properties`, quando `lotusnotescrawler.use.diiop` è impostato su `true`, DIIOP (CORBA) viene utilizzato per sottoporre a scansione un server Domino. Il rilevatore si collega direttamente al server Domino con HTTP e DIIOP.

Per configurare una configurazione modalità IBM (Lotus) Notes DIIOP IBM per la scansione

- 1 Copiare i file della libreria Lotus Notes Java `Notes.jar` e `NCSO.jar` nella directory `c:\Program Files\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\plugins`.

Possono trovarsi nelle directory di installazione di un client IBM (Lotus) Notes e di un server IBM (Lotus) Domino in cui è installato Domino Designer.

Il file di `Notes.jar` si trova nelle seguenti directory di installazione predefinite del client IBM (Lotus) Notes:

- IBM Notes 8

`C:\Program Files\IBM\lotus\notes\jvm\lib\ext\Notes.jar`

- Lotus Notes 7

`C:\Program Files\lotus\notes\jvm\lib\ext\Notes.jar`

Utilizzare la versione del file JAR corrispondente alla versione del client IBM (Lotus) Notes.

Vedere ["Target di IBM \(Lotus\) Notes supportati"](#) a pagina 1932.

Il file `NCSO.jar` si trova nelle seguenti directory di installazione predefinite del server IBM (Lotus) Domino, quando viene installato Domino Designer:

- IBM Notes 8

`C:\Program Files\IBM\lotus\Notes\Data\domino\java\NCSO.jar`

- **Lotus Notes 7**

`C:\Program Files\lotus\notes\data\domino\java\NCSO.jar`

2 Nel file `Crawler.properties`, impostare la seguente proprietà:

`lotusnotescrawler.use.diiop = true`

- 3** Avviare il servizio HTTP sul server Domino.
- 4** Avviare il servizio DIIOP sul server Domino.
- 5** Sul server Domino, impostare l'opzione Consenti alle connessioni HTTP di esplorare i database su true.
- 6** Durante la creazione di target, immettere le credenziali di un'utente che dispone di una password Internet.

Impostazione delle scansioni di database SQL

Il capitolo contiene i seguenti argomenti:

- [Impostazione delle scansioni del server di database SQL](#)
- [Target di database SQL supportati](#)
- [Configurazione ed esecuzione di scansioni database SQL](#)
- [Installazione del driver JDBC per target di SQL Database.](#)
- [Proprietà di configurazione scansione database SQL](#)

Impostazione delle scansioni del server di database SQL

È possibile configurare la scansione di database Oracle, SQL Server o DB2.

Vedere ["Configurazione ed esecuzione di scansioni database SQL"](#) a pagina 1940.

Per configurare la scansione dei database SQL, completare i seguenti processi:

Tabella 67-1 Configurazione di una scansione database SQL

Passo	Azione	Descrizione
1	Verificare che il database SQL sia presente nell'elenco dei target supportati.	Vedere "Target di database SQL supportati" a pagina 1939.
2	Fare clic su Gestisci > Scansione Discover > Target di Discover per creare un target di database SQL e configurare le scansioni dei database SQL.	Vedere "Configurazione ed esecuzione di scansioni database SQL" a pagina 1940.

Passo	Azione	Descrizione
3	Configurare altre eventuali opzioni di scansione per il target di database SQL.	Vedere "Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover" a pagina 1830.
4	Installare il driver JDBC per il database SQL, se necessario.	Vedere "Installazione del driver JDBC per target di SQL Database." a pagina 1943.
5	Avviare la scansione del database SQL. Fare clic su Gestisci > Scansione Discover > Target di Discover .	Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.
6	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Gestione delle scansioni target di Network Discover/Cloud Storage Discover" a pagina 1853.

Target di database SQL supportati

I seguenti database SQL sono stati testati con scansioni di target di Network Discover:

- 10g, 11g (11.2) e 12c (12.1) (*vendor_name* è `oracle`)

Nota: Oracle 10g è obsoleto in Symantec Data Loss Prevention 15.1.

- SQL Server 2005, 2014 e 2016 (il *vendor_name* è `sqlserver`)

Nota: SQL Server 2005 è obsoleto in Symantec Data Loss Prevention 15.1.

- DB2 10.5 (il *vendor_name* è `db2`)

Contattare il supporto di Symantec Data Loss Prevention per informazioni sulla scansione di altri database SQL.

Configurazione ed esecuzione di scansioni database SQL

È possibile configurare ed eseguire scansioni su database SQL per identificare quali database contengono dati confidenziali, oppure rilevare la presenza non opportuna di dati confidenziali.

La scansione dei database SQL viene eseguita per un tipo di dati colonna specifico. La scansione dei database SQL estrae i dati dei seguenti tipi di connettività database Java (JDBC): CLOB, BLOB, BIGINT, CHAR, LONGVARCHAR, VARCHAR, TINYINT, SMALLINT, INTEGER, REAL, DOUBLE, FLOAT, DECIMAL, NUMERIC, DATE, TIME e TIMESTAMP. La mappatura tra questi tipi di colonna e quelli di un database specifico dipende dall'implementazione del driver JDBC per la scansione.

Per configurare una scansione per un Database SQL

- 1 Nella console di amministrazione di Enforce Server, accedere a **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su **Nuovo target** e utilizzare il menu a discesa per selezionare il tipo di target **Database SQL**.
- 3 Nella scheda **Generale**, digitare il **Nome** del target Discover.
Digitare un nome univoco per il target, con un massimo di 255 caratteri.
- 4 Selezionare **Gruppo di politiche**.
Se nessun altro gruppo di politiche è stato selezionato, viene utilizzato il gruppo di politiche predefinito. Per applicare un gruppo di politiche, selezionare il gruppo di politiche da utilizzare per il target. È possibile assegnare più gruppi di politiche a un target.
- 5 Specificare le opzioni di pianificazione.

Scegliere **Avvia processo di scansione come pianificato** per configurare una pianificazione per la scansione del target specificato. Selezionare un'opzione a partire dall'elenco a discesa della pianificazione per visualizzare i campi aggiuntivi. Selezionare **Sospendi scansione in questo periodo** per sospendere automaticamente le scansioni durante l'intervallo di tempo specificato. È possibile ignorare la sospensione della scansione di un target passando alla schermata Target di Discover e facendo clic sull'icona di avvio per la voce del target. La finestra di pausa rimane intatta e tutte le scansioni future che vengono eseguite in base a tale finestra possono essere interrotte come specificato. È inoltre possibile riavviare una scansione interrotta facendo clic sull'icona Continua relativa alla voce del target.

- 6 Nella scheda **Destinazione**, in **Server di scansione ed endpoint di destinazione**, selezionare il Discover Server (o più Discover Server) in cui si desidera eseguire la scansione.

Soltanto i server di rilevamento configurati come Discover Server sono visualizzati nell'elenco. Se è presente solo un Discover Server nella rete, il nome di quel server viene automaticamente specificato. Prima di configurare i target, è necessario configurare i Discover Server. È necessario specificare almeno un server prima di poter eseguire una scansione del target.

- 7 Nella scheda **Contenuto sottoposto a scansione**, selezionare o immettere le credenziali.
- 8 Selezionare uno dei seguenti metodi per l'immissione dei database:

- **Usa server di database da un file caricato**

Creare e salvare un file di testo (.txt) con i server che si desidera sottoporre a scansione. Fare clic su **Sfoggia** per individuare l'elenco e su **Carica** per importarlo. Vengono utilizzati il nome utente e la password specificati nella scheda **Contenuto sottoposto a scansione** della pagina **Aggiungi target Database SQL**.

Immettere i database utilizzando la seguente sintassi. Il nome del produttore può essere `oracle`, `db2` o `sqlserver`. L'origine dati è il nome secondario della stringa di connessione JDBC per tale driver e database. La documentazione del driver JDBC descrive questo nome secondario. Se lo si desidera, è possibile immettere il numero massimo di righe da sottoporre a scansione per ciascuna tabella del database.

```
vendor_name:datasource[, maximum-rows-to-scan]
```

Ad esempio:

```
oracle:@//oracleserver.company.com:1521/mydatabase  
db2://db2server.company.com:50000/mydatabase,300
```

Per alcuni SQL Server, è necessario specificare anche il nome dell'istanza SQL, come nel seguente esempio:

```
sqlserver://sqlserver.company.com:1433/mydatabase;  
instance=myinstance
```

- **Specifica server di database**

Fare clic su **Aggiungi radici di contenuti > Immissione manuale** per utilizzare un editor di riga per specificare i database da sottoporre a scansione. Le informazioni relative ai database SQL immesse qui hanno la precedenza sui valori predefiniti e si applicano solo al database specificato. Se lo si desidera, è possibile immettere il numero massimo di righe da sottoporre a scansione per ciascuna tabella del database. Utilizzare la seguente sintassi:

```
vendor-name:datasource[, [username, password]  
[, maximum-rows-to-scan]]
```

9 Nella scheda **Filtri**, immettere i valori facoltativi Filtri di inclusione e Filtri di esclusione.

Utilizzare i Filtri di inclusione e i Filtri di esclusione per specificare i database e le tabelle SQL che Symantec Data Loss Prevention deve elaborare o saltare.

Quando vengono utilizzati sia i Filtri di inclusione, sia i Filtri di esclusione, i secondi hanno la precedenza. Qualsiasi tabella che corrisponde ai Filtri di inclusione viene sottoposta a scansione, a meno che non corrisponda anche ai Filtri di esclusione, nel qual caso non viene sottoposta a scansione.

Se si lascia vuoto il campo Filtri di inclusione Symantec Data Loss Prevention ricerca la corrispondenza in tutte le tabelle. Queste tabelle vengono restituite dalla query relativa alle tabelle dei database SQL target. Se si immette qualsiasi valore nel campo, Symantec Data Loss Prevention analizza solo database e tabelle corrispondenti al filtro specificato.

La sintassi è un modello per il database, una barra verticale e un modello per il nome della tabella. I modelli multipli possono essere separati con virgole. Viene applicata la corrispondenza tra modelli standard. Ad esempio, "?" corrisponde a un carattere singolo.

Poiché la corrispondenza tra i nomi della tabella non fa distinzione tra maiuscole e minuscole per molti database, viene eseguita la conversione con le maiuscole. Il nome della tabella nel modello e il nome della tabella a cui viene fatto corrispondere vengono convertiti in maiuscole prima della corrispondenza.

Nel seguente esempio verrebbe abbinata la tabella dei dipendenti in tutti i database.

```
*|employee
```

Nel seguente esempio verrebbero abbinate le tabelle dei dipendenti in tutti i database Oracle.

```
oracle:*|*
```

Per SQL Server 2005 e DB2, la query predefinita per le tabelle restituisce i nomi delle tabelle nel formato *schema_name.table_name*. I Filtri di inclusione e i Filtri di esclusione per SQL Server e DB2 dovrebbero corrispondere a questo formato.

Vedere i seguenti esempi:

```
sqlserver:*|HRschema.employee  
sqlserver:*|*.employee
```

10 Selezionare la scheda **Avanzate** per le opzioni di ottimizzazione della scansione. Nella scheda **Avanzate**, è possibile configurare le opzioni di limitazione o la modalità inventario per la scansione.

- **Opzioni di limitazione**
 Immettere il numero massimo di righe oppure di byte da elaborare al minuto per ciascun server di rilevamento. Se si selezionano entrambe le opzioni, la velocità di scansione è inferiore rispetto a entrambe le opzioni. La velocità di scansione è inferiore rispetto al numero di righe e al numero di byte specificato al minuto. Per i byte, specificare l'unità di misura dall'elenco a discesa. Le opzioni sono byte, KB (kilobyte) o MB (megabyte).
- **Scansione inventario**
 Fornire il numero di incidenti da produrre prima di passare all'elemento successivo da sottoporre a scansione. L'elemento successivo è il database successivo dell'elenco nella scheda **Contenuto sottoposto a scansione**. Per verificare se esistono dati confidenziali in un target, senza sottoporli tutti a scansione, configurare la modalità inventario per la scansione. L'impostazione di soglie per gli incidenti può migliorare le prestazioni della scansione saltando all'elemento successivo da sottoporre a scansione, invece di sottoporli tutti a scansione.
 Vedere ["Creazione di un inventario delle posizioni di dati riservati non protetti"](#) a pagina 1849.

Installazione del driver JDBC per target di SQL Database.

Per ogni tipo di database da sottoporre a scansione è necessario installare un driver JDBC sul server di rilevazione di &pn.NetworkDiscover.

Per installare il driver JDBC

- 1 Ottenere il driver JDBC rilevante.
 - Il driver di Oracle è già installato con il server Network Discover nella directory dei driver SQL predefinita `Protect/lib/jdbc`.
 Il driver JDBC è il driver Oracle JDBC versione 10.2.0.3.0.
 - Per il Microsoft SQL Server, è possibile scaricare il driver open source jTDS sul sito Source Forge <http://jtds.sourceforge.net/>.
 La versione 1.2.2 del driver jTDS JDBC è stata testata con Network Discover.
 - Per DB2, i file JAR del driver IBM si trovano nella distribuzione IBM DB2, sotto la cartella di Java. È possibile scaricarli sul sito IBM <http://www.ibm.com/db2>.
 La versione 1.4.2 del driver IBM JDBC è stata testata con Network Discover.
- 2 Copiare i file di driver nella directory di driver SQL `Protect/lib/jdbc`.

- 3 Modificare i permessi dei file di driver JDBC in modo che l'utente Proteggi disponga almeno del permesso di lettura.
- 4 È inoltre possibile che sia necessario modificare il file `sqldatabasecrawler.properties` per specificare i nomi JAR corretti per i driver selezionati.

Vedere ["Proprietà di configurazione scansione database SQL"](#) a pagina 1944.

Proprietà di configurazione scansione database SQL

Le seguenti proprietà di configurazione possono essere modificate nel file di configurazione `sqldatabasecrawler.properties` su Network Discover Server:

- **`driver_class.vendor_name`**

Specifica il nome della classe del driver JDBC da utilizzare. Il file JAR per questo driver deve essere incluso nella directory definita in `sqldrivers.dir` e definita come `driver_jar.vendor_name`.

Esempio:

```
driver_class.sqlserver = net.sourceforge.jtds.jdbc.Driver
```

- **`driver_subprotocol.vendor_name`**

Specifica la porzione di sottoprotocollo della stringa di connessione JDBC.

Esempio:

```
driver_subprotocol.sqlserver = jtds:sqlserver
```

- **`driver_jar.vendor_name`**

Specifica l'elenco di file JAR richiesti dal driver. I file JAR sono memorizzati nella directory definita in `sqldrivers.dir`.

Vedere ["Installazione del driver JDBC per target di SQL Database."](#) a pagina 1943.

Esempi:

```
driver_jar.sqlserver = jtds-1.2.2.jar  
driver_jar.db2 = db2jcc.jar, db2jcc_license_cu.jar
```

- **`driver_table_query.vendor_name`**

Specifica la ricerca da eseguire per restituire un elenco di tabelle di cui eseguire la scansione. Tipicamente, la ricerca dovrebbe restituire tutte le tabelle utente nel database. Tenere presente che l'account database che emette la ricerca necessita di diritti appropriati concessi dall'amministratore del database.

È necessario utilizzare un account per eseguire la scansione in grado di eseguire `driver_table_query` in `sqldatabasecrawler.properties` e restituire risultati. È possibile verificare la configurazione di scansione utilizzando `sqlplus` per accedere come utente di

scansione ed eseguire la ricerca. Se si ottengono risultati, si dispone dell'autorizzazione per completare la scansione. Se non si ottengono risultati, è necessario modificare la ricerca o modificare i privilegi per l'utente di scansione.

Esempio:

```
driver_table_query.sqlserver = SELECT table_schema  
+ '.' + table_name FROM information_schema.tables
```

- **driver_row_selector.vendor_name**

Specifica il formato della ricerca da utilizzare per selezionare le righe dalla tabella. Questo nome venditore varia, in base al database. Gli esempi sono inclusi nel file di configurazione `sqldatabasecrawler.properties` per i database più comuni.

Le seguenti variabili di sostituzione sono utilizzate nella ricerca:

```
0=TABLENAME  
1=COLUMNS  
2=ROWNUM
```

Esempio:

```
driver_row_selector.sqlserver = SELECT TOP {2} {1} FROM {0}
```

- **quote_table_names.vendor_name**

Specifica se i nomi della tabella sono racchiusi tra virgolette prima della creazione della ricerca della selezione della riga. L'attivazione della funzionalità consente la scansione di tabelle con nomi numerici. Ad esempio, Payroll.1 diventa "Payroll"."1" quando il nome è racchiuso tra virgolette.

Esempio:

```
quote_table_names.sqlserver=true
```

- **sqldrivers.dir**

Specifica la posizione della directory in cui si trovano i file JAR del driver JDBC.

Impostazione delle scansioni di server SharePoint

Il capitolo contiene i seguenti argomenti:

- [Impostazione delle scansioni di server SharePoint](#)
- [Informazioni sulle scansioni di server SharePoint](#)
- [Target del server SharePoint supportati](#)
- [Privilegi di accesso per le scansioni SharePoint](#)
- [Informazioni sugli insiemi di mapping di accesso alternativo](#)
- [Configurazione ed esecuzione delle scansioni dei server SharePoint](#)
- [Configurazione Network Protect per i server SharePoint](#)
- [Installazione della soluzione SharePoint su front end Web in un gruppo](#)
- [Attivazione della scansione SharePoint senza installare la soluzione SharePoint](#)
- [Configurazione delle scansioni SharePoint per l'uso dell'autenticazione Kerberos](#)
- [Risoluzione dei problemi delle scansioni di SharePoint](#)

Impostazione delle scansioni di server SharePoint

Per configurare la scansione di server SharePoint, completare il seguente processo:

Tabella 68-1 Impostazione della scansione di un server SharePoint

Passaggio	Azione	Descrizione
1	Verificare che il server SharePoint sia presente nell'elenco dei target supportati.	Vedere "Target del server SharePoint supportati" a pagina 1949.
2	Facoltativo: verificare di disporre di autorizzazioni sufficienti a installare la soluzione SharePoint sui front-end Web in una farm. Verificare inoltre che l'utente della scansione disponga dell'autorizzazione a eseguire la scansione del server SharePoint.	Vedere "Privilegi di accesso per le scansioni SharePoint" a pagina 1949. Vedere "Installazione della soluzione SharePoint su front end Web in un gruppo" a pagina 1958. Vedere "Configurazione ed esecuzione delle scansioni dei server SharePoint" a pagina 1950.
3	Facoltativo: installare la soluzione SharePoint sui front-end Web in una farm. Facoltativo: configurare il server o i server Discover per eseguire la scansione di SharePoint senza utilizzare la soluzione SharePoint.	Vedere "Installazione della soluzione SharePoint su front end Web in un gruppo" a pagina 1958. Vedere "Attivazione della scansione SharePoint senza installare la soluzione SharePoint" a pagina 1960.
4	Fare clic su Gestisci > Scansione Discover > Target di Discover per creare un target di SharePoint e configurare le scansioni dei server di SharePoint.	Vedere "Configurazione ed esecuzione delle scansioni dei server SharePoint" a pagina 1950.
5	Configurare altre eventuali opzioni di scansione per il target SharePoint.	Vedere "Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover" a pagina 1830.
6	Avviare la scansione del server SharePoint.	Fare clic su Gestisci > Scansione Discover > Target di Discover . Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.
7	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Gestione delle scansioni target di Network Discover/Cloud Storage Discover" a pagina 1853.

Informazioni sulle scansioni di server SharePoint

Il server Network Discover individua una vasta gamma di dati riservati esposti sui server SharePoint. Comunica con Enforce Server per ottenere informazioni sulle politiche e sui target

di scansione. Invia le informazioni sui dati riservati esposti che trova a Enforce Server per il reporting e la riparazione.

I seguenti tipi di elementi SharePoint sono sottoposti a scansione:

- Pagine wiki
- Blog
- Voci di calendario
- Attività
- Attività di progetto
- Messaggi di discussione
- Elenchi di contatti
- Annunci
- Collegamenti
- Sondaggi
- Gestione dei problemi
- Elenchi personalizzati
- Documenti nella libreria di documenti

Nota: Soltanto l'ultima versione di un documento viene sottoposta a scansione.

La comunicazione tra il Discover Server e il front end Web (WFE) di SharePoint è basata su SOAP.

La comunicazione è protetta quando i siti Web SharePoint sono configurati per l'uso di SSL.

Per HTTPS, la convalida del certificato SSL del server non è l'impostazione predefinita. Per abilitare la convalida del certificato SSL del server, attivare l'impostazione avanzata `Discover.ValidateSSLCertificates`. Quindi importare il certificato SSL del server in Discover Server.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Vedere ["Importazione di certificati SSL in Enforce o Discover server"](#) a pagina 272.

Se il sito SharePoint specificato è configurato per utilizzare una porta che non è quella predefinita (80), assicurarsi che il server SharePoint consenta al server di rilevamento Discover di comunicare sulla porta richiesta.

L'accesso degli utenti al contenuto è basato sui diritti per l'utente specificato in SharePoint. Immettere le credenziali dell'utente per specificare tale utente quando si configura una scansione di SharePoint.

Vedere ["Configurazione ed esecuzione delle scansioni dei server SharePoint"](#) a pagina 1950.

Target del server SharePoint supportati

I seguenti target del server SharePoint sono supportati:

- Microsoft Office SharePoint Server 2010 SP2
- Microsoft Office SharePoint Server 2013 SP1
- Microsoft Office SharePoint Server 2016

Privilegi di accesso per le scansioni SharePoint

Per eseguire la scansione SharePoint, gli account utente devono disporre di diritti sufficienti per accedere a e sfogliare il contenuto del sito di SharePoint. Devono inoltre avere l'autorizzazione per richiamare i servizi Web e l'autorizzazione per ottenere l'elenco di controllo di accesso (ACL).

Questi diritti corrispondono alle autorizzazioni di SharePoint di livello inferiore "Esplorazione directory", "Utilizzo interfacce remote" ed "Enumerazione autorizzazioni". Consultare la documentazione di Microsoft SharePoint per ulteriori informazioni sulle autorizzazioni e sui livelli di autorizzazione di SharePoint. Se l'account utente non dispone del diritto "Enumerazione autorizzazioni", non è possibile ottenere l'ACL per il contenuto di SharePoint.

Per i livelli di autorizzazione seguenti in SharePoint sono già definite le autorizzazioni riportate di seguito:

- Controllo completo (include Esplorazione directory, Utilizzo interfacce remote ed Enumerazione autorizzazioni)
- Progettazione (include Esplorazione directory e Utilizzo interfacce remote)
- Collaborazione (include Esplorazione directory e Utilizzo interfacce remote)

Informazioni sugli insiemi di mapping di accesso alternativo

SharePoint richiede che tutti gli URL utilizzati per l'accesso a un'applicazione Web siano definiti nell'amministrazione centrale come interni o pubblici e la soluzione Symantec SharePoint richiede che l'utente fornisca uno di tali URL definiti come destinazione di scansione. Utilizzare gli insiemi di mapping di accesso alternativo di SharePoint per definire gli URL dell'applicazione

Web da utilizzare per la scansione. Per informazioni sugli insiemi di mapping di accesso alternativo vedere <http://technet.microsoft.com/en-us/library/cc288609%28office.12%29.aspx>.

Configurazione ed esecuzione delle scansioni dei server SharePoint

Prima di eseguire una scansione, è necessario configurare un target utilizzando la seguente procedura.

Se si decide di utilizzarla, la soluzione SharePoint deve essere installata sul front-end Web in una farm.

Vedere "[Installazione della soluzione SharePoint su front end Web in un gruppo](#)" a pagina 1958.

È possibile eseguire la scansione dei repository SharePoint senza utilizzare la soluzione SharePoint. Le scansioni di SharePoint che non utilizzano la soluzione SharePoint presentano le seguenti limitazioni:

- Non è possibile utilizzare un'applicazione Web come radice dei contenuti per la scansione. È invece necessario estrarre manualmente le raccolte di siti da utilizzare come radici dei contenuti.
Vedere "[Per enumerare gli URL di raccolta siti](#)" a pagina 1961.
- I dettagli degli incidenti SharePoint non includono informazioni relative alle autorizzazioni.
- Non è possibile utilizzare le azioni di FlexResponse server per riparare gli incidenti SharePoint.

Vedere "[Attivazione della scansione SharePoint senza installare la soluzione SharePoint](#)" a pagina 1960.

Per configurare un nuovo target per la scansione di un server SharePoint

- 1 Fare clic su **Gestisci > Scansione Discover > Target di Discover > Nuovo target > Server > SharePoint**.
- 2 Nella scheda **Generale**, digitare il nome del target.
- 3 Selezionare i gruppi di politiche che contengono le politiche per questa scansione.

4 Selezionare le opzioni di pianificazione.

Scegliere **Avvia processo di scansione come pianificato** per pianificare la scansione del target specificato. Selezionare un'opzione a partire dall'elenco a discesa di pianificazione per visualizzare ulteriori campi.

Selezionare **Sospendi scansione in questo periodo** per sospendere automaticamente le scansioni durante l'intervallo di tempo specificato. È possibile ignorare la sospensione della scansione di un target passando alla schermata Target di Discover e facendo clic sull'icona di avvio per la voce del target. Il periodo di sospensione rimane inalterato e tutte le scansioni future che vengono eseguite in base alla finestra di scansione vengono sospese come specificato. È inoltre possibile riavviare una scansione interrotta facendo clic sull'icona Continua relativa alla voce del target.

Vedere ["Pianificazione delle scansioni di Network Discover/Cloud Storage Discover"](#) a pagina 1833.

5 Nella scheda **Destinazione**, in **Server di scansione ed endpoint di destinazione**, selezionare il Discover Server (o più Discover Server) in cui si desidera eseguire la scansione.

Soltanto i server di rilevamento configurati come Discover Server sono visualizzati nell'elenco. Se è presente solo un Discover Server nella rete, il nome di quel server viene automaticamente specificato. Prima di configurare i target, è necessario configurare i Discover Server. È necessario specificare almeno un server prima di poter eseguire una scansione del target.

6 Per l'opzione **Modalità di scansione**, selezionare una delle opzioni seguenti:

- Selezionare **Utilizza server singolo per la scansione** per eseguire le scansioni utilizzando solo un server. Se nel passaggio precedente è stato selezionato più di un server, Symantec Data Loss Prevention seleziona automaticamente uno dei server all'avvio della scansione.
- Selezionare **Utilizza tutti i server selezionati per la scansione in una griglia** per attivare la funzionalità di scansione della griglia che distribuisce il carico di lavoro della scansione su più server. Quando si inizializza una scansione, a uno dei server è assegnato il ruolo di Elemento principale griglia che coordina le azioni degli altri server.

Nota: È necessario selezionare almeno due server affinché il target della scansione possa eseguire una scansione della griglia. Symantec consiglia di applicare la stessa configurazione hardware e software a tutti i server di rilevamento che si intende utilizzare per le scansioni della griglia. Prima di eseguire per la prima volta una scansione della griglia, assicurarsi che la porta di comunicazione della griglia configurata nel file di `ScanManager.properties` sia aperta su tutti i server nella griglia.

Vedere ["Configurazione della scansione della griglia"](#) a pagina 1876.

- 7 Nella scheda **Contenuto sottoposto a scansione**, immettere le credenziali per la scansione.

È possibile utilizzare una di queste tre modalità di autenticazione:

- **Windows** (predefinito)

Nota: Selezionare questa opzione se per il gruppo di politiche assegnato è stata configurata l'azione FlexResponse server di **SharePoint Encrypt**.

- **Moduli**

- **Attestazioni**, solo per Microsoft Active Directory Federation Services (ADFS)
Se si sceglie l'autenticazione **Attestazioni**, immettere il **Nome servizio federativo**. Il **Nome servizio federativo** è l'URL del server ADFS. È possibile trovare il nome corretto nella sezione Proprietà dei servizi federativi della console ADFS.

È possibile specificare un nome utente predefinito per l'accesso a tutti i siti SharePoint, eccetto quelli specificati utilizzando l'editor **Aggiungi**.

Se si specificano siti SharePoint con l'editor **Aggiungi**, è possibile specificare credenziali distinte per ogni sito.

Gli account utente devono disporre delle autorizzazioni "Esplorazione directory" in SharePoint per eseguire la scansione. Per recuperare le autorizzazioni, l'account utente necessita del livello di autorizzazione "Enumerazione autorizzazioni" di SharePoint.

Vedere "[Privilegi di accesso per le scansioni SharePoint](#)" a pagina 1949.

- 8 Specificare i siti SharePoint da sottoporre a scansione.

Per ogni sito, immettere un URL target per la raccolta di siti, il sito o l'applicazione web SharePoint da sottoporre a scansione. Tutti gli elementi nei relativi siti figlio e secondari sono sottoposti a scansione.

Per un'applicazione Web, specificare ad esempio: `http://www.sharepoint.com:2020`

Per una raccolta di siti, specificare ad esempio:

`http://www.sharepoint.com:2020/Sites/collection`

Per un sito o un sito secondario, specificare ad esempio:

`http://www.sharepoint.com:2020/Sites/mysharepoint/sub/mysite`

Per il sito SharePoint, utilizzare l'URL pubblico anziché l'URL interno.

La sintassi seguente viene applicata per l'URL e le credenziali in ogni riga.

URL, [username,password]

Selezionare uno dei metodi seguenti di immissione della posizione per il server SharePoint:

- File caricato

Selezionare **Esegui scansione di siti da un file caricato**. Creare e salvare un file di testo (.txt) che elenca i server che si desidera sottoporre a scansione. Creare il file utilizzando un editor di testo ASCII e immettere un URL per riga. Quindi fare clic su **Sfoglia** per individuare il file con l'elenco. Fare clic su **Carica ora** per importarlo.

- Singole voci

Selezionare **Esegui scansione di siti**. Fare clic su **Aggiungi** per utilizzare un editor di riga per specificare i server da sottoporre a scansione. Le informazioni sui server immesse qui hanno la precedenza sui valori predefiniti e si applicano solo al percorso specificato.

9 In **Tipo di scansione**, selezionare **Esegui scansione solo di elementi nuovi o modificati (scansione incrementale)**. Questa opzione è il valore predefinito per i nuovi target.

Se sono state modificate la politica o altre definizioni in una scansione esistente, è possibile configurare la scansione successiva in modo che sia una scansione completa. Selezionare la seguente opzione:

Esegui scansione di tutti gli elementi alla scansione successiva. Le scansioni successive saranno incrementali.

Se si desidera eseguire sempre la scansione di tutti gli elementi in questo target, selezionare la seguente opzione:

Esegui sempre scansione di tutti gli elementi (scansione completa)

10 Nella scheda **Filtri**, selezionare i filtri di percorso.

Utilizzare i **Filtri di inclusione** e i **Filtri di esclusione** per specificare gli elementi che Symantec Data Loss Prevention deve elaborare o ignorare. Se si lascia vuoto il campo, Symantec Data Loss Prevention ricerca la corrispondenza in tutti gli elementi. Se si immette un qualsiasi valore per il filtro di inclusione, Symantec Data Loss Prevention sottopone a scansione solo gli elementi corrispondenti al filtro specificato. Delimitare le voci con una virgola, ma non utilizzare spazi.

È possibile fornire filtri utilizzando espressioni regolari, o percorsi relativi alla posizione del sito SharePoint. I filtri possono includere una raccolta di siti, un sito secondario, una cartella, un nome di file o un'estensione di file. I filtri non possono includere il protocollo e il nome host. I filtri di percorso non sono applicati agli allegati di un elemento, come un allegato .doc di un elemento di elenco.

Ad esempio: per escludere il sito `https://app-1234.foo.com/sites/travel/XYZ`, il filtro di esclusione `*XYZ` funziona, ma `https://app*` e `https://app-1234.foo.com/sites/travel/XYZ*` non funzionano.

Tutti i filtri del percorso eseguono la distinzione tra maiuscole e minuscole.

Per il **Filtro di inclusione**, la corrispondenza dell'espressione regolare viene applicata ai file, ma non alle cartelle.

Per il **Filtro di esclusione**, la corrispondenza dell'espressione regolare viene applicata ai file e alle cartelle.

Soltanto il percorso fino al primo "?" o "*" viene considerato in caso di corrispondenza con una cartella o un file.

Quando tutti i filtri di percorso specificati sono relativi, la cartella corrispondente viene ignorata e le statistiche sulla scansione non comprendono gli elementi nelle cartelle ignorate.

Per ottenere i risultati migliori, iniziare il filtro di inclusione o esclusione con un carattere jolly.

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

11 Nella scheda **Filtri**, selezionare i filtri di data.

I filtri di data consentono di includere elementi dal processo di corrispondenza in base alle relative date. Vengono sottoposti a scansione tutti gli elementi che corrispondono ai filtri di data specificati.

Vedere ["Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica"](#) a pagina 1844.

12 Nella scheda **Filtri**, selezionare i filtri di dimensione.

I filtri di dimensione consentono di escludere elementi dal processo di corrispondenza in base alla relativa dimensione. Symantec Data Loss Prevention include solo gli elementi che corrispondono ai filtri di dimensione specificati. Se si lascia vuoto questo campo, Symantec Data Loss Prevention ricerca la corrispondenza per elementi o documenti di tutte le dimensioni.

Vedere ["Filtraggio dei target di Discover per dimensione dell'oggetto"](#) a pagina 1843.

13 Selezionare la scheda **Avanzate** per le opzioni di ottimizzazione della scansione. Nella scheda **Avanzate**, è possibile configurare le opzioni di limitazione e impostare la modalità inventario per la scansione.

- **Opzioni di limitazione**

Specificare il numero massimo di elementi da elaborare al minuto per server di rilevazione o il numero massimo di byte da elaborare al minuto per server di rilevazione. Per i byte, specificare l'unità di misura dall'elenco a discesa. Le opzioni sono byte, KB (kilobyte) o MB (megabyte).

Nota: La limitazione di byte è applicata solo dopo il recupero di ogni elemento. Di conseguenza, il traffico di rete reale può non corrispondere esattamente alla limitazione di byte impostata.

- **Scansione inventario**

Fornire il numero di incidenti da produrre prima di passare al sito successivo da sottoporre a scansione (un URL nella scheda **Contenuto sottoposto a scansione**). Per verificare se esistono dati confidenziali in un target, senza sottoporli tutti a scansione, configurare la modalità inventario per la scansione. L'impostazione di soglie per gli incidenti può migliorare le prestazioni della scansione passando al sito successivo da sottoporre a scansione, invece di sottoporli tutti a scansione. Dopo che la soglia di incidenti è stata raggiunta, la scansione di questo sito viene interrotta e inizia quella del sito seguente. Poiché il processo è asincrono, è possibile che venga creato qualche incidente in più di quelli specificati dalla soglia.

14 Nella scheda **Proteggi**, specificare le preferenze di riparazione per i file che contengono informazioni riservate.

Vedere ["Configurazione Network Protect per i server SharePoint"](#) a pagina 1956.

Configurazione Network Protect per i server SharePoint

Utilizzare Network Protect per mettere in quarantena automaticamente in una posizione sicura i file riservati trovati sui server SharePoint.

La funzionalità di quarantena è supportata nello stesso sito SharePoint del file sottoposto a scansione e anche in altre posizioni SharePoint, tra cui altri archivi SharePoint. Tuttavia, il rilascio dalla quarantena è supportato solo all'interno dello stesso sito SharePoint del file in quarantena.

Con Network Protect attivato, viene visualizzata una scheda nella pagina **Aggiungi target SharePoint** che contiene le opzioni di riparazione Network Protect. Per utilizzare Network Protect, è necessario possedere una politica e una regola di risposta configurate nella console di amministrazione Enforce Server. Inoltre, le credenziali di scansione (nome utente e password) devono essere presenti nella scheda **Aggiungi destinazione file system** per questo target.

Note:

- Per mettere in quarantena file di SharePoint utilizzando Network Protect, gli utenti esistenti devono prima disinstallare il plug-in Symantec Data Loss Prevention SharePoint Quarantine FlexResponse.
- Per sbloccare file SharePoint riservati dalla quarantena, si deve proseguire con l'installazione della versione di SharePoint Symantec Data Loss Prevention dal plug-in Quarantine FlexResponse.
- Per informazioni sull'installazione e la disinstallazione dei plug-in FlexResponse, fare riferimento alla *Symantec Data Loss Prevention Guida all'implementazione del plug-in SharePoint Quarantine FlexResponse*

Per configurare Network Protect per i server SharePoint

- 1 Creare una politica con una regola di risposta. Accedere a **Gestisci > Politiche > Regole di risposta** e fare clic su **Aggiungi regola di risposta**.
Vedere ["Informazioni sulle regole di risposta"](#) a pagina 1468.
- 2 Selezionare **Risposta automatica**.
- 3 Fare clic su **Avanti**.

4 Per **Azione**, selezionare **Network Protect: metti file in quarantena**.

Facoltativamente è possibile lasciare un file marker al posto del file che è stato rimosso selezionando la casella di controllo **File marker**. Inserire il testo del marker nella casella **Testo marker**. Il file di marker è un file di testo. Il testo del marker può contenere variabili sostitutive. Far clic all'interno della casella **Testo marker** per visualizzare un elenco di variabili di inserimento.

Il nome del file marker è il nome di file originale più un'estensione .txt. Le estensioni di file predefinite conservate sono elencate nel file di proprietà

`ProtectRemediation.properties`. Se il file originale era di un altro tipo, il file originale viene spostato nell'area di quarantena. Le estensioni di file conservate includono `txt`, `doc`, `xls`, `ppt`, `java`, `c`, `cpp`, `h` e `js`. Ad esempio, un file denominato `myfile.pdf` avrebbe un nome di file del marker `myfile.pdf.txt`.

È possibile creare una nuova sottodirectory per i file messi in quarantena da ogni scansione (il valore predefinito). È possibile modificare il valore predefinito e aggiungere le informazioni di scansione al nome del file (versione) in una directory di quarantena.

Modificare il file di proprietà `ProtectRemediation.properties` per modificare il valore predefinito.

Nota: Solo Network Protect consente di mettere in quarantena file riservati. Per sbloccare file riservati dalla quarantena, installare e configurare la versione di SharePoint dal plug-in Quarantine FlexResponse. Per ulteriori informazioni, consultare la *Guida all'implementazione del plug-in SharePoint Quarantine FlexResponse di Symantec Data Loss Prevention*.

5 Fare clic su **Salva**.

6 Aggiungere una nuova politica o modificare una politica esistente.

Vedere ["Configurazione di politiche"](#) a pagina 422.

7 Fare clic sulla scheda **Risposta**.

8 Nel menu a discesa, selezionare una delle regole di risposta create in precedenza.

9 Fare clic su **Aggiungi regola di risposta**.

Tale regola di risposta specifica quindi la risposta automatica quando la politica attiva un incidente durante la scansione di un file.

Possono esistere diverse regole di risposta con diverse condizioni per una politica.

10 Creare un target del server SharePoint Network Discover o modificare un target esistente.

Vedere ["Configurazione ed esecuzione delle scansioni dei server SharePoint"](#) a pagina 1950.

- 11 Con Network Protect attivato nella licenza, una scheda **Proteggi** viene visualizzata nella pagina target **SharePoint**, che contiene le opzioni di riparazione di Network Protect.

In **Riparazione protezione consentita**, selezionare l'opzione **Quarantena**.

- 12 In **Quarantena su SharePoint**, specificare la posizione di SharePoint in cui i file vengono messi in quarantena e anche le credenziali di accesso in scrittura per la posizione.

Se necessario, è possibile selezionare una credenziale denominata dall'archivio credenziali nel menu a discesa **Usa credenziali salvate**.

- 13 In **Credenziale di protezione**, specificare la credenziale di accesso scrittura per la posizione del file di cui è stata eseguita la scansione.

Per spostare i file per la quarantena durante la riparazione, la definizione del target di Network Discover deve avere accesso in scrittura sia per la posizione di quarantena sia per la posizione del file originale. Specificare il percorso (posizione) in cui i file vengono copiati o messi in quarantena. Digitare il nome utente e la password di accesso scrittura per tale posizione.

Normalmente, le condivisioni sottoposte a scansione richiedono solo credenziali di accesso in lettura.

Specificare la credenziale di accesso in scrittura della condivisione, se diversa da quella di accesso in lettura.

Se necessario, è possibile selezionare una credenziale denominata dall'archivio credenziali nel menu a discesa **Usa credenziali salvate**.

Nota: L'azione della regola di risposta automatica **Network Protect: File in quarantena** permette a Symantec Data Loss Prevention di mettere in quarantena file riservati memorizzati in archivi Microsoft SharePoint 2016 e 2013, senza dover installare la soluzione SharePoint.

Installazione della soluzione SharePoint su front end Web in un gruppo

Per eseguire la scansione di un target SharePoint utilizzando Network Discover, è necessario installare la soluzione Symantec SharePoint sui front end Web in un gruppo.

Il target SharePoint in esecuzione su Network Discover comunica con la soluzione SharePoint e recupera il contenuto dopo l'autenticazione del target con SharePoint. È possibile configurare l'applicazione per l'uso di SSL se è richiesto il trasferimento protetto di dati tra Network Discover e i server SharePoint.

Per il processo di installazione della soluzione SharePoint sono necessarie specifiche autorizzazioni.

Vedere ["Privilegi di accesso per le scansioni SharePoint"](#) a pagina 1949.

Symantec SharePoint è una soluzione con versione e non è compatibile con le versioni precedenti. Se si esegue l'upgrade da Symantec Data Loss Prevention versione 14.x o versione precedente, è necessario disinstallare la soluzione SharePoint corrente e installare la versione 15.1. [Tabella 68-2](#) elenca la versione della soluzione SharePoint compatibile con la versione in uso di Symantec Data Loss Prevention.

Tabella 68-2 Compatibilità con le versioni della soluzione Symantec SharePoint

Versione della soluzione Symantec SharePoint	Versioni di Symantec Data Loss Prevention compatibili
Nessun numero di versione	Da 11.0 a 11.5
11.5.1	11.5.1
11.6	11.6, 11.6.1, 11.6.2
12.0	12.0, 12.0.1
12.5	12.5, 12.5.1, 12.5.2
14.0	14.0, 14.0.1, 14.0.2
14.5	14.5, 14.5 MP1
14.6	14.6, 14.6 MP1
15.0	15.0, 15.0 MP1
15.1	15.1

Per installare la soluzione Symantec SharePoint

- 1 Copiare il programma di installazione della soluzione SharePoint `Symantec_DLP_Solution_15.1.exe` in una directory temporanea sul front-end Web di SharePoint. Questo file si trova nella directory `DLP_Home\New_Installs\SharePoint`, dove `DLP_Home` è il nome della directory in cui è stato decompresso il software Symantec Data Loss Prevention.
- 2 Avviare il servizio Amministrazione Windows SharePoint Services sul server SharePoint. Sul server SharePoint, fare clic su **Start > Programmi > Strumenti di amministrazione > Amministrazione centrale SharePoint**.
- 3 Fare doppio clic sul file `Symantec_DLP_Solution_15.1.exe`. Il programma di installazione della soluzione Symantec Data Loss Prevention viene avviato.

- 4 Fare clic su **Avanti**. Il programma di installazione esegue una serie di verifiche preliminari.
 Se una di queste verifiche non riesce, correggere il problema e riavviare il programma di installazione.
 Fare clic su **Avanti**.
- 5 Accettare il contratto di licenza di Symantec e fare clic su **Avanti**.
- 6 Il programma di installazione copia i file e distribuisce la soluzione a tutte le applicazioni Web nel gruppo SharePoint.
- 7 Dopo l'installazione, verificare che la soluzione SharePoint sia stata correttamente distribuita al server o al gruppo di server.
- 8 Connettersi a **Amministrazione centrale SharePoint**. Sul server SharePoint, selezionare **Start > Programmi > Strumenti di amministrazione > Amministrazione centrale SharePoint**.
- 9 Per SharePoint 2007, fare clic sulla scheda **Operazioni**. Nella sezione **Configurazione globale**, selezionare **Gestione soluzioni**.
- 10 Per SharePoint 2010, 2013 e 2016, fare clic su **Impostazioni di sistema**. Quindi selezionare **Gestisci soluzioni farm**.
- 11 Verificare la distribuzione. Se la soluzione è installata correttamente, l'elenco include **symantec_dlp_solution.wsp**.
- 12 Se la soluzione deve essere rimossa, utilizzare le funzionalità di ritiro e annullamento della distribuzione di SharePoint.

Attivazione della scansione SharePoint senza installare la soluzione SharePoint

È possibile attivare la scansione SharePoint senza installare la soluzione SharePoint del front-end Web della farm SharePoint. È possibile adottare questo approccio se si dispone di più farm SharePoint in reti isolate, ad esempio.

La scansione dei repository SharePoint senza utilizzare la soluzione SharePoint comporta le seguenti limitazioni:

- Non è possibile utilizzare un'applicazione Web come radice dei contenuti per la scansione. È invece necessario estrarre manualmente le raccolte di siti da utilizzare come radici dei contenuti.
 Vedere ["Per enumerare gli URL di raccolta siti"](#) a pagina 1961.
- I dettagli degli incidenti SharePoint non includono informazioni relative alle autorizzazioni.
- Non è possibile utilizzare le azioni FlexResponse server per riparare gli incidenti SharePoint, compresa l'azione di risposta SharePoint Encrypt.

Nota: L'azione della regola di risposta smart **Quarantena Network Protect SharePoint** e l'azione della regola di risposta automatica **Network Protect: File in quarantena** consentono a Symantec Data Loss Prevention di mettere in quarantena i file riservati memorizzati in archivi Microsoft SharePoint 2013 e 2016 senza dover installare la soluzione SharePoint.

Per attivare la scansione SharePoint senza installare la soluzione SharePoint

- 1 Su ciascun server di rilevamento Discover che si desidera utilizzare per eseguire la scansione degli archivi SharePoint senza utilizzare la soluzione SharePoint, aprire il file `.../Protect/config/Crawler.properties` in un editor di testo.
- 2 Aggiungere `sharepointcrawler.use.plugin=false` al file `Crawler.properties`.
- 3 Salvare il file modificato.
- 4 Riciclare il server di rilevazione Discover.

Per enumerare gli URL di raccolta siti

- 1 Aprire Windows PowerShell e immettere il seguente comando, dove "http://MyWebApp" è l'URL dell'applicazione Web (interruzione di riga aggiunta per la leggibilità):

```
Get-SPWebApplication http://MyWebApp | Get-SPSite | Select Url |  
Out-File -FilePath "C:\spSites.txt"
```

- 2 Utilizzare il file `spSites.txt` per immettere le raccolte siti durante la configurazione del target Discover.

Configurazione delle scansioni SharePoint per l'uso dell'autenticazione Kerberos

Se lo si desidera, una scansione SharePoint può utilizzare l'autenticazione Kerberos.

SharePoint deve già essere installato per interagire con l'autenticazione Kerberos.

Il Discover Server deve quindi essere configurato per comunicare con il Key Distribution Center (KDC) e il server SharePoint.

Per configurare il Discover Server per l'autenticazione Kerberos

- 1 Creare un file denominato `krb5.conf` che contiene l'area di autenticazione e le informazioni KDC. In Windows, questo file si chiama solitamente `krb5.ini`. Un file di esempio si trova nella cartella `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (in una configurazione predefinita di Symantec Data Loss Prevention su Windows).

Vedere ["Creazione del file di configurazione per l'integrazione con Active Directory"](#) a pagina 142.

- 2 Copiare questo file nel Discover Server nella cartella `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\jre\lib\security\` (in una configurazione predefinita di Symantec Data Loss Prevention su Windows).
- 3 Aggiornare l'area di autenticazione e i parametri del server della directory predefiniti (aree di autenticazione) in questo file.

```
[libdefaults]
    default_realm = ENG.COMPANY.COM

[realms]
ENG.COMPANY.COM = {
    kdc = engADserver.emg.company.com
}
MARK.COMPANY.COM = {
    kdc = markADserver.emg.company.com
}
```

Vedere ["Creazione del file di configurazione per l'integrazione con Active Directory"](#) a pagina 142.

- 4 Sul Discover Server, aggiornare il file `Protect.properties` nella cartella `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (in una configurazione predefinita di Symantec Data Loss Prevention su Windows). Aggiornare la proprietà che punta al file `krb5.ini` aggiornato.

```
# Kerberos Configuration Information
java.security.krb5.conf=C:\Program Files\Symantec\Data Loss Prevention\Enforce Ser
```

Risoluzione dei problemi delle scansioni di SharePoint

[Tabella 68-3](#) fornisce suggerimenti per la risoluzione dei problemi con le scansioni SharePoint.

Vedere ["Risoluzione dei problemi delle scansioni di griglia"](#) a pagina 1882. fornisce suggerimenti per la risoluzione dei problemi con le scansioni delle griglie nei server SharePoint.

Tabella 68-3 Risoluzione dei problemi delle scansioni di SharePoint

Problema	Procedura consigliata
Se viene specificato un URL interno di SharePoint, solo la raccolta di siti predefinita viene sottoposta a scansione.	Specificare l'URL pubblico per il sito SharePoint. Tutte le raccolte di siti vengono sottoposte a scansione.
Nessuna raccolta di siti, o solo la raccolta di siti predefinita, viene sottoposta a scansione quando il sito di Discover Server e di SharePoint sono in domini differenti.	<p>Specificare l'URL della raccolta di siti/sito/applicazione Web con un nome di dominio completo.</p> <p>Per convalidare l'accesso da Discover Server, provare ad accedere all'URL di SharePoint da un browser. Se il nome breve non funziona, provare a usare il nome completo del dominio.</p> <p>Soltanto la raccolta di siti predefinita è sottoposta a scansione se l'URL dell'applicazione Web non contiene il nome di dominio completo.</p>
I byte segnalati come sottoposti a scansione non corrispondono al numero di byte nel contenuto.	<p>Per migliorare la prestazione, le statistiche di scansione non comprendono gli oggetti nelle cartelle che vengono ignorate (filtrate).</p> <p>Il contenuto dinamico, come i file <code>.aspx</code>, può cambiare dimensione.</p> <p>È possibile scegliere l'impostazione <code>Discover.countAllFilteredItems</code> di Advanced Server per ottenere statistiche di scansione più accurate.</p> <p>Vedere "Impostazioni server avanzate" a pagina 279.</p>
Le scansioni non funzionano correttamente con Kerberos configurato.	<p>In caso di difficoltà con l'autenticazione Kerberos, controllare i punti seguenti:</p> <ul style="list-style-type: none"> ■ Assicurarsi che la risoluzione DNS per il controller di dominio e i server di SharePoint funzioni correttamente dal server di rilevazione. ■ Assicurarsi che l'integrazione del client sia abilitata per la zona in cui l'applicazione Web viene eseguita. ■ Considerare di aggiungere le aree di autenticazione di dominio al file <code>C:/SymantecDLP/jre/lib/security/krb5.ini</code>. Ad esempio: <pre>[domain_realms] .MYDOMAIN.COM=MYDOMAIN.COM</pre>
Le scansioni che utilizzano l'autenticazione basata su attestazioni non riescono a causa di un errore di connessione ADFS.	Verificare che il Nome servizio federativo sia stato inserito correttamente. Il Nome servizio federativo è l'URL del server ADFS. È possibile trovare il nome corretto nella sezione Proprietà dei servizi federativi della console ADFS.

Problema	Procedura consigliata
Risoluzione dei problemi generali	Symantec Data Loss Prevention registra gli errori di scansione nel registro di scansione e nei registri del lettore di file.

Impostazione delle scansioni di server Exchange

Il capitolo contiene i seguenti argomenti:

- [Impostazione della scansione di server di repository Exchange](#)
- [Informazioni sulle scansioni di server Exchange](#)
- [Destinazioni Exchange Server supportate](#)
- [Configurazione della scansioni del server Exchange](#)
- [Configurazione delle scansioni Exchange per utilizzare l'autenticazione Kerberos](#)
- [Configurazioni di esempio e casi di utilizzo per le scansioni Exchange](#)
- [Risoluzione dei problemi delle scansioni di Exchange](#)

Impostazione della scansione di server di repository Exchange

È possibile eseguire la scansione di server Exchange 2007 SP2 (e successive), 2010, 2013 e 2016 (on-site).

Tabella 69-1 Impostazione della scansione di server Exchange

Passo	Azione	Descrizione
1	Verificare che i servizi Web di Exchange e il servizio Autodiscover siano attivati sul server Exchange e siano accessibili al server Network Discover.	Per informazioni sui servizi Web di Exchange e sul servizio Autodiscover, vedere la documentazione di Microsoft Exchange.
2	Se è necessario l'accesso protetto tra Discover Server e i servizi Web di Exchange o il server Active Directory, configurare HTTPS e LDAPS.	Per impostazione predefinita, Symantec Data Loss Prevention consente connessioni HTTPS solo al server Active Directory e ai servizi Web di Exchange. Per consentire connessioni HTTP, impostare <code>Discover.Exchange.UseSecureHttpConnections</code> in Dettagli server > Impostazioni avanzate del server su <code>false</code> . Vedere "Impostazioni server avanzate" a pagina 279.
3	Verificare che le credenziali utente di Exchange siano in grado di rappresentare tutte le cassette postali che si desidera sottoporre a scansione.	Per informazioni sull'attivazione della rappresentazione per le credenziali, vedere la documentazione di Microsoft Exchange.
4	Accedere a Gestisci > Scansione Discover > Target di Discover per creare un target di Exchange e configurare le scansioni dei server di Exchange.	Vedere "Configurazione della scansioni del server Exchange" a pagina 1968.
5	Configurare altre eventuali opzioni di scansione per il target Exchange.	Vedere "Opzioni di configurazione dei target di scansione di Network Discover/Cloud Storage Discover" a pagina 1830.
6	Avviare la scansione del server Exchange.	Accedere a Gestisci > Scansione Discover > Target di Discover . Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.
7	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Gestione delle scansioni target di Network Discover/Cloud Storage Discover" a pagina 1853.

Informazioni sulle scansioni di server Exchange

È possibile eseguire la scansione di server Exchange 2007 SP2 (e successive), 2010, 2013 e 2016 (on-site). La scansione di Exchange non richiede un agente sul server Exchange e non effettua la ricerca in ciascun server Exchange. Mediante il servizio di individuazione automatica, recupera informazioni sul server e la casella postale di Exchange da Active Directory ed estrae i dati direttamente dai server Exchange appropriati mediante il protocollo SOAP (Simple Object Access Protocol). Per ulteriori informazioni sul servizio di individuazione automatica di Exchange vedere <http://technet.microsoft.com/en-us/library/bb124251.aspx>.

Il server Network Discover individua una gamma di dati riservati esposti sui server Exchange, inclusi i messaggi di posta elettronica, gli elementi del calendario, i contatti, il journal e gli elementi contrassegnati. Network Discover non esegue la scansione di dispositivi o cassette postali della sala.

La comunicazione è sicura quando il server Exchange è configurato per l'uso di SSL (HTTPS). La comunicazione con il server Active Directory è sicura quando è configurata per l'uso di LDAPS.

Per HTTPS, la convalida del certificato SSL del server non è l'impostazione predefinita. Per abilitare la convalida del certificato SSL del server, attivare l'impostazione avanzata `Discover.ValidateSSLCertificates`. Quindi importare il certificato SSL del server in Discover Server.

Per impostazione predefinita, Network Discover usa connessioni protette ai server Exchange e Active Directory. È possibile disattivare l'accesso protetto a Exchange e Active Directory impostando l'opzione `Discover.Exchange.UseSecureHttpConnections` in **Dettagli server** > **Impostazioni server avanzate** su `false`.

Vedere ["Impostazioni server avanzate"](#) a pagina 279.

Vedere ["Importazione di certificati SSL in Enforce o Discover server"](#) a pagina 272.

Nota: Network Discover non supporta la scansione di target Exchange mediante i gruppi di distribuzione dinamici.

Destinazioni Exchange Server supportate

Symantec Data Loss Prevention supporta le seguenti destinazioni Exchange Server:

- Microsoft Exchange Server 2007 SP3 (obsoleto in Symantec Data Loss Prevention 15.1)
- Microsoft Exchange Server 2010 SP3
- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016 (on-site)

Per utilizzare il connettore servizi Web di Exchange, è necessario che i servizi Web di Exchange e il servizio Autodiscover siano attivati sul server Exchange e siano accessibili al server Network Discover.

È possibile eseguire la scansione degli oggetti dati archiviati nelle cartelle pubbliche, quali:

- Messaggi e-mail
- Allegati dei messaggi
- Documenti di Microsoft Word

- Fogli di calcolo Excel

La scansione Exchange opera anche sulla posta archiviata negli archivi personali di Exchange 2013 e 2016.

Configurazione della scansioni del server Exchange

Prima di eseguire una scansione, configurare un target seguendo la procedura descritta.

Per configurare un nuovo target per la scansione di un server Exchange

- 1 Selezionare **Gestisci > Scansione Discover > Target di Discover > Nuovo target > Server > Exchange**.
- 2 Nella scheda **Generale** immettere il nome di questo target di scansione.
- 3 Selezionare i gruppi di politiche che contengono le politiche per questa scansione.
- 4 Selezionare le opzioni di pianificazione.

Scegliere **Avvia processo di scansione come pianificato** per pianificare la scansione del target specificato. Selezionare un'opzione a partire dall'elenco a discesa di pianificazione per visualizzare ulteriori campi.

Selezionare **Sospendi scansione in questo periodo** per sospendere automaticamente le scansioni durante l'intervallo di tempo specificato. È possibile ignorare la sospensione della scansione di un target passando alla schermata Target di Discover e facendo clic sull'icona di avvio per la voce del target. Il periodo di sospensione rimane inalterato e tutte le scansioni future che vengono eseguite in base alla finestra di scansione vengono sospese come specificato. È inoltre possibile riavviare una scansione interrotta facendo clic sull'icona Continua relativa alla voce del target.

Vedere "[Pianificazione delle scansioni di Network Discover/Cloud Storage Discover](#)" a pagina 1833.

- 5 Nella scheda **Destinazione**, selezionare i Network Discover Server dove eseguire la scansione.

- 6 Nella scheda **Contenuto sottoposto a scansione** immettere le credenziali per la scansione.

Tutti i nomi utente Exchange devono includere il nome di dominio, ad esempio:

`DOMAIN_NAME\user_name`

Assicurarsi che le credenziali dell'utente fornite siano in grado di rappresentare tutte le cassette postali che si desidera sottoporre a scansione. Per informazioni sulla configurazione di Exchange Impersonation, vedere

<http://msdn.microsoft.com/en-us/library/bb204095.aspx>.

Vedere "Autenticazione tramite password per il contenuto sottoposto a scansione Network Discover" a pagina 1835.

- 7 Immettere un URL di destinazione per il server Microsoft Active Directory. Ad esempio, **ldaps://dc.domain.com:636**.

Nota: è possibile specificare solo un server Active Directory per ogni target di Discover.

- 8 Selezionare **Cartelle pubbliche** per eseguire la scansione di tutte le cartelle pubbliche sul server Exchange. L'utente con le credenziali specificate deve avere accesso a queste cartelle pubbliche.

Nota: negli ambienti Exchange misti in cui sono distribuiti i server Exchange 2007, 2010 e 2013, Network Discover esegue la scansione solo delle cartelle pubbliche della versione specificata dalle credenziali immesse nel target di Exchange Network Discover. Per esplorare le cartelle pubbliche nelle versioni 2007, 2010 e 2013 negli ambienti misti, creare un target di Network Discover separato per ciascuna versione.

È possibile selezionare questa opzione oltre a **Tutti gli utenti su server di directory** o **Utenti e gruppi di directory**.

- 9 Selezionare **Cassette postali** per eseguire la scansione delle cassette postali dell'utente sui server Exchange. Scegliere uno dei metodi seguenti per l'immissione delle voci da sottoporre a scansione sul server Exchange.

- **Tutti gli utenti su server di directory**

Se un server di directory è disponibile, selezionare **Server di directory** dall'elenco a discesa.

Per utilizzare questa opzione, selezionare la connessione del server di directory già specificata oppure fare clic sul collegamento **Crea nuova connessione directory** per configurare un'altra connessione di directory.

Vedere "Configurazione delle connessioni a server di directory" a pagina 162.

- **Utenti e gruppi di directory**

Se sono disponibili gruppi di utenti di directory, selezionare i gruppi da includere in questo target.

Per utilizzare questa opzione, i gruppi di directory devono essere configurati. Se non è configurato alcun gruppo di directory, fare clic sul collegamento **Crea nuovo gruppo di utenti** per passare alla pagina per configurare i gruppi di utenti di directory.

Vedere "[Configurazione di gruppi di utenti](#)" a pagina 847.

- **Specificare le cassette postali dell'utente da includere in questo target**

Immettere le cassette postali specifiche. I caratteri alfanumerici e i caratteri speciali seguenti sono consentiti nei nomi delle cassette postali:

! # \$ % ' - ^ _ ` { }

È possibile combinare questa opzione con gli utenti e i gruppi di directory. Non sono necessari gruppi di directory per l'opzione relativa alle cassette postali dell'utente.

- **Archivi personali**

Selezionare questa opzione per eseguire la scansione delle cassette postali dell'archivio personale di Exchange 2010 e 2013 per gli utenti specificati.

10 Nella scheda **Filtri** selezionare i filtri del percorso.

Utilizzare **Filtri di inclusione** e **Filtri di esclusione** per specificare gli elementi che Symantec Data Loss Prevention deve elaborare o ignorare. Se il campo è vuoto, Symantec Data Loss Prevention cerca una corrispondenza con tutti gli elementi. Se si immette un qualsiasi valore per il filtro di inclusione, Symantec Data Loss Prevention sottopone a scansione solo gli elementi corrispondenti al filtro specificato. Delimitare le voci con una virgola, ma non utilizzare spazi.

È possibile fornire i filtri mediante l'utilizzo di espressioni regolari o percorsi relativi alla posizione del sito di Exchange. I filtri possono includere un nome di una cartella o di un file. Tutti i filtri del percorso eseguono la distinzione tra maiuscole e minuscole.

Exchange può aggiungere un identificatore e-mail alla fine del percorso. Per cercare una corrispondenza con il filtro, aggiungere un carattere jolly alla fine. Ad esempio, per filtrare in base all'"elemento della cartella pubblica di esempio", utilizzare il filtro seguente:

```
*/folder/*/sample public folder item*
```

È possibile fornire i filtri mediante l'utilizzo di espressioni regolari o percorsi relativi alla posizione del sito di Exchange. I filtri possono includere una raccolta di siti, un sito, un sottosito, una cartella, un nome di file o un'estensione di file. Tutti i filtri del percorso eseguono la distinzione tra maiuscole e minuscole.

Per **Filtri di inclusione** la corrispondenza delle espressioni regolari viene applicata ai file, ma non alle cartelle.

Per **Filtri di esclusione** la corrispondenza delle espressioni regolari viene applicata ai file e alle cartelle.

Soltanto il percorso fino al primo "?" o "*" viene considerato in caso di corrispondenza con una cartella o un file.

Quando tutti i filtri del percorso specificati sono relativi, la cartella corrispondente viene ignorata e le statistiche di scansione non includono gli elementi nelle cartelle ignorate.

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

11 Nella scheda **Filtri** selezionare i filtri delle dimensioni.

I filtri di dimensione consentono di escludere elementi dal processo di corrispondenza in base alla relativa dimensione. Symantec Data Loss Prevention include solo gli elementi che corrispondono ai filtri delle dimensioni specificati. Se si lascia questo campo vuoto, Symantec Data Loss Prevention cerca la corrispondenza con gli elementi di tutte le dimensioni.

Vedere ["Filtraggio dei target di Discover per dimensione dell'oggetto"](#) a pagina 1843.

- 12 Nella scheda **Filtri** selezionare una scansione differenziale (opzionale).

Selezionare **Esegui scansione solo di file aggiunti o modificati dopo l'ultima scansione completa** in modo che Symantec Data Loss Prevention esegua la scansione solo degli elementi o dei documenti che sono stati aggiunti o modificati dall'ultima scansione completa. La prima scansione deve essere una scansione completa (base iniziale). Una scansione completa si verifica se si seleziona questa opzione prima che Symantec Data Loss Prevention esegua una scansione di questo target per la prima volta.

- 13 Selezionare i filtri della data.

I filtri della data consentono di includere gli elementi per il processo di corrispondenza in base alle date. Viene eseguita la scansione di tutti gli elementi che corrispondono ai filtri della data specificati.

vedere ["Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica"](#) a pagina 1844.

- 14 Selezionare la scheda **Avanzate** affinché le opzioni ottimizzino la scansione. Nella scheda **Avanzate** è possibile configurare le opzioni di limitazione e impostare la modalità di inventario per la scansione.

■ **Opzioni di limitazione**

È possibile utilizzare la limitazione per limitare la larghezza di banda usata dalla scansione o il carico sul server Exchange. Specificare il numero massimo di elementi da elaborare al minuto per server di rilevazione o il numero massimo di byte da elaborare al minuto per server di rilevazione. Per i byte, specificare l'unità di misura dall'elenco a discesa. Le opzioni sono byte, KB (kilobyte) o MB (megabyte).

■ **Scansione inventario**

Immettere il numero di incidenti da generare prima di completare la scansione. Per verificare se su un target esistono dati riservati, senza eseguirne la scansione completa, configurare la modalità di inventario per la scansione.

Dopo che la soglia di incidenti è stata raggiunta, la scansione viene interrotta. Poiché il processo è asincrono, è possibile che venga creato un numero di incidenti superiore a quello specificato nella soglia di incidenti.

Configurazione delle scansioni Exchange per utilizzare l'autenticazione Kerberos

Se lo si desidera, una scansione Exchange può utilizzare l'autenticazione Kerberos.

Exchange deve già essere installato per interagire con l'autenticazione Kerberos.

Il Discover Server deve poi essere configurato per comunicare con il Key Distribution Center (KDC) ed Exchange Server.

Per configurare Discover Server per autenticazione Kerberos

- 1 Creare un file denominato `krb5.conf` che contiene l'area di autenticazione e le informazioni KDC. In Windows, questo file si chiama solitamente `krb5.ini`. Un file di esempio si trova nella cartella `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (in una configurazione predefinita di Symantec Data Loss Prevention su Windows).

Vedere ["Creazione del file di configurazione per l'integrazione con Active Directory"](#) a pagina 142.

- 2 Copiare questo file nel Discover Server nella cartella `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\jre\lib\security\` (in una configurazione predefinita di Symantec Data Loss Prevention su Windows).
- 3 Aggiornare l'area di autenticazione e i parametri del server della directory predefiniti (aree di autenticazione) in questo file.

```
[libdefaults]
    default_realm = ENG.COMPANY.COM

[realms]
ENG.COMPANY.COM = {
    kdc = engADserver.emg.company.com
}
MARK.COMPANY.COM = {
    kdc = markADserver.emg.company.com
}
```

Vedere ["Creazione del file di configurazione per l'integrazione con Active Directory"](#) a pagina 142.

- 4 Sul Discover Server, aggiornare il file `Protect.properties` nella cartella `C:\Programmi\Symantec\Data Loss Prevention\Enforce Server\15.1\Protect\config` (in una configurazione predefinita di Symantec Data Loss Prevention su Windows). Aggiornare la proprietà che punta al file `krb5.ini` aggiornato.

```
# Kerberos Configuration Information
java.security.krb5.conf=C:\Program Files\Symantec\Data Loss Prevention\Enforce Ser
```

Configurazioni di esempio e casi di utilizzo per le scansioni Exchange

La [Tabella 69-2](#) elenca le opzioni da selezionare nella scheda **Contenuto sottoposto a scansione** durante la configurazione di un target Exchange.

Verificare che le credenziali utente fornite siano in grado di rappresentare tutte le cassette postali che si desidera sottoporre a scansione. Per informazioni sulla configurazione della rappresentazione di Exchange, vedere <http://msdn.microsoft.com/en-us/library/bb204095.aspx>.

Tabella 69-2 Casi di utilizzo della scansione di Exchange

Caso di utilizzo	Descrizione
Scansione di tutte le cassette postali degli utenti e le cartelle pubbliche	<p>Selezionare le seguenti opzioni nell'interfaccia utente:</p> <ul style="list-style-type: none"> ■ Cartelle pubbliche ■ Cassette postali > Tutti gli utenti su server di directory <p>Le credenziali devono avere l'autorizzazione per rappresentare tutte le cassette postali da sottoporre a scansione.</p>
Scansione di tutte le cassette postali degli utenti (ma non delle cartelle pubbliche).	<p>Selezionare Cassette postali > Tutti gli utenti su server di directory nell'interfaccia utente.</p> <p>Le credenziali devono avere l'autorizzazione per rappresentare tutte le cassette postali da sottoporre a scansione.</p>
Scansione di tutte le cartelle pubbliche.	<p>Selezionare Cartelle pubbliche nell'interfaccia utente.</p>
Scansione di gruppi o utenti specifici.	<p>Selezionare Cassette postali > Utenti e gruppi di directory nell'interfaccia utente.</p> <p>Per esplorare un gruppo di directory, selezionarlo tra i gruppi dell'elenco. Tutte le cassette postali utente del gruppo vengono sottoposte a scansione. È possibile fare clic su Crea nuovo gruppo di utenti per creare un nuovo gruppo di directory.</p> <p>Per eseguire la scansione di utenti specifici, inserire un elenco di valori separati da virgole di nomi di cassetta postale degli utenti.</p> <p>Le credenziali devono avere l'autorizzazione per rappresentare tutte le cassette postali da sottoporre a scansione.</p>
Scansione di un archivio personale di Exchange 2010.	<p>Selezionare Cassette postali > Tutti gli utenti su server di directory > Archivi personali o Cassette postali > Utenti e gruppi di directory > Archivi personali nell'interfaccia utente. Se necessario, specificare quali cassette postali sottoporre a scansione. Network Discover esegue la scansione degli archivi personali associati alle cassette postali specificate.</p>

Risoluzione dei problemi delle scansioni di Exchange

In caso di problemi con le scansioni di Exchange è possibile trovare ulteriori informazioni qui:

- `FileReader0.log`: questo file registra tutte le richieste e le risposte SOAP tra Network Discover e i servizi Web di Exchange.

Per configurare il registro del lettore di file in modo che elenchi le richieste SOAP, modificare il file `FileReaderLogging.properties` nel modo seguente:

```
java.util.logging.FileHandler.level = FINEST
org.apache.cxf.interceptor.LoggingInInterceptor.level = FINEST
org.apache.commons.beanutils.converters.level = WARNING
```

Vedere ["File di registro operativi"](#) a pagina 336.

Nota: È presente solo la riga `java.util.logging.FileHandler.level = FINEST`. È necessario aggiungere le altre righe come specificato nell'esempio in alto.

- Registri di Exchange: è possibile trovare utili informazioni di risoluzione dei problemi nei registri creati da Microsoft Exchange Server.

Informazioni sui rilevatori Network Discover

Il capitolo contiene i seguenti argomenti:

- [Configurazione della scansione di server di Microsoft Exchange](#)
- [Funzionamento dei rilevatori di Network Discover](#)
- [Risoluzione dei problemi dei rilevatori](#)
- [Processi del rilevatore](#)
- [Struttura delle directory di installazione del rilevatore](#)
- [File di configurazione del sistema di scansione](#)
- [Opzioni di configurazione del controller del rilevatore](#)

Configurazione della scansione di server di Microsoft Exchange

Il rilevatore Exchange è un'utilità standalone che consente di estrarre dati da Microsoft Exchange e di inviare i dati su Network Discover per l'elaborazione dei contenuti.

Il rilevatore Exchange accede alle cassette postali cliente sul server Exchange mediante un client Outlook connesso.

Il rilevatore Exchange consente di specificare quale profilo MAPI dovrebbe essere utilizzato per estrarre dati dalla struttura di Exchange. Il rilevatore Exchange utilizza Profili per collegarsi all'Exchange Server attraverso l'interfaccia MAPI. In seguito pubblica i file su Discover.

È possibile utilizzare il rilevatore Exchange per eseguire le seguenti attività:

- Eseguire la scansione di cartelle pubbliche mediante un specifico account per trovare dati riservati.
- Eseguire la scansione di tutti gli elementi delle cassette postali mediante un account di amministratore che può accedere a tutte le cassette postali.
- Eseguire la scansione di cassetta postale dell'utente mediante l'account di amministratore.
- Eseguire la scansione di una cassetta postale di un singolo utente con nome utente e password conosciuti.

Per configurare la scansione di server Microsoft Exchange, completare il seguente processo:

Tabella 70-1 Configurazione di un rilevatore Exchange

Passaggio	Azione	Descrizione
1	Verificare che la versione del server Exchange sia 2003 o 2007.	
2	Installare il rilevatore Exchange su un computer con Microsoft Outlook 2003 o 2007 installato e un profilo valido di Outlook configurato.	
3	Configuri <code>ProfileName</code> e l'impostazione <code>perDNMailbox</code> .	
4	Eseguire qualsiasi configurazione manuale modificando i file di configurazione e proprietà.	
5	Sull'Enforce Server, aggiungere un nuovo target di Exchange.	Vedere "Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover" a pagina 1826.
6	Avviare la scansione di Exchange. Avviare il rilevatore sul computer rilevatore e avviare inoltre la scansione sull'Enforce Server.	Vedere "Avvio della scansione del file system" a pagina 1990.
7	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Risoluzione dei problemi dei rilevatori" a pagina 1978.

Funzionamento dei rilevatori di Network Discover

I rilevatori sono le applicazioni stand-alone che raccolgono contenuti e metadati da un archivio e li inviano a Network Discover per l'elaborazione.

Ad esempio, in una configurazione a due livelli potrebbe esserci un Enforce Server e un server Network Discover connesso a un server di Documentum su cui è installato un rilevatore.

È possibile eseguire le seguenti attività sui computer di questa configurazione:

- In Enforce server, definire la destinazione di scansione (in questo esempio, Documentum).
- Sul server di Documentum, installare il rilevatore Documentum, configurare il rilevatore per pubblicare contenuti nel server Network Discover e avviare (o arrestare) un rilevatore.
- Sull'Enforce Server, avviare o arrestare la scansione di una destinazione (con l'icona di avvio) e visualizzare il report degli incidenti.

Il sistema del rilevatore comunica con il server Network Discover utilizzando il protocollo HTTP.

Quando il rilevatore viene eseguito, esegue le seguenti attività:

- Si connette all'archivio in modalità nativa e analizza l'archivio per leggere il contenuto e i metadati.
- Estrae il testo e alcuni metadati.
- Pubblica le informazioni estratte sul server Network Discover.
- Network Discover analizza il testo e i metadati e applica il rilevamento.

Vedere ["Informazioni su Network Discover/Cloud Storage Discover"](#) a pagina 1819.

Risoluzione dei problemi dei rilevatori

Dopo l'avvio di una scansione, i contenuti e i metadati vengono estratti dall'archivio. Quindi questi contenuti vengono trasferiti al controller di scansione e al server Network Discover.

Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.

Se un rilevatore non elabora gli oggetti, fare ricorso ai seguenti suggerimenti:

Tabella 70-2 Suggerimenti per la risoluzione dei problemi del rilevatore

Problema	Suggerimenti
Il rilevatore non è in esecuzione.	<p>Verificare che il rilevatore sia stato installato correttamente.</p> <p>Sul sistema in cui il rilevatore è stato installato, assicurarsi che i processi del rilevatore siano in esecuzione.</p> <p>Vedere "Processi del rilevatore" a pagina 1980.</p>
Gli incidenti non vengono visualizzati nei report.	<p>Verificare che il target di scansione sia configurato correttamente. I rilevatori possono inviare contenuti solo a un target dello stesso tipo. Più rilevatori dello stesso tipo possono indirizzare contenuti in una scansione di Network Discover di quel tipo.</p> <p>Verificare che la scansione non sia bloccata.</p>

Problema	Suggerimenti
<p>La scansione non viene avviata.</p>	<p>Cercare nella cartella <i>in uscita</i>.</p> <p>Vedere "Struttura delle directory di installazione del rilevatore" a pagina 1981.</p> <p>Se un dato rilevatore non invia un contenuto su Network Discover tale contenuto viene messo in coda nella cartella <i>in uscita</i>.</p> <p>Gli elementi che vengono visualizzati e nascosti in questa cartella indicano l'avanzamento normale.</p>

Problema	Suggerimenti
La ricerca appare bloccata.	<p>Se un rilevatore non riesce a inviare un contenuto a Network Discover il contenuto del rilevatore viene messo in coda nel sistema del rilevatore. Il sistema del rilevatore deve avere accesso al server Network Discover. Gli avvisi di sistema come quello relativo a spazio su disco ridotto o a servizi non attivi dovrebbero essere eliminati in entrambi i sistemi prima dell'installazione.</p> <p>Per verificare il contenuto ricevuto sul server Network Discover, visualizzare la pagina delle statistiche della scansione. Per visualizzare le statistiche di scansione, fare clic sulla scansione in esecuzione nell'elenco delle scansioni target.</p> <p>Verificare che le informazioni di scansione si spostino nel processo di scansione controllando i registri e le directory temporanee.</p> <p>Vedere "Struttura delle directory di installazione del rilevatore" a pagina 1981.</p> <p>Se la scansione è bloccata, controllare le seguenti posizioni sul computer del rilevatore per diagnosticare il problema:</p> <ul style="list-style-type: none">■ La cartella <code>/logs</code> La cartella <code>/scanner_typeScanner/logs</code> ha lo stato di avvio, arresto e connessione del rilevatore su Network Discover. Informazioni simili sono presenti nella finestra della console. Controllare i file di registro per verificare che un rilevatore sia correttamente in esecuzione.■ La cartella <code>/failed</code> Gli elementi presenti nella cartella <code>/failed</code> indicano una mancata corrispondenza dei tipi di rilevatore tra il nuovo obiettivo e il rilevatore. Ad esempio, se è specificato un rilevatore Exchange nel nuovo target, ma il rilevatore è SharePoint, gli elementi vengono visualizzati nella cartella <code>/failed</code>.■ La cartella <code>/in uscita</code> Gli elementi che vengono visualizzati e nascosti in questa cartella indicano l'avanzamento normale. Se gli oggetti permangono in questa cartella e non vengono utilizzati (rimangono visualizzati), è indicato un problema nell'estrazione del testo e dei metadati. Se un dato rilevatore non invia un contenuto su Network Discover, tale contenuto viene messo in coda nella cartella <code>/in uscita</code>.■ La directory <code>/scanner_typeScanner/scanner</code> ha lo stato della connessione del rilevatore nell'archivio, nelle informazioni di ricerca per indicizzazione dell'archivio e nei dati recuperati.

Processi del rilevatore

Tabella 70-3 fornisce informazioni sui processi del rilevatore Network Discover in un sistema operativo Windows.

Tabella 70-3 Processi di Discover

Processi	Eseguibile	Descrizione
ScannerController	<i>scanner_typeScanner_Console.exe</i> o <i>scanner_typeScanner_Service.exe</i>	Processo che configura e controlla il connettore, invia il contenuto al server Network Discover e invia il messaggio di fine scansione a Network Discover.
Connettore	<i>scanner_typeScanner.exe</i>	Processo che estrae documenti e metadati dall'archivio.
ImportModule	ImportSlave.exe	Processo che estrae testo e metadati dai documenti scaricati dal connettore.
KeyView	KVoop.exe	Il processo KeyView esegue l'estrazione di testo e metadati da tipi di documento noti.
Binslave	BinSlave.exe	Processo che tenta di estrarre testo da tipi di documento sconosciuti.

Struttura delle directory di installazione del rilevatore

Tabella 70-4 descrive la struttura delle directory per i file di configurazione del rilevatore di Network Discover.

Tabella 70-4 Struttura delle directory di installazione

Percorso	Descrizione
<i>/tipo_scannerScanner</i>	
<i>....bin</i>	I file per l'esecuzione, l'avvio e l'arresto del rilevatore.
<i>.....Clean.exe</i>	Cancella tutti i file e registri temporanei nella directory <i>/scanner</i> .
<i>.....EncryptPassword.exe</i>	Può essere usato per crittografare i nomi utente e le password nel file <i>tipo_scannerScanner.cfg</i> .
<i>...../tipo_scannerScanner_Console.exe</i>	Lancia il rilevatore come applicazione console (con una finestra). Premere CTRL+C per arrestare il rilevatore.

Percorso	Descrizione
...../tipo_scannerScanner_Service.exe	Avvia il rilevatore come applicazione senza una finestra. In genere, questo avvio è usato solo quando il rilevatore è registrato ed eseguito come servizio Windows o UNIX.
....../config	I file di configurazione si trovano in questa directory.
...../ScannerController.properties	Il file di configurazione per ScannerController.
...../ScannerControllerLogging.properties	Il file di proprietà per la registrazione del rilevatore.
...../tipo_scannerScanner.cfg	Il file di configurazione per il connettore. Questo file viene copiato nella directory /scanner prima dell'avvio del processo secondario.
....../logs	Contiene i file di registro per il processo ScannerController.
....../outgoing	I file XML con contenuto e i metadati sono messi in coda in questa cartella prima di essere inviati al server Network Discover.
....../scanner	La directory contenente i file binari, di registro e temporanei.
...../outgoing	Alcuni connettori (ad esempio Exchange e SharePoint2003) non possono essere configurati per scrivere i file .idx nellacartella ./outgoing. Li scrivono invece nella cartella ./scanner/outgoing e ScannerController li sposta nella directory ./outgoing di modo che possano essere inviati al server Network Discover.
...../failed	Se il server Network Discover non può analizzare i file XML e restituisce un codice di errore 500, ScannerController sposta il documento XML all'origine dell'errore nella cartella ./failed.

File di configurazione del sistema di scansione

Le opzioni di configurazione possono essere modificate dopo l'installazione e prima che si inizi una scansione modificando i seguenti file sul sistema di scansione.

Nome del file

Attività di configurazione

`ScannerController.properties`

Nel file `ScannerController.properties`, è possibile configurare le seguenti opzioni:

- Definire l'informazione di connessione al server Network Discover.
- Comprimere i contenuti per ridurre il carico sulla rete.
- Attivare e disattivare la scansione incrementale. La configurazione supplementare può essere richiesta nel file `Vontusscanner_typeScanner.cfg`.

Vedere ["Opzioni di configurazione del controller del rilevatore"](#) a pagina 1983.

`ScannerControllerLogging.properties`

Nel file di `ScannerControllerLogging.properties`, è possibile configurare le seguenti opzioni:

- Specificare i livelli di registrazione da `.level = INFO` a `.level = FINEST`.

`Vontusscanner_typeScanner.cfg`

Nel file di `Vontusscanner_typeScanner.cfg`, è possibile configurare le seguenti opzioni:

- Specificare i processi multipli (eseguire in sequenza).
- Definire le credenziali di accesso.
Vedere ["Password crittografate nei file di configurazione"](#) a pagina 1840.
- Definire i filtri.
- Definire le limitazioni.
- Le impostazioni specifiche sono inoltre disponibili per ogni tipo di scanner.

Opzioni di configurazione del controller del rilevatore

La configurazione iniziale del rilevatore viene eseguita durante l'installazione. Dopo l'installazione, è possibile modificare o specificare ulteriori impostazioni di scansione.

[Tabella 70-5](#) fornisce una spiegazione dei parametri comunemente modificati nel file `ScannerController.properties`.

Tabella 70-5 Parametri comunemente modificati in ScannerController.properties

Parametro	Impostazione predefinita	Descrizione
discover.host	localhost	Il nome host o l'indirizzo IP del server Network Discover a cui il rilevatore instrada il contenuto. Prima di configurare questo valore, è necessario aggiungere il server Network Discover all'Enforce Server e accedervi dal rilevatore verificato.
discover.port	8090	La porta di Network Discover a cui il rilevatore instrada i dati.
discover.compress	true	Specificare se il contenuto deve essere compresso o meno prima di instradarlo al server Network Discover. La compressione riduce il carico di rete, ma utilizza ulteriore CPU sul computer del rilevatore e sul server Network Discover.
discover.retry.interval	1000	Il tempo in millisecondi che il rilevatore deve aspettare prima di riprovare a connettersi al server Network Discover dopo una disconnessione o un problema precedente.
scanner.send.endofscanmarker	true	Se questo parametro è impostato su false, il rilevatore viene eseguito fino all'arresto manuale nella console di Enforce Server. La scansione viene rieseguita dall'inizio dopo essere arrivata alla fine dell'elenco di scansione.
scanner.incremental	false	Quando è true, il rilevatore esegue la scansione solo dei documenti creati o modificati dopo l'ultima scansione completa. Quando è false, viene eseguita la scansione di tutti i file ad ogni scansione.
dre.fake.port	disattivato http://localhost:19821	Usato solo da determinati rilevatori per impedire che il contenuto venga instradato a un processo non corretto. Deve anche essere modificato con valori per DREHost e ACIPort nel file <code>scanner_typeScanner.cfg</code> . dre.fake.port specifica la porta a cui ScannerController esegue il binding. Verifica che il connettore non tenti di inviare contenuto a qualche altro processo.
queue.folder.path	disattivato ./scanner/outgoing	Usato solo con determinati rilevatori per risolvere la differenza tra la posizione in cui i file <code>.idx</code> sono scritti e quella in cui dovrebbero trovarsi. Questo parametro è per i rilevatori di Exchange e SharePoint 2003.

Impostazione della scansione di file system

Il capitolo contiene i seguenti argomenti:

- [Impostazione della scansione remota di file system](#)
- [Target supportati del rilevatore file system](#)
- [Installazione dei rilevatori file system](#)
- [Avvio della scansione del file system](#)
- [Installazione di rilevatori file system invisibile dalla riga di comando](#)
- [Opzioni di configurazione per i rilevatori file system](#)
- [Configurazione di esempio per la scansione dell'unità C su un computer Windows](#)
- [Configurazione di esempio per la scansione della directory /usr in UNIX](#)
- [Esempio di configurazione per la scansione con filtri di inclusione](#)
- [Esempio di configurazione per la scansione con filtri di esclusione](#)
- [Esempio di configurazione per la scansione con filtri di inclusione e esclusione](#)
- [Esempio di configurazione per la scansione con filtri di data](#)
- [Esempio di configurazione per la scansione con filtri di dimensione di file](#)
- [Esempio di configurazione per le scansioni che ignorano collegamenti simbolici su sistemi UNIX](#)

Impostazione della scansione remota di file system

La scansione dei file system che non sono condivisioni file o server viene eseguita con un'installazione computer multipla. Nel computer con il file system, il software di scansione invia i dati al server Network Discover per l'elaborazione.

Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.

Per le condivisioni file, utilizzare il target del file server.

Vedere ["Impostazione delle scansioni di file system"](#) a pagina 1906.

Per configurare la scansione dei file system, completare i seguenti processi:

Tabella 71-1 Impostazione di un rilevatore del file system

Passaggio	Azione	Descrizione
1	Verificare che il file system si trovi nell'elenco dei target supportati. Il rilevatore del file system può eseguire la scansione dei file system locali su server Windows, Linux, AIX e Solaris remoti.	Vedere "Target supportati del rilevatore file system" a pagina 1987.
2	Nel server che contiene il file system, installare il rilevatore del file system. La configurazione per la scansione dei file system richiede l'installazione del software del rilevatore nel computer in cui si trova il file system. Su Linux, AIX e Solaris, l'utente principale deve installare il rilevatore.	Vedere "Installazione dei rilevatori file system" a pagina 1988. Vedere "Installazione di rilevatori file system invisibile dalla riga di comando" a pagina 1992.
3	Eseguire eventuali configurazioni manuali modificando i file di configurazione e di proprietà.	Vedere "Opzioni di configurazione per i rilevatori file system" a pagina 1992.
4	Su Enforce Server, aggiungere un nuovo target file system del rilevatore.	Vedere "Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover" a pagina 1826.
5	Avviare la scansione del file system. Avviare il rilevatore sul computer rilevatore e avviare inoltre la scansione sull'Enforce Server.	Vedere "Avvio della scansione del file system" a pagina 1990.
6	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Risoluzione dei problemi dei rilevatori" a pagina 1978.

Target supportati del rilevatore file system

È possibile eseguire la scansione dei seguenti sistemi Windows remoti:

- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

È possibile eseguire la scansione dei seguenti file system Linux:

- Red Hat Enterprise Linux 5.x

Nota: Obsoleto in Symantec Data Loss Prevention 15.1.

- Red Hat Enterprise Linux 6.x
- Red Hat Enterprise Linux 7.4

È possibile eseguire la scansione dei seguenti file system AIX:

- AIX 6.5

Nota: Obsoleto in Symantec Data Loss Prevention 15.1.

- AIX 7.1

AIX richiede le seguenti librerie di runtime C, come Java 1.5 e Java 7 JRE:

- `xlC.aix50.rte` (v8.0.0.0+)
- `xlC.rte` (v8.0.0.0+)

È possibile eseguire la scansione dei seguenti file system Solaris a 32 bit (i sistemi a 64 bit non sono supportati):

- Solaris 9 (piattaforma SPARC)

Nota: Obsoleto in Symantec Data Loss Prevention 15.1.

- Solaris 10 (piattaforma SPARC)

Solaris richiede i seguenti livelli di patch per il rilevatore:

- Solaris 9, 115697-01

I file system su sistemi UNIX possono inoltre essere sottoposti a scansione tramite il protocollo SFTP. Questo protocollo fornisce un metodo simile alla scansione di file basati sulla

condivisione, invece che utilizzare il Rilevatore file system. Contattare i servizi professionali Symantec per dettagli.

Installazione dei rilevatori file system

Il rilevatore file system deve essere installato nel computer insieme al file system che si desidera sottoporre a scansione.

Su Linux, AIX e Solaris, l'utente principale deve installare il rilevatore.

Se un utente diverso da quello che ha eseguito l'installazione del rilevatore vuole eseguirlo, è necessario modificare le autorizzazioni. Su Linux, AIX e Solaris, è necessario fornire le autorizzazioni appropriate a file e directory.

Per installare il rilevatore file system

- 1 Nel computer con il file system da sottoporre a scansione, scaricare o copiare (come file binario) il file di installazione pertinente in una directory temporanea. Il file si trova nella directory `DLP_Home\Symantec_DLP_15.0_Win\Scanners` o `DLP_Home/Symantec_DLP_15.0_Lin/Scanners`, in cui *DLP_Home* è il nome della directory in cui è stato decompresso il software Symantec Data Loss Prevention.

Il file ha uno dei seguenti nomi:

- `SymantecDLPScanners_windows_x32_15.0.exe`
- `SymantecDLPScanners_Aix_15.0.sh`
- `SymantecDLPScanners_Unix_x32_15.0.sh` (per sistemi Linux a 32 bit)
- `SymantecDLPScanners_Unix_x64_15.0.sh` (per sistemi Linux a 64 bit)

Nota: Nei sistemi Linux è possibile installare sia il rilevatore a 32 bit, sia quello a 64 bit. Symantec consiglia la versione a 64 bit.

- `SymantecDLPScanners_Solaris_15.0.sh`

2 Avviare il programma di installazione del rilevatore.

Utilizzare il flag `-c` per installare un rilevatore con un comando di console (invece che con GUI).

GUI di Windows:

`SymantecDLPScanners_windows_x32_15.0.exe`

GUI di Linux a 32 bit:

`./SymantecDLPScanners_Unix_x32_15.0.sh`

Console di Linux a 32 bit:

`./SymantecDLPScanners_Unix_x32_15.0.sh -c`

3 Se opportuno, confermare la versione del rilevatore che si desidera installare (a 32 o 64 bit).

4 Confermare il contratto di licenza.

5 Selezionare **Rilevatore file system.**

6 Selezionare la directory di destinazione dell'installazione (ovvero la directory in cui si desidera installare il rilevatore file system SymantecDLP).

7 Per Windows, selezionare la cartella Menu di avvio (scorciatoia nel menu di **avvio). L'impostazione predefinita è **rilevatore file system SymantecDLP**.**

8 Immettere le seguenti informazioni relative alla connessione per il server Network Discover:

- Host Discover (IP o nome host del server)
- Porta Discover

9 Configurare il rilevatore file system immettendo le seguenti informazioni:

- Directory di scansione
Elenco delle directory da sottoporre a scansione. Delimitare con una virgola (nessuno spazio).
- Il percorso include il filtro
Vengono sottoposti a scansione soltanto i percorsi che includono tutte le stringhe specificate qui. Delimitare con una virgola (nessuno spazio).
- Il percorso esclude il filtro
Vengono sottoposte a scansione tutte le directory tranne quelle che contengono le stringhe specificate qui. Delimitare le voci mediante virgole, ma senza utilizzare spazi.

Tenere presente che i nomi di file **Includi filtro** o **Escludi filtro** si riferiscono alla radice del file system. Specificare i percorsi completi o le sottodirectory, secondo le necessità.

10 Il rilevatore viene installato.

11 Selezionare la modalità di avvio.

Mentre si eseguono test o verifiche iniziali sul corretto funzionamento del rilevatore, non selezionare nessuna di queste opzioni, ma avviare il rilevatore manualmente.

È possibile selezionare una delle seguenti opzioni (o nessuna):

- Installare come servizio su un sistema Windows
- Iniziare dopo l'installazione.

12 L'installazione del rilevatore di file è completa nel computer del rilevatore.

13 Eseguire eventuali configurazioni manuali modificando i file di configurazione e di proprietà.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.

Vedere ["File di configurazione del sistema di scansione"](#) a pagina 1982.

14 Su Enforce Server, creare un Nuovo target per il tipo di file system del rilevatore.

15 Avviare la scansione sia sul computer del rilevatore che su Enforce Server.

Vedere ["Avvio della scansione del file system"](#) a pagina 1990.

Avvio della scansione del file system

Assicurarsi che il rilevatore sia installato e configurato sul computer target e che un nuovo target venga aggiunto a Enforce Server.

Vedere ["Installazione dei rilevatori file system"](#) a pagina 1988.

Avviare quindi la scansione.

Le procedure sono differenti per ognuno dei seguenti scenari:

- Un rilevatore per target (prima procedura).
- Più rilevatori per un target (seconda procedura).

Per avviare una scansione del file system con un rilevatore per un target

1 Accedere a Enforce Server.

Selezionare **Gestisci > Scansione Discover > Target di Discover** per visualizzare l'elenco dei target.

2 Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.

- 3 Sul computer del rilevatore avviare il rilevatore File system.

In Windows selezionare **Start > Rilevatore file system Vontu > Console rilevatore file system Vontu**.

Su UNIX immettere il seguente comando:

```
/opt/FileSystemScanner/bin/FileSystemScanner_Console
```

- 4 Il rilevatore avvia il processo di scansione dei dati.

Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.

- 5 Se la scansione non progredisce normalmente, è possibile eseguire una procedura di risoluzione dei problemi.

Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.

- 6 Arrestare e riavviare il rilevatore ogni volta che si modifica il file di configurazione. Per arrestare il rilevatore, premere CTRL-C nella finestra della console.

Per avviare una scansione del file system con più scanner per un target

- 1 Su ciascuno dei computer del rilevatore avviare il rilevatore File system.

In Windows selezionare **Start > Rilevatore file system Vontu > Console rilevatore file system Vontu**.

Su UNIX immettere il seguente comando:

```
/opt/FileSystemScanner/bin/FileSystemScanner_Console
```

Assicurarsi che ogni rilevatore sia stato avviato e che abbia inviato informazioni. Controllare la cartella `outgoing` su ogni computer.

Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.

- 2 Accedere a Enforce Server.

Selezionare **Gestisci > Scansione Discover > Target di Discover** per visualizzare l'elenco dei target.

- 3 Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.

- 4 Il rilevatore avvia il processo di scansione dei dati.

Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.

- 5 Se la scansione non progredisce normalmente, è possibile eseguire una procedura di risoluzione dei problemi.

Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.

- 6 Arrestare e riavviare il rilevatore ogni volta che si modifica il file di configurazione. Per arrestare il rilevatore, premere CTRL-C nella finestra della console.

Installazione di rilevatori file system invisibile dalla riga di comando

Per automatizzare l'installazione, è possibile preconfigurare un file di testo `varfile` con le scelte dell'installazione e poi lanciare l'installazione da una riga di comando.

Un altro metodo per installare un rilevatore è utilizzare un'installazione interattiva.

Vedere ["Installazione dei rilevatori file system"](#) a pagina 1988.

Per automatizzare l'installazione del rilevatore di file

- 1 Creare un file di testo, ad esempio `FileSystemScanner.varfile`.
- 2 Immettere i parametri specifici e salvare il file sulla stessa posizione dello script shell rilevante per l'installazione del rilevatore.

```
sys.programGroup.allUsers$Boolean=true
discover.host=test-server.test.lab
discover.port=8090
sys.service.selected.417$Boolean=true
job.0.excludeFilters=
sys.languageId=en
sys.programGroup.linkDir=/usr/local/bin
installService$Boolean=false
sys.installationDir=/opt/FileSystemScanner
sys.programGroup.enabled$Boolean=true
job.0.includeFilters=
job.0.directory=/home/text_files/text_scan/text
sys.service.startupType.417=auto
startAfterInstall$Boolean=false
```

- 3 Per eseguire l'installazione con il `varfile`, digitare il seguente comando (per Linux):

```
# ./FileSystemScanner_Unix_11.6.sh
-varfile FileSystemScanner.varfile -q
```

Il parametro `-q` esegue un'installazione invisibile.

Opzioni di configurazione per i rilevatori file system

[Tabella 71-2](#) fornisce una descrizione dei parametri principali nel file `VontuFileSystemScanner.cfg`.

Tabella 71-2 Parametri nel file VontuFileSystemScanner.cfg

Tipo	Parametro	Descrizione
Contenuto sottoposto a scansione	DirectoryPathCSVs	Elenco di directory separate da virgola da sottoporre a scansione.
Contenuto sottoposto a scansione	DirectoryCantHaveCSVs	Escludere i filtri dei percorsi. Delimitare le voci mediante virgole, ma senza utilizzare spazi.
Contenuto sottoposto a scansione	DirectoryMustHaveCSVs	Includere i filtri dei percorsi. Delimitare le voci mediante virgole, ma senza utilizzare spazi.
Contenuto sottoposto a scansione	DirectoryAfterDate	Filtro date (in giorni rispetto alla data corrente).
Contenuto sottoposto a scansione	DirectoryBeforeDate	Filtro date (in giorni rispetto alla data corrente).
Contenuto sottoposto a scansione	DirectoryFileMatch	Per eseguire la scansione di file senza un'estensione sui sistemi Linux o Solaris, impostare questo parametro sul seguente valore: DirectoryFileMatch=*
Contenuto sottoposto a scansione	ImportPreImportMinLength	Dimensione minima di file.
Contenuto sottoposto a scansione	ImportPreImportMaxLength	Dimensione massima di file.
Limitazione	ImportPoliteness	Specificare il lasso di tempo (in millisecondi) di attesa tra i documenti del modulo di importazione.

Tipo	Parametro	Descrizione
Limitazione	PollingMaxNumber	<p>Il numero dei file che vengono aggregati prima di essere importati in ogni file XML inviato a Network Discover.</p> <p>Vedere "Ottimizzazione delle risorse con le opzioni di limitazione delle scansioni di Network Discover/Cloud Storage Discover" a pagina 1847.</p>

Configurazione di esempio per la scansione dell'unità C su un computer Windows

Eseguire la scansione dell'unità C su un computer Windows

Questa configurazione si trova nel file `VontuFileSystemScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

```
DirectoryPathCSVs=C:\
DirectoryMustHaveCSVs=
DirectoryCantHaveCSVs=
```

Configurazione di esempio per la scansione della directory /usr in UNIX

Scansione della directory /usr in un computer UNIX.

Questa configurazione si trova nel file `VontuFileSystemScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

```
DirectoryPathCSVs=/usr
DirectoryMustHaveCSVs=
DirectoryCantHaveCSVs=
```

Esempio di configurazione per la scansione con filtri di inclusione

Eseguire la scansione di file e directory selezionati utilizzando i filtri di inclusione.

Questa configurazione si trova nel file `VontuFileSystemScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

Includere solo i file che hanno `tmp` nel percorso della directory `C:\Windows`.

```
DirectoryPathCSVs=C:\Windows
DirectoryMustHaveCSVs=*/tmp/*
DirectoryCantHaveCSVs=
```

Includere solo i file con l'estensione `tmp` o se il nome della directory include `xml` nel percorso.

```
DirectoryPathCSVs=C:\Windows
DirectoryMustHaveCSVs=*/xml/*, *.tmp
DirectoryCantHaveCSVs=
```

Includere solo i file che hanno l'estensione `txt` nella directory Unix `/home/data`.

```
DirectoryPathCSVs=/home/data
DirectoryMustHaveCSVs=*.txt
DirectoryCantHaveCSVs=
```

Esempio di configurazione per la scansione con filtri di esclusione

Eeguire la scansione di file e directory selezionati utilizzando i filtri di esclusione.

Questa configurazione si trova nel file `VontuFileSystemScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

Escludere tutti i file con l'estensione `exe` nella directory `C:\Windows`.

```
DirectoryPathCSVs=C:\Windows
DirectoryMustHaveCSVs=
DirectoryCantHaveCSVs=*.exe
```

Escludere tutti i file con l'estensione `tmp` o se il nome della directory contiene `bin` nella directory **UNIX** `/home/data`.

```
DirectoryPathCSVs=/home/data
DirectoryMustHaveCSVs=
DirectoryCantHaveCSVs=*/bin/*, *.tmp
```

Esempio di configurazione per la scansione con filtri di inclusione e esclusione

Sottoporre a scansione i file e le directory usando filtri di esclusione e inclusione.

Questa configurazione si trova nel file `VontuFileSystemScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

Sottoporre a scansione tutte le directory con `temp` nel percorso che finisce con `pdf`. Escludere file nell'ambito della directory `bin` o che finisce con `tmp` nell'ambito del directory `C:\data`.

```
DirectoryPathCSVs=C:\data
DirectoryMustHaveCSVs=*/temp/*,*.pdf
DirectoryCantHaveCSVs=*/bin/*,*.tmp
```

Esempio di configurazione per la scansione con filtri di data

I parametri `DirectoryBeforeDate` e `DirectoryAfterDate` consentono di specificare un intervallo di date entro le quali i documenti devono essere modificati affinché il rilevatore le elabori.

Utilizzare il parametro `DirectoryAfterDate` per immettere un numero di giorni rispetto alla data corrente dopo la quale la pagina deve essere modificata. Un numero negativo specifica una data passata.

Utilizzare il parametro `DirectoryBeforeDate` per immettere un numero di giorni rispetto alla data corrente prima della quale la pagina deve essere modificata.

Negli esempi, `DirectoryBeforeDate` e `DirectoryAfterDate` sono entrambi necessari.

Questa configurazione si trova nel file `VontuFileSystemScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

Sottoporre a scansione tutti i file `pdf` modificati negli ultimi sei mesi.

```
DirectoryMustHaveCSVs=*.pdf
DirectoryAfterDate=-180
DirectoryBeforeDate=0
```

Sottoporre a scansione tutti i file che sono stati modificati tra 60 e 360 giorni prima della data corrente.

```
DirectoryAfterDate=-360
DirectoryBeforeDate=-60
```


Esempio di configurazione per la scansione con filtri di dimensione di file

Eseguire la scansione di file utilizzando filtri di dimensione di file per limitare il numero di elementi sottoposti a scansione.

Questa configurazione si trova nel file `VontuFileSystemScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

Viene eseguita la scansione di tutti i file la cui dimensione è tra 3000 e 4000 byte. I file la cui dimensione non rientra in quell'intervallo non sono importati.

```
ImportPreImportMinLength=3000
ImportPreImportMaxLength=4000
ImportEmptyFiles=false
```

Viene eseguita la scansione dei file `doc` la cui dimensione è maggiore di 4 KB.

```
DirectoryMustHaveCSVs=*.doc
ImportPreImportMinLength=4096
ImportEmptyFiles=false
```

Esempio di configurazione per le scansioni che ignorano collegamenti simbolici su sistemi UNIX

Eseguire la scansione di un sistema UNIX ignorando tutti i collegamenti simbolici.

Specificare un file contenente tutti i file che il rilevatore deve esaminare. Soltanto tali file sono sottoposti a scansione. Posizionare tale file al di fuori della directory di installazione del rilevatore. Nell'esempio, questo file è denominato `/opt/test/filenames.txt`.

Questa configurazione si trova nel file `VontuFileSystemScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori file system"](#) a pagina 1992.

Assicurarsi che `DirectoryPathCSVs` e i parametri correlati siano trasformati in commento. Inoltre, assicurarsi che il parametro `PollingMethod` sia presente solo una volta nel file di configurazione.

```
PollingMethod=1
FilePollFilename=/opt/test/filenames.txt
```

Impostazione della scansione di server Web

Il capitolo contiene i seguenti argomenti:

- [Configurazione di una scansione remota di Web Server](#)
- [Target supportati del Web Server \(rilevatore\)](#)
- [Installazione di rilevatori Web Server](#)
- [Avvio delle scansioni del server Web](#)
- [Opzioni di configurazione per i rilevatori Web Server](#)
- [Configurazione di esempio per una scansione del sito Web senza autenticazione](#)
- [Esempio di configurazione per la scansione di un sito Web con autenticazione di base](#)
- [Configurazione di esempio per una scansione del sito Web con autenticazione basata sulla forma](#)
- [Esempio di configurazione per una scansione di siti Web con NTLM](#)
- [Esempio di filtraggio di URL per una scansione di siti Web](#)
- [Esempio di filtraggio in base alla data per una scansione di siti Web](#)

Configurazione di una scansione remota di Web Server

Il rilevatore Web Server può recuperare documenti di siti Web.

Il rilevatore utilizza dei crawler per trovare pagine Web ed elaborarle per il contenuto e i collegamenti ad altri siti Web. Al termine del recupero di documenti con i crawler dal sito Web,

il rilevatore Web Server importa il contenuto recuperato nel formato di file indice (IDX). Il rilevatore invia quindi i file IDX a Network Discover per l'elaborazione del contenuto. Il rilevatore Web Server può recuperare il contenuto da vari tipi di documenti, inclusi documenti Web, file Word, Excel e PDF.

Il rilevatore Web Server cerca collegamenti e contenuto da indicizzare nelle pagine Web. Il crawler elabora il contenuto della pagina e accetta o rifiuta di recuperare la pagina. Se la pagina viene accettata, il crawler cerca collegamenti nella pagina, li filtra e mette in coda quelli accettati per il processo di indicizzazione. Se la pagina viene rifiutata, il crawler cerca collegamenti solo se la configurazione prevede di seguire i collegamenti sulle pagine rifiutate. I collegamenti sono filtrati prima di essere aggiunti alla coda del crawler. Il crawler recupera quindi il contenuto delle pagine accettate. Il crawler richiede il collegamento successivo nella coda e il processo viene ripetuto.

Per configurare la scansione di Web Server, completare il processo seguente:

Tabella 72-1 Configurazione di un rilevatore Web Server

Passaggio	Azione	Descrizione
1	Il rilevatore Web Server può sottoporre a scansione i siti Web. È stato testato con Web Server IIS e Apache.	Vedere "Target supportati del Web Server (rilevatore)" a pagina 1999.
2	Sul server con accesso in lettura al sito Web, installare il rilevatore Web Server.	Vedere "Installazione di rilevatori Web Server" a pagina 2000.
3	Eseguire eventuali configurazioni manuali modificando i file di configurazione e di proprietà.	Vedere "Opzioni di configurazione per i rilevatori Web Server" a pagina 2003.
4	Su Enforce Server, aggiungere un nuovo target file system del rilevatore.	Vedere "Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover" a pagina 1826.
5	Avviare la scansione del file system. Avviare il rilevatore sul computer rilevatore e avviare inoltre la scansione sull'Enforce Server.	Vedere "Avvio delle scansioni del server Web" a pagina 2002.
6	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Risoluzione dei problemi dei rilevatori" a pagina 1978.

Target supportati del Web Server (rilevatore)

Il rilevatore Web Server supporta la scansione di un sito Web HTTP statico.

Installazione di rilevatori Web Server

Il rilevatore Web Server deve essere installato sul computer che ha accesso ai siti Web che si intende sottoporre a scansione.

Per installare il rilevatore Web Server

- 1 Nel computer con il file system da sottoporre a scansione, scaricare o copiare (come file binario) il file di installazione pertinente in una directory temporanea. Il file si trova nella directory `DLP_Home\Symantec_DLP_15.0_Win\Scanners 0`
`DLP_Home/Symantec_DLP_15.0_Lin/Scanners`, in cui `DLP_Home` è il nome della directory in cui è stato decompresso il software Symantec Data Loss Prevention.

Il file ha uno dei seguenti nomi:

- `SymantecDLPScanners_windows_x32_15.0.exe`
- `SymantecDLPScanners_Unix_15.0_x32.sh` (per sistemi Linux a 32 bit)

- 2 Avviare il programma di installazione del rilevatore.

Utilizzare il flag `-c` per installare un rilevatore con un comando di console (invece che con GUI).

GUI di Windows:

```
SymantecDLPScanners_windows_x32_15.0.exe
```

GUI di Linux:

```
./SymantecDLPScanners_Unix_x32_15.0.sh
```

Console di Linux:

```
./SymantecDLPScanners_Unix_15.0.sh -c
```

- 3 Confermare la versione del rilevatore che si desidera installare (a 32 o 64 bit).
- 4 Confermare il contratto di licenza.
- 5 Selezionare **Rilevatore Web Server**.
- 6 Selezionare la **directory di destinazione** dell'installazione (ovvero la directory in cui si desidera installare il rilevatore Web Server).

Fare clic su **Avanti**.

- 7 Selezionare la cartella del menu Start (scorciatoia nel menu **Start**). L'impostazione predefinita è **Rilevatore WebServer Symantec DLP**.

Fare clic su **Avanti**.

- 8 Immettere le seguenti informazioni sulla connessione per il server Network Discover:

- Host Discover (IP o nome host del server)
- Porta Discover

Fare clic su **Avanti**.

9 Configurare il rilevatore Web Server immettendo le seguenti informazioni:

- URL iniziale
Immettere l'URL da dove la scansione ha inizio.
- Filtro di inclusione
Vengono sottoposti a scansione soltanto i percorsi che includono tutte le stringhe specificate qui. Delimitare le voci con una virgola, ma non utilizzare spazi. È possibile utilizzare caratteri jolly.
- Filtro di esclusione percorsi
Vengono sottoposti a scansione tutti i percorsi tranne quelli che contengono le stringhe specificate qui. Delimitare le voci con una virgola, ma non utilizzare spazi. È possibile utilizzare caratteri jolly.

Fare clic su **Avanti**.

10 Il rilevatore viene installato.

11 Selezionare la modalità di avvio.

Mentre si eseguono test o verifiche iniziali sul corretto funzionamento del rilevatore, non selezionare nessuna di queste opzioni, ma avviare il rilevatore manualmente.

È possibile selezionare una delle seguenti opzioni (o nessuna):

- Installare come servizio su un sistema Windows
- Avviare dopo l'installazione.

Fare clic su **Avanti**.

Fare clic su **Fine**.

12 L'installazione del rilevatore Web server è completata nel computer del rilevatore.

13 Eseguire eventuali configurazioni manuali modificando i file di configurazione e di proprietà.

Vedere ["Opzioni di configurazione per i rilevatori Web Server"](#) a pagina 2003.

Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.

Vedere ["File di configurazione del sistema di scansione"](#) a pagina 1982.

14 In Enforce Server, creare un **nuovo target** per il tipo di Web Server del rilevatore.

15 Avviare la scansione sia sul computer del rilevatore che su Enforce Server.

Vedere ["Avvio delle scansioni del server Web"](#) a pagina 2002.

Avvio delle scansioni del server Web

Assicurarsi che il rilevatore sia installato e configurato nel computer target e che un nuovo target sia aggiunto a Enforce Server.

Vedere ["Installazione di rilevatori Web Server"](#) a pagina 2000.

Avviare quindi la scansione.

Le procedure sono differenti per ognuno dei seguenti scenari:

- Un rilevatore per target (prima procedura).
- Molteplici rilevatori per un target (seconda procedura).

Per avviare una scansione del server Web con un rilevatore per un target

- 1 Accedere a Enforce Server.
Selezionare **Gestisci > Scansione Discover > Target di Discover** per visualizzare l'elenco dei target.
- 2 Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.
- 3 Nel computer del rilevatore, avviare il rilevatore del server Web.
Fare clic su **Avvia > Rilevatore WebServer > Console rilevatore WebServer**.
- 4 Il rilevatore avvia il processo di scansione dei dati.
Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.
- 5 Se la scansione non progredisce normalmente, è possibile eseguire una procedura di risoluzione dei problemi.
Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.
- 6 Arrestare e riavviare il rilevatore ogni volta che si modifica il file di configurazione. Per arrestare il rilevatore, premere CTRL-C nella finestra della console.

Per avviare una scansione del server Web con molteplici rilevatori per un target

- 1 In ognuno dei computer rilevatori, avviare il rilevatore del server Web.
Fare clic su **Avvia > Rilevatore WebServer > Console rilevatore WebServer**.
Assicurarsi che ogni rilevatore sia stato avviato e che abbia inviato informazioni. Controllare la cartella `outgoing` su ogni computer.
Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.
- 2 Accedere a Enforce Server.
Selezionare **Gestisci > Scansione Discover > Target di Discover** per visualizzare l'elenco dei target.
- 3 Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.

- 4 Il rilevatore avvia il processo di scansione dei dati.
Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.
- 5 Se la scansione non progredisce normalmente, è possibile eseguire una procedura di risoluzione dei problemi.
Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.
- 6 Arrestare e riavviare il rilevatore ogni volta che si modifica il file di configurazione. Per arrestare il rilevatore, premere CTRL-C nella finestra della console.

Opzioni di configurazione per i rilevatori Web Server

[Tabella 72-2](#) fornisce una spiegazione del file `VontuWebServerScanner.cfg`.

Tabella 72-2 Parametri nel file `VontuWebServerScanner.cfg`

Tipo	Parametro	Descrizione
Contenuto sottoposto a scansione	URL	L'URL valido della prima pagina che il crawler inizia a elaborare. Se si desidera recuperare più di una pagina, la pagina Web iniziale deve contenere collegamenti ad altre pagine Web. È necessario includere <code>http://</code> nel parametro di configurazione.
Contenuto sottoposto a scansione	NavDirAllowCSVs	L'elenco con i filtri di inclusione per i percorsi. Questo elenco include le stringhe che l'URL di una pagina deve contenere perché il rilevatore elabori la pagina. Utilizzare il parametro <code>NavDirCheck</code> per specificare come e quando il rilevatore deve verificare tali stringhe. Utilizzare * come carattere jolly. Delimitare le voci con una virgola, ma non utilizzare spazi.
Contenuto sottoposto a scansione	NavDirDisallowCSVs	L'elenco con i filtri di esclusione per i percorsi. Questo elenco include le stringhe che l'URL di una pagina deve contenere perché il rilevatore elabori la pagina. Utilizzare il parametro <code>NavDirCheck</code> per specificare come e quando il rilevatore deve verificare tali stringhe. Utilizzare * come carattere jolly. Delimitare le voci con una virgola, ma non utilizzare spazi.

Tipo	Parametro	Descrizione
Contenuto sottoposto a scansione	NavDirCheck	<p>Un numero di maschera bit per bit utilizzato per determinare dove e come il rilevatore verifica le stringhe NavDirAllowCSVs e NavDirDisallowCSVs. Se l'URL di una pagina non contiene una delle stringhe NavDirAllowCSVs o NavDirDisallowCSVs, il rilevatore non elabora la pagina.</p> <p>Vedere "Esempio di filtraggio di URL per una scansione di siti Web" a pagina 2007.</p>
Contenuto sottoposto a scansione	Estensioni	<p>Immettere le estensioni di file per limitare i tipi di documento che il rilevatore può elaborare. Se si immettono molteplici estensioni, separarle con virgole. Utilizzare * come carattere jolly. Non inserire spazi prima o dopo le virgole.</p> <p>Esempio per recuperare solo i documenti con estensione .doc o .html:</p> <pre>Extensions=*.doc,*.html*</pre>
Contenuto sottoposto a scansione	MaxLinksPerPage	<p>Il numero massimo di collegamenti che una pagina può avere. Le pagine con molti collegamenti sono spesso pagine di navigazione e questo parametro può essere usato per escluderle.</p>
Contenuto sottoposto a scansione	StayOnSite	<p>È possibile configurare il crawler affinché rimanga sul sito Web iniziale oppure segua i collegamenti a siti Web esterni in domini differenti da quello del sito Web iniziale. Per impostazione predefinita, il crawler rimane sul dominio del sito Web iniziale.</p>
Contenuto sottoposto a scansione	AfterDate	<p>Il numero di giorni dopo i quali una pagina deve essere modificata prima di essere salvata. Immettere il numero di giorni rispetto alla data corrente. Un numero negativo specifica una data passata.</p>
Contenuto sottoposto a scansione	BeforeDate	<p>Il numero di giorni prima dei quali una pagina deve essere modificata prima di essere salvata. Immettere il numero di giorni rispetto alla data corrente. Un numero negativo specifica una data passata.</p>

Tipo	Parametro	Descrizione
Autenticazione	LoginMethod	<p>Il metodo di autenticazione per il sito. Il valore deve essere <code>AUTHENTICATE</code>, <code>FORMPOST</code> o <code>FORMGET</code>.</p> <p>Vedere "Esempio di configurazione per la scansione di un sito Web con autenticazione di base" a pagina 2006.</p> <p>Vedere "Configurazione di esempio per una scansione del sito Web con autenticazione basata sulla forma" a pagina 2006.</p>
Autenticazione	LoginURL	La pagina che contiene il modulo di accesso.
Autenticazione	LoginUserValue	Il nome utente per l'autenticazione (testo semplice o crittografato).
Autenticazione	LoginPassValue	<p>La password per l'autenticazione. Crittografare questa password.</p> <p>Vedere "Password crittografate nei file di configurazione" a pagina 1840.</p>
Autenticazione	LoginUserField	Il nome del campo modulo nome utente (per i metodi di accesso <code>FORMPOST</code> o <code>FORMGET</code>).
Autenticazione	LoginPassField	<p>Il nome del campo modulo password (per i metodi di accesso <code>FORMPOST</code> o <code>FORMGET</code>). Crittografare questa password.</p> <p>Vedere "Password crittografate nei file di configurazione" a pagina 1840.</p>
Proxy	ProxyHost	Il nome host o l'indirizzo IP del server proxy.
Proxy	ProxyPort	Il numero di porta del server proxy.
Proxy	ProxyUsername	Il nome utente (testo semplice o crittografato) per il server proxy.
Proxy	ProxyPassword	<p>La password per il server proxy. Crittografare questa password.</p> <p>Vedere "Password crittografate nei file di configurazione" a pagina 1840.</p>
Limitazione	PageDelay	Il numero di secondi tra il download di una pagina e la richiesta della pagina successiva.
Limitazione	BatchSize	Il numero di file che vengono aggregati in ogni file XML inviato a Network Discover.

Configurazione di esempio per una scansione del sito Web senza autenticazione

Eseguire la scansione di un sito Web senza autenticazione.

Questa configurazione si trova nel file `VontuWebServerScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori Web Server"](#) a pagina 2003.

```
#####  
//#    Jobs  
#####  
URL=http://www.cnn.com
```

Esempio di configurazione per la scansione di un sito Web con autenticazione di base

Eseguire la scansione di un sito Web protetto con l'autenticazione standard.

Questa configurazione si trova nel file `VontuWebServerScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori Web Server"](#) a pagina 2003.

```
#####  
//#    Jobs  
#####  
URL=http://site.domain.com  
LoginURL=http://domain.server.com/login.html  
LoginMethod=AUTHENTICATE  
LoginUserValue=some_user  
LoginPassValue=9sfIy8vw
```

Configurazione di esempio per una scansione del sito Web con autenticazione basata sulla forma

Eseguire la scansione di un sito Web protetto con autenticazione basata sulla forma.

Questa configurazione si trova nel file `VontuWebServerScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori Web Server"](#) a pagina 2003.

```
#####  
//#    Jobs  
#####
```

```
URL= http://wiki.symantec.corp/dashboard.action

LoginMethod=FORMPOST
LoginURL=http://wiki.symantec.corp/login.action

LoginUserField=os_username
LoginUserValue=some_user

LoginPassField=os_password
LoginPassValue=9sfIy8vw
```

Esempio di configurazione per una scansione di siti Web con NTLM

Eseguire la scansione di un sito Web protetto con NTLM.

Assicurarsi che `NTLMUsername` sia nel formato `Dominio\nome utente`.

Questa configurazione si trova nel file `VontuWebServerScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori Web Server"](#) a pagina 2003.

```
//#####
//#   Jobs
//#####
URL=http://some_site
NTLMUsername=Some_Domain\some_domain_user
NTLMPassword=9sfIy8vw
```

Esempio di filtraggio di URL per una scansione di siti Web

Utilizzare il parametro `NavDirCheck` per determinare dove e come il rilevatore verifica le stringhe `NavDirAllowCSVs` e `NavDirDisallowCSVs`.

Creare il numero `NavDirCheck` aggiungendo alcuni dei seguenti numeri:

Parametro	Valore	Descrizione
URL	1	È necessario immettere 1 per consentire al rilevatore di verificare se l'URL di una pagina contiene una qualsiasi delle stringhe specificate nel parametro <code>NavDirAllowCSVs</code> o <code>NavDirDisallowCSVs</code> .

Parametro	Valore	Descrizione
Senza distinzione maiuscole/minuscole	64	Se si aggiunge 64 al valore dell'URL, il rilevatore verifica la corrispondenza dell'URL di una pagina con le stringhe specificate nel parametro <code>NavDirAllowCSVs</code> o <code>NavDirDisallowCSVs</code> . La distinzione maiuscole/minuscole è disattivata per questa corrispondenza.
Prima del download	128	Se si aggiunge 128 al valore dell'URL, il rilevatore verifica se l'URL ha una qualsiasi stringa <code>NavDirAllowCSVs</code> o <code>NavDirDisallowCSVs</code> prima del download della pagina.
Struttura valida del sito	512	Se si aggiunge 512 al valore dell'URL, il rilevatore verifica di nuovo i valori <code>NavDirAllowCSVs</code> e <code>NavDirDisallowCSVs</code> per il sito per determinare che il sito è ancora valido prima di aggiornarlo. Se non si include questa impostazione, le modifiche di tali valori non vengono mai verificate. Se il sito non è valido, non viene scaricato.

Nel seguente esempio, l'analizzatore cerca negli URL le corrispondenze con le stringhe "archivio" o "prova". La distinzione maiuscole/minuscole è disattivata e viene ricercata una corrispondenza con una parola intera o parte della stessa. Se l'URL contiene una di queste stringhe, la pagina non viene elaborata.

```
NavDirDisallowCSVs=*archive*,*test*
NavDirCheck=65
```

Nell'esempio seguente, il rilevatore cerca negli URL le corrispondenze con le stringhe "notizie" o "home". La distinzione maiuscole/minuscole è disattivata e viene ricercata una corrispondenza con una parola intera o parte della stessa. Se l'URL non contiene una di queste stringhe, la pagina non viene elaborata.

```
NavDirAllowCSVs=*news*,*home*
NavDirCheck=65
```

Esempio di filtraggio in base alla data per una scansione di siti Web

Il seguente esempio consente di recuperare i documenti modificati 365 giorni prima della data corrente e 7 giorni dopo la data corrente.

```
AfterDate=-365
BeforeDate=7
```

Impostazione della scansione di archivi Documentum

Il capitolo contiene i seguenti argomenti:

- [Configurazione della scansione remota degli archivi Documentum](#)
- [Target Documentum \(rilevatore\) supportati](#)
- [Installazione dei rilevatori di Documentum](#)
- [Avvio di scansioni Documentum](#)
- [Opzioni di configurazione per i rilevatori di Documentum](#)
- [Configurazione di esempio per la scansione di tutti i documenti in un archivio Documentum](#)

Configurazione della scansione remota degli archivi Documentum

Il rilevatore di Documentum sottopone a scansione gli archivi di Documentum.

Per installare l'esame degli archivi di Documentum, completare il seguente processo:

Tabella 73-1 Configurazione dell'analizzatore di Documentum

Passaggio	Azione	Descrizione
1	Verificare che l'archivio di Documentum sia presente nell'elenco dei target supportati.	Vedere " Target Documentum (rilevatore) supportati " a pagina 2010.

Passaggio	Azione	Descrizione
2	Il rilevatore di Documentum può essere installato su qualsiasi computer con connettività di rete al computer che ospita il broker del documento di Documentum.	Vedere "Installazione dei rilevatori di Documentum" a pagina 2010.
3	Eseguire eventuali configurazioni manuali modificando i file di configurazione e di proprietà.	Vedere "Opzioni di configurazione per i rilevatori di Documentum" a pagina 2014.
4	Su Enforce Server, aggiungere un nuovo target del rilevatore di Documentum.	Vedere "Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover" a pagina 1826.
5	Iniziare la scansione di Documentum. Avviare il rilevatore sul computer rilevatore e avviare inoltre la scansione sull'Enforce Server.	Vedere "Avvio di scansioni Documentum" a pagina 2013.
6	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Risoluzione dei problemi dei rilevatori" a pagina 1978.

Target Documentum (rilevatore) supportati

Il rilevatore Documentum supporta la scansione di un archivio Documentum Content Server 5.3.x o 6.6.x e 6.7. Tutte le versioni sono obsolete in Symantec Data Loss Prevention 15.1.

Installazione dei rilevatori di Documentum

Il rilevatore di Documentum può essere installato su qualsiasi computer con connettività di rete al computer che ospita il broker di documenti Documentum.

Per installare e distribuire il rilevatore di Documentum

- 1 Sul computer con connettività di rete al computer che ospita il broker di documenti Documentum, scaricare il file di installazione. Scaricare o copiare (come file binario) il file `SymantecDLPScanners_windows_x32_15.0.exe` in una directory temporanea. Il file si trova nella directory `DLP_Home\Symantec_DLP_15.0_Win\Scanners` dove `DLP_Home` è il nome della directory in cui è stato decompresso il software Symantec Data Loss Prevention.

- 2 Avviare il programma di installazione del rilevatore su questo computer.

`SymantecDLPScanners_windows_x32_15.0.exe`

Nota: Questo analizzatore deve essere installato sui server Windows a 32 bit.

- 3 Confermare la versione del rilevatore che si desidera installare (32 bit).
- 4 Confermare il contratto di licenza.
- 5 Selezionare **Rilevatore Documentum**.
- 6 Selezionare la directory di destinazione dell'installazione, ossia la cartella in cui si desidera che venga installato il rilevatore Documentum.

Per impostazione predefinita la cartella è `C:\Programmi\DocumentumScanner\`.

Fare clic su **Avanti**.

- 7 Selezionare la cartella Menu di avvio (scorciatoia nel menu di **Avvio**).

Il valore predefinito è **Rilevatore Documentum SymantecDLP**.

Fare clic su **Avanti**.

- 8 Immettere le seguenti informazioni sulla connessione per il server Network Discover:

- Host Discover (IP o nome host del server)
- Porta Discover

- 9 Fare clic su **Avanti**.

10 Immettere i seguenti valori di configurazione di Documentum per il rilevatore:

Doc Broker Host	Il nome del server in cui è memorizzato l'archivio per il DocBase.
Doc Base	Il nome dell'archivio che si desidera venga recuperato dal rilevatore di Documentum.
Nome utente	Specificare un account con pieni diritti di accesso ai file di Documentum che si desidera sottoporre a scansione.
Password	Password dell'account. Questa password è testo normale nel file di configurazione.
Host WebTop	Il nome dell'host dell'interfaccia Web nell'archivio dei contenuti di Documentum.
Porta WebTop	Il numero di porta dell'interfaccia Web.

11 Fare clic su **Avanti**.

12 Il rilevatore viene installato.

13 Selezionare la modalità di avvio.

Mentre si eseguono test o verifiche iniziali sul corretto funzionamento del rilevatore, non selezionare nessuna di queste opzioni, ma avviare il rilevatore manualmente.

È possibile selezionare una delle seguenti opzioni (o nessuna):

- Installare come servizio su un sistema Windows
- Avviare dopo l'installazione.

Per impostazione predefinita, il rilevatore viene avviato manualmente.

14 L'installazione del rilevatore di Documentum è completa nel computer del rilevatore.

15 Eseguire qualsiasi configurazione manuale modificando i file di configurazione e proprietà.

Vedere ["Opzioni di configurazione per i rilevatori di Documentum"](#) a pagina 2014.

Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.

Vedere ["File di configurazione del sistema di scansione"](#) a pagina 1982.

16 Dopo l'installazione del rilevatore di Documentum, copiare il file `dmcl40.dll` dalla directory di installazione di Documentum `bin` alla cartella `\DocumentumScanner\scanner` nella directory di installazione del rilevatore.

Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.

17 Nell'Enforce Server, creare un nuovo target per il tipo di Documentum del rilevatore.

18 Avviare la ricerca sia sul computer del rilevatore che sull'Enforce Server.

Vedere ["Avvio di scansioni Documentum"](#) a pagina 2013.

Avvio di scansioni Documentum

Assicurarsi che il rilevatore sia installato e configurato nel computer target e che un nuovo target sia aggiunto a Enforce Server.

Vedere ["Installazione dei rilevatori di Documentum"](#) a pagina 2010.

Avviare quindi la scansione.

Le procedure sono differenti per ognuno dei seguenti scenari:

- Un rilevatore per target (prima procedura).
- Molteplici rilevatori per un target (seconda procedura).

Per avviare una scansione Documentum con un rilevatore per un target

- 1 Accedere a Enforce Server.
Selezionare **Gestisci > Scansione Discover > Target di Discover** per visualizzare l'elenco dei target.
- 2 Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.
- 3 Nel computer del rilevatore, avviare il rilevatore Documentum.
Fare clic su **Avvia > Rilevatore Documentum > Console rilevatore Documentum**.
- 4 Il rilevatore avvia il processo di scansione dei dati.
Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.
- 5 Se la scansione non progredisce normalmente, è possibile eseguire una procedura di risoluzione dei problemi.
Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.
- 6 Arrestare e riavviare il rilevatore ogni volta che si modifica il file di configurazione. Per arrestare il rilevatore, premere CTRL-C nella finestra della console.

Per avviare una scansione Documentum con molteplici rilevatori per un target

- 1 In ognuno dei computer rilevatori, avviare il rilevatore Documentum.
Fare clic su **Avvia > Rilevatore Documentum > Console rilevatore Documentum**.
Assicurarsi che ogni rilevatore sia stato avviato e che abbia inviato informazioni. Controllare la cartella `outgoing` su ogni computer.
Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.
- 2 Accedere a Enforce Server.
Selezionare **Gestisci > Scansione Discover > Target di Discover** per visualizzare l'elenco dei target.
- 3 Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.

- 4 Il rilevatore avvia il processo di scansione dei dati.
Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.
- 5 Se la scansione non progredisce normalmente, è possibile eseguire una procedura di risoluzione dei problemi.
Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.
- 6 Arrestare e riavviare il rilevatore ogni volta che si modifica il file di configurazione. Per arrestare il rilevatore, premere CTRL-C nella finestra della console.

Opzioni di configurazione per i rilevatori di Documentum

[Tabella 73-2](#) fornisce una spiegazione del file `VontuDocumentumScanner.cfg`.

Tabella 73-2 Parametri nel file `VontuDocumentumScanner.cfg`

Parametro	Descrizione
<code>DocBase</code>	Nome dell'archivio che si desidera venga recuperato da Documentum.
<code>UserName</code>	Specificare un account con diritti di accesso ai file di Documentum che si desidera sottoporre a scansione.
<code>Password</code>	<p>Password per l'account specificato in UserName. Crittografare questa password.</p> <p>Vedere "Password crittografate nei file di configurazione" a pagina 1840.</p>
<code>ExtensionCSVs</code>	<p>Elenco dei tipi di file da sottoporre a scansione (filtro di inclusione), ad esempio:</p> <p><code>ExtensionCSVs=*.doc,*.htm,*.ppt,*.xls</code></p> <p>Delimitare con una virgola (nessuno spazio).</p>

Parametro	Descrizione
ImportRefReplaceWithCSVs	<p>Elenco separato da virgole di uno o due valori utilizzati per generare l'URL dei documenti sottoposti a scansione.</p> <p><i>primo_valore,secondo_valore</i></p> <p>Se il client dell'interfaccia di Documentum è un desktop di Windows o un client desktop, il primo valore è concatenato a sinistra di id-documento. La seconda stringa è concatenata a destra, ad esempio:</p> <p><i>primo_valoreid_documentosecondo_valore</i></p> <p>Se l'interfaccia di Documentum WebTop (basata sul Web) è l'interfaccia client, è necessario solo un valore, ad esempio:</p> <p>ImportRefReplaceWithCSVs= http://documentum-server.mycompany.com:8080/ webtop/component/drl?objectId=</p>
AfterDate	<p>Età massima per i documenti da sottoporre a scansione. Ad esempio, se si imposta <i>AfterDate</i> su cinque giorni, viene eseguita la scansione solo dei documenti che non hanno più di cinque giorni. <i>AfterDate</i> esamina la data dell'ultima modifica.</p> <p>È possibile immettere uno dei valori seguenti:</p> <p><i>N</i> di ore</p> <p><i>N</i> di giorni</p> <p><i>N</i> di settimane</p> <p><i>N</i> di mesi</p> <p>Il rilevatore di Documentum non supporta la scansione incrementale automatica. Tuttavia è possibile eseguire manualmente scansioni incrementali mediante l'impostazione dei parametri <i>AfterDate</i> e <i>BeforeDate</i>.</p>

Parametro	Descrizione
BeforeDate	<p>Età minima dei documenti da sottoporre a scansione. Ad esempio, se si imposta <code>AfterDate</code> su cinque giorni, viene eseguita la scansione solo dei documenti che non hanno più di cinque giorni. <code>AfterDate</code> esamina la data dell'ultima modifica.</p> <p>È possibile immettere uno dei valori seguenti:</p> <p><code>N</code> di ore</p> <p><code>N</code> di giorni</p> <p><code>N</code> di settimane</p> <p><code>N</code> di mesi</p>
FolderCSVs	<p>Specificare le cartelle dell'archivio da cui recuperare i documenti. Tutte le voci devono iniziare con una barra, ma devono contenere anche altri caratteri. Lasciare la voce vuota per specificare tutte le cartelle. I file CAB sono considerati cartelle. Ad esempio:</p> <p><code>FolderCSVs=/support,/clients,/marketing,/finance</code></p>

Tabella 73-3 mostra il parametro `host` nel file `dmcl.ini`.

```
[DOCBROKER_PRIMARY]
host = documentum-server.mycompany.com
```

Durante l'installazione del rilevatore di Symantec Data Loss Prevention, il parametro `host` viene impostato nel file `dmcl.ini`. Se il broker di documenti Documentum (server) cambia in un secondo momento, il file deve essere modificato in modo che rimandi al nuovo server.

Tabella 73-3 File `dmcl.ini`

Parametro	Descrizione
host	Computer che ospita il broker di documenti Documentum (server).

Configurazione di esempio per la scansione di tutti i documenti in un archivio Documentum

Eseguire la scansione di tutti i documenti nell'archivio.

La configurazione è nel file `VontuDocumentumScanner.cfg`.

Vedere ["Opzioni di configurazione per i rilevatori di Documentum"](#) a pagina 2014.

```
//#####  
//#    Jobs  
//#####  
[JOBS]  
NUMBER=1  
0=Job0  
[Job0]  
DocBase=Vontu_1  
UserName=Administrator  
Password=mypassword  
ImportRefReplaceWithCSVs=  
    http://documentum-server.mycompany.com:8080/webtop/  
    component/drl?objectId=  
LogFile = Job0.log
```

Impostazione della scansione di archivi Livelink

Il capitolo contiene i seguenti argomenti:

- [Configurazione della scansione remota degli archivi OpenText \(Livelink\)](#)
- [Target del rilevatore OpenText \(Livelink\) supportati](#)
- [Creazione di un'origine dati ODBC per SQL Server](#)
- [Installazione di rilevatori Livelink](#)
- [Avvio delle scansioni di OpenText \(Livelink\)](#)
- [Opzioni di configurazione per rilevatori Livelink](#)
- [Configurazione di esempio per la scansione di un database LiveLink](#)

Configurazione della scansione remota degli archivi OpenText (Livelink)

Il rilevatore Livelink può eseguire la scansione di un database OpenText (Livelink).

Per configurare la scansione di archivi OpenText (Livelink), completare il seguente processo:

Tabella 74-1 Configurazione del rilevatore OpenText (Livelink)

Passaggio	Azione	Descrizione
1	Verificare che l'archivio OpenText (Livelink) si trovi nell'elenco di target supportati.	Vedere "Target del rilevatore OpenText (Livelink) supportati" a pagina 2019.

Passaggio	Azione	Descrizione
2	Creare un'origine dati ODBC per SQL Server. Installare il rilevatore Livelink.	Vedere "Creazione di un'origine dati ODBC per SQL Server" a pagina 2019. Vedere "Installazione di rilevatori Livelink" a pagina 2020.
3	Eseguire eventuali configurazioni manuali modificando i file di configurazione e di proprietà.	Vedere "Opzioni di configurazione per rilevatori Livelink" a pagina 2024.
4	Su Enforce Server, aggiungere un nuovo target Livelink del rilevatore.	Vedere "Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover" a pagina 1826.
5	Avviare la scansione Livelink. Avviare il rilevatore sul computer rilevatore e avviare inoltre la scansione sull'Enforce Server.	Vedere "Avvio delle scansioni di OpenText (Livelink)" a pagina 2022.
6	Verificare che l'esecuzione della scansione stia avvenendo correttamente.	Vedere "Risoluzione dei problemi dei rilevatori" a pagina 1978.

Target del rilevatore OpenText (Livelink) supportati

Il rilevatore Livelink supporta la scansione dei target di OpenText (Livelink) Server 9.x. Questa versione è obsoleta in Symantec Data Loss Prevention 15.1.

Creazione di un'origine dati ODBC per SQL Server

Questa procedura presuppone che il database Livelink sia un database SQL Server. Se si dispone di un database Oracle Livelink, contattare il supporto di Symantec Data Loss Prevention per specifiche istruzioni.

Per creare un'origine dati ODBC per SQL Server

- 1 Fare clic su **Pannello di controllo > Strumenti di amministrazione > Origini dati (ODBC)**.

Nota: Con i sistemi Windows a 64 bit, utilizzare lo strumento Amministratore ODBC a 32 bit per configurare l'origine dati. La versione a 32 bit è disponibile all'indirizzo `c:\windows\syswow64\odbcad32.exe`.

- 2 Fare clic sulla scheda **DSN di sistema**.

- 3 Fare clic su **Aggiungi**.
- 4 Selezionare **SQL Server**.
- 5 Assegnargli un nome (ad esempio, "OpenText"). Il file `VontuLivelinkScanner.cfg` fa riferimento a questo nome.
- 6 Fare clic su **Avanti**.
- 7 Selezionare **Autenticazione SQL Server tramite ID e password di accesso immessi dall'utente**.
- 8 Selezionare l'opzione **Connessione a SQL Server** per ottenere impostazioni predefinite per ulteriori opzioni di configurazione ed immettere le credenziali di SQL Server.
- 9 Fare clic su **Avanti**. Accettare i valori predefiniti.
- 10 Fare clic su **Avanti**. Accettare i valori predefiniti.
- 11 Fare clic su **Fine**.

Installazione di rilevatori Livelink

Installare il rilevatore Livelink su un computer con accesso al database OpenText (Livelink).

Per installare un rilevatore Livelink

- 1 Creare un'origine dati ODBC per SQL Server.
Vedere ["Creazione di un'origine dati ODBC per SQL Server"](#) a pagina 2019.
- 2 Sul computer con accesso al database OpenText (Livelink), scaricare il file di installazione. Scaricare o copiare (come file binario) il file `SymantecDLPScanners_windows_x32_15.0.exe` in una directory temporanea. Il file si trova nella directory `DLP_Home\Symantec_DLP_15.0_Win\Scanners` dove `DLP_Home` è il nome della directory in cui è stato decompresso il software Symantec Data Loss Prevention.
- 3 Avviare il programma di installazione del rilevatore su questo computer.
`SymantecDLPScanners_windows_x32_15.0.exe`

Nota: Questo analizzatore deve essere installato sui server Windows a 32 bit.

- 4 Confermare la versione del rilevatore che si desidera installare (32 bit).
- 5 Confermare il contratto di licenza.
- 6 Selezionare **Rilevatore Livelink**.

- 7 Selezionare la directory di destinazione dell'installazione, ossia la cartella in cui si desidera che venga installato il rilevatore Livelink.

Per impostazione predefinita la cartella è `C:\Programmi\LivelinkScanner\`.

Fare clic su **Avanti**.

- 8 Selezionare la cartella del menu Start (scorciatoia nel menu **Start**).

Il valore predefinito è **Rilevatore Livelink SymantecDLP**.

Fare clic su **Avanti**.

- 9 Immettere le seguenti informazioni sulla connessione per il server Network Discover:

- Host Discover (IP o nome host del server)
- Porta Discover

Fare clic su **Avanti**.

- 10 Immettere i seguenti valori di configurazione di Livelink per il rilevatore:

Host Livelink	Il nome host o l'indirizzo IP del server Livelink.
Porta Livelink	La porta HTTP del server Livelink.
Nome utente Livelink	Il nome utente da utilizzare quando si esegue la scansione.
Password Livelink	La password da utilizzare quando si esegue la scansione. Crittografare questa password. Vedere "Password crittografate nei file di configurazione" a pagina 1840.
Nome connessione di Livelink	Il nome della connessione di Livelink API. Questo nome è <code>dbconnection</code> nel file <code>opentext.ini</code> sul server Livelink.
Porta Livelink API	Questa porta deve essere 2099 a meno che non sia stata modificata nel file <code>opentext.ini</code> sul server Livelink. La porta predefinita è 2099.
DSN ODBC	Il nome dell'origine dati ODBC sul computer su cui viene eseguito il rilevatore Livelink.
Nome utente SQL	Nome utente da utilizzare per connettersi all'origine dati ODBC.
Password SQL	Password da utilizzare per connettersi all'origine dati ODBC. Crittografare questa password. Vedere "Password crittografate nei file di configurazione" a pagina 1840.

Fare clic su **Avanti**.

- 11 Il rilevatore viene installato.

12 Selezionare la modalità di avvio.

Mentre si eseguono test o verifiche iniziali sul corretto funzionamento del rilevatore, non selezionare nessuna di queste opzioni, ma avviare il rilevatore manualmente.

È possibile selezionare una delle seguenti opzioni (o nessuna):

- Installare come servizio su un sistema Windows
- Avviare dopo l'installazione.

Per impostazione predefinita, il rilevatore viene avviato manualmente.

13 L'installazione del rilevatore Livelink è completa nel computer del rilevatore.

14 Eseguire eventuali configurazioni manuali modificando i file di configurazione e di proprietà.

Vedere ["Opzioni di configurazione per rilevatori Livelink"](#) a pagina 2024.

Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.

Vedere ["File di configurazione del sistema di scansione"](#) a pagina 1982.

15 Copiare i seguenti file dall'installazione Livelink alla cartella `\LivelinkScanner\scanner:`

- `LAPI_ATTRIBUTES.dll`
- `LAPI_BASE.dll`
- `LAPI_DOCUMENTS.dll`
- `LAPI_USERS.dll`
- `LLKERNEL.dll`

16 Creare un'origine dati ODBC per l'istanza di database utilizzata da OpenText (Livelink).
Il file `VontuLivelinkScanner.cfg` fa riferimento a quest'origine dati.

Vedere ["Creazione di un'origine dati ODBC per SQL Server"](#) a pagina 2019.

17 Nell'Enforce Server, creare un nuovo target per il tipo di Livelink del rilevatore.

18 Avviare la scansione sia sul computer del rilevatore che su Enforce Server.

Vedere ["Avvio delle scansioni di OpenText \(Livelink\)"](#) a pagina 2022.

Avvio delle scansioni di OpenText (Livelink)

Assicurarsi che il rilevatore sia installato e configurato nel computer target e che un nuovo target sia aggiunto a Enforce Server.

Vedere ["Installazione di rilevatori Livelink"](#) a pagina 2020.

Avviare quindi la scansione.

Le procedure sono differenti per ognuno dei seguenti scenari:

- Un rilevatore per target (prima procedura).
- Molteplici rilevatori per un target (seconda procedura).

Per avviare una scansione Livelink con un rilevatore per un target

- 1 Accedere a Enforce Server.
Selezionare **Gestisci > Scansione Discover > Target di Discover** per visualizzare l'elenco dei target.
- 2 Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.
- 3 Nel computer del rilevatore, avviare il rilevatore Livelink.
Fare clic su **Start > Rilevatore Livelink Vontu > Console rilevatore Livelink Vontu**.
- 4 Il rilevatore avvia il processo di scansione dei dati.
Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.
- 5 Se la scansione non progredisce normalmente, è possibile eseguire una procedura di risoluzione dei problemi.
Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.
- 6 Arrestare e riavviare il rilevatore ogni volta che si modifica il file di configurazione. Per arrestare il rilevatore, premere CTRL-C nella finestra della console.

Per avviare una scansione Livelink con molteplici rilevatori per un target

- 1 In ognuno dei computer rilevatori, avviare il rilevatore Livelink.
Fare clic su **Start > Rilevatore Livelink Vontu > Console rilevatore Livelink Vontu**.
Assicurarsi che ogni rilevatore sia stato avviato e che abbia inviato informazioni. Controllare la cartella `outgoing` su ogni computer.
Vedere ["Struttura delle directory di installazione del rilevatore"](#) a pagina 1981.
- 2 Accedere a Enforce Server.
Selezionare **Gestisci > Scansione Discover > Target di Discover** per visualizzare l'elenco dei target.
- 3 Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio.
- 4 Il rilevatore avvia il processo di scansione dei dati.
Vedere ["Funzionamento dei rilevatori di Network Discover"](#) a pagina 1977.

- 5 Se la scansione non progredisce normalmente, è possibile eseguire una procedura di risoluzione dei problemi.
Vedere ["Risoluzione dei problemi dei rilevatori"](#) a pagina 1978.
- 6 Arrestare e riavviare il rilevatore ogni volta che si modifica il file di configurazione. Per arrestare il rilevatore, premere CTRL-C nella finestra della console.

Opzioni di configurazione per rilevatori Livelink

Tabella 74-2 fornisce una spiegazione del file `VontuLivelinkScanner.cfg`.

Tabella 74-2 Parametri nel file `VontuLivelinkScanner.cfg`

Tipo	Parametro	Descrizione
Connettività	<code>OpenTextServer</code>	Il nome host o l'indirizzo IP del server Livelink.
Connettività	<code>OpenTextPort</code>	La porta HTTP del server Livelink.
Connettività	<code>OpenTextUsername</code>	Il nome utente da utilizzare quando si esegue la scansione.
Connettività	<code>OpenTextPassword</code>	La password da utilizzare quando si esegue la scansione. Crittografare questa password. Vedere "Password crittografate nei file di configurazione" a pagina 1840.
Connettività	<code>LLConnection</code>	Il nome della connessione di OpenText (Livelink attivo) API. Questo parametro è il nome di <code>dbconnection</code> nel file <code>opentext.ini</code> sul server Livelink.
Connettività	<code>LLApiPort</code>	Questo valore deve essere 2099 a meno che non sia stato modificato nel file <code>opentext.ini</code> sul server di OpenText (Livelink).
Connettività	<code>DSN</code>	Il nome dell'origine dati ODBC sul computer su cui viene eseguito il rilevatore OpenText (Livelink).
Connettività	<code>SQLUserName</code>	Nome utente da utilizzare per connettersi all'origine dati ODBC.
Connettività	<code>SQLPassWord</code>	Password da utilizzare per connettersi all'origine dati ODBC. Crittografare questa password. Vedere "Password crittografate nei file di configurazione" a pagina 1840.

Tipo	Parametro	Descrizione
Limitazione	BatchSize	<div>Il numero di file che vengono aggregati prima di essere importati in ogni file XML inviato a Network Discover.</div> <div>Vedere "Ottimizzazione delle risorse con le opzioni di limitazione delle scansioni di Network Discover/Cloud Storage Discover" a pagina 1847.</div>

Configurazione di esempio per la scansione di un database LiveLink

Eseguire la scansione nel database LiveLink.

La configurazione è nel file `VontuLivelinkScanner.cfg`.

Vedere ["Opzioni di configurazione per rilevatori Livelink"](#) a pagina 2024.

```
//#####  
//#    Jobs  
//#####  
[JOBS]  
Number=1  
0=Job0  
[Job0]  
OpenTextServer=mydatabase-Livelink.test.lab  
OpenTextPort=80  
OpenTextUsername=Admin  
OpenTextPassword=Livelink  
LLConnection=LivelinkDB  
LLApiPort=2099  
DSN=Livelink  
SQLUserName=lldbuser  
SQLPassWord=Livelink
```

Impostazione dei servizi Web per target di scansione personalizzati

Il capitolo contiene i seguenti argomenti:

- [Configurazione dei servizi Web per target di scansione personalizzati](#)
- [Informazioni sulla configurazione della lingua di definizione del servizio Web \(WSDL\)](#)
- [Esempio di un client Java di servizi Web](#)
- [Codice campione Java per l'esempio di Servizi Web](#)

Configurazione dei servizi Web per target di scansione personalizzati

Il tipo di target di servizi Web consente ai clienti di creare rilevatori personalizzati. Questi rilevatori personalizzati inviano il contenuto e i metadati a Network Discover come richieste SOAP (Simple Object Access Protocol). Il server Network Discover diventa un host di servizi Web.

Vedere ["Informazioni sulla configurazione della lingua di definizione del servizio Web \(WSDL\)"](#) a pagina 2027.

È disponibile un esempio di client SOAP Java.

Vedere ["Esempio di un client Java di servizi Web"](#) a pagina 2027.

Per configurare servizi web personalizzati per Network Discover, completare il processo seguente:

Tabella 75-1 Configurazione di un target di scansione personalizzato

Passaggio	Azione	Descrizione
1	Aggiungere un tipo di target di servizi Web.	Vedere "Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover" a pagina 1826.
2	Avviare la scansione.	Selezionare il target di scansione nell'elenco dei target, quindi fare clic sull'icona Avvio. Vedere "Gestione delle scansioni target di Network Discover/Cloud Storage Discover" a pagina 1853.
3	Salvare e modificare il file WSDL e creare un client (come un client Java) o una richiesta SOAP.	Vedere "Informazioni sulla configurazione della lingua di definizione del servizio Web (WSDL)" a pagina 2027. È disponibile un esempio di client Java. Vedere "Esempio di un client Java di servizi Web" a pagina 2027.
4	Eseguire il client e verificare i risultati.	Vedere "Esempio di un client Java di servizi Web" a pagina 2027.

Informazioni sulla configurazione della lingua di definizione del servizio Web (WSDL)

La lingua di definizione del servizio Web (WSDL) può essere scaricata dall'URL seguente quando un target di servizi Web è in esecuzione. La porta indicata è quella predefinita. Immettere la posizione del server Network Discover e il numero di porta.

`http://discover_server:8090/?wsdl`

Consultare la guida in linea per un esempio di richiesta WSDL e SOAP di servizi Web.

Esempio di un client Java di servizi Web

La procedura e il codice seguenti forniscono un esempio di servizi Web. Questo esempio invia il contenuto e i metadati di tutti i file a una cartella del server Network Discover.

Per creare ed eseguire un client Java di servizi Web

- 1 Accedere a Enforce Server e creare un tipo di target di servizi Web di Network Discover.
Vedere ["Aggiunta di un nuovo target di Network Discover/Cloud Storage Discover"](#) a pagina 1826.

Utilizzare le impostazioni predefinite. Il numero di porta predefinito del rilevatore è 8090.

- 2 Avviare la scansione.
- 3 Accedere al seguente URL:

```
http://discover_server:8090/?wsdl
```

Salvare la pagina come file WSDL denominato `DiscoverSOAPTTarget.wsdl` in una cartella (ad esempio `cartella_esempio`).

Modificare l'URL per sostituire il numero di porta 8090 se il numero di porta del rilevatore è differente nel passaggio 1.

- 4 Installare Java Development Kit (JDK) se non è disponibile nel sistema.
- 5 Impostare come cartella principale di Java quella in cui si è installato JDK.

```
JAVA_HOME=jdk_install_dir
```

- 6 Installare Apache CXF, un framework di servizi open source.
Vedere <http://cxf.apache.org/>
- 7 Trasformare WSDL in codice Java.

```
apache-cxf-installdir\bin\wsdl2java  
-client sample_folder\DiscoverSOAPTTarget.wsdl
```

I file di origine Java sono creati automaticamente nei pacchetti `com.vontu.discover` e `com.vontu.wsdl.discoversoaptarget`.

- 8 Modificare un file denominato `DiscoverSOAPClient.java` nella `cartella_esempio` e inserire il codice Java. Posizionare il nuovo codice all'inizio di questo file. Cambiare le costanti in base alle esigenze.

Vedere ["Codice campione Java per l'esempio di Servizi Web"](#) a pagina 2029.

- 9 Compilare il codice Java con il comando seguente:

```
javac DiscoverSOAPClient.java
```


10 Eseguire il programma utilizzando il comando seguente:

```
java DiscoverSOAPClient
```

11 Su Enforce Server, verificare che sia segnalato il numero previsto di elementi per il target di Network Discover creato nel passaggio 1.

Codice campione Java per l'esempio di Servizi Web

Inserire il seguente codice sorgente all'inizio del file nominato `DiscoverSOAPClient.java`.

Vedere ["Esempio di un client Java di servizi Web"](#) a pagina 2027.

```
import javax.xml.datatype.DatatypeFactory;
import javax.xml.namespace.QName;
import java.io.ByteArrayOutputStream;
import java.io.File;
import java.io.FileInputStream;
import java.net.URL;
import java.util.Date;

import com.vontu.discover.ComponentContentType;
import com.vontu.discover.ComponentType;
import com.vontu.discover.DocumentType;
import com.vontu.discover.ProcessDocumentsType;
import com.vontu.wsdl.discoversoaptarget.DiscoverSOAPTargetPortType;
import com.vontu.wsdl.discoversoaptarget.DiscoverSOAPTargetService;
import com.sun.org.apache.xerces.internal.impl.dv.util.Base6

public class DiscoverSOAPClient

{
    private static final QName SERVICE_NAME = new QName(
        "http://www.vontu.com/wsdl/DiscoverSOAPTarget.wsdl",
        "DiscoverSOAPTarget_Service");
    private static final String OWNER = "DiscoverSOAPClient";
    private static final String BODY = "This is the body";
    private static final String TYPE = "Text";
    private static final String ENCODING = "base64";

    //Change this value according to your needs
    private static final String TEST_FOLDER_NAME = "c:\\temp\\data";

    //Change this based on your discover host name and scanner port
```

```
private static final String WSDL_PATH =
    "http://localhost:8090/?wsdl";

public static void main(String []args)
{
    try
    {
        URL wsdl = new URL(WSDL_PATH);
        File folder = new File(TEST_FOLDER_NAME);
        DiscoverSOAPTargetService service =
            new DiscoverSOAPTargetService(wsdl, SERVICE_NAME);
        DiscoverSOAPTargetPortType client = service.getDiscoverPort();
        for(File file : folder.listFiles())
        {
            if(file.isDirectory())
            {
                //only files in the test folder are sent to Discover
                continue;
            }
            System.out.println(file);
            ProcessDocumentsType processDocumentsType =
                new ProcessDocumentsType();
            DocumentType documentType = new DocumentType();
            processDocumentsType.getDocument().add(documentType);
            documentType.setOwner(OWNER);
            documentType.setURI(file.toString());
            GregorianCalendar time = new GregorianCalendar();
            time.setTime(new Date(file.lastModified()));
            documentType.setLastModifiedDate(
                DatatypeFactory.newInstance().
                    newXMLGregorianCalendar(time));
            documentType.setLastModifiedDate(
                DatatypeFactory.newInstance().
                    newXMLGregorianCalendar(time));

            //create a component
            ComponentType body = new ComponentType();
            documentType.setComponent(body);
            body.setName(file.getName());

            //add body
            ComponentContentType bodyContent =
                new ComponentContentType();
```

```

        body.setComponentContent(bodyContent);
bodyContent.setType(TYPE);
bodyContent.setContent(BODY);

ComponentType attachment = new ComponentType();
body.getComponent().add(attachment);
attachment.setName(file.getName());

//add some content to the component
ComponentContentType attachmentContent =
    new ComponentContentType();
attachment.setComponentContent(attachmentContent);
attachmentContent.setType(ENCODING);

ByteArrayOutputStream bytes =
    new ByteArrayOutputStream();
FileInputStream in = new FileInputStream(file);
byte[] buf = new byte[1024];

for(;;)
{
    int len = in.read(buf);
    if(len == -1)
    {
        break;
    }
    bytes.write(buf,0,len);
}

attachmentContent.setContent(
    Base64.encode(bytes.toByteArray()));

//make the SOAP call
client.processDocuments(processDocumentsType);
}

} catch(Exception e)
{
}
}
}

```

Individuazione e prevenzione di perdita di dati su endpoint

- [Capitolo 76. Panoramica di Symantec Data Loss Prevention per endpoint](#)
- [Capitolo 77. Riepilogo di DLP Agent per supporto Mac](#)
- [Capitolo 78. Utilizzo di Endpoint Prevent](#)
- [Capitolo 79. Utilizzo di Endpoint Discover](#)
- [Capitolo 80. Utilizzo delle configurazioni agente](#)
- [Capitolo 81. Utilizzo di gruppi di agenti](#)
- [Capitolo 82. Gestione di Symantec DLP Agent](#)
- [Capitolo 83. Utilizzo del controllo applicazioni](#)
- [Capitolo 84. Utilizzo di Endpoint FlexResponse](#)
- [Capitolo 85. Utilizzo degli strumenti Endpoint](#)

Panoramica di Symantec Data Loss Prevention per endpoint

Il capitolo contiene i seguenti argomenti:

- [Informazioni sull'individuazione e prevenzione della perdita di dati su endpoint](#)
- [Linee guida per la creazione di politiche endpoint](#)

Informazioni sull'individuazione e prevenzione della perdita di dati su endpoint

Per utilizzare funzionalità di Endpoint Discover o Endpoint Prevent, è necessario distribuire DLP Agent ed Endpoint Server.

Sia Endpoint Prevent sia Endpoint Discover applicano politiche di Data Loss Prevention per proteggere i dati sensibili o a rischio. I dati sensibili o a rischio possono includere numeri di carta di credito o nomi, indirizzi e numeri di identificazione. È possibile configurare entrambi i prodotti per riconoscere e proteggere i file che contengono dati sensibili.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Endpoint Prevent impedisce ai dati sensibili di essere spostati all'esterno degli endpoint e dei desktop virtuali supportati. Ad esempio, Endpoint Prevent può impedire a un file che contiene numeri di carta di credito di essere trasferito su supporti connessi tramite eSATA, USB o Firewire. Endpoint Prevent impedisce ai file sensibili di essere trasferiti su condivisioni di rete mentre Endpoint Prevent è in grado di monitorare e impedire il trasferimento dei dati alle applicazioni specificate.

Endpoint Discover esegue la scansione delle unità disco rigido interne di un endpoint per identificare i dati confidenziali memorizzati e consentire azioni per inserire in inventario, proteggere o riassegnare questi dati. Consente una scansione ad alte prestazioni in parallelo di migliaia endpoint con un effetto minimo sul sistema. Ogni DLP Agent può eseguire la scansione di circa 5 GB/h. Gli utenti possono configurare scansioni di Endpoint Discover per utilizzare più Endpoint Server al fine di aumentare le prestazioni e la disponibilità di scansione. Endpoint Discover può mettere automaticamente in quarantena i file confidenziali in locale in una cartella sul computer endpoint di Windows (in una cartella crittografata) o a distanza in una cartella in rete. [Tabella 76-1](#) fornisce la descrizione di queste funzionalità e indica dove trovare ulteriori informazioni.

Vedere ["Informazioni su Endpoint Discover"](#) a pagina 78.

È possibile configurare le impostazioni dell'agente, raggruppare gli agenti, impostare regole di risposta, verificare lo stato dell'agente e risolvere i problemi degli agenti.

Tabella 76-1 Funzionalità di Endpoint

Funzionalità	Descrizione	Informazioni aggiuntive
Configurazione agente	È possibile selezionare quali canali di ingresso dell'endpoint monitorare e ottimizzare il monitoraggio scegliendo i filtri appropriati. È inoltre possibile configurare i limiti di larghezza di banda della comunicazione dell'agente del server e il consumo delle risorse dell'agente.	Vedere "Informazioni sulle configurazioni dell'agente" a pagina 2110.
Gruppi di agenti	Utilizzare i gruppi di agenti per inviare configurazioni di agente a gruppi di agenti.	Vedere "Informazioni sui gruppi di agenti" a pagina 2181.
Gestione e stato dell'agente	È possibile esaminare lo stato dell'integrità del DLP Agent ed eseguire le attività di risoluzione dei problemi e di gestione.	Vedere "Informazioni sull'amministrazione di Symantec DLP Agent" a pagina 2194.
Controllo applicazioni	È possibile configurare questa funzionalità per monitorare le applicazioni relative alla masterizzazione di CD/DVD, IM, e-mail o client HTTP/S.	Vedere "Informazioni sul controllo delle applicazioni" a pagina 2231.
FlexResponse	È possibile creare le regole di risposta che riparano automaticamente gli incidenti.	Vedere "Informazioni su Endpoint FlexResponse" a pagina 2248.

Funzionalità	Descrizione	Informazioni aggiuntive
Strumenti di Endpoint	Utilizzare gli strumenti di Endpoint per completare le varie attività di manutenzione sull'endpoint come arrestare i servizi watchdog, ispezionare il database dell'agente e riavviare gli agenti di Mac.	Vedere "Informazioni sulla gestione delle password dell'agente" a pagina 2259 a pagina 2259.

Durante la distribuzione del proprio endpoint, tenere conto delle differenze nelle funzionalità supportate tra DLP Agent per Mac o Windows. Vedere ["Informazioni sul supporto a livello di funzionalità di DLP Agent"](#) a pagina 2038.

Linee guida per la creazione di politiche endpoint

Symantec Data Loss Prevention utilizza un'architettura di rilevamento a due livelli per analizzare l'attività sugli endpoint. Il rilevamento avviene direttamente su DLP Agent o su Endpoint Server, in base alle esigenze. Endpoint Server può eseguire tutti i tipi di rilevamento, come Exact Data Matching (EDM), Indexed Document Matching (IDM) e Directory Group Matching (DGM). Gli agenti possono eseguire Described Content Matching (DCM) e Indexed Document Matching (IDM). Symantec Data Loss Prevention può rilevare localmente su parole chiave, espressioni regolari e identificatori dati. Deve inviare il contenuto di input a Endpoint Server per rilevare le impronte di dati esatte o impronte documento indicizzate.

Nota: Gli agenti in esecuzione su endpoint Mac possono eseguire solo il rilevamento IDM e DCM.

Il rilevamento a due livelli ha implicazioni per i tipi di regole di rilevamento e regole di risposta che possono essere combinate in una politica e utilizzate negli endpoint. Ha inoltre implicazioni per l'ottimizzazione di prestazioni e utilizzo di sistema di Symantec Data Loss Prevention sugli endpoint. Durante la creazione di politiche applicate agli endpoint, sono consigliate le seguenti linee guida.

Non creare una politica che combina una regola di rilevamento lato server con una regola di risposta Endpoint Prevent. Ad esempio, non combinare una regola EDM o DGM con una regola di risposta Endpoint: blocca o Endpoint: notifica. Se una regola di rilevamento lato server attiva una regola di risposta Endpoint Prevent, Symantec Data Loss Prevention non può eseguire la regola di risposta Endpoint Prevent e il sistema visualizza un messaggio di errore.

Vedere ["Creazione di politiche per limitare l'effetto potenziale del rilevamento in due fasi"](#) a pagina 469.

Durante la creazione di una politica endpoint che include una regola di rilevamento lato server, combinare tale regola di rilevamento con una regola di rilevamento lato agente in una regola composta. Questa pratica aiuta Symantec Data Loss Prevention a eseguire il rilevamento sull'endpoint senza inviare il contenuto all'Endpoint Server. Symantec Data Loss Prevention preserva la larghezza di banda di rete e migliora le prestazioni eseguendo il rilevamento sull'endpoint.

Ad esempio, è possibile accoppiare una regola di rilevamento EDM con una regola di rilevamento parola chiave in una regola composta. In una regola composta, tutte le condizioni devono essere rispettate prima che Symantec Data Loss Prevention registri una corrispondenza. Per contro, se una condizione non viene rispettata, Symantec Data Loss Prevention determina che non è presente alcuna corrispondenza senza necessità di verificare la seconda condizione. Ad esempio, per registrare una corrispondenza il contenuto deve rispettare la prima condizione E tutte le altre condizioni nella stessa regola. Quando viene configurata la regola composta in questo modo, DLP Agent verifica prima il contenuto di input rispetto alla regola lato agente. Se non è presente alcuna corrispondenza, Symantec Data Loss Prevention non deve inviare il contenuto a Endpoint Server. Tuttavia, se viene creata una regola composta che coinvolge una politica DCM o EDM, il contenuto è ancora inviato all'Endpoint Server.

Prima di combinare una regola di rilevamento lato server (ad esempio, una regola EDM) con una regola di risposta Tutto: limita conservazione dati incidenti che conserva i file originali per gli incidenti endpoint, considerare le implicazioni della larghezza di banda nel conservare i file originali. Quando invia dati a un Endpoint Server per l'analisi, DLP Agent invia dati testo o dati binari in base ai requisiti della politica. Quando possibile, DLP Agent invia testo per ridurre l'utilizzo della larghezza di banda. Per impostazione predefinita, Symantec Data Loss Prevention elimina i file originali per gli incidenti endpoint. Se una regola di risposta conserva i file originali per gli incidenti endpoint, DLP Agent deve inviare i dati binari all'Endpoint Server. In questo caso, verificare che la rete sia in grado di gestire l'incremento del traffico tra DLP Agent ed Endpoint Server senza compromettere le prestazioni.

Combinare le regole di rilevamento lato agente (ad esempio, DCM) con una regola di risposta Endpoint Prevent nella stessa politica. Symantec Data Loss Prevention può eseguire una regola di risposta Endpoint Prevent solo quando una regola di rilevamento DLP Agent attiva la risposta.

[Tabella 76-2](#) elenca le regole di risposta e rilevamento che non possono essere combinate.

Tabella 76-2 Regole di risposta e di rilevamento incompatibili

Non combinare queste regole di rilevamento basate su server...	...con queste regole di risposta Endpoint Prevent.
<ul style="list-style-type: none"> ■ Contenuto corrispondente a dati esatti (EDM) ■ Mittente/utente corrispondente a directory (DGM con profilo) ■ Destinatario corrispondente a directory (DGM con profilo) 	<ul style="list-style-type: none"> ■ Endpoint: blocca ■ Endpoint: notifica ■ Endpoint: operazione annullata dall'utente

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

Riepilogo di DLP Agent per supporto Mac

Il capitolo contiene i seguenti argomenti:

- [Informazioni sul supporto a livello di funzionalità di DLP Agent](#)
- [Installazione dell'agente Mac e dettagli sulle funzionalità degli strumenti](#)
- [Caratteristiche di gestione dell'agente Mac](#)
- [Panoramica delle tecnologie di rilevamento dell'agente Mac e delle funzionalità di creazione di politiche](#)
- [Supporto di monitoraggio dell'agente Mac](#)
- [Caratteristiche delle impostazioni dell'agente avanzate di Endpoint Prevent per l'agente Mac](#)
- [Funzionalità dei target Endpoint Discover per Mac](#)
- [Supporto Endpoint Discover per file system Mac](#)
- [Supporto di impostazioni agente avanzate di Endpoint Discover per Mac](#)

Informazioni sul supporto a livello di funzionalità di DLP Agent

Symantec Data Loss Prevention consente di monitorare gli endpoint Windows e Mac. Tuttavia, il supporto di livello funzionalità varia in base al sistema operativo.

I seguenti argomenti riepilogano il supporto di livello funzionalità DLP Agent per Mac relativo a Windows. È importante tenere presenti le differenze del supporto di livello funzionalità quando si pianifica la distribuzione.

Il supporto di livello di funzionalità agente per endpoint Mac include quanto segue:

- **Installazione**
Vedere ["Supporto di installazione agente Mac"](#) a pagina 2039.
- **Strumenti endpoint**
Vedere ["Funzionalità degli strumenti per endpoint Mac"](#) a pagina 2040.
- **Posizione endpoint**
Vedere ["Posizione endpoint agente Mac"](#) a pagina 2041.
- **Gruppi di agenti**
Vedere ["Funzionalità gruppi agente Mac"](#) a pagina 2041.
- **Tecnologie di rilevamento**
Vedere ["Tecnologie di rilevazione dell'agente Mac"](#) a pagina 2042.
- **Regole di risposta e di politica**
Vedere ["Funzionalità della regola di risposta della politica dell'agente Mac"](#) a pagina 2047.
- **Supporto di monitoraggio**
Vedere ["Supporto di monitoraggio dell'agente Mac"](#) a pagina 2061.
- **Impostazioni dell'agente avanzate Endpoint Prevent**
Vedere ["Caratteristiche delle impostazioni dell'agente avanzate di Endpoint Prevent per l'agente Mac"](#) a pagina 2057.
- **Funzionalità Endpoint Discover**
Vedere ["Funzionalità dei target Endpoint Discover per Mac"](#) a pagina 2058.
Vedere ["Supporto Endpoint Discover per file system Mac"](#) a pagina 2059.
Vedere ["Supporto di impostazioni agente avanzate di Endpoint Discover per Mac"](#) a pagina 2059.

Installazione dell'agente Mac e dettagli sulle funzionalità degli strumenti

È possibile installare manualmente un agente o utilizzare gli strumenti di distribuzione degli endpoint (ad esempio, Apple Remote Desktop e Casper) per installare agenti su molti endpoint Mac.

Supporto di installazione agente Mac

Per installare DLP Agent su endpoint Mac, creare un pacchetto di installazione nella schermata **Pacchetto agenti** della console di amministrazione Enforce Server.

[Tabella 77-1](#) fornisce informazioni aggiuntive relative al supporto di installazione.

Tabella 77-1 Supporto di installazione agente Mac

Supportato	Non supportato
<ul style="list-style-type: none"> ■ Installazione della riga di comando per l'installazione manuale di un singolo agente. ■ È possibile trovare più informazioni nell'argomento "Operazioni per l'installazione di DLP Agent su Mac" del <i>Manuale di installazione di Symantec Data Loss Prevention</i>. ■ Installazione di molti agenti tramite gli strumenti di distribuzione endpoint. ■ È possibile individuare più informazioni nell'argomento "Installazione silenziosa di DLP Agent su endpoint Mac" nel <i>Manuale di installazione di Symantec Data Loss Prevention</i>. 	<ul style="list-style-type: none"> ■ Programma di installazione basato su UI per singola installazione manuale dell'agente. ■ Disattivazione della password di disinstallazione dell'agente utilizzando l'attività di risoluzione dei problemi Attiva password di disinstallazione.

Funzionalità degli strumenti per endpoint Mac

[Tabella 77-2](#) fornisce informazioni sul supporto degli strumenti per gli endpoint per il DLP Agent Mac.

Tabella 77-2 Funzionalità degli strumenti per endpoint

Supportato	Non supportato
<ul style="list-style-type: none"> ■ create_package ■ DeviceID ■ logdump ■ start_agent ■ uninstall_agent ■ vontu_sqlite3 ■ service_shutdown 	<ul style="list-style-type: none"> ■ GetAppInfo È possibile usare l'applicazione di controllo dell'attività per raccogliere le stesse informazioni. Vedere "Definizione dei nomi binari delle applicazioni macOS" a pagina 2244.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Caratteristiche di gestione dell'agente Mac

Symantec Data Loss Prevention fornisce la possibilità di generare informazioni di posizione per gli incidenti registrati da DLP Agent Mac.

Posizione endpoint agente Mac

Tabella 77-3 Posizione endpoint agente Mac

Supportato	Non supportato
<ul style="list-style-type: none"> Posizione automatica 	<ul style="list-style-type: none"> Manuale Se l'opzione Manuale è selezionata, tutti gli incidenti indicano che l'incidente è stato registrato mentre l'agente si trovava fuori dalla rete d'impresa.

Vedere ["Configurazione della posizione dell'endpoint"](#) a pagina 2076.

Funzionalità gruppi agente Mac

Tabella 77-4 Funzionalità gruppi agente Mac

Supportato	Non supportato
<ul style="list-style-type: none"> Condizione gruppo di server Endpoint Attributi agente: <ul style="list-style-type: none"> Dominio host agente Tipo host agente Versione host agente Utente connesso Dominio utente connesso Attributi personalizzati basati su Active Directory 	Attributi personalizzati basati su Active Directory

Vedere ["Creazione e gestione degli attributi dell'agente"](#) a pagina 2184.

Panoramica delle tecnologie di rilevamento dell'agente Mac e delle funzionalità di creazione di politiche

DLP Agent di Mac supporta Described Content Matching (DCM), che include il rilevamento tramite l'identificatore dati, l'espressione regolare e regole di parola chiave. DLP Agent di Mac supporta Indexed Document Matching (IDM). DLP Agent di Mac supporta Directory Group Matching (DGM) per le politiche basate su Gruppi utenti che applicano la regola Mittente/utente basato su gruppo di server di directory. L'agente supporta inoltre diverse regole di risposta per Endpoint Prevent e Endpoint Discover.

Tecnologie di rilevazione dell'agente Mac

Le seguenti funzionalità di tecnologia di rilevamento si applicano sia a Endpoint Prevent sia a Endpoint Discover.

Tabella 77-5 Supporto della tecnologia di rilevazione per endpoint Mac

Supportato	Non supportato
	<ul style="list-style-type: none">■ Exact Data Matching (EDM)■ Vector Machine Learning (VML)■ Rilevamento a due fasi■ Directory Group Matching (DGM) per le politiche basate su Gruppi utenti che applicano la regola Destinatario basato su gruppo di server di directory.

Supportato	Non supportato
<ul style="list-style-type: none"> ■ Described Content Matching (DCM) per rilevare il contenuto e il contesto seguenti: <ul style="list-style-type: none"> ■ Identificatori di dati Vedere "Introduzione agli identificatori di dati" a pagina 681. ■ Parole chiave Vedere "Introduzione alla corrispondenza con parole chiave" a pagina 771. ■ Espressioni regolari Vedere "Introduzione alla corrispondenza con espressioni regolari" a pagina 787. ■ Proprietà file Vedere "Introduzione al rilevamento di proprietà di file" a pagina 808. ■ Criteri utente, destinatario e mittente Vedere "Introduzione alla corrispondenza con identità descritte" a pagina 835. ■ Firme di protocollo Vedere "Introduzione al monitoraggio di protocolli per la rete" a pagina 821. ■ Destinazioni, dispositivi e protocolli Vedere "Introduzione al rilevamento di eventi endpoint" a pagina 824. ■ Directory Group Matching (DGM) per le politiche basate su Gruppi utenti che applicano la regola Mittente/utente basato su gruppo di server di directory. Vedere "Configurazione della condizione Mittente/utente basato su gruppo di server di directory" a pagina 851. ■ Indexed Document Matching (IDM) che utilizza la corrispondenza parziale nei seguenti scenari di rilevazione: <ul style="list-style-type: none"> ■ I dati spostati su dispositivi di archiviazione rimovibili e condivisioni di rete tramite operazioni Salva con nome vengono monitorati mediante IDM con corrispondenza parziale ■ I dati incollati su browser o altre applicazioni configurate vengono monitorati tramite l'IDM con corrispondenza parziale Vedere "Introduzione a Indexed Document 	

Supportato	Non supportato
Matching (IDM)" a pagina 569.	

Scenari della politica di tecnologia di rilevamento agente Mac

Se una politica utilizza sia le tecnologie di sostegno supportate sia quelle non supportate, il DLP Agent Mac applica le regole di rilevamento DCM e IDM nelle eccezioni e nelle politiche che non forniscono corrispondenze per le tecnologie di rilevazione non supportate.

[Tabella 77-6](#) descrive le configurazioni della politica che l'organizzazione può usare e definisce se il rilevamento deve essere applicato agli endpoint Mac per ciascuna di esse.

Tabella 77-6 Regole della politica e scenari di rilevamento per gli endpoint Mac

Configurazione della politica	Rilevamento applicato agli endpoint Mac	Descrizione
Regola DCM OR Regole VML o EDM	La regola DCM viene applicata	Se la politica utilizza la corrispondenza delle parole chiave con la corrispondenza dell'indice EDM (collegato tramite l'espressione OR), i documenti che contengono la parola chiave registrano gli incidenti. Tuttavia, se il documento non contiene la parola chiave ma corrisponde all'indice EDM, non viene registrato alcun incidente. L'indice EDM non viene applicato.
Regola DCM AND Regole VML o EDM	Non vengono applicate regole	Se la politica utilizza la corrispondenza delle parole chiave con la corrispondenza esatta dell'indice EDM (collegato tramite l'espressione AND), i documenti che contengono la parola chiave registrano gli incidenti, anche se il documento corrisponde all'indice EDM. L'indice EDM non viene applicato.

Configurazione della politica	Rilevamento applicato agli endpoint Mac	Descrizione
<p>Regola di eccezione in una politica che contiene il rilevamento DCM</p> <p>OR</p> <p>Regola di eccezione in una politica che contiene regole EDM o VML</p>	Viene applicata l'eccezione DCM	<p>Se la politica utilizza un'eccezione con corrispondenza delle parola chiave (ad esempio, "riservato") e utilizza la corrispondenza del profilo EDM (collegato dall'espressione O), il documento che contiene la parola chiave "riservato" viene escluso dal monitoraggio.</p> <p>Tuttavia, se il documento non contiene la parola chiave "riservato" ma corrisponde all'indice EDM, il documento non viene escluso dal monitoraggio. In questo scenario viene applicata solo la regola di eccezione DCM. I documenti che corrispondono all'indice EDM non vengono esclusi dal monitoraggio.</p>
<p>Regola di eccezione in una politica che contiene il rilevamento DCM</p> <p>AND</p> <p>Regola di eccezione in una politica che contiene EDM o VML</p>	Non vengono applicate eccezioni	<p>Se la politica utilizza un'eccezione con corrispondenza delle parola chiave (ad esempio, "riservato") e la corrispondenza del profilo EDM (collegato dall'espressione AND), il documento che contiene la parola chiave "riservato" viene esclusa dal monitoraggio anche se il documento corrisponde all'indice EDM. I documenti che corrispondono all'indice EDM non vengono esclusi dal monitoraggio.</p>
<p>Regola DCM</p> <p>AND</p> <p>Regola di eccezione in una politica che contiene EDM o VML</p>	La regola DCM viene applicata	<p>Se la politica utilizza la corrispondenza delle parole chiave (ad esempio "riservato") e un'eccezione del profilo EDM (collegato tramite l'espressione AND), i documenti che contengono la parola chiave registrano gli incidenti.</p> <p>Tuttavia, i documenti che corrispondono all'indice EDM non vengono esclusi dal monitoraggio.</p>

Vedere ["Informazione sulla creazione di politiche per Endpoint Prevent"](#) a pagina 2073.

Funzionalità della regola di risposta della politica dell'agente Mac

Le seguenti funzionalità della regola di risposta della politica si applicano a Endpoint Prevent e Endpoint Discover come descritto.

Vedere ["Informazioni sul monitoraggio di politiche con regole di risposta per Endpoint Server"](#) a pagina 2073.

Funzionalità delle regole di risposta di Endpoint Discover su Mac

Se le regole di risposta non supportate fanno parte di una politica applicata agli endpoint Mac, gli incidenti vengono registrati, ma l'agente non applica le regole di risposta non supportate.

Tabella 77-7 Regole di risposta di Symantec Data Loss Prevention

Supportato	Non supportato
<ul style="list-style-type: none"> ■ Aggiungi nota ■ Registrazione a un server Syslog ■ Invia notifica e-mail ■ Imposta stato ■ Limita conservazione dati incidenti 	<ul style="list-style-type: none"> ■ File in quarantena Endpoint Discover: ■ Endpoint FlexResponse

Funzionalità delle regole di risposta di Endpoint Prevent su Mac

Nella maggior parte dei casi, se le regole di risposta non supportate fanno parte di una politica applicata agli endpoint Mac, gli incidenti vengono registrati, ma l'agente non applica le regole di risposta.

Tabella 77-8 Regole di risposta di Endpoint Prevent

Supportate	Non supportate
<ul style="list-style-type: none"> ■ Endpoint: notifica ■ Endpoint: blocca ■ Endpoint Prevent: crittografia ■ Aggiungi nota ■ Registrazione a un server Syslog ■ Invia notifica e-mail ■ Imposta stato ■ Limita conservazione dati incidenti 	<ul style="list-style-type: none"> ■ Endpoint: operazione annullata dall'utente ■ Endpoint FlexResponse ■ Regola di risposta Limita conservazione dati incidenti combinata con la configurazione Endpoint: blocca utilizzata con Accesso ai file di applicazione <p>Se queste regole di risposta vengono utilizzate insieme, i file riservati vengono bloccati, ma i file bloccati non sono accessibili nell'incidente Accesso ai file di applicazione.</p>

Vedere ["Azioni delle regole di risposta per il rilevamento di endpoint"](#) a pagina 1470.

Supporto di monitoraggio dell'agente Mac

La seguente sezione fornisce informazioni su canali, applicazioni e filtri di file monitorati da DLP Agent Mac.

Tabella 77-9 Monitoraggio dei canali supportati su endpoint Mac

Supportato	Non supportato
<ul style="list-style-type: none"> ■ Destinazioni <ul style="list-style-type: none"> ■ Archivi rimovibili Vedere "Funzionalità dispositivo di archiviazione rimovibile agente Mac" a pagina 2049. ■ Appunti <ul style="list-style-type: none"> ■ Incolla Vedere "Funzionalità degli Appunti supportate su agenti Mac" a pagina 2051. ■ E-mail <ul style="list-style-type: none"> ■ Outlook Vedere "Funzionalità e-mail dell'agente Mac" a pagina 2052. ■ Web <ul style="list-style-type: none"> ■ Firefox (HTTPS) ■ Chrome (HTTPS) ■ Safari (HTTPS) Vedere "Funzionalità del browser dell'agente Mac" a pagina 2053. ■ Applicazioni configurate <ul style="list-style-type: none"> ■ Accesso ai file di applicazione Vedere "Funzionalità Controllo applicazioni dell'agente Mac" a pagina 2054. ■ Condivisioni di rete <ul style="list-style-type: none"> ■ Copia nella condivisione Vedere "Funzionalità Copia in condivisione di rete per agente Mac" a pagina 2056. ■ Monitoraggio basato su posizione Se si utilizza Automatico per la posizione endpoint, i DLP Agent eseguiti su endpoint Mac supportano questa funzionalità. 	<ul style="list-style-type: none"> ■ Destinazioni <ul style="list-style-type: none"> ■ CD/DVD ■ Unità locale ■ Stampante/Fax ■ Appunti <ul style="list-style-type: none"> ■ Copia ■ E-mail <ul style="list-style-type: none"> ■ Lotus Notes ■ Web <ul style="list-style-type: none"> ■ IE (HTTPS) ■ Edge (HTTPS) ■ HTTP ■ FTP ■ Applicazioni configurate <ul style="list-style-type: none"> ■ Archiviazione cloud ■ Condivisioni di rete <ul style="list-style-type: none"> ■ Copia nell'unità locale ■ Monitoraggio basato su posizione Se si utilizza Manuale per la posizione endpoint, tutti gli agenti Mac sono identificati come esterni alla rete aziendale. ■ Device Control <ul style="list-style-type: none"> ■ Archiviazione USB ■ Condivisione di rete ■ Blocca STAMP

L'agente Mac non supporta il monitoraggio di file salvati dalle applicazioni Microsoft Office nelle seguenti posizioni cloud e Web:

- Condivisioni di WebDAV

- SharePoint
- SharePoint Online
- OneDrive
- OneDrive for Business

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Funzionalità dispositivo di archiviazione rimovibile agente Mac

[Tabella 77-10](#) fornisce informazioni sulle funzionalità di archiviazione rimovibili per il DLP Agent Mac.

Tabella 77-10 Funzionalità dispositivo di archiviazione rimovibile agente Mac

Supportato	Non supportato
<ul style="list-style-type: none"> ■ I file system di archiviazione rimovibili includono HFS+ (tutte le versioni di macOS Extended), FAT ed exFAT ■ Filtri di tipo file applicati all'estensione di file ■ Dispositivi USB installati come dispositivo di archiviazione di massa ■ Dispositivi di archiviazione rimovibili USB 2.0 e 3.0 ■ Operazioni di copia di file, incluso il supporto per queste applicazioni: Finder e Terminale ■ Documenti salvati su un dispositivo di archiviazione rimovibile mediante l'operazione Salva con nome dalle seguenti applicazioni: <ul style="list-style-type: none"> ■ Microsoft Office 2011 ■ TextEdit ■ Anteprima ■ Utilità di archiviazione ■ Acrobat Reader ■ I file riservati bloccati vengono spostati automaticamente sulla posizione di recupero dei file Vedere "Recupero dei file riservati negli endpoint Mac" a pagina 2130. ■ Ripristino dei file 	<ul style="list-style-type: none"> ■ Filtraggio tipo file true. L'agente Mac non ricerca la corrispondenza di una firma di file quando filtra determinati tipi di file. L'agente utilizza l'estensione file per applicare i filtri del tipo di file. Vedere "Impostazioni Filtra per proprietà file" a pagina 2116. ■ Percorso file di recupero configurabile. Quando viene applicata una regola di risposta di blocco, i file di recupero vengono spostati nella cartella di recupero sull'endpoint Mac. La posizione della cartella di recupero è \$HOME/My Recovered Files, dove \$HOME corrisponde alla directory iniziale dell'utente di endpoint. Il file viene salvato nella posizione di recupero per impedirne una perdita completa. La posizione di recupero è specificata nel pop-up Blocca. Vedere "Recupero dei file riservati negli endpoint Mac" a pagina 2130. ■ Copie di file su file system di dispositivi di archiviazione rimovibili NTFS ■ Tipi di file per iWorks 2013 e versioni superiori ■ Dispositivi di archiviazione rimovibili USB 1.0 ■ Pop-up di regole di risposta quando i comandi sudo vengono utilizzati per spostare file riservati su dispositivi di archiviazione rimovibili. Si verifica il rilevamento, vengono eseguite regole di risposta appropriate e vengono inviate risposte pop-up predefinite. ■ Trasferimenti di file tramite Media Transfer Protocol (MTP) ■ Pop-up quando vengono utilizzati terminali di riga di comando (ad esempio, client SSH) da macchine remote per spostare file riservati su dispositivi di archiviazione rimovibili ■ Nomi file effettivi in incidenti per file di Microsoft Office. Quando un file Office viene salvato su un dispositivo di archiviazione rimovibile mediante un'operazione Salva con nome, l'agente Mac visualizza il nome del file effettivo nell'incidente. Per altre applicazioni, l'agente Mac potrebbe acquisire un nome di file temporaneo che macOS crea durante il processo Salva con nome. Vedere "Informazioni sugli elenchi di incidenti endpoint" a pagina 1594.

Vedere ["Informazioni sul monitoraggio di dispositivi di archiviazione rimovibili"](#) a pagina 2061.

I seguenti problemi noti si applicano al supporto del DLP Agent Mac per i dispositivi rimovibili di archiviazione. L'ID del problema è un numero interno di Symantec utilizzato solo per scopi di tracciamento.

Tabella 77-11 Problemi noti relativi all'archiviazione su dispositivi rimovibili

Descrizione	Soluzione alternativa
Un'operazione di copia di più file tramite il Finder viene bloccata quando un file contiene dati riservati.	Nessuno
I file sensibili che sono stati recuperati possono non contenere più commenti di tipo metadati Spotlight.	Nessuno
Se una politica con parola chiave che utilizza una regola di risposta Blocca rileva informazioni sensibili che vengono spostate da un endpoint Mac a un dispositivo di archiviazione rimovibile e vengono trovate informazioni sensibili in un file di pacchetto (ad esempio .pkg, .dmg o .lpdf), il file sensibile viene bloccato e il resto del file di pacchetto viene spostato nella destinazione specificata. In seguito a questo processo il file di pacchetto spesso si corrompe.	Nessuno

Funzionalità degli Appunti supportate su agenti Mac

[Tabella 77-12](#) elenca il monitoraggio delle operazioni di Incollamento appunti supportate e non supportate.

Tabella 77-12 Caratteristiche Incollamento appunti

Supportato	Non supportato
<ul style="list-style-type: none"> ■ Controllo dei dati degli Appunti incollati in specifiche applicazioni ■ Controllo Incollamento appunti per le seguenti applicazioni (benché il monitoraggio dell'incollamento in generale necessiti ancora di essere attivato): <ul style="list-style-type: none"> ■ Firefox ■ Google Chrome <p>Nota: Il controllo Incollamento appunti è attivato automaticamente quando si attiva il canale di monitoraggio HTTPS Chrome. Quando i dati sensibili sono incollati dagli Appunti in questo scenario, l'agente registra gli incidenti HTTPS.</p> <ul style="list-style-type: none"> ■ Safari ■ Cisco Jabber ■ Skype 	<ul style="list-style-type: none"> ■ Controllo delle applicazioni a 32 bit ■ Controllo delle applicazioni con sandbox. Tra altre applicazioni, Microsoft Office 2016 (Word, Excel, PowerPoint e Outlook) è in modalità sandbox. È possibile identificare altre applicazioni in modalità sandbox passando al Controllo delle attività e avviando una ricerca nella colonna Sandbox. ■ Controllo dei dati copiati da una finestra dell'applicazione chat in un'altra finestra della stessa applicazione chat. Le applicazioni chat interessate possono includere Jabber e Skype.

Vedere ["Informazioni sul monitoraggio degli Appunti"](#) a pagina 2067.

I seguenti problemi noti si applicano alla funzionalità di controllo Incollamento appunti di DLP Agent per Mac.

Tabella 77-13 Problemi noti del controllo Incollamento appunti

Descrizione	Soluzione alternativa
Gli incidenti duplicati sono creati quando l'impostazione Incollamento appunti è attivata per i browser controllati tramite la funzionalità Controllo applicazioni e anche il canale di monitoraggio HTTPS del browser è attivato.	Disattivazione di Incollamento appunti per il browser nella schermata Controllo applicazioni .
Alcune applicazioni utilizzano le operazioni di incollamento non avviate dall'utente endpoint, rischiando di provocare incidenti di falsi positivi.	Symantec consiglia di verificare il comportamento dell'applicazione prima di attivare il controllo Incollamento appunti.

Funzionalità e-mail dell'agente Mac

[Tabella 77-14](#) elenca il supporto monitoraggio di Outlook.

Tabella 77-14 Caratteristiche di Outlook

Supportato	Non supportato
<ul style="list-style-type: none"> ■ Microsoft Outlook 2011 e 2016 ■ Monitoraggio di informazioni sensibili in tutti i campi di email e inviti a riunioni, nonché nei relativi allegati ■ Rilevamento di informazioni sensibili e possibilità di impedire che lascino un endpoint Mac quando vengono inviate da Outlook ■ Rilevamento e protezione di informazioni sensibili nei formati testo semplice e HTML ■ Possibilità di ignorare e monitorare allegati in base al tipo e alla dimensione del file ■ Possibilità di monitorare dati con Outlook connesso o meno alla rete 	<ul style="list-style-type: none"> ■ Monitoraggio dei dati incollati in Outlook ■ Monitoraggio di contatti contenuti in un elenco di distribuzione (DL) non espanso ■ Possibilità di monitorare i dati quando il mittente o l'utente corrisponde al gruppo di utenti (politiche EDM) ■ Monitoraggio di messaggi di fuori sede ■ Utilizzo dei filtri di monitoraggio dei file basati su firme (in Outlook 2011 e 2016)

Tabella 77-15 Problema noto di Outlook 2016

Descrizione	Soluzione alternativa
Se un invito a riunione contiene dati riservati e viene bloccato, l'invito rimane nel calendario del mittente.	Nessuna

Vedere ["Informazioni sul monitoraggio della rete endpoint"](#) a pagina 2063.

Funzionalità del browser dell'agente Mac

[Tabella 77-16](#) elenca le informazioni relative alle funzionalità del browser del DLP Agent Mac. Queste funzionalità si applicano al supporto del monitor per i browser Firefox, Chrome e Safari.

Tabella 77-16 Funzionalità del browser

Supportato	Non supportato
<ul style="list-style-type: none"> ■ Impedire che informazioni riservate vengano caricate sui siti HTTP e HTTPS. ■ Filtrare in base a dimensione e tipo di file ■ Monitorare i processi secondari ■ Monitorare i dati incollati ■ Monitorare i file caricati tramite trascinamento 	<ul style="list-style-type: none"> ■ Monitorare i dati inline

Vedere ["Informazioni sul monitoraggio della rete endpoint"](#) a pagina 2063.

I seguenti problemi noti si applicano al supporto del DLP Agent Mac per i browser.

Tabella 77-17 Problemi noti relativi al browser dell'agente Mac

Descrizione	Soluzione alternativa
Gli incidenti duplicati vengono creati per gli utenti che hanno eseguito l'upgrade da una versione precedente di Symantec Data Loss Prevention in cui Chrome veniva monitorato tramite la funzionalità Monitora accesso a file applicazione .	Disattivare l'impostazione Monitora accesso a file applicazione nella schermata Controllo applicazioni . Vedere "Modifica delle impostazioni di controllo delle applicazioni" a pagina 2232.
Diversi URL vengono visualizzati in un incidente quando gli utenti caricano lo stesso file riservato in più schede del browser. Ad esempio, diversi URL vengono visualizzati in un incidente quando un utente carica un file riservato in gmail.com e box.net in esecuzione in due schede.	Nessuno
Vengono visualizzate finestre pop-up di blocco e notifica sconosciuto per l'URL quando i file riservati vengono caricati tramite un processo figlio.	Nessuno
I pop-up Blocca mostrano l'URL della pagina Web di sfondo quando i file riservati vengono caricati tramite estensioni in Firefox (ad esempio Gmail Notifier).	Nessuno
Se un utente tenta di incollare dati riservati sul browser Safari quando è utilizzata una risposta Endpoint Prevent: Block, i dati vengono bloccati. Tuttavia, l'azione di blocco cancella il contenuto degli Appunti, impedendo all'utente di incollare il contenuto in altre applicazioni.	Nessuno

Funzionalità Controllo applicazioni dell'agente Mac

[Tabella 77-18](#) elenca il supporto per le impostazioni Controllo applicazioni.

Tabella 77-18 Funzionalità Controllo applicazioni

Supportato	Non supportato
<ul style="list-style-type: none"> ■ Controllo e prevenzione dei caricamenti del file tramite browser (Chrome, Firefox e Safari) ■ Controllo e prevenzione dei file inviati per e-mail in Outlook 2011 e Outlook 2016 ■ Inserimento di applicazioni in lista bianca Attivare l'impostazione Archiviazione rimovibile nell'area Configurazione controllo applicazioni, Destinazioni per utilizzare questa funzionalità. È possibile reperire ulteriori informazioni sull'inserimento in lista bianca. Vedere "Come ignorare applicazioni macOS" a pagina 2245. ■ Controllo tramite l'impostazione di controllo dell'accesso Accesso ai file di applicazione, Apri nell'area Configurazione controllo applicazioni, Accesso ai file di applicazione ■ Controllo tramite l'impostazione di controllo Appunti, Incolla nell'area Configurazione controllo applicazioni, Appunti ■ Controllo tramite l'impostazione Configurazione controllo applicazioni: Accesso ai file di applicazione, Apri 	<ul style="list-style-type: none"> ■ I seguenti campi non vengono applicati alle applicazioni Mac: <ul style="list-style-type: none"> ■ Nome interno ■ Nome file originale ■ Nome editore ■ Controllo tramite le impostazioni Unità locale e Stampa/Fax nell'area Configurazione controllo applicazioni, Destinazioni ■ Controllo tramite l'impostazione di monitoraggio nell'area Configurazione controllo applicazioni ■ Controllo tramite l'impostazione di controllo Appunti, Copia nell'area Configurazione controllo applicazioni, Appunti ■ Controllo tramite le impostazioni HTTP e FTP nell'area Configurazione controllo applicazioni, Web ■ Controllo tramite l'impostazione Configurazione controllo applicazioni: Accesso ai file di applicazione, Leggi L'impostazione predefinita di sistema è Apri. ■ Controllo dei dati incollati dagli Appunti per applicazioni a 32 bit.

Vedere ["Informazioni sul controllo delle applicazioni"](#) a pagina 2231.

Il seguente problema noto si applica al supporto di DLP Agent per Mac per le applicazioni.

Tabella 77-19 Problema noto di Controllo applicazioni

Descrizione	Soluzione alternativa
<p>Vengono creati incidenti duplicati e i pop-up visualizzati quando i dati sensibili vengono spostati nei seguenti protocolli o applicazioni:</p> <ul style="list-style-type: none"> ■ Chrome ■ Safari ■ Firefox ■ Outlook 	<p>Disattivare queste applicazioni nella schermata Controllo applicazioni.</p>

Funzionalità Copia in condivisione di rete per agente Mac

[Funzionalità Copia in condivisione di rete per agente Mac](#) elenca le funzionalità Copia in condivisione di rete supportate e non supportate.

Tabella 77-20 Funzionalità Copia in condivisione di rete

Supportato	Non supportato
<ul style="list-style-type: none"> Endpoint: notifica regola di risposta Endpoint: blocca regola di risposta I seguenti protocolli di rete: <ul style="list-style-type: none"> Apple Filing Protocol (AFP) Common Internet File System (CIFS) File Transfer Protocol (FTP) (compresi Secure File Transfer Protocol [SFTP] e FTP Secure [FTPS]) Network File System (NFS) Secure message block (SMB) 	<ul style="list-style-type: none"> WebDAV Endpoint: regola di risposta FlexResponse Endpoint Prevent: operazione annullata dall'utente

Vedere ["Informazioni sul monitoraggio della condivisione di rete"](#) a pagina 2066.

Filtro dall'agente Mac in base alle funzionalità delle proprietà del file

[Tabella 77-21](#) elenca le funzionalità del filtro delle proprietà del file per il DLP Agent Mac.

Nota: Il supporto indicato si applica inoltre al monitoraggio dell'archiviazione rimovibile.

Tabella 77-21 Filtra per proprietà file

Supportato	Non supportato
<ul style="list-style-type: none"> Tipo di file Dimensione file Percorso file <p>Nota: I filtri del percorso file sono supportati per Accesso ai file di applicazione ma non per il monitoraggio degli Archivi rimovibili.</p> <ul style="list-style-type: none"> Monitoraggio dell'estensione dei file 	<p>Il DLP Agent Mac non esegue la corrispondenza del tipo di file true quando filtra i tipi di file. L'agente utilizza l'estensione file per applicare i filtri del tipo di file.</p> <p>Vedere "Filtraggio tipo file true" a pagina 2120.</p>

Vedere ["Impostazioni Filtra per proprietà file"](#) a pagina 2116.

Filtro dall'agente Mac in base alle funzionalità delle proprietà del rete

Tabella 77-22 elenca le funzionalità del filtro delle proprietà per il DLP Agent Mac.

Tabella 77-22 Filtra per proprietà di rete

Supportato	Non supportato
<ul style="list-style-type: none">Filtraggio per tipo di file, dimensione e percorsoCopie di file da endpoint Mac su condivisioni di rete	<ul style="list-style-type: none">Filtraggio tramite indirizzi IPCopie di file da condivisioni di rete su endpoint Mac

Vedere "Impostazioni di Filtra per proprietà di rete" a pagina 2121.

Caratteristiche delle impostazioni dell'agente avanzate di Endpoint Prevent per l'agente Mac

Impostazioni dell'agente avanzate supportate

- FileSystem.APPS_LIST_USES_TRUNCATE_FILE_FOR_BLOCK_RULE
- FileSystem.ENABLE_FILE_RESTORATION
- FileSystem.IGNORE_STORAGE_BUS_TYPE
- FileSystem.MONITOR_APPLICATION_CHILD_PROCESS_FILE_ACCESS
- FileSystem.NUM_OF_LISTENER_THREADS
- FileSystem.THREAD_POOL_MAX_CAPACITY

Impostazioni dell'agente avanzate non supportate

- FileSystem.DRIVER_FILE_OPEN_REQUEST_TIMEOUT
- FileSystem.ENABLE_VEP_FILE_ELIMINATION
- FileSystem.MAX_BACKLOG
- FileSystem.NUM_TIMES_TO_OVERWRITE_FILE

Vedere "Impostazioni agente avanzate" a pagina 2133.

Funzionalità dei target Endpoint Discover per Mac

Tabella 77-23 Funzionalità dei target Endpoint Discover

Supportato	Non supportato
<ul style="list-style-type: none">■ Utilizzo di più Endpoint Server per una scansione Endpoint Discover■ Utilizzo di filtri per includere o escludere tipi di file e percorsi file specifici, nonché utilizzo di caratteri jolly (*)■ Utilizzo di filtri per includere o escludere in base alle dimensioni file■ Scansione dei file aggiunti o modificati dall'ultima scansione completa■ Scansione dei file modificati per ultimi■ Esecuzione di scansioni incrementali■ Impostazione della prossima scansione e della scansione completa■ Regolazione del timeout inattività della scansione■ Impostazione della durata massima di scansione■ Attivazione della scansione durante l'inattività dell'utente■ Scansione di computer specifici tramite indirizzo IP o nome host	<ul style="list-style-type: none">■ Utilizzo delle variabili ambientali per includere o escludere le posizioni file (ad esempio, <i>\$Windows\$</i>)■ Utilizzo medio della CPU a lungo termine■ Durata minima rimanente della batteria■ Quarantena endpoint■ Sospensione delle scansioni

Vedere ["Informazioni sulla scansione di Endpoint Discover"](#) a pagina 2080.

Nota: Per macOS, la data e l'ora di un file (la data e l'ora di creazione, modifica o accesso di un file) non cambia se si copia il file da una posizione a un'altra. Se si esegue una scansione completa di Endpoint Discover e, in seguito, qualche file viene spostato localmente nel percorso della cartella di destinazione di Endpoint Discover, ma l'ultima modifica era è avvenuta prima della scansione completa, la scansione incrementale successiva non esamina questi file. Poiché la data e l'ora dei file è precedente alla scansione completa, anche se i file sono stati aggiunti alla cartella di destinazione dopo la scansione, non vengono riconosciuti come file da considerare per una scansione incrementale.

In tal caso, Symantec consiglia di eseguire una scansione completa invece di una scansione incrementale.

Vedere ["Informazioni sulla scansione completa di Endpoint Discover"](#) a pagina 2082.

Vedere ["Informazioni sulla scansione incrementale di Endpoint Discover"](#) a pagina 2082.

Supporto Endpoint Discover per file system Mac

[Tabella 77-24](#) elenca il supporto per i file system di cui Endpoint Discover può eseguire la scansione.

Tabella 77-24 File system Endpoint Discover supportati

Supportato	Non supportato
<ul style="list-style-type: none"> ■ HFS+ (tutte le versioni di macOS Extended) ■ FAT ■ exFAT 	NTFS

Supporto di impostazioni agente avanzate di Endpoint Discover per Mac

Sono supportate le seguenti impostazioni agente avanzate:

- Discover.CRAWLER_THREAD_PRIORITY.str
- Discover.POST_SCAN_REPORT_INTERVAL.int
- Discover.SCAN_ONLY_WHEN_IDLE.int
- Discover.SECONDS_UNTIL_IDLE.int
- Discover.STANDARD_REPORT_INTERVAL.int

Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.

Utilizzo di Endpoint Prevent

Il capitolo contiene i seguenti argomenti:

- [Informazioni sul monitoraggio di Endpoint Prevent](#)
- [Informazione sulla creazione di politiche per Endpoint Prevent](#)
- [Come implementare Endpoint Prevent](#)

Informazioni sul monitoraggio di Endpoint Prevent

Le politiche di Endpoint Prevent individuano e bloccano le informazioni confidenziali che escono dagli endpoint o dai desktop virtuali nell'organizzazione. Endpoint Server distribuisce le politiche ai DLP Agent o le applica direttamente ai file inviati dai DLP Agent. Secondo il tipo di politica creata, la politica viene applicata dai DLP Agent direttamente o da Endpoint Server. Quando i DLP Agent o gli Endpoint Server rilevano un'attività che viola una regola di politica, viene generato un incidente. È possibile esaminare e riparare gli incidenti visualizzati nell'elenco di incidenti degli endpoint.

Nota: I gruppi di politiche assegnati a un Endpoint Server si applicano ugualmente solo agli agenti Windows collegati.

Endpoint Prevent può eseguire diversi tipi di monitoraggio. La seguente tabella fornisce i riferimenti ai tipi di monitoraggio che è possibile selezionare.

Tabella 78-1 Monitoraggio di Endpoint Prevent

Tipo di monitoraggio
Informazioni sul monitoraggio di dispositivi di archiviazione rimovibili
Informazioni sul monitoraggio della rete endpoint

Tipo di monitoraggio
Informazioni sul controllo CD/DVD
Informazioni sul monitoraggio di stampa/fax
Informazioni sul monitoraggio della condivisione di rete
Informazioni sul monitoraggio degli Appunti
Informazioni sul controllo applicazioni
Informazioni sul controllo applicazioni dell'archiviazione cloud
Informazioni sul supporto del desktop virtuale con Endpoint Prevent

Endpoint Prevent monitora l'attività degli endpoint a prescindere dal fatto che siano collegati a un Endpoint Server. Se un endpoint è scollegato dalla rete e non può collegarsi a un Endpoint Server, Endpoint Prevent continua a monitorare l'endpoint. Tutti gli incidenti sono memorizzati in Agent Store fino a quando l'endpoint si ricollega a Endpoint Server. Se Agent Store supera il limite di dimensione specificato, vengono eliminati i file più vecchi fino a rientrare nel limite di dimensione. Endpoint Prevent non smette di monitorare l'endpoint se Agent Store supera il limite di dimensione specificato.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Vedere ["Informazioni su DLP Agent Store"](#) a pagina 2129.

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

Vedere ["Supporto di monitoraggio dell'agente Mac"](#) a pagina 2061.

Informazioni sul monitoraggio di dispositivi di archiviazione rimovibili

Endpoint Prevent consente di bloccare i dati trasferiti dall'unità disco rigido a un dispositivo rimovibile su endpoint Windows e Mac. [Informazioni sul monitoraggio di dispositivi di archiviazione rimovibili](#) elenca i dispositivi rimovibili supportati dove applicabile.

Tabella 78-2 Dispositivi di archiviazione rimovibili supportati

Dispositivo	Supportato su endpoint Windows	Supportato su endpoint Mac
Scheda Flash compatta	Sì	Sì
Unità rimovibili eSATA	Sì	No
Dispositivi connessi via FireWire	Sì	Sì

Dispositivo	Supportato su endpoint Windows	Supportato su endpoint Mac
Schede di memoria, incluse le schede SDHC e SDXC	Sì	Sì
Unità flash e memory stick USB	Sì	Sì
Dispositivi di archiviazione Thunderbolt	No	Sì
Dispositivi che usano il protocollo MTP (Media Transfer Protocol)	Sì	No

I file system di archiviazione rimovibili supportati per macOS sono:

- HFS+ (tutte le versioni di macOS Extended)
- FAT
- FAT32
- exFAT

I file system di archiviazione rimovibili per Windows sono:

- NTFS
- FAT
- FAT32

Quando il DLP Agent individua che si è verificato un incidente, i dati non sono trasferiti. Un incidente è creato e inviato all'Endpoint Server. Quando si ha un incidente, il DLP Agent visualizza una finestra di notifica che informa l'utente dell'incidente verificatosi. La notifica richiede inoltre una giustificazione per il trasferimento di file. Questa giustificazione è visualizzata nell'istantanea dell'incidente.

Vedere ["Impostazione delle preferenze di report"](#) a pagina 1634.

Ad esempio, un utente copia un file di Microsoft Word che contiene cartelle mediche da un endpoint a unità flash USB. Il DLP Agent blocca il trasferimento di questo file all'unità flash. Quando il file viene bloccato, viene visualizzata una notifica sullo schermo dell'utente, indicante che il trasferimento di file è una violazione di una politica specifica. La finestra di notifica inoltre fornisce una casella di testo in cui l'utente può giustificare lo spostamento del file nell'unità flash. La giustificazione che l'utente fornisce è visibile nell'istantanea di questo incidente.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Vedere ["Funzionalità dispositivo di archiviazione rimovibile agente Mac"](#) a pagina 2049.

Informazioni sul monitoraggio della rete endpoint

Endpoint Prevent consente di monitorare o bloccare vari tipi di eventi di rete, tra cui:

- HTTP/HTTPS
- E-mail/SMTP
- FTP

Endpoint Prevent consente di bloccare le violazioni di rete indipendentemente se l'endpoint è collegato o meno alla rete aziendale. Ad esempio, un utente prende con sé un laptop della società e accede a una connessione Internet wireless in un bar. Symantec DLP Agent può ancora rilevare, rimuovere o bloccare il trasferimento di qualsiasi file sulla rete non protetta. Gli incidenti generati quando l'endpoint non è connesso all'Endpoint Server sono memorizzati in un database temporaneo. Gli incidenti rimangono nel database fino a che la connessione non viene ripristinata. Dopo il ripristino della connessione all'Endpoint Server, gli incidenti sono inviati all'Endpoint Server.

Monitoraggio del browser e HTTP/HTTPS

DLP Agent può monitorare le applicazioni e le pagine Web HTTP o HTTPS. Ad esempio, può monitorare e impedire il trasferimento di informazioni riservate da Microsoft Internet Explorer, Mozilla Firefox, Google Chrome o qualunque altra applicazione HTTP. Il monitoraggio HTTPS consente di monitorare o impedire il trasferimento di qualsiasi file a un sito HTTPS crittografato dai browser Web Internet Explorer, Google Chrome e Firefox. La prevenzione HTTPS e HTTP inoltre consente il blocco del trasferimento di messaggi e-mail e allegati mediante applicazioni e-mail Web. Gli incidenti includono informazioni su messaggi, IP e URL di destinazione.

I seguenti browser sono configurati per essere monitorati automaticamente dopo aver attivato il canale HTTP/HTTPS:

- IE (HTTPS) su endpoint Windows
- Firefox (HTTPS) su endpoint Mac e Windows
- Chrome (HTTPS) su endpoint Mac e Windows
- Safari (HTTPS) su endpoint Mac

Il supporto di specifiche funzionalità dei browser varia tra gli endpoint Mac e quelli Windows. Vedere ["Funzionalità del browser dell'agente Mac"](#) a pagina 2053.

Monitoraggio di applicazioni e-mail

Endpoint Prevent monitora le applicazioni e-mail più comuni: Microsoft Outlook e Lotus Notes. Può monitorare e impedire qualsiasi informazione trasferita da queste applicazioni indipendentemente dal protocollo e-mail. Gli allegati come pure il contenuto nell'oggetto e nel corpo del messaggio sono analizzati. Gli incidenti comprendono le informazioni sulla posizione dell'endpoint, mittente, destinatario, oggetto e messaggio dell'e-mail.

Monitoraggio del protocollo FTP

Il monitoraggio FTP impedisce il trasferimento di file a un archivio esterno mediante il protocollo FTP. Ad esempio, un utente tenta di inviare un file che viola una politica a un archivio di file remoto utilizzando l'applicazione FTP Mozilla Filezilla. Endpoint Prevent impedisce il trasferimento del file alla posizione FTP. Un incidente viene creato per la violazione e viene visualizzato nella sezione dei report endpoint di Enforce Server. L'istantanea dell'incidente contiene informazioni su quali utenti hanno tentato di inviare il file tramite FTP. Visualizza il file all'origine della violazione e l'indirizzo IP del server FTP di destinazione.

Nota: Alcuni tipi di rete non corrispondono alla condizione di monitoraggio del nome di file. Questi eventi di rete non contengono nomi di file e pertanto non possono corrispondere a questa condizione. I tipi di monitoraggio di rete che non possono corrispondere alla condizione del nome di file includono corpo e testo del messaggio Outlook e HTTP/HTTPS.

Tutti gli incidenti sono indicati in Endpoint Prevent nella sezione Report.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Vedere ["Informazioni sul controllo delle applicazioni"](#) a pagina 2231.

Informazioni sul controllo CD/DVD

Il controllo CD/DVD è compatibile con tutte le principali applicazioni di masterizzazione CD/DVD.

Il controllo CD/DVD endpoint è progettato per monitorare tipi di file specifici. I filtri dalle prestazioni sono disponibili nella sezione di configurazione dell'agente. Utilizzarli per specificare i tipi di file controllati da Endpoint Prevent. È inoltre possibile verificare l'effetto del controllo sull'applicazione di masterizzazione CD/DVD.

Per consentire la protezione CD/DVD, è necessario selezionare l'attivazione/disattivazione di CD/DVD nella scheda **Canali** della pagina di configurazione di Endpoint Server. È inoltre possibile creare una politica per i file copiati in un masterizzatore CD/DVD. Creare una regola di destinazione endpoint o un protocollo con CD/DVD come destinazione. È necessario specificare i criteri del contenuto per la politica. Le politiche possono essere create utilizzando le condizioni booleane AND/OR. Specificare i criteri dei contenuti solo utilizzando la condizione AND nel generatore della politica.

Ad esempio, si desidera creare una politica che impedisca ai file con la parola chiave Farallon di essere masterizzati in un DVD. L'applicazione di masterizzazione DVD è Roxio 9. Creare una politica vuota con una regola di tipo dispositivo o un protocollo. Selezionare il tipo del dispositivo CD/DVD e inoltre far corrispondere una regola Contenuto corrispondente a parola chiave. Immettere Farallon come parola chiave. Completare la creazione della regola con una regola di risposta Endpoint: blocca. Dopo aver salvato la politica, DLP Agent blocca la masterizzazione su un DVD di qualsiasi file contenente la parola chiave Farallon.

Selezionando il tipo di dispositivo CD/DVD, è stato specificato che la politica influisce solo sui file masterizzati in un CD/DVD. Le unità disco rigido endpoint e i supporti multimediali USB non vengono influenzati. Combinando le regole di corrispondenza parola chiave e tipo dispositivo, si garantisce che DLP Agent blocchi solo i file con parola chiave specificata. Gli agenti non bloccano tutti i file inviati all'applicazione CD/DVD. Se viene creata la regola Blocca CD/DVD senza la regola parola chiave congiunta, la politica blocca ogni file inviato all'applicazione di masterizzazione. Oppure, bloccherebbe i file che contengono la parola chiave nell'unità disco rigido dell'endpoint, oltre ai supporti USB connessi.

Nota: I file di dimensioni inferiori a 64 byte non vengono rilevati durante la lettura del monitoraggio CD/DVD. I file di dimensioni superiori a 64 byte vengono rilevati normalmente.

Vedere ["Linee guida per la creazione di politiche endpoint"](#) a pagina 2035.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Informazioni sul monitoraggio di stampa/fax

Endpoint Prevent consente di monitorare e impedire la stampa e l'invio via fax di informazioni riservate. Endpoint Prevent utilizza lo stesso meccanismo per monitorare i dati stampati e inviati via fax. Endpoint Prevent può monitorare i processi di stampa avviati da un'applicazione o mediante l'utilità **Stampa** nativa di Esplora risorse di Windows.

Endpoint Prevent analizza ogni pagina di un file mentre viene inviata alla stampante o al fax. Ciò significa che le pagine iniziali del file possono essere stampate o inviate via fax se una violazione viene rilevata a metà del file. Ad esempio, un utente invia un documento di 10 pagine a una stampante. Se Endpoint Prevent rileva una violazione nella terza pagina, arresta il processo di stampa. Le pagine una e due vengono stampate ma non quelle da tre a dieci. Endpoint Prevent invia un incidente a Endpoint Server che contiene le informazioni sul file e il testo corrispondente.

Nota: Endpoint Prevent non monitora il testo sul frontespizio di un fax.

DLP Agent può inoltre monitorare e bloccare l'intero processo di stampa. DLP Agent monitora sempre i file PDF stampati da Adobe Acrobat in questo modo. È possibile impostare DLP Agent per monitorare i file stampati da Microsoft Word, PowerPoint ed Excel quando si attiva **Monitora intero file**.

Vedere ["Impostazioni della stampante/fax"](#) a pagina 2132.

L'istantanea incidente contiene informazioni relative all'endpoint che ha inviato il file con la violazione, il file con la violazione, il nome e tipo della stampante. Il tipo di stampante può essere una stampante collegata localmente, una stampante condivisa o l'opzione **Stampa su**

file selezionata dall'utente. Quando si attiva **Monitora intero file**, l'istantanea incidente elenca la posizione in cui si trova il file.

Vedere ["Impostazione delle preferenze di report"](#) a pagina 1634.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Informazioni sul monitoraggio della condivisione di rete

Il monitoraggio della condivisione di rete impedisce agli utenti di spostare file riservati da una condivisione di rete a un endpoint e viceversa.

Per gli endpoint Windows, è possibile usare qualsiasi regola di risposta endpoint per il monitoraggio di condivisioni di rete. Per gli endpoint Mac, è possibile usare le regole di risposta Endpoint: notifica e Endpoint: blocca.

La funzionalità Copia nell'unità locale impedisce agli utenti di spostare dati riservati da un'unità di rete a un'unità locale su un endpoint Windows utilizzando Esplora risorse di Windows. Ad esempio, si ha una condivisione di rete remota etichettata `g:` e un'unità locale etichettata `c:`. È possibile creare una politica che impedisce agli utenti di spostare dati riservati dall'unità `g:` all'unità `c:`. È anche possibile creare filtri nella configurazione agente che monitorano o ignorano i file per tipo, dimensione e percorso applicabili agli endpoint Windows.

La funzionalità Copia nell'unità locale monitora le operazioni di copia di Esplora risorse di Windows. Altri tipi di operazioni di copia nella condivisione di rete, come trasferimenti FTP, applicazioni di terzi, operazioni di salvataggio, utilità della riga di comando o applicazioni copia e incolla, non sono coperte da questa funzionalità.

La funzionalità Copia nella condivisione impedisce agli utenti di spostare dati riservati da un'unità locale su un endpoint Windows o Mac in un'unità di condivisione di rete. È possibile creare una politica che blocca la copia di dati riservati dall'unità `c:` all'unità `g:`. È anche possibile creare filtri nella configurazione agente che monitorano o ignorano i file per tipo, dimensione e percorso. I filtri creati si applicano a endpoint Windows e Mac.

Vedere ["Configurazione dei filtri di file"](#) a pagina 2117.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Vedere ["Funzionalità Copia in condivisione di rete per agente Mac"](#) a pagina 2056.

Protocolli di monitoraggio della condivisione di rete supportati sugli endpoint Windows

Endpoint Prevent impedisce il trasferimento di dati riservati dagli endpoint di Windows tramite Windows Explorer, oltre ad applicazioni di terzi, browser di file e interfacce della riga di comando che utilizzano uno qualsiasi dei servizi redirector di rete Windows seguenti:

- LAN Manager (LanMan)

- Remote Desktop Protocol (RDP)
- Web Distributed Authoring and Versioning (WebDAV)

La funzionalità Copia nella condivisione monitora le condivisioni su rete come le condivisioni Windows, DFS, NAS e UNIX configurate tramite le condivisioni Samba, Microsoft Remote Desktop e WebDAV a cui si accede tramite un redirector WebDAV predefinito.

Protocolli di monitoraggio della condivisione di rete supportati negli endpoint Mac

Endpoint Prevent impedisce il trasferimento di dati riservati dagli endpoint Mac tramite Finder, i comandi del terminale e i seguenti protocolli di trasferimento di file:

- Apple Filing Protocol (AFP)
- Common Internet File System (CIFS)
- File Transfer Protocol (FTP) (compresi Secure File Transfer Protocol [SFTP] e FTP Secure [FTPS])
- Network File System (NFS)
- Secure Message Block (SMB)

Informazioni sul monitoraggio degli Appunti

Endpoint Prevent impedisce agli utenti di copiare e incollare dati riservati da un'applicazione all'altra con Appunti di Windows. Endpoint Prevent non impedisce agli utenti di copiare e incollare dati riservati nella stessa applicazione.

Ad esempio, se un utente copia informazioni riservate da un documento Word e le incolla in un messaggio IM, Endpoint Prevent blocca il trasferimento. Il blocco si verifica perché le funzioni di copia e incolla utilizzano Appunti di Windows. L'utente riceve una notifica pop-up in cui è indicato il motivo per cui il trasferimento è stato bloccato. Nel report endpoint, l'istantanea di incidente contiene un incidente e il testo delle informazioni incollate nel messaggio e-mail. Gli incidenti vengono creati al momento delle operazioni di taglio, copia o incolla.

Vedere ["Impostazione delle preferenze di report"](#) a pagina 1634.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Vedere ["Funzionalità degli Appunti supportate su agenti Mac"](#) a pagina 2051.

Informazioni sul controllo applicazioni

Per impostazione predefinita, Symantec Data Loss Prevention controlla applicazioni quali Microsoft Outlook, Cisco Jabber, Skype, Google Chrome e Mozilla Firefox. È possibile configurare modifiche globali alle applicazioni predefinite. È possibile impostare Symantec

Data Loss Prevention per controllare gli elementi della lista bianca o della lista nera, le applicazioni CD/DVD, le applicazioni che usano funzioni degli Appunti e infine le applicazioni che caricano contenuti in Internet.

Nota: Gli utenti endpoint devono attivare l'estensione Symantec per consentire al DLP Agent di monitorare Safari. Vedere ["Abilitare il monitoraggio nel browser Safari"](#) a pagina 2115.

Symantec Data Loss Prevention consente di controllare le applicazioni di terzi per client di messaggia istantanea, e-mail o HTTP/S. Sono esempi di tali applicazioni Yahoo Messenger (YM), AIM e Mozilla Thunderbird. Per controllare queste applicazioni, le si aggiunge alla schermata **Controllo applicazioni** (**Sistema > Agenti > Controllo applicazioni**).

Il protocollo SPDY è disattivato automaticamente per impedire la perdita di dati in HTTPS. È possibile disattivare questa impostazione mediante l'impostazione agente avanzata NetworkMonitor.DISABLE_SPDY_PROTOCOL. Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.

Vedere ["Informazioni sul controllo delle applicazioni"](#) a pagina 2231.

Vedere ["Funzionalità Controllo applicazioni dell'agente Mac"](#) a pagina 2054.

Informazioni sul controllo applicazioni dell'archiviazione cloud

Il controllo applicazioni dell'archiviazione cloud di Endpoint fornisce assistenza per il monitoraggio e la prevenzione per le applicazioni di sincronizzazione e condivisione file nel cloud. È possibile accedere alle impostazioni del controllo applicazioni dell'archiviazione cloud nella schermata **Sistema > Agenti > Controllo applicazioni**.

Se un utente endpoint aggiorna un contenuto nei file che un'applicazione cloud sincronizza, l'applicazione cloud tenta di caricare il file sul servizio cloud. Se un utente aggiunge un contenuto sensibile, Symantec Data Loss Prevention impedisce il caricamento nel cloud del file.

DLP Agent monitora e blocca i file riservati che un utente tenta di salvare dalle applicazioni Microsoft Office 2010, 2013 e 2016 (Word, Excel e PowerPoint) in posizioni di archiviazione cloud e Web. Le seguenti destinazioni sono monitorate per impostazione predefinita:

- Box
- Condivisione di WebDAV
- SharePoint
- SharePoint Online
- Microsoft OneDrive
- Microsoft OneDrive for Business

L'agente monitora anche i file caricati in Box da applicazioni Microsoft Office supportate (compreso Outlook) tramite il componente aggiuntivo Box for Office. È possibile attivare questa funzionalità nella schermata **Configurazione agente**. Vedere ["Impostazioni di archiviazione cloud"](#) a pagina 2131.

Se si utilizza una regola di risposta del blocco nella politica, Symantec Data Loss Prevention crea un incidente di archiviazione cloud e il contenuto sensibile viene messo in quarantena nell'endpoint. L'utente di endpoint può ripristinare la versione del file precedente dalla posizione di ripristino configurata, dove il file viene conservato per un tempo indefinito. Vedere ["Impostazioni posizione area di recupero dei file"](#) a pagina 2129.

Non è possibile eliminare alcuna delle applicazioni cloud predefinite presenti nella schermata **Controllo applicazioni**. Se si desidera monitorare un'applicazione di archiviazione cloud non elencata in questa schermata, è possibile aggiungerla. Vedere ["Aggiunta di un'applicazione Windows"](#) a pagina 2237.

È possibile consentire caricamenti di file sensibili da utenti aziendali in account Box aziendali e impedire caricamenti di file sensibili in account Box non aziendali (per endpoint Windows). Questa funzionalità monitora e impedisce caricamenti di file tramite l'applicazione Box Sync nonché dalle applicazioni di Microsoft Office Word, Excel, PowerPoint e Outlook (versioni 2010, 2013 e 2016) tramite il componente aggiuntivo Box for Office. Vedere ["Impostazioni Ignora identità utente per applicazioni di archiviazione cloud"](#) a pagina 2124.

Tabella 78-3 elenca le applicazioni di archiviazione cloud predefinite monitorate da Symantec Data Loss Prevention.

Tabella 78-3 Nomi di marche e nomi binari di applicazioni di archiviazione cloud monitorate

Nomi di marca	Nome binario
Box	BoxSync.exe
Dropbox	Dropbox.exe
Google Drive	googledrivesync.exe
HighTail	Hightail.exe
iCloud	iCloudDrive.exe
Microsoft OneDrive	OneDrive.exe
Microsoft Skydrive	SkyDrive.exe

Informazioni sul supporto del desktop virtuale con Endpoint Prevent

Endpoint Prevent può monitorare i desktop virtuali e impedire agli utenti remoti di copiare i dati sensibili che sono accessibili tramite un desktop virtuale. È possibile installare un DLP

Agent in ciascun desktop virtuale. Eseguendo un DLP Agent nell'ospite virtuale, è possibile impedire a un utente di copiare i dati riservati accessibili dal desktop virtuale ospitato a un computer o a un dispositivo remoto che potrebbe non essere sicuro. È possibile configurare DLP Agent per monitorare i volumi di archiviazione, le richieste di stampa e invio fax, gli Appunti e l'attività di rete sul desktop virtuale.

Endpoint Prevent può monitorare i desktop virtuali ospitati da uno qualsiasi dei seguenti software di virtualizzazione:

- Server di virtualizzazione Microsoft Hyper-V
- Microsoft Remote Desktop Services
- Server di virtualizzazione VMware View
- VMware Fusion
- Citrix XenDesktop e Citrix XenApp/server dell'applicazione

Vedere ["Informazioni sul supporto di Citrix XenDesktop e Citrix XenApp"](#) a pagina 2070.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Informazioni sul supporto di Citrix XenDesktop e Citrix XenApp

DLP Agent è installato in Citrix XenDesktop e Citrix XenApp/server dell'applicazione, dove può rilevare l'invio di dati confidenziali a un computer client Citrix.

Prestazioni e distribuzione

[Tabella 78-4](#) fornisce consigli di distribuzione e dettagli sulle prestazioni.

Tabella 78-4 Distribuzione e prestazioni di Citrix

Prodotto	Consigli di distribuzione e dettagli sulle prestazioni
Citrix XenApp	<ul style="list-style-type: none"> ■ È necessario installare il software DLP Agent su ogni host del server XenApp e su tutti i singoli server di applicazioni che pubblicano applicazioni tramite XenApp. ■ Tutti i rilevamenti su Citrix XenApp vengono eseguiti in un singolo thread (tutte le attività dell'utente sono analizzate in sequenza). ■ I test di Symantec indicano che il software DLP Agent può supportare un massimo di 40 client simultanei per server Citrix. Tuttavia, le prestazioni di rilevamento variano a seconda dell'hardware del server, del tipo di applicazioni utilizzate e delle attività eseguite dai client Citrix. È necessario verificare le caratteristiche delle prestazioni di DLP Agent per l'ambiente.

Prodotto	Consigli di distribuzione e dettagli sulle prestazioni
Citrix XenDesktop	<ul style="list-style-type: none"> ■ È necessario installare il software DLP Agent in ogni computer virtuale sul server di XenDesktop. ■ Il software DLP Agent può connettersi a un server Endpoint Prevent o a un server Endpoint Prevent condiviso con agenti non Citrix. Non è possibile connettersi a un server Endpoint Prevent riservato per Citrix XenApp. <p>Nota: Se si utilizza lo stesso server sia per agenti Citrix che per agenti non Citrix, non è possibile configurare gli eventi indipendentemente per ogni ambiente.</p>

Restrizione del server di rilevamento per Symantec DLP Agents in Citrix XenApp

Symantec non consiglia di utilizzare un singolo server di rilevamento di Endpoint Prevent sia con computer endpoint fisici sia con server Citrix XenApp. Quando si utilizza la console di amministrazione di Enforce Server per configurare eventi di endpoint da monitorare, è necessario deselezionare eventi di CD/DVD e dell'unità locale per agenti Citrix XenApp. Questi elementi sono presenti nella schermata **Configurazione dell'agente**, ma non sono supportati per Citrix XenApp. L'utilizzo dello stesso Endpoint Server per agenti non Citrix limita la funzionalità di tali agenti, perché è necessario disattivare gli eventi dell'unità locale e del CD/DVD per il server nel suo complesso.

Per supportare DLP Agent sia su server Citrix XenApp sia su computer endpoint fisici, Symantec consiglia di distribuire due Endpoint Server e di assicurarsi che ogni server sia riservato per agenti di Citrix XenApp o per le installazioni di agenti endpoint fisici.

Copertura del monitoraggio endpoint virtualizzato Citrix

DLP Agent monitora le seguenti posizioni e attività nell'endpoint virtualizzato Citrix:

- Volumi
- Richieste di stampa/fax
- Appunti
- Rete
- Scansione dei file Microsoft Office
- Ripristino dei file nelle unità del client Citrix
- Monitoraggio dell'accesso ai file delle applicazioni e dei file caricati nei browser

Nota: Se XenApp trasmette un'applicazione direttamente su un computer endpoint, il Symantec DLP Agent che viene distribuito sul server XenApp non può monitorare l'applicazione trasmessa.

Incidenti registrati dagli endpoint virtualizzati Citrix

Tutti gli incidenti generati su unità Citrix da DLP Agent appaiono come incidenti **Dispositivo di archiviazione rimovibile**. Nella console di amministrazione di Enforce Server non è possibile deselezionare l'evento **Archivi rimovibili** per le unità Citrix. L'evento **Archivi rimovibili** è sempre monitorato da agenti distribuiti nei server Citrix.

Nota: Gli indirizzi IP nelle istantanee incidente contengono l'indirizzo IP del computer virtuale XenDesktop o del server XenApp e non un client Citrix.

Informazioni sull'implementazione di VMware Fusion

Le impostazioni che vengono applicate quando si implementano endpoint virtuali VMware Fusion determinano ciò che può essere monitorato da Symantec Data Loss Prevention.

Le seguenti impostazioni influiscono sul supporto di monitoraggio di Symantec Data Loss Prevention:

- **Maggiore inclusione** consente a Symantec Data Loss Prevention di monitorare i file che si trovano sull'endpoint virtualizzato di Windows e sul file system dell'host Mac o di spostarli.
- **Maggiore isolamento** consente a Symantec Data Loss Prevention di monitorare dati che si trovano sull'endpoint virtualizzato di Windows o di spostarli.

Informazioni sulla RRC

La RRC (Rules Results Caching, memorizzazione dei risultati delle regole nella cache) è una forma di prerilevamento di DLP Agent. In seguito alla memorizzazione nella cache delle informazioni sui contenuti che non corrispondono a una regola, DLP Agent può ignorare il contenuto. La RRC accelera il rilevamento perché consente a DLP Agent di eseguire solo il rilevamento di contenuti nuovi o modificati di recente.

Soltanto i risultati della regola DMC (Described Content Matching) possono essere memorizzati nella cache in DLP Agent. Altri tipi di rilevamento, ovvero Exact Data Matching (EDM), File Properties Type (FPT) e Indexed Data Matching (IDM), non sono applicabili alla RRC. Inoltre la RRC non è applicabile al protocollo o alle regole di rilevamento di gruppo.

Vedere ["Rilevamento della perdita di dati"](#) a pagina 387.

Ogni volta che le politiche associate a DLP Agent vengono modificate, la cache RRC viene eliminata. I risultati della RRC precedenti vengono cancellati ed è necessario eseguire di nuovo la scansione di tutto il contenuto. Tuttavia, al completamento della scansione iniziale, le scansioni successive possono essere completate molto più rapidamente.

Per impostazione predefinita la RRC è attiva. Se non si desidera la RRC, selezionare le impostazioni avanzate dell'agente e disattivarle.

Informazione sulla creazione di politiche per Endpoint Prevent

Le politiche di Endpoint Prevent eseguono condizioni DCM e VML localmente sull'endpoint. Una politica di Endpoint Prevent contiene una regola di risposta che crea un'interazione in tempo reale dell'utente. L'interazione dell'utente blocca un trasferimento di file o informa l'utente di una violazione della politica. Queste notifiche sono quindi allegate all'incidente.

Le politiche endpoint differiscono anche riguardo a dove viene eseguito il rilevamento. Il rilevamento per le politiche DGM e EDM viene eseguito su Endpoint Server. Il rilevamento per le politiche IDM e DCM viene eseguito direttamente da Symantec DLP Agent.

Le regole di risposta Blocca, Notifica e Operazione annullata dall'utente sono eseguite solo da Symantec DLP Agent.

Poiché il rilevamento per le politiche EDM e DGM viene eseguito su Endpoint Server, il rilevamento richiede più tempo e utilizza più larghezza di banda. Questo perché il contenuto dei file viene inviato a Endpoint Server per il rilevamento. Quando un agente esegue il rilevamento per le politiche DCM e IDM, invia solo gli incidenti a Endpoint Server.

Vedere ["Linee guida per la creazione di politiche endpoint"](#) a pagina 2035.

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

Vedere ["Scenari della politica di tecnologia di rilevamento agente Mac"](#) a pagina 2045.

Informazioni sul monitoraggio di politiche con regole di risposta per Endpoint Server

Le regole di risposta specifiche di Endpoint comprendono Endpoint: blocca, Endpoint: notifica, Endpoint: metti file in quarantena e Endpoint: operazione annullata dall'utente. Endpoint: blocca arresta lo spostamento di dati che violano politiche. Endpoint: notifica informa l'utente della violazione che si è verificata, ma non blocca o arresta lo spostamento dei dati. Endpoint: metti file in quarantena sposta un file con informazioni riservate dall'unità locale a una posizione sicura. Endpoint: metti file in quarantena è disponibile solo per Endpoint Discover. Endpoint: operazione annullata dall'utente consente all'utente endpoint di decidere se consentire o meno il trasferimento di dati. Tutte le regole generano una finestra pop-up contenente informazioni sulla politica violata. Ogni regola richiede che l'utente fornisca una giustificazione per l'azione. Endpoint: blocca, Endpoint: notifica e Endpoint: operazione annullata dall'utente sono applicabili a tutte le politiche di rilevamento di Endpoint Prevent eseguite sull'endpoint. Ad esempio, per il monitoraggio USB, HTTP/HTTPS, E-mail/STMP, FTP, CD/DVD, eSATA e Stampa/fax sono utilizzate le regole Endpoint: blocca e Endpoint: notifica.

Le regole di risposta Endpoint: notifica, Endpoint: blocca e Endpoint: operazione annullata dall'utente non sono applicabili a:

- Violazioni in Endpoint Discover

- Violazioni nei sistemi di monitoraggio di unità locali

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

Vedere ["Funzionalità della regola di risposta della politica dell'agente Mac"](#) a pagina 2047.

Informazioni su Endpoint: blocca

È possibile creare una politica per limitare il trasferimento di dati dall'endpoint. Ad esempio, si desidera bloccare il trasferimento di qualsiasi testo, e-mail o file contenente la parola chiave *Farallon* dal computer. È possibile creare una politica di corrispondenza con parole chiave utilizzando *Farallon* come parola chiave della violazione.

Vedere ["Flusso di lavoro per l'implementazione di politiche"](#) a pagina 384.

Si desidera inoltre utilizzare questa politica in tutti gli endpoint. Nella sezione delle regole di risposta, selezionare **Endpoint: blocca** come regola di risposta. Questa regola di risposta è applicabile solo all'endpoint. Se un file viene trasferito dall'unità disco rigido in un'unità CD/DVD, una notifica viene visualizzata su quell'endpoint. La notifica indica che l'azione viola la politica con la parola chiave *Farallon*.

La regola di risposta Endpoint: blocca impedisce lo spostamento del file. Tuttavia, si desidera avere anche un record del motivo che ha generato la violazione. Nella regola di risposta, è possibile creare una serie di giustificazioni. Queste giustificazioni permettono all'utente endpoint che ha commesso la violazione di spiegare il motivo della violazione. Le giustificazioni possono includere la formazione dell'utente, uno spostamento di file approvato dal responsabile o altro.

Informazioni su Endpoint: notifica

È possibile creare una politica e una regola di risposta che informa gli utenti endpoint mediante la regola di risposta Endpoint: notifica. La regola di risposta Endpoint: notifica visualizza un messaggio che descrive la violazione e informa l'utente endpoint sulla politica appropriata.

Ad esempio, un utente endpoint invia un e-mail che contiene la parola *Farallon* nel corpo del messaggio. Endpoint: notifica genera un incidente che è inviato all'Endpoint Server e visualizza una notifica sull'endpoint. La notifica indica la politica che è stata violata e che l'azione dell'endpoint è ora monitorata. L'utente endpoint indica una ragione per la violazione, accetta la notifica e l'e-mail procede normalmente. Endpoint: notifica non impedisce il movimento di dati, notifica soltanto agli utenti le violazioni della politica. La giustificazione dell'utente endpoint per la violazione diventa parte del report incidente inviato a Enforce Server.

Non tutti i gruppi di politiche e le politiche sono applicabili alle regole di risposta endpoint. Se si tenta di creare una politica con regole e risposte non compatibili, si ha un messaggio di errore. L'errore informa che la politica non è compatibile con le regole di risposta endpoint.

Le regole di risposta possono fare la distinzione tra gli incidenti creati nella rete aziendale e quelli creati all'esterno della rete aziendale. Questa condizione consente di specificare se la

regola è sempre attiva o se lo è solo quando l'endpoint viene connesso o disconnesso dalla rete aziendale.

Informazioni sulla regola di risposta Endpoint: operazione annullata dall'utente

È possibile creare una regola di risposta che consente agli utenti endpoint di decidere se consentire o meno il trasferimento di dati riservati dai loro computer. È possibile usare la regola di risposta Operazione annullata dall'utente per informare gli utenti endpoint sulle politiche aziendali appropriate. Ad esempio, se un utente endpoint invia informazioni riservate via e-mail e riceve la notifica Operazione annullata dall'utente, può annullare il trasferimento di dati. L'utente viene in questo modo informato sulle politiche dell'azienda. Inoltre, se esiste la legittima necessità per l'utente endpoint di trasferire dati riservati, può consentire l'azione. I dati vengono quindi trasferiti normalmente.

In entrambi i casi, Symantec DLP Agent genera un incidente che è inviato a Enforce Server.

Gli utenti endpoint hanno a disposizione uno specifico intervallo di tempo per decidere se ignorare o meno la politica. Se l'intervallo di tempo viene superato, la politica blocca automaticamente il trasferimento di dati e genera un incidente. Per impostazione predefinita, l'intervallo di tempo è limitato a 60 secondi. Tale opzione si applica a tutte le violazioni di quella politica che si verificano nei 10 secondi successivi.

Se molteplici violazioni della stessa politica vengono bloccate, l'utente endpoint deve immettere la giustificazione una sola volta. La giustificazione è visualizzata nell'istantanea dell'incidente. L'istantanea incidente indica inoltre l'azione intrapresa. L'istantanea incidente contiene una delle seguenti azioni:

- Utente notificato, azione: consentito
- Utente notificato, azione: annullato
- Utente notificato, azione: timeout annullato
- Utente notificato, azione: timeout consentito

Nota: È possibile specificare se consentire o meno all'azione predefinita di un timeout di bloccare o autorizzare il trasferimento di dati.

Vedere ["Configurazione dell'azione Endpoint Prevent: operazione annullata dall'utente"](#) a pagina 1557.

Vedere ["Linee guida per la creazione di politiche endpoint"](#) a pagina 2035.

Come implementare Endpoint Prevent

Endpoint Prevent controlla ogni endpoint per i dati spostati da una posizione all'altra. Se Endpoint Prevent rileva una violazione, blocca il trasferimento dei dati. Endpoint Prevent informa l'utente circa la violazione e può richiedere una giustificazione da parte dell'utente. L'implementazione di Endpoint Prevent richiede il completamento dei seguenti processi in ordine.

Tabella 78-5 Passaggi di implementazione

Passaggio	Azione	Per ulteriori informazioni
1	Aggiungere un Endpoint Server.	Vedere "Aggiunta di un server di rilevazione" a pagina 268.
2	Creare le configurazioni dell'agente endpoint.	Vedere "Informazioni sulle configurazioni dell'agente" a pagina 2110.
3	Impostare la posizione dell'endpoint. Questo è un passaggio facoltativo.	Vedere "Configurazione della posizione dell'endpoint" a pagina 2076.
4	Installare Symantec DLP Agent.	Per i dettagli dell'installazione, consultare il <i>Manuale di installazione di Symantec Data Loss Prevention</i> .
5	Creare una politica dell'endpoint.	Vedere "Informazione sulla creazione di politiche per Endpoint Prevent" a pagina 2073.
6	Creare le regole di risposta dell'endpoint.	Vedere "Azioni delle regole di risposta per il rilevamento di endpoint" a pagina 1470.
7	Configurare i report.	Vedere "Informazioni sui report Symantec Data Loss Prevention" a pagina 1632.

Vedere ["Introduzione a Directory Group Matching \(DGM\) sincronizzato"](#) a pagina 846.

Configurazione della posizione dell'endpoint

La posizione dell'endpoint viene utilizzata per definire in che modo Symantec Data Loss Prevention determina se l'endpoint è connesso o meno alla rete aziendale. È possibile specificare se Endpoint Server deve rilevare automaticamente la presenza dell'endpoint nella rete aziendale. È anche possibile specificare nomi di dominio o indirizzi IP utilizzabili per determinare manualmente se l'endpoint è connesso alla rete.

Utilizzando il metodo automatico per determinare la posizione dell'endpoint, Symantec Data Loss Prevention identifica se il computer è all'interno o all'esterno della rete aziendale in base alla connessione di DLP Agent a Endpoint Server.

Il metodo automatico è descritto di seguito:

- All'interno della rete aziendale:
Se DLP Agent è connesso a Endpoint Server, Symantec Data Loss Prevention identifica l'agente come all'interno della rete aziendale. La connessione di DLP Agent a Endpoint Server è transitoria, nel senso che l'agente si disconnette da Endpoint Server dopo un determinato periodo di tempo. Durante il periodo di connessione transitoria, Symantec Data Loss Prevention considera l'agente come all'interno della rete aziendale.
- All'esterno della rete aziendale:
Questo stato indica che DLP Agent è disconnesso da Endpoint Server. DLP Agent può essere disconnesso in modo anormale da Endpoint Server. Ad esempio, una disconnessione anormale si ha in caso di disconnessione dell'interfaccia di rete che connette l'agente a Endpoint Server. Se DLP Agent viene disconnesso anormalmente, Symantec Data Loss Prevention identifica l'endpoint come all'esterno della rete aziendale.

Vedere ["Informazioni sullo stato dell'agente"](#) a pagina 2199.

Se si utilizza il metodo manuale per determinare la posizione dell'endpoint, è necessario dapprima indicare un intervallo di nomi di dominio o indirizzi IP. Symantec Data Loss Prevention usa quindi queste informazioni per determinare se l'endpoint è connesso alla rete aziendale. Se un intervallo di nomi di dominio è configurato, DLP Agent esegue una ricerca DNS inversa sull'indirizzo IP host. Abbina quindi i nomi host DNS recuperati ai nomi di dominio configurati nell'elenco. Se un intervallo di indirizzi IP è configurato, DLP Agent abbina l'indirizzo IP host in base all'elenco di indirizzi IP configurati. Ogni singolo indirizzo IP host deve essere all'interno della rete aziendale perché l'endpoint sia considerato connesso alla rete aziendale.

I nomi di dominio non devono contenere caratteri jolly e devono essere suffissi semplici, ad esempio, symantec.com.

Gli indirizzi IP possono contenere caratteri jolly al posto di un singolo blocco. Ad esempio, 192.168.*.*.

Vedere ["Informazioni sul monitoraggio di Endpoint Prevent"](#) a pagina 2060.

Per configurare l'impostazione Posizione endpoint

- 1 Accedere a **Sistema > Agenti > Posizione endpoint**. Vengono visualizzate le impostazioni correnti relative alla posizione dell'endpoint. Per impostazione predefinita, la determinazione della posizione dell'endpoint è impostata su **Automatico**.
- 2 Fare clic su **Configura**.
- 3 Selezionare un elemento per configurare il modo in cui Enforce Server determina la posizione dell'endpoint.
 - Selezionare **Automaticamente** per consentire a Endpoint Server di determinare se un agente si trova all'interno o all'esterno della rete aziendale.

Nota: È necessario usare la posizione endpoint automatica per identificare le posizioni degli endpoint Mac. La posizione endpoint manuale non è supportata per i DLP Agent in esecuzione su endpoint Mac.

- Selezionare **Manualmente** e immettere un elenco di nomi di dominio o indirizzi IP nel campo appropriato. Immettere un solo nome di dominio o indirizzo IP per riga.

4 Fare clic su **Salva**.

Le modifiche diventano effettive dopo la connessione dell'agente a Endpoint Server.

Vedere ["Come implementare Endpoint Prevent"](#) a pagina 2076.

Vedere ["Endpoint Server - Configurazione di base"](#) a pagina 255.

Vedere ["Posizione endpoint agente Mac"](#) a pagina 2041.

Informazioni sulle regole di risposta di Endpoint Prevent con impostazioni locali differenti

È possibile creare notifiche di regole di risposta endpoint differenti che sono specifiche delle impostazioni locali di un endpoint. Le impostazioni locali sono definite nel sistema operativo dell'endpoint.

Ad esempio, è possibile creare notifiche di regole di risposta in inglese, francese o giapponese. Se il giapponese è la lingua scelta per le impostazioni locali, le notifiche sono visualizzate in quella lingua sullo schermo dell'utente. Se un altro utente con impostazioni locali francesi viola la stessa politica, viene visualizzata la versione in francese della notifica.

Enforce Server consente di specificare molteplici notifiche utente. Tuttavia, la prima lingua specificata è quella predefinita. Non è possibile eliminare le notifiche di risposta nella lingua predefinita. È possibile aggiungere o eliminare qualsiasi notifica o lingua non specificata come lingua predefinita. All'installazione, la lingua predefinita è quella di Enforce Server. Se la lingua desiderata non è supportata, Enforce Server prova a visualizzare la notifica in inglese.

Ad esempio, si ha un endpoint con impostazioni locali in giapponese e uno con impostazioni locali in vietnamita. La lingua vietnamita non è supportata. Se si ha una violazione sul computer con impostazioni locali in giapponese, Enforce Server visualizza la notifica in giapponese. Se non è disponibile alcuna notifica in giapponese, Enforce Server visualizza la notifica nella lingua predefinita. Se il computer con impostazioni locali in vietnamita viola una politica, Enforce Server visualizza la notifica in inglese in quanto le notifiche in vietnamita non sono supportate. Se la notifica in inglese non è disponibile, Enforce Server visualizza la notifica nella lingua predefinita.

Se la prima lingua aggiunta non è supportata sull'endpoint, quella lingua non può essere considerata come lingua predefinita. L'endpoint deve contenere specifici dettagli sulla lingua perché questa sia considerata come la lingua predefinita. Sebbene il testo della notifica sia

visualizzato in una lingua non supportata, i pulsanti della finestra di notifica e la barra del titolo sono visualizzati nella lingua definita nelle impostazioni locali predefinite di Enforce Server.

Se si desidera definire una lingua non supportata come lingua predefinita, selezionare **Altro** come prima lingua. L'etichetta **Altro** rimuove tutte le altre lingue nell'elenco. Utilizzare le opzioni di configurazione Endpoint per modificare il testo delle etichette delle finestre pop-up. Non è possibile specificare risposte in altre lingue se si seleziona l'opzione **Altro**. L'impostazione **Altro** visualizza notifiche in quella lingua su ogni endpoint, indipendentemente dalle impostazioni locali degli endpoint.

Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.

Nota: L'impostazione predefinita di tutte le impostazioni locali in inglese è Inglese (Stati Uniti). L'impostazione predefinita di tutte le impostazioni locali in francese è Francese. Ad esempio, l'impostazione Francese (Francia) supporta tutti le varianti di Francese, quali Francese (Canada) e Francese (Francia).

Vedere ["Configurazione delle regole di risposta di Endpoint Prevent per differenti impostazioni locali"](#) a pagina 2079.

Configurazione delle regole di risposta di Endpoint Prevent per differenti impostazioni locali

È possibile configurare regole di risposta diverse per differenti impostazioni locali. Le prime impostazioni locali designate diventano quelle predefinite. Non è possibile eliminare queste impostazioni locali, ma è possibile eliminare le altre.

Vedere ["Informazioni sulle regole di risposta di Endpoint Prevent con impostazioni locali differenti"](#) a pagina 2078.

Configurazione di una regola di risposta localizzata

- 1 Accedere a **Gestisci > Politiche > Regole di risposta**.

Vedere ["Configurazione di regole di risposta"](#) a pagina 1491.

- 2 Creare la regola di risposta normalmente.
- 3 Fare clic sul collegamento **Aggiungi lingua**.
- 4 Selezionare la lingua che si desidera usare.

Se si desidera specificare una lingua non supportata come lingua predefinita, selezionare **Altro**.

- 5 Digitare il testo nei campi di visualizzazione e di giustificazione utilizzando la lingua designata.
- 6 Fare clic su **Salva**.

Utilizzo di Endpoint Discover

Il capitolo contiene i seguenti argomenti:

- [Funzionamento di Endpoint Discover](#)
- [Informazioni sulla scansione di Endpoint Discover](#)
- [Preparazione dell'impostazione di Endpoint Discover](#)
- [Impostazione e configurazione di Endpoint Discover](#)
- [Creazione di una scansione Endpoint Discover](#)
- [Gestione delle scansioni target Endpoint Discover](#)

Funzionamento di Endpoint Discover

Endpoint Discover consente di esaminare un'unità locale dell'organizzazione per identificare tutti i dati che sono un rischio potenziale. Endpoint Discover invia una notifica quando trova un file che viola le politiche e identifica la posizione del file nel sistema endpoint. Endpoint Discover può eseguire la scansione di qualsiasi unità locale connessa all'endpoint. Non può eseguire la scansione di unità CD/DVD o dispositivi rimovibili come unità eSATA, unità flash USB o schede SD.

Vedere ["Informazioni sulla scansione di Endpoint Discover"](#) a pagina 2080.

Informazioni sulla scansione di Endpoint Discover

Endpoint Discover esegue la scansione dell'unità locale degli endpoint per trovare gli eventuali file attualmente esistenti che violano le politiche. Endpoint Discover esegue la scansione di tutte le unità locali sugli endpoint. Ad esempio, se il computer ha due unità locali fisiche

installate, Endpoint Discover cerca in entrambe gli eventuali file che violano le politiche. Endpoint Discover non sottopone a scansione le unità montate tramite una rete o i supporti rimovibili quali unità eSATA, unità flash o schede SD.

È possibile utilizzare Endpoint Discover per sottoporre a scansione tutti gli endpoint in un'organizzazione o solo quelli specificati.

Nota: A partire da Symantec Data Loss Prevention 15.0, Two Tier Detection (TTD) non è più supportato. Tuttavia, anche se viene generata una richiesta Two Tier Detection per le versioni di DLP Agent precedenti a 15.0, Endpoint Server ignora questi agenti e non esegue questa richiesta.

Per avviare o arrestare una scansione configurata per un Endpoint Server, DLP Agent deve essere collegato a Endpoint Server. Se DLP Agent non è collegato a Endpoint Server, la scansione comincia quando si ricollega a Endpoint Server. Una scansione è completa solo quando tutti gli endpoint hanno completato la scansione. Se un endpoint è scollegato da Endpoint Server, la scansione non può completarsi finché quell'endpoint non si ricollega o viene raggiunto il timeout della scansione. Se un endpoint viene scollegato dopo l'inizio di una scansione, l'endpoint continua la scansione non in linea e comunica lo stato dopo essersi ricollegato a Endpoint Server. Se l'endpoint rimane scollegato e supera un periodo di timeout configurato, la scansione segnala uno stato di timeout.

In un ambiente a carico bilanciato, selezionarle tutti gli Endpoint Server che si connettono a un sistema di bilanciamento del carico. In modo che quando gli endpoint si connettono a uno di questi Endpoint Server, gli endpoint ricevano gli stessi dettagli di scansione.

Tutti gli incidenti sono memorizzati in Agent Store fino a quando il computer si ricollega a Endpoint Server. Se Agent Store supera il limite di dimensione specificato, la scansione attende che Agent Store si ricollega a Endpoint Server e trasferisce gli incidenti.

Vedere ["Informazioni su DLP Agent Store"](#) a pagina 2129.

Informazioni sulla scansione degli endpoint target

È possibile utilizzare le scansioni mirate di Endpoint Discover per effettuare le seguenti operazioni:

- Definire una scansione di Endpoint Discover che utilizza molteplici Endpoint Server per sottoporre a scansione gli endpoint.
- Definire una scansione di Endpoint Discover per sottoporre a scansione singoli endpoint. Il target Endpoint Discover può essere configurato per sottoporre a scansione endpoint specifici. È possibile identificare gli endpoint utilizzando il nome host o l'indirizzo IP. È inoltre possibile caricare un file con l'elenco degli endpoint per nome host e indirizzo IP. Le politiche di scansione si applicano solo a questi endpoint specificati.

Vedere ["Creazione di una scansione Endpoint Discover"](#) a pagina 2089.

Durante la creazione di un target Endpoint Discover è possibile utilizzare una delle seguenti opzioni, come descritto nella seguente tabella:

Tabella 79-1 Opzioni per la creazione di un target Endpoint Discover

Opzione	Descrizione
Specificare gli Endpoint Server senza specificare gli endpoint	In questo caso, Enforce Server invia i dettagli di scansione agli Endpoint Server specificati. Quando gli endpoint si connettono agli Endpoint Server specificati, i dettagli di scansione sono inviati a loro.
Specificare gli Endpoint Server e gli endpoint	In questo caso, Enforce Server invia i dettagli di scansione agli Endpoint Server specificati. Quando l'endpoint specificato si connette all'Endpoint Server specificato, i dettagli di scansione sono inviati agli endpoint specificati. Quindi, solo gli endpoint specificati eseguono la scansione e ottimizzano la larghezza di banda della rete e risparmiano tempo.

Informazioni sulla scansione completa di Endpoint Discover

Un target di Endpoint Discover può essere configurato per utilizzare l'opzione di scansione completa. Questa opzione esegue la scansione di tutti i file nell'endpoint.

Se la politica o i filtri sono stati modificati significativamente in un target endpoint esistente e si desidera rendere effettive le modifiche, potrebbe essere necessario eseguire una scansione completa anziché una scansione incrementale.

Vedere ["Informazioni sulla scansione incrementale di Endpoint Discover"](#) a pagina 2082.

Vedere ["Uso dei filtri di inclusione ed esclusione"](#) a pagina 2097.

Informazioni sulla scansione incrementale di Endpoint Discover

Per impostazione predefinita, i target di Endpoint Discover vengono creati come target di scansione incrementale. In una scansione incrementale, DLP Agent esegue la scansione solo dei file che sono stati aggiunti o modificati dall'inizio della precedente scansione. Quando si esegue per la prima volta il target di scansione, DLP Agent esamina tutti i file nell'endpoint.

Nota: Con l'aggiunta del supporto alla scansione incrementale per Endpoint Discover, l'opzione di scansione differenziale non è più disponibile. Tuttavia, se sono presenti degli endpoint con le versioni 14.6 e 15.0 di DLP Agent e si esegue una scansione incrementale di Endpoint Discover, gli agenti della versione 14.6 continuano a eseguire la scansione differenziale. Vedere ["Scansione di elementi nuovi o modificati con scansioni differenziali"](#) a pagina 1872. per ulteriori informazioni sulla scansione differenziale.

Vedere ["Informazioni sulla scansione completa di Endpoint Discover"](#) a pagina 2082.

Vedere ["Uso dei filtri di inclusione ed esclusione"](#) a pagina 2097.

Funzionamento della scansione incrementale per Endpoint Discover

Nella scansione incrementale, DLP Agent ricorda la data, l'ora e la posizione file dell'ultima scansione di file. Queste informazioni si chiamano checkpoint. DLP Agent salva il checkpoint nel proprio database locale, per poterlo utilizzare per riprendere la scansione da dove è stata interrotta l'ultima volta.

Le scansioni incrementali si completano nelle seguenti fasi:

- Fase 1: DLP Agent esegue la scansione dei file che non è stato possibile analizzare nella precedente esecuzione dello stesso target Endpoint Discover.
- Fase 2: DLP Agent esegue la scansione solo dei file che sono stati aggiunti o modificati dall'ultimo checkpoint.

I seguenti esempi descrivono la sequenza di scansione incrementale per due endpoint.

- Quando la scansione precedente è incompleta nell'endpoint 1 e completa nell'endpoint 2. La scansione incrementale viene eseguita in due fasi:

Per l'endpoint 1:

- Fase 1: completamento della precedente scansione incompleta.
- Fase 2: scansione solo dei file che sono stati aggiunti o modificati dall'ultimo checkpoint.

Per l'endpoint 2:

- La fase 1 non è applicabile poiché la precedente scansione era completa.
- La fase 2 è applicabile e la scansione incrementale analizza solo dei file che sono stati aggiunti o modificati dall'ultimo checkpoint.

L'esempio precedente è riassunto nella seguente tabella:

Tabella 79-2 Scansione incrementale eseguita in due fasi

Fasi	La scansione precedente non è completa nell'endpoint 1	La scansione precedente è completa nell'endpoint 2
Fase 1	Applicabile	Non applicabile
Fase 2	Applicabile	Applicabile

- Considerare un altro esempio, in cui una nuova scansione target Endpoint Discover viene eseguita per la prima volta con l'opzione di scansione incrementale; in questo caso solo la fase 2 è applicabile. La scansione incrementale esamina tutti i file aggiunti o modificati dopo il 1° gennaio 1970 (epoca).

Nota: Symantec consiglia di eseguire una scansione completa invece di una scansione incrementale nei seguenti casi:

- Eseguire una scansione target Endpoint Discover e successivamente modificare il percorso del filtro per includere un file che non faceva parte della precedente scansione target Endpoint Discover. Se questo file non è stato modificato dall'ultimo checkpoint, non viene esaminato se si esegue una scansione incrementale.
- Per macOS, la data e l'ora di un file (la data e l'ora di creazione, modifica o accesso di un file) non cambia se si copia il file da una posizione a un'altra. Se si esegue una scansione completa Endpoint Discover e, in seguito, qualche file viene spostato localmente nel percorso della cartella di destinazione di Endpoint Discover, ma l'ultima modifica era avvenuta prima della scansione completa, la scansione incrementale successiva non esamina questi file. Poiché la data e l'ora dei file è precedente alla scansione completa, anche se i file sono stati aggiunti alla cartella di destinazione dopo la scansione, non vengono riconosciuti come file da considerare per una scansione incrementale.

Informazioni sulle scansioni parallele negli endpoint target

Endpoint Server può ricevere più scansioni da Enforce Server ed eseguirle in parallelo purché gli endpoint target specificati non siano sovrapposti. Qualora ci sia una sovrapposizione, ovvero se lo stesso endpoint è l'oggetto di due diverse scansioni, è necessario che la prima scansione si completi affinché la seconda possa iniziare.

Considerare i seguenti scenari che descrivono la sequenza di scansione parallela per i DLP Agent A, B, C e D, tutti connessi allo stesso Endpoint Server. La seguente scansione di target Endpoint Discover viene eseguita nei DLP Agent specificati:

- La scansione 1 viene eseguita nei DLP Agent A e B
- La scansione 2 viene eseguita nei DLP Agent C e D
- La scansione 3 viene eseguita nei DLP Agent A e C

Scenario 1:

In questo caso, si avviano le scansioni 1 e 2 una dopo l'altra. Di conseguenza, i DLP Agent A e B ricevono i dettagli della scansione 1 e i DLP Agent C e D ricevono i dettagli della scansione 2. Poiché non ci sono DLP Agent sovrapposti in queste scansioni, la scansione 1 e la scansione 2 vengono eseguite in parallelo.

Scenario 2:

In questo caso, prima si avvia la scansione 1 e poi si avvia la scansione 3. Di conseguenza, i DLP Agent A e B ricevono i dettagli della scansione 1 e il DLP Agent C riceve i dettagli della scansione 3. In questo scenario, il DLP Agent A è l'endpoint sovrapposto e può eseguire solo una scansione per volta. Di conseguenza, i DLP Agent A e B eseguono la scansione 1 e il DLP Agent C esegue la scansione 3. Il DLP Agent A non inizia a eseguire la scansione 3 non

appena finisce la scansione 1. Il DLP Agent A attende il completamento della scansione 1 nel DLP Agent B, prima di poter iniziare a eseguire la scansione 3.

È possibile eseguire le scansioni parallele. Non esiste un limite rigido sul numero di scansioni parallele che è possibile eseguire. Tuttavia, esistono i seguenti fattori limitanti:

- Dimensione e complessità della politica
- Intervallo di polling di DLP Agent (ServerCommunicator.CONNECT_POLLING_INTERVAL_SECONDS.int)
Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.
- Memoria di Endpoint Server

Tuttavia, in linea di massima, nei laboratori di prova è stato possibile eseguire 30 scansioni parallele per computer Endpoint Server con una memoria di 9 GB per una complessità media della politica e con un intervallo di polling di DLP Agent di 15 minuti.

Vedere ["Creazione di una scansione Endpoint Discover"](#) a pagina 2089.

Vedere ["Creazione di un nuovo target Endpoint Discover"](#) a pagina 2091.

Ottimizzazione della scansione per le prestazioni dell'endpoint

Per impostazione predefinita, Endpoint Discover esegue la scansione delle risorse dell'endpoint, il che può ridurre al minimo le attività dell'utente sull'endpoint. È possibile ottimizzare le prestazioni dell'endpoint procedendo quanto segue:

- Gestire le risorse, come utilizzo medio a lungo termine della CPU e durata della batteria minima restante, quando Endpoint Discover esegue la scansione degli endpoint.
Vedere ["Impostazioni di Utilizzo delle risorse per le scansioni Endpoint Discover"](#) a pagina 2128.

Nota: I DLP Agent eseguiti su endpoint Mac non usano la gestione di larghezza di banda CPU e l'impostazione di durata della batteria minima.

Vedere ["Funzionalità dei target Endpoint Discover per Mac"](#) a pagina 2058.

- Configurare DLP Agent per eseguire una scansione Endpoint Discover mentre l'utente endpoint è inattivo. Impostare il tempo di inattività dell'utente regolando le seguenti impostazioni avanzate dell'agente.
Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.
- Discover.SCAN_ONLY_WHEN_IDLE.int
- Discover.SECONDS_UNTIL_IDLE.int

Preparazione dell'impostazione di Endpoint Discover

Prima di cominciare l'installazione e la configurazione delle scansioni Endpoint Discover è necessario eseguire tutti i passaggi fondamentali.

[Tabella 79-3](#) elenca i passaggi obbligatori.

Tabella 79-3 Passaggi fondamentali di Endpoint Discover

Passaggio	Azione	Ulteriori informazioni
1	Aggiungere un server Endpoint Prevent se non ve n'è già uno o modificarne uno esistente.	Un server Endpoint Prevent monitora, impedisce e fornisce le funzionalità di scansione per i DLP Agent. Vedere "Endpoint Server - Configurazione di base" a pagina 255.
2	Creare un gruppo di politiche.	Vedere "Creazione di un gruppo di politiche per Endpoint Discover" a pagina 2086.
3	Creare una politica.	Vedere "Creazione di una politica per Endpoint Discover" a pagina 2087.
4	Aggiungere una regola.	Vedere "Aggiunta di una regola per Endpoint Discover" a pagina 2088.

Vedere ["Impostazione e configurazione di Endpoint Discover"](#) a pagina 2089.

Creazione di un gruppo di politiche per Endpoint Discover

Il processo di creazione di un gruppo di politiche per Endpoint Discover è identico a quello per Network Discover. La distribuzione di questi gruppi non avviene su nodi differenti del sistema ma sui Symantec DLP Agent. Dopo aver creato il gruppo di politiche, è possibile assegnarvi specifiche politiche.

Per creare un gruppo di politiche

- 1 Accedere a **Sistema > Server e rilevatori > Gruppi di politiche**.
- 2 Nella schermata **Elenco gruppo di politiche** visualizzata, fare clic su **Aggiungi**.
- 3 Immettere un nome (256 caratteri al massimo) e una descrizione per il gruppo di politiche. Scegliere un nome informativo in quanto gli altri utenti dovranno accedere al gruppo al momento della scelta dei gruppi di politiche da associare a ruoli, politiche e target di Endpoint Discover.

- 4 Scegliere il server di rilevamento da assegnare al gruppo di politiche. Questo passaggio è facoltativo.

È possibile assegnare il gruppo di politiche a tutti i server di rilevamento o a singoli server. Tenere presente che Symantec Data Loss Prevention assegna automaticamente tutti i gruppi di politiche a tutti i server Endpoint Discover.

- 5 Fare clic su **Salva**.

Vedere ["Impostazione e configurazione di Endpoint Discover"](#) a pagina 2089.

Vedere ["Creazione e modifica di gruppi di politiche"](#) a pagina 447. per ulteriori informazioni sulla creazione di un gruppo di politiche.

Creazione di una politica per Endpoint Discover

Vedere ["Linee guida per la creazione di politiche endpoint"](#) a pagina 2035.

È possibile impostare lo stato della politica come Attivo o Sospendi. L'impostazione predefinita dello stato delle politiche è Attiva. Se si seleziona Sospendi, la politica non viene applicata agli agenti DLP.

Le seguenti istruzioni si applicano alla creazione di una politica vuota. È inoltre possibile creare politiche basate su modelli preesistenti. Le seguenti istruzioni usano i dati del campione e le istruzioni specifiche per spiegare come creare una politica.

Per creare una politica per Endpoint Discover

- 1 Accedere a **Gestisci > Politiche > Elenco politiche** su Enforce Server.
- 2 Fare clic su **Aggiungi politica** e su **Avanti**.
- 3 Selezionare **Aggiungere una politica vuota**.
- 4 Inserire un nome per identificare la politica nel campo **Nome**.
- 5 Inserire i dettagli sulla politica nel campo **Descrizione** della nuova politica.
- 6 Selezionare il gruppo di politiche che si desidera associare a questa politica dal menu a discesa.

Dopo aver creato la politica, è necessario aggiungere regole alla politica.

Vedere ["Aggiunta di una regola per Endpoint Discover"](#) a pagina 2088.

Vedere ["Impostazione e configurazione di Endpoint Discover"](#) a pagina 2089.

Vedere ["Aggiunta di una nuova politica o di un modello di politica"](#) a pagina 421. per ulteriori informazioni sull'aggiunta di una nuova politica.

Aggiunta di una regola per Endpoint Discover

Dopo aver creato una politica per Endpoint Discover, è necessario aggiungere regole alla politica. È possibile aggiungere una o più regole a una politica. È necessario aggiungere almeno una regola a una politica.

Vedere ["Creazione di una politica per Endpoint Discover"](#) a pagina 2087.

Per aggiungere una regola a una politica

- 1 Nella scheda Rilevamento, fare clic su **Aggiungi regola** per aggiungere una regola per la politica.
- 2 Selezionare una regola appropriata. Ad esempio, selezionare l'opzione **Contenuto corrispondente a espressione regolare**.
- 3 Selezionare la politica che si desidera utilizzare nel menu a discesa.

Questa procedura collega l'elenco creato precedentemente alla regola.

- 4 Fare clic su **Avanti**.

Vedere ["Impostazione e configurazione di Endpoint Discover"](#) a pagina 2089.

Vedere ["Aggiunta di una regola a una politica"](#) a pagina 424. per ulteriori informazioni su come aggiungere una regola a una politica.

Informazioni sulla quarantena di endpoint

È possibile creare una regola di risposta automatica che consente a Endpoint Discover di spostare file da un'unità locale in una posizione protetta. Se una scansione di Endpoint Discover trova un file contenente dati riservati, il file viene messo in quarantena e rimosso dalla posizione non protetta. La posizione protetta può essere sull'unità locale o sulla rete aziendale. È possibile creare file marker che sostituiscono i dati riservati. I file marker indicano agli utenti endpoint che il file conteneva informazioni riservate e che è stato messo in quarantena. È possibile includere variabili nel testo marker che descrivono gli aspetti dell'incidente quali il nome di file, la politica violata e la posizione della cartella sicura.

Le regole di risposta specifiche dell'endpoint comprendono Endpoint: blocca, Endpoint: notifica e Operazione annullata dall'utente non sono applicabili per Endpoint Discover.

Nota: La quarantena dell'endpoint non è disponibile per i DLP Agent in esecuzione su endpoint Mac.

La posizione di quarantena può essere una cartella protetta sull'unità locale o una condivisione file remota accessibile dall'endpoint mediante la rete aziendale. È possibile scegliere se attivare delle credenziali per la posizione protetta o consentire a qualsiasi utente anonimo di accedere alla posizione.

Nota: Le cartelle EFS non possono supportare l'accesso anonimo.

Non tutti i gruppi di politiche e le politiche sono applicabili alle regole di risposta endpoint. Se si tenta di creare una politica con regole e risposte non compatibili, si ha un messaggio di errore. L'errore informa che la politica non è compatibile con le regole di risposta endpoint.

Vedere ["Linee guida per la creazione di politiche endpoint"](#) a pagina 2035.

Vedere ["Come implementare Endpoint Prevent"](#) a pagina 2076.

Vedere ["Configurazione dell'azione Endpoint Discover: metti file in quarantena"](#) a pagina 1545.

Impostazione e configurazione di Endpoint Discover

Per implementare Endpoint Discover, è necessario attenersi a un insieme specifico di attività. Queste attività sono simili a quelle di Network Discover, ma non identiche.

Completare le seguenti attività di configurazione:

Tabella 79-4 Implementazione di Endpoint Discover

Passaggio	Azione	Ulteriori informazioni
Passaggio 1	Creare un target di Endpoint Discover.	Vedere "Creazione di una scansione Endpoint Discover" a pagina 2089.
Passaggio 2	Installare Symantec DLP Agent.	Per i dettagli dell'installazione, consultare il <i>Manuale di installazione di Symantec Data Loss Prevention</i> .
Passaggio 3	Configurare i report.	Vedere "Informazioni sui report Symantec Data Loss Prevention" a pagina 1632.

Vedere ["Preparazione dell'impostazione di Endpoint Discover"](#) a pagina 2086.

Creazione di una scansione Endpoint Discover

Per creare una scansione Endpoint Discover, si imposta un target Endpoint Discover . Successivamente, configurare il target che corrisponde ai requisiti di scansione.

Il target Endpoint Discover può essere inoltre configurato per sottoporre a scansione posizioni specifiche sugli endpoint. La scansione può utilizzare filtri per sottoporre a scansione unità locali, tipi di file o cartelle e individuare violazioni di politica. Ad esempio, l'unità fissa o la cartella `Documenti` in Windows può essere configurata come filtro.

Tabella 79-5 Passaggi per configurare le impostazioni di scansione per un target di scansione Endpoint Discover

Passaggio	Descrizione	Ulteriori informazioni
1	Configurare un nuovo target Endpoint Discover.	Accedere alla schermata Gestisci > Scansione Discover > Target di Discover e fare clic su Nuovo target, File system endpoint . Vedere " Creazione di un nuovo target Endpoint Discover " a pagina 2091.
2	Configurare la scansione incrementale o completa	Si impostano queste informazioni nella scheda Generale quando si configura il nuovo target. Vedere " Informazioni sulla scansione incrementale di Endpoint Discover " a pagina 2082. Vedere " Informazioni sulla scansione completa di Endpoint Discover " a pagina 2082.
3	Configurare gli endpoint di destinazione	Si impostano queste informazioni nella scheda Destinazione quando si configura il nuovo target. Vedere " Informazioni sulla scansione degli endpoint target " a pagina 2081.
4	Aggiungere i filtri per posizione, dimensione file, data e tipo di file al target Endpoint Discover.	Si immettono queste informazioni nella scheda Filtri quando si configura il nuovo target. Vedere " Informazioni sui filtri di Endpoint Discover " a pagina 2096.
5	Configurare il timeout inattività di scansione e le impostazioni di durata massima delle scansioni.	Si impostano queste informazioni nella scheda Avanzate quando si configura il nuovo target. Vedere " Configurazione delle impostazioni timeout scansione di Endpoint Discover " a pagina 2104.

Nota: Non è possibile programmare scansioni Endpoint Discover mirate. Ogni scansione deve essere avviata manualmente. Anche operazioni come interrompere la scansione, consentire che la scansione venga completata o che vada in timeout devono essere eseguite manualmente. Non è possibile sospendere una scansione Endpoint Discover.

Creazione di un nuovo target Endpoint Discover

Per un nuovo target Endpoint Discover immettere il nome del target, il gruppo di politiche e l'Endpoint Server in cui possono essere eseguite le scansioni.

Questi campi obbligatori vanno impostati quando si aggiunge un nuovo target.

Per configurare i campi obbligatori per un target

- 1 Nella console di amministrazione di Enforce Server selezionare **Gestisci > Scansione Discover > Target di Discover**.
- 2 Fare clic su **Nuovo target**, quindi selezionare **File system** sotto **Endpoint**.

3 Compilare quanto segue nella scheda **Generale**.

Nome	Immettere un nome per il target Endpoint Discover.
Gruppi di politiche	<p>Selezionare il gruppo di politiche Endpoint Discover creato.</p> <p>Vedere "Creazione di un gruppo di politiche per Endpoint Discover" a pagina 2086.</p> <p>Se non è stato selezionato nessun altro gruppo di politiche, viene utilizzato il Gruppo di politiche predefinite. È possibile assegnare più gruppi di politiche a un solo target.</p> <p>L'amministratore definisce i gruppi di politiche nella pagina Elenco gruppo di politiche. Se il gruppo di politiche che si desidera utilizzare non appare nell'elenco, contattare l'amministratore Symantec Data Loss Prevention.</p>
Esecuzione scansione	<p>Selezionare l'opzione Esegui scansione solo di elementi nuovi o modificati (scansione incrementale) per una scansione incrementale. Questa opzione è predefinita per i nuovi target.</p> <p>Vedere "Informazioni sulla scansione incrementale di Endpoint Discover" a pagina 2082.</p> <p>Vedere "Funzionamento della scansione incrementale per Endpoint Discover" a pagina 2083.</p> <p>Nota: Quando si seleziona questa opzione, i filtri di data per Esegui scansione solo di file aggiunti o modificati e per Esegui scansione solo di ultimi file utilizzati sono disattivati nella scheda Filtri.</p> <p>In caso di modifica della politica o di altre definizioni in una scansione esistente, configurare la scansione successiva in modo che sia una scansione completa per essere certi di includere tutte le politiche. Selezionare l'opzione Esegui sempre scansione di tutti gli elementi (scansione completa).</p> <p>Vedere "Informazioni sulla scansione completa di Endpoint Discover" a pagina 2082.</p> <p>Nota: Se si cambia il tipo di scansione da incrementale a completa, la scansione incrementale reimposta il checkpoint. La configurazione di scansione modificata viene utilizzata per i file sottoposti a scansione a partire da quel checkpoint.</p>

4 Configurare i seguenti elementi nella scheda **Destinazione** della sezione **Server di scansione ed endpoint di destinazione**.

Server

Selezionare uno (o più) Endpoint Server da utilizzare per eseguire la scansione.

Soltanto i server di rilevamento configurati come Endpoint Server vengono visualizzati nell'elenco. Prima di configurare i target è necessario configurare gli Endpoint Server. È necessario specificare almeno un server prima di poter eseguire una scansione del target.

Endpoint target

Nel campo **Immetti nomi host e indirizzi IP**, immettere esattamente il nome host o l'indirizzo IP dell'endpoint connesso ai server di scansione selezionati. Il rilevamento a due livelli non viene eseguito per gli endpoint selezionati. Fare clic su **Aggiungi** per aggiungere questi agenti specificati all'elenco degli agenti target.

Nota: I caratteri jolly non sono supportati nel nome host.

È possibile creare un file con un elenco dei nomi host o degli indirizzi IP degli agenti target. Questo file deve contenere un nome host o indirizzo IP per riga. Nel campo **Aggiungi nomi host e indirizzi IP da un file**, fare clic su **Sfoglia** per individuare questo file e quindi fare clic su **Carica**.

5 Configurare gli elementi nella scheda **Filtri**.

Vedere ["Filtraggio dei target di Discover per dimensione dell'oggetto"](#) a pagina 1843.

Filtri di inclusione

Immettere gli elementi da includere nel monitoraggio della scansione Endpoint Discover.

Vedere ["Informazioni sui filtri di Endpoint Discover"](#) a pagina 2096.

Filtri di esclusione

Immettere gli elementi da escludere nel monitoraggio della scansione Endpoint Discover.

Vedere ["Informazioni sui filtri di Endpoint Discover"](#) a pagina 2096.

Ignora documenti di dimensioni inferiori a

Escludere gli elementi più piccoli di una determinata dimensione immettendo un numero nel campo accanto a **Ignora documenti di dimensioni inferiori a**. Selezionare quindi l'unità di misura appropriata (byte, KB o MB) dall'elenco a discesa accanto.

Ignora documenti di dimensioni superiori a

Escludere gli elementi più grandi di una determinata dimensione immettendo un numero nel campo accanto a **Ignora documenti di dimensioni superiori a**. Selezionare quindi l'unità di misura appropriata (byte, KB o MB) dall'elenco a discesa accanto.

Esegui scansione solo di file aggiunti o modificati...

Selezionare questa opzione per includere i file in base alla data di aggiunta o modifica. Endpoint Discover esegue la scansione soltanto degli elementi dopo la data specificata in **Dopo**, prima della data specificata in **Prima** o tra le date specificate.

Nota: Se la data in **Il o dopo** è successiva alla data in **Prima**, nessun elemento viene sottoposto a scansione. Se la data in **Prima** e la data in **Il o dopo** sono uguali, nessun elemento viene sottoposto a scansione. Questo perché l'ora presunta per il parametro **Prima** è 0:00 e quella di **Il o dopo** è 24:00.

Quando si seleziona questa opzione, è possibile selezionare anche le opzioni seguenti:

- **Il o dopo:** per includere gli elementi creati o modificati (a seconda di quali sono più recenti) dopo una data particolare, digitare la data. È anche possibile fare clic sul widget data e selezionare una data.
- **Prima:** per includere gli elementi creati o modificati (a seconda di quali sono più recenti) prima di una data particolare, digitare la data. È anche possibile fare clic sul widget data e selezionare una data.

Vedere "[Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica](#)" a pagina 1844.

Esegui scansione solo di ultimi file utilizzati... Selezionare questa opzione per includere i file in base all'ultima data di accesso.

Endpoint Discover esegue la scansione soltanto degli elementi dopo la data specificata in **Dopo**, prima della data specificata in **Prima** o tra le date specificate.

Nota: Se la data in **Dopo** è successiva alla data in **Prima**, nessun elemento viene sottoposto a scansione. Se la data in **Prima** e la data in **Dopo** sono uguali, nessun elemento viene sottoposto a scansione. Questo perché l'ora presunta per il parametro **Prima** è 0:00 e quella di **Dopo** è 24:00.

Quando si seleziona questa opzione, è possibile selezionare anche le opzioni seguenti:

- **Dopo:** per includere gli elementi a cui si ha effettuato l'accesso dopo una data particolare, digitare la data. È anche possibile fare clic sul widget data e selezionare una data.
- **Prima:** per includere gli elementi a cui si ha effettuato l'accesso prima di una data particolare, digitare la data. È anche possibile fare clic sul widget data e selezionare una data.

Vedere "[Filtraggio di target di Discover in base alla data dell'ultimo accesso o modifica](#)" a pagina 1844.

6 Configurare gli elementi nella scheda **Avanzate**.

Timeout inattività scansione

Immettere il timeout inattività di scansione in ore o minuti per interrompere la scansione di Endpoint Discover se nessun endpoint comunica lo stato della scansione a Enforce Server per un periodo di tempo specificato. Per disattivare **Timeout inattività scansione**, selezionare Indefinito per la durata.

Vedere ["Configurazione delle impostazioni timeout scansione di Endpoint Discover"](#) a pagina 2104.

Durata massima scansione

Immettere la durata massima della scansione in minuti, ore o giorni per l'esecuzione di una scansione di Endpoint Discover. Per disattivare **Durata massima scansione**, selezionare Indefinito per la durata. Quando una scansione di Endpoint Discover supera la durata impostata in Durata massima scansione, la scansione di Endpoint Discover viene interrotta e visualizza lo stato di timeout.

Vedere ["Configurazione delle impostazioni timeout scansione di Endpoint Discover"](#) a pagina 2104.

7 Fare clic su **Salva** per salvare tutti gli aggiornamenti al target.

Informazioni sui filtri di Endpoint Discover

I filtri di Endpoint Discover consentono di ottimizzare il tempo necessario a Endpoint Discover per il completamento di una scansione. I filtri si impostano per includere ed escludere:

- Tipi di file
- Percorsi di cartelle
- Dimensione del file
- Data di aggiunta o modifica del file
- Data ultimo accesso al file

Vedere ["Creazione di una scansione Endpoint Discover"](#) a pagina 2089.

Vedere ["Uso dei filtri di inclusione ed esclusione"](#) a pagina 2097.

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

Uso dei filtri di inclusione ed esclusione

I filtri di inclusione ed esclusione consentono di ridurre il numero di elementi da sottoporre a scansione.

Utilizzare il campo **Filtri di inclusione** per specificare gli elementi che Symantec Data Loss Prevention dovrà elaborare. Se si lascia vuoto il campo **Filtri di inclusione**, Symantec Data Loss Prevention ricerca la corrispondenza con tutti gli oggetti del target selezionato. Se si immette qualsiasi valore nel campo, Symantec Data Loss Prevention analizza solo gli elementi corrispondenti al filtro specificato.

Utilizzare il campo **Filtri di esclusione** per specificare gli elementi che Symantec Data Loss Prevention non deve elaborare. Se si lascia vuoto il campo **Filtri di esclusione**, Symantec Data Loss Prevention analizza tutti gli elementi nel target selezionato. Se si immette qualsiasi valore nel campo, Symantec Data Loss Prevention analizza solo gli elementi non corrispondenti al filtro specificato.

Quando vengono utilizzati sia i filtri di inclusione che i filtri di esclusione, quest'ultimi hanno la precedenza.

La [Tabella 79-6](#) elenca gli oggetti che è possibile includere o escludere utilizzando i filtri.

Tabella 79-6 Elementi filtrabili

Elemento da filtrare	Descrizione
Tipi di file	È possibile fornire estensioni di file in Filtri di inclusione e Filtri di esclusione , rispettivamente per includere o escludere i tipi di file.
Percorsi di cartelle	<p>È possibile fornire percorsi di cartelle in Filtri di inclusione e Filtri di esclusione, rispettivamente per includere o escludere le cartelle.</p> <p>È possibile specificare un filtro di percorso cartella per gli endpoint sia Windows che Mac negli stessi campi Filtri di inclusione e Filtri di esclusione.</p> <p>È possibile utilizzare le variabili ambientali per includere o escludere le posizioni file.</p> <p>Vedere "Utilizzo delle variabili di ambiente nelle scansioni Endpoint Discover" a pagina 2100.</p>

Ogni volta che si modificano i valori dei filtri di inclusione o esclusione per un target di Endpoint Discover con l'opzione di scansione incrementale selezionata, a seconda del tipo di modifica, si consiglia di eseguire la scansione successiva con l'opzione di scansione completa selezionata.

Ad esempio, se si esegue una scansione target incrementale di Endpoint Discover con il filtro di inclusione `*.docx`, vengono analizzati tutti i file con l'estensione `.docx` che sono stati aggiunti o modificati dopo la scansione precedente. Successivamente se si modifica il valore del filtro di inclusione `*.pdf` e si esegue una scansione incrementale, vengono analizzati solo i file PDF che sono stati modificati dopo l'ultima scansione (con il filtro di inclusione `*.docx`). Se si desidera eseguire la scansione di tutti i file PDF, è necessario eseguire la scansione target di Endpoint Discover con l'opzione di scansione completa selezionata.

Vedere ["Informazioni sulla scansione incrementale di Endpoint Discover"](#) a pagina 2082.

La tabella [Tabella 79-7](#) mostra la sintassi da utilizzare per l'aggiunta di filtri.

Tabella 79-7 Sintassi per filtri di inclusione ed esclusione

Sintassi	Descrizione
* (asterisco)	<p>Utilizzare questo carattere sostitutivo per la corrispondenza con zero o più caratteri.</p> <p>Il criterio <code>*.txt;*.doc</code> di un filtro di inclusione rileva solo file, documenti o cartelle con le estensioni <code>.txt</code> o <code>.doc</code> e ignora tutto il resto.</p> <p>Il criterio <code>*.*</code> aggiunto al termine del percorso funziona in modo analogo a <code>*</code>. Ad esempio un filtro come <code>\$Desktop\$/*</code> o <code>\$Desktop\$/*.*</code> hanno lo stesso significato.</p> <p>Se <code>*.*</code> separa un percorso di directory, Symantec Data Loss Prevention richiede un file o una cartella con un punto (.) che corrisponde al criterio. Ad esempio, <code>/Users/joe/Pack*.*.son</code> rileva <code>/Users/joe/Package.json</code> o <code>/Users/joe/Pack.son</code>, ma non <code>/Users/Joe/Packson</code>.</p> <p>Un criterio <code>*/documentation/*;*/specs/*</code> rileva solo la corrispondenza con sottodirectory specifiche di una condivisione file. Questo criterio di filtro di esempio seleziona solo i file contenuti nelle due sottodirectory denominate <code>documentation</code> e <code>specs</code>.</p>
? (punto interrogativo)	<p>Utilizzare questo carattere sostitutivo per la corrispondenza con un carattere nella posizione in cui si trova.</p> <p>Un criterio <code>*.??</code> di un filtro di inclusione rileva solo file con un'estensione a due caratteri. Questo esempio rileva file come <code>hello.go</code> e <code>hello.py</code>, ma non <code>hello.c</code> o <code>hello.cpp</code>.</p>
, (virgola)	Corrisponde a un OR logico. Delimitare le voci mediante virgole.
Caratteri barra (/) e barra rovesciata (\)	Questi caratteri sono equivalenti. Rappresentano in genere separatori di directory, anche se in macOS la barra rovesciata è un carattere valido in un nome file.

Sintassi	Descrizione
Caratteri escape	Il processo di corrispondenza non supporta i caratteri escape, quindi non è possibile stabilire una corrispondenza esplicita con un punto interrogativo, una virgola o un asterisco. In genere i caratteri speciali non sono supportati negli elementi filtro.

Di seguito sono riportati alcuni esempi aggiuntivi per i filtri di inclusione ed esclusione:

- Per eseguire la scansione dell'intero disco eccetto le cartelle Windows e Programmi su Windows, utilizzare il filtro di esclusione con valore: `$Windows$/*,$ProgramFiles$/*`
- Per eseguire la scansione dell'intero disco eccetto le cartelle Windows e Programmi su Windows e /usr, /sbin, /opt su Mac, utilizzare il filtro di esclusione con valore:
`$Windows$/*,$ProgramFiles$/*,/usr/*,/sbin/*,/opt/*`
- Per eseguire la scansione solo dei file di Office su computer Windows e Mac, utilizzare il filtro di inclusione con valore: `*.docx,*.doc,*.pptx,*.ppt,*.xlsx,*.xls`
- Per eseguire la scansione solo dei file di Office su computer Windows e Mac eccetto le cartelle Windows e Programmi su Windows e /usr, /sbin, /opt su Mac, utilizzare i seguenti filtri:
Filtro di inclusione con valore: `*.docx,*.doc,*.pptx,*.ppt,*.xlsx,*.xls`
Filtro di esclusione con valore: `$Windows$/*,$ProgramFiles$/*,/usr/*,/sbin/*,/opt/*`

Vedere ["Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione"](#) a pagina 2099.

Configurazione dei filtri di Endpoint Discover per includere o escludere elementi dalla scansione

I filtri di inclusione ed esclusione consentono di includere o escludere file e posizioni da una scansione di Endpoint Discover.

Per configurare i filtri di inclusione o di esclusione:

- 1 Nella console di amministrazione di Enforce Server accedere alla schermata **Gestisci > Scansione Discover > Target di Discover > Nuovo target > Endpoint > File System**.
- 2 Fare clic sul nome della scansione alla quale si desidera aggiungere i filtri di inclusione o esclusione.

3 Fare clic sulla scheda **Filtri**.

Per impostazione predefinita, nel campo **Escludi** sono visualizzati i seguenti filtri:

```
$Windows$/*,/Applications/*,/System/*/.Spotlight*,*.mp3,*.wma,*.wav,
*.vox,*.aac,*.3gp,*.dat,*.avi,*.mpeg,*.wmv,*.mov,*.mp4,*.dylib,*.jar,
*.dll,*.exe,$ProgramFiles$/*,/opt/*,/sbin/*,/bin/*,/usr/bin/*,
/Library/Manufacturer/*
```

Nota: È possibile configurare quali filtri visualizzare nel campo **Filtri di esclusione** aggiornando il file di `SymantecDLPManager` nell'host di Enforce Server.

I filtri elencati si applicano a endpoint Windows e Mac. I filtri sono solo in inglese.

- 4 Inserire nomi di file o percorsi nel campo **Filtri di inclusione** e nel campo **Filtri di esclusione** per selezionare un sottoinsieme di elementi che Symantec Data Loss Prevention deve elaborare. Delimitare le voci mediante virgole, senza spazi. Il filtro del percorso fa distinzione tra maiuscole e minuscole.

Utilizzare * (asterisco) alla fine di un percorso per includere o escludere tutto il contenuto nella cartella specificata. Ad esempio, se si immette `C:/Users/*`, `/Users/*` nel campo **Includi filtro**, tutto il contenuto della cartella `C:/Users` negli endpoint Windows e della cartella `/Users/` negli endpoint Mac OS X viene sottoposto a scansione.

I nomi di file dei filtri di inclusione e di esclusione sono relativi alla radice del file system. Specificare i percorsi completi o le sottodirectory, come necessario. È consentito l'uso di alcuni caratteri jolly.

- 5 Fare clic su **Salva**.

Vedere ["Creazione di una scansione Endpoint Discover"](#) a pagina 2089.

Vedere ["Uso dei filtri di inclusione ed esclusione"](#) a pagina 2097.

Utilizzo delle variabili di ambiente nelle scansioni Endpoint Discover

È possibile usare le variabili di ambiente per includere o escludere posizioni di file indipendentemente dalla versione di Windows supportata, dal profilo utente o dalla piattaforma dell'endpoint. Ad esempio, è possibile che si desideri creare un target Endpoint Discover che esegue la scansione della sola cartella `Programmi` in tutti gli endpoint o della sola cartella `Documenti` in tutti i profili utente di tutti gli endpoint.

Nota: Le variabili di ambiente non sono supportate per i DLP Agent eseguiti su endpoint Mac.

La [Tabella 79-8](#) elenca i tipi di variabili di ambiente utilizzabili.

Tabella 79-8 Tipi di variabile di ambiente

Tipo variabile	Elemento	Descrizione
Variabile definita dal sistema operativo	%	Utilizzare questo tipo di variabile per eseguire la scansione dei percorsi specifici del sistema operativo dell'endpoint. Ad esempio, utilizzare %TEMP% per eseguire la scansione della cartella <code>TEMP</code> su tutti gli endpoint target.
Variabile definita da Symantec Data Loss Prevention	\$	Utilizzare questa variabile per la scansione di tutti i percorsi profilo utente su un singolo endpoint. Ad esempio, utilizzare \$Documents\$ * per eseguire la scansione della cartella <code>Documenti</code> in tutti i profili utente presenti negli endpoint target.

Le variabili che includono o escludono i percorsi del profilo utente (definiti da Symantec Data Loss Prevention o dal sistema operativo) vengono risolte con tutti i profili utente presenti nell'endpoint. Se ad esempio in un endpoint esistono due profili utente e si specifica **\$Documenti\$*** nel filtro di inclusione, Symantec Data Loss Prevention esegue la scansione di `C:\Users\User1\Documenti\` e di `C:\Users\User2\Documenti`.

La [Tabella 79-9](#) elenca le variabili definite da Symantec Data Loss Prevention.

Tabella 79-9 Variabili di ambiente

Variabile definita da Symantec Data Loss Prevention	Percorso risolto per impostazione predefinita
\$CommonAdminTools\$	%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programmi\Administrative Tools
\$CommonOEMLinks\$	%ALLUSERSPROFILE%\OEM Links
\$CommonPrograms\$	%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs
\$CommonStartMenu\$	%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu
\$CommonStartup\$	%ALLUSERSPROFILE%\Microsoft\Windows\Start Menu\Programs\Startup
\$CommonTemplates\$	%ALLUSERSPROFILE%\Microsoft\Windows\Templates
\$Cookies\$	%APPDATA%\Microsoft\Windows\Cookies
\$Desktop\$	%USERPROFILE%\Desktop
\$Documents\$	%USERPROFILE%\Documents
\$Favorites\$	%USERPROFILE%\Favorites
\$Fonts\$	%WINDIR%\Fonts
\$History\$	%LOCALAPPDATA%\Microsoft\Windows\History

Variabile definita da Symantec Data Loss Prevention	Percorso risolto per impostazione predefinita
\$InternetCache\$	%LOCALAPPDATA%\Microsoft\Windows\Temporary Internet Files
\$LocalAppData\$	%LOCALAPPDATA% (o %USERPROFILE%\AppData\Local)
\$LocalizedResourcesDir\$	%WINDIR%\Resources\0409
\$Music\$	%USERPROFILE%\Music
\$NetHood\$	%APPDATA%\Microsoft\Windows\Network Shortcuts
\$Pictures\$	%USERPROFILE%\Pictures
\$PrintHood\$	%APPDATA%\Microsoft\Windows\Printer Shortcuts
\$ProgramData\$	%ProgramData% (o %SystemDrive%\ProgramData)
\$ProgramFiles\$	%ProgramFiles% (o %SystemDrive%\Program Files)
\$ProgramFilesCommon\$	%ProgramFiles%\Common Files
\$ProgramFilesCommonX64\$	%ProgramFiles%\Common Files
\$ProgramFilesCommonX86\$	%ProgramFiles%\Common Files
\$ProgramFilesX64\$	%ProgramFiles% (o %SystemDrive%\Program Files)
\$ProgramFilesX86\$	%ProgramFiles% (o %SystemDrive%\Program Files)
\$Programs\$	%APPDATA%\Microsoft\Windows\Start Menu\Programs
\$Public\$	%PUBLIC% (o %SystemDrive%\Users\Public)
\$PublicDesktop\$	%PUBLIC%\Desktop
\$PublicDocuments\$	%PUBLIC%\Documents
\$PublicDownloads\$	%PUBLIC%\Downloads
\$PublicGameTasks\$	%ALLUSERSPROFILE%\Microsoft\Windows\GameExplorer
\$PublicMusic\$	%PUBLIC%\Music
\$PublicPictures\$	%PUBLIC%\Pictures
\$PublicVideos\$	%PUBLIC%\Videos
\$Recent\$	%APPDATA%\Microsoft\Windows\Recent
\$ResourceDir\$	%WINDIR%\Resources

Variabile definita da Symantec Data Loss Prevention	Percorso risolto per impostazione predefinita
\$RoamingAppData\$	%USERPROFILE%\AppData\Roaming
\$SampleMusic\$	%PUBLIC%\Music\Sample Music
\$SamplePictures\$	%PUBLIC%\Pictures\Sample Pictures
\$SamplePlaylists\$	%PUBLIC%\Music\Sample Playlists
\$SampleVideos\$	%PUBLIC%\Videos\Sample Videos
\$SendTo\$	%APPDATA%\Microsoft\Windows\SendTo
\$StartMenu\$	%APPDATA%\Microsoft\Windows\Start Menu
\$Startup\$	%USERPROFILE%\Microsoft\Windows\Start Menu\Programmi\StartUp
\$System\$	%WINDIR%\system32
\$SystemX86\$	%WINDIR%\system32
\$Templates\$	%APPDATA%\Microsoft\Windows\Templates
\$UserProfiles\$	%SystemDrive%\Users
\$Videos\$	%USERPROFILE%\Videos
\$Windows\$	%WINDIR%

Vedere ["Esempi di filtri di inclusione"](#) a pagina 2103.

Esempi di filtri di inclusione

Nella sezione seguente viene illustrato un esempio di un filtro di inclusione di Endpoint Discover che utilizza le variabili di ambiente.

Vedere ["Utilizzo delle variabili di ambiente nelle scansioni Endpoint Discover"](#) a pagina 2100.

Tabella 79-10 Esempio di filtro di inclusione

Stringa filtro	Spiegazione
*.doc, \$Documents\$	<p>La scansione di Endpoint Discover monitora:</p> <ul style="list-style-type: none"> ■ Tutti i documenti *.doc su tutte le unità fisse associate alla scansione ■ Tutti i file nel percorso di file \Documenti\

Configurazione delle impostazioni timeout scansione di Endpoint Discover

Una scansione Endpoint Discover potrebbe non essere completata se uno o più endpoint sono disconnessi e non sono in grado di interagire con Endpoint Server. L'impostazione **Timeout inattività scansione** può essere configurata in modo da interrompere la scansione di Endpoint Discover se nessun endpoint comunica lo stato della scansione a Enforce Server per un periodo di tempo specificato.

È possibile configurare **Durata massima scansione** per definire la durata massima di esecuzione di una scansione di Endpoint Discover. Quando una scansione di Endpoint Discover supera la durata impostata in **Durata massima scansione**, la scansione di Endpoint Discover viene interrotta e visualizza lo stato di timeout.

La cronologia scansione di Endpoint Discover indica come stato scansione **Timeout**. Per accedere alla cronologia scansione, selezionare **Gestisci > Cronologia scansioni** nella console di amministrazione di Enforce Server.

Configurazione dell'impostazione Timeout inattività scansione

- 1 Individuare **Timeout inattività scansione** nella scheda delle impostazioni **Avanzate** della schermata **Gestisci > Scansione Discover > Target di Discover > Nuovo target > Endpoint > File system**.
- 2 Digitare il tempo desiderato e selezionare **Minuti** o **Ore**.

Il valore immesso deve essere superiore al valore di intervallo di polling (ServerCommunicator.CONNECT_POLLING_INTERVAL_SECONDS.int).

Vedere "[Impostazioni agente avanzate](#)" a pagina 2133.

Nota: Per disattivare **Timeout inattività scansione**, selezionare **Indefinito** per la durata.

- 3 Fare clic su **Salva** per salvare le impostazioni.

Configurazione dell'impostazione Durata massima scansione

- 1 Individuare **Durata massima scansione** nella scheda di impostazioni **Avanzate**.
- 2 Digitare il tempo desiderato e selezionare **Minuti**, **Ore** o **Giorni**.

Nota: Per disattivare **Durata massima scansione**, selezionare **Indefinito** per la durata.

- 3 Fare clic su **Salva** per salvare le impostazioni.

Gestione delle scansioni target Endpoint Discover

Dopo avere creato ed eseguito una scansione Endpoint Discover è possibile eseguire una serie di attività di gestione. Queste attività possono includere:

- Gestione delle scansioni Endpoint Discover in corso. Vedere ["Informazioni sulla gestione delle scansioni Endpoint Discover"](#) a pagina 2105.
- Riparazione degli incidenti Endpoint Discover. Vedere ["Informazioni sulla risoluzione degli incidenti Endpoint Discover"](#) a pagina 2108.
- Attivazione della memorizzazione dei risultati delle regole nella cache (RRC). Vedere ["Informazioni sulla RRC"](#) a pagina 2072.
- Creazione di report endpoint. Vedere ["Informazioni sui report endpoint"](#) a pagina 2108.

Informazioni sulla gestione delle scansioni Endpoint Discover

Per gestire i target di scansione il Endpoint Discover è possibile eseguire quanto segue:

- Avviare, interrompere e sospendere le scansioni sui target.
- Monitorare lo stato durante l'esecuzione di una scansione target.
- Selezionare i target per visualizzare i dettagli.
- Modificare o eliminare i target.
- Gestire più target.
- Ordinare e filtrare target per semplificare la gestione.
- Specificare il numero dei target da visualizzare.
- Controllare la cronologia scansioni
Vedere ["Gestione delle cronologie di scansione di Network Discover/Cloud Storage Discover"](#) a pagina 1856.
- Gestisci server
Vedere ["Gestione di server Network Discover/Cloud Storage Discover"](#) a pagina 1864.
- Controllare lo stato scansioni
 - Completato: indica che tutti i DLP Agent hanno completato correttamente la scansione.
 - Timeout: indica che uno o più DLP Agent inclusi nella scansione non hanno risposto a Endpoint Server con uno stato di scansione entro il periodo di timeout configurato.
Vedere ["Configurazione delle impostazioni timeout scansione di Endpoint Discover"](#) a pagina 2104.
 - Arrestato: indica che l'amministratore ha arrestato la scansione.
 - In esecuzione: indica che almeno un DLP Agent ha iniziato a eseguire la scansione.

- Pronto: indica che una scansione target di Endpoint Discover è configurata e pronta all'esecuzione.
- Avvio in corso: indica che la scansione è iniziata e uno o più DLP Agent potrebbero non avere ancora ricevuto i dettagli della scansione.
- In coda: indica che Endpoint Server è inattivo e la scansione rimane nello stato In coda fino a quando questo Endpoint Server torna disponibile.
- Informazioni sulle risposte alle scansioni
Vedere ["Informazioni sulla risoluzione degli incidenti Endpoint Discover"](#) a pagina 2108.
- Informazioni sull'interpretazione dei risultati e dello stato delle scansioni
Vedere ["Informazioni sui report incidente per Network Discover/Cloud Storage Discover"](#) a pagina 1610.

Informazioni sui dettagli della scansione Endpoint Discover di endpoint target

È possibile visualizzare informazioni dettagliate di ogni endpoint target di Endpoint Discover in un report di scansione, che include informazioni generali e statistiche sulla scansione. È anche possibile scaricare un report statistico della scansione in formato CSV.

Per visualizzare informazioni dettagliate su una scansione, selezionare **Gestisci > Scansione Discover > Cronologia scansioni**. Selezionare la scansione Endpoint Discover di endpoint target, quindi fare clic sul collegamento nella colonna **Stato**.

Vedere ["Informazioni sulla gestione delle scansioni Endpoint Discover"](#) a pagina 2105.

[Tabella 79-11](#) riassume i dettagli nella sezione **Generale**, che elenca informazioni sulla scansione.

Tabella 79-11 Informazioni generali su una scansione

Informazioni generali su una scansione	Descrizione
Tipo di target	Il tipo e l'icona del target che è stato sottoposto a scansione.
Nome target	Il nome del target.
Stato	Lo stato della scansione: Completato, Timeout, Arrestato o In esecuzione.
Tipo di scansione	Il tipo di scansione, come incrementale o completa.
Ora di inizio	La data e l'ora di inizio della scansione.
Ora di fine	La data e l'ora in cui la scansione è stata completata.

[Tabella 79-12](#) riassume i dettagli nella sezione **Statistiche scansione**, che fornisce informazioni dettagliate su una scansione.

Tabella 79-12 Statistiche scansione

Icona	Descrizione
Elaborato	Numero di byte analizzati tra tutti i DLP Agent inclusi nelle scansioni.
Tempo di esecuzione (gg:hh:mm:ss)	La durata della scansione. Se la scansione è ancora in corso, il contatore continua ad avanzare. Il totale non include i periodi di tempo durante i quali la scansione è stata sospesa.
Elementi sottoposti a scansione	Il numero di elementi sottoposti a scansione.
Byte sottoposti a scansione	Il numero di byte sottoposti a scansione.
Elementi filtrati	Numero di elementi filtrati quando sono stati selezionati i campi Filtri di inclusione e Filtri di esclusione .
Byte filtrati	Numero di byte filtrati quando sono stati selezionati i campi Filtri di inclusione e Filtri di esclusione .
Elementi non elaborati	Numero degli elementi che non è stato possibile sottoporre a scansione a causa di un errore di sistema.
Numero corrente di incidenti	Il numero di incidenti rilevati durante la scansione corrente, meno gli incidenti eventualmente eliminati. È possibile fare clic su questo numero per visualizzare un elenco di incidenti per questa scansione.
Agenti che avviano una scansione	Numero di DLP Agent che hanno ricevuto i dettagli di scansione e stanno cominciando a eseguire la scansione.
Agenti che eseguono scansioni	Numero di DLP Agent che stanno eseguendo la scansione.
Agenti mai segnalati	Numero di DLP Agent che non hanno mai riportato a Endpoint Server e quindi non hanno ricevuto i dettagli di scansione.
Agenti che non generano report	Numero di DLP Agent che non riportano a Endpoint Server secondo il tempo impostato nel campo Timeout inattività scansione nella scheda Avanzate nella schermata Gestisci > Scansione Discover > Target di Discover > Nuovo target > Endpoint > File system . Vedere "Creazione di un nuovo target Endpoint Discover" a pagina 2091.
Agenti completati	Numero di DLP Agent che hanno completato la scansione.
Agenti arrestati	Numero di DLP Agent che hanno arrestato la scansione.

Icona	Descrizione
Scarica report statistico completo	Scarica un report con tutte le statistiche sulla scansione in formato CSV.

Informazioni sulla risoluzione degli incidenti Endpoint Discover

Gli incidenti generati a causa di violazioni di Endpoint Discover vengono visualizzati nella scheda Discover della sezione Incidenti. Gli incidenti vengono contrassegnati con un'icona specifica di endpoint. È possibile riparare manualmente gli incidenti Endpoint Discover utilizzando le regole di risposta smart, le regole di risposta di quarantena o creare una risposta personalizzata utilizzando l'API Endpoint FlexResponse. Vedere il *Manuale per sviluppatori di plug-in di Endpoint FlexResponse di Symantec Data Loss Prevention*.

Vedere ["Informazioni sugli elenchi di incidenti endpoint"](#) a pagina 1594.

Per riparare gli incidenti Endpoint Discover è possibile utilizzare le seguenti funzionalità:

- Regole di risposta smart
Vedere ["Informazioni sulle regole di risposta automatica"](#) a pagina 1478.
- Regole di risposta di quarantena
Vedere ["Informazioni sulla quarantena di endpoint"](#) a pagina 2088.
- Endpoint FlexResponse
Vedere ["Informazioni su Endpoint FlexResponse"](#) a pagina 2248.

Vedere ["Informazioni sui report endpoint"](#) a pagina 2108.

Informazioni sui report endpoint

Utilizzare i report incidente per gestire e riparare gli incidenti sugli endpoint. Symantec Data Loss Prevention segnala un incidente quando rileva dati che corrispondono ai parametri di rilevamento di una regola di politica. Tali dati possono includere il contenuto di un file specifico, il mittente o il destinatario di un'e-mail, le proprietà di un allegato o molti altri tipi di informazioni. Ogni dato corrispondente ai parametri di rilevamento viene denominato corrispondenza e un singolo incidente può includere un numero qualsiasi di corrispondenze.

I report di Endpoint Discover sono elencati nella sezione Report Discover. Gli incidenti di Endpoint Discover vengono contrassegnati per distinguerli da altri tipi di incidenti di Discover.

I report di Endpoint Prevent sono elencati nella scheda **Report** di Enforce Server.

È possibile visualizzare i seguenti report:

- Riepilogo generale - Endpoint
- Incidenti - Tutti
- Incidenti - Nuovo

- Riepilogo politica
- Riepilogo stato
- Problemi principali

Se viene creato un incidente che include le giustificazioni dell'utente, queste sono incluse nel report nella sezione Istantanea incidente. Ad esempio, se si verifica una violazione che richiede all'utente di immettere la risposta `Errore utente`, il report incidente include il testo SPECIALE: `risposta digitata dall'utente: "Errore utente"`.

Se l'utente seleziona una giustificazione predefinita, la giustificazione appare nel report. Le giustificazioni sono visualizzate nel report dettagliato sotto l'intestazione Giustificazione.

Le giustificazioni e le notifiche non sono compatibili con Endpoint Discover, quindi nessuna giustificazione è inclusa nei report di Endpoint Discover.

È anche possibile creare report personalizzati per Endpoint Discover ed Endpoint Prevent. Tuttavia, se l'utente non è in rete nel momento in cui viene immessa la giustificazione, la sezione relativa alla giustificazione nell'istantanea incidente rimane vuota.

Vedere ["Informazioni sui report Symantec Data Loss Prevention"](#) a pagina 1632.

Vedere ["Come implementare Endpoint Prevent"](#) a pagina 2076.

Vedere ["Impostazione e configurazione di Endpoint Discover"](#) a pagina 2089.

Utilizzo delle configurazioni agente

Il capitolo contiene i seguenti argomenti:

- [Informazioni sulle configurazioni dell'agente](#)
- [Aggiunta e modifica di configurazioni agente](#)
- [Applicazione di configurazioni agente a un gruppo di agenti](#)
- [Configurazione dello stato di connessione dell'agente](#)

Informazioni sulle configurazioni dell'agente

La pagina di **Configurazione agente** sulla console di amministrazione Enforce Server consente di configurare le impostazioni dell'agente.

Ogni configurazione contiene il monitoraggio e altre opzioni per gli agenti. Queste opzioni determinano i tipi di rilevamento che possono essere utilizzati sugli endpoint. È anche possibile specificare i filtri e i limiti di consumo delle risorse. È possibile creare tutte le configurazioni agente desiderate. La protezione degli endpoint Symantec Data Loss Prevention deve contenere almeno una configurazione agente. È possibile modificare la configurazione predefinita tutte le volte che si desidera.

I gruppi di agenti possono usare solo una configurazione per volta. Tuttavia è possibile associare una configurazione di agente a più gruppi di agenti. È anche possibile clonare le configurazioni dell'agente.

Vedere ["Aggiunta e modifica di configurazioni agente"](#) a pagina 2111.

Vedere ["Informazioni sulla clonazione delle configurazioni agente"](#) a pagina 2111.

Vedere ["Visualizzazione e gestione dei gruppi di agenti"](#) a pagina 2189.

Vedere ["Applicazione di configurazioni agente a un gruppo di agenti"](#) a pagina 2179.

Informazioni sulla clonazione delle configurazioni agente

È possibile clonare le configurazioni agente. Le configurazioni clonate sono identiche a quelle da cui sono state clonate. Clonare le configurazioni agente per mantenere invariata la maggior parte dei dettagli dell'entità e apportare modifiche minime. Fare clic sull'icona di clonazione accanto all'icona di modifica per clonare una configurazione. Quando si clona una configurazione, appare una versione modificabile della configurazione clonata. È necessario rinominare la configurazione clonata per poter distinguere tra l'originale e il clone.

La pagina della configurazione agente contiene informazioni su tutte le configurazioni agente disponibili.

È anche possibile fare clic su **Aggiungi configurazione** per creare nuove configurazioni agente.

Vedere ["Aggiunta e modifica di configurazioni agente"](#) a pagina 2111.

Aggiunta e modifica di configurazioni agente

È possibile aggiungere configurazioni agente scegliendo **Sistema > Agenti > Configurazione agente** e facendo clic sul pulsante **Aggiungi configurazione**. Fare clic su una configurazione agente per modificarla.

La seguente tabella mostra le schede da utilizzare per creare o modificare configurazioni agente.

Tabella 80-1 Schede di configurazione agente disponibili

Scheda	Descrizione
Canali	Utilizzare questa scheda per selezionare gli aspetti degli elementi endpoint da monitorare. Vedere "Impostazioni di canale" a pagina 2112.
Filtri canale	Utilizzare questa scheda per creare e modificare i filtri di monitoraggio. Vedere "Impostazioni di Filtri canale" a pagina 2115.
Device Control	Utilizzare questa scheda per controllare l'accesso degli utenti endpoint ai dispositivi e le copie STAMP. Vedere "Impostazioni di Device Control" a pagina 2125.

Scheda	Descrizione
Impostazioni	<p>Utilizzare questa scheda per definire le impostazioni di comunicazione server, le risorse di monitoraggio agenti e il percorso di recupero dei file.</p> <p>Vedere "Impostazioni dell'agente" a pagina 2126.</p>
Impostazioni avanzate	<p>È anche possibile specificare impostazioni avanzate per gli agenti. Tali impostazioni hanno effetto sulle modalità con cui i Symantec DLP Agent gestiscono le informazioni, rilevano le violazioni e vengono eseguiti sugli endpoint.</p> <p>Nota: Prima di modificare impostazioni avanzate, contattare il supporto Symantec.</p> <p>Vedere "Impostazioni agente avanzate" a pagina 2133.</p>

Nota: Se si modifica una configurazione agente esistente, fare clic sul pulsante **Salva** per applicare le modifiche a tutti i gruppi di agenti associati alla configurazione. Se si crea una nuova configurazione, la configurazione viene salvata ed è possibile applicarla nella schermata **Gruppi di agenti**.

È possibile applicare impostazioni di monitoraggio specifiche se l'agente Windows è all'interno o all'esterno della rete aziendale. Vedere ["Impostazione di canali specifici da monitorare in base alla posizione dell'endpoint"](#) a pagina 2179.

Vedere ["Informazioni sull'amministrazione di Symantec Data Loss Prevention"](#) a pagina 80.

Vedere ["Configurazione di base di server"](#) a pagina 244.

Vedere ["Controlli server"](#) a pagina 242.

Vedere ["Informazioni sulle configurazioni dell'agente"](#) a pagina 2110.

Vedere ["Applicazione di configurazioni agente a un gruppo di agenti"](#) a pagina 2179.

Impostazioni di canale

Utilizzare la sezione **Attiva monitoraggio** della scheda **Canali** per selezionare gli aspetti degli elementi endpoint da monitorare.

Vedere ["Impostazioni di Attiva monitoraggio"](#) a pagina 2113.

Nota: È possibile impostare canali specifici da monitorare se l'endpoint Windows si trova all'interno o all'esterno della rete aziendale selezionando **Consenti canali diversi per endpoint che si trovano dentro e fuori la rete aziendale**. Vedere ["Impostazione di canali specifici da monitorare in base alla posizione dell'endpoint"](#) a pagina 2179.

Impostazioni di Attiva monitoraggio

Utilizzare l'area **Attiva monitoraggio** della scheda **Canali** per selezionare le applicazioni e le destinazioni endpoint (canali) da monitorare.

Nota: È possibile definire impostazioni di monitoraggio specifiche se l'endpoint Windows si trova all'interno o all'esterno della rete aziendale selezionando **Consenti monitoraggio diverso per endpoint che si trovano dentro e fuori la rete aziendale**. Vedere ["Impostazione di canali specifici da monitorare in base alla posizione dell'endpoint"](#) a pagina 2179.

Campo	Descrizione
Destinazioni	<p>Controllare le seguenti destinazioni sugli endpoint di Windows:</p> <ul style="list-style-type: none"> ■ Archivi rimovibili ■ CD/DVD ■ Unità locale ■ Stampante/Fax <p>È possibile monitorare il canale di Archivi rimovibili sugli endpoint Mac.</p>
Appunti	<p>Attivare il monitoraggio degli appunti per le operazioni di copia e incolla da e verso le applicazioni monitorate.</p> <p>Selezionare Copia per monitorare e impedire la copia dei dati negli appunti sugli endpoint Windows.</p> <p>Selezionare Incolla per monitorare e impedire la copia dei dati negli appunti sugli endpoint Mac.</p> <p>Nota: Alcune applicazioni utilizzano le operazioni di incollamento non avviate dall'utente endpoint, rischiando di provocare incidenti di falsi positivi. Symantec consiglia di verificare il comportamento dell'applicazione prima di attivare il controllo Incollamento appunti. Vedere "Funzionalità degli Appunti supportate su agenti Mac" a pagina 2051.</p> <p>È inoltre necessario confermare che l'applicazione che si desidera controllare sia stata aggiunta alla schermata Controllo applicazioni.</p> <p>Vedere "Informazioni sul controllo delle applicazioni" a pagina 2231.</p>
E-mail	<p>Selezionare le applicazioni e-mail da monitorare:</p> <ul style="list-style-type: none"> ■ Outlook su endpoint Windows e Mac ■ Lotus Notes su endpoint Windows

Campo	Descrizione
Web	<p>Selezionare le applicazioni Web da monitorare.</p> <p>È possibile monitorare il traffico sui seguenti protocolli Web:</p> <ul style="list-style-type: none"> ■ IE (HTTPS) monitora il traffico HTTPS per Internet Explorer negli endpoint Windows supportati ■ Edge (HTTPS) monitora il traffico HTTPS per Microsoft Edge negli endpoint Windows supportati ■ Firefox (HTTPS) monitora il traffico HTTPS per Firefox su endpoint Windows e Mac ■ Chrome (HTTPS) monitora il traffico HTTPS per Google Chrome sugli endpoint Windows e Mac supportati Monitorare Google Chrome in esecuzione sugli endpoint Windows in modalità Metro attivando la funzionalità Accesso ai file di applicazione. Consentire l'accesso ai file dell'applicazione passando a Controllo applicazioni > Google Chrome e confermando che Monitora accesso a file applicazione sia attivato. Vedere "Modifica delle impostazioni di controllo delle applicazioni" a pagina 2232. ■ Safari (HTTPS) monitora il traffico HTTPS per Safari su endpoint Windows e Mac. Gli utenti endpoint devono attivare l'estensione Symantec per consentire al DLP Agent di monitorare Safari. Vedere "Abilitare il monitoraggio nel browser Safari" a pagina 2115. ■ HTTP monitora il traffico HTTP per Internet Explorer, le app di Windows, Firefox e Google Chrome sugli endpoint Windows supportati ■ FTP monitora il traffico FTP, compreso traffico tramite app Windows sugli endpoint Windows supportati
Applicazioni configurate	<p>Selezionare le applicazioni da monitorare:</p> <ul style="list-style-type: none"> ■ Accesso ai file di applicazione per monitorare le applicazioni Windows e Mac configurate nella schermata Controllo applicazioni. Vedere "Informazioni sul controllo delle applicazioni" a pagina 2231. ■ Archiviazione cloud per monitorare le applicazioni archiviazione cloud Windows supportate. Vedere "Informazioni sul controllo applicazioni dell'archiviazione cloud" a pagina 2068.

Campo	Descrizione
Condivisioni di rete	<p>Selezionare per monitorare i file trasferiti a o dall'unità locale e da una condivisione di rete.</p> <p>Selezionare Copia nell'unità locale per monitorare i file spostati dalle condivisioni di rete agli endpoint Windows.</p> <p>Selezionare Copia nella condivisione per monitorare i file spostati dagli endpoint Windows e Mac alle condivisioni di rete.</p> <p>È inoltre possibile creare filtri nella configurazione agente che monitora o ignora i file per tipo, dimensione e percorso. I filtri creati si applicano a endpoint Windows e Mac. Vedere "Configurazione dei filtri di file" a pagina 2117.</p>

Abilitare il monitoraggio nel browser Safari

Gli utenti endpoint devono abilitare l'estensione Symantec per consentire a DLP Agent di monitorare Safari. Una volta che DLP Agent è stato installato su un endpoint Mac e che l'utente endpoint apre il browser Safari, viene visualizzata la finestra di dialogo **Safari: estensioni**, che ricorda agli utenti di abilitare l'estensione Symantec. Se gli utenti non attivano l'estensione e chiudono la finestra di dialogo del promemoria, è possibile impostare la schermata di promemoria in modo tale che venga visualizzata di nuovo a intervalli specifici. La durata predefinita dell'intervallo è di 10 secondi. È possibile modificare la durata dell'intervallo promemoria nella configurazione dell'agente.

Vedere ["Promemoria per attivazione dell'estensione per Safari"](#) a pagina 2127.

È possibile confermare lo stato di monitoraggio del browser Safari nella schermata **Panoramica agente**.

Vedere ["Schermata Panoramica agente"](#) a pagina 2195.

È possibile identificare gli endpoint in cui il browser Safari non è ancora abilitato nella schermata **Eventi di agente**.

Vedere ["Informazioni sugli eventi di agente"](#) a pagina 2214.

Per attivare il monitoraggio nel browser Safari

- 1 Fare clic su **OK** nella finestra di dialogo **Attiva estensione Symantec per Safari** che viene visualizzata per impostazione predefinita.
- 2 Selezionare l'estensione **Symantec** per attivare l'estensione.

Impostazioni di Filtri canale

Utilizzare la scheda **Filtri canale** per filtrare gli elementi endpoint che si desidera monitorare.

La scheda **Filtri canale** è divisa nelle seguenti sezioni:

- **Filtra per proprietà file**
 Vedere ["Impostazioni Filtra per proprietà file"](#) a pagina 2116.
- **Filtra per proprietà di rete**
 Vedere ["Impostazioni di Filtra per proprietà di rete"](#) a pagina 2121.
- **Ignora identità utente per applicazioni di archiviazione cloud**
 Vedere ["Impostazioni Ignora identità utente per applicazioni di archiviazione cloud"](#) a pagina 2124.
- **Filtra per proprietà stampante**
 Vedere ["Impostazioni di Filtra per proprietà stampante"](#) a pagina 2124.

Nota: È possibile impostare filtri specifici se l'endpoint Windows si trova all'interno o all'esterno della rete aziendale selezionando **Consenti filtri diversi per endpoint che si trovano dentro e fuori la rete aziendale**. Vedere ["Impostazione di canali specifici da monitorare in base alla posizione dell'endpoint"](#) a pagina 2179.

Impostazioni Filtra per proprietà file

Utilizzare la sezione **Filtra per proprietà file** per creare e modificare i filtri di monitoraggio. Se si utilizza questa opzione, è possibile ottimizzare le prestazioni e ridurre i falsi positivi filtrando i file prima che avvenga il rilevamento. In base ai filtri impostati, DLP Agent monitora o ignora i dati in base a protocollo, destinazione, dimensioni, tipo e percorso file. I filtri esistenti sono elencati in questa sezione. I filtri vengono eseguiti nell'ordine in cui compaiono nell'elenco, come determinato dalla colonna **Ordina**.

Nota: DLP Agent installato sugli endpoint Mac non filtra tramite una corrispondenza di firme file per tutti i tipi di file. L'agente utilizza invece l'estensione file per applicare i filtri del tipo di file. Vedere ["Filtro dall'agente Mac in base alle funzionalità delle proprietà del file"](#) a pagina 2056.

Quando si filtra in modo da ignorare i file per tipo, l'agente filtra i file in base all'estensione o alla firma dei file. Se i file che si desidera filtrare (ad esempio file `DOC`) sono contenuti in altri file (ad esempio file `ZIP`), il file che si desidera filtrare viene comunque inviato al motore di rilevazione. L'agente non estrae il contenuto dei file contenitori quali `ZIP` durante il processo di filtraggio, in modo che l'agente non possa leggere e quindi filtrare i contenuti dei file.

Quando si filtra in base al percorso dei file, la lettera dell'unità viene ignorata e viene filtrato il percorso specificato per ogni lettera di unità sull'agente. Ad esempio, se si immette `c:\temp`, `c:\temp` e `d:\temp` vengono filtrati su un agente con due unità locali.

È possibile aggiungere o modificare i filtri:

- Per creare un nuovo filtro, fare clic su **Aggiungi filtro monitoraggio**.

- Per modificare un filtro esistente, fare clic sul filtro nell'elenco.
- Per cancellare un filtro esistente, fare clic sulla "X" rossa corrispondente.
- Per cambiare l'ordine in cui viene applicato un filtro, fare clic sul numero del filtro nella colonna **Ordina**. Quindi selezionare l'ordine di esecuzione per tale filtro nell'elenco a discesa. Le modifiche vengono applicate dopo avere fatto clic su **Salva** nella parte superiore dello schermo.
- Scegliere **Controlla** o **Ignora** per specificare cosa fare con i file che non corrispondono ad alcun filtro nella sezione **Filtra per proprietà di rete**.

Vedere ["Configurazione dei filtri di file"](#) a pagina 2117.

Configurazione dei filtri di file

È possibile configurare DLP Agent per monitorare specifici tipi di file, applicazioni, protocolli o posizioni. La configurazione di questi elementi consente di migliorare potenzialmente le prestazioni di monitoraggio. Configurare DLP Agent in **Sistema > Agenti > Configurazione agente**. Selezionare quindi una configurazione agente e fare clic su **Aggiungi filtro monitoraggio**.

La pagina **Configura server - Filtro file** include le seguenti tre sezioni:

- **Operazione filtro**
- **Canale endpoint**
- **Attributi file**

La sezione **Operazione filtro** consente di determinare se il filtro deve monitorare o meno gli attributi seguenti. È possibile includere file da monitorare o escludere file dal protocollo o dalla destinazione pertinente.

È possibile selezionare una delle opzioni seguenti:

- **Monitora**
- **Ignora** (non eseguire il monitoraggio)

Nella sezione **Canale endpoint** è possibile selezionare destinazioni, protocolli o applicazioni che si desidera filtrare. Selezionare almeno un'opzione. Selezionare gli elementi che Endpoint Server deve monitorare.

È possibile scegliere uno dei seguenti elementi:

Destinazioni

Archivi rimovibili

CD/DVD

Unità locale

Protocolli

Allegato e-mail

Allegato HTTP/HTTPS

Trasferimento file IM

Nota: Questa impostazione è applicabile solo a DLP Agent versione 14.0.x e precedenti.

Trasferimento FTP

Applicazioni configurate

Accesso ai file di applicazione

Archiviazione cloud

Condivisioni di rete

Copia nell'unità locale

Copia nella condivisione

L'opzione Accesso ai file di applicazione consente di monitorare qualsiasi applicazione visualizzata nella pagina Controllo applicazioni.

Vedere ["Informazioni sul controllo delle applicazioni"](#) a pagina 2231.

Nella sezione **Attributi file** è possibile specificare i filtri da applicare. Le informazioni immesse in questa sezione sono valide per il monitoraggio dell'accesso ai file di applicazione e all'unità locale. Selezionare **Unità locale** o **Accesso ai file di applicazione** per modificare il campo **Percorso file nella destinazione**.

È possibile specificare i seguenti attributi di filtro:

- **Dimensione**
 È possibile specificare una dimensione minima, massima o di base dei file che si desidera sottoporre a scansione.
- **Tipo**
 Specificare i tipi di file esatti che si desidera filtrare. Questa sezione è precaricata con tipi di file comuni. Se si specificano tipi di file supplementari, immettere ogni tipo di file su una riga distinta.
 Vedere ["Filtraggio tipo file true"](#) a pagina 2120.
- **Percorso file nella destinazione**
 Specificare i percorsi del file system da analizzare. Immettere un percorso per riga. Se si specificano dei percorsi da includere, Symantec Data Loss Prevention monitora solo i file in quei percorsi. Se si lascia vuoto questo campo, Symantec Data Loss Prevention monitora tutti i file eccetto quelli eventualmente specificati altrove. Questo filtro viene utilizzato per il monitoraggio dell'unità locale, il controllo dell'applicazione di archiviazione cloud, l'accesso ai file di applicazione e la copia su condivisioni e unità locali. È possibile usare le variabili di ambiente per includere o escludere posizioni di file indipendentemente dal profilo utente o dalla piattaforma dell'endpoint. Ad esempio, se si immette:

\$PublicDownloads\$

%TEMP%

C:\test*

Symantec Data Loss Prevention esegue la scansione della cartella di download in tutti i profili utenti, nella cartella Temp e nella cartella Test.

Vedere ["Utilizzo delle variabili di ambiente nelle scansioni Endpoint Discover"](#) a pagina 2100.

I filtri di monitoraggio dell'endpoint vengono eseguiti sempre nell'ordine in cui sono visualizzati. Se si desidera modificare l'ordine di esecuzione dei filtri, contattare il supporto Symantec. La modifica dell'ordine dei filtri di monitoraggio dell'endpoint può comportare l'arresto del monitoraggio delle informazioni riservate da parte degli agenti.

Vedere ["Informazioni sulle configurazioni dell'agente"](#) a pagina 2110.

Configurazione di filtri di condivisione di rete

Il seguente contenuto fornisce un elenco dei percorsi di rete che è possibile utilizzare per filtrare copie di file su condivisioni di rete e copie di file da condivisioni di rete su unità locali. I filtri che si utilizzano per monitorare copie di condivisioni di rete sono validi quando vengono utilizzati con altri canali di monitoraggio, pertanto è necessario crearli separatamente.

Come linea guida generale, i filtri di percorso devono iniziare con \\ e terminare con *.

Aggiungere ogni filtro a una nuova riga nel campo. Se si separano i filtri utilizzando delle virgole [,] o dei punti e virgola [;], il sistema ignora il filtro.

I seguenti caratteri invalidano i filtri:

- Punti interrogativi [?]
- Barre dritte [/]
- Doppie barre dritte [//]
- Doppie barre rovesciate [\\]
Le doppie barre rovesciate possono essere utilizzate solo all'inizio del percorso.
- Minore di [<]
- Maggiore di [>]
- Barra verticale [[]]
- Virgolette [""]

Tabella 80-2 Dettagli del percorso di condivisione di rete

Condivisione di rete	Descrizione	Percorsi validi	Caratteri e percorsi non validi
Generale	Per filtri basati su IP, è possibile utilizzare percorsi e asterischi [*] per la corrispondenza con caratteri jolly. Aggiungere un asterisco per ogni otetto. I percorsi specificati nel formato UNC di Windows vengono gestiti automaticamente per gli endpoint Mac.	Filtro basato su IP: \\10.211.*.*\path\ Filtro unità condivisa specifico (in questo caso l'unità c):\\10.211.*.*\c\$\	\\10.211.*.*\path** \\10.211.*.*\path/* //10.211.*.*\path/* \\10.211.201.*\path\
Condivisione RDP	I percorsi devono iniziare con \\rdp,\\RDP o \\tsclient.	\\rdp\e\ \\RDP\c\testshare\ \\tsclient\e\sharedPath\	\\rdp*
WebDAV	Le condivisioni basate sul Web sono accessibili dai browser e dai file system. Ad esempio, le condivisioni di SharePoint possono essere installate su unità. In queste istanze, la porzione <i>DavWWWRoot</i> non è visibile in Windows Explorer, ma è necessario aggiungere questa stringa ai percorsi per eseguire il filtraggio per il protocollo WebDAV.	\\10.211.*.*\DavWWWRoot\	\\10.211.*.**

Filtraggio tipo file true

Il DLP Agent per Windows può filtrare tipi specifici di file da monitorare in base ai dati di firma del file, noti anche come tipo file true. I dati della firma del file, di norma una breve sequenza di byte all'inizio del file, vengono utilizzati per identificare o verificare il tipo di file.

Nota: Il filtraggio in DLP Agent per Mac utilizza solo l'estensione del file; il filtraggio del vero tipo di file non è supportato per DLP Agent per Mac.

Poiché il DLP Agent per Windows può filtrare in base al tipo di file true, l'agente è in grado di identificare e filtrare correttamente i file con estensione non corrispondente al file originale. Ad esempio, se un utente modifica il nome dell'estensione del file .doc in .jpg, l'agente può identificare il file in base alla sua firma come file doc e monitorarlo o ignorarlo in base al filtro di configurazione dell'agente.

Nota: I file di testo (.txt) non contengono i dati della firma del file; di conseguenza, l'agente può solamente monitorare o ignorare questi tipi di file in base all'estensione del file. Il filtraggio del tipo true non è possibile per i file TXT.

Vedere ["Impostazioni Filtra per proprietà file"](#) a pagina 2116.

Tabella 80-3 elenca i tipi di file e le estensioni corrispondenti che il DLP Agent per Windows può filtrare utilizzando il filtraggio del tipo di file true.

Tabella 80-3 File supportati per il filtraggio del tipo di file true su endpoint Windows

Tipo di file	Estensioni file filtrate
Adobe Acrobat	.pdf
Microsoft Office	.doc, .dot, .pps, .ppt, .xla, .xls, .wiz, .db, .msc, .msi, .mtw, .spo, .vsd, .wps, .pub
Office Open XML	.docx, .pptx, .xlsx, .dotx, .potx
OpenOffice	.odt, .ott, .ods, .odp, .otp, .ots, .odg, .otg
OpenOffice (creato utilizzando Microsoft Office)	.odt, .odp, .ods
ZIP e PKZIP	.zip, .jar, .xpi
StarOffice	.stw, .sxw, .sxc, .sxi, .sti, .stc, .std, .sxd
Archivio RAR	.rar
Symantec Information Centric Encryption (ICE)	.ice Nota: I file con crittografia ICE hanno l'estensione .html. Tuttavia, se si imposta il filtro dei file su .html, DLP Agent monitora o ignora sia i file con crittografia ICE sia i normali file HTML. Per monitorare o ignorare solo i file con crittografia ICE, impostare il filtro dei file su .ice. L'estensione .ice è la pseudo estensione dei file HTML con crittografia ICE.

Impostazioni di Filtra per proprietà di rete

È possibile utilizzare la sezione **Filtra per proprietà di rete** per creare filtri associati alla rete che indicano all'agente di monitorare o ignorare traffico in base all'indirizzo IP o al dominio. Immettere gli indirizzi IP, i domini HTTP, i domini FTP e i domini HTTPS che si desidera filtrare nella casella appropriata.

Vedere ["Filtro dall'agente Mac in base alle funzionalità delle proprietà del rete"](#) a pagina 2057.

Filtraggio di indirizzi IP

È possibile filtrare solo indirizzi IP su endpoint Windows. Per il filtraggio di indirizzi IP, utilizzare le seguenti regole. Immettere tutti i filtri basati su IP che si desidera utilizzare. Se si lascia vuoto questo campo, Symantec Data Loss Prevention ispeziona tutti i pacchetti. Il formato dei filtri di protocollo IP (trovato nelle definizioni di protocollo e nelle definizioni dei filtri di protocollo) è il seguente:

```
ip_protocol_filter                := protocol_filter_multiple_entries [; *]
protocol_filter_multiple_entries := protocol_filter_entry
                                [; protocol_filter_multiple_entries]
protocol_filter_entry             := +|- , destination_subnet_description,
                                source_subnet_description
destination_subnet_description    := subnet_description
source_subnet_description         := subnet_description
subnet_description               := network_ip_address / bitmask
                                | *
```

Nota: Separare ogni voce con una virgola per monitorare o ignorare correttamente gli elementi specificati.

Ogni flusso viene valutato in ordine rispetto alle voci di filtro finché una voce non corrisponde ai parametri IP del flusso.

Un segno meno (-) all'inizio della voce indica che il flusso viene scartato. Un segno più (+) all'inizio della voce indica che il flusso viene mantenuto.

Una descrizione di rete subnet di * significa che qualsiasi pacchetto corrisponde a questa voce.

Una maschera di bit di subnet di 32 significa che la voce deve corrispondere all'indirizzo di rete esatto. Ad esempio, un filtro di +, 10.67.0.0/16, *, -, *, * cerca la corrispondenza con tutti i flussi che riguardano la rete 10.67.x.x ma non cerca la corrispondenza con alcun altro traffico.

Nota: Più si è specifici quando si definiscono le caratteristiche di riconoscimento, più specifici sono i risultati. Ad esempio, se si definisce solo un indirizzo IP specifico, vengono acquisiti solo gli incidenti che hanno coinvolto tale indirizzo IP. Se non si definisce alcun indirizzo IP o se si definisce un ampio intervallo di indirizzi IP, si ottengono risultati più vasti. Includere almeno una clausola segno più (+) e una clausola segno meno (-) per specificare esplicitamente cosa è incluso e cosa è escluso.

Filtraggio di domini

I filtri di domini devono essere applicati separatamente per HTTP e HTTPS. Per aggiungere filtri per un qualsiasi sito Web che supporta HTTP e HTTPS, aggiungere singoli filtri per HTTP e HTTPS nelle rispettive caselle di testo. Il filtro di indirizzi IP funziona con tutti gli altri protocolli di rete.

Nota: È possibile utilizzare filtri HTTP e HTTPS per monitorare e ignorare domini per browser su endpoint Windows e Mac. Vedere ["Impostazioni di Attiva monitoraggio"](#) a pagina 2113.

Per il filtraggio di nomi di domini HTTP/HTTPS, utilizzare le seguenti regole:

È possibile utilizzare filtri per includere (ispezionare) o escludere (ignorare) messaggi da mittenti specifici. È anche possibile utilizzare filtri per includere o escludere destinatari specifici. La sintassi di filtro specifica dipende dal protocollo.

Il seguente è un esempio di filtri di domini

```
Domain Filter      := <Domain Filter Entry> [,<Domain Filter Entry>]  
Domain Filter Entry := {*|{-|+}<metadata value>}
```

È possibile utilizzare i seguente simboli:

- Nella voce di dominio è possibile utilizzare il simbolo carattere jolly (*).
Ad esempio, *symantec.com ricerca la corrispondenza di www.symantec.com, www.dlp.symantec.com e tutti i domini che terminano con symantec.com.
- Un segno meno (-) all'inizio della voce indica che l'URL viene ignorato.
- Un segno più (+) all'inizio dell'entrata indica che URL è ispezionato.
- Se si aggiunge un asterisco (*) alla fine dell'espressione del filtro, tutti i domini URL che non corrispondono esplicitamente a una delle maschere di filtro vengono ignorati.

Questi filtri vengono eseguiti da sinistra a destra finché non viene individuata la prima corrispondenza o l'agente non raggiunge il termine delle voci di filtro.

Ad esempio, se il filtro è il seguente:

```
-sales.symantec.com, +*symantec.com, *
```

Le richieste HTTP in sales.symantec.com vengono ignorate e tutte le richieste che vengono inviate su qualsiasi altro dominio di symantec.com vengono sottoposte a ispezione. L'ultimo asterisco nel filtro esclude tramite filtraggio tutti gli altri domini come www.xyz.com.

Nota: Se si lascia vuoto il filtro HTTP/HTTPS, tutti gli URL vengono ispezionati.

Impostazioni Ignora identità utente per applicazioni di archiviazione cloud

Utilizzare la sezione **Ignora identità utente per applicazioni di archiviazione cloud** per specificare gli account cloud aziendali approvati per i caricamenti di file riservati.

L'aggiunta di informazioni sugli account cloud aziendali impedisce agli utenti di caricare file riservati negli account Box personali. DLP Agent monitora e impedisce i caricamenti di questi tipi di file tramite l'applicazione Box Sync e il componente aggiuntivo Box for Office.

Nota: i file riservati vengono spostati nella posizione di recupero dei file e rimangono lì finché gli utenti endpoint non li eliminano. Vedere ["Impostazioni posizione area di recupero dei file"](#) a pagina 2129.

Per attivare questa funzionalità:

- 1 Assicurarsi che il canale **Archiviazione cloud** nella configurazione dell'agente sia attivato.
- 2 Immettere gli account di archiviazione cloud da escludere dal monitoraggio nella configurazione dell'agente.

Ad esempio immettere *mario_rossi@azienda.com* per ignorare l'account utente *mario_rossi* nel dominio *azienda.com*. È possibile immettere un carattere jolly (*) per specificare un dominio degli account di archiviazione cloud da ignorare. Ad esempio immettere **@azienda.com* per ignorare tutti gli account di archiviazione cloud con *azienda.com* nel dominio.

Nota: Aggiungere più account di archiviazione cloud da ignorare aggiungendoli in nuove righe nel campo **Ignora identità utente per applicazioni di archiviazione Cloud**.

Impostazioni di Filtra per proprietà stampante

Utilizzare la sezione **Filtra per proprietà stampante** per specificare le stampanti approvate per i caricamenti di file riservati. È possibile impostare DLP Agent per ignorare le stampanti locali, le stampanti PDF e le stampanti di rete. È possibile usare un carattere jolly (*) per ignorare una serie di stampanti.

L'aggiunta di stampanti approvate impedisce agli utenti di stampare informazioni riservate con stampanti personali o non approvate.

Nota: Aggiungere più stampanti da ignorare aggiungendole alle nuove righe nel campo **Filtra per proprietà stampante**. Non utilizzare virgola [,] o punto e virgola [;] per separare più stampanti; questi separatori impediscono il filtraggio delle stampanti.

Specifica delle stampanti locali da ignorare

Immettere il nome della stampante locale da ignorare. Ad esempio, per ignorare solo una stampante chiamata *HP Color LaserJet CP4020*, immettere **HP Color LaserJet CP4020**. Per ignorare i documenti stampati XPS, immettere **Microsoft XPS Document Writer**.

È possibile ignorare una serie di stampanti utilizzando un carattere jolly [*] nel filtro di stampa. Ad esempio, immettere **HP Color LaserJet*** per ignorare tutte le stampanti con il prefisso *HP Color LaserJet*.

Nota: Per ignorare una stampante con un asterisco [*] nel nome, è necessario inserire un carattere di escape dopo l'asterisco nel filtro. Ad esempio, se il nome di stampante è *Nome*Stampante*, immettere **Nome*\Stampante**.

Specifica delle stampanti PDF da ignorare

È possibile immettere il nome della stampante PDF particolare che si desidera ignorare. Ad esempio, immettere **Microsoft Print to PDF** per ignorare i dati stampati dalle applicazioni Microsoft Office. È possibile ignorare i dati inviati a tutte le stampanti con PDF nel nome immettendo ***PDF***.

Specifica delle stampanti di rete

Per ignorare le stampanti di rete immettere il nome della rete e il nome della stampante. Ad esempio, immettere **\\printserver\HP Color LaserJet CP4020** per ignorare la stampante HP Color LaserJet CP4020 situata sul server chiamato *printserver*.

È possibile ignorare una serie di stampanti di rete utilizzando un carattere jolly [*] nel filtro di stampa.

Di seguito vengono forniti alcuni esempi di filtri per le stampanti di rete:

- **\\printerserver2\HP Color LaserJet CP4020*** ignora tutte le stampanti che iniziano con *HP Color LaserJet CP4020* ospitato su *printerserver2*.
- **\\printerserver*\HP Color LaserJet CP4020*** ignora tutte le stampanti che iniziano con *HP Color LaserJet CP4020* ospitate su tutti i server con il prefisso *printerserver*.

Impostazioni di Device Control

Utilizzare la scheda **Device Control** per impostare il livello di accesso degli utenti endpoint di Windows alle condivisioni di rete e ai dispositivi di archiviazione USB. L'accesso può essere impostato come bloccato e di sola lettura. È inoltre possibile utilizzare la scheda per bloccare le copie STAMP.

Nota: È possibile impostare diverse configurazioni di accesso se l'endpoint Windows si trova all'interno o all'esterno della rete aziendale. Selezionare **Consenti controlli dispositivo diversi per endpoint che si trovano dentro e fuori la rete aziendale**. Vedere ["Impostazione di canali specifici da monitorare in base alla posizione dell'endpoint"](#) a pagina 2179.

La scheda **Device Control** fornisce i seguenti comandi:

- **Archiviazione USB**

È possibile impostare l'agente per bloccare soltanto o per consentire l'accesso in sola lettura ai dispositivi di archiviazione USB. Altri dispositivi di archiviazione non USB (ad esempio unità eSATA, dispositivi MTP e hard disk virtuali [VHD]) non sono controllati.

- **Condivisioni di rete**

È possibile impostare l'agente per bloccare soltanto o per consentire l'accesso in sola lettura alle condivisioni di rete.

- **Blocca STAMP**

È possibile selezionare questo elemento per impedire agli utenti endpoint di copiare le schermate utilizzando il tasto STAMP o quando premono la combinazione di tasti [MAIUSC + STAMP]. L'attivazione di **Blocca STAMP** si applica agli endpoint Windows 7, 8 e 10, ma non agli endpoint in esecuzione negli ambienti virtuali.

Se si imposta l'accesso a un dispositivo e un utente endpoint supera i limiti di accesso, l'agente impone l'accesso e viene visualizzato un pop-up nell'endpoint. Il pop-up informa l'utente che l'accesso al dispositivo è limitato. Il pop-up viene visualizzato la prima volta che l'utente endpoint supera i limiti di accesso, ma non per le violazioni successive.

Impostazioni dell'agente

La scheda **Impostazioni** è divisa nelle seguenti sezioni:

- **Comunicazione server**

Vedere ["Impostazioni di comunicazione del server"](#) a pagina 2127.

- **Attivazione estensione Safari**

Vedere ["Promemoria per attivazione dell'estensione per Safari"](#) a pagina 2127.

- **Utilizzo delle risorse a livello dell'host endpoint**

Vedere ["Impostazioni di Utilizzo delle risorse a livello dell'host endpoint"](#) a pagina 2127.

- **Utilizzo delle risorse per le scansioni Endpoint Discover**

Vedere ["Impostazioni di Utilizzo delle risorse per le scansioni Endpoint Discover"](#) a pagina 2128.

- **Posizione area di recupero dei file**

Vedere ["Impostazioni posizione area di recupero dei file"](#) a pagina 2129.

- **Modalità provvisoria**

Vedere ["Impostazioni modalità provvisoria"](#) a pagina 2131.

- **Archiviazione cloud**

Vedere ["Impostazioni di archiviazione cloud"](#) a pagina 2131.

- **Stampante/Fax**

Vedere ["Impostazioni della stampante/fax"](#) a pagina 2132.

- **Crittografia incentrata sulle informazioni**

Vedere ["Impostazioni di Crittografia incentrata sulle informazioni per i DLP Agent"](#) a pagina 2133.

Impostazioni di comunicazione del server

Utilizzare la sezione **Comunicazione server** per impostare la quantità massima di larghezza di banda (in megabit o kilobit al secondo) che DLP Agent può usare per caricare i dati in e scaricare i dati da Endpoint Server durante il periodo di connessione.

Vedere ["Informazioni su DLP Agent Store"](#) a pagina 2129.

L'impostazione predefinita dell'accelerazione di consumo è 5 Mbps. Per modificare l'accelerazione della larghezza di banda, selezionare Mbps o Kbps, quindi immettere un numero nella casella per il massimo al secondo. Se si lascia un campo vuoto, non viene applicata alcuna accelerazione per la direzione del traffico di comunicazione.

Campo	Descrizione
Regolazione da agente	Velocità massima a cui DLP Agent carica gli incidenti, lo stato e gli eventi su Endpoint Server.
Regolazione verso agente	Velocità massima a cui DLP Agent scarica gli aggiornamenti delle politiche e delle configurazioni dell'agente da Endpoint Server.

Promemoria per attivazione dell'estensione per Safari

L'impostazione **Promemoria per attivazione dell'estensione per Safari** consente di impostare la frequenza di visualizzazione della finestra di dialogo che ricorda agli utenti di endpoint di attivare l'estensione Symantec. Gli utenti di endpoint devono attivare l'estensione per abilitare il monitoraggio di Safari.

Vedere ["Abilitare il monitoraggio nel browser Safari"](#) a pagina 2115.

Impostazioni di Utilizzo delle risorse a livello dell'host endpoint

Utilizzare la sezione **Utilizzo delle risorse a livello dell'host endpoint** per impostare lo spazio su disco massimo per **Dimensioni Agent Store**. DLP Agent utilizza Agent Store per archiviare temporaneamente incidenti e altri dati su ciascun host di endpoint.

Vedere ["Informazioni su DLP Agent Store"](#) a pagina 2129.

È possibile specificare una percentuale dell'unità disco rigido o un limite di archiviazione. Fare clic sul pulsante di opzione appropriato per scegliere una percentuale dello spazio su disco o un limite di archiviazione.

Campo	Descrizione
Limite % spazio totale su disco	Per la percentuale, immettere la cifra nella casella corrispondente. La percentuale predefinita è il 5% dello spazio su disco totale.
Limite assoluto di dimensione dello spazio su disco	Selezionare il pulsante di opzione per questa opzione, immettere la dimensione specifica nel campo e scegliere l'unità di misura dall'elenco a discesa (byte, KB, MB o GB).

Impostazioni di Utilizzo delle risorse per le scansioni Endpoint Discover

Utilizzare la sezione **Utilizzo delle risorse per le scansioni Endpoint Discover** per gestire le risorse quando Endpoint Discover esegue la scansione di endpoint.

Nota: Le funzionalità di utilizzo medio della CPU a lungo termine e di durata della batteria minima rimanente non sono attualmente supportate per gli agenti in esecuzione su endpoint Mac.

Campo	Descrizione
Utilizzo medio della CPU a lungo termine	<p>Specificare la percentuale media massima delle risorse della CPU che possono essere utilizzate per scansioni di rilevamento in un determinato periodo. Se Symantec DLP Agent supera questo limite CPU massimo, il rilevamento di Endpoint Discover termina, ma quello di Endpoint Protect continua normalmente. Il valore predefinito è 20%.</p> <p>Nota: Qualsiasi modifica applicata alla soglia delle risorse della CPU deve entrare in vigore immediatamente. Se si applica una modifica durante una scansione, essa entra in vigore dopo che l'agente ha ripreso la scansione.</p>

Campo	Descrizione
Durata minima rimanente della batteria	Specificare una quantità minima della batteria necessaria per eseguire gli agenti. Se il livello della batteria scende al di sotto di questo minimo, la rilevazione di Endpoint Discover si arresta, ma quella di Endpoint Protect funziona normalmente. Il valore predefinito è 30%.

Informazioni su DLP Agent Store

Quando DLP Agent non è collegato a Endpoint Server, archivia temporaneamente gli incidenti, le richieste di rilevamento in due fasi e le azioni di risposta localmente sull'host endpoint. DLP Agent archivia i metadati di incidenti e rilevamento e i dati e i metadati delle azioni di risposta in un piccolo database crittografato installato con DLP Agent. DLP Agent archivia i dati degli incidenti e il contenuto per le richieste di rilevamento in due fasi sul file system dell'host endpoint. Questi dati sono crittografati e la chiave di crittografia si trova nel database dell'agente.

Il parametro **Dimensioni Agent Store** limita la quantità di dati che DLP Agent archivia sull'host endpoint. La dimensione predefinita dell'Agent Store è il 5% dello spazio su disco totale. Alternativamente, è possibile impostare un limite di archiviazione assoluto. Il limite indicato in **Dimensioni Agent Store** si applica a tutti i dati archiviati sull'host endpoint, inclusi i dati nel database dell'agente e quelli archiviati nel file system dell'host.

Se il limite indicato in **Dimensioni Agent Store** viene oltrepassato, DLP Agent elimina i dati dall'host endpoint secondo una priorità definita fino a che la dimensione è di nuovo inferiore al limite in **Dimensioni Agent Store**. Se DLP Agent deve eliminare incidenti, l'ordine di eliminazione è il seguente:

- 1) Dati delle richieste di rilevamento in due fasi (dapprima i meno recenti)
- 2) Incidenti di Endpoint Discover (dapprima i meno recenti)
- 3) Incidenti di Endpoint Prevent (dapprima i meno recenti)

Vedere ["Aggiunta e modifica di configurazioni agente"](#) a pagina 2111.

Impostazioni posizione area di recupero dei file

Utilizzare la sezione **Posizione area di recupero dei file** per specificare i parametri di recupero dei file. La posizione di recupero dei file è il punto in cui vengono archiviate le copie dei dati di cui il DLP Agent ha bloccato il trasferimento. Queste copie vengono conservate fino al recupero da parte dell'utente, oppure eliminate automaticamente dopo un certo periodo di tempo.

Nota: I file recuperati dagli incidenti dell'applicazione di sincronizzazione cloud non vengono rimossi dall'endpoint.

Campo	Descrizione
Posizione area di recupero dei file	<p>Specificare il percorso della directory di recupero dei file. Il valore predefinito per gli endpoint Windows è <code>%USERPROFILE%\File recuperati</code>.</p> <p>Il percorso di recupero dei file per gli endpoint Mac è <code>\$HOME/File recuperati</code>. Si tratta di un percorso fisso. Vedere "Recupero dei file riservati negli endpoint Mac" a pagina 2130.</p>
Tempo rimanente alla scadenza	<p>Specificare il lasso di tempo prima che i file vengano automaticamente cancellati dalla cartella di recupero dei file. Il valore predefinito è di 48 ore.</p>

Recupero dei file riservati negli endpoint Mac

Quando una regola di risposta di blocco è implementata in una politica e un file riservato è spostato da un endpoint Mac in un dispositivo endpoint, Symantec Data Loss Prevention sposta il file in un percorso locale nell'endpoint. Il percorso è fisso, in questo modo l'utente endpoint non può modificarlo e il percorso non può essere modificato dalla console di amministrazione Enforce Server.

La posizione del file Mac è `$HOME/File recuperati`, dove `$HOME` corrisponde alla directory della pagina iniziale dell'utente endpoint.

I file recuperati sono separati per cartella. Ogni cartella è nominata secondo l'applicazione in cui il file è stato spostato. Inoltre, un file `ReadMe.txt` è creato nella stessa cartella da cui è stato spostato il file riservato. Questo file indica dove si trovava il file originariamente. Ad esempio, se un utente tenta di utilizzare TextEdit per salvare un file riservato in un dispositivo di archiviazione rimovibile collegato a un endpoint Mac, Symantec Data Loss Prevention sposta il file nel percorso `$HOME/File recuperati /TextEdit` e crea un file `ReadMe.txt` con informazioni sul file originali.

Il recupero occasionale dei file non riesce. Questo accade se le autorizzazioni per la cartella di recupero sono state modificate o se l'autenticazione utente non è riuscita. In questo caso, Symantec Data Loss Prevention sposta il file riservato nella cartella della directory principale `/File recuperati alternativi` tramite un account con privilegi elevati per garantire il recupero dei file senza la loro eliminazione.

Gli utenti endpoint possono recuperare file riservati da entrambe le posizioni (`$HOME/File recuperati` e cartella della directory principale `/File recuperati alternativi`), nonché recuperare file eliminati. Symantec Data Loss Prevention elimina file in diverse situazioni. Se un utente copia un file riservato dall'endpoint in un dispositivo rimovibile tramite l'operazione di taglio, il file viene eliminato. Per recuperare il file, l'utente deve individuarlo nella posizione

di recupero e spostarlo nella posizione originale. Inoltre, un file riservato in un dispositivo rimovibile viene eliminato quando le informazioni riservate vi vengono aggiunte e il file viene salvato. In questo caso, l'operazione di salvataggio viene bloccata e il file eliminato. Gli utenti endpoint possono recuperare il file in `$HOME/File recuperati`.

Impostazioni modalità provvisoria

È possibile utilizzare la sezione **Modalità provvisoria** per attivare o disattivare il monitoraggio degli endpoint Windows in esecuzione in modalità provvisoria. Questa impostazione è attivata per impostazione predefinita.

Una volta attivata, questa impostazione indica al DLP Agent di monitorare gli endpoint Windows in esecuzione nei seguenti tipi di modalità provvisoria:

- Modalità provvisoria
- Modalità provvisoria con rete
- Modalità provvisoria con prompt dei comandi

Se l'endpoint è in esecuzione in modalità provvisoria o in modalità provvisoria con prompt dei comandi, la comunicazione tra il DLP Agent e l'Endpoint Server si arresta. Ciò significa, ad esempio, che gli incidenti non vengono inviati all'Endpoint Server e alle configurazioni non vengono inviati all'agente. La comunicazione riprende quando l'agente viene riavviato in modalità normale o modalità provvisoria con rete.

Impostazioni di archiviazione cloud

È possibile utilizzare la sezione **Archiviazione cloud** per attivare il monitoraggio dell'archiviazione cloud per file salvati da Microsoft Office in posizioni cloud e Web. Questa impostazione è attivata per impostazione predefinita.

Vedere ["Informazioni sul controllo applicazioni dell'archiviazione cloud"](#) a pagina 2068.

Quando l'impostazione è attivata, vengono monitorati anche i file caricati da applicazioni Microsoft Office in Box tramite il componente aggiuntivo Box for Office.

Utilizzare i filtri IP per identificare le condivisioni di WebDAV da escludere o includere nel monitoraggio. Immettere i filtri nell'area **Filtri IP** della scheda **Filtri canale** nella configurazione dell'agente.

Utilizzare i filtri di dominio per monitorare o ignorare i file salvati in condivisioni di WebDAV, in SharePoint o in posizioni di archiviazione cloud. Immettere i filtri nell'area **Filtri di dominio** della scheda **Filtri canale** nella configurazione dell'agente.

Vedere ["Impostazioni di Filtra per proprietà di rete"](#) a pagina 2121.

Nota: I filtri non si applicano alle applicazioni di sincronizzazione cloud.

Tabella 80-4 elenca le voci di esempio utilizzate per filtrare i dati salvati dalle applicazioni Microsoft Office in posizioni cloud (dominio) e Web (IP).

Tabella 80-4 Filtraggio delle posizioni cloud e Web

Destinazione	Esempio	Risultato
Dominio	<i>-*syndlp-my.sharepoint.com*</i>	L'agente ignora i file salvati in SharePoint (con il dominio <i>syndlp-my.sharepoint.com</i>).
	<i>+*inc-powerpoint.officeapps*,*</i>	L'agente monitora i file salvati negli URL con il dominio <i>inc-powerpoint.officeapps</i> e ignora tutti gli altri URL.
IP	<i>-,10.211.203.251/16,*;+,*,*</i>	L'agente ignora tutti i file spostati verso destinazioni che corrispondono all'indirizzo IP <i>10.211.x.x</i> .

Vedere ["Informazioni sul controllo applicazioni dell'archiviazione cloud"](#) a pagina 2068.

Impostazioni della stampante/fax

È possibile impostare i DLP Agent per monitorare i dati inviati dalle applicazioni Microsoft Office a una stampante. Se sono presenti dati riservati nel file di stampa, l'agente può arrestare il processo di stampa nella pagina che contiene i dati riservati o impedire la stampa dell'intero documento.

Selezionare una delle opzioni seguenti nell'area di **Stampante/fax**.

■ **Monitora solo le pagine stampate/inviata via fax**

L'impostazione predefinita monitora i dati stampati e inviati via fax nella sequenza pagina per pagina. Se l'agente rileva dati riservati, blocca il processo di stampa nella pagina in cui si trovano i dati riservati, nonché le pagine successive. Ad esempio, se un utente endpoint stampa un documento di 10 pagine e i dati riservati si trovano nella pagina 9, l'agente consente la stampa delle pagine 1-8 e impedisce la stampa delle pagine nove e 10, quindi registra un incidente.

Nota: Se si attiva **Monitora solo le pagine stampate/inviata via fax** (anche utilizzando una regola di risposta Limita conservazione dati incidenti), il file del buffer di stampa (un semplice file di testo) viene conservato nell'istantanea incidente quando c'è una violazione della politica.

■ **Monitora intero file**

Questa impostazione blocca l'intero processo di stampa (da Word, PowerPoint ed Excel) se una pagina contiene dati riservati. Ad esempio, se un utente endpoint stampa un documento di 10 pagine e i dati riservati si trovano nella pagina dieci, l'agente impedisce la stampa di tutte e dieci le pagine, quindi registra un incidente.

Nota: Se si utilizza una regola di risposta Limita conservazione dati incidenti e si attiva **Monitora intero file**, il file originale viene conservato nell'istantanea incidente quando c'è una violazione della politica.

Impostazioni di Crittografia incentrata sulle informazioni per i DLP Agent

Utilizzare la sezione **Crittografia incentrata sulle informazioni** per attivare il monitoraggio Crittografia incentrata sulle informazioni per i file riservati che vengono trasferiti a un dispositivo di archiviazione rimovibile.

Quando **Attiva crittografia incentrata sulle informazioni** è attivato, DLP Agent monitora e blocca i file riservati che un utente tenta di trasferire da un'unità locale a un dispositivo di archiviazione rimovibile. Quando l'utente trasferisce un file riservato, a seconda della politica e della regola di risposta, la copia del file viene bloccata o all'utente viene chiesto di fare clic su **Crittografa** nel pop-up della regola di risposta **Crittografa** e quindi il file viene crittografato nel dispositivo di archiviazione rimovibile.

Nota: Applicare la licenza di Endpoint Prevent ICE per utilizzare questa funzionalità.

Per informazioni su come Symantec Data Loss Prevention interagisce con Symantec ICE, fare riferimento al *Manuale di distribuzione di Symantec Information Centric Encryption* all'indirizzo:

https://support.symantec.com/en_US/article.DOC9707.html

Vedere "[Configurazione di Enforce Server per connettersi al cloud ICE Symantec](#)" a pagina 229.

Impostazioni agente avanzate

Le seguenti impostazioni riguardano solo DLP Agent. Queste impostazioni non devono essere modificate senza l'assistenza del supporto Symantec. Se si desidera apportare modifiche a questa schermata, contattare il supporto Symantec prima di intervenire.

[Tabella 80-5](#) fornisce un elenco delle impostazioni dell'agente, con il valore predefinito e la descrizione di ogni impostazione.

Nota: Se si cambiano le impostazioni avanzate dell'agente e gli agenti si connettono agli Endpoint Server in un ambiente con bilanciamento del carico, è necessario applicare le stesse modifiche a tutti gli Endpoint Server nell'ambiente con bilanciamento del carico.

Vedere ["Caratteristiche delle impostazioni dell'agente avanzate di Endpoint Prevent per l'agente Mac"](#) a pagina 2057.

Vedere ["Supporto di impostazioni agente avanzate di Endpoint Discover per Mac"](#) a pagina 2059.

Tabella 80-5 Impostazioni avanzate dell'agente

Nome dell'impostazione	Valori predefiniti	Descrizione
AgentManagement.DISABLE_ENABLE_TASK_TIMEOUT_SECONDS.int	300	Il periodo di tempo, in secondi, per il quale l'attività di risoluzione dei problemi Disattiva o Attiva agente attende prima di inviare l'evento di sistema L'agente richiede il riavvio.

Nome dell'impostazione	Valori predefiniti	Descrizione
AgentTamperProtection.ENABLE_AGENT_TAMPER_PROTECTION.int	7	<p>Questa impostazione attiva la protezione dalle alterazioni nell'agente dell'endpoint Symantec Data Loss Prevention.</p> <p>Un'impostazione di 0 disattiva completamente la protezione dalle alterazioni.</p> <p>Un'impostazione di 1 impedisce l'eliminazione o la modifica dei file dell'agente o del watchdog.</p> <p>Un'impostazione di 2 impedisce l'arresto dei servizi dell'agente o del watchdog.</p> <p>Un'impostazione di 3 impedisce l'eliminazione, la modifica o l'arresto dei file e dei servizi dell'agente o del watchdog.</p> <p>Un'impostazione di 4 impedisce l'eliminazione dei servizi dell'agente o del watchdog dal registro del sistema operativo.</p> <p>Un'impostazione di 7 attiva la protezione di file, servizi e registro.</p>
AgentThreadPool.IDLE_TIME_IN_SECONDS.int	60	<p>Il tempo massimo di inattività di un thread prima che venga rimosso dal pool di thread. I thread sono noti anche come attività dell'agente.</p>
AgentThreadPool.MAX_CAPACITY.int	20	<p>Il numero massimo di thread nel pool di thread. I thread possono essere attivi o inattivi.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
AgentThreadPool.MIN_CAPACITY.int	2	Il numero minimo di thread consentiti nel pool di thread. Il pool di thread deve contenere sempre questo numero di thread. I thread possono essere attivi o inattivi.
AggregatorCommunicator.ENABLE_ENDPOINT_DATAFLOW_CACHING.int	1	Se attivata (1), questa impostazione impedisce all'agente di scaricare dati, come politiche e file di configurazione, che sono già stati scaricati. Immettere 0 per disattivare questa impostazione.
ApplicationConnector.KEY_LENGTH.int	64	La lunghezza della chiave, in byte, usata per oscurare la comunicazione tra l'agente e gli hook delle applicazioni.
ApplicationConnector.MAX_CONNECTIONS.int	255	Il numero massimo di hook delle applicazioni (per tipo di hook) che possono collegarsi contemporaneamente all'agente.
ApplicationConnector.TEMPORARY_DIRECTORY.str	%TMP%	La posizione temporanea in cui gli hook delle applicazioni memorizzate i contenuti oscurati.
AttributeResolver.ATTRIBUTE_REFRESH_INTERVAL_IN_DAY.int	7	Il numero di giorni di attesa per l'agente prima di aggiornare le informazioni sugli attributi di Active Directory. Se l'agente trova informazioni più vecchie del numero di giorni indicati, contatta il server di Active Directory. Se il valore è impostato su 0, l'agente non contatta il server AD per recuperare informazioni sugli attributi.

Nome dell'impostazione	Valori predefiniti	Descrizione
Clipboard.ENABLE_CLIPBOARD_KEYBOARD_AND_MOUSE_VIEWER.int	1	<p>Attiva il monitoraggio di mouse e tastiera per le operazioni di copia negli Appunti.</p> <p>Se si osservano comportamenti imprevisti nelle applicazioni, immettere 0 per disattivare questa impostazione.</p> <p>Nota: Disattivando questa impostazione possono verificarsi incidenti di falsi positivi se l'agente impedisce a un'applicazione di accedere ai dati degli Appunti.</p>
ClipboardViewer.SLEEP_TIME_IN_MS.int	10	<p>Il ritardo temporale, in millisecondi, prima che l'agente recuperi i contenuti dagli Appunti dell'endpoint.</p>
CommLayer.MAX_FRAME_SIZE_KILOBYTES.int	8	<p>La dimensione massima di ogni frame in uscita. Questo è il numero massimo di kilobyte per frame letti dalle applicazioni.</p> <p>La modifica a questa impostazione viene applicata a tutte le nuove connessioni. Le modifiche non hanno effetto sulle connessioni esistenti.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
CommLayer.NO_TRAFFIC_TIMEOUT_SECONDS.int	300 secondi (5 minuti)	<p>L'intervallo di heartbeat a livello di applicazione. Per rilevare connessioni inattive l'agente usa un messaggio di heartbeat a livello di applicazione. Data Loss Prevention chiude la connessione per cui non ha ricevuto un heartbeat nell'intervallo di timeout specificato. L'agente non invia heartbeat e si affida invece al keepalive TCP. Un valore 0 indica che l'heartbeat deve essere disattivato. Questo valore è usato anche come valore del timeout dell'handshake delle applicazioni.</p> <p>La modifica a questa impostazione viene applicata alle connessioni nuove ed esistenti.</p> <p>È possibile immettere un valore tra 60 e 86400 secondi.</p>
ComponentLoaderSettings.MAX_COMPONENT_SHUTDOWN_TIME.int	60000	Il periodo di tempo massimo, in millisecondi, che l'agente attende l'arresto di un componente.
ComponentLoaderSettings.PROCESS_PRIORITY.str	NORMAL	Il livello di priorità che definisce la priorità di esecuzione del DLP Agent sull'endpoint. È possibile immettere NORMAL e ABOVE_NORMAL .

Nome dell'impostazione	Valori predefiniti	Descrizione
CrashDump.ENABLE_CRASH_DUMP_COLLECTION.int	1	L'impostazione che consente al sistema di creare un file di dump quando il DLP Agent si arresta in modo anomalo. Impostando questo valore su 1 si consente la creazione del file di dump in caso di arresto anomalo. Immettere 0 per disattivare il file.
CrashDump.MAX_DAYS_TO_KEEP_DUMP.int	2	Il tempo massimo, in giorni, di archiviazione del file di dump in caso di arresto anomalo.
CrashDump.MAX_NUMBER_OF_FILES_IN_DUMP_FOLDER.int	3	Il numero massimo di file da conservare nella cartella di dump in caso di arresto anomalo.
Detection.CHUNK_OVERLAP.int	45	Il numero di caratteri che ogni blocco prende in prestito dalla fine del blocco precedente.
Detection.CHUNK_SIZE.int	65536	La dimensione in byte del blocco di testo.
Detection.DAR_KVOOP_PRIORITY.str	BELOW_NORMAL	La priorità del processo kvoop esterno durante l'estrazione di testo per le scansioni di Endpoint Discover.

Nome dell'impostazione	Valori predefiniti	Descrizione
Detection.ENABLE_METADATA.str	off	Consente il rilevamento sui metadati del file quando un utente tenta di trasferire o stampare un file. Se l'impostazione è attiva, è possibile rilevare i metadati per file Microsoft Office e PDF. Per i file Microsoft Office, sono supportati i metadati OLE, i quali includono i campi Titolo, Oggetto, Autore e Parole chiave. Per i file PDF, solo i metadati del dizionario informazioni documento sono supportati, i quali includono campi come Autore, Titolo, Oggetto, Creazione e Date di aggiornamento. Il contenuto Extensible Metadata Platform (XMP) non è rilevato. L'attivazione di questa opzione può provocare falsi positivi.
Detection.FILE_HEADER_KB_TO_READ.int	1	La quantità massima di byte letti per il rilevamento del tipo di file personalizzato. Impostare questo valore ad almeno 37 KB per consentire al rilevamento sul DLP Agent di determinare il tipo di file ISO.
Detection.FILTER_TIMEOUT.int	420000	Il limite di tempo, in millisecondi, per filtrare il testo.
Detection.LOCAL_DRIVE_KVOOP_PRIORITY.str	BELOW_NORMAL	La priorità del processo kvoop esterno durante l'estrazione di testo per gli eventi dell'unità locale.
Detection.MARKUP_AS_TEXT.str	off	Interrompe il rilevamento su qualsiasi testo con tag XML o HTML associati.

Nome dell'impostazione	Valori predefiniti	Descrizione
Detection.MAX_DETECTION_TIME.int	900000	Il periodo di tempo massimo in millisecondi per completare il rilevamento endpoint.
Detection.MAX_FILTER_FILE_SIZE.int	31457280	La dimensione di file massima in byte per i filtri di testo.
Detection.MAX_IDM_FILE_SIZE	30000000	La dimensione di file massima per l'estrazione di contenuto IDM.
Detection.MAX_NUM_MATCHES.int	300	Il numero massimo di corrispondenze per un determinato verificatore di corrispondenze.
Detection.MAX_QUEUE_SIZE.int	10000	Il numero massimo di elementi simultaneamente in attesa del rilevamento.
Detection.MIN_EXTRACTED_CHARS_FOR_TEXT_IDM_MATCH	30	La dimensione minima del contenuto normalizzato prima che il contenuto convertito sia indicizzato, altrimenti viene cercata una corrispondenza esatta in base al contenuto non elaborato (binario). Deve corrispondere al parametro min_normalized_size nel file Indexer.properties.
Detection.NEWLINE_ELIMINATION.str	on	Determina se le nuove righe vengono eliminate prima del rilevamento.

Nome dell'impostazione	Valori predefiniti	Descrizione
Detection.RULESRESULTSCACHE_ENABLED.str	on	<p>Rules Results Caching (RRC) consente di memorizzare nella cache i risultati del contenuto di un DLP Agent che non viola una politica.</p> <p>Vedere "Informazioni sulla RRC" a pagina 2072.</p> <p>Per impostazione predefinita, RRC è attivato. Se non si desidera utilizzare RRC, impostare questo parametro su off.</p>
Detection.RULESRESULTSCACHE_FAST_CACHE_SIZE.int	2048	<p>La dimensione del database RRC di primo livello, ovvero il database Livello 1. RRC invia le nuove voci dei file registrati che non violano politiche al database Livello 1. Quando il database Livello 1 è pieno, le voci vengono scaricate nel database Livello 2 per liberare spazio nel database Livello 1.</p>
Detection.SHORT_DAR_DETECTION_TIME.int	2000	<p>Il periodo di tempo in millisecondi necessario per il rilevamento di un file prima che il file sia considerato troppo grande.</p>
Detection.TRACKED.CHANGES.str	off	<p>Consente il rilevamento del contenuto modificato col passare del tempo (contenuto Revisioni) nei documenti di Microsoft Office. L'utilizzo di questa opzione può ridurre il tasso di accuratezza per identificatori dati e IDM.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
Detection.TWO_TIER_IDM_ENABLED.str	Vedere la descrizione	<p>Attiva il rilevamento in due fasi per IDM e DLP Agent. Impostare su "off" per utilizzare IDM sull'endpoint. Impostare su "on" per utilizzare il rilevamento in due fasi.</p> <p>Per le nuove installazioni, l'impostazione predefinita è "off", di modo che DLP Agent utilizzi IDM sull'endpoint.</p> <p>Per gli upgrade, l'impostazione predefinita è "off", in modo da mantenere la stessa funzionalità per le politiche IDM esistenti distribuite all'endpoint.</p>
Detection.UNICODE_NORMALIZATION.str	on	Trasforma i caratteri specifici in UNICODE prima del rilevamento. Questa trasformazione è necessaria per la corrispondenza con politiche contenenti dati in molte lingue asiatiche.
DeviceControl.SHOW_NOTIFICATION.int	1	<p>Questa impostazione visualizza i messaggi a comparsa quando un utente di endpoint supera i limiti di accesso al dispositivo.</p> <p>Immettere 0 per disattivare i pop-up.</p>
Discover.CRAWLER_THREAD_PRIORITY.str	BELOW_NORMAL	La priorità dei thread di Discover durante la scansione delle unità.

Nome dell'impostazione	Valori predefiniti	Descrizione
Discover.SCAN_ONLY_WHEN_IDLE.int	2	<p>Determina se l'agente esegue una scansione di Endpoint Discover quando l'utente endpoint è inattivo.</p> <p>Se il valore impostato è 1, l'agente esegue la scansione di Endpoint Discover solo quando l'utente endpoint è inattivo.</p> <p>Se il valore impostato è 2, l'agente esegue la scansione di file di piccole dimensioni quando l'endpoint è attivo e quella di file di grandi dimensioni quando l'utente endpoint è inattivo. I file il cui rilevamento richiede un tempo superiore al valore di Detection.SHORT_DAR_DETECTION_TIME sono considerati grandi.</p> <p>Se il valore impostato è 0, la scansione viene eseguita indipendentemente dall'attività dell'utente.</p>
Discover.SECONDS_UNTIL_IDLE.int	120	<p>Se l'agente non rileva alcuna attività dell'utente in questo periodo di tempo (in secondi), l'utente viene considerato inattivo. Periodi di tempo brevissimi, inferiori a 60 secondi, potrebbero non essere rispettati in modo preciso.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
Discover.STANDARD_REPORT_INTERVAL.int	900000	<p>L'intervallo di tempo in millisecondi tra due report di stato relativi a scansioni di Endpoint Discover.</p> <p>Per creare una connessione transitoria tra l'agente e Endpoint Server, immettere un intervallo superiore al valore di EndpointCommunications.IDLE_TIMEOUT_IN_SECONDS.int.</p>
EncryptionDriver.FORCE_UNLOAD_TIMEOUT.int	10	L'intervallo di tempo in secondi che DLP Agent attende prima di arrestare il driver di crittografia dopo il timeout.
EncryptionDriver.LISTENER_THREADS_COUNT.int	1	<p>Si tratta di un'impostazione di ottimizzazione delle prestazioni. Se si verificano molti accessi a file crittografati e molti file vengono crittografati, aumentando il numero di thread del listener si migliora la reattività della crittografia e dell'accesso ai file. In genere, per endpoint con un singolo utente, un thread del listener offre buone prestazioni. Gli endpoint multiutente possono avere bisogno di più thread del listener.</p>
EncryptionDriver.MESSAGE_HANDLER_THREADS_COUNT.int	10	<p>Si tratta di un'impostazione di ottimizzazione delle prestazioni. Questa impostazione controlla il numero massimo di thread che gestiscono la reattività quando si crittografano i file o quando si accede ai file crittografati.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
EndpointCommunications.HEARTBEAT_INTERVAL_IN_SECONDS.int	270	

Nome dell'impostazione	Valori predefiniti	Descrizione
		<p>L'intervallo di tempo in secondi tra messaggi heartbeat.</p> <p>Endpoint Server invia messaggi heartbeat per rilevare le connessioni inattive con singoli agenti quando nessun altro traffico è inviato o ricevuto. Endpoint Server calcola il tempo tra l'ultimo traffico di dati inviato o ricevuto dall'agente e l'ora corrente.</p> <p>Un traffico di dati è un qualsiasi byte inviato o ricevuto da Endpoint Server, inclusi i byte dei messaggi heartbeat. Quando la durata specificata viene superata, Endpoint Server invia un messaggio heartbeat all'agente. Se il valore dell'impostazione viene modificato nella configurazione degli agenti, il nuovo valore viene immediatamente applicato a tutte le connessioni aperte con gli agenti a cui quella configurazione è applicata, nonché a tutte le connessioni successive.</p> <p>Nota: I messaggi heartbeat definiti dall'applicazione sono trattati dai Network Appliance come traffico e, a differenza dei keepalive TCP, non vengono mai ignorati. I messaggi heartbeat non vengono considerati come messaggi normali per determinare se la connessione è inattiva. L'invio o la ricezione di un messaggio heartbeat non comporta la reimpostazione del tempo di inattività.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
		Immettere un valore tra 0 e 1000000000. Immettere 0 per disattivare l'heartbeat dell'agente.
EndpointCommunications.IDLE_TIMEOUT_IN_SECONDS.int	30	<p>Il periodo di tempo massimo durante il quale una connessione inattiva viene mantenuta aperta.</p> <p>La connessione viene chiusa allo scadere dell'intervallo di tempo in secondi specificato.</p> <p>Questo timeout si applica solo durante la fase di funzionamento normale della connessione, dopo le fasi di handshake SSL e di handshake dell'applicazione.</p> <p>Immettere un valore tra 0 e 1000000000. Immettere 0 per impedire la chiusura delle connessioni inattive.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
EndpointLocation.MATCHES_ALL_INTERFACES_FOR_MANUAL_SETTING.int	1	<p>Il valore, in base all'interfaccia di rete, che definisce se l'endpoint è considerato come appartenente o non appartenente alla rete aziendale. Questa impostazione si applica quando l'impostazione Manualmente in Posizione endpoint è selezionata.</p> <p>Quando il valore è 1, Enforce Server considera l'agente sulla rete aziendale se l'IP dell'endpoint corrisponde a tutti gli indirizzi IP inseriti nel campo IP nella schermata Posizione endpoint.</p> <p>Quando il valore è 0, Enforce Server considera l'agente sulla rete aziendale se l'IP dell'endpoint corrisponde ad almeno uno degli indirizzi IP inseriti nel campo IP nella schermata Posizione endpoint.</p>
ExtensionEnablement.DISPLAY_SAFARI_EXTENSION_NOTIFICATION.int	1	<p>Controlli di valore se la finestra di dialogo Safari: estensioni viene visualizzata sull'endpoint.</p> <p>Quando il valore è 0, la finestra Safari: estensioni non viene visualizzata sull'endpoint.</p> <p>Vedere "Abilitare il monitoraggio nel browser Safari" a pagina 2115.</p>
FileService.MAX_CACHE_SIZE.int	250	<p>Il numero massimo di percorsi di file recentemente aperti che sono stati registrati per ogni processo endpoint.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
FileSystem.APPS_LIST_USES_TRUNCATE_FILE_FOR_BLOCK_RULE	<ul style="list-style-type: none"> ■ TextEdit ■ Microsoft PowerPoint TextEdit	<p>Questa impostazione impedisce gli incidenti duplicati e riduce al minimo i pop-up dell'applicazione, gli arresti anomali e i blocchi quando un utente endpoint modifica un file riservato che si trova in un dispositivo di archiviazione rimovibile per Mac utilizzando TextEdit e Microsoft PowerPoint. Quando questa impostazione è attivata, i file temporanei che contengono informazioni riservate vengono troncati anziché eliminati. Questa impostazione rimuove contenuto dai file temporanei.</p> <p>Se si osserva un comportamento imprevisto nelle applicazioni, è anche possibile ignorare il monitoraggio dell'applicazione. Vedere "Come ignorare applicazioni macOS" a pagina 2245.</p>
FileSystem.DRIVER_FILE_OPEN_REQUEST_TIMEOUT.int	10	<p>Consente di configurare il valore di timeout in secondi per una richiesta di apertura di file inviata da un driver all'agente. Questa impostazione è utile nel caso in cui il connettore del file system sia lento nel rispondere al driver. Se la connessione è lenta, il sistema non funziona correttamente. Ogni richiesta di apertura di file viene posticipata dal driver in attesa della risposta dell'agente. È obbligatorio specificare questa impostazione e il valore 0 non è consentito.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
FileSystem.ENABLE_FILE_RESTORE.int	1	Questa impostazione consente di attivare o disattivare il ripristino di file. Il ripristino di file consente di recuperare il file originale nel caso venga sovrascritto con un file più recente contenente dati riservati. Per impostazione predefinita, il ripristino di file è attivato. Immettere 0 per disattivare questa impostazione.

Nome dell'impostazione	Valori predefiniti	Descrizione
FileSystem.ENABLE_VEP_FILE_ELIMINATION.int	3	

Nome dell'impostazione	Valori predefiniti	Descrizione
		<p>Questa impostazione consente di selezionare il canale di rilevamento per cui viene creato un file <code>.vep</code>. Questo processo esegue inoltre il rilevamento del file originale e risolve tutte le violazioni di condivisione per <code>EDPA.exe</code> e <code>KVOOP.exe</code>, quando necessario.</p> <p>Nota: È possibile modificare questa impostazione se l'ambiente in uso non include:</p> <ul style="list-style-type: none"> ■ Politiche di conservazione di dati ■ Politiche di rilevamento in due fasi <p>È possibile utilizzare i seguenti valori:</p> <ul style="list-style-type: none"> ■ Il valore 0 crea un file <code>.vep</code> per tutti i canali. ■ Il valore 1 esegue il rilevamento del file originale. Un file <code>.vep</code> viene creato per i file sottoposti a scansione spostati in unità rimovibili. ■ Il valore 2 esegue il rilevamento dei file che vengono spostati tramite i canali di archiviazione cloud e accesso ai file di applicazione, nonché tramite applicazioni per CD/DVD. Un file <code>.vep</code> viene creato per tutti gli altri file sottoposti a scansione. ■ Il valore 3 esegue il rilevamento dei file che vengono spostati tramite i canali di archiviazione cloud, archivi rimovibili e

Nome dell'impostazione	Valori predefiniti	Descrizione
		accesso ai file di applicazione. Un file .vep viene creato per tutti gli altri file sottoposti a scansione.

Nome dell'impostazione	Valori predefiniti	Descrizione
FileSystem.IGNORE_STORAGE_BUS_TYPE.str	Nessuno	

Nome dell'impostazione	Valori predefiniti	Descrizione
		<p>Questa impostazione determina quali dispositivi di archiviazione sono ignorati da Symantec Data Loss Prevention. In genere questa impostazione viene definita quando si intende consentire la copia di informazioni riservate in dispositivi esterni forniti dall'azienda quali unità USB o schede SD.</p> <p>Immettere All per ignorare i dispositivi rimovibili collegati a endpoint Windows. I dispositivi USB e FireWire non sono monitorati.</p> <p>Immettere None per monitorare tutti i dispositivi di archiviazione collegati a endpoint Windows o Mac.</p> <p>È possibile configurare Symantec Data Loss Prevention affinché ignori i dispositivi di archiviazione collegati a endpoint Mac indicando il tipo di BUS del dispositivo che si desidera ignorare. È possibile generare il tipo di BUS per un dispositivo utilizzando lo strumento DeviceID. Vedere "Informazioni sulle utilità ID periferica" a pagina 2266.</p> <p>È possibile indicare i seguenti tipi di BUS per i dispositivi rimovibili per Mac:</p> <ul style="list-style-type: none"> ■ USB ■ Secure Digital ■ FireWire <p>Nota: Se si indicano più dispositivi di archiviazione da</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
		ignorare, utilizzare un punto e virgola (;) per separare ogni impostazione.
FileSystem.MAX_BACKLOG	20	Il numero massimo di file di istantanea creati durante il monitoraggio di dispositivi di archiviazione rimovibili.
FileSystem.MONITOR_APPLICATION_CHILD_PROCESS_FILE_ACCESS.INT	1	Questa impostazione consente all'utente di attivare o disattivare la funzionalità Accesso ai file di applicazione che monitora i processi secondari. Immettere 1 per attivare la funzionalità o 0 per disattivarla.
FileSystem.MONITOR_READ_ONLY_VOLUMES.int	1	Determina se il monitoraggio DLP avviene nel caso di una copia di Explorer se il volume di destinazione è di sola lettura. Immettere 1 per continuare a monitorare i volumi di sola lettura in un'operazione di copia di Explorer. Immettere 0 per interrompere il monitoraggio di volumi di sola lettura in un'operazione di copia di Explorer.
FileSystem.NUM_OF_LISTENER_THREADS	1	Il numero di thread di listener che ascoltano le richieste del driver del file system. È possibile immettere un qualsiasi valore intero positivo.

Nome dell'impostazione	Valori predefiniti	Descrizione
FileSystem.NUM_TIMES_TO_OVERWRITE_FILE.int	2	Questa impostazione indica quante volte un file viene sovrascritto con un modello sicuro prima di essere cancellato durante la prevenzione. Il valore 0 indica che il file non può essere sovrascritto.
FileSystem.THREAD_POOL_MAX_CAPACITY	20	Il numero massimo di thread che il pool di thread del file system può utilizzare per soddisfare le richieste del file system.
FileSystem.USE_CDDVD_DEFAULT_EXCLUDE_PATHS.int	1	<p>Questa impostazione consente all'utente di escludere qualsiasi file aperto da un'applicazione per CD/DVD dalle directory seguenti:</p> <ul style="list-style-type: none"> ■ Directory dell'applicazione. Ad esempio, <code>c:\programmi\roxio</code> se l'applicazione è Roxio. ■ Directory di sistema. Ad esempio, <code>%windir%\system32</code>. ■ Programmi\File comuni <p>Per impostazione predefinita, questa impostazione è attivata.</p>
FlexResponse.MAX_INCIDENT_FILE_SIZE.int	31457280	Riservata per uso futuro.
FlexResponse.PLUGIN_HOST_LOG_MAXFILE_SIZE.long	5120000	La dimensione massima di un file di registro di plug-in. Il numero predefinito è in byte.
FlexResponse.PLUGIN_HOST_LOG_MAX_NUMBER_OF_FILES.long	1	Il numero massimo di file di registro di plug-in che possono essere conservati.

Nome dell'impostazione	Valori predefiniti	Descrizione
FlexResponse.PLUGIN_HOST_MESSAGE_TIMEOUT.long	180000	Il lasso di tempo durante il quale l'host del plug-in può elaborare i messaggi. Il valore è in millisecondi.
FlexResponse.PLUGIN_HOST_STARTUP_TIMEOUT.long	30000	Il lasso di tempo disponibile per l'avvio dell'host del plug-in. Il valore è in millisecondi. In caso di mancato avvio dell'host del plug-in entro il periodo di tempo specificato, l'host invia un evento di operazione non riuscita al registro.
FlexResponse.PLUGIN_QUEUE_LIMIT	100	Il numero di richieste di chiamata del plug-in FlexResponse nella coda.
GroupResolution.DAYS_DATA_STALING.int	7	Il periodo di tempo in giorni durante il quale l'agente conserva le informazioni sul gruppo utenti Active Directory (AD). Se le informazioni sono più vecchie del valore impostato, l'agente contatta il server AD.
Hooking.APPLICATION_LOAD_TIMEOUT.int	300000	Specifica l'intervallo in millisecondi durante il quale l'agente cerca di eseguire l'hook dell'applicazione se il caricamento dell'applicazione richiede troppo tempo.

Nome dell'impostazione	Valori predefiniti	Descrizione
Hooking.CLOUD_STORAGE_HOOKING.int	0	<p>Immettere 1 per consentire a DLP Agent di bloccare i file che vengono spostati nelle applicazioni di archiviazione cloud.</p> <p>Questa impostazione è valida per le applicazioni Microsoft Office 2010 e 2013 che salvano dati nell'applicazione di archiviazione cloud Box.</p> <p>Questa impostazione si applica solo agli agenti 14.0.x.</p>
Hooking.EXPLORER_APPLICATION_HOOKING.int	1	<p>Consente a DLP Agent di rilevare quando un utente esegue una stampa con il pulsante destro del mouse in Esplora risorse. Per disattivare questo monitoraggio, impostare il valore 0.</p>
Hooking.EXPLORER_HOOKING.int	7	<p>Consente a DLP Agent di monitorare il traffico di Esplora risorse.</p>
Hooking.SIP_Agent_OSX_VERSION_COMPATABILITY.str	<p>Per una nuova installazione:</p> <p>14.5.0:10.11.6; 14.6.0:10.11.6; 15.0.0:10.11.6; 15.0.0:10.12.5</p> <p>Per i sistemi sottoposti a upgrade, le voci precedenti vengono aggiunte alle impostazioni predefinite.</p>	<p>Consente a DLP Agent di monitorare le applicazioni protette con System Integrity Protection (SIP). Per le ultime versioni di Mac OS supportate e per informazioni sull'aggiunta del monitoraggio per macOS aggiornato, vedere symantec.com/docs/TECH235226 nel centro di supporto Symantec.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
Hooking.USE_LOADLIBRARYW_FROM_IMAGE.int	0	<p>Il metodo per trovare l'indirizzo della funzione LoadLibraryW. È possibile specificare il valore 0 o 1.</p> <p>Il valore 0 utilizza l'API GetProcAddress per trovare la libreria.</p> <p>Il valore 1 legge la tabella delle esportazioni di kernel32.dll per trovare la libreria.</p>
IncidentHandler.CACHE_SIZE_THRESHOLD.int	30	La percentuale di spazio utilizzato nella cache del database endpoint che provoca la sospensione di Endpoint Discover.
IncidentHandler.MAX_BACKOFF.int	3600000	Il tempo di attesa massimo in millisecondi prima che l'agente invii di nuovo un incidente al server se il primo tentativo non riesce.
IncidentHandler.MAX_INCIDENT_FILE_SIZE	31457280	La dimensione in byte del file più grande che l'agente deve inviare in relazione a un incidente.
IncidentHandler.MAX_TTD_FILE_SIZE	31457280	La dimensione in byte del file più grande che l'agente deve inviare per il rilevamento in due fasi.
IncidentHandler.MIN_BACKOFF.int	30000	Il tempo di attesa massimo in millisecondi prima che l'agente invii di nuovo un incidente a Endpoint Server se il primo tentativo non riesce.
IncidentHandler.PERSISTER_MAX_DAR_ENTRIES.int	5	Il numero massimo di incidenti di Endpoint Discover mantenuti nella coda.

Nome dell'impostazione	Valori predefiniti	Descrizione
IncidentHandler.PERSISTER_MAX_ENTRIES.int	25	Il limite massimo di incidenti nell'Agent Store prima che l'agente inizi a rimuovere gli incidenti.
IncidentHandler.SENDER_CHUNK_SIZE.int	65536	La dimensione in byte dei blocchi del database da leggere durante l'invio di file.
LocalizationManager.LOCALE_RECEIVING_DELAY_ON_NEWUSER_LOGON_IN_SECONDS.int	2	Il numero di secondi durante i quali l'agente attende prima di recuperare le impostazioni locali dell'utente. È possibile immettere un valore tra 1 e 20 secondi.
Logging.OperationLogFileSize.long	5120000	La dimensione del file di registro operativo. Questa impostazione specifica la dimensione massima in byte del registro operativo. I registri che superano il valore impostato non sono conservati.
Logging.OperationLogMaxFiles.int	30	Il numero massimo di registri operativi per scansione che vengono conservati. Se il valore impostato viene superato, i file di registro operativi vengono eliminati dalla cartella fino a che il numero rientra nel limite indicato. I file di registro vengono eliminati in base alla data in cui sono stati creati. I file di registro meno recenti sono eliminati per primi. Questa impostazione non è applicabile all'intera directory.

Nome dell'impostazione	Valori predefiniti	Descrizione
Logging.OperationLogTTL.int	90	Il numero di giorni durante i quali i registri operativi sono conservati nella directory. Se il registro operativo non viene aperto o modificato nel periodo specificato, il file viene cancellato.
MonitorSystemUsers.CLIPBOARD.int	0	Attiva il monitoraggio dell'utente di sistema per la funzionalità Appunti. Per impostazione predefinita, è disattivata. Impostare il valore 1 per attivarla.
MonitorSystemUsers.LOCAL_DRIVE.int	0	Attiva il monitoraggio dell'utente di sistema per la funzionalità Unità locale. Per impostazione predefinita, è disattivata. Impostare il valore 1 per attivarla.
MonitorSystemUsers.NETWORK.int	0	Attiva il monitoraggio dell'utente di sistema per i protocolli di rete nel driver (HTTP, FTP). Per impostazione predefinita, è disattivata. Impostare il valore 1 per attivarla.
MonitorSystemUsers.PRINT_FAX.int	0	Consente il monitoraggio dell'utente di sistema per la funzionalità Stampa/fax. Per impostazione predefinita, è disattivata. Impostare il valore 1 per attivarla.

Nome dell'impostazione	Valori predefiniti	Descrizione
NetworkMonitor.APPLY_TYPE_PREFILTERS_TO_FPR.int	0	

Nome dell'impostazione	Valori predefiniti	Descrizione
		<p>Consente di ignorare la risoluzione del percorso del file (FPR) per i trasferimenti di dati su HTTP e FTP. Il DLP Agent utilizza FPR per definire il percorso ai file caricati da un utente carica dall'endpoint, ovvero da un'applicazione o dal file system dell'endpoint, tramite un browser e quando il browser apre un file in background. Il motore di rilevamento utilizza quindi il percorso completo quando esegue la scansione di ogni file alla ricerca di dati riservati.</p> <p>Impostato su 1 se le prestazioni del browser peggiorano. Questa impostazione impedisce all'agente di definire un percorso completo per ogni file spostato tramite un browser. Inoltre, l'agente non monitora le posizioni di file temporanei che il browser utilizza e i percorsi file predefiniti.</p> <p>Per assicurarsi che le prestazioni del browser siano ottimizzate, aggiungere un filtro di monitoraggio che ignora i file temporanei normalmente utilizzati dai browser. Utilizzare le seguenti impostazioni per il filtro Ignora:</p> <ul style="list-style-type: none"> ■ Selezionare Ignora (non eseguire il monitoraggio). ■ Selezionare Allegato HTTP/HTTPS. ■ Immettere i tipi di file da ignorare nel campo Tipo. Ad esempio, immettere <i>INI</i> e <i>TMP</i> per filtrare i file

Nome dell'impostazione	Valori predefiniti	Descrizione
		<p>temporanei utilizzati normalmente dai browser durante il caricamento di file.</p> <p>Vedere "Configurazione dei filtri di file" a pagina 2117.</p>
NetworkMonitor.DISABLE_SPDY_PROTOCOL	1	<p>L'impostazione predefinita (1) consente il monitoraggio dei protocolli SPDY e HTTP2 per Internet Explorer e Firefox in esecuzione sugli endpoint.</p> <p>Impostare il valore 0 per disattivarla. La disattivazione di questa impostazione consente agli utenti endpoint di attivare i protocolli SPDY e HTTP2. L'attivazione di SPDY può influire sul monitoraggio delle perdite di dati.</p>
NetworkMonitor.ENABLE_HTTP_GET_MONITORING.int	0	<p>Attiva il monitoraggio delle richieste HTTP/HTTPS GET. Per impostazione predefinita, è disattivata. Impostare il valore 1 per attivarla.</p>
NetworkMonitor.HTTP_DETECTION_TIMEOUT.int	120	<p>Il tempo di attesa in secondi dell'agente durante una scansione di dati HTTP e HTTPS.</p>
NetworkMonitor.IM_DETECTION_SESSION_TIMEOUT.int	120	<p>La durata, in secondi, della finestra della sessione di rilevamento per tutti i client di messaggistica istantanea.</p>
NetworkMonitor.MIN_BYTE_COUNT_TO_IDENTIFY_PROTOCOL.int	200	<p>Il numero di byte nel pacchetto che l'agente ignora in una determinata sessione di rete prima dell'inizio del rilevamento.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
NetworkMonitor.THREAD_POOL_MAX_CAPACITY	20	Il numero di thread di listener in esecuzione che ascoltano le richieste del driver di rete.
NetworkMonitor.NUM_OF_LISTENER_THREADS.int	60000	Il numero massimo di thread che possono essere utilizzati dal pool di thread di rete per soddisfare le richieste di rilevamento nella rete.
PluginInstaller.TAMPERPROOFING_IGNORE_PROCESS_TIMEOUT.int	15000	Consente di specificare un intervallo di tempo in millisecondi per ignorare tutti i processi di breve durata che non caricano plug-in. Se il processo termina prima del raggiungimento del limite di tempo, il programma di installazione di plug-in non viene avviato.
PostProcessor.ENABLE_FLEXRESPONSE.int	0	Consente di attivare o disattivare Endpoint FlexResponse. Per impostazione predefinita, Endpoint FlexResponse è disattivato. Impostare il valore 1 per attivare Endpoint FlexResponse.
PostProcessor.ENCRYPT_WITH_CANCEL_DEFAULT_ACTION.int	1	L'impostazione predefinita 1 blocca lo spostamento del file se l'utente endpoint non seleziona un'azione nel pop-up Crittografia entro il periodo specificato. Immettere 2 per consentire l'azione.

Nome dell'impostazione	Valori predefiniti	Descrizione
PostProcessor.FILE_SYSTEM_USER_RESPONSE_TIMEOUT.int	60	Il tempo in secondi durante il quale gli utenti endpoint devono selezionare un'azione di risposta alla notifica pop-up Operazione annullata dall'utente. Questa impostazione si applica solo agli eventi generati in seguito a tentativi di trasferire file che violano una politica.
PostProcessor.NETWORK_USER_RESPONSE_TIMEOUT.int	60	Il tempo in secondi durante il quale gli utenti endpoint devono selezionare un'azione di risposta alla notifica pop-up Operazione annullata dall'utente. Questa impostazione si applica solo agli eventi HTTP e FTP.
PostProcessor.NOTIFY_ON_FIXED_DRIVE.int	0	Attiva le notifiche di risposta per gli incidenti che sono stati riparati dall'unità. Per impostazione predefinita, le notifiche sono disattivate. Impostare il valore 1 per attivarla.
PostProcessor.NOTIFY_WITH_CANCEL_DEFAULT_ACTION	1	L'azione predefinita da intraprendere se un utente endpoint non seleziona l'azione nella notifica pop-up Operazione annullata dall'utente entro l'intervallo di tempo specificato. Immettere 1 per bloccare l'azione o 0 per consentirla.

Nome dell'impostazione	Valori predefiniti	Descrizione
PostProcessor.OTHER_USER_RESPONSE_TIMEOUT	60	Il tempo in secondi durante il quale gli utenti endpoint devono selezionare un'azione di risposta alla notifica pop-up Operazione annullata dall'utente. Questa impostazione si applica solo agli eventi Appunti, Stampa, E-mail e HTTPS.
Quarantine.MAX_QUEUE_SIZE.int	100	Il numero massimo di richieste di quarantena nella coda. Le richieste in eccesso sono eliminate e non vengono messe in quarantena.
ResponseCache.AFAC_TIMEOUT	10000	Il periodo di tempo in millisecondi durante il quale un incidente di Accesso ai file di applicazione è memorizzato nella cache. Gli incidenti duplicati che si verificano durante tale periodo di tempo non sono generati e non restituiscono messaggi di regole di risposta.
ResponseCache.CD_TIMEOUT.int	2000	Il periodo di tempo in millisecondi durante il quale un incidente di CD/DVD è memorizzato nella cache. Gli incidenti duplicati che si verificano durante tale periodo di tempo non sono generati o non restituiscono notifiche pop-up di Prevent.

Nome dell'impostazione	Valori predefiniti	Descrizione
ResponseCache.FTP_TIMEOUT.int	60000	Il periodo di tempo in millisecondi durante il quale un incidente di FTP è memorizzato nella cache. Gli incidenti duplicati che si verificano durante tale periodo di tempo non sono generati o non restituiscono notifiche pop-up di Prevent.
ResponseCache.HTTP_TIMEOUT.int	60000	<p>Il periodo di tempo in millisecondi durante il quale un incidente di HTTP/HTTPS è memorizzato nella cache. Gli incidenti duplicati che si verificano durante tale periodo di tempo non sono generati o non restituiscono notifiche pop-up di Prevent.</p> <p>Regolare questa impostazione se si hanno molteplici incidenti e pop-up Blocca. Ciò avviene quando una regola di risposta Blocca è implementata, uno qualsiasi dei canali HTTPS è attivato e gli utenti caricano cartelle che contengono dati riservati da un browser Web in applicazioni Web.</p> <p>Impostare il valore 120000 millisecondi o un valore più grande per impedire molteplici incidenti e pop-up Blocca.</p>
ResponseCache.MAX_SIZE.int	100	Il numero massimo di incidenti memorizzati nella cache.
ServerCommunicator.CONNECT_BACKOFF_DURATION_MULTIPLIER.int	2	Il fattore per il quale ogni ultimo periodo di backoff viene moltiplicato.

Nome dell'impostazione	Valori predefiniti	Descrizione
ServerCommunicator.CONNECT_POLLING_INTERVAL_SECONDS.int	900	<p>Il periodo di tempo (in secondi) durante il quale l'agente attende prima di avviare le connessioni.</p> <p>Il valore minimo specificato dipende dalla differenza di tempo minima tra il momento in cui Enforce Server e Endpoint Server comunicano. Il valore minimo che è possibile specificare per mantenere una connessione persistente è 10. È possibile immettere un valore tra 60 e 86400 secondi per mantenere una connessione non persistente.</p>
ServerCommunicator.INITIAL_CONNECT_BACKOFF_DURATION_SECONDS.int	30	<p>La durata in secondi dell'interruzione temporanea dell'agente dopo il primo errore di backoff.</p> <p>Immettere un valore inferiore al valore di ServerCommunicator.MAX_CONNECT_BACKOFF_DURATION_SECONDS.int.</p>
ServerCommunicator.MAX_CONNECT_BACKOFF_DURATION_SECONDS.int	1800	<p>La durata massima in secondi dell'interruzione temporanea dell'agente prima che effettui il failover sul server successivo.</p> <p>È possibile immettere un valore tra 60 e 86400 secondi.</p>
ServerRedundancy.FAILOVER_INTERVAL.long	3600	<p>L'intervallo di tempo in secondi durante il quale un agente cerca di connettersi a un Endpoint Server prima di effettuare il failover su un nuovo Endpoint Server.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
ServerRedundancy.MAX_TIME_BETWEEN_CONNECTION_ATTEMPTS.long	600	Il tempo di attesa massimo dell'agente tra due tentativi di connessione allo stesso Endpoint Server.
Transport.ALLOW_EXPIRED_CERTIFICATES.int	1	Determina se i certificati scaduti sono accettati o meno. Questa impostazione è applicata a tutte le nuove connessioni dell'agente.
Transport.AUTO_FLUSH_LIMIT_KILOBYTES.int	16	La quantità massima di dati in uscita, in kilobyte, da aggiungere alla coda per una connessione prima dello scaricamento automatico. Immettere un valore inferiore al valore di Transport.MAX_OUTBOUND_KILOBYTES_TO_BUFFER.int.
Transport.DNS_HOST_CACHE_TIMEOUT_SECONDS.int	86.400	Il timeout in secondi per la cache dell'host DNS. Le risoluzioni dei nomi sono mantenute nella memoria per il numero di secondi indicato. Impostare il valore 0 per disattivare completamente la memorizzazione nella cache o -1 per conservare tutte le voci memorizzate. Questa impostazione è applicata a tutte le nuove connessioni dell'agente. È possibile immettere un valore tra -1 e 604800 secondi.

Nome dell'impostazione	Valori predefiniti	Descrizione
Transport.MAX_CONNECT_WAIT_SECONDS.int	30	<p>Il tempo di attesa in secondi per la corretta esecuzione della chiamata di connessione.</p> <p>Questa impostazione è applicata a tutte le nuove connessioni dell'agente.</p> <p>È possibile immettere un valore tra 1 e 300 secondi.</p>
Transport.MAX_INBOUND_KILOBYTES_TO_BUFFER.int	100	<p>La quantità massima di dati in entrata, in kilobyte, da aggiungere alla coda per una connessione.</p> <p>È possibile immettere un valore tra 16 e 2048 secondi.</p>
Transport.MAX_OUTBOUND_KILOBYTES_TO_BUFFER.int	100	<p>La quantità massima di dati in uscita, in kilobyte, da aggiungere alla coda per una connessione.</p> <p>È possibile immettere un valore tra 16 e 2048 secondi.</p> <p>Immettere un valore superiore al valore di CommLayer.MAX_FRAME_SIZE_KILOBYTES.int.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
Transport.MAX_SSL_SESSION_LIFETIME_SECONDS.int	86.400	<p>Il periodo di tempo durante il quale l'agente riutilizza l'ID di una sessione SSL. Una volta trascorso il tempo indicato, l'ID della sessione SSL viene eliminato dall'agente e una nuova sessione SSL viene aperta alla successiva connessione con Endpoint Server.</p> <p>Questa impostazione si applica alle nuove connessioni dell'agente.</p> <p>Immettere 0 per disattivare il riutilizzo dell'ID di una sessione SSL.</p>
Transport.VERIFY_SERVER_HOSTNAME.int	0	<p>Controlla se il certificato di Endpoint Server (nome distinto/comune del server) viene verificato nel client durante il processo di handshake di SSL.</p> <p>Questa impostazione si applica alle nuove connessioni.</p> <p>Immettere 1 per attivare l'impostazione.</p>
UI.BUTTON_ENCRYPT_ALLOW.str	Vuoto	<p>Controlla il testo sul pulsante Crittografa della notifica pop-up della regola di risposta Crittografa. Modificare questa impostazione se si utilizzano impostazioni locali non supportate. La lingua predefinita è l'inglese.</p>

Nome dell'impostazione	Valori predefiniti	Descrizione
UI.BUTTON_OK.str	OK	Controlla il testo sul pulsante OK nel messaggio di notifica all'utente. Modificare questa impostazione se si utilizzano impostazioni locali non supportate. La lingua predefinita è l'inglese.
UI.BUTTON_OKTOALL.str	OK To All	Controlla il testo sul pulsante OK To All nel messaggio di notifica all'utente. Modificare questa impostazione se si utilizzano impostazioni locali non supportate. La lingua predefinita è l'inglese.
UI.CONSECUTIVE_TRANSACTION_TIME.str	10	Il tempo massimo in secondi tra due operazioni di file affinché siano considerate come una singola transazione.
UI.ENCRYPT_CANCEL_MSG_TITLE.str	Vuoto	Immettere il testo per personalizzare il titolo del messaggio della regola di risposta Crittografa .
UI.ENCRYPT_CANCEL_TITLEBAR.str	Vuoto	Immettere il testo per personalizzare il titolo della finestra di dialogo della regola di risposta Crittografa .
UI.MONITOR_MSG_TITLE.str		Il titolo di un messaggio pop-up di notifica.
UI.MONITOR_TITLEBAR.str	Warning	Controlla il messaggio statico nella barra del titolo per il messaggio di notifica Endpoint: notifica. Modificare questa impostazione se si utilizzano impostazioni locali non supportate. L'impostazione predefinita è Warning.

Nome dell'impostazione	Valori predefiniti	Descrizione
UI.NOTIFY_CANCEL_MSG_TITLE	Vuoto	Immettere il testo per personalizzare il titolo del messaggio della regola di risposta Operazione annullata dall'utente .
UI.NOTIFY_CANCEL_TITLEBAR	Vuoto	Immettere il testo per personalizzare il titolo della finestra di dialogo della regola di risposta Operazione annullata dall'utente .
UI.NO_SCAN.int	0	Se si imposta un valore differente da 0, la finestra di dialogo della scansione non viene visualizzata.
UI.NWC_EVENT_LIMIT_FS.int	5	Il numero massimo di eventi che possono essere messi in coda prima che venga accettata un'azione predefinita per altri incidenti. Questa impostazione si applica soltanto agli eventi di file system.
UI.NWC_EVENT_LIMIT_NW.int	2	Il numero massimo di eventi che possono essere messi in coda prima che venga accettata un'azione predefinita per altri incidenti. Questa impostazione si applica soltanto agli eventi di rete.
UI.POPUP_QUEUE_LIMIT.int	100	Il limite di notifiche pop-up che un utente può visualizzare in una singola sessione. Queste notifiche pop-up richiedono una giustificazione dell'utente per la convalida. Se il limite viene superato, le notifiche pop-up in eccesso contengono automaticamente una giustificazione Non applicabile (N/A).

Nome dell'impostazione	Valori predefiniti	Descrizione
UI.PREVENT_MSG_TITLE.str		Il titolo di un messaggio pop-up Blocca.
UI.PREVENT_TIMEOUT.int	300	L'attesa in secondi prima che l'incidente venga generato. Se questo limite viene superato, l'incidente viene creato indipendentemente dalla scelta dell'utente nella finestra.
UI.PREVENT_TITLEBAR.str	Blocked	Controlla il messaggio statico nella barra del titolo per la finestra di dialogo di notifica Endpoint: blocca.
UI.PREVENT_WINPOSITION.int	0	Posizione iniziale della finestra di dialogo di Prevent.
UI.QUARANTINE_PROMPT.str	Il file è in quarantena in:	Controlla il testo che specifica la posizione dei dati in quarantena.
UI.SCAN_BAR.str	(vuoto)	Questa impostazione consente di modificare il testo nel corpo della finestra di scansione. Il testo è statico e viene visualizzato indipendentemente dalle impostazioni locali dell'endpoint.
UI.SCAN_DELAY.int	0	Il periodo di tempo in secondi prima della visualizzazione della finestra di dialogo di scansione.
UI.SCAN_EMAIL.int	0	Questa impostazione attiva l'alternanza per la scansione E-mail. Se il valore impostato è 0, gli utenti non possono selezionare il monitoraggio delle e-mail.

Nome dell'impostazione	Valori predefiniti	Descrizione
UI.SCAN_FTP.int	0	Questa impostazione attiva l'alternanza per la scansione FTP. Se il valore impostato è 0, gli utenti non possono selezionare il monitoraggio FTP.
UI.SCAN_HTTP.int	0	Questa impostazione attiva l'alternanza per il monitoraggio HTTP. Se per questa impostazione è specificato 0, gli utenti non possono selezionare il monitoraggio HTTP.
UI.SCAN_PRINTFAX.int	0	Questa impostazione attiva l'alternanza per la scansione Stampa/Fax. Se per questa impostazione è specificato 0, gli utenti non possono selezionare il monitoraggio Stampa/Fax.
UI.SCAN_REMOVABLEMEDIA.int	1	Questa impostazione attiva l'alternanza per la scansione dei supporti rimovibili. Se per questa impostazione è specificato 0, gli utenti non possono selezionare il monitoraggio dei supporti rimovibili.
UI.SCAN_SHOWTIME.int	2	Tempo minimo, in secondi, per cui rimane visualizzata la finestra di dialogo per la scansione.
UI.SCAN_TITLE.str	(vuoto)	Questa impostazione consente di immettere il titolo della finestra di dialogo per la scansione visibile all'utente. Il titolo è un messaggio statico che viene visualizzato indipendentemente dalle impostazioni internazionali dell'endpoint.

Nome dell'impostazione	Valori predefiniti	Descrizione
UI.USERINPUT_PROMPT.str	Altri	Controlla il prompt che viene visualizzato nei messaggi pop-up di blocco e notifica nel campo di immissione dell'utente. Modificare questo prompt se si utilizzano impostazioni internazionali non supportate. La lingua predefinita è l'inglese.
UninstallPassword.RETRY_LIMIT.int	3	Definisce il numero di volte che un utente può tentare di disinstallare DLP Agent senza immettere la password corretta per la disinstallazione.

Impostazione di canali specifici da monitorare in base alla posizione dell'endpoint

È possibile definire impostazioni di monitoraggio specifiche in base alla posizione dell'endpoint, se all'interno o all'esterno della rete aziendale. Ad esempio, è possibile impostare i DLP Agent per monitorare le copie nelle condivisioni di rete solo quando l'endpoint è fuori dalla rete aziendale, dove c'è una possibilità significativa di perdita di dati.

Questa funzionalità si applica agli agenti della versione 15.0 (e versione successiva). Gli agenti della versione 14.6.x e quelli precedenti applicano le impostazioni per la configurazione **interna alla rete aziendale**.

Nota: I DLP Agent eseguiti su endpoint Mac supportano questa funzionalità quando la posizione endpoint è impostata su **Automatico**. Se si utilizza **Manuale** per la posizione endpoint, tutti gli agenti Mac sono identificati come **esterni alla rete aziendale**.

Vedere ["Configurazione della posizione dell'endpoint"](#) a pagina 2076.

Applicazione di configurazioni agente a un gruppo di agenti

È possibile applicare qualsiasi configurazione agente a qualunque gruppo di agenti. Utilizzare la pagina **Applica configurazione** per assegnare configurazioni agente a gruppi di agenti.

Vedere ["Informazioni sulle configurazioni dell'agente"](#) a pagina 2110.

Applicazione di una configurazione agente a un gruppo di agenti

- 1 Accedere alla schermata **Sistema > Agenti > Configurazione agente**.
- 2 Fare clic sul pulsante **Applica configurazione**.

Viene visualizzata la schermata **Gruppi di agenti**. Assegnare la configurazione agente a un gruppo di agenti.

Vedere ["Aggiornamento delle configurazioni obsolete dell'agente"](#) a pagina 2191.

Vedere ["Aggiunta e modifica di configurazioni agente"](#) a pagina 2111.

Vedere ["Endpoint Server - Configurazione di base"](#) a pagina 255.

Configurazione dello stato di connessione dell'agente

È possibile impostare il periodo di connessione per gli agenti per specificare il periodo di segnalazione. Le impostazioni definite in questa schermata sono applicabili a tutti gli Endpoint Server registrati. L'impostazione predefinita è 18 ore.

Nota: l'impostazione definita deve essere 5 minuti superiore all'intervallo di polling dell'agente (ServerCommunicator.CONNECT_POLLING_INTERVAL_SECONDS.int). Vedere ["Impostazioni agente avanzate"](#) a pagina 2133.

Per configurare lo stato di connessione dell'agente

- 1 Selezionare **Sistema > Impostazioni > Generale**.
- 2 Fare clic su **Configura**.
- 3 Individuare l'area **Configurazione stato connessione agente**.
- 4 Immettere le ore e i minuti per specificare quanto tempo deve trascorrere prima che un agente venga visualizzato come un agente che non invia segnalazioni.
- 5 Salvare le modifiche.

Utilizzo di gruppi di agenti

Il capitolo contiene i seguenti argomenti:

- Informazioni sui gruppi di agenti
- Sviluppo di una strategia per distribuire gruppi di agenti
- Panoramica del processo di distribuzione del gruppo di agenti
- Creazione e gestione degli attributi dell'agente
- Visualizzazione e gestione dei gruppi di agenti
- Visualizzazione dei conflitti di gruppo
- Modifica dei gruppi

Informazioni sui gruppi di agenti

I gruppi di agenti consentono di raggruppare e configurare gli agenti secondo le caratteristiche specifiche dell'utente o del computer, ad esempio paese, posizione e nome del reparto. Queste caratteristiche sono denominate attributi dell'agente. È possibile utilizzare gli attributi per creare gruppi e assegnare configurazioni specifiche ai gruppi in base alle esigenze aziendali. I gruppi di agenti possono essere usati per distribuire e gestire un numero elevato di agenti. È inoltre possibile utilizzare i gruppi di agenti per escludere temporaneamente determinati agenti, in base agli attributi, da politiche che influenzano altre configurazioni a scopo di test.

Un Endpoint Server può supportare più gruppi di agenti. Un Endpoint Server può scoprire dinamicamente a quale gruppo di agenti appartiene un particolare agente, in base alle definizioni di gruppo di agenti e agli attributi dell'agente, e assegnare la configurazione a un agente che appartiene al gruppo di agenti appropriato. L'assegnazione di una configurazione dell'agente per Endpoint Server è inoltre supportata con un gruppo per Endpoint Server.

Con i gruppi di agenti, gli attributi degli utenti connessi e dei computer endpoint possono essere utilizzati per creare condizioni di gruppo. Symantec Data Loss Prevention fornisce sei attributi

predefiniti. È possibile creare altri attributi definiti dall'utente in base agli attributi di Active Directory. Ad esempio è possibile creare una condizione di gruppo in base a un attributo di posizione, quali tutti gli utenti (agenti) situati a New York, e un attributo di reparto, quali tutti gli utenti che fanno parte del reparto Risorse umane. Per tale gruppo è possibile distribuire una configurazione in cui viene monitorata l'archiviazione rimovibile. In questo esempio, la definizione del gruppo di agenti ha due condizioni: posizioni e nomi di reparto.

I gruppi di agenti semplificano la gestione delle eccezioni di configurazione dell'agente autorizzando un raggruppamento logico di agenti endpoint in base alle condizioni. Ad esempio, se si è attivato il monitoraggio della messaggistica istantanea per i dipendenti statunitensi, a eccezione dei dipendenti del Texas, è possibile disporre di un gruppo denominato "Texas Stati Uniti" e disattivare il monitoraggio della messaggistica istantanea per tale gruppo. Tutti i nuovi agenti aggiunti al gruppo "Texas Stati Uniti" ottengono automaticamente una configurazione con il monitoraggio della messaggistica istantanea disattivato.

È possibile distribuire le modifiche di configurazione in fasi con i gruppi di agenti. Inoltre è possibile creare gruppi per le eccezioni per monitorare determinati computer o set di computer in modo diverso. Ad esempio è possibile creare un gruppo del personale dirigente per i casi in cui tale personale non è soggetto alle configurazioni che si applicano al resto dell'organizzazione.

La capacità di modificare un'azione del gruppo di agenti è utile quando è necessario risolvere i problemi in Symantec Data Loss Prevention. Ad esempio è possibile creare un gruppo temporaneo che disattiva il monitoraggio e determinate configurazioni per i dipendenti (che, ad esempio, stampano con un'applicazione specifica) per ovviare a un problema di sicurezza e quindi ripristinare il gruppo di dipendenti precedente quando il problema di stampa è stato risolto.

Vedere ["Sviluppo di una strategia per distribuire gruppi di agenti"](#) a pagina 2182.

Sviluppo di una strategia per distribuire gruppi di agenti

Prima di iniziare a implementare i gruppi di agenti, considerare le configurazioni dell'agente necessarie nel proprio ambiente. Di seguito un elenco di controllo di alto livello delle attività di pianificazione:

1. Identificare le configurazioni dell'agente univoco necessarie nel proprio ambiente. Considerare tutti gli agenti e come si desidera raggrupparli.
2. Annotarsi quale agente ottiene quali configurazioni.
3. Annotarsi gli attributi delle Active Directory utilizzati per creare i gruppi.
4. Organizzare i gruppi in modo che nessun utente appartenga a più di un gruppo. In altri termini, organizzare i gruppi in modo che non si sovrappongano.

Vedere ["Panoramica del processo di distribuzione del gruppo di agenti"](#) a pagina 2183.

Panoramica del processo di distribuzione del gruppo di agenti

La definizione e la gestione di gruppi basati su attributi di agenti comportano diverse attività e diversi passaggi: definizione degli attributi, creazione di gruppi, assegnazione di configurazioni per la distribuzione dei gruppi e risoluzione dei conflitti di gruppo. La [Tabella 81-1](#) fornisce una panoramica del processo di distribuzione dei gruppi di agenti, con riferimenti incrociati a procedure più dettagliate.

Tabella 81-1 Implementazione della strategia del gruppo di agenti

Passaggio	Azione	Per ulteriori informazioni
Passaggio 1	Definire gli attributi da utilizzare per creare i gruppi.	Vedere "Creazione e gestione degli attributi dell'agente" a pagina 2184.
Passaggio 2	Verificare che le definizioni degli attributi siano corrette con lo strumento di verifica degli attributi.	Vedere "Verifica le ricerche dell'attributo con lo strumento Attribute Query Resolver" a pagina 2187.
Passaggio 3	Distribuire gli attributi agli agenti. L'agente riceve le query relative agli attributi dell'agente e il set dei risultati degli attributi viene generato e salvato sull'agente.	Vedere "Applicazione di un attributo nuovo o modificato agli agenti" a pagina 2188.
Passaggio 4	Visualizzare i valori di attributo segnalati dagli agenti per verificare che restituiscano i valori di attributo previsti.	
Passaggio 5	Creare i gruppi desiderati utilizzando gli attributi definiti.	Vedere "Creazione di un nuovo gruppo di agenti" a pagina 2190.
Passaggio 6	Assegnare una configurazione dell'agente al gruppo.	Vedere "Assegnazione delle configurazioni per distribuire i gruppi" a pagina 2192.
Passaggio 7	Verificare che le assegnazioni siano corrette assicurandosi che ciascun gruppo contenga il numero previsto di agenti.	Vedere "Visualizzazione e gestione dei gruppi di agenti" a pagina 2189.

Passaggio	Azione	Per ulteriori informazioni
Passaggio 8	Verificare periodicamente se esistono conflitti di gruppi di agenti. In caso positivo, risolverli.	Vedere "Visualizzazione dei conflitti di gruppo" a pagina 2192.

Creazione e gestione degli attributi dell'agente

Per accedere alla schermata **Attributi agente** dalla schermata **Sistema > Agenti > Gruppi di agenti**, fare clic sul collegamento **Gestisci attributi agente**.

I gruppi di agenti vengono definiti con gli attributi dell'agente. Nella schermata **Attributi agente** è possibile visualizzare un elenco di attributi predefiniti e definiti dall'utente. Si tenga presente che, se l'elenco contiene solo attributi predefiniti, i pulsanti **Esporta**, **Applica modifiche** e **Annulla modifiche** non sono disattivati. Queste azioni possono essere eseguite solo per gli attributi definiti dall'utente.

In questa schermata è possibile utilizzare i pulsanti per

- Creare nuovi attributi. Vedere ["Creazione di un nuovo attributo dell'agente"](#) a pagina 2185.
- Esportare gli attributi. Vedere ["Verifica le ricerche dell'attributo con lo strumento Attribute Query Resolver"](#) a pagina 2187.
- Applicare le modifiche degli attributi. Si tenga presente che i valori degli attributi non vengono recuperati da Active Directory finché non si fa clic su **Applica**. Vedere ["Applicazione di un attributo nuovo o modificato agli agenti"](#) a pagina 2188.
- Annullare le modifiche degli attributi. Vedere ["Annullare le modifiche apportate agli attributi dell'agente"](#) a pagina 2188.

Utilizzare il pulsante **Filtri** per filtrare l'elenco di attributi in base a qualsiasi intestazione.

Esistono due tipi di attributi dell'agente: predefiniti e definiti dall'utente. Gli attributi predefiniti non possono venire eliminati o modificati. Symantec Data Loss Prevention fornisce sei attributi predefiniti:

Tabella 81-2 Attributi predefiniti

Attributo	Definizione
Dominio host agente	Dominio a cui è unito il computer host dell'agente
Dominio utente connesso	Domino dell'utente attualmente connesso
Nome host agente	Nome del computer dell'endpoint su cui è installato l'agente

Attributo	Definizione
Tipo host agente	Architettura del sistema operativo, ad esempio x86 o x64
Versione host agente	Sistema operativo; ad esempio, macOS, Windows 7
Utente connesso	Utente attualmente connesso

Gli attributi definiti dall'utente vengono creati dall'amministratore allo scopo di creare i gruppi. È possibile creare gli attributi definiti dall'utente in base agli attributi di Active Directory (AD). Gli attributi definiti dall'utente possono venire eliminati o modificati.

Nota: Gli attributi definiti dall'utente non sono supportati per i computer su cui è in esecuzione macOS.

Vedere ["Creazione di un nuovo attributo dell'agente"](#) a pagina 2185.

Vedere ["Funzionalità gruppi agente Mac"](#) a pagina 2041.

Creazione di un nuovo attributo dell'agente

È possibile creare un raggruppamento logico degli agenti endpoint in base a condizioni basate su attributi di agente definiti dall'utente. Per gli attributi definiti dall'utente, l'agente esegue una ricerca Active Directory in grado di risolvere i valori di attributo. Quando un agente si avvia, vengono eseguite le ricerche e i risultati di attributi vengono inseriti nella cache.

Per creare gli attributi definiti dall'utente, seguire i seguenti passaggi:

1. Selezionare **Gruppi di agenti** dal menu **Sistema > Agenti**. Quindi, fare clic sul collegamento **Gestisci attributi agente**.
2. Nella schermata **Attributi agente**, fare clic su **Nuovo** per avviare la procedura di creazione dell'attributo.

Verrà visualizzata la schermata **Configura attributo agente**.

3. Aggiungere il nome dell'attributo. I nomi possono contenere da 1 a 100 caratteri.
4. Aggiungere una descrizione dell'attributo. Le descrizioni devono contenere solo caratteri alfanumerici.
5. Selezionare un dominio scegliendo fra Dominio utente o Dominio computer.

Esistono due tipi di attributi per gruppi di agenti definiti dall'utente:

- Dominio utente: attributi relativi all'utente collegato; ad esempio, l'attributo di dominio "dipartimento".

- Dominio computer: attributi relativi al computer; ad esempio, attributo computer "posizione".
 - 6. Aggiungere un filtro di ricerca. Per definire un filtro di ricerca è possibile scegliere tra gli attributi applicati esistenti.
 - 7. Specificare un attributo Active Directory.
Soltanto gli attributi Active Directory sono supportati per gli attributi del gruppo di agenti definito dall'utente.
 - 8. Fare clic su **Salva**. L'opzione **Salva** consente di salvare l'attributo ma non di applicarlo.
 - 9. Eseguire un test dell'attributo e correggere tutti gli eventuali problemi.
Per eseguire una test, esportare gli attributi dalla schermata **Elenco attributi** ed esaminare l'attributo. Quindi utilizzare lo strumento di test Attribute Query Resolver che viene eseguito sull'host di Windows in cui è installato l'endpoint per verificare l'attributo.
Vedere ["Verifica le ricerche dell'attributo con lo strumento Attribute Query Resolver"](#) a pagina 2187.
 - 10. **Applica** gli attributi testati. Gli agenti iniziano a eseguire i report dei valori dell'attributo appena risolvono gli attributi su Active Directory.
Vedere ["Applicazione di un attributo nuovo o modificato agli agenti"](#) a pagina 2188.
 - 11. Verificare che gli agenti stiano creando il report dei valori di attributo. Accedere alla schermata **Sistema > Agenti > Panoramica > Elenco agenti** e verificare che gli agenti stiano creando il report dei valori di attributo. È possibile selezionare una particolare voce dell'agente e visualizzarne il **riquadro di anteprima**. Il **riquadro di anteprima** elenca tutti gli attributi predefiniti e definiti dall'utente e i loro valori, conflitti e avvisi.
Vedere ["Utilizzo della schermata Elenco agenti"](#) a pagina 2197.
- Vedere ["Definizione di un filtro di ricerca per la creazione di attributi definiti dall'utente"](#) a pagina 2186.

Definizione di un filtro di ricerca per la creazione di attributi definiti dall'utente

È possibile utilizzare sia gli attributi predefiniti sia gli attributi definiti dall'utente applicati. Di seguito è riportata la sintassi tipica per un filtro di ricerca:

```
(&(objectCategory=Person)
(objectClass=User)(uid=$LoggedinUser$))
```

Il valore incorporato nei segni del dollaro (\$) rappresenta l'attributo dell'agente che è possibile scegliere quando si fa clic sull'elenco a discesa **Seleziona da attributi esistenti** nella schermata **Configura attributo agente**.

Vedere ["Verifica le ricerche dell'attributo con lo strumento Attribute Query Resolver"](#) a pagina 2187.

Verifica le ricerche dell'attributo con lo strumento Attribute Query Resolver

È possibile verificare la correttezza delle definizioni dell'attributo mediante lo strumento Attribute Query Resolver. In primo luogo, esportare gli attributi in un file XML:

1. Accedere alla schermata **Sistema > Agenti > Gruppi di agenti > Attributi agente**.
2. Fare clic su **Esporta** per esportare i dati degli attributi in un file XML.
3. Fare clic su **Salva file** nella finestra di dialogo **Apertura agent-attributes.xml**.
4. Fare clic su **OK** per completare l'attività di esportazione.

Nota: Lo strumento Attribute Query Resolver recupera gli attributi dell'utente attualmente collegato.

Successivamente, utilizzare questo file XML per verificare gli attributi con lo strumento Attribute Query Resolver.

Nota: Per poter utilizzare questo strumento è necessario disporre dei privilegi di amministratore.

1. Copiare `AttributeQueryResolver.exe` e `aqp.dll` dalla cartella degli strumenti distribuibili dell'agente sull'endpoint della stessa cartella.
2. Eseguire il comando (ad esempio)

```
c:\AttributeQueryResolver.exe -aq=agent-attributes.xml
```
3. Attributi con errori vengono visualizzati in uscita con valori vuoti. Ad esempio, se l'attributo **E-mail utente** contenesse un errore, verrebbe visualizzato come **E-mail utente=** senza il valore. Possono verificarsi errori se un utente fornisce un filtro di ricerca sbagliato, se un attributo specificato non esiste in Active Directory o se Active Directory non è raggiungibile.

È possibile accedere al file di log `AttributeQueryResolver.log` per visualizzare i dettagli degli errori dell'attributo. In questo registro errori dell'attributo, i file senza errori visualizzano un `Error code : 0` (nessun errore). Gli attributi con errori visualizzano un codice errore e una descrizione dell'errore. Ad esempio, l'attributo dell'e-mail dell'utente con un attributo vuoto in uscita (che indica un errore) visualizza il seguente messaggio di errore:

```
2014-01-21 20:41:48 | AttributeQueryResolver | SEVERE | Attribute : User  
Email Error code: -2147463161 Error description : E_ADS_PROPERTY_INVALID
```

Qualora si fornisse allo strumento Attribute Query Resolver un file XML non valido come parametro o non si disponesse dei diritti necessari per utilizzare lo strumento, verrà registrato il seguente errore GRAVE:

```
AttributeQueryResolver | SEVERE | Query store is not open.
```

Se le definizioni dell'attributo sono corrette, è possibile distribuire gli attributi agli agenti. In caso di errori, modificare gli attributi con errori, esportarli ed eseguirli con lo strumento Attribute Query Resolver. Ripetere questa procedura fino all'eliminazione di tutti gli errori.

Vedere ["Applicazione di un attributo nuovo o modificato agli agenti"](#) a pagina 2188.

Applicazione di un attributo nuovo o modificato agli agenti

Gli attributi agente di recente creazione appaiono nella schermata **Attributi agente** con l'etichetta **Nuovo**. Dopo la modifica di un attributo agente, l'attributo presenta lo stato **Modificato**. In entrambi i casi, per attivare gli attributi è necessario applicarli agli agenti. Per applicare le modifiche agli agenti:

1. Fare clic su **Applica modifiche** nella pagina **Attributi agente**.
2. Verificare le modifiche visualizzate nel pop-up **Applica modifiche** e fare clic su **Applica modifiche**. Se si rilevano discrepanze fare clic su **Annulla** e tornare alle schermate precedenti per correggere gli errori.
3. Esaminare la schermata **Attributi agente** aggiornata. Il valore **Stato** degli attributi agente appena applicati ora dovrebbe essere **Aggiornato**.

Vedere ["Annullare le modifiche apportate agli attributi dell'agente"](#) a pagina 2188.

Annullare le modifiche apportate agli attributi dell'agente

Dopo aver modificato determinati attributi e averli verificati con lo strumento Attribute Query Resolver, è possibile che si verifichino problemi con gli attributi modificati. È possibile annullare le modifiche per tornare allo stato originale degli attributi. Per annullare le modifiche, attenersi ai seguenti passaggi:

1. Fare clic su **Annulla modifiche**.
2. Nella finestra di dialogo **Annulla modifiche**, verifica l'elenco degli attributi modificati.
3. Fare clic su **Annulla modifiche** per annullare le modifiche appena apportate.

Vedere ["Modifica degli attributi agente definiti dall'utente"](#) a pagina 2188.

Modifica degli attributi agente definiti dall'utente

È possibile modificare gli attributi agente definiti dall'utente nella schermata **Sistema > Agente > Gruppi di agenti > Attributi agente** :

1. Fare clic sull'attributo nella colonna **Nome**. Gli attributi definiti dall'utente sono tutti di **Tipo Definito dall'utente**.
2. Modificare i campi attributo nella schermata **Sistema > Agenti > Gruppi di agenti > Modifica attributo agente**.
3. Fare clic su **Salva**.

Nota: Non è possibile modificare gli attributi agente predefiniti.

Vedere "[Visualizzazione e gestione dei gruppi di agenti](#)" a pagina 2189.

Visualizzazione e gestione dei gruppi di agenti

È possibile utilizzare gruppi di agenti per avviare il raggruppamento logico dei computer endpoint in base alle condizioni. I gruppi di agenti possono basarsi su

- Attributi degli agenti
- Nomi dell'Endpoint Server
- Nomi host dell'Endpoint

Gli agenti vengono valutati e inclusi in specifici gruppi in base all'ordine di priorità delle condizioni. L'ordine di priorità delle condizioni va dalla più alta alla più bassa.

1. Il nome di un host dell'agente che viene indicato nell'elenco "Includi sempre" nella definizione del gruppo di agenti.
2. Un agente che si collega a un gruppo di Endpoint server quando esiste un gruppo di Endpoint server corrispondente.
3. Un gruppo di agenti con un attributo definito dall'utente, dove l'agente soddisfa la condizione del suo gruppo.

Ad esempio, se un agente appartiene a entrambi i gruppi "Gruppo nome host Endpoint" e "Attributo agente", dal momento che il gruppo nome host Endpoint ha la priorità più alta fra i tre tipi di gruppo, l'agente appartiene al gruppo di nomi host dell'Endpoint.

Verificare lo stato del gruppo di agenti e gestire i gruppi dell'agente nella schermata **Sistema > Agenti > Gruppi di agenti**. Per visualizzare i conflitti tra i gruppi di agenti, fare clic su **Visualizza conflitti di gruppo agenti** sul lato destro della schermata.

Le informazioni relative ai gruppi degli agenti vengono suddivise in diverse colonne all'interno di questa pagina. Fare clic su qualsiasi intestazione di colonna per ordinare le voci alfanumericamente in tale colonna. Per ordinare in ordine inverso fare di nuovo clic sull'intestazione di colonna.

Utilizzare questi pulsanti per eseguire le seguenti operazioni:

- **Nuovo** : creare un nuovo gruppo di agenti.
- **Elimina** : eliminare i gruppi di agenti selezionati.
- **Attiva** : attivare i gruppi di agenti selezionati.
- **Disattiva** : disattivare i gruppi di agenti selezionati.
- **Assegna configurazione** : assegnare una configurazione ai gruppi di agenti creati o aggiornati.
- **Aggiorna configurazione** : aggiornare una configurazione per i gruppi di agenti selezionati.
- **Filtri** : riorganizzare questo elenco di gruppi di agenti per una migliore visualizzazione.

Vedere ["Informazioni sui gruppi di agenti"](#) a pagina 2181.

Vedere ["Panoramica del processo di distribuzione del gruppo di agenti"](#) a pagina 2183.

Vedere ["Condizioni gruppo di agenti"](#) a pagina 2190.

Condizioni gruppo di agenti

Una definizione del gruppo di agenti può avere più condizioni. Inoltre, i seguenti operatori sono supportati per le condizioni del gruppo:

- Condizioni AND implicite
- OR è una condizione supportata da più valori specificati per la condizione
- Clausola Equal _TO
- Carattere jolly (*) per specificare più valori. Ad esempio, "Fin*" corrisponde sia a "Finanza" sia a "Fincon"

È possibile accedere alla schermata principale **Gruppi di agenti** nella console di amministrazione di Enforce Server in **Sistema > Agenti > Gruppi di agenti**.

Vedere ["Creazione di un nuovo gruppo di agenti"](#) a pagina 2190.

Creazione di un nuovo gruppo di agenti

Per creare un gruppo di agenti:

1. Accedere alla schermata **Sistema > Panoramica > Elenco agenti**.
2. Fare clic su **Muovo** per creare un nuovo gruppo. Questa azione consente di accedere alla schermata **Crea nuovo gruppo di agenti**.
3. Immettere il nome del gruppo nel campo **Nome**. Il nome è un campo obbligatorio e deve contenere da 1 a 100 caratteri.
4. Aggiungere una descrizione facoltativa.

5. Fare clic su un pulsante per definire la condizione del gruppo come **Attributi utente** o **Server Endpoint**.
6. Selezionare gli attributi per la condizione dall'elenco **Seleziona attributo agente** e assegnare i valori da far corrispondere per creare una condizione.
7. Aggiungere i nomi degli host dell'agente alla casella **Includi sempre questi agenti** se si dispone di agenti che si desidera includere sempre in questo gruppo.
8. Una volta terminato, fare clic su **Salva** o **Annulla** per ricominciare.
9. Assegnare la configurazione per distribuire il gruppo. Vedere ["Assegnazione delle configurazioni per distribuire i gruppi"](#) a pagina 2192.

Nota: Assegnare una configurazione al gruppo attiva il gruppo.

Vedere ["Panoramica del processo di distribuzione del gruppo di agenti"](#) a pagina 2183.

Vedere ["Assegnazione delle configurazioni per distribuire i gruppi"](#) a pagina 2192.

Aggiornamento delle configurazioni obsolete dell'agente

Quando la configurazione di un agente viene aggiornata ma prima che le modifiche vengano applicate a un gruppo di agenti, il gruppo di agenti ha una configurazione obsoleta. Le configurazioni obsolete dell'agente vengono visualizzate nell'elenco **Sistema > Agenti > Gruppi agenti** insieme al loro nome contrassegnato da un punto esclamativo rosso. Per aggiornare una configurazione obsoleta del gruppo:

1. Nella schermata **Sistema > Agenti > Gruppi agenti**, selezionare un gruppo di agenti per aggiornare la configurazione.
2. Fare clic sulla casella di controllo per il gruppo di agenti con la configurazione obsoleta che si desidera aggiornare.
3. Fare clic su **Aggiorna configurazioni**.
4. Verificare il nome e lo stato del gruppo nella finestra di dialogo **Aggiorna configurazioni** e fare clic su **OK**.
5. Verificare che ogni configurazione del gruppo sia stata aggiornata assicurandosi che non vi siano più punti esclamativi rossi dopo i nomi delle configurazioni dell'agente.

Nota: Se un agente non è in linea, la sua configurazione non verrà aggiornata finché l'agente non tornerà online.

Vedere ["Verificare che le assegnazioni dei gruppi siano corrette"](#) a pagina 2192.

Assegnazione delle configurazioni per distribuire i gruppi

Per distribuire i gruppi creati o aggiornati, è necessario assegnare le configurazioni ai gruppi. Per assegnare una configurazione a un gruppo o a un set di gruppi:

1. Selezionare i gruppi nella schermata **Sistema > Agenti > Gruppi di agenti** facendo clic sulle caselle di controllo a sinistra di ciascun gruppo.
2. Fare clic su **Assegna configurazione** nella barra delle azioni.
3. Scegliere una configurazione nella finestra di dialogo **Assegna configurazione**.
4. Fare clic su **OK** nella finestra di dialogo **Assegna configurazione**.
5. Quando la pagina **Gruppi di agenti** viene aggiornata, vengono visualizzati i nomi **Configurazione assegnata** per i gruppi.

Vedere ["Aggiornamento delle configurazioni obsolete dell'agente"](#) a pagina 2191.

Verificare che le assegnazioni dei gruppi siano corrette

Confermare di disporre del numero previsto di agenti in ciascuno dei gruppi:

1. Accedere a **Sistema > Agenti > Panoramica > Report riepilogativi**.
2. Fare clic su **Filtri avanzati e riepilogo** e selezionare **Riepiloga per: Gruppi di agenti**.
3. Verificare di disporre del numero previsto di agenti di reporting in ciascuno dei gruppi:

Vedere ["Visualizzazione dei conflitti di gruppo"](#) a pagina 2192.

Visualizzazione dei conflitti di gruppo

In qualità di amministratore endpoint è possibile determinare il gruppo di agenti corretto per ciascun computer endpoint sulla base dei valori di attributo che l'agente sull'endpoint segnala a Endpoint Server. Per evitare i conflitti di gruppo, è necessario pianificare attentamente l'implementazione. Controllare inoltre periodicamente se vi sono conflitti di gruppo.

È possibile visualizzare i conflitti nella schermata **Visualizza conflitti**. A questo scopo fare clic sul collegamento **Visualizza conflitti di gruppo agenti** nella schermata **Sistema > Agenti > Gruppi di agenti**. Nella schermata **Visualizza conflitti**, sotto l'intestazione **Gruppi in conflitto**, sono visualizzati i nomi dei gruppi in conflitto.

Se un determinato agente è idoneo a fare parte di più di un gruppo, si genera un conflitto. Per i conflitti semplici, dove il gruppo 2 è un sottoinsieme del gruppo 1, Symantec Data Loss Prevention risolve automaticamente il conflitto a favore del gruppo 2. Ad esempio, se si dispone dei due gruppi:

1. Gruppo USA={Paese=USA}
2. Gruppo Texas= {Paese=USA e Stato=Texas}

il conflitto tra il gruppo "USA" e il gruppo "Texas" viene risolto a favore del gruppo "Texas" perché il gruppo "Texas" è un sottoinsieme del gruppo "USA".

Non esiste alcun meccanismo per la risoluzione automatica dei conflitti di gruppo per i gruppi in conflitto che non sono un sottoinsieme. Ad esempio, se si dispone di un gruppo denominato USA_HR in cui Paese=USA e Reparto=HR e un gruppo USA_VP in cui Paese=USA e Nomina=VP, gli agenti che appartengono ai vicepresidenti nel reparto HR generano un conflitto. Poiché Reparto=HR non è un sottoinsieme di Nomina=VP (o viceversa), il conflitto non può essere risolto e gli agenti in conflitto vengono messi in uno stato di avviso e continuano ad appartenere allo stesso gruppo a cui appartenevano prima che sorgesse il conflitto. Symantec Data Loss Prevention segnala questi conflitti più complessi. Per risolvere i conflitti di gruppo, è necessario modificare le definizioni del gruppo.

Vedere ["Modifica dei gruppi"](#) a pagina 2193.

Modifica dei gruppi

È possibile modificare i gruppi affinché gli agenti abbiano una configurazione diversa nella pagina **Sistema > Agenti > Panoramica > Visualizza tutti i gruppi**. La capacità di cambiare la configurazione di un agente da un gruppo a un altro è utile in molte situazioni, soprattutto quando è necessario risolvere un problema relativo a Symantec Data Loss Prevention.

Ad esempio, i dipendenti del gruppo di compravendita Texas possono avere difficoltà a stampare con l'applicazione della borsa. Questo problema è serio per l'azienda in quanto i dipendenti non possono lavorare senza avere la possibilità di stampare. È possibile spostare gli agenti del gruppo di compravendita Texas in un gruppo temporaneo, denominato "Risoluzione dei problemi del gruppo di compravendita", con il monitoraggio della stampa disattivato fino a quando non si riesce a risolvere il problema relativo agli endpoint degli agenti e rimediare alla situazione. Dopo che il problema è stato risolto, è possibile ripristinare il gruppo di compravendita Texas per attivare il monitoraggio della stampa.

Per modificare i gruppi per le configurazioni degli agenti:

1. Fare clic sulle caselle di controllo per le voci degli agenti che si desidera spostare.
2. Fare clic su **Modifica gruppo**.
3. Scegliere un nuovo gruppo dal menu **Sistema > Agenti > Elenco agenti > Gruppo di agenti**.
4. Fare clic su **OK**.

Vedere ["Informazioni sull'amministrazione di Symantec DLP Agent"](#) a pagina 2194.

Gestione di Symantec DLP Agent

Il capitolo contiene i seguenti argomenti:

- [Informazioni sull'amministrazione di Symantec DLP Agent](#)
- [Informazioni sui registri DLP Agent](#)
- [Informazioni sulla gestione delle password dell'agente](#)

Informazioni sull'amministrazione di Symantec DLP Agent

Dopo aver installato i Symantec DLP Agent, è possibile amministrarli da Enforce Server. Enforce Server fornisce un'interfaccia che può essere usata per:

- Visualizzare informazioni sul Symantec DLP Agent.
- Visualizzare lo stato dei Symantec DLP Agent distribuiti.
- Visualizzare eventi per Symantec DLP Agent.
- Generare report per i Symantec DLP Agent distribuiti.
- Risolvere problemi relativi ai Symantec DLP Agent distribuiti.

Per visualizzare e gestire Symantec DLP Agent, accedere a Enforce Server di Symantec Data Loss Prevention, quindi fare clic su **Sistema > Agenti**.

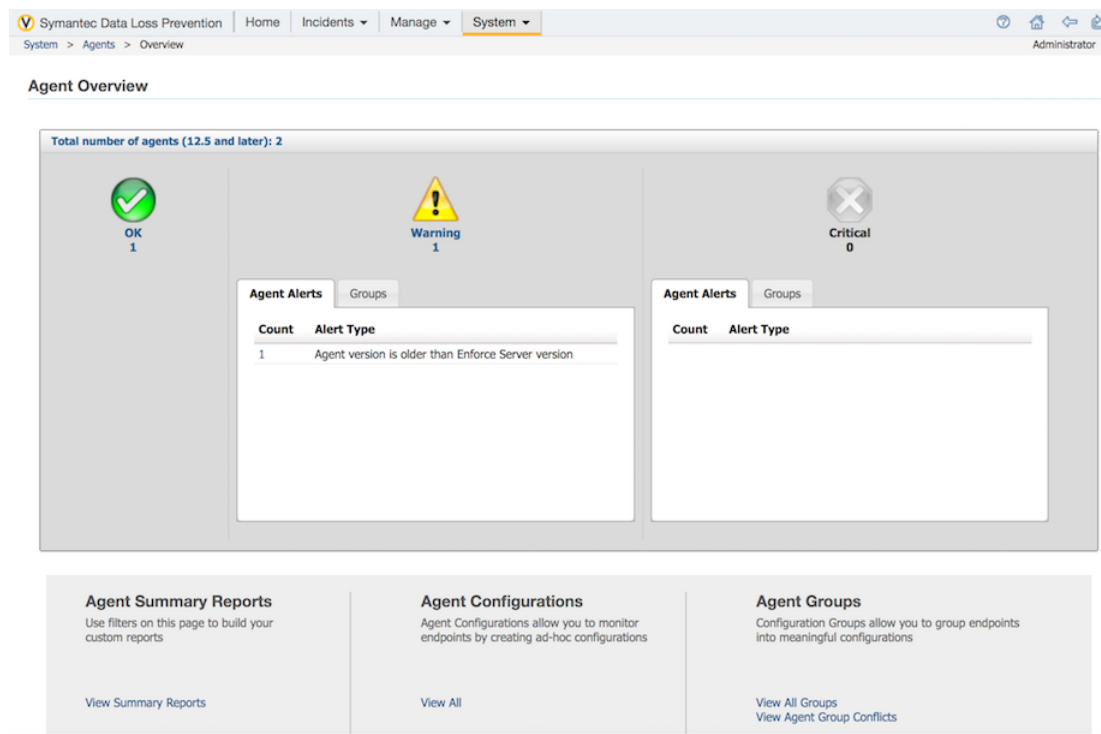
Vedere ["Schermata Panoramica agente"](#) a pagina 2195.

Vedere ["Informazioni sugli eventi di agente"](#) a pagina 2214.

Schermata Panoramica agente

La schermata **Panoramica agente** fornisce una vista riassuntiva di tutti i DLP Agent distribuiti. È possibile utilizzare questa schermata per visualizzare lo stato dell'integrità di DLP Agent e per avviare la risoluzione dei problemi di tutti gli agenti che registrano un avviso. I DLP Agent sono raggruppati per stato e quindi categorizzati per tipo di avviso. I tipi di avviso con il numero più elevato di agenti interessati sono visualizzati per primi. I tipi di avviso con il numero minore di agenti interessati sono elencati per ultimi.




Figura 82-1 Dashboard Integrità agente



È possibile iniziare a risolvere il problema associato a un avviso facendo clic su un'icona di stato o sul collegamento a sinistra del tipo di avviso. Dopo aver fatto clic sull'icona di stato o sul collegamento, viene visualizzata la schermata **Elenco agenti**. Vedere ["Utilizzo della schermata Elenco agenti"](#) a pagina 2197.

I DLP Agent sono raggruppati nei seguenti stati:

Tabella 82-1 Stati DLP Agent

Stato DLP Agent	Descrizione stato
 OK	<p>Uno stato OK indica che i DLP Agent in questo stato funzionano normalmente. Questo stato indica che:</p> <ul style="list-style-type: none"> ■ I servizi e i driver del file system di DLP Agent sono in esecuzione ■ La cache DLP Agent è stata creata ed è disponibile ■ DLP Agent sta generando report a Endpoint Server come previsto
 Avviso	<p>Uno stato Avviso indica che i DLP Agent in questo stato hanno riscontrato condizioni che possono richiedere un intervento.</p> <p>Gli avvisi dell'agente includono in genere quanto segue:</p> <ul style="list-style-type: none"> ■ Versione DLP Agent di livello inferiore ■ Errore di risoluzione gruppo Active Directory ■ Si è verificato un errore con il plug-in ■ È necessario riavviare DLP Agent <p>La seguente sezione fornisce un elenco completo degli stati Avviso.</p> <p>Vedere "Risoluzione dei problemi associati agli avvisi agente" a pagina 2217.</p>
 Critico	<p>Uno stato Critico indica che i DLP Agent in questo stato hanno registrato condizioni che richiedono attenzione immediata:</p> <p>Gli avvisi agente di tipo Critico sono in genere simili ai seguenti:</p> <ul style="list-style-type: none"> ■ Un driver non è in esecuzione ■ La versione di DLP Agent non è compatibile con Endpoint Server ■ Le autorizzazioni Active Directory sono in conflitto con le autorizzazioni Symantec Data Loss Prevention ■ DLP Agent non è in grado di generare report per Endpoint Server ■ DLP Agent non è in grado di monitorare le applicazioni macOS protette con System Integrity Protection (SIP) <p>La seguente sezione fornisce un elenco completo degli stati Critico.</p> <p>Vedere "Risoluzione dei problemi associati agli avvisi agente" a pagina 2217.</p>

La schermata **Panoramica agente** consente di accedere rapidamente ai report riepilogativi dell'agente, alle configurazioni agente e ai gruppi dell'agente.

Tabella 82-2 Funzionalità di gestione agenti

Sezione	Descrizione
Report riepilogativi agente	I report riepilogativi agente consentono di riepilogare i dati agente e di creare report. Vedere "Utilizzo della schermata Report riepilogativi" a pagina 2203.
Configurazione agente	È possibile configurare le impostazioni dell'agente nella schermata Configurazione agente . Vedere "Informazioni sulle configurazioni dell'agente" a pagina 2110.
Gruppi di agenti	È possibile visualizzare i gruppi di agenti esistenti e risolvere i conflitti tra gruppi di agenti. Vedere "Informazioni sui gruppi di agenti" a pagina 2181. Vedere "Visualizzazione dei conflitti di gruppo" a pagina 2192.

Vedere ["Utilizzo della schermata Elenco agenti"](#) a pagina 2197.

Vedere ["Informazioni sugli eventi di agente"](#) a pagina 2214.

Utilizzo della schermata Elenco agenti

Accedere alla schermata **Elenco agenti** facendo clic sul collegamento dello stato di un agente o del tipo di avviso nella schermata **Sistema > Agenti > Panoramica**. La schermata **Elenco agenti** consente di gestire gli agenti mediante la visualizzazione dei dettagli e dello stato di un agente. Selezionare un agente per visualizzare le informazioni corrispondenti, ad esempio lo stato, gli eventuali conflitti di un gruppo di agenti e il nome host dell'agente. È inoltre possibile utilizzare questa schermata per modificare gli agenti.

Vedere ["Informazioni sullo stato dell'agente"](#) a pagina 2199.

È possibile usare la schermata **Elenco agenti** per eseguire le attività di gestione degli agenti.

Nota: utilizzare la funzionalità **Filtri** per eseguire o rimuovere i filtri selezionati. Vedere ["Filtraggio di agenti"](#) a pagina 2202.

Tabella 82-3 Attività di gestione degli agenti

Attività di gestione agenti	Descrizione
Risoluzione dei problemi	<p>Questo menu consente di eseguire le attività di risoluzione dei problemi seguenti:</p> <ul style="list-style-type: none"> Attiva Attiva gli agenti disattivati. Gli agenti attivati si riconnettono automaticamente con Endpoint Server e ottengono le politiche più correnti. L'attivazione di un agente comporta il monitoraggio su tale endpoint. Gli agenti attivati possono registrare gli eventi su Endpoint Server. Disattiva Arresta il monitoraggio ed eventuali scansioni attive degli agenti. Imposta livello registro Imposta il livello di registrazione per l'agente specificato. Il supporto tecnico Symantec usa i registri dell'agente per la risoluzione dei problemi. Nota: si consiglia di contattare il supporto tecnico Symantec prima di modificare il livello di registro per un agente. Vedere "Informazioni sui registri DLP Agent" a pagina 2226. Reimposta livello registro Reimposta il livello di registrazione per l'agente specificato sul livello INFO predefinito. Il supporto tecnico Symantec usa i registri dell'agente per la risoluzione dei problemi. Vedere "Informazioni sui registri DLP Agent" a pagina 2226. Imposta Analisi in corso Selezionare questa opzione se si ritiene che vi siano problemi con l'agente. È possibile impostare questo stato indipendentemente dal fatto che l'agente sia in esecuzione, disattivato o arrestato. Un'icona supplementare, ovvero un flag, viene visualizzata accanto all'icona di stato principale dell'agente. Rimuovi Analisi in corso Rimuove lo stato Imposta Analisi in corso per gli agenti selezionati.
Elimina	<p>Elimina l'agente.</p> <p>Quando si elimina un agente, si rimuovono l'agente e tutti gli eventi associati da Endpoint Server. L'agente non è più visibile nella console di amministrazione di Enforce Server. Quando si elimina un agente da Endpoint Server, non lo si disinstalla dall'endpoint.</p>
Modifica Server	<p>Consente di modificare l'Endpoint Server a cui si connette l'agente.</p> <p>È possibile specificare l'Endpoint Server primario nonché gli Endpoint Server secondari nel caso in cui il server primario si guasti e l'agente debba cambiare connessione.</p> <p>Vedere "Selezione di un altro server Endpoint Prevent" a pagina 2213.</p>

Attività di gestione agenti	Descrizione
Modifica gruppo	Consente di assegnare l'agente selezionato a un gruppo di agenti selezionato. Vedere "Schermata di conferma dell'attività dell'agente" a pagina 2211.
Riavvia	Riavvia l'agente selezionato.
Arresta	Arresta l'agente selezionato. Vedere "Informazioni sugli eventi di agente" a pagina 2214.
Estrai registri	Consente di estrarre i registri e i registri operativi di un agente. È possibile estrarre i registri o i registri operativi di un agente o entrambi i set di registri. L'estrazione dei registri di un agente comporta due fasi: <ul style="list-style-type: none"> ■ Fare clic sul pulsante Estrai registri per scaricare i registri di un agente dall'endpoint su Endpoint Server. ■ Scaricare i registri di un agente da Endpoint Server tramite Enforce Server. È possibile completare questa azione nella schermata Sistema > Server e rilevatori > Registri > Aggregazione. Vedere "Raccolta dei registri e dei file di configurazione del server" a pagina 351. Quando i registri vengono estratti dall'endpoint, vengono archiviati su Endpoint Server in un formato non crittografato. Dopo che i registri sono stati raccolti da Endpoint Server, vengono eliminati da Endpoint Server e archiviati solo su Enforce Server. È possibile raccogliere solo i registri da un endpoint alla volta.
Attiva password di disinstallazione	Impedisce all'agente eseguito su endpoint Windows di venire disinstallato se non si digita la password di disinstallazione dell'agente durante il processo di disinstallazione. Vedere "Informazioni sulla gestione delle password dell'agente" a pagina 2227.
Disattiva password di disinstallazione	Consente all'agente eseguito su endpoint Windows di venire disinstallato senza immettere la password di disinstallazione dell'agente. Nota: Agent DLP assume lo stato Avviso quando la password di disinstallazione è disattivata.

Vedere ["Schermata Panoramica agente"](#) a pagina 2195.

Vedere ["Informazioni sui filtri e sulle opzioni di riepilogo per i report"](#) a pagina 1677.

Vedere ["Informazioni sugli eventi di agente"](#) a pagina 2214.

Vedere ["Utilizzo della schermata Report riepilogativi"](#) a pagina 2203.

Informazioni sullo stato dell'agente

La schermata Elenco agenti consente di visualizzare le informazioni più aggiornate relative all'agente. È possibile utilizzare queste informazioni per esaminare lo stato dell'agente, l'orario

dell'ultimo aggiornamento, il sistema operativo dell'agente e la versione. [Tabella 82-4](#) fornisce un elenco degli stati e dei dettagli dell'agente.

Tabella 82-4 Stato dell'agente

Sezione	Descrizione
Stato	<p>Visualizza lo stato corrente dell'agente.</p> <p>Lo stato dell'agente include quanto segue:</p> <ul style="list-style-type: none"> ■ OK Indica che il driver di servizio e del file system dell'agente sono in esecuzione, che la cache è stata creata ed è disponibile e che la connessione funziona come previsto. ■ Avviso Indica che potrebbe essere necessario controllare l'agente. Ad esempio, Symantec Data Loss Prevention assegna questo stato quando la condivisione di dati endpoint si avvicina al limite di archiviazione. ■ Critico Indica che si sono verificati dei problemi durante la connessione transitoria con l'agente. L'agente potrebbe non funzionare per un determinato periodo di tempo. La politica e la configurazione potrebbero essere scadute. L'agente potrebbe non essere compatibile con l'Enforce Server. ■ Analisi in corso Indica che il sistema sta analizzando l'agente in questione. Gli agenti possono essere sottoposti ad analisi per una serie di diversi motivi, tra i quali l'invio di numerosi incidenti di falsi positivi e l'impossibilità a collegarsi all'Endpoint Server. ■ Nessuna analisi in corso Selezionare questo elemento per rimuovere un agente dall'analisi. ■ Livello registro modificato Indica che il livello del registro dell'agente è stato modificato o reimpostato. Vedere "Informazioni sui registri DLP Agent" a pagina 2226. ■ Livello registro predefinito Selezionare questo elemento per cambiare il livello di registro. Vedere "Informazioni sui registri DLP Agent" a pagina 2226.
Avvisi	<p>Consente di visualizzare il numero di messaggi di avviso e avvisi critici che si verificano in un agente. Per consultare l'elenco degli avvisi di un determinato agente, fare clic sulla voce dell'agente interessato per visualizzare la schermata Eventi.</p> <p>Vedere "Informazioni sugli eventi di agente" a pagina 2214.</p>
Nome computer	Visualizza il nome dell'endpoint.
Nome utente	Visualizza il nome dell'utente endpoint che ha acceduto. Se più utenti hanno effettuato l'accesso all'endpoint, viene visualizzato <i>Multiplo</i> .

Sezione	Descrizione
Gruppo di agenti	Visualizza il nome del gruppo di agenti.
Configurazione agente	<p>Visualizza la configurazione dell'agente in uso:</p> <ul style="list-style-type: none"> ■ Altre configurazioni (non corrente) Indica che viene applicata una configurazione personalizzabile. ■ Configurazione corrente Indica che viene applicata la configurazione più aggiornata. ■ Configurazione obsoleta Indica che la configurazione è obsoleta. ■ Configurazione sconosciuta/eliminata Indica che la configurazione è stata eliminata. Gli agenti visualizzano questo stato di configurazione finché non ricevono una configurazione aggiornata da parte di un Endpoint Server. ■ Configurazione predefinita Indica che viene applicata la configurazione predefinita. Durante l'installazione viene applicata la configurazione predefinita.
Stato connessione	<p>Visualizza lo stato corrente della connessione dell'agente.</p> <p>Lo stato della connessione dell'agente include quanto segue:</p> <ul style="list-style-type: none"> ■ Sconosciuto Agenti con stato sconosciuto. ■ Report DLP Agent attualmente collegati alla rete aziendale. ■ Non generante report DLP Agent attualmente non collegati alla rete aziendale. <p>Vedere "Configurazione della posizione dell'endpoint" a pagina 2076.</p>
Ora ultimo aggiornamento	Visualizza data e ora dell'ultimo aggiornamento dell'agente sull'Enforce Server.
SO	Visualizza il sistema operativo dell'agente.
Piattaforma	Visualizza il tipo di processore dell'agente.
Endpoint Server	Elenca l'Endpoint Server nel quale è registrato l'agente.
Indirizzo IP	Visualizza l'indirizzo IP endpoint.
Versione	Visualizza la versione di endpoint.

Vedere ["Schermata Panoramica agente"](#) a pagina 2195.

Vedere ["Informazioni sui filtri e sulle opzioni di riepilogo per i report "](#) a pagina 1677.

Filtraggio di agenti

È possibile filtrare quali agenti vengono visualizzati nella schermata **Elenco agenti** facendo clic su **Filtri**. Una volta completata la selezione dei criteri di filtro, fare clic sulla casella di controllo.

Fare clic su un'intestazione colonna per ordinare alfanumericamente le voci. Per ordinare nell'ordine inverso, fare di nuovo clic sull'intestazione di colonna. Per impostazione predefinita, Symantec Data Loss Prevention elenca gli agenti in base al nome endpoint. Selezionare elementi nelle intestazioni colonna per visualizzare solo gli agenti contenenti i dati selezionati.

È possibile filtrare gli agenti visualizzati in base a una serie di criteri, tra cui configurazione agente, nome server e indirizzo IP dell'agente. Inoltre è possibile filtrare gli eventi dell'agente in base a set di criteri specifici associati a Symantec DLP Agent. Il riepilogo e il filtraggio degli agenti consente di visualizzare gli agenti in base a criteri specifici e nell'ordine desiderato. Ad esempio, è possibile visualizzare gli agenti ai quali è associato il valore **Configurazione predefinita**, quindi visualizzare gli agenti aggiornati negli ultimi 7 giorni. È possibile fare clic su una colonna per ordinare gli agenti in base alla data dell'ultimo aggiornamento.

Nota: Fare clic su **Seleziona tutto** per selezionare tutti gli agenti che soddisfano i criteri del filtro, indipendentemente dagli agenti attualmente visualizzati sulla griglia. Questa selezione è utile quando gli agenti si estendono su più pagine. Fare clic sulla casella nell'angolo superiore sinistro della griglia per selezionare tutti gli agenti visualizzati sulla griglia.

È possibile filtrare gli agenti visualizzati nella griglia utilizzando i seguenti elementi:

Tabella 82-5 Filtraggio di agenti

Elemento da filtrare	Descrizione
Categoria di avvisi	Consente di applicare un filtro in base a ciascuna delle categorie di avviso dell'agente.
Stato	Selezionare uno stato di avviso dell'agente.
Nome computer	Inserire il nome di un endpoint che si desidera visualizzare. Il valore alfanumerico immesso mostra tutti gli endpoint contenenti la stringa del valore. Ad esempio, per visualizzare gli endpoint con 123 in qualsiasi punto del nome, immettere 123.
Nome utente	Inserire il nome di un utente associato a un endpoint che si desidera visualizzare.
Gruppo di agenti	Selezionare un gruppo di agenti per visualizzare tutti gli agenti inclusi nel gruppo.

Elemento da filtrare	Descrizione
Configurazione agente	Selezionare una configurazione agente.
Stato connessione	Selezionare uno stato di connessione.
Ora ultimo aggiornamento	Selezionare un orario di aggiornamento. Questo valore rappresenta l'ultima volta in cui Enforce Server ha ricevuto dati dall'agente.
SO	Inserire il nome del sistema operativo che si desidera visualizzare. Il valore alfanumerico immesso mostra tutti gli endpoint contenenti la stringa del valore. Ad esempio, per visualizzare gli endpoint con Mac in qualsiasi punto del nome, immettere Mac.
Piattaforma	Selezionare 32bit o 64bit .
Endpoint Server	Fare clic sul nome Endpoint Server per visualizzare l'agente associato a tale server. È anche possibile selezionare Eliminati per visualizzare gli agenti che attualmente trasmettono a server Endpoint Server eliminati.
Indirizzo IP	Immettere un indirizzo IP associato ad un agente.
Versione	Digitare la versione dell'agente che si desidera visualizzare.

Vedere ["Utilizzo della schermata Elenco agenti"](#) a pagina 2197.

Utilizzo della schermata Report riepilogativi

Utilizzare la schermata **Report riepilogativi** (**Sistema > Agenti > Panoramica > Riepilogo > Report**) per riepilogare le informazioni sull'agente e creare report.

Nota: completare le attività di gestione dell'agente nella schermata Elenco agenti. Vedere ["Utilizzo della schermata Elenco agenti"](#) a pagina 2197.

È possibile selezionare quali DLP Agent vengono visualizzati in un report. A questo scopo filtrare gli eventi dell'agente secondo un set di criteri specifici. Ad esempio è possibile riepilogare gli agenti in base alla configurazione dell'agente associata e filtrare tali configurazioni secondo gli agenti aggiornati più recenti.

È possibile generare un report filtrato in base a un numero di criteri, tra cui la configurazione dell'agente, il nome del server e l'indirizzo IP dell'agente. I report riepilogativi prendono il nome dal criterio di riepilogo. Se si esegue nuovamente un report con nuovi criteri, il nome del report cambia di conseguenza.

Per creare un report riepilogativo di DLP Agent

- 1 Selezionare un elemento nell'elenco **Data** per visualizzare gli agenti in base all'ultima ora di connessione.
- 2 Fare clic su **Filtri avanzati e riepilogo**.
- 3 Selezionare un elemento nell'elenco **Riepiloga per** per selezionare i criteri in base a cui eseguire il riepilogo.

Vedere [Tabella 82-6](#) a pagina 2205.

È possibile eseguire il riepilogo in base agli elementi riportati di seguito:

- Configurazione agente
 - Gruppo di agenti
 - IP agente
 - Stato agente
 - Versione agente
 - Avvisi
 - Stato connessione
 - Endpoint Server
 - Stato analisi
 - Livello registro
 - SO
 - Piattaforma
 - Categoria stato
 - Sottocategoria stato
 - Password di disinstallazione
- 4 Fare clic su **Aggiungi filtro** se si desidera aggiungere altri filtri. La [Tabella 82-6](#) elenca i filtri avanzati.
 - 5 Fare clic su **Applica** per generare il report utilizzando i filtri specificati.
 - 6 Fare clic su **Salva > Salva con nome** per salvare il report creato.
 - 7 Fare clic su **Invia** per inviare il report via e-mail.
 - 8 Fare clic su **Esporta tutto: CSV** per scaricare un file CSV del report.

Tabella 82-6 Filtri avanzati e riepilogo

Filtro primario	Condizioni disponibili	Filtro secondario
Configurazione agente	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	Configurazione agente : selezionare la configurazione di DLP Agent che si desidera includere o escludere dal report.
Stato configurazione agente	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ Configurazione corrente : è il numero di agenti che stanno eseguendo la versione più recente della configurazione dell'agente. ■ Configurazione obsoleta : è il numero di agenti che stanno eseguendo una versione precedente della configurazione dell'agente. ■ Configurazione sconosciuta/eliminata : è il numero di agenti che stanno eseguendo una versione sconosciuta della configurazione dell'agente.
Gruppo di agenti	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	Selezionare un gruppo di agenti dall'elenco.
Stato gruppo di agenti	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ Eliminato : indica i gruppi di agenti che sono stati eliminati. ■ Disattivato : indica i gruppi di agenti che sono stati disattivati. ■ Attivato : indica i gruppi di agenti attualmente in uso.
IP agente	<ul style="list-style-type: none"> ■ Contiene Ignora maiuscole/minuscole ■ Non contiene Ignora maiuscole/minuscole ■ Corrisponde esattamente ■ Non corrisponde esattamente ■ Corrisponde esattamente a Ignora maiuscole/minuscole ■ Inizia con ■ Termina con 	IP agente : immettere l'indirizzo IP che si desidera filtrare.

Filtro primario	Condizioni disponibili	Filtro secondario
Stato agente	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ Critico : consente di filtrare i DLP Agent che segnalano uno stato Critico. ■ OK : consente di filtrare i DLP Agent che segnalano uno stato OK. ■ Avviso : consente di filtrare i DLP Agent che segnalano uno stato Avviso.
Versione agente	<ul style="list-style-type: none"> ■ Contiene Ignora maiuscole/minuscole ■ Non contiene Ignora maiuscole/minuscole ■ Corrisponde esattamente ■ Non corrisponde esattamente ■ Corrisponde esattamente a Ignora maiuscole/minuscole ■ Inizia con ■ Termina con 	Versione agente : immettere il numero della versione di DLP Agent che si desidera venga filtrato.
Avvisi	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	Avvisi : immettere l'avviso di DLP Agent che si desidera venga filtrato.
Stato connessione	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ Non generante report : consente di filtrare i DLP Agent che non sono attualmente connessi alla rete aziendale. ■ Generante report : consente di filtrare i DLP Agent che sono attualmente connessi alla rete aziendale. ■ Sconosciuto : consente di filtrare i DLP Agent che hanno uno stato di connessione sconosciuto.
Endpoint Server	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<p>Endpoint Prevent Server : selezionare il Endpoint Prevent Server che si desidera filtrare. Vengono filtrati i DLP Agent che generano un report per questo server.</p> <p>Se si seleziona Eliminato, vengono visualizzati tutti gli endpoint che generano un report per gli Endpoint Server eliminati.</p>

Filtro primario	Condizioni disponibili	Filtro secondario
Stato analisi	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ Analisi in corso ■ Nessuna analisi in corso
Livello registro	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ Personalizza : selezionare tutti i DLP Agent con livelli di registro impostati su un valore diverso dal livello INFO. ■ Impostazione predefinita : selezionare tutti i DLP Agent con livelli di registro impostati sul livello INFO predefinito.
Nome computer	<ul style="list-style-type: none"> ■ Contiene Ignora maiuscole/minuscole ■ Non contiene Ignora maiuscole/minuscole ■ Corrisponde esattamente ■ Non corrisponde esattamente ■ Corrisponde esattamente a Ignora maiuscole/minuscole ■ Inizia con ■ Termina con 	Nome computer : immettere il nome del computer che si desidera utilizzare come filtro.
SO	<ul style="list-style-type: none"> ■ Contiene Ignora maiuscole/minuscole ■ Non contiene Ignora maiuscole/minuscole ■ Corrisponde esattamente ■ Non corrisponde esattamente ■ Corrisponde esattamente a Ignora maiuscole/minuscole ■ Inizia con ■ Termina con 	SO : immettere il nome del sistema operativo che si desidera utilizzare come filtro.
Piattaforma	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ a 32 bit ■ a 64 bit

Filtro primario	Condizioni disponibili	Filtro secondario
Categoria stato	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ Risoluzione gruppo utenti AD ■ Stato modifica configurazione agente ■ Stato modifica gruppo di agenti ■ Stato monitoraggio agente ■ Stato plug-in AIM ■ Stato dump di arresto anomalo ■ Unità del file system ■ Stato plug-in Lotus Notes ■ Stato plug-in Outlook ■ Stato reporting ■ Compatibilità software

Filtro primario	Condizioni disponibili	Filtro secondario
Sottocategoria stato		<ul style="list-style-type: none"> ■ Risoluzione gruppo utenti AD : consente di filtrare i DLP Agent in base a una risoluzione di un gruppo utenti AD riuscita o meno. ■ Stato modifica configurazione agente : consente di filtrare i DLP Agent in base alla data dell'ultimo aggiornamento della configurazione dell'agente. ■ Stato modifica gruppo di agenti : consente di filtrare i DLP Agent in base alla data dell'ultimo aggiornamento del gruppo di agenti. ■ Stato monitoraggio agente : consente di filtrare i DLP Agent in base allo stato monitorato. ■ Stato plug-in AIM : consente di filtrare i DLP Agent che hanno plug-in di AOL Instant Messenger che non sono stati installati, che sono stati riparati o che sono stati manomessi. ■ Stato dump di arresto anomalo : consente di filtrare i DLP Agent per cui sono disponibili dump di arresto anomalo o i DLP Agent che non dispongono di un dump di arresto anomalo. ■ Driver del file system : consente di filtrare i DLP Agent che utilizzano lo stato dei driver del file system con gli agenti. ■ Stato plug-in Lotus Notes : consente di filtrare i DLP Agent che hanno plug-in di Lotus Notes che non sono stati installati, che sono stati riparati o che sono stati manomessi. ■ Stato plug-in Outlook : consente di filtrare i DLP Agent che hanno plug-in di Microsoft Outlook che non sono stati installati, che sono stati riparati o che sono stati manomessi. ■ Stato reporting : consente di filtrare i DLP Agent che generano report o meno. ■ Compatibilità software : consente di filtrare i DLP Agent in base alla compatibilità con Endpoint Server.

Filtro primario	Condizioni disponibili	Filtro secondario
Password di disinstallazione	<ul style="list-style-type: none"> ■ È uno qualsiasi dei seguenti valori ■ Non è alcuno dei seguenti valori 	<ul style="list-style-type: none"> ■ Disattivato : filtra i DLP Agent in cui la password di disinstallazione è disattivata. ■ Attivato : filtra i DLP Agent in cui la password di disinstallazione è attivata.
Nome utente	<ul style="list-style-type: none"> ■ Contiene Ignora maiuscole/minuscole ■ Non contiene Ignora maiuscole/minuscole ■ Corrisponde esattamente ■ Non corrisponde esattamente ■ Corrisponde esattamente a Ignora maiuscole/minuscole ■ Inizia con ■ Termina con 	Immettere il nome dell'utente o il termine di ricerca che si desidera utilizzare come filtro.

I report riepilogativi prendono il nome dal criterio di riepilogo. Se si esegue nuovamente un report con nuovi criteri, il nome del report cambia di conseguenza.

La [Tabella 82-7](#) descrive le colonne che vengono visualizzate nel report riepilogativo creato.

Tabella 82-7 Dettagli dei report riepilogativi

Elemento	Descrizione
Criterio di riepilogo	Identifica gli elementi riepilogati nel report.
Totale	Elenca il numero totale di agenti associati ai criteri di riepilogo.
Stato connessione	Elenca il numero di agenti attualmente connessi alla rete.
Stato integrità	Elenca il numero di agenti contrassegnati con lo stato di integrità OK , Avviso o Critico .
Stato configurazione	Elenca il numero di agenti che stanno eseguendo una versione corrente, obsoleta o sconosciuta della configurazione dell'agente.

Vedere ["Schermata Panoramica agente"](#) a pagina 2195.

Vedere ["Utilizzo della schermata Elenco agenti"](#) a pagina 2197.

Vedere ["Informazioni sulle configurazioni dell'agente"](#) a pagina 2110.

Vedere ["Informazioni sugli eventi di agente"](#) a pagina 2214.

Schermata di conferma dell'attività dell'agente

A seconda dell'attività dell'agente selezionato, è possibile consultare una delle seguenti pagine di conferma. Alcune della pagine di conferma richiedono l'immissione di maggiori informazioni per completare l'attività. Altre pagine di conferma richiedono solo di confermare l'attività. La tabella seguente descrive le differenti pagine di conferma dell'attività dell'agente:

Tabella 82-8 Pagine di conferma dell'attività dell'agente

Attività	Dettagli sulla pagina
Elimina	<p>Confermare che si desidera eliminare Symantec DLP Agent.</p> <p>Fare clic su OK per confermare l'eliminazione.</p>
Modifica Endpoint Server	<p>Immettere l'indirizzo IP o il nome host e il numero di porta per modificare gli Endpoint Server a cui i DLP Agent inviano report.</p> <p>Vedere "Selezione di un altro server Endpoint Prevent" a pagina 2213.</p>
Cambia gruppo	<p>Selezionare il gruppo di agenti dove si desidera spostare l'agente selezionato.</p> <p>L'agente viene spostato nel gruppo selezionato dopo che l'agente si collega all'Endpoint Server.</p>
Riavvia	<p>Fare clic su OK per confermare che si desidera riavviare Symantec DLP Agent.</p>

Attività	Dettagli sulla pagina
Arresta	<p>Confermare che si desidera arrestare gli agenti selezionati. È necessario selezionare una delle opzioni seguenti:</p> <ul style="list-style-type: none"> ■ Arrestare DLP Agent e non riavviare l'agente se viene riavviato il computer endpoint. Symantec DLP Agent non viene riavviato se viene riavviato il computer endpoint. ■ Arrestare DLP Agent e riavviare l'agente se viene riavviato il computer endpoint. Symantec DLP Agent viene arrestato ma viene riavviato automaticamente quando viene riavviato il computer endpoint. <p>Dopo l'arresto dell'agente, non è possibile riavviarlo dalla console di amministrazione di Enforce Server.</p> <p>Selezionare l'opzione di arresto e poi fare clic su OK.</p>
Estrai registri	<p>Selezionare il tipo di registri agente che si desidera, quindi fare clic su OK. È possibile selezionare uno delle seguenti tipi di registri:</p> <ul style="list-style-type: none"> ■ Registri di servizi ■ Registri operativi <p>È necessario selezionare almeno un tipo di registro.</p>
Disattiva	<p>Confermare che si desidera disattivare Symantec DLP Agent. Questa operazione non elimina l'agente.</p> <p>Fare clic su OK per confermare.</p> <p>Nota: Dopo la disattivazione di un agente, gli aggiornamenti della configurazione e le richieste di Endpoint Discover dall'Endpoint Server non sono ricevute.</p>
Attiva	<p>Confermare che si desidera attivare Symantec DLP Agent.</p> <p>Fare clic su OK per confermare.</p> <p>Nota: Dopo aver attivato l'agente, riavviarlo. Il riavvio dell'agente assicura di avere la politica, gli aggiornamenti di configurazione e le richieste di Endpoint Discover più recenti.</p>

Attività	Dettagli sulla pagina
Reimposta livello registro	Reimpostare il livello di registrazione per un agente Symantec Data Loss Prevention sul livello predefinito INFO . Il supporto tecnico Symantec usa i registri dell'agente per la risoluzione dei problemi.
Imposta livello registro	<p>Impostare il livello del registro per un agente Symantec Data Loss Prevention. Il supporto tecnico Symantec usa i registri dell'agente per la risoluzione dei problemi.</p> <p>Nota: Si consiglia di contattare il supporto tecnico Symantec prima di cambiare il livello del registro per un agente.</p>
Imposta Analisi in corso	Nessuna pagina di conferma per questa attività.
Rimuovi Analisi in corso	Nessuna pagina di conferma per questa attività.
Attiva password di disinstallazione	Confermare che si desidera attivare la password di disinstallazione per gli agenti selezionati.
Disattiva password di disinstallazione	Confermare che si desidera disattivare la password di disinstallazione per gli agenti selezionati. Una volta selezionato, lo stato degli agenti diventa Avviso.

Selezione di un altro server Endpoint Prevent

L'attività **Modifica Endpoint Server** consente di cambiare i server Endpoint Prevent con i quali interagiscono i DLP Agent. Mentre si esegue questa attività è anche possibile definire server Endpoint Prevent alternativi ai quali possono connettersi i DLP Agent. La possibilità di definire server Endpoint Prevent alternativi garantisce:

- Ridondanza nei casi in cui il server Endpoint Prevent assume lo stato non in linea.
- Possibilità per i DLP Agent di connettersi ad altri server Endpoint Prevent quando l'endpoint è situato in un'altra posizione geografica o viene spostato in un altro gruppo di politiche.
- Possibilità per i DLP Agent di alternare i server Endpoint Prevent se al server Endpoint Prevent primario è già collegato il numero massimo di DLP Agent.

Per cambiare i server Endpoint Prevent con i quali interagisce DLP Agent:

- 1 Inserire l'indirizzo IP o il nome host del server Endpoint Prevent primario.
- 2 Immettere il numero di porta del server Endpoint Prevent primario.

Nota: I valori di porta devono essere inclusi tra 1 e 65535.

- 3 Per aggiungere un server Endpoint Prevent alternativo fare clic sul segno più (+) per aggiungere un'altra voce.
- 4 Inserire l'indirizzo IP o il nome host del server Endpoint Prevent alternativo.
- 5 Immettere il numero di porta del server Endpoint Prevent alternativo.

Nota: I valori di porta devono essere inclusi tra 1 e 65535.

- 6 Per aggiungere un ulteriore server Endpoint Prevent alternativo, ripetere il passaggio 3.
- 7 Se sono state aggiunte troppe voci server Endpoint Prevent è possibile eliminare una voce facendo clic sul segno meno (-) accanto alla voce.
- 8 Una volta completata l'aggiunta o la modifica dei server Endpoint Prevent, fare clic su **OK** per salvare le modifiche.

Informazioni sugli eventi di agente

La schermata **Eventi di agente** (**Sistemi > Agenti > Eventi**) elenca gli eventi che si sono verificati sugli agenti. Questi eventi possono includere modifiche nel file di database, nella connessione, nel driver del file system e nel servizio. È possibile filtrare e riassumere l'elenco degli eventi e fare clic sulle singole voci per vedere più dettagli.

Le informazioni sull'evento sono suddivise in diverse colonne. Fare clic su qualsiasi intestazione di colonna per ordinare le voci alfanumericamente in tale colonna. Per utilizzare l'ordine inverso, fare di nuovo clic sull'intestazione della colonna. Per impostazione predefinita, Symantec Data Loss Prevention elenca gli eventi nell'ordine in cui si sono verificati.

Tabella 82-9 Schermata degli eventi di gestione agente

Voce	Descrizione
Tipo	<p>Visualizza il tipo di evento, che comprende i seguenti valori possibili:</p> <ul style="list-style-type: none"> ■ Grave ■ Informazioni agente ■ OK

Voce	Descrizione
Ora	Visualizza la data e l'ora dell'evento.
Nome computer	Visualizza l'indirizzo IP o il nome host dell'endpoint.
Categoria	Elenca la categoria di evento, come lo stato del servizio dell'agente, lo stato della connessione, il driver del file system o l'archivio dati.
Sottocategoria	Visualizza la sottocategoria dell'evento come Connessione attiva o Connessione chiusa.

È possibile fare clic su qualunque evento per visualizzare la schermata dei relativi dettagli di evento dell'agente.

Vedere ["Schermata Dettagli eventi dell'agente"](#) a pagina 2216.

È possibile riassumere la visualizzazione degli elementi nella schermata Eventi in base agli elementi elencati in [Tabella 82-9](#). È anche possibile filtrare le informazioni visualizzate nella schermata **Eventi** utilizzando una serie di criteri, compreso il nome del computer, le sottocategorie dell'agente, le informazioni dal riepilogo eventi e il tipo di evento. Il riepilogo e il filtraggio degli eventi consentono di visualizzare i dati dell'agente nell'ordine desiderato. Ad esempio è possibile riepilogare gli agenti in base al nome del computer e filtrare secondo gli agenti aggiornati più di recente.

È possibile eliminare gli eventi dell'agente selezionando un evento e facendo clic su **Elimina**.

Vedere ["Informazioni sui filtri e sulle opzioni di riepilogo per i report"](#) a pagina 1677.

Vedere ["Risoluzione dei problemi associati agli avvisi agente"](#) a pagina 2217.

Riepilogo degli eventi dell'agente

Dopo avere selezionato e applicato i criteri di filtraggio e ordinamento nella schermata Eventi (**Sistema > Agenti > Eventi**), nella schermata **Eventi** viene visualizzato un riepilogo che corrisponde alle selezioni.

È possibile fare clic su ogni colonna per ordinare gli agenti. Fare clic su un numero per visualizzare gli agenti che soddisfano i criteri.

Nella colonna all'estrema sinistra viene visualizzata l'opzione di ordinamento selezionata nell'elenco **Riepiloga per**.

Tabella 82-10 Riepilogo degli eventi dell'agente

Colonna	Descrizione
Nome computer	Visualizza i nomi dei computer.
Totale	Elenca il numero degli agenti connessi.

Colonna	Descrizione
Grave	Elenca il numero di agenti con uno stato di avviso.
Avviso	Elenca il numero di agenti con uno stato di avviso.
Informazioni	Elenca il numero di eventi associati all'agente. Fare clic su questo numero per visualizzare altre informazioni sull'evento o sugli eventi.

Schermata Dettagli eventi dell'agente

La schermata **Dettagli eventi dell'agente** visualizza tutte informazioni disponibili per l'evento selezionato. Questo schermata non è modificabile.

Tabella 82-11 Schermata **Dettagli eventi dell'agente**

Sezione	Titolo	Opzioni
Generali	Tipo	<p>Indica il tipo di evento generale che si è verificato. I tipi di eventi possibili sono:</p> <ul style="list-style-type: none"> ■ Grave Indica un errore che richiede attenzione immediata. ■ Avviso Indica un problema che non è abbastanza grave per generare un errore. ■ Informazioni Elenca le informazioni sull'agente. ■ Orario Fornisce l'ora in cui si è verificato l'evento. ■ Nome computer Fornisce il nome dell'endpoint.

Sezione	Titolo	Opzioni
Messaggio		<p>Fornisce dettagli sull'evento.</p> <ul style="list-style-type: none"> ■ Riepilogo Una breve descrizione dell'evento. ■ Dettaglio Ulteriori informazioni sull'evento. ■ Categoria Una categoria di evento come la condivisione di dati, lo stato della connessione, il driver del file system o lo stato del servizio dell'agente. ■ Sottocategoria La sottocategoria dell'evento come Connessione attiva o Connessione persa. ■ Valore esteso Qualsiasi informazione aggiuntiva sull'evento. Ad esempio, se un file è stato rimosso dalla condivisione dei dati, i metadati del file sono visualizzati in questo campo.

Vedere ["Informazioni sugli eventi di agente"](#) a pagina 2214.

Risoluzione dei problemi associati agli avvisi agente

La seguente sezione fornisce informazioni sulla risoluzione dei problemi associati agli avvisi agente. È possibile visualizzare gli avvisi agente nella schermata **Panoramica agente**.

Vedere ["Schermata Panoramica agente"](#) a pagina 2195.

- Avviso
Vedere [Tabella 82-12](#) a pagina 2218.
- Critico
Vedere [Tabella 82-13](#) a pagina 2221.

[Tabella 82-12](#) elenca i dettagli degli avvisi agente e fornisce informazioni su come risolvere i problemi degli agenti negli endpoint Mac.

Tabella 82-12 Risoluzione dei problemi associati agli avvisi agente di tipo Avviso

Avviso agente	Causa	Correzione
Plug-in DLP Outlook manomesso	Il plug-in Outlook è stato modificato, disattivato o eliminato.	Per correggere il problema: <ul style="list-style-type: none"> ■ Riavviare Outlook. ■ Verificare che il plug-in di Outlook Outlook2k3 Addin sia attivato in Outlook. ■ Eseguire Outlook per almeno 15 secondi, quindi riavviarlo. ■ Verificare che il plug-in di Outlook Outlook2k3 Addin sia attivato.
Installazione plug-in DLP Outlook non riuscita	L'installazione del plug-in Outlook non è riuscita.	Eseguire manualmente <code>AgentInstaller.msi</code> per riparare l'installazione dell'agente.
Plug-in DLP Lotus Notes manomesso	Il plug-in Lotus Notes è stato modificato.	Per correggere il problema: <ul style="list-style-type: none"> ■ Riavviare Lotus Notes. ■ Disinstallare l'agente. ■ Riavviare l'endpoint e installare l'agente.
Installazione plug-in DLP Lotus Notes non riuscita	L'installazione del plug-in Lotus Notes non è riuscita.	Eseguire manualmente <code>AgentInstaller.msi</code> per riparare l'installazione dell'agente.
Plug-in DLP AIM manomesso	Il plug-in AIM è stato modificato o l'installazione del plug-in non è riuscita.	Per correggere il problema: <ul style="list-style-type: none"> ■ Riavviare AIM. ■ Disinstallare l'agente. ■ Riavviare l'endpoint e installare l'agente.
Installazione plug-in DLP AIM non riuscita	L'installazione del plug-in AIM non è riuscita.	Eseguire manualmente <code>AgentInstaller.msi</code> per riparare l'installazione dell'agente.
Risoluzione gruppo di utenti di Active Directory non riuscita	Le autorizzazioni Active Directory sono in conflitto con Symantec Data Loss Prevention. Inoltre ad Active Directory potrebbero mancare degli attributi.	Verificare che le credenziali passate all'agente dispongano delle autorizzazioni necessarie per estrarre le informazioni degli utenti connessi da Active Directory.

Avviso agente	Causa	Correzione
Agente disattivato da utente Enforce	L'agente è stato disattivato dall'amministratore che ha eseguito l'attività di risoluzione dei problemi Disattiva nella schermata Elenco agenti .	<p>Avviare l'agente Windows mediante la schermata Elenco agenti. È anche possibile avviare l'agente con il comando <code>sc</code>.</p> <p>Vedere "Utilizzo della schermata Elenco agenti" a pagina 2197.</p> <p>Per gli agenti Mac è necessario utilizzare lo strumento <code>agent_start</code> per l'avvio dell'agente.</p> <p>Vedere "Avvio dei DLP Agent eseguiti negli endpoint Mac" a pagina 2270.</p>
L'agente richiede il riavvio	L'amministratore può disattivare o attivare il monitoraggio della perdita di dati sugli endpoint eseguendo l'attività di risoluzione dei problemi Disattiva o Attiva nella schermata Elenco agenti . Il monitoraggio è attivato per impostazione predefinita dopo l'installazione dell'agente. Tuttavia, quando l'amministratore esegue le attività Attiva o Disattiva e l'agente è occupato, è possibile che lo stato dell'agente non venga aggiornato e continui a essere Avviso .	<p>Riavviare l'agente nella schermata Elenco agenti.</p> <p>Vedere "Utilizzo della schermata Elenco agenti" a pagina 2197.</p>
Dump di arresto anomalo agente disponibile nell'endpoint per l'analisi	<p>Se l'agente si blocca, Enforce Server visualizza l'avvertimento agente Avviso. In questo scenario viene creato un file di registro che il supporto Symantec utilizza per individuare la causa dell'arresto dell'agente.</p> <p>Le cause dell'arresto dell'agente possono essere le seguenti:</p> <ul style="list-style-type: none"> ■ Problemi temporanei dell'ambiente ■ Problemi sconosciuti dell'agente <p>Se l'agente si arresta spesso, contattare il supporto Symantec e fornire i file di dump dell'arresto disponibili nel percorso <code>/AgentInstallDirectory/_MemDumpFiles/</code> nell'endpoint.</p>	<p>Per correggere il problema:</p> <ul style="list-style-type: none"> ■ Chiudere l'agente nella schermata Elenco agenti. Vedere "Utilizzo della schermata Elenco agenti" a pagina 2197. ■ Individuare i file di dump dell'arresto (*.dmp) nel percorso <code>/AgentInstallDirectory/_MemDumpFiles/</code> del rispettivo endpoint. ■ Eliminare i file di dump dell'arresto. ■ Riavviare l'agente nella schermata Elenco agenti.

Avviso agente	Causa	Correzione
Versione agente precedente alla versione di Enforce Server	<p>La versione dell'agente è anteriore di una o più versioni a quella dell'istanza Endpoint Server alla quale si collega. Se ad esempio la versione di Endpoint Server è 15.0 e quella dell'agente è 14.6.x, l'agente visualizza un Avviso. Se la versione di Endpoint Server è 14.6 e quella dell'agente è 14.x, l'agente visualizza lo stato OK.</p> <p>Le caratteristiche disponibili in Enforce e Endpoint Server non sono disponibili per gli agenti che mostrano un Avviso.</p>	Aggiornare l'agente alla versione più recente.
Rilevamento attributi gruppo di agenti non riuscito	Questo avviso appare se l'agente non è in grado di raccogliere i dati richiesti da Active Directory e di conseguenza Enforce Server non è in grado di spostare l'agente in un gruppo di agenti. L'agente non può raccogliere i dati se si verifica un problema di autorizzazioni Active Directory o se gli attributi richiesti non sono presenti in Active Directory.	<p>Per correggere il problema:</p> <ul style="list-style-type: none"> ■ Verificare la sintassi della query per gli attributi Active Directory. ■ Utilizzare <code>AttributeQueryResolver.exe</code> per verificare le query Active Directory definite in Enforce Server. Vedere "Informazioni sui gruppi di agenti" a pagina 2181.
Conflitti gruppo di agenti	Endpoint Server assegna automaticamente l'agente a un gruppo di agenti in base agli attributi endpoint impostati durante la configurazione del gruppo di agenti. Se l'endpoint rileva più condizioni Gruppo di agenti, produce una segnalazione di tipo Avviso.	<p>Per correggere il problema:</p> <ul style="list-style-type: none"> ■ Verificare le impostazioni del gruppo di agenti. Vedere "Informazioni sui gruppi di agenti" a pagina 2181. ■ Ricreare il gruppo di agenti e utilizzare attributi che soddisfano le condizioni dell'agente.
Password di disinstallazione agente disattivata	Questo avviso viene visualizzato quando l'amministratore disattiva la password di disinstallazione dell'agente eseguendo l'attività Disattiva password di disinstallazione nella schermata Elenco agenti .	<p>Per correggere il problema, attivare la password di disinstallazione dell'agente eseguendo l'attività Attiva password di disinstallazione nella schermata Elenco agenti.</p> <p>Vedere "Utilizzo della schermata Elenco agenti" a pagina 2197.</p>

Tabella 82-13 Risoluzione dei problemi associati agli avvisi agente di tipo Critico

Avviso agente	Causa	Correzione
L'agente non sta generando report	L'agente non ha inoltrato una segnalazione a un Endpoint Server entro il periodo di tempo stabilito. Se l'agente non contatta l'istanza dopo 18 ore, Symantec Data Loss Prevention indica che l'agente non sta generando report. Gli agenti che non inoltrano report non ricevono politiche e informazioni di configurazione aggiornate, pertanto vengono contrassegnati con un avviso agente di tipo Critico.	<p>Per correggere il problema:</p> <ul style="list-style-type: none"> ■ Verificare che l'endpoint in cui è installato l'agente esista. Se non esiste, eliminare l'agente da Enforce Server. Vedere "Utilizzo della schermata Elenco agenti" a pagina 2197. ■ Verificare che l'agente sia in esecuzione nell'endpoint. ■ Verificare la connessione di rete tra Endpoint Server e l'endpoint.
Versione agente non supportata	La versione dell'agente è anteriore di due versioni a quella dell'istanza Endpoint Server alla quale si collega. Se ad esempio la versione di Endpoint Server è 15.0 e quella dell'agente è 12.0.x, viene visualizzato un avviso agente Critico . Le caratteristiche disponibili in Enforce e Endpoint Server non sono disponibili per questi agenti. Symantec Data Loss Prevention segnala questi agenti con un avviso di tipo Critico perché non dispongono delle funzionalità Symantec Data Loss Prevention più aggiornate e potrebbero non funzionare nel modo previsto.	Aggiornare l'agente alla versione più recente.
Unità di file system non attiva	<p>Il servizio agente non è in grado di comunicare con il driver Symantec Data Loss Prevention installato nell'endpoint. I motivi possono essere i seguenti:</p> <ul style="list-style-type: none"> ■ I driver del file system sono stati eliminati. ■ Symantec Data Loss Prevention identifica il driver come non valido. Ciò si verifica in determinati casi se driver è stato modificato. ■ Le comunicazioni tra Symantec Data Loss Prevention e il driver agente sono interrotte a causa di un attacco. 	<p>Per correggere il problema:</p> <ul style="list-style-type: none"> ■ Riavviare l'endpoint. ■ Reinstallare l'agente.

Avviso agente	Causa	Correzione
Una applicazione Mac OS non è monitorata	DLP Agent monitora le applicazioni macOS protette da System Integrity Protection (SIP) in macOS da 10.11 a 10.12. Se si aggiorna la versione di macOS oltre quella supportata, l'agente non monitora più le applicazioni protette da SIP. L'agente continua a monitorare tutti gli altri canali.	Fare riferimento a http://www.symantec.com/docs/TECH235226 per informazioni sul monitoraggio delle applicazioni protette da SIP.
Estensione Safari non attivata	L'utente endpoint non ha attivato l'estensione Symantec sul browser Safari.	L'utente endpoint deve riattivare l'estensione Symantec sul browser Safari. Vedere " Abilitare il monitoraggio nel browser Safari " a pagina 2115.
Estensione Safari disattivata	L'utente endpoint ha disattivato l'estensione Safari.	L'utente endpoint deve riattivare l'estensione Symantec sul browser Safari. Vedere " Abilitare il monitoraggio nel browser Safari " a pagina 2115.
Installazione estensione Safari non riuscita	La versione di Safari in esecuzione sull'endpoint non è supportata.	L'estensione Safari richiede Safari versione 10 o successiva. Aggiornare il browser per attivare il monitoraggio. Vedere " Abilitare il monitoraggio nel browser Safari " a pagina 2115.

Informazioni sulla rimozione di Symantec DLP Agent

È possibile che sia necessario disinstallare Symantec DLP Agent dagli endpoint. La disinstallazione di Symantec DLP Agent può essere eseguita nei modi seguenti:

Tabella 82-14 Rimozione di Symantec DLP Agent

[Rimozione di un DLP Agent da un endpoint Windows](#)

[Rimozione dei DLP Agent dagli endpoint Windows mediante il software di gestione del sistema](#)

[Rimozione dei DLP Agent dagli endpoint Mac mediante il software di gestione del sistema](#)

[Rimozione di un DLP Agent da un endpoint Mac](#)

Rimozione dei DLP Agent dagli endpoint Windows mediante il software di gestione del sistema

Seguire questa procedura se si è scelto di nascondere il servizio Symantec Data Loss Prevention nell'elenco Installazione applicazioni (ARP) durante l'installazione. Poiché Symantec

DLP Agent non compare nell'ARP, non è possibile usare tale elenco per il processo di disinstallazione. È necessario usare il comando MSI per rimuovere Symantec DLP Agent. Eseguire la disinstallazione con il comando MSI solo se si è scelto di nascondere Symantec DLP Agent nell'elenco ARP durante l'installazione.

Per rimuovere l'agente con il comando MSI

- 1 Aprire la finestra del prompt dei comandi.
- 2 Immettere la stringa:

```
msiexec /x AgentInstall_15_1.msi
```

È possibile aggiungere varie opzioni differenti a questo prompt dei comandi.

- 3 Fare clic su **OK**.

Symantec DLP Agent viene disinstallato.

Per rimuovere manualmente l'agente se l'agente non è visualizzato nell'ARP

- 1 Aprire la finestra del prompt dei comandi.
- 2 Immettere il seguente comando dove *[guid]* è il codice prodotto. È possibile individuare il GUID nel Registro di sistema di Windows o nel file `uninstall_agent.bat`.

È possibile aggiungere varie altre opzioni a questo prompt dei comandi:

```
msiexec /x {guid}
```

- 3 Immettere qualsiasi comando opzionale alla fine del comando:

```
msiexec /x AgentInstall_15_1.msi
```

4 Fare clic su **OK**.

È possibile aggiungere opzioni al comando di disinstallazione come `SilentMode` o `Logname`. `SilentMode` consente la disinstallazione di Symantec DLP Agent senza visualizzare un'interfaccia utente sul desktop. L'installazione viene eseguita in background sulla stazione di lavoro e non è visibile all'utente. `Logname` consente di configurare qualsiasi file di registro desiderato. Tuttavia, questa opzione è disponibile solo se si dispone del programma di installazione originale. In caso contrario, è necessario usare il codice prodotto.

Il codice per un'installazione invisibile è:

```
/QN:silentmode
```

Il codice per `Logname` è:

```
/Lv _logname
```

`msi.exe` include varie altre opzioni. Per ulteriori opzioni, vedere la guida MSI.

Vedere ["Informazioni sulla rimozione di Symantec DLP Agent"](#) a pagina 2222.

Rimozione di un DLP Agent da un endpoint Windows 7

Se si disinstallano agenti da un endpoint in cui è in esecuzione Windows 7, è necessario eseguire il prompt dei comandi in modalità **Prompt dei comandi con privilegi elevati**. Questo passaggio è necessario a causa della natura del sistema operativo Windows. Non è possibile installare l'agente utilizzando lo script `install_agent.bat` senza prima attivare la modalità Prompt dei comandi con privilegi elevati.

Per attivare la modalità Prompt dei comandi con privilegi elevati in Windows 7

- 1 Fare clic sul menu **Start**.
- 2 Nel campo **Cerca programmi e file**, digitare **prompt dei comandi**.
Il programma **Prompt dei comandi** è visualizzato nell'elenco dei risultati.
- 3 Tenere premuto il tasto MAIUSC e fare clic con il pulsante destro del mouse sulla voce **Prompt dei comandi** nell'elenco dei risultati. Selezionare **Esegui come amministratore** o **Esegui come altro utente**.
- 4 Se è stato selezionato **Esegui come altro utente**, immettere le credenziali per un utente con privilegi di amministratore.
- 5 Il prompt dei comandi viene avviato in modalità Prompt dei comandi con privilegi elevati. Installare i Symantec DLP Agent sull'endpoint utilizzando questo prompt dei comandi.

Vedere ["Informazioni sulla rimozione di Symantec DLP Agent"](#) a pagina 2222.

Rimozione di un DLP Agent da un endpoint Windows

È possibile disinstallare manualmente i Symantec DLP Agent. La disinstallazione manuale è solo possibile se il Symantec DLP Agent è stato configurato per apparire nell'elenco **Installazione applicazioni** dell'endpoint durante la distribuzione.

Nota: La disinstallazione degli agenti Windows 7/8.1 si effettua in modalità **Prompt dei comandi con privilegi elevati**.

Per disinstallare l'agente manualmente

- 1 Accedere a **Start > Pannello di controllo** e fare doppio clic su **Installazione applicazioni**.
- 2 Selezionare **Installazione agenti**.
- 3 Fare clic su **Rimuovi**.

Vedere ["Informazioni sulla rimozione di Symantec DLP Agent"](#) a pagina 2222.

Rimozione dei DLP Agent dagli endpoint Mac mediante il software di gestione del sistema

Seguire i seguenti passaggi per rimuovere i DLP Agent dagli endpoint Mac mediante il software di gestione del sistema (SMS).

Rimozione dell'agente

- 1 Individuare il comando `uninstall_agent` e copiarlo in una posizione temporanea nell'endpoint.

Questo strumento si trova nel file `Symantec_DLP_15.1_Agent_Mac-IN.zip`.

- 2 Aggiungere il comando di disinstallazione al proprio SMS.

```
sudo /tmp/uninstall_agent -prompt=n
```

```
/rm -f /tmp/uninstall_agent
```

Sostituire `/tmp` con la posizione del comando `uninstall_agent`.

- 3 Individuare gli agenti da disinstallare ed eseguire la disinstallazione.

Rimozione di un DLP Agent da un endpoint Mac

È possibile disinstallare DLP Agent per Mac eseguendo lo strumento di disinstallazione dal percorso predefinito di installazione dell'agente: `/Library/Manufacturer/Endpoint Agent`.

Per disinstallare DLP Agent dagli endpoint Mac

- 1 Individuare il comando `uninstall_agent` e copiarlo in una posizione temporanea nell'endpoint.

Questo strumento si trova nel file `Symantec_DLP_15.1_Agent_Mac-IN.zip`.

Aprire l'app Terminal.

- 2 Eseguire il seguente comando:

```
$sudo ./uninstall_agent
```

Nota: È possibile esaminare i registri di disinstallazione sull'applicazione Terminal eseguendo questo comando: `sudo ./uninstall_agent -prompt=no -log=console`. Per impostazione predefinita, i registri sono salvati nel file `uninstall_agent.log`

Informazioni sui registri DLP Agent

I registri DLP Agent contengono dati operativi e di servizio per tutti i DLP Agent. Più componenti vengono registrati per ciascun DLP Agent. La quantità di informazioni registrate può essere configurata impostando il livello di registrazione per ciascun componente DLP Agent. Una volta configurato il livello di registrazione per un componente DLP Agent, è possibile prelevare il registro e inviarlo al supporto Symantec. Il supporto Symantec può usare il registro per risolvere un problema o per migliorare le prestazioni di un'installazione di un endpoint Symantec Data Loss Prevention.

Vedere ["Impostazione dei livelli di registro per un agente di endpoint"](#) a pagina 2226.

Vedere ["Raccolta dei registri e dei file di configurazione del server"](#) a pagina 351.

Impostazione dei livelli di registro per un agente di endpoint

È possibile configurare la quantità di dati che vengono registrati per un agente. A questo scopo specificare il livello di registro per ciascun componente dell'agente. Il supporto tecnico Symantec può utilizzare questi dati per risolvere i problemi o per migliorare le prestazioni per l'installazione di un endpoint di Symantec Data Loss Prevention.

Vedere ["Informazioni sui registri DLP Agent"](#) a pagina 2226.

Nota: Symantec consiglia di contattare il supporto prima di modificare un livello di registro per un agente.

Per impostare i livelli di registro per un agente

- 1 Nella console di amministrazione di Enforce Server selezionare **Sistema > Agenti > Panoramica**.
- 2 Fare clic su uno stato dell'agente.
- 3 Selezionare un agente.
- 4 Selezionare **Risolvi problemi > Imposta livello registro** per i DLP Agent correnti.
- 5 Selezionare un livello di registro dall'elenco a discesa **Livello registro**.
- 6 Se si desidera modificare il livello di registro per tutti i componenti di questo agente, selezionare **Tutti i componenti logger agente**.
- 7 Se si modifica il livello di registro per componenti specifici di questo agente, immettere il nome di ciascun componente nel campo fornito. Se si immettono più nomi di componente, utilizzare una virgola per separare il nome di ciascun componente. I nomi dei componenti non possono contenere più di 255 caratteri.
- 8 Fare clic su **OK** per salvare le modifiche.

Nella schermata **Elenco agenti** viene visualizzata un'icona accanto all'agente per indicare la modifica del livello di registro.

Si consiglia di ripristinare le impostazioni predefinite dei livelli di registro dell'agente al termine della risoluzione dei problemi. Solo le informazioni generali sull'agente vengono registrate dopo la reimpostazione dei livelli di registro.

Per reimpostare i livelli di registro per tutti i componenti di un agente di endpoint sul livello di registrazione predefinito

- 1 Nella console di amministrazione di Enforce Server selezionare **Sistema > Agenti > Panoramica**.
- 2 Fare clic su uno stato dell'agente.
- 3 Selezionare un agente.
- 4 Selezionare **Risolvi problemi > Reimposta livello registro**.

Nella schermata **Panoramica agente** viene visualizzata un'icona accanto all'agente per indicare il livello di registro aggiornato.

Informazioni sulla gestione delle password dell'agente

Utilizzare la schermata **Gestione password agente** (**Sistema > Agenti > Password agente**) per aggiungere o modificare la password di disinstallazione di DLP Agent e la password degli strumenti di Endpoint. La password di disinstallazione impedisce agli utenti non autorizzati di rimuovere Symantec DLP Agent. La password degli strumenti di Endpoint concede l'accesso ai vari strumenti di gestione dell'agente.

Nota: Soltanto gli amministratori con il ruolo di amministratore server possono utilizzare la schermata **Gestione password agente**. Vedere ["Gestione e aggiunta di ruoli"](#) a pagina 129.

Quando si crea o modifica una password, questa viene applicata agli agenti quando si connettono a Endpoint Server. Inoltre, le password di disinstallazione o degli strumenti di Endpoint create durante il processo di creazione dei pacchetti dell'agente vengono conservate fino a quando gli agenti si connettono a Endpoint Server.

È possibile disattivare la password di disinstallazione determinati agenti nella schermata **Elenco agenti**. Vedere ["Utilizzo della schermata Elenco agenti"](#) a pagina 2197.

È possibile utilizzare la schermata **Gestione password agente** per completare le seguenti attività relative alla password dell'agente:

- Creare una nuova password di disinstallazione o degli strumenti di Endpoint se non è stata creata durante il processo di creazione dei pacchetti dell'agente.
 Vedere ["Creazione di una nuova password di disinstallazione dell'agente o degli strumenti di Endpoint"](#) a pagina 2228.
- Modificare una password esistente di disinstallazione o degli strumenti di Endpoint.
 Vedere ["Modifica della password esistente di disinstallazione dell'agente o degli strumenti di Endpoint"](#) a pagina 2229.
- Mantenere una password creata durante il processo di creazione dei pacchetti dell'agente.
 È possibile scegliere se pubblicare o meno una password di disinstallazione o degli strumenti di Endpoint nei nuovi agenti aggiunti deselezionando la casella di controllo relativa a ciascuna password.
 Vedere ["Conservazione delle password esistenti di disinstallazione dell'agente o degli strumenti di Endpoint"](#) a pagina 2229.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Creazione di una nuova password di disinstallazione dell'agente o degli strumenti di Endpoint

Creare una nuova password di disinstallazione dell'agente o degli strumenti di Endpoint utilizzando la schermata **Gestione password agente**. La nuova password si applica a tutti gli agenti, compresi quelli installati successivamente.

Nota: Il processo sovrascrive tutte le password applicate in precedenza.

Completare i seguenti passaggi per creare una nuova password:

1. Fare clic su **Configura** nella schermata **Gestione password agente**.
2. Selezionare una casella di controllo in corrispondenza della password da cambiare:

- **Applica nuova password di disinstallazione**

- **Applica nuova password strumenti**

È possibile selezionare entrambe le caselle di controllo per cambiare contemporaneamente entrambe le password.

3. Immettere e confermare la password.
4. Fare clic su **Salva** per applicare la nuova password.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2227.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Modifica della password esistente di disinstallazione dell'agente o degli strumenti di Endpoint

È possibile cambiare le password di disinstallazione dell'agente o degli strumenti di Endpoint in qualsiasi momento. Quando si cambia una password utilizzando la schermata **Gestione password agente**, vengono sovrascritte tutte le password applicate in precedenza. Vengono inoltre sovrascritte le password per i nuovi agenti aggiunti. La password si applica a tutti gli agenti.

Completare i seguenti passaggi per cambiare una password esistente:

1. Fare clic su **Configura** nella schermata **Gestione password agente**.
2. Immettere e confermare la nuova password.
3. Fare clic su **Salva** per applicare la nuova password.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2227.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Conservazione delle password esistenti di disinstallazione dell'agente o degli strumenti di Endpoint

È possibile mantenere le password esistenti di disinstallazione dell'agente o degli strumenti di Endpoint a seconda delle proprie esigenze aziendali. È possibile mantenere le password applicate durante il processo di creazione dei pacchetti dell'agente impedendo alla schermata **Gestione password agente** di applicare le password a tutti gli agenti.

Quando si mantengono le password esistenti, gli agenti utilizzano le password aggiunte durante il processo di creazione dei pacchetti dell'agente. Se una password di disinstallazione non è stata utilizzata durante il processo di creazione dei pacchetti dell'agente, gli agenti rimangono senza password di disinstallazione. Le password aggiunte in precedenza utilizzando la schermata **Gestione password agente** rimangono attive.

Completare i seguenti passaggi per mantenere le password:

1. Fare clic su **Configura** nella schermata **Gestione password agente**.
2. Deselezionare una casella di controllo in corrispondenza della password da mantenere:
 - **Applica nuova password di disinstallazione**
 - **Applica nuova password strumenti**
È possibile selezionare entrambe le caselle di controllo per mantenere entrambe le password.
3. Fare clic su **Salva**.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2227.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Utilizzo del controllo applicazioni

Il capitolo contiene i seguenti argomenti:

- [Informazioni sul controllo delle applicazioni](#)
- [Informazioni sull'aggiunta di applicazioni](#)
- [Aggiunta di un'applicazione Windows](#)
- [Aggiunta di un'applicazione macOS](#)
- [Come ignorare applicazioni macOS](#)
- [Informazioni sul monitoraggio Accesso ai file di applicazione](#)
- [Implementazione del monitoraggio Accesso ai file di applicazione](#)

Informazioni sul controllo delle applicazioni

Symantec Data Loss Prevention consente di controllare le applicazioni per la masterizzazione di CD/DVD, IM, e-mail o client HTTP/S. Per impostazione predefinita, Symantec Data Loss Prevention controlla applicazioni quali Apple iTunes, Microsoft Outlook o Mozilla Firefox.

Utilizzare la schermata Controllo applicazioni (**Sistema > Agenti > Controllo applicazioni**) per esaminare e modificare le impostazioni di controllo delle applicazioni.

È possibile usare le impostazioni di controllo per verificare come e se DLP Agent monitora le seguenti attività:

- Dati spostati nella rete
- Dati stampati o inviati via fax
- Dati spostati in e da Appunti endpoint

- Dati spostati in applicazioni
- Dati spostati nel cloud utilizzando applicazioni di sincronizzazione cloud
- Dati scritti su un CD o DVD
- Dati spostati tra USB, condivisione di rete e dischi locali e un'applicazione

È possibile aggiungere applicazioni che la società utilizza e che non sono elencate nella pagina Controllo applicazioni. Ad esempio, se si intende controllare Trillian, è possibile aggiungere l'applicazione alla pagina Controllo applicazioni. Dopo aver aggiunto Trillian, Symantec Data Loss Prevention controlla i file inviati dal client sulla rete.

Nota: È possibile rimuovere qualsiasi applicazione aggiunta, ma non quelle fornite dal sistema.

Vedere ["Aggiunta di un'applicazione Windows"](#) a pagina 2237.

Vedere ["Aggiunta di un'applicazione macOS"](#) a pagina 2241.

Vedere ["Elenco delle applicazioni CD/DVD"](#) a pagina 2235.

Vedere ["Implementazione del monitoraggio Accesso ai file di applicazione"](#) a pagina 2246.

Vedere ["Funzionalità Controllo applicazioni dell'agente Mac"](#) a pagina 2054.

Modifica delle impostazioni di controllo delle applicazioni

È possibile configurare le modifiche globali delle applicazioni che vengono visualizzate per impostazione predefinita nella schermata **Controllo applicazioni**. È possibile associare i metadati della lista nera o della lista bianca al controllo di rete, alle applicazioni CD/DVD e alle applicazioni che utilizzano le funzioni di stampa/fax o degli Appunti. È inoltre possibile specificare se non si desidera che Symantec Data Loss Prevention controlli le applicazioni per le attività di rete, stampa/fax, Appunti o file system. Ad esempio è possibile escludere le attività degli Appunti per Microsoft Outlook. È possibile modificare le impostazioni per Microsoft Outlook in modo da escludere l'attività degli Appunti nella schermata **Informazioni applicazione**.

Per modificare le impostazioni di controllo delle applicazioni

- 1 Individuare e fare clic sull'applicazione di cui si desidera modificare le impostazioni.
- 2 Selezionare un elemento nella sezione **Tipo applicazione**.
 - Generico
 - CD/DVD
 - Archiviazione cloud

È possibile apportare le modifiche a questa selezione solo se si sta modificando un'applicazione definita dall'utente.

3 Selezionare gli elementi nella sezione **Configurazione controllo applicazioni** :

Destinazioni	Archivi rimovibili	Controlla il passaggio di dati tra dispositivi di archiviazione rimovibili e l'applicazione.
	Stampa/Fax	Monitora i dati stampati o inviati via fax.
	Unità locali	Monitora i dati che passano tra i dischi locali e un'applicazione.
Appunti	Appunti, Copia	Monitora i dati copiati negli Appunti dell'endpoint. Nota: Se si è attivato il controllo HTTPS per Google Chrome, si consiglia di lasciare il monitoraggio di Incolla disattivato per evitare la duplicazione degli incidenti. L'attivazione del controllo HTTPS per Google Chrome attiva automaticamente il monitoraggio di Incollamento appunti.
	Appunti, Incolla	Monitora i dati incollati dagli Appunti.
Web	HTTP	Monitora i dati trasferiti sulla rete tramite HTTP.
	FTP	Monitora i dati trasferiti sulla rete tramite FTP.

Accesso ai file di applicazione	Accesso ai file di applicazione, Apri	<p>Selezionare Accesso ai file di applicazione, Apri per monitorare i file aperti dall'applicazione.</p> <p>Selezionare l'opzione Apri file solo se l'applicazione si blocca o si arresta.</p> <p>Quando questa opzione è selezionata, l'applicazione non apre un file se contiene informazioni riservate. Tuttavia Symantec Data Loss Prevention esegue la scansione del file indipendentemente dal fatto che l'applicazione legga il contenuto, il che riduce le prestazioni.</p> <p>Nota: Se si è attivato il controllo HTTPS per Google Chrome, si consiglia di lasciare questa impostazione disattivata per evitare la duplicazione degli incidenti. L'attivazione del controllo HTTPS per Google Chrome attiva automaticamente il controllo delle applicazioni.</p> <p>Vedere "Informazioni sul monitoraggio Accesso ai file di applicazione" a pagina 2245.</p>
	Accesso ai file di applicazione, Leggi	<p>Selezionare l'opzione Accesso ai file di applicazione, Leggi per monitorare i contenuti dei file quando l'applicazione legge il file. Questa selezione è consigliata perché fornisce le prestazioni migliori.</p>
Condivisioni di rete	Copia in condivisione di rete	<p>Selezionare per monitorare i file copiati tra una condivisione di rete e un'applicazione.</p>

- 4 Selezionare **Fornisci questo contenuto crittografato dall'applicazione durante la lettura di file ICE** nella sezione **Crittografia incentrata sulle informazioni** per consentire all'applicazione di leggere i file crittografati copiati in un dispositivo di archiviazione rimovibile.

Nota: Questa opzione si applica soltanto alle applicazioni Windows.

Se questa opzione è disattivata per un'applicazione e l'applicazione è utilizzata scaricare un file pre-crittografato in un dispositivo di archiviazione rimovibile, l'applicazione aggiunge un'ulteriore estensione `.html` al nome di questo file. In tal caso, è necessario rimuovere manualmente l'estensione HTML aggiuntiva dal nome del file. Come best practice, Symantec consiglia di selezionare l'opzione **Fornisci questo contenuto crittografato dall'applicazione durante la lettura di file ICE** per tutte le applicazioni.

- 5 Salvare le modifiche.
- 6 Riavviare l'applicazione da controllare. Il riavvio dell'applicazione garantisce che il controllo delle applicazioni non venga interrotto.

Vedere ["Informazioni sul controllo delle applicazioni"](#) a pagina 2231.

Controllo delle applicazioni di messaggistica istantanea su endpoint Mac

Symantec Data Loss Prevention può monitorare i dati incollati sui messaggi istantanei e i file caricati tramite applicazioni di messaggistica istantanea.

Le applicazioni macOS di messaggistica istantanea Skype e Cisco Jabber sono fornite nella schermata **Controllo applicazioni** per impostazione predefinita. È possibile aggiungere ulteriori applicazioni di messaggistica istantanea. Vedere ["Aggiunta di un'applicazione macOS"](#) a pagina 2241.

Per monitorare le applicazioni di messaggistica istantanea

- 1 Attivare il canale **Incolla** da monitorare nella schermata **Configurazione agente**.
Vedere ["Impostazioni di Attiva monitoraggio"](#) a pagina 2113.
- 2 Selezionare **Appunti** e scegliere **Incolla** per l'applicazione di messaggistica istantanea che si desidera monitorare nella schermata **Controllo applicazioni**.

Vedere ["Modifica delle impostazioni di controllo delle applicazioni"](#) a pagina 2232.

Elenco delle applicazioni CD/DVD

La tabella seguente elenca le applicazioni di masterizzazione di CD/DVD visualizzate per impostazione predefinita nella schermata **Controllo applicazioni**. Non è possibile eliminare le applicazioni di masterizzazione predefinite. Se si possiede un'applicazione di masterizzazione di CD/DVD non elencata in tale schermata, è possibile aggiungerla. Vedere ["Aggiunta di un'applicazione Windows"](#) a pagina 2237.

La tabella elenca il nome commerciale delle applicazioni di masterizzazione di CD/DVD di terze parti come pure il nome binario delle versioni specifiche.

Tabella 83-1 Nomi commerciali e nomi binari delle applicazioni di masterizzazione di CD/DVD

Marca	Nome binario
BsCLIP	BsCLiP.exe
B's Recorder GOLD	BSGOLD.exe
BurnAware	burnaware_data.exe

Marca	Nome binario
CheetahBurner	CheetahBurner.exe
CommandBurner	CmdBurn.exe
CopyToDVD	c2cman.exe
CopyToDVD DVD	copytocd.exe
Creator 10	Creator10.exe
DeepBurner	DeepBurner.exe
GEAR per Windows	gear.exe
Mkisofs	mkisofs.exe
Nero	nero.exe
NeroStartSmart	NeroStartSmart.exe
RecordNow	RecordNow.exe
Roxio	Creator.exe
Roxio_Central	Roxio_Central.exe
Roxio5	Creatr50.exe
Roxio Mediahub	Mediahub.exe
SilentNight Microburner	microburner.exe
StarBurn	StarBurn.exe

Nota: Quando si utilizza un masterizzatore di CD/DVD, i file di testo di dimensioni inferiori a 64 byte non sono rilevati durante la masterizzazione su ISO. I file di testo di dimensioni superiori a 64 byte vengono rilevati normalmente.

Informazioni sull'aggiunta di applicazioni

È possibile utilizzare la schermata **Informazioni applicazione** per aggiungere applicazioni alle politiche di monitoraggio. Per impostazione predefinita, i DLP Agent controllano l'attività degli Appunti, di stampa, di rete (HTTP e FTP) e del file system (disco rimovibile, unità locale e condivisione di rete) per tutte le applicazioni. Aggiungere applicazioni se si desidera che i DLP Agent controllino i file aperti o letti da tali applicazioni. È anche possibile aggiungere

applicazioni quando si desidera impedire a Symantec Data Loss Prevention il monitoraggio dell'applicazione.

La seguente tabella elenca i tipi di applicazioni che è possibile aggiungere:

Tabella 83-2 Tipi di applicazioni che è possibile aggiungere

Tipo di applicazione	Esempio
CD/DVD	InfraRecorder
Browser Internet	Opera
Messaggeria istantanea	Viber
SMTP	Mozilla Thunderbird
Sincronizzazione cloud	SpiderOak

Vedere ["Aggiunta di un'applicazione Windows"](#) a pagina 2237.

Vedere ["Aggiunta di un'applicazione macOS"](#) a pagina 2241.

Aggiunta di un'applicazione Windows

È possibile aggiungere applicazioni Windows da controllare che non sono già presenti nella schermata **Controllo applicazioni**.

Vedere ["Informazioni sull'aggiunta di applicazioni"](#) a pagina 2236.

Aggiunta di un'applicazione

- 1 Accedere a **Sistema > Agenti > Controllo applicazioni**.
- 2 Fare clic su **Aggiungi applicazione, Windows** per visualizzare la schermata **Informazioni applicazione**.

3 Immettere le informazioni.

Oltre che nel campo **Nome**, è necessario immettere informazioni in almeno uno dei seguenti campi: **Nome binario**, **Nome interno** o **Nome file originale**.

Nota: Se si intende aggiungere un'applicazione Windows 10 (app di Windows), immettere l'ID del pacchetto applicazione in **Nome interno** e lasciare vuoti i campi **Nome binario**, **Nome file originale** e **Nome editore**. L'immissione di informazioni in questi campi potrebbe causare l'arresto del monitoraggio dell'applicazione da parte di DLP Agent dopo un upgrade del sistema.

Vedere ["Utilizzo dello strumento GetAppInfo"](#) a pagina 2240.

Nome	Digitare il nome dell'applicazione. Questo campo è obbligatorio.
Nome binario	Digitare il nome del file binario. Includere un carattere di escape (\) tra il nome dell'applicazione e l'estensione di file. Ad esempio, se si intende aggiungere Firefox, digitare firefox\exe .
Nome interno	Digitare il nome dell'applicazione.
Nome file originale	Digitare il nome di file dell'applicazione. Includere un carattere di escape (\) tra il nome dell'applicazione e l'estensione di file. Ad esempio, se si intende aggiungere Firefox, digitare firefox\exe .
Nome editore	<p>Digitare il nome dell'editore. Questo campo è facoltativo.</p> <p>Se si immette il nome dell'editore, è possibile selezionare l'opzione Verifica nome editore. Questa opzione verifica la correttezza del nome dell'editore dell'applicazione. L'uso dell'opzione Verifica nome editore può influire sulle prestazioni in quanto aumenta le risorse di sistema.</p> <p>È inoltre possibile aggiungere dettagli sul nome dell'editore per l'applicazione. Il nome dell'editore indica il produttore del software. L'aggiunta del nome dell'editore consente a Symantec Data Loss Prevention di verificare l'applicazione anche se il nome binario è stato cambiato. Il nome dell'editore è usato soprattutto per identificare i processi di Symantec. È tuttavia possibile aggiungere il nome dell'editore per qualsiasi delle applicazioni in uso. L'aggiunta del nome dell'editore è facoltativa.</p>

4 Selezionare un elemento nella sezione **Tipo applicazione**.

- **Generico**
- **CD/DVD**
- **Archiviazione cloud**

5 Selezionare gli elementi nella sezione **Configurazione controllo applicazioni** :

Destinazioni	Archivi rimovibili	Controlla il passaggio di dati tra dispositivi di archiviazione rimovibili e l'applicazione.
	Stampa/Fax	Monitora i dati stampati o inviati via fax.
	Unità locali	Monitora i dati che passano tra i dischi locali e un'applicazione.
Appunti	Appunti, Copia	Monitora i dati copiati negli Appunti dell'endpoint. Nota: Se si è attivato il controllo HTTPS per Google Chrome, si consiglia di lasciare il monitoraggio di Incolla disattivato per evitare la duplicazione degli incidenti. L'attivazione del controllo HTTPS per Google Chrome attiva automaticamente il monitoraggio di Incollamento appunti.
	Appunti, Incolla	Monitora i dati incollati dagli Appunti.
Web	HTTP	Monitora i dati trasferiti sulla rete tramite HTTP.
	FTP	Monitora i dati trasferiti sulla rete tramite FTP.

Accesso ai file di applicazione	Accesso ai file di applicazione, Apri	<p>Selezionare Accesso ai file di applicazione, Apri per monitorare i file aperti dall'applicazione.</p> <p>Selezionare l'opzione Apri file solo se l'applicazione si blocca o si arresta.</p> <p>Quando questa opzione è selezionata, l'applicazione non apre un file se contiene informazioni riservate. Tuttavia Symantec Data Loss Prevention esegue la scansione del file indipendentemente dal fatto che l'applicazione legga il contenuto, il che riduce le prestazioni.</p> <p>Nota: Se si è attivato il controllo HTTPS per Google Chrome, si consiglia di lasciare questa impostazione disattivata per evitare la duplicazione degli incidenti. L'attivazione del controllo HTTPS per Google Chrome attiva automaticamente il controllo delle applicazioni.</p> <p>Vedere "Informazioni sul monitoraggio Accesso ai file di applicazione" a pagina 2245.</p>
	Accesso ai file di applicazione, Leggi	<p>Selezionare l'opzione Accesso ai file di applicazione, Leggi per monitorare i contenuti dei file quando l'applicazione legge il file. Questa selezione è consigliata perché fornisce le prestazioni migliori.</p>
Condivisioni di rete	Copia in condivisione di rete	<p>Selezionare per monitorare i file copiati tra una condivisione di rete e un'applicazione.</p>

- 6 Salvare le modifiche.
- 7 Riavviare l'applicazione da controllare. Il riavvio dell'applicazione garantisce che il controllo delle applicazioni non venga interrotto.

Vedere ["Informazioni sul controllo delle applicazioni"](#) a pagina 2231.

Utilizzo dello strumento GetAppInfo

È possibile utilizzare lo strumento `GetAppInfo.exe` per generare informazioni sull'applicazione. Ricorrere a questo strumento quando si aggiungono applicazioni e si utilizza la funzionalità Controllo applicazioni. La funzionalità Controllo applicazioni controlla i dati che gli utenti trasferiscono nelle applicazioni.

Individuare questa applicazione in `SymantecDLPWinAgentTools_14.0.zip` nella directory `DLP\Symantec_DLP_14_Win\14.0_Win\Endpoint\%x86 O %x64`.

Per utilizzare lo strumento GetAppInfo

- 1 Avviare `GetAppInfo.exe`.
- 2 Immettere il percorso dell'applicazione o fare clic su **Sfoglia** e selezionarlo.
- 3 Fare clic su **Get Info**.

Lo strumento consente di visualizzare le informazioni sull'applicazione riportate di seguito:

- Commenti
 - Nome interno
 - Nome della società
 - Copyright
 - Versione del prodotto
 - Descrizione del file
 - Marchi di fabbrica legali
 - Build privata
 - Versione del file
 - Nome di file originale
 - Build speciale
 - Nome dell'autore
- 4 Conservare le informazioni sull'applicazione visualizzate dallo strumento. Utilizzare le informazioni sull'applicazione quando si aggiunge un'applicazione nella schermata Controllo applicazioni.

Vedere ["Aggiunta di un'applicazione Windows"](#) a pagina 2237.

Vedere ["Informazioni sul monitoraggio Accesso ai file di applicazione"](#) a pagina 2245.

Aggiunta di un'applicazione macOS

È possibile aggiungere applicazioni macOS a 64 bit da controllare che non sono già presenti nella schermata **Controllo applicazioni**.

Vedere ["Informazioni sull'aggiunta di applicazioni"](#) a pagina 2236.

Aggiunta di un'applicazione

- 1 Accedere a **Sistema > Agenti > Controllo applicazioni**.
- 2 Fare clic su **Aggiungi applicazione, Mac** per visualizzare la schermata **Informazioni applicazione**.

3 Immettere le informazioni.

Oltre che nel campo **Nome**, è necessario immettere informazioni nel campo **Nome binario**. Non immettere informazioni nei campi **Nome interno** o **Nome file originale** per le applicazioni macOS.

- **Nome**

- **Nome binario**

Vedere "[Definizione dei nomi binari delle applicazioni macOS](#)" a pagina 2244.

4 Selezionare **Generico** nella sezione **Tipo applicazione**.

5 Selezionare gli elementi nella sezione **Configurazione controllo applicazioni** :

Nota: solo gli elementi elencati nella tabella sono supportati per il controllo delle applicazioni sugli endpoint Mac.

Destinazioni	Archivi rimovibili	Controlla il passaggio di dati tra dispositivi di archiviazione rimovibili e l'applicazione.
Appunti	Appunti, Incolla	Monitora i dati incollati dagli Appunti.
Accesso ai file di applicazione	Accesso ai file di applicazione, Apri	<p>Selezionare Accesso ai file di applicazione, Apri per monitorare i file aperti dall'applicazione.</p> <p>Selezionare l'opzione Apri file solo se l'applicazione si blocca o si arresta.</p> <p>Quando questa opzione è selezionata, l'applicazione non apre un file se contiene informazioni riservate. Tuttavia Symantec Data Loss Prevention esegue la scansione del file indipendentemente dal fatto che l'applicazione legga il contenuto, il che riduce le prestazioni.</p> <p>Nota: Se si è attivato il controllo HTTPS per Google Chrome, si consiglia di lasciare questa impostazione disattivata per evitare la duplicazione degli incidenti. L'attivazione del controllo HTTPS per Google Chrome attiva automaticamente il controllo delle applicazioni.</p> <p>Vedere "Informazioni sul monitoraggio Accesso ai file di applicazione" a pagina 2245.</p>
Condivisioni di rete	Copia in condivisione di rete	Selezionare per monitorare i file copiati tra una condivisione di rete e un'applicazione.

- 6 Salvare le modifiche.
- 7 Riavviare l'applicazione da controllare. Il riavvio dell'applicazione garantisce che il controllo delle applicazioni non venga interrotto.

Definizione dei nomi binari delle applicazioni macOS

Quando si desidera monitorare le applicazioni macOS, aggiungerle alla schermata Controllo applicazioni utilizzando i nomi binari dell'applicazione.

Nota: Esaminare le informazioni di supporto per un riepilogo delle funzionalità e del supporto di monitoraggio degli Appunti. Vedere ["Funzionalità degli Appunti supportate su agenti Mac"](#) a pagina 2051.

Per definire i nomi binari dell'applicazione per un'applicazione macOS:

1. Eseguire l'applicazione da monitorare.
2. Avviare l'applicazione di controllo dell'attività.
3. Immettere il nome dell'applicazione da monitorare nel campo di ricerca nella parte superiore destra.

Nota: DLP Agent monitora solo le operazioni di Incollamento appunti per applicazioni macOS a 64 bit. Confermare che l'applicazione che si desidera aggiungere mostri **64 bit** nella colonna **Tipo** se si desidera monitorare il canale Incollamento appunti.

4. Fare doppio clic sull'applicazione nella colonna **Nome processo** per visualizzare una finestra di dialogo. La finestra di dialogo fornisce file di apertura, statistiche e memoria e informazioni sulle porte per l'applicazione.
5. Fare clic sulla scheda **Apri file e porte** per visualizzare dettagli sull'applicazione.
6. Individuare la riga in cui è visualizzato il percorso per l'applicazione. Ad esempio, il percorso per Safari è `/Applications/Safari.app/Contents/MacOS/Safari`.
7. Individuare e annotare il nome binario che segue `/MacOS/`.
8. Immettere il nome binario nel campo **Nome binario** della schermata **Sistema > Agenti > Controllo applicazioni**.

Vedere ["Aggiunta di un'applicazione macOS"](#) a pagina 2241.

Come ignorare applicazioni macOS

È possibile configurare Symantec Data Loss Prevention in modo che ignori le applicazioni macOS che si bloccano o si arrestano a causa del monitoraggio. Solitamente si configura Symantec Data Loss Prevention in modo che ignori solo le applicazioni che l'azienda identifica come critiche dal punto di vista aziendale. Ignorare questi tipi di applicazioni fa sì che funzionino correttamente. Tuttavia ignorare le applicazioni comporta anche il rischio di perdita di dati.

Nota: Per impostazione predefinita, Microsoft Excel e Adobe Reader sono ignorati dal monitoraggio sugli endpoint Mac.

Per escludere le applicazioni macOS dal monitoraggio:

- 1 Registrare il nome dell'applicazione e il nome binario dell'applicazione che si desidera venga ignorata da Symantec Data Loss Prevention.

Per ottenere queste informazioni, aprire l'applicazione su un endpoint Mac e individuare le informazioni necessarie nella schermata di **controllo delle attività**.
- 2 Accedere a **Sistema > Agenti > Controllo applicazioni**.
- 3 Fare clic su **Aggiungi applicazione**.
- 4 Immettere il nome dell'applicazione nel campo **Nome**.
- 5 Immettere il nome binario nel campo **Nome binario**.
- 6 Selezionare **Generico** nell'elenco **Tipo applicazione**. Non effettuare altre selezioni.
- 7 Lasciare tutte le altre selezioni disattivate.
- 8 Salvare le modifiche.

Symantec Data Loss Prevention ignora l'applicazione specificata subito dopo avere salvato le modifiche.

Informazioni sul monitoraggio Accesso ai file di applicazione

Quando si attiva la funzionalità Accesso ai file di applicazione, DLP Agent esegue il monitoraggio dei dati in uscita dalle applicazioni sugli endpoint. Per attivare questa funzionalità si aggiunge il protocollo con etichetta Monitoraggio protocollo o endpoint e si impostano regole di risposta in una politica. Quindi si attiva la funzionalità Accesso ai file di applicazione nella configurazione dell'agente.

Nota: Non è possibile usare la funzionalità Accesso ai file di applicazione per monitorare i trasferimenti di dati in linea tramite browser (HTTPS) o messaggistica istantanea.

È possibile attivare le applicazioni predefinite nella schermata **Controllo applicazioni**. È anche possibile impostare Symantec Data Loss Prevention per il monitoraggio delle applicazioni non trovate nella schermata **Controllo applicazioni** aggiungendo tali applicazioni.

Se un utente trasferisce un file che contiene informazioni riservate, l'endpoint visualizza una notifica. A seconda delle politiche attive e della risposta Endpoint Prevent, è possibile che non venga consentito l'accesso al file. È possibile esaminare gli incidenti di Accesso ai file di applicazione nella schermata **Incidenti > Endpoint**.

Vedere ["Implementazione del monitoraggio Accesso ai file di applicazione"](#) a pagina 2246.

Vedere ["Aggiunta e modifica di configurazioni agente"](#) a pagina 2111.

Vedere ["Aggiunta di un'applicazione Windows"](#) a pagina 2237.

Implementazione del monitoraggio Accesso ai file di applicazione

L'implementazione della funzionalità Accesso ai file di applicazione è una procedura in vari passaggi. Vedere [Tabella 83-3](#) a pagina 2246.

Potenzialmente l'attivazione della funzionalità riduce le prestazioni dell'applicazione negli endpoint. È possibile utilizzare variabili di ambiente nei filtri del percorso per specificare le posizioni di file da monitorare, migliorando le prestazioni dell'applicazione.

Vedere ["Utilizzo delle variabili di ambiente nelle scansioni Endpoint Discover"](#) a pagina 2100.

Tabella 83-3 Implementazione di Accesso ai file di applicazione

Passaggio	Azione	Descrizione
1	Creare una nuova politica o aggiornare una politica esistente.	Attivare il protocollo Monitoraggio protocollo o endpoint, quindi selezionare opzioni per configurare Accesso ai file di applicazione. Vedere "Configurazione di regole di politica" a pagina 427.
2	Definire regole di risposta per la politica.	Vedere "Gestione di regole di risposta" a pagina 1489.
3	Creare un gruppo di politiche distribuito in un Endpoint Server.	Vedere "Gruppi di politiche" a pagina 377.

Passaggio	Azione	Descrizione
4	Attivare la funzionalità Accesso ai file di applicazione nella configurazione dell'endpoint.	<p>Utilizzare filtri di ambiente, file e cartella per ottimizzare le prestazioni del monitoraggio di file. La funzionalità Accesso ai file di applicazione esegue il monitoraggio di tutti i file aperti o letti da un'applicazione. Ciò può ridurre le prestazioni dell'applicazione e creare falsi positivi. È possibile usare le variabili di ambiente per specificare posizioni in cui potrebbero trovarsi i dati riservati.</p> <p>Vedere "Aggiunta e modifica di configurazioni agente" a pagina 2111.</p> <p>Vedere "Configurazione dei filtri di file" a pagina 2117.</p>
5	Aggiungere un'applicazione dalla schermata Controllo applicazioni.	<p>Molte applicazioni sono elencate nella schermata Controllo applicazioni. Se si aggiunge un'applicazione, è necessario attivare la funzionalità di monitoraggio Accesso ai file di applicazione e selezionare un'attività da monitorare, Leggere o Apri.</p> <p>Vedere "Aggiunta di un'applicazione Windows" a pagina 2237.</p>

Utilizzo di Endpoint FlexResponse

Il capitolo contiene i seguenti argomenti:

- [Informazioni su Endpoint FlexResponse](#)
- [Distribuzione di Endpoint FlexResponse](#)
- [Informazioni sulla distribuzione di plug-in Endpoint FlexResponse agli endpoint](#)
- [Distribuzione dei plug-in di Endpoint FlexResponse con una procedura di installazione invisibile](#)
- [Informazioni sull'utilità Endpoint FlexResponse](#)
- [Distribuzione del plug-in Endpoint FlexResponse mediante l'utilità Endpoint FlexResponse](#)
- [Attivazione di Endpoint FlexResponse su Enforce Server](#)
- [Disinstallazione di un plug-in Endpoint FlexResponse mediante l'utilità Endpoint FlexResponse](#)
- [Recupero di un plug-in Endpoint FlexResponse da un endpoint specifico](#)
- [Recupero di un elenco di plug-in di Endpoint FlexResponse da un endpoint](#)

Informazioni su Endpoint FlexResponse

Symantec Data Loss Prevention fornisce un set di azioni di regole di risposta che è possibile specificare per riparare un incidente. Queste azioni includono registrazione, invio di un'e-mail, blocco di un'azione dell'utente finale, notifica a un utente e altre risposte.

È anche possibile utilizzare il plug-in Endpoint FlexResponse per fornire azioni di risposta supplementari. Questi plug-in contengono istruzioni personalizzate per azioni di riparazione

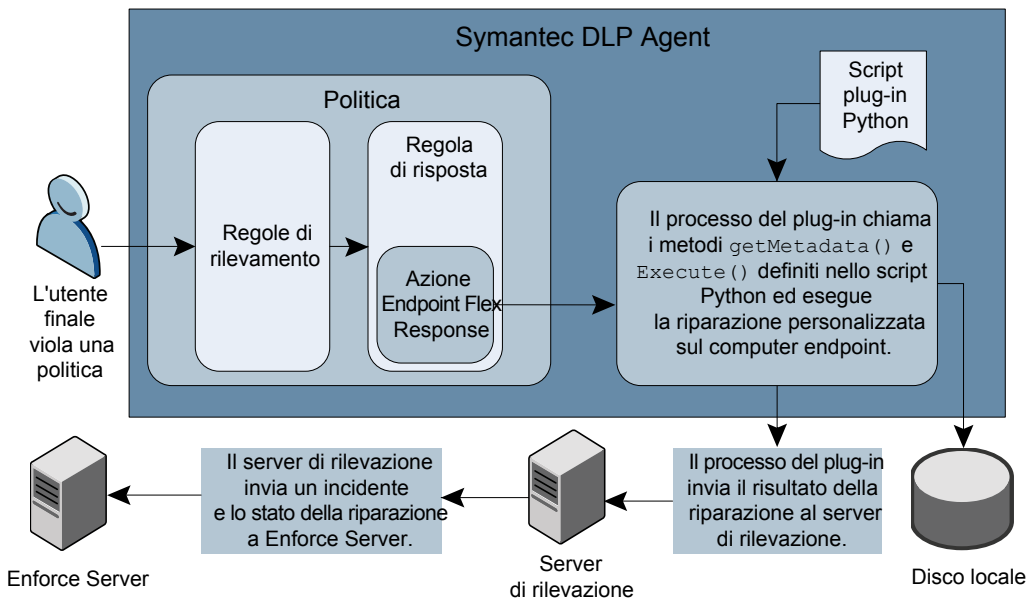
eseguite negli endpoint. Le regole di Endpoint FlexResponse sono applicabili solo alle regole di risposta automatiche. Non è possibile creare azioni di regole di Endpoint FlexResponse per regole di risposta smart.

I clienti di Symantec Data Loss Prevention possono contattare Symantec o i partner Symantec per ottenere i plug-in di Endpoint FlexResponse. Inoltre, gli sviluppatori che conoscono il linguaggio di programmazione Python possono creare script personalizzati per plug-in di Endpoint FlexResponse utilizzando una API fornita da Symantec. Queste azioni di riparazione personalizzate possono includere crittografia, applicazione di DRM o revisione di informazioni riservate.

L'utilità Endpoint FlexResponse consente di distribuire i plug-in di Endpoint FlexResponse su endpoint di Symantec Data Loss Prevention in cui sono necessarie azioni di Endpoint FlexResponse. È possibile distribuire manualmente i plug-in mediante l'utilità Endpoint FlexResponse, oppure utilizzare il software SMS (System Management Software, software di gestione del sistema) per distribuire l'utilità e quindi i plug-in. Dopo la distribuzione di un plug-in di Endpoint FlexResponse su un endpoint, utilizzare la console di amministrazione di Enforce Server per aggiungere un'azione **Endpoint: FlexResponse** a una regola di risposta e quindi aggiungere la regola di risposta a una politica attiva.

Figura 84-1 mostra la sequenza delle attività che generano un'azione di Endpoint FlexResponse.

Figura 84-1 Processo dei plug-in di Endpoint FlexResponse



È possibile utilizzare le regole di Endpoint FlexResponse sui seguenti tipi di destinazioni e protocolli di endpoint:

- Endpoint Discover

Nota: Endpoint FlexResponse non è attualmente disponibile per le scansioni di Endpoint Discover eseguite su agenti Mac.

- Monitoraggio dell'unità locale
- Dispositivi di archiviazione rimovibili
- SMTP
- HTTP(S)

Distribuzione di Endpoint FlexResponse

Attenersi alla procedura illustrata di seguito per distribuire i plug-in Endpoint FlexResponse.

Tabella 84-1 Distribuzione di Endpoint FlexResponse

Passaggio	Azione	Descrizione
Passaggio 1	Ottenere o creare un file zip del plug-in Endpoint FlexResponse.	Contattare un partner o un rappresentante Symantec. I plug-in Endpoint FlexResponse non sono disponibili con l'installazione predefinita di Symantec Data Loss Prevention.
Passaggio 2	Configurare le credenziali Endpoint sul server Enforce Server.	Vedere "Configurazione delle credenziali endpoint" a pagina 168. Questo passaggio è facoltativo.
Passaggio 3	Distribuire il plug-in agli endpoint mediante l'utilità Endpoint FlexResponse e software di gestione sistemi (SMS) di terzi.	Vedere "Informazioni sulla distribuzione di plug-in Endpoint FlexResponse agli endpoint" a pagina 2251.
Passaggio 4	Attivare le azioni Endpoint FlexResponse sul server Enforce Server.	Vedere "Attivazione di Endpoint FlexResponse su Enforce Server" a pagina 2255.
Passaggio 5	Aggiungere le azioni Endpoint FlexResponse alle regole di risposta.	Vedere "Aggiunta di una nuova regola di risposta" a pagina 1490.

Informazioni sulla distribuzione di plug-in Endpoint FlexResponse agli endpoint

È necessario installare Symantec DLP Agent sugli endpoint prima di distribuire i plug-in Endpoint FlexResponse. Gli agenti devono essere connessi a un Endpoint Server attivo.

Vedere *Manuale di installazione di Symantec Data Loss Prevention* per informazioni sull'installazione degli agenti.

È necessario distribuire i plug-in Endpoint FlexResponse su ciascun endpoint in cui sono necessarie azioni Endpoint FlexResponse. È possibile distribuire il plug-in con un'installazione manuale o un'installazione invisibile. I metodi di installazione invisibile richiedono l'uso di software di gestione sistemi (SMS) per distribuire e installare il software in tutti gli endpoint. Potrebbe essere necessario creare script SMS per accedere alla cartella di installazione.

Questa sezione presuppone che si sia creato o ottenuto con altro metodo un plug-in Endpoint FlexResponse compresso in un file ZIP.

La distribuzione del plug-in Endpoint FlexResponse negli endpoint richiede i seguenti passaggi:

- | | |
|-------------|---|
| Passaggio 1 | Copiare l'utilità Endpoint FlexResponse negli endpoint.
Vedere "Informazioni sull'utilità Endpoint FlexResponse" a pagina 2252. |
| Passaggio 2 | Copiare i moduli Python di terzi richiesti dal plug-in negli endpoint. |
| Passaggio 3 | Attivare Endpoint FlexResponse in Enforce Server. Vedere "Attivazione di Endpoint FlexResponse su Enforce Server" a pagina 2255. |
| Passaggio 4 | <p>Distribuire il plug-in Endpoint FlexResponse mediante l'utilità Endpoint FlexResponse. (<code>flrinst.exe</code>). Utilizzare una delle opzioni seguenti:</p> <ul style="list-style-type: none"> ■ Distribuire manualmente il plug-in su un singolo endpoint. Questa opzione è più utile quando si sviluppa o si testa un plug-in Endpoint FlexResponse.
Vedere "Distribuzione del plug-in Endpoint FlexResponse mediante l'utilità Endpoint FlexResponse" a pagina 2254. ■ Distribuire il plug-in utilizzando un processo di installazione invisibile e software SMS. Questa opzione è più utile quando si sta distribuendo un plug-in Endpoint FlexResponse pronto per la produzione.
Vedere "Distribuzione dei plug-in di Endpoint FlexResponse con una procedura di installazione invisibile" a pagina 2252. |
| Passaggio 5 | <p>Creare regole di risposta che utilizzano azioni Endpoint: FlexResponse che fanno riferimento al plug-in e aggiungere tali regole a una politica attiva.</p> <p>Vedere "Implementazione del rilevamento delle politiche" nel <i>Manuale dell'amministratore di sistema di Symantec Data Loss Prevention</i>.</p> |

Distribuzione dei plug-in di Endpoint FlexResponse con una procedura di installazione invisibile

È possibile utilizzare il software SMS (System Management Software, software di gestione del sistema) per distribuire i plug-in di Endpoint FlexResponse su più endpoint. Sebbene i dettagli della creazione di script di installazione per il software SMS non rientrino nell'ambito del presente documento, tenere presente i requisiti seguenti:

- È necessario installare i Symantec DLP Agent sugli endpoint prima di distribuire i plug-in di Endpoint FlexResponse. Gli agenti devono essere connessi a un Endpoint Server attivo.
- È necessario installare l'utilità Endpoint FlexResponse (`flrininst.exe`) su ciascun endpoint su cui si distribuiranno i plug-in di Endpoint FlexResponse.
- È necessario rendere disponibile a ciascun endpoint il pacchetto Endpoint FlexResponse (file `.zip`). È possibile copiare il pacchetto su ciascun endpoint o renderlo disponibile su un'unità di rete accessibile da tutti gli endpoint.
- Per distribuire il plug-in, utilizzare le opzioni della riga di comando dell'utilità Endpoint FlexResponse quando si creano gli script di installazione. Vedere [Tabella 84-3](#) a pagina 2253.
- Rimuovere l'utilità Endpoint FlexResponse dopo avere distribuito il plug-in. Se si lascia l'utilità installata sugli endpoint, un utente malintenzionato può utilizzare l'utilità per disinstallare o modificare il plug-in di Endpoint FlexResponse.

Vedere ["Informazioni sull'utilità Endpoint FlexResponse"](#) a pagina 2252.

Per ulteriori informazioni sulla distribuzione con il software SMS, consultare la documentazione dell'applicazione SMS.

L'utilità Endpoint FlexResponse è disponibile solo presso Symantec o i partner Symantec. Non è inclusa con la distribuzione di Symantec Data Loss Prevention.

Informazioni sull'utilità Endpoint FlexResponse

L'utilità Endpoint FlexResponse consente di gestire i plug-in Endpoint FlexResponse. L'utilità Endpoint FlexResponse non fa parte del download Symantec Data Loss Prevention predefinito ed è disponibile solo presso Symantec o i partner Symantec.

Prima di eseguire l'utilità, comprimere gli script Python in un unico file ZIP.

Tabella 84-2 Azioni dell'utilità Endpoint FlexResponse

Azione	Descrizione
Distribuzione (installazione) di plug-in	Utilizzare l'opzione <code>install</code> per distribuire i plug-in in un endpoint.

Azione	Descrizione
Disinstallazione di plug-in	Utilizzare l'opzione <code>uninstall</code> per disinstallare i plug-in da un endpoint.
Recupero dei plug-in distribuiti	Utilizzare l'opzione <code>retrieve</code> per recuperare un plug-in specifico che è già stato distribuito su un endpoint.
Vedere l'elenco dei plug-in distribuiti	Utilizzare l'opzione <code>list</code> per recuperare un elenco di tutti i plug-in distribuiti in un endpoint specifico. L'elenco include i nomi dei plug-in distribuiti.

L'utilità Endpoint FlexResponse va eseguita dalla cartella in cui è distribuito Symantec DLP Agent. La posizione di questa cartella è configurabile. Per impostazione predefinita, la directory si trova nel percorso:

`C:\Programmi\Manufacturer\Endpoint Agent\`

Il nome dell'utilità è `flrinst.exe`. L'utilità usa la seguente sintassi:

```
flrinst.exe -op=install|uninstall|retrieve|list -package=<nome_pacchetto>
-p=<password_Tools>
```

Tabella 84-3 Opzioni dell'utilità Endpoint FlexResponse

Opzione	Descrizione
<code>-op=install uninstall retrieve list</code>	Utilizzare uno dei seguenti argomenti: <ul style="list-style-type: none"> ■ <code>install</code>: distribuisce un plug-in ■ <code>uninstall</code>: rimuove un plug-in ■ <code>list</code>: visualizza un elenco di plug-in distribuiti ■ <code>retrieve</code>: recupera un plug-in e lo salva come file di testo modificabile. Il file di testo è incluso in un file ZIP salvato nel directory in cui è stata eseguita l'utilità.
<code>-package=<nome_pacchetto></code>	Quando si specifica l'opzione <code>-op=install</code> , specifica il percorso al pacchetto (file ZIP) contenente il plug-in Endpoint FlexResponse. Il nome del pacchetto esegue la distinzione tra maiuscole e minuscole. Quando si specifica l'opzione <code>-op=retrieve</code> o <code>-op=uninstall</code> , specifica il nome del pacchetto.

Opzione	Descrizione
<code>-p=<password_Tools></code>	<p>Specificare la password strumenti configurata per la distribuzione di Symantec Data Loss Prevention.</p> <p>Se una password strumento non è stata configurata, usare la password predefinita "VontuStop".</p> <p>Nota: A partire da Symantec Data Loss Prevention versione 11.1.1 la password non è più facoltativa.</p>

Se è stata creata una password strumenti per la distribuzione di Symantec Data Loss Prevention, è possibile trasferire tale password all'utilità Endpoint FlexResponse mediante l'opzione `-p`. Questa password è necessaria per installare e disinstallare un plug-in. La password strumenti viene configurata durante l'installazione di Symantec Data Loss Prevention. Per ulteriori informazioni, consultare il *Manuale di installazione di Symantec Data Loss Prevention*.

Se non è stata configurata una password strumenti, un utente finale può recuperare e modificare plug-in installati in precedenza mediante la password predefinita, `VontuStop`. Symantec consiglia di configurare una password strumenti per impedire tale tipo di accesso. In alternativa è possibile impostare l'applicazione SMS in modo da rimuovere l'utilità Endpoint FlexResponse dopo l'uso. L'eliminazione dell'utilità impedisce le modifiche o la disinstallazione non autorizzata dei plug-in.

Distribuzione del plug-in Endpoint FlexResponse mediante l'utilità Endpoint FlexResponse

L'utilità Endpoint FlexResponse consente di distribuire i plug-in Endpoint FlexResponse. I plug-in devono essere in formato `.zip`.

Per distribuire un plug-in Endpoint FlexResponse

- 1 In un endpoint, aprire una finestra dei comandi e raggiungere la directory degli strumenti di installazione di Symantec DLP Agent. Il percorso predefinito di questa directory è
`C:\Program Files\Manufacturer\Endpoint Agent\`
- 2 Immettere il seguente comando:

```
flrinst.exe -op=install
           -package=<path_to_plugin>
           -p=<myToolsPassword>
```

Dove:

- `<myToolsPassword>` è la password strumenti per la distribuzione di Symantec Data Loss Prevention. Se non è stata specificata una password per Strumenti, utilizzare la password predefinita: `VontuStop`.
- `<path_to_plugin_name>` è il percorso completo del file `.zip` del plug-in.

Ad esempio:

```
flrinst -op=install -package=C:\installs\myFlexResponse_plugin.zip
-p=myToolsPassword
```

Vedere ["Distribuzione di Endpoint FlexResponse"](#) a pagina 2250.

Vedere ["Informazioni sull'utilità Endpoint FlexResponse"](#) a pagina 2252.

Attivazione di Endpoint FlexResponse su Enforce Server

Prima di poter utilizzare i plug-in di Endpoint FlexResponse nelle regole di risposta, è necessario attivare la funzionalità Endpoint FlexResponse tramite Enforce Server. Per impostazione predefinita, la funzionalità Endpoint FlexResponse non è attivata. Attivare la funzionalità Endpoint FlexResponse in **Impostazioni agente avanzate**.

Per attivare la funzionalità Endpoint FlexResponse

- 1 Accedere alla console di amministrazione di Enforce Server, selezionare **Sistema > Agenti > Configurazione agente** e aprire la configurazione dell'agente attualmente applicata all'Endpoint Server connesso agli agenti dove si sta distribuendo il plug-in di Endpoint FlexResponse.
- 2 Fare clic sulla scheda **Impostazioni agente avanzate**.
- 3 Individuare l'impostazione `PostProcessor.ENABLE_FLEXRESPONSE.int`.
- 4 Modificarla e impostarla su **1**.
- 5 Fare clic su **Salva e applica**.

Vedere ["Aggiunta di una nuova regola di risposta"](#) a pagina 1490.

Vedere ["Distribuzione di Endpoint FlexResponse"](#) a pagina 2250.

Vedere ["Informazioni sulla distribuzione di plug-in Endpoint FlexResponse agli endpoint"](#) a pagina 2251.

Disinstallazione di un plug-in Endpoint FlexResponse mediante l'utility Endpoint FlexResponse

Per disinstallare un plug-in Endpoint FlexResponse da un endpoint

- 1 In un endpoint, aprire una finestra di comando e accedere alla directory di installazione di Symantec DLP Agent. Il percorso predefinito della directory è:

C:\Programmi\Manufacturer\agente di endpoint.

- 2 Immettere il seguente comando:

```
flrinst.exe -op=uninstall  
            -package=<Plug-in name>  
            -p=<myToolsPassword>
```

Dove:

- <Plug-in name> è il nome del file .zip del pacchetto del plug-in.
- <myToolsPassword> è la password di strumenti per la distribuzione Symantec Data Loss Prevention. Se non è stata specificata una password per Strumenti, utilizzare la password predefinita: VontuStop.

Ad esempio:

```
flrinst -op=uninstall -package=myFlexResponse_plugin.zip  
-p=myToolsPassword
```

Recupero di un plug-in Endpoint FlexResponse da un endpoint specifico

Per recuperare un plug-in specifico da un endpoint, seguire la procedura descritta di seguito. È possibile utilizzare la funzione di recupero solo su un endpoint alla volta. Il plug-in viene visualizzato nella directory di installazione di Symantec DLP Agent come file .zip. Lo script del plug-in è un file di testo con l'estensione .py ed è situato in un file .zip.

Per modificare il plug-in, modificare il file .py. Se si apportano modifiche, è necessario comprimere di nuovo il file ZIP e ridistribuire il plug-in all'endpoint affinché le modifiche abbiano effetto. I plug-in modificati interessano solo i singoli endpoint in cui sono stati modificati.

Per recuperare un plug-in Endpoint FlexResponse da un endpoint specifico

- 1 Sull'endpoint aprire una finestra per il prompt dei comandi e accedere alla directory di installazione di Symantec DLP Agent:

Il percorso predefinito della directory è `c:\Programmi\Manufacturer\Endpoint Agent\`.

- 2 Immettere il comando seguente:

```
flrinstr -op=retrieve -package=<Nome plug-in> -p=<Password strumenti>
```

dove:

- *<Password strumenti>* è la password degli strumenti per la distribuzione di Symantec Data Loss Prevention. Se non si è specificata una password per gli strumenti, utilizzare la password predefinita: `VontuStop`.
- *<Nome plug-in>* è il nome del file `.zip` del plug-in.

Ad esempio:

```
flrinstr -op=retrieve -package=Plug-in_FlexResponse.zip -p=PasswordStrumenti
```

Recupero di un elenco di plug-in di Endpoint FlexResponse da un endpoint

Per recuperare l'elenco dei plug-in che sono stati distribuiti su un endpoint specifico, seguire la procedura descritta. È possibile utilizzare la funzione di elenco solo con i singoli endpoint. Non è possibile utilizzare la funzione di elenco con un set di endpoint.

L'elenco di plug-in contiene solo il nome del pacchetto di plug-in. L'elenco non contiene alcun tipo di descrizione dei plug-in. Symantec consiglia di utilizzare nomi descrittivi per i plug-in in modo che sia possibile riconoscerli nell'elenco.

Per recuperare l'elenco di plug-in di Endpoint FlexResponse da un endpoint

- 1 Su un endpoint aprire una finestra di comando e accedere alla directory degli strumenti di installazione di Symantec DLP Agent. La posizione predefinita di questa directory è `c:\Programmi\Manufacturer\Endpoint Agent\`.

- 2 Immettere il comando seguente:

```
flrinstr.exe -op=list -p=<Password strumenti>
```

Dove: *<Password strumenti>* è la password degli strumenti per la distribuzione di Symantec Data Loss Prevention. Se non si è specificata una password per gli strumenti, utilizzare la password predefinita: `VontuStop`.

Ad esempio:

```
flrinstr -op=list -p=Password strumenti
```

L'elenco dei plug-in di Endpoint FlexResponse distribuiti viene visualizzato nella finestra di comando.

Utilizzo degli strumenti Endpoint

Il capitolo contiene i seguenti argomenti:

- [Informazioni sugli strumenti di endpoint](#)

Informazioni sugli strumenti di endpoint

Symantec Data Loss Prevention fornisce una serie di strumenti che aiutano a operare con Symantec DLP Agent.

Spostare questi strumenti in una directory sicura. Gli strumenti di endpoint funzionano con il file di archivio chiavi individuato nella directory Installazione agenti. Per funzionare correttamente, gli strumenti e il file di archivio chiavi devono trovarsi nella stessa cartella.

Nota: Prima di copiare gli strumenti di Endpoint nella directory Installazione agenti sugli endpoint Mac, modificare le autorizzazioni di ogni strumento per renderlo eseguibile. Vedere ["Utilizzo degli strumenti Endpoint con macOS"](#) a pagina 2262.

Ogni strumento richiede una password per funzionare. Immettere la password degli strumenti di Endpoint durante il processo di creazione dei pacchetti dell'agente. È possibile gestire la password degli strumenti di Endpoint utilizzando la schermata **Gestione password agente**.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2227.

In [Tabella 85-1](#) sono elencate alcune delle attività che è possibile portare a termine mediante gli strumenti endpoint:

Tabella 85-1 Elenco delle attività degli strumenti di endpoint

Attività	Nome e posizione dello strumento	Ulteriori informazioni
Arrestare l'agente e i servizi watchdog	<p>service_shutdown</p> <p>Disponibile per agenti Windows nel file Symantec_DLP_15.1_Agent_Win-IN.zip.</p> <p>Disponibile per agenti Mac nel file Symantec_DLP_15.1_Agent_Mac-IN.zip.</p>	<p>Vedere "Arresto dell'agente e dei servizi watchdog su endpoint Windows" a pagina 2261.</p> <p>Vedere "Interruzione del servizio dell'agente degli endpoint Mac" a pagina 2262.</p>
Analizzare i file di database a cui accede l'agente	<p>vonu_sqlite3</p> <p>Disponibile per agenti Windows nel file Symantec_DLP_15.1_Agent_Win-IN.zip.</p> <p>Disponibile per agenti Mac nel file Symantec_DLP_15.1_Agent_Mac-IN.zip.</p>	Vedere "Ispezione dei file di database utilizzati dall'agente" a pagina 2263.
Visualizzazione di file di registro estesi	<p>logdump</p> <p>Disponibile per agenti di Windows nel file Symantec_DLP_15.1_Agent_Win-IN.zip.</p> <p>Disponibile per agenti Mac nel file Symantec_DLP_15.1_Agent_Mac-IN.zip.</p>	Vedere "Visualizzazione dei file di registro estesi" a pagina 2265.
Creazione delle informazioni sul dispositivo	<p>DeviceID.exe per dispositivi rimovibili Windows.</p> <p>Disponibile per agenti Windows nel file Symantec_DLP_15.1_Agent_Win-IN.zip.</p> <p>DeviceID per dispositivi rimovibili Mac.</p> <p>Disponibile per agenti Mac nel file Symantec_DLP_15.1_Agent_Mac-IN.zip.</p>	Vedere "Informazioni sulle utilità ID periferica" a pagina 2266.
Creazione di informazioni su applicazioni di terze parti	<p>GetAppInfo</p> <p>Disponibile per agenti Windows nel file Symantec_DLP_15.1_Agent_Win-IN.zip.</p>	Vedere "Utilizzo dello strumento GetAppInfo" a pagina 2240.
Avvio di DLP Agent installati su endpoint Mac	<p>start_agent</p> <p>Disponibile per agenti Mac sull'endpoint in /Library/Manufacturer/Endpoint Agent.</p>	Vedere "Avvio dei DLP Agent eseguiti negli endpoint Mac" a pagina 2270.

Vedere ["Funzionalità degli strumenti per endpoint Mac"](#) a pagina 2040.

Utilizzo di strumenti endpoint con Windows 7/8.1/10

Se si utilizzano strumenti endpoint su un computer in cui è in esecuzione Windows 7/8.1/10, eseguire il prompt dei comandi in modalità Prompt dei comandi con privilegi elevati. Questa procedura è richiesta a causa della natura del sistema operativo Windows. Non è possibile eseguire gli strumenti endpoint senza attivare la modalità Prompt dei comandi con privilegi elevati.

Per attivare la modalità Prompt dei comandi con privilegi elevati in Windows 7

- 1 Fare clic sul menu **Start**.
- 2 Nel campo **Cerca programmi e file**, digitare **prompt dei comandi**.
Il programma **Prompt dei comandi** è visualizzato nell'elenco dei risultati.
- 3 Tenere premuto il tasto MAIUSC e fare clic con il pulsante destro del mouse sulla voce **Prompt dei comandi** nell'elenco dei risultati. Selezionare **Esegui come amministratore** o **Esegui come altro utente**.
- 4 Se è stato selezionato **Esegui come altro utente**, immettere le credenziali per un utente con privilegi di amministratore.

Per attivare la modalità Prompt dei comandi con privilegi elevati in Windows 8.1/10

- 1 Visualizzare il prompt dei comandi.
 - In modalità Desktop, fare clic con il pulsante destro del mouse sull'icona di Windows e selezionare **Prompt dei comandi (amministratore)**, quindi fare clic sul menu **Start**.
 - In modalità Metro, digitare **cmd** nel campo **Cerca programmi e file**.
- 2 Tenere premuto il tasto MAIUSC e fare clic con il pulsante destro del mouse su **Prompt dei comandi** nell'elenco dei risultati.
- 3 Selezionare **Esegui come amministratore**.

Arresto dell'agente e dei servizi watchdog su endpoint Windows

Lo strumento Service_Shutdown.exe consente di arrestare DLP Agent e i servizi watchdog sugli endpoint Windows. Come misura di verifica delle alterazioni, non è possibile per un utente arrestare DLP Agent o il servizio watchdog. Questo strumento consente agli utenti con diritti di amministratore di arrestare contemporaneamente entrambi i servizi di Symantec Data Loss Prevention.

Per eseguire lo strumento Service_Shutdown.exe

- ◆ Nella directory di installazione, eseguire il seguente comando:

```
service_shutdown [-p=password]
```

dove la directory di installazione è la directory in cui è stato installato Symantec Data Loss Prevention e [-p=password] è la password specificata in precedenza. Se non si digita una password, viene chiesto di farlo. La password predefinita è *VontuStop*.

È necessario eseguire lo strumento Service_Shutdown.exe nella stessa directory del file di archivio chiavi di DLP Agent.

Vedere ["Informazioni sulla gestione delle password dell'agente" a pagina 2259](#) a pagina 2259.

Utilizzo degli strumenti Endpoint con macOS

Se si utilizzano gli strumenti Endpoint in un endpoint che esegue macOS, modificare le autorizzazioni per rendere ciascuno strumento eseguibile. Completare questo passaggio preliminare prima di copiare uno strumento nella cartella di installazione dell'agente. DLP Agent impedisce le modifiche delle autorizzazioni ai file presenti nella cartella di installazione dell'agente. Se non si modificano le autorizzazioni, non è possibile eseguire lo strumento Endpoint negli endpoint.

Completare la seguente procedura per utilizzare gli strumenti Endpoint negli endpoint Mac:

- 1 Copiare lo strumento Endpoint nell'endpoint. Ad esempio, copiare lo strumento in `/Users/<nome_utente>/Downloads/Tools/`.
- 2 Impostare le definizioni eseguibili utilizzando un comando sudo dall'applicazione Terminale.
Ad esempio, utilizzare il seguente comando se si desidera impostare le autorizzazioni di eseguibilità per lo strumento Service_Shutdown:

```
sudo chmod 755 service_shutdown
```

- 3 Copiare lo strumento Endpoint nella directory di installazione di DLP Agent.

Ripetere questi passaggi per ogni strumento Endpoint che si intende utilizzare.

Vedere ["Informazioni sulla gestione delle password dell'agente" a pagina 2259](#) a pagina 2259.

Interruzione del servizio dell'agente degli endpoint Mac

Lo strumento Service_Shutdown consente di arrestare il servizio DLP Agent negli endpoint Mac. Come misura di prevenzione delle alterazioni, gli utenti non possono arrestare il servizio DLP Agent sugli endpoint Mac. Tuttavia, un amministratore con accesso root può utilizzare lo strumento Service_Shutdown per arrestare il servizio Symantec Data Loss Prevention.

Per arrestare l'agente negli endpoint Mac:

- 1 Impostare le autorizzazioni dello strumento Service_Shutdown per renderlo eseguibile. Vedere ["Utilizzo degli strumenti Endpoint con macOS"](#) a pagina 2262.
- 2 Copiare lo strumento Service_Shutdown nella cartella di installazione di DLP Agent nell'endpoint Mac.
- 3 Eseguire il comando seguente come utente principale tramite l'applicazione Terminale:

```
#sudo ./service_shutdown  
  
-p=<tools_password>
```

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Ispezione dei file di database utilizzati dall'agente

Lo strumento `vontu_sqlite3` consente di ispezionare i file di database utilizzati dal DLP Agent. Fornisce un'interfaccia SQL per cercare e aggiornare file di database. Senza questo strumento, non è possibile visualizzare il contenuto di un file di database in quanto è crittografato. Utilizzare questo strumento quando si desidera analizzare o apportare modifiche ai file di Symantec Data Loss Prevention.

Nota: È necessario disporre di diritti di amministratore per utilizzare lo strumento su endpoint Windows. È necessario disporre dell'accesso sudo o alla radice per modificare il database degli agenti su endpoint Mac.

Per eseguire lo strumento vontu_sqlite3.exe negli endpoint Windows

- 1 Eseguire il seguente script dalla directory di installazione dell'agente Symantec Data Loss Prevention.

```
vontu_sqlite3 -db=database_file [-p=password]
```

dove *database_file* è il file di database e *password* è la password per gli strumenti.

I file di database di Symantec Data Loss Prevention per agenti Windows si trovano nella directory di installazione di DLP Agent e hanno l'estensione *.ead. Dopo avere eseguito il comando, viene richiesta la password.

- 2 Immettere la password predefinita `VontuStop` a meno che non sia già stata creata una password univoca.

Per immettere istruzioni SQL per la visualizzazione o l'aggiornamento del database, è disponibile una shell dei comandi.

Per una documentazione completa sui comandi disponibili in tale shell, consultare la pagina Web all'indirizzo <http://www.sqlite.org/sqlite.html>.

Per eseguire lo strumento vontu_sqlite3 negli endpoint Mac

- 1 Impostare le autorizzazioni dello strumento vontu_sqlite3 per renderlo eseguibile. Vedere ["Utilizzo degli strumenti Endpoint con macOS"](#) a pagina 2262.
- 2 Eseguire il seguente script dalla directory di installazione dell'agente Symantec Data Loss Prevention.

```
sudo ./vontu_sqlite3 -db=database_file [-p=password]
```

dove *database_file* è il file di database e *password* è la password per gli strumenti specificati.

Eseguire questo comando utilizzando l'applicazione Terminal. Lo strumento `vontu_sqlite3` si trova in `/Library/Manufacturer/Endpoint Agent/`.

- 3 Immettere la password predefinita `VontuStop` a meno che non sia già stata creata una password univoca.

Per immettere istruzioni SQL per la visualizzazione o l'aggiornamento del database, è disponibile una shell dei comandi.

Per una documentazione completa sui comandi disponibili in tale shell, consultare la pagina Web all'indirizzo <http://www.sqlite.org/sqlite.html>.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Visualizzazione dei file di registro estesi

Lo strumento `logdump.exe` consente agli utenti con privilegi di amministratore di visualizzare file di registro estesi per DLP Agent. I file di registro estesi sono nascosti per motivi di sicurezza. Generalmente, è necessario visualizzare i file di registro solo con il personale di supporto di Symantec Data Loss Prevention. Senza questo strumento, non è possibile visualizzare alcun file di registro di DLP Agent.

Nota: È necessario disporre di diritti di amministratore per utilizzare lo strumento su endpoint Windows. È necessario disporre dell'accesso `sudo` o alla radice per modificare il database degli agenti su endpoint Mac.

Per eseguire lo strumento `logdump` negli endpoint Windows

- 1 Eseguire il seguente script dalla directory di installazione dell'agente Symantec Data Loss Prevention.

```
logdump -log=log_file [-p=password]
```

dove `log_file` è il file di registro che si desidera visualizzare e `password` è la password degli strumenti specificati. Tutti i file di registro estesi di Symantec Data Loss Prevention sono presenti nella directory di installazione di Symantec Data Loss Prevention Agent. I nomi di file sono nel formato `edpa_extnumero_file.log`. Dopo aver eseguito questo comando, il registro non è più nascosto.

Nota: Quando si utilizza Windows PowerShell per eseguire `logdump.exe`, il file di registro deve essere racchiuso tra virgolette. Ad esempio, eseguire:

```
logdump "-log=log_file" [-p=password]
```

Tutti i file di registro estesi di Symantec Data Loss Prevention sono presenti nella directory di installazione di Symantec Data Loss Prevention Agent. I nomi di file sono nel formato `edpa_extnumero_file.log`. Dopo aver eseguito questo comando, il registro non è più nascosto.

- 2 (Facoltativo) Stampare il contenuto di un altro registro da questa vista.

Per eseguire lo strumento logdump negli endpoint Mac

- 1 Impostare le autorizzazioni dello strumento logdump per renderlo eseguibile. Vedere ["Utilizzo degli strumenti Endpoint con macOS"](#) a pagina 2262.
- 2 Eseguire i seguenti script dalla directory di installazione dell'agente Symantec Data Loss Prevention.

```
sudo ./logdump -log=log_file [-p=password]
```

dove *log_file* è il file di registro che si desidera visualizzare e *password* è la password degli strumenti specificati.

Tutti i file di registro estesi di Symantec Data Loss Prevention sono presenti nella directory di installazione di Symantec Data Loss Prevention Agent. I nomi di file sono nel formato *edpa_extnumero_file.log*. Dopo aver eseguito questo comando, il registro non è più nascosto.

- 3 (Facoltativo) Stampare il contenuto di un altro registro da questa vista.

Per stampare il contenuto di un altro registro

- 1 Dalla finestra di comando, eseguire:

```
logdump -log=log_file -p=password > deobfuscated_log_file_name
```

- 2 Digitare di nuovo la password per stampare il registro.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Informazioni sulle utilità ID periferica

Symantec Data Loss Prevention fornisce *DeviceID.exe* per i dispositivi rimovibili Windows e *DeviceID* per i dispositivi rimovibili Mac per la configurazione del rilevamento nei dispositivi endpoint.

Vedere ["Informazioni sul rilevamento di dispositivi endpoint"](#) a pagina 826.

Le utilità ID periferica ricercano tutti i dispositivi connessi del computer e restituiscono la stringa Device Instance ID negli endpoint Windows e le informazioni regex negli endpoint Mac.

In genere le utilità ID periferica consentono la copia di informazioni riservate a dispositivi esterni forniti dall'azienda quali unità USB o schede SD.

Vedere ["Utilizzo dell'utilità ID periferica per Windows"](#) a pagina 2267.

Vedere ["Utilizzo dell'utilità ID periferica per Mac"](#) a pagina 2269.

Tabella 85-2 Output di esempio dell'utilità ID periferica per Windows

Risultato	Descrizione
Volume	Volume o punto di installazione rilevato dallo strumento DeviceID.exe. Ad esempio: Volume: E:\
Dev ID	L'ID istanza periferica per ciascun dispositivo. Ad esempio: USBSTOR\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\5F73HF00Y9DBOG0DXJ
Regex	L'espressione regolare che individua l'istanza del dispositivo. Ad esempio: USBSTOR\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\5F73HF00Y9DBOG0DXJ

Tabella 85-3 Output di esempio dell'utilità ID periferica per Mac

Risultato	Descrizione
Fornitore	Fornitore rilevato dallo strumento ID periferica. Ad esempio: SanDisk&.*
Modello	Modello rilevato dallo strumento ID periferica. Ad esempio: SanDisk&Cruzer Blade&.*
Numero di serie	Numero di serie rilevato dallo strumento ID periferica. Ad esempio: SanDisk&Cruzer Blade&DER45TG5444

Utilizzo dell'utilità ID periferica per Windows

L'utilità ID periferica consente di estrarre le stringhe ID istanza periferica e di determinare quali dispositivi sono riconosciuti dal sistema ai fini del rilevamento. Per utilizzare lo strumento è necessario disporre dei diritti di amministratore.

Vedere ["Informazioni sulle utilità ID periferica"](#) a pagina 2266.

Vedere ["Informazioni sul rilevamento di dispositivi endpoint"](#) a pagina 826.

Per utilizzare l'utilità ID periferica

- 1 Ottenere l'utilità `DeviceID.exe`.

Questa utilità è disponibile con il pacchetto di utilità Endpoint Server.

Vedere ["Informazioni sulla gestione delle password dell'agente" a pagina 2259](#) a pagina 2259.

- 2 Copiare l'utilità `DeviceID.exe` sul computer in cui si desidera determinare gli ID dispositivo.
- 3 Installare i dispositivi che si desidera esaminare sul computer in cui si è copiata l'utilità `DeviceID.exe`.

Ad esempio, è possibile inserire uno o più dispositivi USB, connettere un'unità disco rigido e così via.

- 4 Eseguire l'utilità `DeviceID.exe` dalla riga di comando.

Ad esempio, se l'utilità `DeviceID.exe` è stata copiata nella directory `C:\Temp`, eseguire il seguente comando:

```
C:\TEMP>DeviceID
```

Per salvare i risultati in un file, digitare il seguente comando:

```
C:\TEMP>DeviceID > deviceids.txt
```

Il file appare nella directory `C:\temp` e contiene l'output del processo `DeviceID`.

- 5 Visualizzare i risultati del processo `DeviceID`.

Il prompt dei comandi visualizza i risultati per ciascun volume o punto di installazione.

Vedere [Tabella 85-2](#) a pagina 2267.

- 6 Valutare con l'utilità `DeviceID` la stringa regex proposta rispetto a un dispositivo attualmente connesso.

Vedere [Tabella 85-4](#) a pagina 2268.

- 7 Utilizzare modelli di espressione regolare per configurare i dispositivi per il rilevamento.

Vedere ["Creazione e modifica delle configurazioni di dispositivi endpoint"](#) a pagina 832.

Tabella 85-4 Valutazione regex ID dispositivo

Parametri di comando	Esempio
<code>DeviceID.exe [-m] [Volume] [Regex]</code>	<pre>DeviceID.exe -m E:\ "USBSTOR\DISK&VEN_UFD&PROD_USB_FLASH_DRIVE&REV_1100\.*"</pre> <p>Nota: La stringa regex va inclusa tra virgolette doppie.</p>
Restituisce	Corrispondenza o Mancata corrispondenza

Utilizzo dell'utilità ID periferica per Mac

Utilizzare l'utilità ID periferica per Mac per generare informazioni regex. Questa funzionalità può essere utilizzata per consentire la copia di informazioni riservate su dispositivi esterni forniti dall'azienda quali unità USB o schede SD.

Vedere ["Informazioni sulle utilità ID periferica"](#) a pagina 2266.

Vedere ["Creazione e modifica delle configurazioni di dispositivi endpoint"](#) a pagina 832.

Per utilizzare l'utilità ID della periferica

- 1 Ottenere l'utilità `DeviceID`.

Questa utilità è disponibile con il pacchetto degli strumenti dell'agente Mac.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

- 2 Copiare l'utilità `DeviceID` sul computer in cui si desidera determinare gli ID dispositivo.
- 3 Installare i dispositivi che si desidera esaminare sul computer in cui si è copiata l'utilità `DeviceID`.

Ad esempio, è possibile inserire uno o più dispositivi USB, connettere un'unità disco rigido, ecc.

- 4 Eseguire l'utilità `DeviceID` dall'applicazione Terminale.

Ad esempio, se si è copiata l'utilità `DeviceID` nella directory `Download`, eseguire il seguente comando:

```
$HOME/Downloads/DeviceID dove $HOME è la directory principale.
```

I risultati di output visualizzano informazioni per ogni volume o punto di installazione nella finestra dell'applicazione Terminale.

- 5 Controllare i risultati di elaborazione di `DeviceID`.
- 6 Utilizzare le informazioni regex per configurare i dispositivi per la rilevazione.

Vedere ["Creazione e modifica delle configurazioni di dispositivi endpoint"](#) a pagina 832.

Tabella 85-5

Parametro di comando	Esempio
<code>./DeviceID > deviceids.txt</code>	<p>Lo strumento estrae le seguenti informazioni sul file <code>deviceids.txt</code> in base alle informazioni raccolte dalla chiavetta collegata:</p> <ul style="list-style-type: none"> ■ Volume: <i>/Volumes/FAT_USB/</i> ■ Tipo (BUS): <i>USB</i> ■ ID periferica Regex per fornitore: <i>JetFlash&.*</i> ■ ID periferica Regex per modello: <i>JetFlash&Mass Storage Device&.*</i> ■ ID periferica Regex per numero di serie: <i>JetFlash&Mass Storage Device&79HC SMJ0RYOHT2FE</i>

Avvio dei DLP Agent eseguiti negli endpoint Mac

È possibile avviare i DLP Agent eseguiti negli endpoint Mac mediante lo strumento `start_agent`. Lo strumento può essere utilizzato se gli agenti sono stati arrestati mediante l'attività di arresto nella schermata **Elenco agenti**.

Questo strumento è disponibile nella directory `/Library/Manufacturer/Endpoint Agent` sull'endpoint.

Nota: È necessario decomprimere questo file zip su un endpoint Mac. Non è possibile utilizzare lo strumento se il file viene decompresso su un endpoint Windows.

Per avviare gli agenti mediante lo strumento `start_agent`:

1 Impostare le autorizzazioni dello strumento `start_agent` per renderlo eseguibile. Vedere ["Utilizzo degli strumenti Endpoint con macOS"](#) a pagina 2262.

2 Nella directory di installazione di Symantec Data Loss Prevention Agent eseguire il seguente comando:

```
sudo ./start_agent
```

dove la directory di installazione è la directory in cui è stato installato Symantec Data Loss Prevention.

3 Accedere alla schermata **Elenco agenti** e verificare che l'agente sia in esecuzione.

Vedere ["Utilizzo della schermata Elenco agenti"](#) a pagina 2197.

Vedere ["Informazioni sulla gestione delle password dell'agente"](#) a pagina 2259 a pagina 2259.

Monitoraggio della perdita di dati in applicazioni cloud

- [Capitolo 86. Utilizzo con Rilevamento applicazioni](#)
- [Capitolo 87. Utilizzo con Cloud Service for Email](#)

Utilizzo con Rilevamento applicazioni

Il capitolo contiene i seguenti argomenti:

- [Informazioni su Rilevamento applicazioni](#)
- [Gestione di Rilevamento applicazioni](#)

Informazioni su Rilevamento applicazioni

È possibile connettersi con molte applicazioni cloud tramite il servizio di rilevamento cloud di Symantec Data Loss Prevention. Il servizio di rilevamento cloud si integra perfettamente con il broker di sicurezza di accesso al cloud (CASB) Symantec CloudSOC.

Symantec CloudSOC include **Securlet** e **Gatelet** con API robuste che si connettono a molte applicazioni SaaS (software-as-a-service), quali Gmail, Google Drive e Salesforce. I **Securlet** ispezionano i dati riservati che vengono esposti nelle applicazioni cloud. I **Gatelet** ispezionano il contenuto in file e documenti durante il caricamento o il download nelle applicazioni cloud. La connessione di Symantec Data Loss Prevention a Symantec CloudSOC tramite il servizio di rilevamento cloud consente di includere le migliori funzionalità di Symantec per il rilevamento delle politiche per tutte le applicazioni SaaS supportate da Symantec CloudSOC.

Symantec Web Security Services (WSS) è un proxy cloud che consente di gestire le politiche di accesso alle applicazioni Web e cloud per gli utenti.

È possibile connettersi a Symantec CloudSOC e WSS distribuendo e configurando il servizio di rilevamento cloud. Per informazioni dettagliate sull'utilizzo del servizio di rilevamento cloud, vedere la Guida introduttiva sul *Servizio di rilevamento cloud di Symantec Data Loss Prevention* qui: www.symantec.com/docs/DOC9414.

Per connettersi con applicazioni on-site è possibile utilizzare il dispositivo Rilevamento API per le app degli sviluppatori. È necessario creare un client REST per le applicazioni a cui si

desidera connettersi. Per informazioni sul REST API, consultare la Guida di riferimento di REST API di rilevamento qui: www.symantec.com/docs/DOC10653.

Nota: Il dispositivo di rilevamento API per le app degli sviluppatori funziona solo con i client REST creati con REST di rilevamento API versione 2.0.

È possibile configurare il rilevamento applicazioni cloud nella pagina **Gestisci > Rilevamento applicazioni > Configurazione**.

Vedere "[Gestione di Rilevamento applicazioni](#)" a pagina 2273.

Gestione di Rilevamento applicazioni

Dopo aver distribuito e configurato il servizio di rilevamento cloud di Symantec Data Loss Prevention o il dispositivo di rilevamento API per le app degli sviluppatori, è possibile configurare il rilevamento applicazioni cloud nella pagina **Gestisci > Rilevamento applicazioni > Configurazione**.

È possibile effettuare le seguenti azioni nella pagina **Gestisci > Rilevamento applicazioni > Configurazione** :

Tabella 86-1 Azioni della pagina di configurazione di Rilevamento applicazioni

Azione	Descrizione
Configurazione del rilevamento applicazioni	<p>È possibile assegnare gruppi di politiche e regole di destinazione a Gatelet, Securlet CloudSOC e applicazioni cui si accede tramite il Servizio API rilevamento cloud:</p> <p>Vedere "Per configurare Rilevamento applicazioni per i Gatelet CloudSOC" a pagina 2274.</p> <p>Vedere "Per configurare Rilevamento applicazioni per i Securlet CloudSOC" a pagina 2275.</p> <p>Vedere "Per configurare il Rilevamento applicazioni per i proxy Web cloud (WSS)" a pagina 2277.</p> <p>Vedere "Per configurare Rilevamento applicazioni per il Servizio API rilevamento cloud" a pagina 2277.</p>
Modifica di una configurazione di rilevamento applicazioni esistente	<p>Per modificare la configurazione di un'applicazione esistente, fare clic sull'icona di modifica per quell'applicazione, modificare la configurazione, quindi fare clic su Salva.</p> <p>Vedere "Per modificare una configurazione di Rilevamento applicazioni" a pagina 2278.</p>

Azione	Descrizione
Eliminazione di una configurazione del rilevamento applicazioni	Per eliminare la configurazione di un'applicazione, fare clic sull'icona di cancellazione per quell'applicazione.
Sincronizzazione delle configurazioni di Rilevamento applicazioni con Symantec CloudSOC	Il pulsante Sincronizza in CloudSOC sulla barra degli strumenti dell'elenco di configurazioni applicazione elimina e sostituisce tutte le configurazioni di Rilevamento applicazioni lato CloudSOC. La best practice per l'aggiornamento di una singola configurazione prevede di modificare la configurazione e fare clic su Salva .

Configurazione di Rilevamento applicazioni

È possibile assegnare gruppi di politiche e regole di destinazione a Gatelet e Securllet CloudSOC, e applicazioni specifiche:

Per configurare Rilevamento applicazioni per i Gatelet CloudSOC

- 1 Accedere alla pagina **Gestisci > Rilevamento applicazioni > Configurazione**.
- 2 Fare clic su **Nuova configurazione**.
Viene visualizzata la pagina **Nuova configurazione**.
- 3 Nel campo **Nome** immettere un nome per la configurazione del rilevamento applicazioni cloud.
- 4 Nell'elenco a discesa **Tipo**, selezionare **Gatelet**.
- 5 Nel campo **Applicazioni**, selezionare una delle opzioni seguenti:
 - **Qualsiasi** : selezionando **Qualsiasi**, i gruppi di politiche e le regole di configurazione specificate vengono applicati a tutte le applicazioni cui si accede attraverso i Gatelet CloudSOC.
 - **Selettivo** : selezionando **Selettivo**, è possibile puntare ai Gatelet di applicazioni cloud specifiche. È possibile inserire il nome dell'applicazione nel campo **Immettere nome applicazione** o selezionarlo da un elenco di applicazioni.
- 6 Nel campo **Gruppi di politiche**, selezionare il gruppo o i gruppi di politiche che si desidera applicare a questa configurazione.
- 7 Nella sezione **Regole**, specificare il **Tipo trasferimento** per determinare la direzione del traffico di rete che si desidera ispezionare. È necessario selezionare almeno un'opzione, **Carica** o **Scarica**. È possibile selezionare entrambe le opzioni ispezionare tutto il traffico di rete.
- 8 Nella sezione **Proprietà dispositivo**, specificare una delle seguenti opzioni:
 - **Qualsiasi** : selezionare questa opzione per ispezionare tutti i dispositivi.

- **Gestito** : selezionare questa opzione per ispezionare solo i dispositivi gestiti dalla propria organizzazione. Se si seleziona questa opzione, è possibile selezionare opzioni aggiuntive per **Stato di proprietà dispositivo** (qualsiasi dispositivo, solo dispositivi aziendali o solo dispositivi personali) e **Stato di condizione dispositivo** (qualsiasi dispositivo, dispositivi conformi alla politica o dispositivi non conformi alla politica).
 - **Non gestito** : selezionare questa opzione per ispezionare solo i dispositivi non gestiti dalla propria organizzazione.
- 9 Nella sezione **Utenti e gruppi**, selezionare una delle opzioni seguenti:
- **Qualsiasi** : selezionare questa opzione per ispezionare il traffico associati a qualsiasi utente.
Se si seleziona questa opzione, è anche possibile specificare eccezioni per utenti o gruppi specifici facendo clic su **Aggiungi eccezioni**.
 - **Selettivo** : selezionare questa opzione per ispezionare utenti o gruppi di utenti specifici.
- 10 Nella sezione **Regioni**, selezionare una delle opzioni seguenti:
- **Qualsiasi** : selezionare questa opzione per ispezionare il traffico associati a qualsiasi area geografica.
Se si seleziona questa opzione, è anche possibile specificare eccezioni per aree geografiche specifiche facendo clic su **Aggiungi eccezioni**.
 - **Selettivo** : selezionare questa opzione per ispezionare aree geografiche specifiche.
- 11 Nella sezione **Proprietà file**, selezionare una delle seguenti opzioni di **Estensioni file** :
- **Qualsiasi** : selezionare questa opzione per ispezionare tutti i tipi di file.
Se si seleziona questa opzione, è anche possibile specificare eccezioni per tipi di file specifici facendo clic su **Aggiungi eccezioni**.
 - **Selettivo** : selezionare questa opzione per ispezionare tipi di file specifici.
- 12 Facoltativo: nella sezione **Dimensione del file**, specificare uno o entrambi i seguenti filtri di inclusione:
- **Più piccolo di** : immettere una dimensione del file in byte al di sotto della quale i file saranno inclusi nell'ispezione.
 - **Più grande di** : immettere una dimensione del file in byte al di sopra della quale i file saranno inclusi nell'ispezione.

13 Fare clic su **Salva**.

Per configurare Rilevamento applicazioni per i Securlet CloudSOC

- 1 Accedere alla pagina **Gestisci > Rilevamento applicazioni > Configurazione**.
- 2 Fare clic su **Nuova configurazione**.

Viene visualizzata la pagina **Nuova configurazione**.

- 3 Nel campo **Nome** immettere un nome per la configurazione del rilevamento applicazioni cloud.
- 4 Nell'elenco a discesa **Tipo**, selezionare **Securlet**.
- 5 Nel campo **Applicazioni**, selezionare una delle opzioni seguenti:
 - **Integrato** : selezionando **Integrato** è possibile scegliere da un elenco di Securlet CloudSOC disponibili per applicazioni specifiche.
 - **Personalizza** : selezionando **Personalizza** è possibile puntare ai Securlet di applicazioni cloud personalizzate. È possibile inserire il nome dell'applicazione nel campo **Immettere nome applicazione**.
- 6 Nel campo **Gruppi di politiche**, selezionare il gruppo o i gruppi di politiche che si desidera applicare a questa configurazione.
- 7 Nella sezione **Regole**, specificare il **Tipo esposizione** per i file che si desidera ispezionare:
 - **Interno** : selezionare questa opzione per ispezionare i file disponibili agli utenti all'interno dell'organizzazione.
 - **Esterno** : selezionare questa opzione per ispezionare i file disponibili agli utenti all'esterno dell'organizzazione.
 - **Pubblico** : selezionare questa opzione per ispezionare i file disponibili a chiunque su Internet.
 - **Non esposto** : selezionare questa opzione per ispezionare i file non disponibili a nessuno.

Se è stata selezionata una certa combinazione di esposizioni **Interno**, **Esterno** o **Pubblico**, è possibile specificare ulteriormente se si desidera trovare qualunque file che corrisponde a uno dei tipi di esposizione, o file che corrispondono a tutti i tipi di esposizione specificati. Ad esempio, se sono stati selezionati sia i tipi di esposizione **Interno** che **Pubblico**, selezionando **Corrispondenza con qualsiasi** vengono considerati i file interni o pubblici. Selezionando **Corrispondenza con tutto** vengono considerati solo i file che sono esposti sia internamente che pubblicamente.
- 8 Nella sezione **Utenti e gruppi**, selezionare una delle opzioni seguenti:
 - **Qualsiasi** : selezionare questa opzione per ispezionare il traffico associati a qualsiasi utente.

Se si seleziona questa opzione, è anche possibile specificare eccezioni per utenti o gruppi specifici facendo clic su **Aggiungi eccezioni**.
 - **Selettivo** : selezionare questa opzione per ispezionare aree geografiche specifiche.
- 9 Nella sezione **Percorsi cartelle**, selezionare una delle opzioni seguenti:
 - **Qualsiasi** : selezionare questa opzione per ispezionare qualunque percorso cartella disponibile.

Se si seleziona questa opzione, è anche possibile specificare percorsi cartella da escludere dall'ispezione facendo clic su **Aggiungi eccezioni**.

- **Selettivo** : selezionare questa opzione per ispezionare percorsi e cartelle specifici.

10 Nella sezione **Proprietà file**, selezionare una delle seguenti opzioni di **Estensioni file** :

- **Qualsiasi** : selezionare questa opzione per ispezionare tutti i tipi di file.
Se si seleziona questa opzione, è anche possibile specificare eccezioni per tipi di file specifici facendo clic su **Aggiungi eccezioni**.
- **Selettivo** : selezionare questa opzione per ispezionare tipi di file specifici.

11 Facoltativo: nella sezione **Dimensione del file**, specificare uno o entrambi i seguenti filtri di inclusione:

- **Più piccolo di** : immettere una dimensione del file in byte al di sotto della quale i file saranno inclusi nell'ispezione.
- **Più grande di** : immettere una dimensione del file in byte al di sopra della quale i file saranno inclusi nell'ispezione.

12 Fare clic su **Salva**.

Per configurare il Rilevamento applicazioni per i proxy Web cloud (WSS)

- 1 Accedere alla pagina **Gestisci > Rilevamento applicazioni > Configurazione**.
- 2 Fare clic su **Nuova configurazione**.
Viene visualizzata la pagina **Nuova configurazione**.
- 3 Nel campo **Nome** immettere un nome per la configurazione del rilevamento applicazioni
- 4 Nell'elenco a discesa **Tipo** selezionare **Proxy Web cloud**.
- 5 Nel campo **Gruppi di politiche**, selezionare il gruppo o i gruppi di politiche che si desidera applicare a questa configurazione.
- 6 Fare clic su **Salva**.

Per configurare Rilevamento applicazioni per il Servizio API rilevamento cloud

- 1 Accedere alla pagina **Gestisci > Rilevamento applicazioni > Configurazione**.
- 2 Fare clic su **Nuova configurazione**.
Viene visualizzata la pagina **Nuova configurazione**.
- 3 Nel campo **Nome** immettere un nome per la configurazione del rilevamento applicazioni
- 4 Nell'elenco a discesa **Tipo**, selezionare **Servizio API rilevamento cloud**.
- 5 Nel campo **Applicazione**, immettere il nome dell'applicazione cui si accede tramite il Servizio API rilevamento cloud.

- 6 Nel campo **Gruppi di politiche**, selezionare il gruppo o i gruppi di politiche che si desidera applicare a questa configurazione.
- 7 Fare clic su **Salva**.

Modifica di una configurazione di Rilevamento applicazioni

È possibile modificare le assegnazioni del gruppo di politiche di ciascuna applicazione:

Per modificare una configurazione di Rilevamento applicazioni

- 1 Accedere alla pagina **Gestisci > Rilevamento applicazioni > Configurazione**.
- 2 Fare clic sull'icona di modifica per il connettore cloud che si desidera modificare.
Viene visualizzata la pagina **Modifica configurazione**.
- 3 Modificare la configurazione.
- 4 Fare clic su **Salva**.

Utilizzo con Cloud Service for Email

Il capitolo contiene i seguenti argomenti:

- [Informazioni su Cloud Service for Email](#)
- [Aggiornamento di domini di posta nella console di amministrazione di Enforce Server](#)
- [Crittografia delle e-mail cloud con Symantec Information Centric Encryption](#)

Informazioni su Cloud Service for Email

Symantec Data Loss Prevention Cloud Service for Email rileva accuratamente i dati riservati contenuti nelle e-mail aziendali inviate da un server Microsoft Exchange, da Microsoft Office 365 Exchange Online o da Google G Suite Gmail. Accelera l'adozione di e-mail nel cloud da parte dell'azienda integrando in modo trasparente i controlli Symantec di prevenzione della perdita di dati leader del mercato con il servizio e-mail nel cloud dell'azienda (sono supportati Google G Suite Gmail e Microsoft Office 365 Exchange online).

Cloud Service for Email monitora e analizza il traffico di e-mail in uscita dai server Microsoft Office 365, Microsoft Office 365 Exchange Online o Google G-Suite Gmail e può crittografare, bloccare, reindirizzare o modificare i messaggi e-mail come specificato nelle politiche aziendali. La crittografia è disponibile in Symantec Information Centric Encryption (ICE).

Questa soluzione consente inoltre di creare le politiche relative alla perdita di dati, esaminare e riparare gli incidenti, nonché amministrare il sistema Data Loss Prevention dalla console di amministrazione di Enforce Server. Cloud Service for Email consente alle aziende di sfruttare l'investimento effettuato nella definizione e nell'amministrazione delle politiche, nonché nei processi di riparazione degli incidenti. La possibilità di utilizzare Cloud Service for Email per monitorare e analizzare il traffico di e-mail di Microsoft Exchange on-site fornisce un percorso di migrazione al cloud, se si prevede di passare a un servizio e-mail nel cloud, come Microsoft Office 365 Exchange Online o Google G-Suite Gmail.

Per informazioni sui passaggi necessari per configurare Symantec Data Loss Prevention Cloud Service for Email, vedere la *Symantec Data Loss Prevention Guida all'implementazione di Cloud Service for Email* nel centro di supporto Symantec <http://www.symantec.com/docs/DOC9008>.

È possibile abbonarsi a questo articolo nel Centro di supporto Symantec per gli aggiornamenti.

Aggiornamento di domini di posta nella console di amministrazione di Enforce Server

Informazioni sull'aggiornamento di domini di posta nella console di amministrazione di Enforce Server

È possibile aggiornare rapidamente i domini di posta elettronica delle e-mail aziendali che si desidera far analizzare da Cloud Service for Email (il Servizio). Questa nuova funzionalità si applica alle e-mail inviate da Microsoft Office 365 in modalità di riflessione. Quando si aggiunge o si rimuove un dominio nella console di amministrazione di Enforce Server, il nuovo elenco viene inviato immediatamente al servizio cloud Symantec. Il servizio verifica e aggiunge i domini. Questa funzionalità consente di aggiornare i domini in qualunque momento.

Il servizio non supporta i domini non aggiunti (in lista bianca) dal servizio cloud di Symantec o nella pagina della console di amministrazione di Enforce Server. Le e-mail di domini non supportati vengono rifiutate (restituite) dal servizio.

Se si è un cliente esistente di Cloud Service for Email, quando si esegue l'upgrade da 14.x a 15.1 o da 15.0 a 15.1, i domini esistenti vengono conservati e il traffico non viene compromesso. In questo caso, le modifiche ai domini in Enforce sono bloccate finché il servizio non ha verificato i domini esistenti.

Vedere "[Aggiornamento dei domini e-mail](#)" a pagina 2280.

Aggiornamento dei domini e-mail

È possibile modificare o rimuovere domini e-mail uno alla volta o importando un file di testo.

Per aggiungere domini e-mail uno alla volta

- 1 Accedere alla schermata **Sistema > Server e rilevatori > Panoramica**. Fare clic sul rilevatore nell'elenco.
Fare clic su **Aggiorna domini e-mail** nella pagina **Domini e-mail**.
- 2 Fare clic su **Aggiungi**.
- 3 Immettere un dominio e-mail.

Per aggiungere i domini in massa aggiungendo un elenco o importando un file di testo

- 1 Andare a **Aggiungi domini e-mail**.
- 2 Fare clic su **Aggiorna domini e-mail**.
- 3 Nella casella **Immetti domini e-mail**, aggiungere i domini e-mail delimitati da virgole o ritorni a capo.
- 4 In alternativa, indicare un nome di file e fare clic su **Carica** per caricare un file di testo con domini e-mail in un formato delimitato da virgola o ritorno a capo.
- 5 Fare clic su **Salva**.

Nota: I nomi di dominio devono essere specifici. I record DNS con carattere jolly come * o `esempio.com` non sono supportati. I sottodomini specifici (quelli che non utilizzando i caratteri jolly) sono supportati.

Una volta aggiunti i domini, è possibile configurare i nomi dopo che Enforce Server si è sincronizzato con la configurazione del cloud. Tutti i domini sono verificati e aggiornati ogni 15 minuti dal servizio cloud Symantec.

Per configurare i domini e-mail nella console di amministrazione di Enforce Server

- 1 Accedere a **Sistema > Server e rilevatori > Panoramica**.
- 2 Selezionare il rilevatore di e-mail nel cloud che si desidera configurare. Viene visualizzata la pagina dei dettagli per quel rilevatore.
- 3 Fare clic su **Aggiorna domini e-mail**.
- 4 Selezionare un dominio, quindi selezionare **Aggiungi** o **Elimina**.

Stati del dominio:

- **Aggiunto** - Il dominio è stato verificato e aggiunto.
- **Riconcilia** - Il servizio cloud Symantec ha cercato di verificare un dominio, ma nel record TXT mancava il codice e non è stato possibile verificare il dominio. È necessario aggiornare il record TXT DNS in modo da poter verificare e aggiungere il dominio.
Il record TXT DNS viene generato automaticamente ogni volta che Symantec effettua il provisioning di ogni istanza di Cloud Service for Email. Ogni dominio utilizzato deve contenere il record di testo DNS.
Dopo l'aggiornamento, fare clic su **Rinvia** per inviare il dominio aggiornato a Symantec.
- **Rimosso** - È stato eliminato un dominio e Symantec l'ha rimosso dalle proprietà del rilevatore.
- **Non valido** - Il dominio che si è tentato di aggiungere in Enforce non ha superato la convalida DNS.

- **Richiesta di rimozione** È stato eliminato un dominio e Symantec non l'ha ancora rimosso dalle proprietà del rilevatore.

Se il servizio cloud di Symantec riscontra dei problemi con i domini di posta elettronica per i quali è stata richiesta la convalida, le notifiche vengono visualizzate nella parte inferiore della pagina **Dettagli rilevatore**. Vengono utilizzati solo domini validi; il rilevatore ignora domini non validi. L'utente è tenuto a verificare che i domini inoltrati siano accettati e validi.

Vedere ["Sovrascrittura degli aggiornamenti tramite i servizi cloud di Symantec"](#) a pagina 2282.

Sovrascrittura degli aggiornamenti tramite i servizi cloud di Symantec

Il team del servizio cloud di Symantec può sovrascrivere la funzionalità **Aggiungi domini** per scopi di supporto. Se è richiesta una sovrascrittura, il messaggio di avvenuta sovrascrittura del controllo da parte del servizio cloud di Symantec viene visualizzato nel riquadro **Eventi di sistema** nella parte inferiore destra della pagina **Dettagli rilevatore**.

Quando il servizio cloud di Symantec detiene il controllo, è ancora possibile aggiungere o rimuovere domini. Tali modifiche non avranno effetto sulle impostazioni del rilevatore fino a quando i servizi cloud non restituiscono il controllo alla console di amministrazione di Enforce Server.

L'opzione **Aggiungi** della pagina **Aggiungi domini** è bloccata nella modalità **Riconcilia**. Durante questo intervallo di tempo, i servizi cloud di Symantec controllano l'aggiornamento. Correggere i domini contrassegnati con **Riconcilia** per assicurarsi che includano il codice del record di testo DNS. Quindi, fare clic su **Rinvia** per inviare i record di dominio corretti al servizio cloud di Symantec.

Crittografia delle e-mail cloud con Symantec Information Centric Encryption

L'integrazione di Symantec Information Centric Encryption (ICE) con Symantec Data Loss Prevention Cloud Service for Email consente di crittografare le e-mail riservate che vengono inviate tramite Microsoft Office 365 Exchange Online o Google G Suite Gmail. La crittografia ICE può essere applicata a allegati di e-mail o al corpo dell'e-mail e agli allegati e-mail.

ICE per e-mail si configura nella console del cloud ICE Symantec e nella console di amministrazione di Enforce Server. È necessario configurare le regole di risposta crittografia per le e-mail che passano attraverso il rilevamento. Vengono visualizzati incidenti nella pagina **Dettagli incidente** con collegamenti alla console di ICE .

Utilizzo di ICE con il Servizio cloud DLP per e-mail

Le tecnologie di crittografia tipiche potrebbero causare la perdita di dati dopo la decrittografia delle e-mail. Una volta decrittografate, le e-mail possono essere inviate ad altri individui e non sono più protette. Tuttavia, la tecnologia di crittografia ICE crittografa e protegge le e-mail e

gli allegati per tutta la durata di un'e-mail, indipendentemente dalla sua posizione. Se un'e-mail o un allegato viola una o più politiche del Servizio cloud DLP per e-mail, il Servizio cloud DLP per e-mail può richiedere al servizio di crittografia ICE di crittografare automaticamente il messaggio. Una volta crittografato, solo gli utenti autorizzati possono leggerlo. ICE può crittografare l'e-mail e gli allegati oppure solo gli allegati.

Con ICE è possibile applicare autorizzazioni granulari alle e-mail con crittografia ICE e determinare cosa un utente può fare con un'e-mail dopo che è stata decrittografata da ICE. È possibile limitare la stampa, la modifica o la condivisione da parte dell'utente dell'allegato dell'e-mail o dell'e-mail e dell'allegato. Quando il Servizio cloud DLP per e-mail identifica un allegato in un'e-mail, o un'e-mail e un allegato che viola una politica, utilizza il servizio di crittografia ICE per crittografarli automaticamente. L'incidente viene visualizzato nella console di amministrazione di Enforce Server. Il Servizio cloud DLP per e-mail registra quindi l'azione nella console del cloud ICE. È possibile fare clic su un collegamento nell'incidente per visualizzare ulteriori dettagli nella console del cloud ICE.

Inizialmente, agli amministratori DLP viene fornito l'accesso di sola lettura alla console del cloud ICE. È sempre possibile assegnare all'amministratore autorizzazioni più ampie in tale console. Gli amministratori DLP devono accedere alla console del cloud ICE quando fanno clic sul collegamento **Visualizza in console cloud ICE**. Dopo l'accesso, è possibile visualizzare ulteriori informazioni sull'incidente nella console del cloud ICE.

Per ulteriori informazioni su ICE, vedere la [Guida in linea ICE](#) o la documentazione ICE in <http://www.symantec.com/docs/DOC9707>.

Vedere "[Implementazione di ICE con Cloud Service for Email](#)" a pagina 2283.

Implementazione di ICE con Cloud Service for Email

[Tabella 87-1](#) fornisce una panoramica dei passaggi da intraprendere per utilizzare ICE nella crittografia di e-mail. I passaggi presuppongono che Cloud Service for Email sia già stato configurato e distribuito. Per ulteriori dettagli, vedere le sezioni relative a riferimenti incrociati.

Tabella 87-1 Panoramica sull'implementazione di ICE con Cloud Service for Email

Passaggio	Azione	Ulteriori informazioni
Passaggio 1	Configurare il servizio ICE.	Per informazioni sul funzionamento e dettagli sulle decrittografia ICE, vedere <i>Guida alla distribuzione di Symantec Information Centric Encryption</i> alla pagina http://www.symantec.com/docs/DOC9707.html .
Passaggio 2	Configurare l'Enforce Server per comunicare con il servizio ICE.	Vedere " Configurazione di Enforce Server per comunicare con il servizio ICE " a pagina 2284.

Passaggio	Azione	Ulteriori informazioni
Passaggio 3	Configurare le regole di risposta che utilizzano la crittografia ICE.	Vedere "Creazione di regole di risposta per la crittografia ICE" a pagina 2285.
Passaggio 4	Fare clic su un incidente per accedere alla console del cloud ICE per ulteriori informazioni.	Vedere "Visualizzazione dei dettagli sugli incidenti ICE" a pagina 2287.

Vedere ["Configurazione di Enforce Server per comunicare con il servizio ICE"](#) a pagina 2284.

Configurazione di Enforce Server per comunicare con il servizio ICE

Per configurare la comunicazione tra Enforce Server e il servizio ICE servono informazioni della console del cloud ICE.

- Nella console del cloud ICE, andare a **Impostazioni > Configurazione avanzata > Servizi esterni**. Copiare le seguenti informazioni da immettere nella console di amministrazione di Enforce Server per configurare la connessione tra la console del cloud ICE e Cloud Service for Email di Data Loss Prevention:
 - URL servizio
 - ID cliente
 - ID dominio
 - ID utente servizio
 - Password servizio
- Nella console di amministrazione di Enforce Server, andare a **Sistema > Impostazioni > Generali > Modifica impostazioni generali** in **Impostazioni di accesso ICE Cloud**.
- Immettere le seguenti informazioni ottenute nella console del cloud ICE:
- URL servizio
 - ID cliente
 - ID dominio
 - ID utente servizio
 - Password servizio
 - Reimmissione della password di servizio

Dopo averle salvate, queste impostazioni vengono trasmesse al servizio cloud DPL e ICE è attivata.

Vedere ["Creazione di regole di risposta per la crittografia ICE"](#) a pagina 2285.

Creazione di regole di risposta per la crittografia ICE

Utilizzare le informazioni in [Tabella 87-2](#) per creare regole per la crittografia ICE. Dopo la tabella sono illustrati i passaggi per la creazione di regole.

È possibile applicare nelle politiche una delle due regole per la crittografia ICE. È possibile crittografare solo gli allegati e-mail oppure gli allegati e-mail e il corpo dell'e-mail. Non è possibile crittografare solo il corpo. Se un messaggio e-mail include più allegati, e un solo allegato viola una condizione della politica, tutti gli allegati vengono crittografati.

Tabella 87-2 Regole di risposta per la crittografia ICE

Nome regola	Nome intestazione	Valore	Funzione
Crittografia dei soli allegati	Metodo di crittografia X	Allegati ICEemail	<p>Crittografa solo gli allegati.</p> <p>Il destinatario vede il messaggio di posta elettronica originale, ma gli allegati vengono sostituiti con file HTML crittografati. Il destinatario viene informato che gli allegati sono crittografati e possono essere decrittografati solo con ICE. Consultare la documentazione ICE per ulteriori informazioni.</p>

Nome regola	Nome intestazione	Valore	Funzione
Crittografia di corpo e allegati	Metodo di crittografia X	ICEemail tutti	<p>Crittografa gli allegati e il corpo dell'e-mail.</p> <p>Il destinatario viene informato che l'e-mail e gli allegati sono crittografati e possono essere decrittografati solo con ICE. Gli allegati sono sostituiti con file HTML crittografati. Consultare la documentazione ICE per ulteriori informazioni.</p>

Creazione di una regola di risposta

- 1 Accedere a **Gestisci > Politiche > Regole di risposta**.
- 2 Fare clic su **Aggiungi regola di risposta**.
- 3 Fare clic su **Risposta automatica** (sono possibili anche regole di risposta smart).
- 4 Immettere un nome nel campo **Nome regola** e una **Descrizione**.
- 5 In opzione, definire una o più **Condizioni** per stabilire quando eseguire la regola di risposta.
- 6 Nel menu a discesa **Azioni**, dalla categoria **Network Prevent** selezionare **Modifica messaggio SMTP**.
- 7 Fare clic su **Aggiungi azione**.
- 8 Nella finestra di dialogo **Network Prevent**, nel campo **Nome intestazione 1** digitare "Metodo di crittografia X."
- 9 Nel campo Valore intestazione 1, digitare "allegati ICEemail" o "ICEemail tutti," a seconda delle politiche di protezione dei dati.
- 10 Fare clic su **Salva**.
- 11 Configurare una politica con la regola di risposta creata.

Nota: Se per qualche motivo (ad esempio informazioni server non valide) non è possibile crittografare l'allegato o l'allegato e il corpo dell'e-mail, Cloud Service for Email inserisce un'intestazione separata in modo che l'e-mail possa essere gestita a valle.

La regola di risposta Crittografia ha la precedenza su una regola di risposta Modifica o Anteponi intestazione. Se oltre a Crittografia è presente anche una regola di risposta Modifica intestazione, viene eseguita solo la regola Crittografia. Tuttavia, una regola di risposta Blocca ha la precedenza su una regola di risposta Crittografia.

Vedere ["Informazioni sulle regole di risposta"](#) nella Guida in linea di Symantec Data Loss Prevention.

Vedere ["Informazioni sulla decrittografia di e-mail con crittografia ICE"](#) a pagina 2287.

Informazioni sulla decrittografia di e-mail con crittografia ICE

È possibile trovare i dettagli sulla decrittografia di e-mail ICE nell'argomento ["Informazioni sull'utilità ICE Symantec"](#) nella Guida in linea della console del cloud ICE.

Vedere ["Visualizzazione dei dettagli sugli incidenti ICE"](#) a pagina 2287.

Visualizzazione dei dettagli sugli incidenti ICE

Andare a **Incidenti > Rete > Incidenti - Nuovo** per visualizzare i dettagli degli incidenti. Fare clic sulla scheda **Cronologia** per visualizzare i dettagli cronologici. Vedere [Figura 87-1](#) a pagina 2288.

Figura 87-1 Dettagli della cronologia per gli incidenti ICE in Enforce

Symantec Data Loss Prevention | Home | Incidents | Manage | System

Incidents > Network > Incidents - New > Network Incident Snapshot

Incident 00000108

Status: **New** | Severity: **High**

SMTP

Key Info | History | Notes | Correlations

History

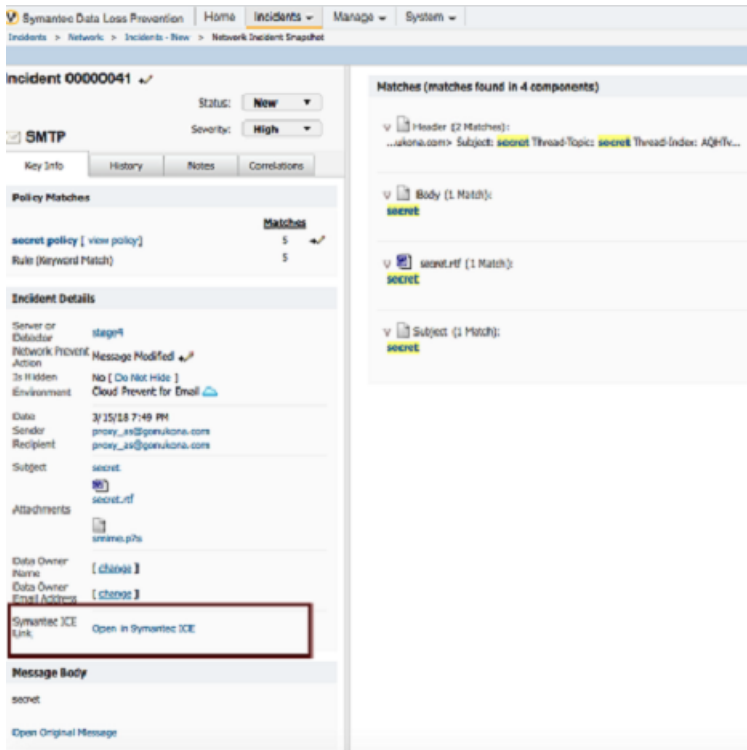
Date	Submitted By	Summary
2/12/18 6:51 AM	O365	Incident data discarded based on response rule
2/12/18 6:51 AM	Administrator	Severity Changed High
2/12/18 6:51 AM	O365	Headers Modified Modified message headers: Added headers: x-encryption-method: ICEemail all
2/12/18 6:51 AM	Administrator	PGP SMTP Message Id <CY1PR0801MB23155A2FB74DC25DEB4FDFA78CF70@CY1PR0801MB2315.namprd08.prod.outlook.com>
2/12/18 6:51 AM	O365	Detected
2/12/18 6:51 AM	Administrator	Status Changed New

Matches (matches found in 1 component)

top secret.txt (1 Match):
encryptall

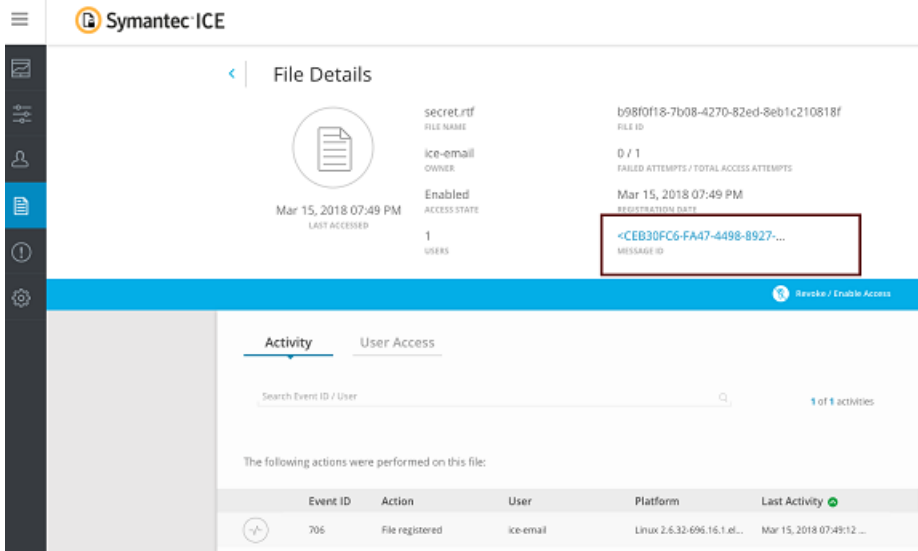
Fare clic sulla scheda **Informazioni chiave** per visualizzare ulteriori dettagli. Vedere [Figura 87-2](#) a pagina 2289.

Figura 87-2 Dettaglio informazioni chiave per incidenti ICE in Enforce



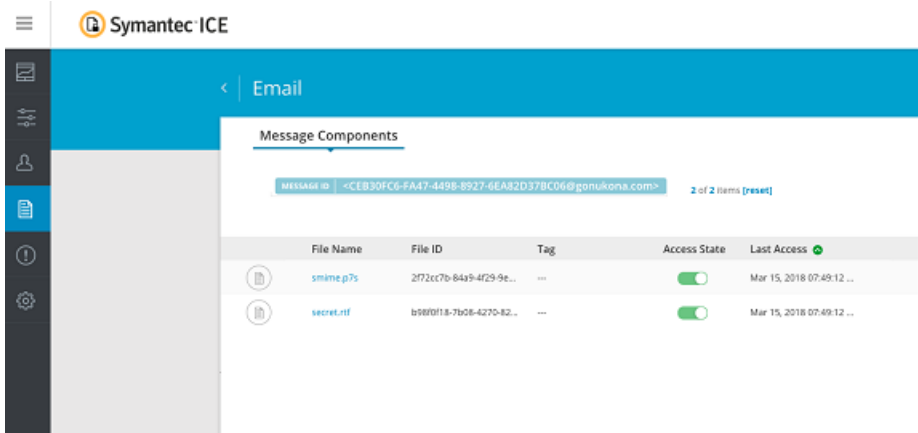
Fare clic su **Apri in Symantec ICE** per ottenere ulteriori informazioni su ogni incidente nella console del cloud ICE. È necessario accedere alla console del cloud ICE per vedere tutti i documenti che sono stati crittografati come parte del messaggio. Vedere [Figura 87-3](#) a pagina 2290.

Figura 87-3 Dettagli file nella console del cloud ICE



Quando si fa clic su un file, vengono visualizzati dettagli aggiuntivi. È possibile fare clic su **ID messaggio** per andare a una pagina per tale messaggio in cui è possibile visualizzare i componenti del messaggio. Vedere [Figura 87-4](#) a pagina 2290.

Figura 87-4 Componenti del messaggio e-mail nella console del cloud ICE



Monitoraggio della perdita di dati mediante dispositivi DLP

- [Capitolo 88. Implementazione e utilizzo di dispositivi DLP](#)
- [Capitolo 89. Distribuzione dei dispositivi DLP](#)
- [Capitolo 90. Attività di post-distribuzione](#)

Implementazione e utilizzo di dispositivi DLP

Il capitolo contiene i seguenti argomenti:

- [Informazioni sui dispositivi DLP](#)
- [Informazioni su come ottenere i file e le licenze di attivazione del dispositivo](#)
- [Informazioni sull'interfaccia da riga di comando \(CLI\)](#)
- [Informazioni su ottimizzazione delle prestazioni e dimensionamento per i dispositivi](#)

Informazioni sui dispositivi DLP

I dispositivi virtuali e hardware per Symantec Data Loss Prevention 15.0 forniscono un modo semplificato per distribuire, sottoporre a upgrade e mantenere i server di rilevamento di Data Loss Prevention. Attivare il dispositivo dalla riga di comando. Quando si configura un dispositivo virtuale, scaricare l'immagine per il software di rilevamento virtuale; i dispositivi hardware sono già dotati del software del dispositivo. Quindi registrare e gestire il dispositivo dalla console di amministrazione di Enforce Server.

I dispositivi virtuali di rilevamento includono:

- Dispositivo Network Prevent for Email
- Dispositivo Network Prevent for Web
- Dispositivo Rilevamento API per le app degli sviluppatori, che fornisce la flessibilità per connettersi alle applicazioni utilizzate all'interno dell'organizzazione. Per istruzioni specifiche sulla configurazione del dispositivo di Rilevamento API per le app degli sviluppatori, vedere *Guida introduttiva di Symantec Data Loss Prevention e dispositivo di rilevamento API per le app degli sviluppatori* all'indirizzo <http://www.symantec.com/docs/DOC10923>.

È necessario creare un client REST per le applicazioni da connettere mediante il dispositivo di rilevamento API per le app degli sviluppatori. Per informazioni sul REST API, consultare la *Symantec Data Loss Prevention Guida di riferimento 2.0 di REST API di rilevamento* all'indirizzo: <http://www.symantec.com/docs/DOC10653>.

Registrare e gestire il dispositivo hardware dalla console di amministrazione di Enforce Server. Il software di Network Prevent for Web è già installato nel dispositivo hardware Symantec DLP-S500.

Vedere "[Informazioni su come ottenere i file e le licenze di attivazione del dispositivo](#)" a pagina 2293.

Informazioni su come ottenere i file e le licenze di attivazione del dispositivo

Sono necessari due file sia per il dispositivo virtuale DLP sia per il dispositivo Hardware DLP:

- Un file di attivazione per il dispositivo.
- Un file di licenza per il software di rilevamento di Data Loss Prevention.

Per ottenere il file di attivazione per il dispositivo virtuale (come descritto in seguito), è necessario fornire un codice di attivazione. È possibile ottenere il codice di attivazione nell'e-mail di conferma di Symantec per il dispositivo virtuale.

È necessario fornire un numero di serie per il dispositivo hardware. È possibile ottenere il numero di serie nell'e-mail di avviso spedizione di Symantec. Non è necessario un codice di attivazione per il dispositivo hardware.

Vedere "[Acquisizione dei file di attivazione e di licenza per il dispositivo virtuale](#)" a pagina 2293.

Vedere "[Acquisizione dei file di licenza per il dispositivo hardware DLP S500-10](#)" a pagina 2295.

Acquisizione dei file di attivazione e di licenza per il dispositivo virtuale

Seguire le procedure riportate di seguito per l'acquisizione del file di attivazione e del file di licenza del software di rilevamento per il dispositivo virtuale DLP. Una volta acquisiti i file, applicare il file di attivazione del dispositivo virtuale nella riga di comando del dispositivo. Quindi, dopo avere scaricato il software di rilevamento nel dispositivo virtuale, è possibile applicare la licenza per il software di rilevamento nella console di amministrazione di Enforce Server.

Acquisizione del file di licenza per l'attivazione del dispositivo per il sistema operativo del dispositivo virtuale

- 1 Accedere a https://support.symantec.com/en_US.html.
- 2 Accedere a **Centro di supporto > MySymantec > Portale delle licenze** ed effettuare l'accesso al proprio account Symantec.
- 3 Dal **Portale delle licenze**, selezionare **Network Protection (Blue Coat License)**.
- 4 Immettere il codice di attivazione dalla quarta colonna della tabella nell'e-mail di conferma di Symantec ricevuta da Enterprise_Efulfill@symantec.com per scaricare il numero di serie. Conservare una copia del numero di serie in un luogo sicuro.
- 5 Fare clic su **Avanti**.
- 6 Fare clic su **Accetto** per accettare la licenza e selezionare **Avanti**.
- 7 Nella pagina **Recupero numero di serie VA**, copiare il **Numero di serie**.
- 8 Fare clic su **Scarica numeri di serie VA per Data Loss Prevention: per uso futuro**.
- 9 Fare clic su **Download licenza** nella colonna di sinistra per continuare.
- 10 Immettere il numero di serie e fare clic su **Invia**.
- 11 Creare una passphrase, inserirla e fare clic su **Avanti**. Conservare una copia della passphrase in un luogo sicuro.
- 12 Scegliere la licenza corrispondente al numero di serie e fare clic su **Scarica file di licenza**. È necessario scaricare il file di attivazione del dispositivo `bcl` e applicarlo durante la configurazione del dispositivo.

Acquisizione del file di licenza e del software di rilevamento Symantec Data Loss Prevention per il dispositivo virtuale

- 1 Tornare indietro a **Download di software (Supporto tecnico > Download > Network Protection (Blue Coat) Downloads)**.
- 2 Accedere a **Sfogliare i miei software e la mia documentazione > DataLossPrevention (DLP) > DLPSYM**. Qui sono disponibili tutti i file necessari per configurare Symantec Data Loss Prevention Enforce Server e il rilevatore del dispositivo virtuale.
- 3 Fare clic sulla licenza per il software acquistato. Le licenze sono
 - **DLP-EML-VA** Per il dispositivo virtuale Symantec Data Loss Prevention Network Prevent for Email.
`SymantecDLPEVA150_License.zip` contiene il file `slf` che è necessario caricare in Enforce Server per attivare il rilevatore del dispositivo.
 - **DLP-WEB-VA** Per il dispositivo virtuale Symantec Data Loss Prevention Network Prevent for Web

`SymantecDLPWA150_License.zip` contiene il file `.slf` che è necessario caricare in Enforce Server per attivare il rilevatore del dispositivo.

- **DLP APIC VA** Per il dispositivo virtuale Rilevamento API per le app degli sviluppatori Symantec Data Loss Prevention

`SymantecDLPAPVA150_License.zip` contiene il file `.slf` che è necessario caricare in Enforce Server per attivare il rilevamento del dispositivo.

- 4 Scaricare il software per il dispositivo stato acquistato.

Vedere ["Panoramica della distribuzione per il dispositivo virtuale"](#) a pagina 2297.

Acquisizione dei file di licenza per il dispositivo hardware DLP S500-10

Seguire queste procedure per ottenere il file di attivazione e il file di licenza del software di rilevamento per il dispositivo hardware DLP. Dopo avere ottenuto i file, applicare il file di attivazione per il dispositivo hardware nella riga di comando. Il software di rilevamento è già disponibile nel dispositivo hardware. Applicare la licenza per il software di rilevamento nella console di amministrazione di Enforce Server.

Come ottenere il file di attivazione del dispositivo per il sistema operativo del dispositivo hardware DLP S500-10

- 1 Accedere a https://support.symantec.com/en_US.html.
- 2 Accedere a **Centro di supporto > MySymantec > Portale delle licenze** ed effettuare l'accesso al proprio account Symantec.
- 3 Dal **Portale delle licenze**, selezionare **Network Protection (Blue Coat) License**.
- 4 Immettere il numero di serie presente nell'e-mail di avviso spedizione di Symantec e fare clic su **Invia**. Il numero di serie è disponibile anche nel dispositivo hardware DLP S500-10.
- 5 Scegliere la licenza corrispondente al numero di serie e fare clic su **Scarica file di licenza**. È necessario scaricare il file di attivazione del dispositivo `bcl` e applicarlo durante la configurazione del dispositivo.

Come ottenere la licenza di rilevamento Symantec Data Loss Prevention per il dispositivo hardware DLP S500-10

- 1 Accedere a https://support.symantec.com/en_US.html.
- 2 Accedere a **Gestione licenze > Gestione licenze Network Protection (Blue Coat)** ed effettuare l'accesso all'account.
- 3 Accedere a **Sfoglia i miei software e la mia documentazione > DataLossPrevention (DLP) > DLPSYM,S500**.

- 4 Fare clic su **Symantec Data Loss Prevention 15.0 Network Prevent for Web Hardware Appliance S500-10**. Qui è possibile trovare tutti i file necessari per la configurazione di DLP Enforce Server e del dispositivo hardware DLP. `SymantecDLPWHA150_License.zip` contiene il file `slf` che è necessario caricare in Enforce Server per attivare il rilevatore del dispositivo.
- 5 Scaricare il file di licenza. Il software Symantec Data Loss Prevention 15.0 Network Prevent for Web è già installato in DLP S500-10.

Vedere ["Panoramica della distribuzione per il dispositivo hardware DLP-S500"](#) a pagina 2302.

Informazioni sull'interfaccia da riga di comando (CLI)

È possibile accedere interfaccia della riga di comando tramite ssh o la console del dispositivo. La riga di comando presenta diverse modalità, tra cui `config` e `enable`. La maggior parte delle l'attività di Symantec Data Loss Prevention e di gestione licenze viene eseguita in modalità `enable`.

Inoltre, è presente una riga di comando per la configurazione iniziale che è accessibile solo dalla console. La riga di comando per la configurazione iniziale è utilizzata per impostare i parametri di base della rete del dispositivo.

L'interfaccia da riga di comando include una guida interna e utilizza il completamento automatico, per una maggiore facilità d'uso. Solo i comandi CLI utilizzati da Data Loss Prevention sono documentati e supportati. Vedere *Riferimento dell'interfaccia da riga di comando di dispositivo Symantec Data Loss Prevention* all'indirizzo <http://www.symantec.com/docs/DOC10599.html> per dettagli su ciascun comando supportato.

Vedere ["Panoramica della distribuzione per il dispositivo virtuale"](#) a pagina 2297.

Informazioni su ottimizzazione delle prestazioni e dimensionamento per i dispositivi

Ogni dispositivo hardware DLP-S500-10 può supportare 10.000 utenti di Network Prevent for Web. Le linee guida per il dimensionamento applicabili a Enforce Server e ai server di rilevamento si applicano anche ai dispositivi. È possibile seguire le linee guida esistenti presentate nella *Guida ai requisiti di sistema di Symantec Data Loss Prevention per 15.0* all'indirizzo www.symantec.com/DOC10602.

Distribuzione dei dispositivi DLP

Il capitolo contiene i seguenti argomenti:

- [Panoramica della distribuzione per il dispositivo virtuale](#)
- [Configurazione del dispositivo virtuale](#)
- [Panoramica della distribuzione per il dispositivo hardware DLP-S500](#)
- [Configurazione del dispositivo DLP-S500](#)
- [Aggiunta di un dispositivo](#)
- [Configurare il dispositivo Rilevamento API per le app degli sviluppatori](#)

Panoramica della distribuzione per il dispositivo virtuale

La distribuzione dei dispositivi è un processo in più fasi. Vedere [Tabella 89-1](#) per una panoramica dei passaggi che è necessario eseguire per distribuire un dispositivo virtuale. Per ulteriori dettagli, vedere le sezioni relative a riferimenti incrociati.

Tabella 89-1 Panoramica della configurazione del dispositivo virtuale

Passaggio	Azione	Ulteriori informazioni
Passaggio 1	Scaricare i file zip da Download software Symantec. Questi file contengono i file compressi <code>ovf</code> (immagine del computer virtuale) per il dispositivo. Il file zip contenente il file <code>ovf</code> contiene anche i file del disco virtuale, i file di informazioni e i file di checksum.	Vedere "Acquisizione dei file di attivazione e di licenza per il dispositivo virtuale" a pagina 2293.
Passaggio 2	Raccogliere le informazioni necessarie per l'installazione.	Vedere "Configurazione del dispositivo virtuale" a pagina 2299.
Passaggio 3	Distribuire l'immagine del computer virtuale, che include sia il sistema operativo che il disco dati, dalla riga di comando in VMware ESXi.	Vedere "Per scaricare e distribuire l'immagine del computer virtuale del dispositivo" a pagina 2300.
Passaggio 4	Immettere il numero di serie (10 cifre) dal file di attivazione. Salvare questo numero; sarà necessario immetterlo di nuovo durante la registrazione del dispositivo con Enforce Server.	Vedere "Per scaricare e distribuire l'immagine del computer virtuale del dispositivo" a pagina 2300.
Passaggio 5	Configurare le interfacce di rete dalla riga di comando.	Vedere "Per scaricare e distribuire l'immagine del computer virtuale del dispositivo" a pagina 2300.
Passaggio 6	Configurare la password della console dalla riga di comando.	Vedere "Per configurare le password" a pagina 2301.
Passaggio 7	Configurare la password di attivazione dalla riga di comando.	Vedere "Per configurare le password" a pagina 2301.
Passaggio 8	Applicare il file di attivazione <code>.bcl</code> per il dispositivo.	Vedere "Per applicare il file di attivazione <code>.bcl</code> per il dispositivo" a pagina 2301.

Passaggio	Azione	Ulteriori informazioni
Passaggio 9	Impostare e configurare il dispositivo per comunicare con la console di amministrazione di Enforce Server. Quindi applicare il numero di serie della licenza dalla console di amministrazione di Enforce Server.	Vedere "Aggiunta di un dispositivo" a pagina 2305. Vedere "Configurare il dispositivo Rilevamento API per le app degli sviluppatori" a pagina 2306.
Passaggio 10	Configurare il componente di rilevamento del dispositivo.	Vedere "Server Network Prevent for Email - Configurazione di base" a pagina 248. Vedere "Server Network Prevent for Web - Configurazione di base" a pagina 251.
Passaggio 11	Configurare un archivio chiavi del server TLS.	Per il dispositivo di rilevamento di e-mail, è disponibile un'opzione per configurare una chiave del server TLS. La chiave privata deve essere una chiave RSA.

Vedere ["Configurazione del dispositivo virtuale"](#) a pagina 2299.

Configurazione del dispositivo virtuale

Dopo aver acquistato una licenza per il dispositivo di rilevamento, applicare il file di attivazione dalla riga di comando all'interno del computer virtuale. Stabilire quindi la connessione tra il dispositivo ed Enforce Server dalla console di amministrazione di Enforce Server.

Nota: È possibile eseguire un solo tipo di rilevamento (ad esempio, Network Prevent for Email) su un dispositivo per volta. Symantec non supporta più tipi di rilevamento sullo stesso dispositivo.

È necessario avere le seguenti informazioni a disposizione per eseguire la configurazione iniziale:

- Indirizzo IP
- Subnet mask
- Indirizzo gateway
- Numero di serie

- Passphrase
- Password della console per accedere all'interfaccia da riga di comando con il protocollo Secure Shell (SSH) e accedere ai comandi avanzati nell'interfaccia da riga di comando
- Password di attivazione per l'accesso amministrativo al dispositivo
- Indirizzo IP del gateway predefinito
- Indirizzo IP del server DNS primario
- Per il dispositivo di Rilevamento API per le app degli sviluppatori, un file di archivio chiavi in formato PKCS12 (.pfx o .p12).
- Per il dispositivo di Rilevamento API per le app degli sviluppatori, un file di archivio attendibilità in formato PKCS12(.pfx o .p12).

Per scaricare e distribuire l'immagine del computer virtuale del dispositivo

- 1 Per scaricare l'immagine del computer virtuale del dispositivo da Download software Symantec.
- 2 Fare clic sull'icona di **accensione** in VMware ESXi per avviare il dispositivo virtuale. La formattazione e la partizione del disco richiedono qualche minuto. Potrebbe venire visualizzata una schermata nera per alcuni momenti durante questo processo di avvio.
- 3 Introdurre il numero di serie (10 cifre) allegato al file di attivazione scaricato da Symantec.
- 4 Dopo l'avvio del dispositivo, quando richiesto, premere **<Enter>** tre volte. Il processo di configurazione comincia.
- 5 Quando viene visualizzata una richiesta, selezionare l'opzione **2: Setup Console** (Configura console) per configurare le interfacce di rete nel dispositivo.
- 6 Immettere l'indirizzo IP del dispositivo virtuale.
- 7 Immettere la subnet mask del dispositivo virtuale.
- 8 Immettere l'indirizzo IP del gateway del dispositivo virtuale.
- 9 Immettere l'indirizzo IP del server DNS per il dispositivo.

Per configurare le password

- 1 Specificare una password della console in **Enter console password** (Immettere la password della console). La password della console consente di accedere all'interfaccia da riga di comando (CLI) utilizzando il protocollo Secure Shell (SSH).
- 2 Specificare una password di attivazione in **Enter enable password** (Immettere la password di attivazione). La password di attivazione consente l'accesso amministrativo utilizzando l'interfaccia da riga di comando.

Nota: Ignorare il messaggio che dice che è possibile accedere alla porta 8082 per l'amministrazione. Questa porta non è attualmente disponibile per gestire il dispositivo virtuale.

Per applicare il file di attivazione .bcl per il dispositivo

Accedere all'interfaccia da riga di comando e applicare il file di attivazione ricevuto da Symantec.

- 1 Immettere il nome host:

```
ssh admin@[your host name here].
```
- 2 Immettere la password della console:

```
[your console password here]
```
- 3 Al prompt, immettere enable:

```
localhost> enable
```
- 4 Immettere la password di attivazione:

```
localhost# [your enable password here]
```
- 5 Per applicare il file di attivazione ricevuto da Symantec e precedentemente salvato nell'URL di un server HTTP e la passphrase configurata nel portale delle licenze Protezione rete, inserire:

```
localhost# licensing load url [your url here] passphrase [your passphrase here]
```

In alternativa, utilizzare il comando `licensing inline` e copiare e incollare la licenza.
- 6 Per verificare che la licenza è stata installata, immettere:

```
localhost# licensing view
```

- 7 Riavviare il dispositivo affinché la licenza abbia effetto:

```
localhost# restart
```

- 8 Accedere alla console di amministrazione di Enforce Server per configurare la comunicazione tra il dispositivo virtuale e la console di amministrazione di Enforce Server.

Vedere ["Aggiunta di un dispositivo"](#) a pagina 2305.

Vedere ["Configurare il dispositivo Rilevamento API per le app degli sviluppatori"](#) a pagina 2306.

Panoramica della distribuzione per il dispositivo hardware DLP-S500

[Tabella 89-2](#) fornisce una panoramica dei passaggi per la distribuzione di un dispositivo hardware DLP-S500. Il dispositivo hardware è dotato di un'immagine virtuale preinstallata e di un file di attivazione.

Tabella 89-2 Panoramica della configurazione del dispositivo hardware

Passaggio	Azione	Ulteriori informazioni
Passaggio 1	Scaricare i file di attivazione e licenza software dal Download software Symantec. Questi file contengono i file compressi <code>ovf</code> (immagine del computer virtuale) per il dispositivo. Il file zip contenente il file <code>ovf</code> contiene anche i file del disco virtuale, i file di informazioni e i file di checksum.	Vedere "Acquisizione dei file di attivazione e di licenza per il dispositivo virtuale" a pagina 2293.
Passaggio 2	Raccogliere le informazioni necessarie per la configurazione.	Vedere "Configurazione del dispositivo DLP-S500" a pagina 2303.
Passaggio 3	Eseguire la configurazione iniziale per l'hardware DLP-S500.	Vedere "Per eseguire la configurazione iniziale per DLP-S500" a pagina 2304.
Passaggio 4	Configurare le interfacce di rete dalla riga di comando.	Vedere "Per configurare le interfacce di rete" a pagina 2304.
Passaggio 5	Specificare una password della console.	Vedere "Per configurare le password" a pagina 2304.

Passaggio	Azione	Ulteriori informazioni
Passaggio 6	Specificare una password di attivazione.	Vedere "Per configurare le password" a pagina 2304.
Passaggio 7	Applicare il file di attivazione .bcl per il dispositivo.	Vedere "Per applicare il file di attivazione .bcl per il dispositivo hardware" a pagina 2305.
Passaggio 8	Configurare il dispositivo e applicare il numero di serie del file di attivazione dalla console di amministrazione di Enforce Server.	Vedere "Aggiunta di un dispositivo" a pagina 2305. Vedere "Configurare il dispositivo Rilevamento API per le app degli sviluppatori" a pagina 2306.
Passaggio 9	Configurare il componente di rilevamento del dispositivo.	Vedere "Server Network Prevent for Web - Configurazione di base" a pagina 251.

Vedere ["Configurazione del dispositivo DLP-S500"](#) a pagina 2303.

Configurazione del dispositivo DLP-S500

Vedere la *Guida introduttiva di DLP-S500* per informazioni sull'accensione dell'hardware DLP-S500, l'installazione su rack del dispositivo e il collegamento dei cavi. Alcune di tali informazioni sono ripetute qui come riferimento.

In DLP-S500 è preinstallato il software DLP. Attualmente, solo Network Prevent for Web è offerto per il dispositivo hardware. Dopo aver configurato l'hardware, configurare il dispositivo di rilevamento nella console di amministrazione di Enforce Server.

È necessario avere le seguenti informazioni a disposizione per eseguire la configurazione iniziale:

- Indirizzo IP di DLP-S500
- Subnet mask
- Password della console per accedere all'interfaccia da riga di comando con il protocollo Secure Shell (SSH) e accedere ai comandi avanzati nell'interfaccia da riga di comando
- Password di attivazione per l'accesso amministrativo al dispositivo.
- Indirizzo IP del gateway predefinito
- Indirizzo IP del server DNS primario

Per eseguire la configurazione iniziale per DLP-S500

- 1 Confermi che un cavo seriale null-modem sia collegato dal dispositivo alla porta seriale di una workstation.
- 2 Aprire un programma di emulazione terminale come Microsoft HyperTerminal, PuTTY, Tera Term o Procomm.
- 3 Configurare le seguenti impostazioni nel software di emulazione terminale:
 - Velocità in baud: 9600
 - Parità: nessuna
 - Controllo di flusso: nessuno
 - Bit di dati: 1
 - Bit di stop: 8
- 4 Accendere il dispositivo (se non è già acceso).
- 5 Dopo l'avvio del dispositivo, quando richiesto, premere **<Enter>** tre volte. Il processo di configurazione comincia.

Per configurare le interfacce di rete

- 1 Quando viene visualizzata la richiesta, selezionare l'opzione **2: Setup Console** (Configura console) per configurare le interfacce di rete.
- 2 Specificare gli indirizzi IP che si desidera utilizzare per il dispositivo in **Enter interface number to configure [3]** (Immettere il numero di interfaccia da configurare)
- 3 Immettere l'indirizzo IP del server DNS.

Per configurare le password

- 1 Specificare una password della console in **Enter console password** (Immettere la password della console). La password della console consente di accedere all'interfaccia da riga di comando (CLI) utilizzando il protocollo Secure Shell (SSH).
- 2 Specificare una password di attivazione in **Enter enable password** (Immettere la password di attivazione). La password di attivazione consente l'accesso amministrativo utilizzando l'interfaccia da riga di comando.

Nota: Ignorare il messaggio che dice che è possibile accedere alla porta 8082 per l'amministrazione. Questa porta non è attualmente disponibile per gestire DLP-S500.

Per applicare il file di attivazione .bcl per il dispositivo hardware

- 1 Immettere il nome host:

```
ssh admin@[your host name here]
```

- 2 Immettere la password della console:

```
[your console password here]
```

- 3 Al prompt, immettere enable:

```
localhost> enable
```

- 4 Immettere la password di attivazione:

```
localhost# [your enable password here]
```

- 5 Per applicare la licenza hardware ricevuta da Symantec e precedentemente salvata nell'URL di un server HTTP, immettere:

```
localhost# licensing load url [your url here]
```

In alternativa, utilizzare il comando `licensing inline` e copiare e incollare la licenza.

- 6 Per verificare che la licenza è stata installata, immettere:

```
localhost# licensing view
```

- 7 Riavviare il dispositivo affinché la licenza abbia effetto:

```
localhost# restart
```

- 8 Accedere alla console di amministrazione di Enforce Server per configurare la comunicazione tra DLP-S500 e la console di amministrazione di Enforce Server.

Vedere ["Aggiunta di un dispositivo"](#) a pagina 2305.

Vedere ["Configurare il dispositivo Rilevamento API per le app degli sviluppatori"](#) a pagina 2306.

Aggiunta di un dispositivo

Dopo aver configurato il dispositivo, è possibile registrare il dispositivo di rilevamento nella console di amministrazione di Enforce Server.

Per aggiungere un dispositivo di rilevamento

- 1 Accedere alla console di amministrazione di Enforce Server come amministratore.
- 2 Accedere a **Sistema > Server e rilevatori**.

- 3 Fare clic su **Aggiungi server...Dispositivo**.
 - 4 Viene visualizzata la schermata **Aggiungi un dispositivo**.
 - 5 Scegliere un tipo di dispositivo di rilevamento da aggiungere e fare clic su **Avanti**.
- Vedere "[Configurare il dispositivo Rilevamento API per le app degli sviluppatori](#)" a pagina 2306.

Configurare il dispositivo Rilevamento API per le app degli sviluppatori

Dopo aver aggiunto il dispositivo Rilevamento API per le app degli sviluppatori, seguire questi passaggi di configurazione:

Per configurare il dispositivo Rilevamento API per le app degli sviluppatori

- 1 Aggiungere un nome per questo dispositivo nel campo **Nome dispositivo**.
- 2 Immettere il numero di serie di 10 cifre ricevuto da Symantec nel campo **Numero di serie**.
- 3 Immettere il nome host o l'indirizzo IP nel campo **Nome host o indirizzo IP**.
- 4 Immettere `admin` nel campo **Nome utente**.
- 5 Immettere la password di amministrazione nel campo **Password**.
- 6 Immettere di nuovo la password nel campo **Immettere di nuovo la password**.

Nota: Questa password è la password di accesso alla **console** configurata precedentemente. Non è la password di **attivazione**.

- 7 Nel campo **Carica archivio chiavi per certificato SSL**, fare clic su **Sfoglia** per selezionare il file archivio chiavi PKCS12.
- 8 Immettere la password archivio chiavi nel campo **Password archivio chiavi**.
- 9 Nel campo **Carica archivio attendibilità per convalidare il certificato client**, fare clic su **Sfoglia** per selezionare il file di archivio attendibilità PKCS12.
- 10 Fare clic su **Salva**.

Ulteriori informazioni sui comandi dell'interfaccia da riga di comando (CLI) si trovano in *Riferimento dell'interfaccia da riga di comando di Symantec Data Loss Prevention* all'indirizzo www.symantec.com/DOCS/DOC10599.html.

Attività di post-distribuzione

Il capitolo contiene i seguenti argomenti:

- [Dissociazione o reimpostazione di un dispositivo DLP](#)
- [Aggiornamento del software del dispositivo](#)
- [File di registro e registrazione per i dispositivi](#)

Dissociazione o reimpostazione di un dispositivo DLP

Enforce Server dissocia automaticamente un dispositivo se il dispositivo viene rimosso da Enforce Server mentre è ancora connesso a Enforce Server. È necessario dissociare manualmente un dispositivo quando viene spostato verso un altro Enforce Server senza essere rimosso dal precedente Enforce Server. Queste sono alcune situazioni in cui è necessario reimpostare un dispositivo:

- Quando si sposta un dispositivo da un'istanza di Enforce Server a un'altra: è necessario dissociare il dispositivo dall'istanza di Enforce precedente prima di connetterlo alla nuova istanza.
- Clonazione di VM: reimpostare l'ID del dispositivo dopo aver clonato le VM. Ogni dispositivo deve avere un ID univoco affinché Enforce possa distinguerlo.
- Ricominciare da zero: eseguire un ripristino delle impostazioni di fabbrica, che riformatta e cancella il disco di dati. Un ripristino delle impostazioni di fabbrica non riporta il dispositivo al software precedente.

Per dissociare un dispositivo da Enforce Server

- ◆ Immettere il seguente comando nell'interfaccia da riga di comando di amministrazione (dopo essere entrati nella modalità `enable`):

```
dlp admin unbind
```

Per eseguire un ripristino delle impostazioni di fabbrica

- 1 Ottenere l'ID del dispositivo.
- 2 Individuare il dispositivo alla console.
- 3 Per riconfigurare il dispositivo per reimpostare l'ID, consultare [Dissociazione o reimpostazione di un dispositivo DLP](#).

Vedere ["Aggiornamento del software del dispositivo"](#) a pagina 2308.

Aggiornamento del software del dispositivo

L'aggiornamento dell'immagine di un dispositivo può essere eseguito dalla pagina **Sistema > Server e rilevatori > Panoramica > Preparazione sistema e aggiornamento dispositivi**.

La sezione **Aggiornamento software dispositivi** è in mezzo a questa pagina. In questa pagina è possibile scegliere le seguenti azioni di aggiornamento per i dispositivi installati:

- **Distribuisce immagine dispositivo**
- **Aggiorna dispositivi**
- **Ripristina aggiornamento dispositivi**
- **Annulla azioni in corso**

Tutti i dispositivi installati vengono visualizzati in questa pagina, con i seguenti dettagli relativi a ciascun dispositivo:

- **Server** - un elenco di tutti i dispositivi, sia hardware che virtuali
- **Fattore di forma**
- **Versione dispositivo corrente**
- **Data installazione**
- **Attivo dal** - data dello stato Attivo
- **Versione disponibile per l'aggiornamento**
- **Preparazione aggiornamento**
- **Versione disponibile per il ripristino** (la versione precedente utilizzata per il ripristino, se presente).

Nota: Quando si eseguono azioni per **Aggiornamento software dispositivi**, la distribuzione di immagini, l'aggiornamento e il riavvio possono richiedere del tempo. È inoltre possibile rilevare un'apparente disconnessione, ma si tratta di un comportamento standard. Al completamento dell'azione viene visualizzato un nuovo stato nelle colonne **Versione o Preparazione aggiornamento**. È inoltre possibile visualizzare nuove informazioni sulla pagina **Server e rilevatori > Dettagli server**.

In generale, per ogni azione eseguita, è necessario:

- Individuare un'immagine (se necessaria per quell'azione).
Selezionare il dispositivo che si desidera aggiornare.
Selezionare l'azione.

Per aggiornare un dispositivo

- 1 Trovare l'immagine di upgrade .bcsi scaricata da Download software Symantec. Caricare l'immagine in un server HTTP locale.
- 2 Accedere a **Sistema > Server e rilevatori > Panoramica > Preparazione sistema e aggiornamento dispositivi**.
- 3 In **Aggiornamento software dispositivi**, selezionare **Distribuisci immagine dispositivo**
- 4 Selezionare il dispositivo che si desidera aggiornare.
- 5 Selezionare l'immagine caricata nel passaggio 1 dal menu **URL immagine programma di installazione**.
- 6 Fare clic su **Esegui azioni per i dispositivi selezionati**. La distribuzione dell'immagine potrebbe richiedere del tempo. Dopo la distribuzione dell'immagine, viene visualizzato **Pronto all'aggiornamento** nella colonna **Preparazione aggiornamento** per il dispositivo selezionato.
- 7 Selezionare **Aggiorna dispositivi** e selezionare il dispositivo che si desidera aggiornare.
- 8 Fare clic su **Esegui azioni per i dispositivi selezionati**.

Nota: Il numero di versione del dispositivo DLP nella pagina **Server e rilevatori** non corrisponde al numero di versione del dispositivo DLP visualizzato nella pagina **Aggiornamento software dispositivi**. La pagina **Aggiornamento software dispositivi** presenta un numero di versione con un ".0" in più. Inoltre, benché i numeri di versione DLP corrispondano, il numero di build per i dispositivi potrebbe essere differente dal numero di build per i server.

Vedere ["File di registro e registrazione per i dispositivi"](#) a pagina 2310.

File di registro e registrazione per i dispositivi

Enforce Server raccoglie i registri dei dispositivi.

Per raccogliere i registri

- ◆ **Accedere a Sistema > Server e rilevatori > Registri** e selezionare il dispositivo dall'elenco.

Per ulteriori informazioni vedere "Gestione di file di registro" nel *Manuale dell'amministratore di Symantec Data Loss Prevention*.

Nota: La sezione **File di configurazione registri** è disattivata per i dispositivi e non può essere utilizzata.

Vedere ["Informazioni su ottimizzazione delle prestazioni e dimensionamento per i dispositivi"](#) a pagina 2296.

Indice

Simboli

1697

A

- accesso basato sui moduli
 - disattivazione 160
- accesso e disconnessione 82
- Account amministratore
 - account e-mail 85
 - informazioni 83
 - password, modifica 84
 - password, reimpostazione 128
- Active Directory 2184
 - attributi 2182
 - attributo 2186
- AdminPasswordReset, utilità 128
- agente 2252
- agenti utente 1808
- aggiornamenti del sistema 238
- aggiornamenti, sistema 238
- AllowHosts, campo 1812
- amministrazione
 - introduzione a 80
- API di reporting 1657
- API di reporting e aggiornamento incidenti
 - privilegi 119
- applicazioni
 - elenchi di incidenti 1621
 - istantanee incidente 1624
 - report incidente 1619
 - riepiloghi degli incidenti 1628
- Appunti 2067
- archivi Web 1704
- archivio credenziali
 - aggiunta dell'autenticazione 168
 - eliminazione di credenziali 169
 - gestione 169
 - modifica di credenziali 169
- archivio delle credenziali
 - credenziali endpoint 168
- attributi 1586, 1591, 1708
 - applicazione 2188
 - definiti dall'utente 2185
 - tipi 2185
- attributi agente 2188
 - definiti dall'utente 2188
- attributi dell'agente
 - gestione 2184
- attributi di stato 1700
- attributi personalizzati 1591, 1706, 1708
 - creazione 1709
 - impostazione manuale dei valori 1710
 - inserimento 1708
 - istantanee incidente 1674
 - modifica 1709
 - opzione Ricerca (istantanea incidente) 1708
 - uso 1708
 - utilizzo 1706
- attributo dell'agente
 - creazione di un nuovo 2185
- autenticazione 226
- Autenticazione del certificato
 - aggiunta di certificati CA 149
 - configurazione 145
 - configurazione dei controlli di revoca 155
 - risoluzione dei problemi 159
- autenticazione del certificato
 - attivazione o disattivazione 147
 - configurazione dei controlli di revoca 153
 - mapping dei valori CN 152
- autenticazione tramite password
 - attivazione o disattivazione 147
 - disattivazione 160
- autorizzazione cloud
 - Box 1836–1837
 - gestione 1836
- avvisi. *Vedere* avvisi di sistema
- avvisi di sistema
 - aggiunta 185
 - informazioni 183
 - modifica 185
 - server di configurazione 183

B

base di dati
 regolazione delle soglie di allerta 217

best practice
 allocazione di memoria ridotta per le politiche endpoint 658
 annullamento della distribuzione di profili inutilizzati 661
 creazione di un'area di gestione temporanea dei documenti 658
 definizione precisa della categoria 656
 DGM con profilo 859
 distribuzione di contenuto generico nel set di training negativo 657
 esecuzione di test negativi 648
 non utilizzo di VML per rilevare grafica o PII 655
 ottimizzazione profilo prima della distribuzione alla produzione 661
 per rilevare contenuto basato su testo e non strutturato 654
 politiche 462, 464–466, 468–469, 471
 raccolta del massimo numero di documenti di esempio 657
 rifiuto del training con livello di precisione superiore al 5% 659
 utilizzo di archivi di documenti 658
 valutazione dei livelli di precisione per fold 659
 VML, riepilogo 653

BindAddress, campo 1812

blocco richieste 1813

C

Campi RequestProcessor 1797, 1803

campi RequestProcessor 1800

Campo AddDefaultHeader 1797

Campo AddDefaultPassHeader 1798

campo AllowHosts 1800

campo BindAddress 1800

campo di accesso informazioni autorità 153

campo minSizeofGetURL 1813

Campo MTA successivo 1796

Campo MTAResubmitPort 1797

Campo ServerSocketPort 1797

Campo TagHighestSeverity 1803

Campo TagPolicyCount 1803

Campo TagScore 1803

caricamento di documenti
 dimensione massima 658

categorie di conservazione 1521

CD/DVD

elenco 2235

informazioni 2064

cerca plug-in
 filtraggio protocollo script 1766

certificati CA
 importazione 272

certificati SSL
 importazione 272

comando iptables 1798–1799

comando telnet 1799

condizioni corrispondenze della politica
 proprietà file 395

condizioni di corrispondenza di politiche composte 401
 endpoint 396
 logica di esecuzione del server 402
 rete 396
 semplici 401
 tipi 392

condizioni di politiche
 Contenuto corrispondente a identificatore dati 700

condizioni per la corrispondenza della politica
 componenti del messaggio 398
 contenuto 393
 contenuto basato sull'indice 393
 corrispondenza contenuto trasversale 398
 eccezioni 400
 rilevamento in due fasi 403

condizioni per la corrispondenza di politiche
 identità e gruppi 397

Configurazione agente
 aggiunta 2111
 informazioni 2110

configurazione agente
 applicazione 2179

configurazione corrispondenza parziale contenuto
 IDM 590

configurazione del sistema, iniziale 83

configurazione di Rilevamento applicazioni
 aggiunta 2274
 Gatelet CloudSOC 2274
 modifica 2278
 Securlet CloudSOC 2275
 Servizio API rilevamento cloud 2277

conflitti di gruppo
 visualizzazione 2192

console. *Vedere* console di amministrazione

- console di amministrazione
 - accesso e disconnessione 82
 - informazioni 81
- console di amministrazione di Enforce Server
 - schermata Profili 85
- Console Enforce. *Vedere* console di amministrazione
- controlli di applicazioni
 - informazioni 2231
- controlli di revoca
 - supporto 153
- controlli di revoca CRLDP
 - configurazione di un proxy 157
 - supporto 153
- controlli di revoca OCSP
 - configurazione 158
 - configurazione di un proxy 157
 - disattivazione 158
 - supporto 153
- controllo applicazioni 2067
 - aggiunta di un'applicazione 2241
 - aggiunta di un'applicazione 2237
- Controllo dei processi avanzato 241
- correlazioni 1590
- corrispondenza parziale contenuto 590
- corrispondenze 1590
- credenziali 167
- credenziali di autenticazione 167
- crittografia dei file 1928
- Crittografia incentrata sulle informazioni
 - DLP Agent 2133
 - impostazioni 2133
 - impostazioni applicazione 2232

D

- dashboard 1637
 - eliminazione 1669
 - modifica 1656
 - visualizzazione 1639
- database
 - creazione di un report 217
 - report 215
 - strumenti diagnostici 215
 - visualizzazione dei dettagli della tabella 218
 - visualizzazione di allocazione spazi tabelle e file di dati 216
- database Oracle
 - impostazione NLS_LANGUAGE 95
 - impostazione NLS_TERRITORY 95

- Dettagli server, schermata
 - configurazione di server 244
- dimensionamento, profili
 - allocazione di memoria 658
 - soglia di rilevanza 658
- dimensioni set di training
 - almeno 50 657
 - consigliati 250 657
- Directory Group Matching (DGM)
 - condizione di mittente/utente basato su una directory con profilo 506
 - Destinatario in base a una condizione Profiled Directory 859
 - implementazione sincronizzata 850
 - Mittente/Utente in base a una condizione Profiled Directory 858
 - sincronizzato 846
- Directory Group Matching (DGM), con profilo
 - con profilo 855
 - condizioni con profilo 857
 - creazione di file origine dati esatti 487
 - flusso di lavoro 856
 - rilevamento in due fasi 856
- Directory Group Matching (DGM), sincronizzata
 - indicizzazione della pianificazione 164
 - Mittente/utente basato su gruppo di server di directory 851
- Directory Group Matching (DGM), sincronizzato
 - Destinatario basato su gruppo di server di directory 852
- disinstallazione 2256
- dispositivi
 - schermata Dettagli server/rilevatore 277
- dispositivi mobili 226
- distribuzione
 - installazione invisibile 2252
 - SMS 2252
 - utilità Endpoint FlexResponse 2254
- DLP Agent
 - impostazioni agente avanzate 2133
 - integrità 2195
- documenti
 - tipi supportati 658
- Dominio host agente 2184
- Dominio utente connesso 2184

E

- e-mail
 - blocco 1800

- quarantena 1802
- eccezioni di gruppo, tipo
 - Destinatario corrispondente a criterio 840
- eccezioni di politica
 - composte 440
 - configurazione 437
- eccezioni di politica, configurazione
 - conteggio delle corrispondenze 431
- eccezioni di politiche
 - aggiunta 434
- elenchi di controllo di accesso (ACL)
 - istantanee incidente 1676
- elenchi di incidenti
 - applicazioni 1621
 - Network Discover/Cloud Storage Discover 1611
 - Network Monitor e Network Prevent 1580
- elenco di plugin 2252
- eliminazione
 - incidenti nascosti 1699
- Endpoint
 - regola di risposta Operazione annullata dall'utente 2075
- endpoint
 - configurazione della posizione dell'endpoint 2076
 - impostazione di regole di risposta per differenti impostazioni locali 2079
 - impostazioni agente avanzate 2133
 - livelli di registro dell'agente 2226
 - politiche per 2035
 - registri agente 2226
 - regola di risposta Quarantena 2088
 - regole di risposta con impostazioni locali differenti 2078
 - regole di risposta e di rilevamento incompatibili 2037
 - report di riepilogo 1605
 - schermata di riepilogo degli incidenti 1605
- Endpoint Discover
 - aggiunta di una regola 2088
 - configurazione di target 2091
 - creazione di un gruppo di politiche 2086
 - creazione di una politica 2087
 - Durata massima scansione 2104
 - Endpoint Discover target 2089
 - endpoint target 2080–2081
 - endpoint target, scansione parallela 2084
 - filtri 2096
 - funzionamento 2080
 - funzionamento della scansione incrementale 2083
 - implementazione 2089
 - impostazioni timeout scansione 2104
 - introduzione 78
 - report 2108
 - scansione 2080
 - scansione completa 2082
 - scansione incrementale 2082
 - Timeout inattività scansione 2104
- Endpoint Discover, scansioni
 - esclusione di elementi o archivi 2099
 - inclusione di elementi o archivi 2099
- Endpoint FlexResponse
 - attivazione su Enforce Server 2255
 - disinstallazione con l'utilità FlexResponse 2256
 - distribuzione 2250
 - distribuzione di plug-in 2251
 - distribuzione di plug-in mediante l'utilità Endpoint FlexResponse 2254
 - informazioni 2248
- Endpoint FlexResponse, utilità 2252
 - opzioni 2253
 - password 2254
- Endpoint Prevent
 - Citrix XenApp 2069
 - Citrix XenDesktop 2069
 - controlli CD/DVD 2064
 - controllo applicazioni 2067
 - creazione di politiche 2073
 - creazione di report su regole di risposta 1602
 - implementazione 2076
 - introduzione 78
 - macchine virtuali 2069
 - Microsoft Hyper-V 2069
 - monitor della rete 2063
 - monitoraggio 2060
 - monitoraggio degli Appunti 2067
 - monitoraggio della condivisione di rete 2066
 - monitoraggio di stampa/fax 2065
 - ospiti virtuali 2069
 - regola di risposta Blocca 2073
 - regola di risposta di blocco 2074
 - regola di risposta di notifica 2074
 - regola di risposta Notifica 2073
 - Remote Desktop Services 2069
 - report 2108
 - supporti rimovibili 2061
 - VMWare View 2069

- Endpoint Server
 - configurazione di base 255
 - configurazione di filtri di file 2117
 - Enforce
 - introduzione 75
 - registrazione 344
 - Enforce Server
 - attivazione di Endpoint FlexResponse 2255
 - avvisi, configurazione per l'invio 183
 - impostazione di regole di risposta per differenti
 - impostazioni locali 2079
 - informazioni 81
 - introduzione 75
 - regole di risposta con impostazioni locali
 - differenti 2078
 - scelta di una lingua diversa dall'inglese 95
 - esportazione attributi agente 2187
 - ethtool 1778
 - eventi dell'agente
 - schermata Dettagli eventi dell'agente 2216
 - eventi di agente
 - informazioni 2214
 - eventi di sistema 171
 - dettagli eventi 176
 - metodi di notifica 172
 - numeri di codice 187
 - report 172
 - report, filtro 174
 - report, salvati 175
 - risposte 180
 - server syslog 182
 - soglie, configurazione 177
 - tipi (gravità) di 177
 - Exact Data Matching (EDM)
 - aggiornamenti dell'indice 481
 - aggiungi i profili 501
 - condizione di politica 482
 - condizione EDM 503
 - conteggio delle corrispondenze 523
 - creazione del file origine dati 486
 - Directory EDM 483
 - eccezioni 482
 - esempio 473
 - file di indice 478
 - flusso di lavoro 484
 - funzionalità 474
 - gestisci i profili 501
 - indicizzazione remota 539
 - limiti di dimensione dell'origine dati 479
 - mapping di campi 480
 - preparazione per l'indicizzazione 488
 - pulizia dell'origine dati 480
 - Remote EDM Indexer, utilità 540
 - rilevamento in due fasi 484
 - Utilità SQL Preindexer 540
 - Exact Data Matching (EDM), configurazione
 - caricamento di origine dati esatti in Enforce 490
 - indicizzatore EDM remoto 490
 - Profilo dati esatti 492
 - Exact Data Matching (EDM), profilo
 - mapping di campi 496
 - pianificazione dell'indicizzazione di profili 499
- ## F
- file di registro 335
 - file di registro di debug 335–336, 352
 - file di registro di installazione 335
 - file di registro operativi 335
 - file in quarantena 1928
 - SharePoint 1956
 - File Plugins.properties 1889
 - filtraggio richieste 1808
 - filtraggio risposte 1809
 - Finestra di rinnovo della password 88
 - FlexResponse server
 - configurazione 1516, 1889, 1891
 - configurazione di proprietà personalizzate
 - per 1891
 - configurazione di un'azione di una regola di
 - risposta 1516
 - distribuzione di un plug-in 1888–1889, 1891
 - panoramica 1885
 - riparazione con 1887, 1895–1896
 - risoluzione dei problemi 1897
 - utilizzo di un'azione di risposta smart con 1895
 - flrnst.exe, utilità
 - disinstallazione dei plug-in 2256
 - distribuzione di plug-in 2254
 - informazioni 2252
 - recupero dell'elenco di plug-in 2257
 - recupero di plug-in 2256
- ## G
- GET, comandi 1789, 1812
 - Gruppi di agenti
 - strategia di distribuzione 2182

- gruppi di agenti 2181
 - aggiornamento obsoleto 2191
 - assegnazione delle configurazioni per la distribuzione 2192
 - creazione di un nuovo 2190
 - processo di distribuzione 2183
 - visualizzazione e gestione 2189
- gruppi di politiche
 - creazione 447
 - distribuzione 378
 - eliminazione 456
 - gestione 446
 - informazioni 377
 - modifica 447
 - predefinito 377
- gruppi di stati
 - aggiunta 1703
 - configurazione 1703
 - eliminazione 1703
- gruppi di utenti
 - creazione 847
- gruppo di agenti
 - condizioni 2190

I

- ICAP 76, 1807, 1811–1812
 - configurazione 1810
- ICE. *Vedere* Information Centric Encryption
- DLP Agent 2133
- ICE Cloud Console 225
- ICE, utilità 226
- Identificatori dati
 - best practice 765
 - clonazione manuale 726
 - configurazione 748
 - convalide 696
 - criteri 695
 - definiti dal sistema 693
 - modifica 699
 - normalizzatori di dati 764
- identificatori dati
 - aggiunta 698
 - convalide opzionali, caratteri accettabili 721
 - convalide opzionali, configurazione 720
 - elenco coperture 702
 - gestione 698
 - modifica dell'input di convalida 727
 - personalizzati, informazioni 751

- Identificatori di dati
 - limitazioni di lingua del modello, circa 751
- identificatori di dati
 - condizione Contenuto corrispondente a
 - identificatore dati 700
 - convalide facoltative, informazioni 695
 - coperture, informazioni 694
 - corrispondenza con diversi componenti 696
 - definiti dal sistema 682
 - elenco di normalizzatori 703
 - estensione 693
 - implementazione di convalide con script
 - personalizzati 765
 - implementazione di criteri 755
 - implementazione, personalizzati 749
 - informazioni 681
 - selezione di convalide 763
- impostazioni avanzate del server 1787
- incidente endpoint
 - elenchi 1594
 - informazioni specifiche al protocollo o alla destinazione 1604
- incidenti 1580, 1585–1587, 1590–1591
 - attributi di stato 1700
 - attributi personalizzati 1706, 1709
 - come impedire che vengano nascosti 1698
 - come nascondere 1696–1697
 - contrassegno automatico ai fini dell'eliminazione 1665
 - eliminazione 1660
 - riparazione 1583
 - visualizzazione 1697
- incidenti nascosti
 - eliminazione 1699
 - visualizzazione 1697
- Indexed Document Matching
 - DocSource.rdx 575
 - EncryptedDocSource.rdx 575
 - EndpointDocSource.rdx 575
 - LegacyEndpointDocSource.rdx 575
 - pianificazione dell'indicizzazione 602
- Indexed Document Matching (IDM)
 - aggiunta di profili di documento 588
 - best practice 609, 611–613
 - condizione di corrispondenza IDM 581
 - configurazione della condizione di corrispondenza 605
 - configurazione di profili di documento 588
 - corrispondenza di contenuti di file esatta 579

corrispondenza di contenuti di file parziale 579
 corrispondenza esatta di file 578
 esclusione di contenuto mediante lista
 bianca 585
 filtraggio per dimensioni file 601
 filtraggio per nome di file 599
 gestione profili documento 586
 implementazione 583
 indicizzazione remota 615
 lista bianca 582
 opzioni di indicizzazione remota 574
 origine dati documento 573
 panoramica 569
 piattaforme 571
 preparazione di un'origine dati di documento per
 l'indicizzazione 583
 Profilo documento 572
 Information Centric Encryption
 DLP Agent 1550
 informazioni 225
 installazione
 plug-in 2252
 internazionalizzazione. *Vedere* lingue e set di caratteri
 Internet Content Adaptation Protocol. *Vedere* ICAP
 Intestazione X-DLP-Max-Severity 1803
 Intestazione X-DLP-Policy-Count 1803
 Intestazione X-DLP-Score 1803
 intestazioni di violazioni di politiche 1802
 intestazioni sulle violazioni della politica
 attivazione 1802
 istantanee 1591
 istantanee di incidenti
 sezione delle corrispondenze 1675
 istantanee incidente
 applicazioni 1624
 informazioni su ACL 1676
 Network Discover/Cloud Storage Discover 1615
 scheda Correlazioni 1674
 scheda cronologia 1673
 sezione di attributi personalizzati 1674
 sezione Politica 1675

L

licenze 237
 lingue e set di caratteri
 scelta di una lingua diversa dall'inglese 95
 set di caratteri, utilizzo 92
 supporti lingue, informazioni 93
 supporti lingue, utilizzo 96

localizzazione. *Vedere* lingue e set di caratteri
 logdump.exe, strumento 2265

M

mail transfer agent. *Vedere* MTA
 manager-certauth.security 158
 manager-certauth.security file 156
 messaggi SOAP 339
 modalità di inoltro 1793
 modalità di prova 248, 1793, 1807
 modalità di riflessione 1793
 modelli di politica
 aggiunta 421
 Applicazione normative internazionali 411
 Applicazione normative statunitensi 408
 creazione di una politica da 405
 definiti dal sistema 376
 Documenti riservati 1324
 esportazione 383, 454
 GDPR 410
 HIPAA e HITECH (incluso PHI) 1416
 importazione 383, 453
 Privacy dei dati relativi allo stato 1451
 Protezione dei dati di clienti e dipendenti 412
 modelli di politica internazionali
 informazioni 803
 modelli di politica, configurazione
 profilo dati esatti, selezione 417
 profilo documento indicizzato, selezione 419
 modelli di politica, tipi
 Applicazione normative colombiane relative ai
 dati personali 417
 Applicazione norme di utilizzo accettabile 415
 modelli di politica, tipo
 Applicazione norme di sicurezza di rete 415
 Protezione dei dati riservati o classificati 413
 Yahoo e MSN Messenger sulla porta 80 1463
 modelli di rilevamento della politica, configurazione
 Codice sorgente 1450
 Codici fiscali britannici 1458
 Codici identificativi dei contribuenti (ITIN) 1422
 Codici SWIFT 1455
 Compatibilità Symantec DLP e Prevenzione 1455
 Comunicazioni con i concorrenti 1323
 Contratti di acquisizione e fusione 1426
 Curriculum 1444
 Data Protection Act (legge sulla protezione dei
 dati) del 1998 1327
 Dati crittografati 1335

- Dati di progetto 1441
 - Destinatari con restrizioni 1443
 - Diagrammi di rete 1432
 - Direttive UE sulla protezione dei dati 1329
 - Documenti di progettazione 1332
 - Documenti di pubblicazione 1442
 - FACTA 2003 (regole Red Flag) 1337
 - File con restrizioni 1443
 - File di password 1437
 - File multimediali 1424
 - File multimediali proprietari 1441
 - Gioco d'azzardo 1342
 - Human Rights Act (legge sui diritti umani) del 1998 1421
 - Informazioni finanziarie 1340
 - Informazioni sui prezzi 1441
 - Linguaggio offensivo 1433
 - Linguaggio razzista 1443
 - Linguaggio sessualmente esplicito 1449
 - marchi di controllo dei servizi di intelligence degli Stati Uniti (CAPCO) e DCID 1/7 1458
 - normativa sull'imparzialità della trasparenza SEC 1447
 - Numeri di carta di credito 1325
 - Numeri di passaporto britannici 1457
 - Numeri di previdenza sociale (SIN) canadesi 1321
 - Numeri di previdenza sociale britannici 1457
 - Numeri di tessera elettorale britannici 1456
 - Numeri Patente di guida del Regno Unito 1456
 - Numero NHS (National Health Service) britannico 1457
 - Payment Card Industry (PCI) Data Security Standard 1437
 - PIPEDA 1439
 - Protezione dei dati dei clienti 1325
 - Protezione dei dati dei dipendenti 1333
 - Relazione Caldicott 1319
 - Sarbanes-Oxley 1445
 - Sicurezza di rete 1433
 - Siti caricamento spyware comuni 1323
 - Siti Web non consentiti 1341
 - Violenza e armi 1460
 - Webmail 1460
 - modelli di rilevamento di politica, configurazione
 - Memorandum OMB 06-16 e disposizioni FIPS 199 1436
 - Regola NASD 2711 e regole NYSE 351 e 472 1427
 - modelli di rilevamento di politiche, configurazione
 - Classificazione GENSER Defense Message System (DMS) 1331
 - Export Administration Regulations (EAR) 1335
 - Gramm-Leach-Bliley 1414
 - International Traffic in Arms Regulations (ITAR) 1422
 - Linee guida sulla sicurezza del NERC per le società elettriche 1430
 - OFAC (Ufficio per il Controllo dei Fondi Stranieri) 1433
 - Regola NASD 3010 e regola NYSE 342 1428
 - modelli di rilevamento politica, configurazione
 - CAN-SPAM Act 1321
 - GDPR
 - Attività bancarie e finanza 1342
 - Identificazione governativa 1365
 - Profilo personale 1401
 - Sanità e assicurazioni 1389
 - Viaggi 1404
 - legge colombiana sulla protezione dei dati personali 1581 1322
 - Regolamento generale per la protezione dei dati
 - Attività bancarie e finanza 1342
 - Identificazione governativa 1365
 - Profilo personale 1401
 - Sanità e assicurazioni 1389
 - Viaggi 1404
 - Social Security Number statunitensi 1460
 - Sostanze illegali 1421
 - modelli politica
 - Regolamento generale per la protezione dei dati 410
 - modello di rilevamento politica, configurazione
 - Bacheca messaggi di Yahoo 1462
 - Monitoraggio a un solo livello 268
 - configurazione di base 256
 - monitoraggio della condivisione di rete 2066
 - MTA 76, 250, 1791, 1793, 1796
 - configurazione 1799
- N**
- Napatech 1780
 - nascondere
 - incidenti 1696–1697
 - nascosti
 - incidenti 1696
 - Network Discover
 - file di quarantena 1928

- file in quarantena
 - SharePoint 1956
 - funzionamento dei rilevatori 1977
 - report incidente 1610
 - Network Discover/Cloud Storage Discover
 - aggiunta di nuovi target 1826
 - configurazione 1823
 - configurazione di target 1830, 1832
 - elenchi di incidenti 1611
 - funzionamento di Discover 1821
 - impostazione 1823
 - introduzione 77, 1819
 - istantanee incidente 1615
 - modifica di target 1828
 - registrazione 341
 - report 1608
 - report incidente 1608, 1610
 - riepiloghi degli incidenti 1618
 - Network Discover/Cloud Storage Discover scansioni
 - autenticazione 1835
 - parallele 1873
 - rimozione dei target 1856
 - scansione della griglia 1874
 - Network Discover/Cloud Storage Discover target
 - rimozione 1856
 - Network Discover/Cloud Storage Discover, scansioni
 - controllo di target 1849
 - elenco di target 1854
 - esclusione di elementi o archivi 1840
 - filtraggio per data modifica 1844
 - filtraggio per data ultimo accesso 1844
 - inclusione di elementi o archivi 1840
 - inventario 1849
 - limitazione 1847
 - ottimizzazione 1847
 - scansioni differenziali 1872
 - Network Monitor
 - configurazione 1787
 - creazione di politiche per 1789
 - implementazione 1776, 1778
 - introduzione 76
 - registrazione 343
 - requisiti per 1776
 - test 1789–1790
 - utilizzo di schede Endace 1787
 - Network Prevent (Email)
 - restituzione di messaggi 1562
 - Network Prevent for Email
 - attivazione delle intestazioni sulle violazioni della politica 1802
 - blocco e-mail 1800
 - configurazione 1793
 - creazione di politiche per 1800
 - implementazione 1791, 1793
 - integrazione di MTA con 1793
 - introduzione 76
 - registrazione 344
 - routing di porte con restrizioni a 1798
 - test 1803
 - Network Prevent for Web
 - configurazione 1807
 - creazione di politiche per 1813
 - implementazione 1805, 1807
 - introduzione 76
 - risoluzione dei problemi 1815
 - test 1815
 - Network Protect
 - file in quarantena 1928
 - SharePoint 1956
 - ICE 1928
 - introduzione 77
 - Symantec Information Centric Encryption 1928
 - network tap 1776, 1779
 - NIC 1777, 1780
 - Nome host agente 2184
 - numeri di codice
 - eventi di sistema 187
- ## O
- Obiettivi di Microsoft Exchange 1976
 - offload di checkum 1778
 - ottimizzazione dei profili
 - modalità 648
 - soglia di similarità 648
- ## P
- PACKET_MMAP, software 1780
 - Pagina iniziale
 - selezione 81
 - panoramica agente
 - schermata riepilogo 2195
 - Panoramica sistema, schermata 273
 - stato dei server 275
 - parametri di ricerca
 - gruppi di parametri 1731

- parametro new_oracle_password 370
- parametro password_file 370
- password 369
 - Vd. anche* Utilità DBPasswordChanger
 - Amministratore 84
 - amministratore 128
 - crittografia per scansioni Network Discover/Cloud Storage Discover 1840
 - modifica 85, 88, 369
 - reimpostazione 128
- password Strumenti 2254
- pcapstart.reg, file 1781
- plug-in
 - distribuzione nell'endpoint 2251
- plug-in di ricerca. *Vedere* informazioni
 - attivazione 1742
 - concatenamento 1742
 - concatenamento di molteplici plug-in 1732
 - concatenamento per script 1769
 - configurazione dello script 1762
 - configurazione LDAP 1757
 - connessione dei server LDAP 1758
 - CSV, funzionamento 1729
 - CSV, set di caratteri 1750
 - delimitatore di file CSV 1750
 - distribuzione 1732
 - implementazione, flusso di lavoro 1733
 - LDAP, funzionamento 1729
 - LDAP, prova 1760
 - linguaggi di script 1729
 - mapping di attributi CSV 1750
 - mapping di attributi LDAP 1758
 - mapping di chiavi CSV 1750
 - output del proprietario di dati 1745
 - output e-mail proprietario dati 1745
 - parametri di ricerca 1737
 - personalizzati 1773
 - personalizzati (precedenti) 1730
 - posizione di file CSV 1750
 - requisiti del file di dati CSV 1748
 - ricarica automatica 1745
 - ricaricamento 1743
 - ricerca automatica 1745
 - script, funzionamento 1729
 - scrittura di script 1763
 - timeout 1745
 - tipi 1728
- plug-in di ricerca, script
 - attivazione credenziali 1767
 - crittografia credenziali 1767
- politica
 - clonazione 452
 - esportazione 451
 - informazioni 451
 - importazione 449
 - informazioni 449
 - referimenti 450
- politiche
 - aggiunta 421
 - aggiunta di regole di risposta 455
 - componenti 375
 - configurazione 422
 - creazione 444
 - distribuzione 378
 - eliminazione 456
 - gestione 444
 - Gruppi utente 382
 - informazioni 373
 - pacchetti di soluzioni 377
 - privilegi, amministrazione 380
 - privilegi, creazione 380
 - privilegi, regole di risposta 380
 - profili dati 381
- politiche violate 1802
- politiche, informazioni
 - implementazione 384
- porte con restrizioni 1797–1798
- posizione dell'endpoint
 - configurazione 2076
- prevenzione della perdita di dati. *Vedere* Symantec Data Loss Prevention
- Privilegi API di reporting 119
- Privilegio aggiornamento incidente 119
- Privilegio reporting incidente 119
- processGets, campo 1813
- Processo BoxMonitor 337
- processo di gestione 337
- proprietà
 - numero minimo di documenti per set di training 649
 - numero minimo di funzionalità da conservare 649
 - significato della soglia delle funzionalità 649
 - soglia di similarità predefinita 649
- protocollo di stato del certificato in linea. *Vedere* controlli di revoca OSCP
- provider di identità
 - autenticazione con 226
- Proxy TLS 248, 1798

punto di distribuzione dell'elenco certificati
revocati. *Vedere* controlli di revoca CRLDP

R

rapporti dashboard
 configurazione 1641
Record MX 249, 1795
registrare
 numero di funzionalità del modello 652
registrazione
 distanza e fiducia 652
 valutazione per ciclo 652
registrazione di errori per ICE Utilità 226
registrazione per ICE Utilità 226
registri
 verifica 187
regole di gruppo, tipo
 Destinatario corrispondente a criterio 840
regole di politica
 composte 440
regole di politica, condizioni
 configuri 427
regole di politica, configurazione
 conteggio delle corrispondenze 431
 gravità della regola 430
regole di politica, gruppo
 aggiunta 424
regole di politica, rilevamento
 aggiunta 424
regole di risposta 1584
 aggiunta 1489
 best practice 1487
 composizione di risposte tramite e-mail 1574
 configurazione 1491
 gestione 1489
 informazioni 1468
 modifica dell'ordinamento 1497
regole di risposta, aggiunta
 automatica 1490
 smart 1490
regole di risposta, azione
 Aggiungi autenticazione a due fattori 1539
 Imposta accesso collaboratore in Anteprima 1535
 Imposta accesso collaboratore in Lettura 1536
 Imposta accesso collaboratore in Modifica 1535
 Imposta accesso file in Lettura completa 1537
 Imposta accesso file in Lettura interna 1538
 Imposta accesso file in Modifica interna 1537
 Rimuovi accesso collaboratore 1534

regole di risposta, azioni
 Aggiungi nota 1510
 Archiviazione cloud: aggiungi tag visivo 1523
 Archiviazione cloud: quarantena 1523
 Azione personalizzata su dati a riposo 1529
 Azione personalizzata su dati in movimento 1540
 Blocca dati in movimento 1539
 Cancella dati in movimento 1543
 Classifica contenuto Enterprise Vault 1519
 configurazione 1493
 Crittografa dati a riposo 1531
 Crittografa dati in movimento 1541
 Elimina dati a riposo 1530
 eliminazione dei dati degli incidenti di rete 1512
 Endpoint Discover: metti file in quarantena 1545
 Endpoint Prevent Encrypt 1550
 Endpoint Prevent: blocca 1547
 Endpoint Prevent: notifica, configurazione 1554
 Endpoint Prevent: operazione annullata
 dall'utente, configurazioni 1557
 Endpoint: FlexResponse 1544
 Esegui DRM su dati a riposo 1531
 Esegui DRM su dati in movimento 1541
 Impedisci download, copia, stampa 1534
 Imposta attributo 1517
 Imposta stato 1518
 Interrompi collegamenti nei dati a riposo 1528
 Invia notifica e-mail 1514
 Limita conservazione dati incidenti 1510
 Marca dati a riposo 1533
 Metti in quarantena dati a riposo 1532
 Metti in quarantena dati in movimento 1542
 Network Prevent: blocca HTTP/HTTPS 1560
 Network Prevent: blocca messaggio SMTP 1562
 Network Prevent: blocca richiesta FTP 1560
 Network Prevent: modifica messaggio
 SMTP 1563
 Network Prevent: rimuovi contenuto
 HTTP/HTTPS 1564
 Network Protect: copia file 1565
 Network Protect: crittografa file,
 configurazione 1567
 Network Protect: metti file in quarantena,
 configurazione 1566
 Quarantena (risposta smart) 1525
 Quarantena SharePoint (risposta smart) 1525
 Registrazione a un server Syslog 1513
regole di risposta, condizioni
 configurazione 1492

- dispositivo endpoint 1500
- gravità 1506
- Monitoraggio protocollo o endpoint 1504
- Numero corrispondenza incidenti 1503
- posizione endpoint 1499
- tipo di incidente 1501
- regole di risposta, informazioni
 - automatica 1478
 - azioni 1468
 - condizioni 1480
 - esecuzione 1478
 - implementazione 1486
 - priorità di esecuzione per le azioni 1481
 - privilegi di creazione 1485
 - rimozione 1498
 - smart 1479
 - smart, configurazione 1492
- regole di risposta, operazioni
 - conservazione dati incidente degli endpoint 1511
- regole di risposta, tipi
 - Applicazioni cloud e dispositivo API 1474
 - archiviazione cloud 1473
 - connettore servizio cloud 1474
 - Dati a riposo (DAR) 1474
 - Dati in movimento (DIM) 1474
 - endpoint 1470
 - Network Protect 1472
 - rete 1471
 - tutti i server di rilevamento 1469
- regole di risposta, tipo
 - Endpoint Prevent: blocca 2074
 - Endpoint Prevent: notifica 2074
 - Endpoint Prevent: operazione annullata dall'utente 2075
 - quarantena di endpoint 2088
- Remote EDM Indexer, utilità
 - creazione di un profilo EDM 543
 - esecuzione 541, 543, 549
 - installazione 542
 - opzioni della riga di comando 552
 - requisiti di utilizzo 541
 - risoluzione dei problemi 554
- report 1591, 1632
 - dashboard 1637
 - elenco delle opzioni 1669
 - eventi di sistema 172
 - incidenti 1635
 - riepiloghi 1643
 - report degli incidenti
 - invio tramite e-mail 1672
 - report del dashboard
 - pianificazione 1654
 - report di dashboard
 - creazione 1639
 - report di incidente
 - impostazione preferenze 1634
 - modifica dei report personalizzati 1656
 - opzioni di riepilogo 1682
 - pianificazione 1650
 - stampa 1673
 - report di sistema
 - pianificazione 1652
 - report incidente 1632
 - applicazioni 1619
 - creazione di report riepilogativi 1644
 - dashboard, configurazione 1641
 - dashboard, creazione 1639
 - eliminazione di report personalizzati 1669
 - esportazione in CSV 1656
 - esportazione in XML 1656
 - filtraggio 1648
 - implementazione di una strategia 1633
 - impostazione di filtri avanzati 1687
 - impostazione di filtri generali 1679
 - introduzione 1635
 - navigazione nella pagina 1670
 - Network Discover 1610
 - opzioni di riepilogo 1671
 - opzioni filtro 1671
 - pianificazione 1652
 - visualizzazione di incidenti 1645
 - visualizzazione di report riepilogativi 1643
 - report incidenti
 - dashboard 1637, 1646
 - filtraggio 1677
 - personalizzazione 1646
 - riepiloghi 1637, 1643, 1677
 - riparazioni incidenti 1573
 - salvataggio 1649
 - report riepilogativi di DLP Agent 2203
 - report riepiloghi 1591
 - REQMOD 1810–1811
 - RequestProcessor, impostazioni 1802
 - RESPMOD 1810–1811
 - Richieste HTTP 252
 - blocco 1813

- richieste HTTP
 - ignorare 1807–1808
- riepiloghi degli incidenti
 - applicazioni 1628
 - Network Discover/Cloud Storage Discover 1618
- rilevamento
 - altri formati accessibili 900
 - applicazioni cloud
 - attributi contestuali 861
 - attributi contestuali 861
 - attributi di esposizione dei dati 868
 - attributi di trasferimento dei dati 871
 - attributi generali 863
 - attributi personalizzati 875
 - attributi utente 867
 - categorie 862
 - configurazione 861
 - best practice 819
 - Corrispondenza allegato messaggio o dimensioni file 813
 - Corrispondenza allegato messaggio o nome file 815
 - Corrispondenza allegato messaggio o tipo file 812
 - dimensione di file 810, 813
 - esempi di nome file 816
 - Firma tipi di file personalizzati 817
 - formati CAD accessibili 899
 - formati di elaborazione di testo 893
 - formati di file di database accessibili 900
 - formati di file di elaborazione di testi accessibili 894
 - formati di foglio di calcolo accessibili 897
 - formati di grafica accessibili 899
 - formati di incapsulamento accessibili 901
 - formati di presentazione accessibili 896
 - formati di testo e markup accessibili 898
 - formati e-mail 898
 - Monitoraggio protocollo, rete 822
 - nome file 811, 815
 - proprietà di file 808
 - rete 821–822
 - sintassi dei nomi di file 816
 - tipo di file 808, 812
 - tipo di file, personalizzato 810, 817
- Rilevamento applicazioni
 - configurazione 2273
 - gestione 2273
 - informazioni 2272
- rilevamento di politiche
 - applicazione endpoint 825
 - contenuto di file 388
 - endpoint 824
 - eventi endpoint 389
 - gravità delle regole 379
 - identità 389
 - lingue 389
 - lingue internazionali 802
 - proprietà di file 388
 - protocollo endpoint 824
 - punteggio di somiglianza 648
 - rete 388
 - tecnologie 390
 - tipi di formato di file identificabili 878
 - utilizzo di VML come eccezione 654
 - Vector Machine Learning (VML) 629
- rilevamento di politiche, condizioni
 - Classe o ID dispositivo endpoint 830
 - Contenuto corrispondente a espressione regolare 789
 - Contenuto corrispondente a parola chiave 779
 - Destinatario basato su gruppo di server di directory 852
 - Mittente/utente basato su gruppo di server di directory 851
 - Mittente/utente corrisponde a criterio 837
 - monitoraggio del protocollo o dell'endpoint 827
 - Posizione endpoint 829
- rilevamento di politiche, configurazione
 - selezione dei componenti del messaggio per la corrispondenza 433
- rilevamento di politiche, corrispondenza con parole chiave
 - esempi 775
 - implementazione 771
 - supporto per caratteri jolly 771
- rilevamento di politiche, corrispondenza con parole chiave, configurazione
 - Contenuto corrispondente a parola chiave 779
- rilevamento di politiche, endpoint
 - Classe o ID dispositivo endpoint 830
 - dispositivi, aggiunta 832
 - dispositivi, configurazione 832
 - dispositivi, informazioni 826
 - monitoraggio del protocollo o dell'endpoint 827
 - Posizione endpoint 829
 - posizioni, informazioni 826

- rilevamento di politiche, espressioni regolari
 - Contenuto corrispondente a espressione regolare 789
 - implementazione 787
 - motore comune 788
 - scrittura 788
- rilevamento di politiche, identità descritte
 - informazioni 835
 - Mittente/utente corrisponde a criterio 837
- rilevamento di politiche, informazioni
 - corrispondenza con parole chiave 771
- rilevamento di politiche, internazionale
 - identificatori di dati 804
 - Trova parole chiave 804
- rilevamento di politiche, prossimità di parole chiave
 - informazioni 773
- rilevamento politica, corrispondenza token EDM
 - implementazione 508
- rilevamento politica, informazioni
 - corrispondenza token EDM 508
- rilevamento politica, internazionale
 - identificatori dati 729
- rilevamento politiche
 - destinazione endpoint 825
- rilevatori
 - impostazioni avanzate 279, 328
 - impostazioni, avanzate 267
 - modifica 267
 - schermata Dettagli server/rilevatore 277
- rilevatori di cloud
 - aggiunta 270
- rilevazione politica
 - introduzione 387
- riparazione 1570
 - archiviazione cloud Box
 - aggiunta di un tag visivo 1904
 - quarantena 1904
 - comandi 1575
 - variabili risposta e-mail 1576
- riparazione degli incidenti 1570
 - comandi 1575
- riparazione incidente
 - variabili risposta e-mail 1576
- rischi dell'utente
 - dettagli dell'utente 1724
 - elenco utenti 1724
 - origini dati dell'utente 1714
 - aggiunta 1716

- rischi utente 1712
 - origini dati utente
 - aggiunta da Active Directory 1718
 - aggiunta da un file 1717
 - definizione di attributi personalizzati 1715
 - riepilogo rischi utente 1725
- rischio utente
 - Identificazione utente 1721
- risoluzione dei problemi
 - configurazione delle proprietà 649
 - debug dei file di registro 652
 - qualità del set di training 659
- RRC. Vedere Rules Results Caching
- Rules Results Caching 2072
- ruoli
 - aggiungi 129
 - aggiunta 114
 - configurazione 114
 - gestione 129
- ruoli, informazioni
 - configurazione 110
 - consigliati 111
 - controllo degli accessi basato sul ruolo 109
 - inclusi con pacchetto di soluzioni 112

S

- Scansione dell'archiviazione cloud Box 1899
- scansione dell'archiviazione cloud Box
 - configurazione 1900
- scansione incrementale 1868–1870
- scansioni
 - scansioni differenziali 1868
 - scansioni incremental 1868–1870
- scansioni Cloud Storage Discover
 - archiviazione cloud Box 1899
 - configurazione 1900
 - autorizzazione archiviazione cloud Box 1837
- scansioni di Network Discover/Cloud Storage Discover
 - eliminazione 1859
 - filtraggio per dimensione dell'oggetto 1843
 - ottimizzazione 1865
 - pianificazione 1833
 - report con informazioni dettagliate 1860
 - report sulla cronologia scansioni 1857
 - stato 1864
- scansioni Endpoint Discover
 - reporting dettagli di scansione 2106
- scansioni Network Discover/Cloud Storage Discover
 - gestione 1853

- monitoraggio 1853
- password crittografate 1840
- reporting 1853
- scheda di interfaccia di rete. *Vedere* NIC
- scheda note
 - istantanee incidente 1674
- Schede Endace 1780
- schede Endace
 - configurazione di Network Monitor per l'utilizzo 1787
 - driver 1780
 - installazione di driver 1781
- schede Napatech
 - configurazione di Network Monitor per l'utilizzo 1788
- Schermata Dettagli server/rilevatore 277
- schermata Panoramica
 - server di rilevazione, aggiunta 268
- schermata Panoramica sistema
 - elenco di errori e avvisi 277
- script oracle_create_user.sql 221
- Script SQL 221
- server (DLP). *Vedere* server di rilevamento ed Enforce Server
- Server di classificazione
 - configurazione 266
- server di classificazione
 - configurazione delle categorie di conservazione 1521
- server di directory (LDAP)
 - configurazione delle connessioni 162
 - connessione 161
- Server di Network Monitor
 - configurazione 246
- server di rilevamento
 - controlli 242
 - eliminazione 271
 - impostazioni avanzate 279
 - informazioni su 241
 - schermata Dettagli server/rilevatore 277
 - schermata Panoramica sistema 273
 - tipi di 74
- server di rilevazione
 - a un solo livello 268
 - aggiunta 268
 - configurazione 244
 - elenco di errori e avvisi 277
 - impostazioni, avanzate 267
 - registrazione 340
 - stato 275
- server Network Discover
 - configurazione di base 254
- Server Network Discover/Cloud Storage Discover
 - configurazione di scansioni parallele 1873
- server Network Discover/Cloud Storage Discover
 - configurazione 1824
- server Network Prevent for Email
 - configurazione 248
- server Network Prevent for Web
 - configurazione 251
- server Network Protect
 - configurazione di base 254
- server proxy 1805
 - configurazione 1810–1812
- server Symantec Data Loss Prevention . *Vedere* server di rilevamento ed Enforce Server
- server syslog 182
- Service_Shutdown.exe, strumento 2261
- Servizi di Symantec DLP
 - arresto 107
- servizi di Symantec DLP
 - arresto 106–107
- Servizi Symantec DLP
 - arresto 102–107
 - avvio 105
- servizi Symantec DLP
 - arresto 104
 - avvio 102–107
- Servizi Web 119
- servizio Web di aggiornamento e reporting di incidenti 338
- set di training
 - negativo 656
 - positivo 656
- sistemi Linux 1798
- SMTP 1800
- software di acquisizione dei pacchetti
 - installazione 1780
- software di acquisizione pacchetti 1777, 1779
- Software WinPcap 1779
- SPAN 1776, 1779
- SQL 369
- SQL Preindexer, utilità
 - opzioni della riga di comando 550
 - risoluzione dei problemi 553
- stampa/fax 2065
- strumenti endpoint 2259
 - strumento logdump.exe 2265

- strumento Service_Shutdown.exe 2261
- strumento vontu_sqlite3.exe 2263
- utilizzo con Windows Vista 2261
- Strumento Attribute Query Resolver 2186–2187
- strumento vontu_sqlite3.exe 2263
- suite di prodotti. *Vedere* Symantec Data Loss Prevention
- supporti lingue
 - informazioni 93
 - utilità supporto lingue 96
- Switch Port Analyzer. *Vedere* SPAN
- Symantec CloudSOC 225
- Symantec Data Loss Prevention
 - amministratore di 80
 - configurazione iniziale del sistema 83
 - suite di prodotti 73
- Symantec DLP Agent
 - Agent Store 2129
 - amministrazione 2194
 - rimozione 2222
 - rimozione manuale 2225
 - rimozione mediante il software di gestione del sistema (SMS) 2222, 2225
 - rimozione su Windows Vista 2224

T

- target Cloud Storage Discover
 - archiviazione cloud Box 1899
- Target di Documentum 2009
- target di endpoint
 - configurazione 2091
- target di Network Discover
 - condivisioni file 1906
 - servizi Web 2026
 - SharePoint 1946
 - siti Web 1998
 - Web Server 1998
- target di SharePoint 1946
- Target Livelink 2018
- Target Lotus Notes 1931
- Target Network Discover 1986
 - database DB2 1938
 - database Oracle 1938
 - database SQL 1938
 - File system del server remoto Windows 1986
 - File system UNIX 1986
 - Livelink 2018
 - SQL Server 2005 1938
 - SQL Server 2014 1938

- target Network Discover
 - Documentum 2009
 - Exchange 1976
 - Lotus Notes 1931
 - personalizzati 2026
 - Server Domino 1931
- test delle politiche
 - allegato 648
 - insieme di test 648
- ticket Endpoint
 - istantanea 1597
- Tipi di MIME 252
- tipi di MIME 1809
- Tipo host agente 2185
- Tomcat
 - aggiunta di certificati 149
 - modifica password dell'archivio Attendibilità 151
- training
 - cross-fold 659
 - processo di valutazione del k-fold 659

U

- Utente connesso 2185
- utenti
 - aggiunta 129
 - gestione 129
- utenti gestiti 226
- utenti non gestiti 226
- utenti, account
 - aggiunta 123
 - configurazione 123
- utenti, autenticazione
 - Active Directory 141
 - integrazione di Enforce con Active Directory 142
 - verifica della connessione di Active Directory 144
- utenti, gestiti e non gestiti 226
- utenti, informazioni
 - configurazione 110
- utenti, password
 - configurazione di efficaci o rotazione 127
- utilità
 - introduzione 367–368
- Utilità DBPasswordChanger
 - esecuzione 369
 - esempio di utilizzo 370
 - individuazione 369
 - introduzione 368–369
 - prerequisiti per l'utilizzo 369
- utilità endpoint 368

Utilità ICE 226
 Utilità Indicizzatore EDM remoto
 introduzione 368
 Utilità logdump.exe 369
 Utilità Service_Shutdown.exe 368
 Utilità SQL Preindexer
 introduzione 368
 utilità sslkeytool
 introduzione 368
 utilità supporto lingue 96
 Utilità vontu_sqlite3.exe 369
 Utilità, ICE
 errori per 226
 UtilitàICE
 registrazione di errori per 226

V

valori dell'attributo 2186
 valori di nome comune (CN) 152
 valori di stato
 aggiunta 1702
 configurazione 1702
 eliminazione 1702
 Vector Machine Learning (VML)
 accettazione del training 631
 caricamento dei contenuti per il training 636
 configurazione delle eccezioni VML 646
 configurazione delle regole VML 645
 creazione di nuovi profili VML 635
 gestione di profili VML 642
 gestione set di training 641
 informazioni 629
 modifica dei nomi dei profili, descrizione 644
 processo di implementazione 633
 punteggio di somiglianza 632
 regolazione dell'allocazione di memoria 640
 regolazione della soglia di similarità 647
 rifiuto del training 631
 scheda Area di lavoro temporanea 635
 scheda Profilo corrente 635
 soglia di similarità 632
 training del contenuto 630
 training del profilo 638
 Verifiche di revoca
 configurazione 155
 Versione host agente 2185
 VIP Access 226
 visualizzazione
 incidenti nascosti 1697

W

WinPcap, software 1780
 installazione 1781

X

X-Filter-Loop: Intestazione riflessa 1798