Note di rilascio di Symantec™ Endpoint Protection 14.3 RU1

Aggiornamento: dicembre 2020

Table of Contents

Dichiarazione sul copyright

Novità di Symantec Endpoint Protection 14.3 RU1

In questa sezione vengono descritte le nuove funzionalità della release corrente.

Funzionalità di protezione

- Include i nuovi agenti Symantec per Mac e per Linux, i quali possono essere installati e gestiti sia da Symantec Endpoint Protection Manager on-premise che dalla console cloud integrata di Cyber Defense Manager.
  Installazione del client Symantec Endpoint Protection per Mac
  Installazione dell'agente Symantec per Linux 14.3 RU1
- Blocca le minacce nuove e sconosciute su macOS monitorando quasi 1.400 comportamenti di file in tempo reale. Il nuovo agente Mac include le funzionalità di protezione basata sui comportamenti. La protezione basata sui comportamenti, detta anche SONAR, utilizza l'intelligenza artificiale e il Machine Learning avanzato per la protezione contro gli attacchi Zero Day con il fine di bloccare in modo efficace le nuove minacce.
  Gestione SONAR
- Blocca file eseguibili non attendibili non portatili (PE), come ad esempio i file PDF e gli script non sono ancora identificati come una minaccia. Nella politica Eccezioni, fare clic su **Eccezioni Windows** > **Accesso file**.
- Impedisce le minacce Web basate sul punteggio di reputazione di una pagina Web. La politica Prevenzione delle intrusioni include il filtraggio della reputazione URL, il quale blocca le pagine Web con punteggi di reputazione inferiori alla soglia specificata. I punteggi di reputazione variano da -10 (non valido) a +10 (buono). L'opzione **Abilita reputazione URL** è abilitata per impostazione predefinita.
- È possibile imporre a Symantec Endpoint Protection di apprendere un'applicazione in base al valore hash dell'applicazione. Nella politica Eccezioni, fare clic su **Eccezioni Windows** > **Applicazione** > **Aggiungi un'applicazione per impronta digitale**.
- Protegge gli endpoint e gli utenti da attacchi basati sul Web su siti dannosi utilizzando la funzionalità di reindirizzamento del traffico di rete. Il reindirizzamento del traffico di rete reindirizza tutto il traffico di rete (qualsiasi porta) o solo il traffico basato sul Web (porte 80 e 443) al servizio Symantec Web Security, il quale consente o blocca il traffico di rete e l'accesso alle applicazioni SaaS in base alla politica aziendale. La politica Reindirizzamento del traffico di rete dispone di un nuovo metodo di reindirizzamento denominato metodo di tunneling. Il metodo di tunneling reindirizza automaticamente tutto il traffico Internet verso Symantec WSS, in cui il traffico è consentito o bloccato in base alle politiche di Symantec Web Security Service. Il metodo di tunneling è considerato una funzionalità beta. Si consiglia di eseguire test approfonditi con le applicazioni in base alle politiche WSS. Broadcom dispone di un sito Web beta in grado di offrire una guida di verifica e la possibilità di lasciare feedback sulla propria esperienza. Accedere al seguente sito Web utilizzando le credenziali Broadcom: Validate.broadcom.com.
  Configurazione del reindirizzamento del traffico di rete
- La politica Integrazioni è stata rinominata nella politica Reindirizzamento del traffico di rete.
- Fornisce il supporto per gli eventi con integrazione MITRE in Symantec EDR. Utilizza il framework MITRE ATT&CK per fornire il contesto di ciò che accade nel proprio ambiente.
- Fornisce il supporto per gli eventi Symantec EDR seguenti, i quali mostrano una maggiore visibilità sugli endpoint:
  - Gli eventi AMSI offrono visibilità sui metodi degli attori delle minacce, i quali possono eludere i tradizionali metodi di interrogazione della riga di comando.
  - Gli eventi ETW forniscono visibilità sugli eventi che si verificano negli endpoint Windows gestiti.
- Include la possibilità di eseguire sia Windows Defender che Symantec Endpoint Protection sullo stesso computer. La scansione Auto-Protect viene eseguita in seguito a Windows Defender ed è in grado di rilevare eventuali minacce non rilevate da Windows Defender. L'opzione **Coesistenza con Windows Defender** garantisce che Auto-Protect venga eseguito in caso di disattivazione di Microsoft Defender. Per disattivare l'opzione, fare clic su Politica di protezione antivirus e antispyware > **Varie** > scheda **Varie**.
- L'attenuazione della catena di attacchi è ora supportata per i client a gestione ibrida.

Symantec Endpoint Protection Manager

- Il database integrato è stato aggiornato al database Microsoft SQL Express. Il database SQL Server Express archivia le politiche e gli eventi di protezione in modo più efficiente rispetto al database integrato predefinito e viene installato automaticamente con Symantec Endpoint Protection Manager.
  Procedure consigliate per l'aggiornamento dal database integrato al database Microsoft SQL Server Express
- Durante l'installazione o l'aggiornamento di Symantec Endpoint Protection Manager, la procedura guidata di configurazione del server di gestione:
  - Installa automaticamente il contenuto LiveUpdate.
  - Fornisce un'opzione per l'utilizzo del certificato TLS per la comunicazione protetta tra SQL Server e Symantec Endpoint Protection Manager.
- LiveUpdate utilizza un nuovo motore in Symantec Endpoint Protection Manager ottimizzato per l'esecuzione sulla console cloud.
  Note di rilascio di LiveUpdate Administrator e nuove correzioni
- L'opzione **Disinstalla automaticamente il software per la sicurezza di terze parti esistente**, non disponibile in 14.3 MP1 è disponibile nuovamente in 14.3 RU1 con una versione aggiornata. Questa opzione viene utilizzata per disinstallare il software per la sicurezza di terze parti. Per accedere a questa opzione, fare clic su pagina **Amministrazione** > **Pacchetti** > **Impostazioni di installazione del client**.
  Rimozione del software di protezione di terze parti in Endpoint Protection 14
  Rimozione del software di protezione di terze parti in Endpoint Protection 14.3 RU1
- La procedura guidata di distribuzione del client utilizzata per la distribuzione dei pacchetti client deve avere le credenziali verificate e deve essere in grado di connettersi a Symantec Endpoint Protection Manager. Se il processo di verifica non riesce, il processo di distribuzione del client si interrompe per mantenere bloccati gli account utente di Active Directory.
  Installazione dei client Symantec Endpoint Protection con Push remoto
- I registri e i report di Stato del computer consentono ora di selezionare un intervallo per i campi **Versione client** e **Versione IPS**. Il filtro **Versione del prodotto** è stato rinominato in **Versione client**.
- L'opzione **Disabilita l'icona della barra delle notifiche** è disponibile per i client in esecuzione su un server terminal e che causano un utilizzo elevato della CPU e della memoria. È possibile disabilitare l'icona dell'area di notifica, nota anche come icona della barra di sistema, per impedire l'esecuzione di più istanze di processi della sessione utente (come SmcGui.exe e ccSvcHost.exe). Attivare questa opzione nella scheda **Client** > **Politiche** > **Impostazioni di sicurezza** > scheda **Generale**.
- Le modalità Whitelist e Blacklist sono state aggiornate per riflettere le funzionalità Elementi consentiti ed Elementi non consentiti. Nella pagina **Client** > scheda **Politiche** > finestra di dialogo **Blocco del sistema**, il file dell'applicazione è stato modificato da **Modalità whitelist** e **Modalità blacklist** a **Modalità Elementi consentiti** e **Modalità Elementi non consentiti**.
- Nella pagina **Amministrazione** > scheda **Server** > **Configura registrazione esterna** > scheda **Generale**, l'opzione **Server di registrazione master** è stata modificata in **Server di registrazione principale**.
- Il tipo di registro **Sistema** > registro **Amministrativo** e registro di **Controllo** elenca il nome del computer.
- I registri del firewall client vengono raccolti in modo da ridurre il numero di notifiche sulla console cloud.
- Oracle Java SE è stato sostituito con OpenJDK.
- Aggiornamento dei componenti di terze parti JQuery a una versione più recente.

Aggiornamenti di client e piattaforme

- Il client Windows supporta Windows 10 20H2 (Windows 10 versione 2009).
- Il client Mac supporta macOS 10.15.7.
- Spostamento dei pacchetti di installazione del client Mac di legacy nella cartella Pacchetti aggiuntivi.

Funzionalità rimosse

- Le opzioni **Gravità rischio** e **Distribuzione rischio per gravità** sono state rimosse dalle notifiche e dai report.
- La scheda **CASMA** e il comando **Analizza** sono stati rimossi, in quanto questa funzionalità è considera obsoleta a partire dalla versione 14.3.
- Il client Mac non supporta più macOS 10.13.

Documentazione

La guida di Symantec Endpoint Protection Manager è ora in linea e contenuta in: Guida all'installazione e all'amministrazione di Symantec Endpoint Protection.

Schema del database

Lo schema del database presenta le seguenti modifiche.

Tabella	Modifica colonna
ALERTS	Aggiunta della colonna ENRICHED_DATA.
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA COMMAND COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG REPORTS SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2 SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG V_ENFORCER_SYSTEM_LOG V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER	Le seguenti colonne sono state rimosse da ciascuna tabella: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Tabella	Modifica colonna
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	• Tipo della colonna CONTENT modificata da 'image' a 'varbinary' • Aggiunta di una colonna indicizzata FILESTREAM_ID • Aggiunta di un indice FILESTREAM_ID • Le seguenti colonne sono state rimosse: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
INVENTORYREPORT	Le seguenti colonne sono state aggiunte: • PRODUCTVERSIONFROM • PRODUCTVERSIONTO • IDS_VERSIONFROM • IDS_VERSIONTO
SEM_AGENT	• Aggiunta della colonna NTR_MESSAGE. • Le seguenti colonne sono state rimosse: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
SEM_AGENT_VERSION	Le seguenti colonne sono state aggiunte: • VERSION • FORMATTED_VERSION • REFRESH_USN • AGENT_VERSION_FORMAT_REFRESH • VERSION1 • VERSION2 • VERSION3 • VERSION4
SEM_SVA	Le seguenti colonne sono state rimosse: • RESERVED_INT1 • RESERVED_INT2 • RESERVED_BIGINT1 • RESERVED_BIGINT2 • RESERVED_CHAR1 • RESERVED_CHAR2 • RESERVED_VARCHAR1
V_ALERTS	Aggiunta della colonna ENRICHED_DATA.

Novità di tutte le release di Symantec Endpoint Protection

Problemi noti e soluzioni alternative per Symantec Endpoint Protection

I problemi riportati in questa sezione si applicano a questa distribuzione di Symantec Endpoint Protection.

Table 1: Problemi di aggiornamento

Problema	Descrizione e soluzione
Symantec Endpoint Protection Manager in una dark network scarica il contenuto del motore del sistema di rilevazione delle intrusioni del client (CIDS) precedente sui nuovi client in quanto LiveUpdate non viene eseguito durante l'aggiornamento [14.3 RU1]	Quando Symantec Endpoint Protection Manager 14.3 RU1 non è in grado di accedere a Internet o a un server di amministrazione LiveUpdate (LUA), mantiene il contenuto obsoleto e incompatibile nella propria cache. Il contenuto obsoleto viene normalmente consegnato ai nuovi client. Per aggiornare il contenuto nella cache del server di gestione, scaricare manualmente le definizioni dei virus certificati e i file .jdb di CIDS. [SEP-69125] Per assicurarsi che i nuovi client non ricevano contenuto obsoleto, installare manualmente un file .jdb di CIDS su SEPM prima di installare i nuovi client o aggiornare i client obsoleti. Download dei file .jdb per aggiornare le definizioni per Endpoint Protection Manager
Impossibile accedere a Symantec Endpoint Protection Manager (SEPM) quando la scheda di interfaccia di rete è disattivata [14.3 RU1]	Se, dopo aver installato Symantec Endpoint Protection Manager, non è possibile accedere alla console di e viene visualizzato il seguente messaggio di errore: `Errore server imprevisto` Questo problema può verificarsi se la scheda di interfaccia di rete del computer è stata disattivata durante l'installazione di SEPM, il quale impedisce la generazione del certificato del server. [SEP-67040] Per verificare se SEPM è stato installato con una scheda di interfaccia di rete disattivata, verificare il certificato del server. Consultare la sezione Errore di installazione da parte di SEPM se non sono disponibili connessioni di rete
Quando si disinstalla SEPM, si utilizza l'opzione per rimuovere il database predefinito e si lascia l'istanza SQL Server Express, viene visualizzato il seguente messaggio di errore: "`Si è verificato un errore durante il tentativo di connessione al server del database`".	Se si disinstalla Symantec Endpoint Protection Manager e si seleziona **Rimuovere soltanto il database e lasciare l'istanza SQL Server Express installata con SEPM**, potrebbe essere visualizzato il seguente messaggio di errore: "`Si è verificato un errore durante il tentativo di connessione al server del database`". Questo problema si verifica dopo l'aggiunta delle credenziali per il DBA dell'utente predefinito e può essere correlato ai privilegi dell'utente. [SEP-68670] Per risolvere questo problema, effettuare la disinstallazione eseguendo il file setup.exe di SEPM e facendo clic sul pulsante **Rimuovere soltanto il database e lasciare l'istanza SQL Server Express installata con SEPM** durante l'installazione.
L'aggiornamento di SQL Server dalla versione 2017 alla versione 2019 non riesce con la modalità FIPS abilitata [14.3]	È possibile che venga visualizzato il messaggio di errore: "The following error has occurred. An error occurred while installing extensibility feature with error message: AppContainer Creation Failed with error message NONE, state. This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms." Ciò si verifica se si dispone di Symantec Endpoint Protection Manager 14.3 abilitato per FIPS e si esegue l'aggiornamento da Microsoft SQL Server 2017 a 2019. [SEP-61473] Per risolvere questo problema, disabilitare FIPS a livello di sistema operativo: 1. In `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools`, fare clic su **Criteri di sicurezza locali** > **Criteri locali** > **Opzioni di sicurezza**, quindi disattivare l'opzione **Crittografia di sistema: utilizza algoritmi FIPS compatibili per crittografia, hash e firma** 2. Eseguire l'aggiornamento da SQL Server versione 2017 alla versione 2019. 3. Dopo l'aggiornamento di SQL Server, riabilitare FIPS. Aggiornamento di SQL Server dalla versione 2017 alla versione 2019 non riuscito con la modalità FIPS abilitata

Problema	Descrizione e soluzione
I nomi personalizzati possono impedire l'aggiornamento della politica firewall durante l'upgrade alla versione 14.2 o successiva	Per l'aggiornamento a Symantec Endpoint Protection 14.2 (o versioni successive), le politiche firewall non possono incorporare le modifiche per IPv6 se alcuni nomi predefiniti sono stati modificati. I nomi predefiniti includono i nomi delle politiche predefinite e dei nomi delle regole predefinite. Se le regole non possono essere aggiornate durante l'upgrade, le opzioni IPv6 non vengono visualizzate. Le nuove politiche o regole create dopo l'aggiornamento non sono interessate. Se possibile, ripristinare il valore predefinito dei nomi modificati. In caso contrario, assicurarsi che le regole personalizzate aggiunte a una politica predefinita non blocchino la comunicazione IPv6 in alcun modo. Fare lo stesso per le nuove politiche o regole che vengono aggiunte.

Table 2: Problemi relativi a Symantec Endpoint Protection Manager

Problema	Descrizione e soluzione
Alcuni eventi EDR non vengono visualizzati nel client [14.3 RU1]	Il client Symantec Endpoint Protection deve eseguire Windows 10 build 14393 (o versioni successive) per la raccolta degli eventi di analisi Symantec EDR per Windows (ETW). [SEP-67175]
La funzionalità di reindirizzamento del traffico di rete presenta alcune limitazioni [14.3 RU1]	• Il servizio di protezione Web di Symantec viene fornito su IPv4 e non su IPv6. [SEP-68700] • Il metodo di reindirizzamento di tunneling: – Viene eseguito solo su Windows 10 x64 versione 1703 e versioni successive (per i canali di manutenzione semestrali). Questo metodo non supporta nessun altro sistema operativo Windows o client Mac. [SEP-67927] – Non supporta periferiche Windows 10 a 64 bit abilitate per HVCI. [SEP-67648] – Reindirizza il traffico in uscita dal client Symantec Endpoint Protection a WSS prima che venga valutato dal firewall del client o dalle regole di reputazione dell'URL. Il traffico viene invece valutato rispetto al firewall WSS e alle regole URL. Ad esempio, se una regola del firewall del client SEP blocca google.com e una regola WSS consente google.com, il client consente agli utenti di accedere a google.com. Il traffico locale in arrivo verso il client viene ancora elaborato dal firewall Symantec Endpoint Protection. [SEP-67488] – Il captive portal di WSS non è disponibile per il metodo di tunneling e il client ignora le credenziali di richiesta. In una release futura, l'autenticazione SAML nell'agente WSS sostituirà il captive portal e sarà disponibile per il client Symantec Endpoint Protection. – Se un computer client si connette a WSS utilizzando il metodo di tunneling e ospita computer virtuali, ciascun utente ospite dovrà installare il certificato SSL disponibile nel portale WSS. – Il traffico della rete locale come la home directory o l'autenticazione di Active Directory non viene reindirizzato. Il metodo di tunneling è attualmente considerato una funzionalità beta.
Voci di registrazione dell'agente duplicate dopo l'aggiornamento da 14.2.x a 14.3 MP1 e versioni successive [14.3 RU1]	L'aggiornamento dei client Symantec Endpoint Protection da 14.2.x a 14.3 MP1 (e versioni successive) crea voci di registrazione dell'agente duplicate per questi client nella pagina **Periferiche** di Symantec Endpoint Protection Manager. Non vi è alcun impatto funzionale ed è possibile continuare a utilizzare le nuove voci per i client 14.3 RU1. Symantec Endpoint Protection Manager rimuoverà le voci precedenti dell'agente.

Problema	Descrizione e soluzione
Autorizzazione degli URL in Symantec Endpoint Security se si utilizza l'opzione di gestione ibrida, i server proxy o un firewall perimetrale [14.3]	Con l'acquisizione di Broadcom di Symantec Enterprise Security, gli URL per la comunicazione da client a cloud sono stati modificati nella versione 14.2.2.1. [CDM-42467] È necessario aggiornare i client alla versione build 14.2.5569.2100 (o versioni successive) nei seguenti casi: • Si utilizza Symantec Endpoint Security per gestire i client e le politiche quando i domini on-premise di Symantec Endpoint Protection Manager sono registrati nella console cloud. • Si utilizzano i server proxy. È possibile autorizzare gli URL in agenti completamente gestiti da cloud o a gestione ibrida, quindi autorizzare il server proxy e/o il firewall del perimetro. Consultare la sezione URL che consentono a SEP e a SES di connettersi ai server Symantec Consultare la sezione Aggiornamento degli agenti Symantec gestiti da cloud alla versione 14.2 UR2 MP1 (o versione successiva).
La console remota di Symantec Endpoint Protection Manager non supporta più la piattaforma Windows a 32 bit [14.3]	A partire dalla versione 14.3 non è più possibile accedere alla console remota di Symantec Endpoint Protection Manager se si esegue una versione di Windows a 32 bit. Oracle Java SE Runtime Environment non supporta più le versioni a 32 bit di Microsoft Windows. [SEP-61106] Se viene visualizzato il seguente messaggio, accedere a Symantec Endpoint Protection Manager in locale: "La versione di C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe non è compatabile con la versione di Windows in esecuzione. Verificare le informazioni sul sistema del computer e contattare l'autore del software."
Viene visualizzato il messaggio di errore "Impossibile installare Microsoft Visual C++ Runtime" durante l'installazione di Symantec Endpoint Protection Manager [14.3]	È possibile che venga visualizzato il seguente messaggio di errore durante l'installazione di Symantec Endpoint Protection Manager su Windows 2012 R2: "Impossibile installare Microsoft Visual C++ Runtime" [SEP-60396] Per risolvere questo problema, attivare Windows e installare gli aggiornamenti corrispondenti. L'aggiornamento di Windows installa Visual C++ 2017 Redistributable, il quale costituisce un prerequisito per l'installazione di Symantec Endpoint Protection Manager 14.3 su Windows 2012 R2.
Aggiornamento per l'attivazione di TLS 1.1 e TLS 1.2 come protocolli di protezione predefiniti di WinHTTP in Windows [14.3]	Dopo aver eseguito l'aggiornamento o l'installazione di Symantec Endpoint Protection Manager versione 14.3 registrata nella console cloud, il server di gestione non caricherà più i registri nel cloud correttamente. È possibile che venga visualizzato il seguente messaggio di errore nel file uploader.log: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Questo problema è causato da un aggiornamento di Microsoft mancante che fornisce il supporto per TLS 1.1 e 1.2. Per risolvere il problema, installare l'aggiornamento di Microsoft: KB3140245. Per ulteriori informazioni, consultare la sezione: Aggiornamento per l'attivazione di TLS 1.1 e TLS 1.2 come protocolli protetti predefiniti di WinHTTP in Windows
Il messaggio "Distribuzione in corso" viene ancora visualizzato in Symantec Endpoint Protection Manager dopo che il client ha ricevuto una politica aggiornata per Endpoint Threat Defense per AD [14.2 RU1 MP1 e versioni successive]	Si tratta di un comportamento previsto. Endpoint Threat Defense per le politiche AD 3.3 è supportato solo sul client a partire dalla versione 14.2 RU1 MP1. È possibile applicare una politica per Symantec Endpoint Threat Defense per Active Directory 3.3 a un gruppo. Questo gruppo contiene alcuni client che eseguono Symantec Endpoint Protection 14.2 RU1 (o versioni precedenti). Questi client ricevono e applicano la politica come previsto, tuttavia lo stato in Symantec Endpoint Protection Manager continua a visualizzare il messaggio Distribuzione in corso.

Table 3: Problemi del client Windows, Mac e Linux

Problema	Descrizione e soluzione
Messaggi errati nel registro del programma di installazione dell'agente Symantec per Linux. [14.3 RU1]	In alcuni casi, il programma di installazione dell'agente registra messaggi errati relativi a una versione del driver non corrispondente o al riavvio richiesto. Questi messaggi non influiscono sulla funzionalità dell'agente.
In una periferica SuSe Linux, zypper rimuove i pacchetti client Linux di SEP durante la rimozione del pacchetto 'at'. [14.3 RU1]	Su una periferica SuSe Linux, il comando 'zypper remove at' rimuove i pacchetti client Linux di SEP in quanto il pacchetto 'at' viene aggiunto come pacchetto dipendente obbligatorio e i comandi zypper tentano automaticamente di rimuovere i pacchetti client di SEP 'sdcss-kmod' e 'sdcss-sepagent' come pacchetti con dipendenze inutilizzate. **Soluzione alternativa**: per rimuovere il pacchetto 'at', eseguire il seguente comando: rpm -e --nodeps at
Problema di aggiornamento su macOS 10.15 e versioni successive [14.3 MP1]	In macOS 10.15 e versioni successive, la funzionalità **Installa Symantec Endpoint Protection su computer remoti** nella procedura guidata di distribuzione client non riesce ad aggiornare il client Symantec Endpoint Protection dalle versioni precedenti alla versione 14.3 MP1. **Soluzione alternativa**: utilizzare **Auto Upgrade di Symantec Endpoint Protection Manager** per eseguire l'aggiornamento del client Symantec Endpoint Protection su macOS 10.15 e versioni successive.
L'installazione del client Windows di Symantec Endpoint Protection 14.3 potrebbe non essere eseguita correttamente a meno che non si installi il supporto SHA-2 [14.3].	Se si eseguono versioni del sistema operativo di legacy (Windows 7 RTM o SP1, Windows Server 2008 R2, R2 SP1 o R2 SP2), è necessario che il supporto per la firma del codice SHA-2 sia installato sui dispositivi per l'installazione degli aggiornamenti di Windows rilasciati il o dopo il mese di luglio 2019. Senza il supporto SHA-2, a volte l'installazione del client Windows non riesce. L'installazione potrebbe non riuscire se si installano i client per la prima volta o si esegue l'aggiornamento automatico da una versione precedente. [SEP-61175/61403] Per ottenere il supporto per la firma del codice SHA-2 di Microsoft, consultare la sezione: Requisiti di supporto per la firma del codice SHA-2 per Windows e WSUS Il client Windows di Symantec Endpoint Protection 14.3 potrebbe non essere in grado di eseguire l'installazione, a meno che il supporto SHA-2 non sia installato
Il client Windows di Symantec Endpoint Protection non viene eseguito quando è installato su Windows 10 1803 abilitato per UWF [14.3]	Se il client di Symantec Endpoint Protection viene eseguito sul sistema operativo Windows 10 RS4 1803 a 32 bit e il filtro di scrittura unificato (UWF) è abilitato e protegge l'unità su cui è installato il client Windows, il client non viene eseguito correttamente. Questo sistema operativo Windows contiene un difetto UWF che impedisce l'esecuzione del client Windows. Per risolvere questo problema: • Eseguire l'aggiornamento a un'altra versione del sistema operativo che non contenga il difetto. • Disabilitare UWF. Consultare la sezione: Endpoint Protection non funzionante in caso di installazione su Windows 10 1803 con UWF abilitato
I client Mac che attivano WSS Traffic Redirection non rispettano le impostazioni proxy personalizzate per LiveUpdate [14.2 RU1 MP1 e versioni successive]	I client Mac gestiti per Symantec Endpoint Protection 14.2 RU1 MP1 sono stati configurati per l'utilizzo delle impostazioni proxy personalizzate per LiveUpdate tramite le impostazioni di comunicazione esterna. Dopo aver attivato WSS Traffic Redirection (WTR) per i client Mac tramite la politica di Symantec Endpoint Protection Manager, viene rilevato che il traffico di LiveUpdate non rispetta più le impostazioni proxy personalizzate. Invece, LiveUpdate cerca di effettuare una connessione diretta. Per risolvere questo problema, utilizzare le impostazioni proxy personalizzate per LiveUpdate solo quando WSS Traffic Redirection è disattivato.
Microsoft Edge consente inaspettatamente i download di PDF con Protezione avanzata attivata [14.2 RU1 MP1 e versioni successive]	Con la Protezione avanzata attivata nel client di Symantec Endpoint Protection è inaspettatamente possibile scaricare file PDF se si utilizza il browser Microsoft Edge. La prevenzione del download di file PDF funziona come previsto con altri browser. La correzione di questo problema è pianificata in una release futura.

In seguito al recente annuncio da parte di Broadcom che Symantec Enterprise Protection è stato ufficialmente unito a Broadcom, Symantec ha eseguito la migrazione della documentazione al Portale della documentazione tecnica di Symantec Security di Broadcom.

Per trovare la documentazione di Endpoint Protection, fare clic sulla scheda **Software Symantec Security**, quindi selezionare **Endpoint Security and Management** > **Endpoint Protection**.

Table 4: Problemi relativi alla documentazione

Problema	Descrizione e soluzione
Gli articoli di HOWTO sono scaduti.	Gli articoli di HOWTO, i quali sono duplicati dagli argomenti della Guida di Symantec Endpoint Protection Manager, sono stati ripubblicati sul sito di Endpoint Protection e ora sono associati a un URL diverso. Per trovare un articolo, utilizzare il **campo di ricerca**.
File PDF	Symantec ha pubblicato tutti i file PDF negli articoli DOC corrispondenti. Queste pagine sono scadute. Per individuare la versione più recente di rilascio del file PDF, accedere alla pagina Documenti correlati. In futuro, Broadcom aggiungerà i file PDF di legacy e i file PDF tradotti.

Per i problemi risolti, consultare:

Nuove correzioni e componenti per Symantec Endpoint Protection 14.3 RU1

Nuove correzioni e componenti per Symantec Endpoint Protection 14.3 MP1

Nuove correzioni e componenti per Symantec Endpoint Protection 14.3

Requisiti di sistema per Symantec Endpoint Protection (SEP)

Generalmente i requisiti di sistema per i seguenti elementi sono gli stessi di quelli dei sistemi operativi su cui sono supportati.

NOTE
Una versione precedente di Symantec Endpoint Protection Manager potrebbe non essere in grado di gestire correttamente un client con una versione successiva. Potrebbero verificarsi problemi relativi agli aggiornamenti del contenuto e alla gestione del client. Ad esempio, Symantec Endpoint Protection Manager 14.0.1 (o una versione precedente) non è in grado di fornire correttamente un client della versione 14.2 con i relativi nomi specifici della versione. Symantec Endpoint Protection Manager per le versioni precedenti alla 14 MP2 non è in grado di fornire correttamente le versioni client successive alla 14.0.1 con i relativi nomi specifici della versione.

Le tabelle seguenti descrivono i requisiti hardware e software per Symantec Endpoint Protection.

Table 5: Requisiti di sistema del software Symantec Endpoint Protection Manager (SEPM)

Componente	Requisiti
Sistema operativo	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** I sistemi operativi desktop non sono supportati. **Note:** L'edizione Windows Server Core non è supportata per la versione 14.2x e quelle precedenti.
Browser Web	I seguenti browser supportano l'accesso a Symantec Endpoint Protection Manager dalla console Web e la visualizzazione della Guida di Symantec Endpoint Protection Manager: • Browser basato su Microsoft Edge Chromium (14.3 e versioni successive) • Microsoft Edge Nota: la versione a 32 bit di Windows 10 non supporta l'accesso della console Web sul browser Edge. • Microsoft Internet Explorer 11 (14.2.x e versioni precedenti) • Mozilla Firefox da 5.x a 83 • Google Chrome 87

Componente	Requisiti
Database	Symantec Endpoint Protection Manager include un database predefinito: • Microsoft SQL Server Express 2014 (per Windows Server 2008 R2) • Microsoft SQL Server Express 2017 • Database Sybase integrato (solo 14.3 MP.x e versioni precedenti) È possibile anche scegliere di utilizzare un database di una delle seguenti versioni di Microsoft SQL Server: • SQL Server 2008 SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012 RTM - SP4 • SQL Server 2014 RTM - SP3 • SQL Server 2016 RTM, SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 e versioni successive) **Note:** I database SQL Server ospitati su Amazon RDS sono supportati (a partire dalla versione 14.0.1 MP2). **Note:** Se Symantec Endpoint Protection utilizza un database SQL Server e l'ambiente utilizza solo TLS 1.2, assicurarsi che SQL Server supporti TLS 1.2. Potrebbe essere necessario applicare delle patch a SQL Server. Questo consiglio vale per SQL Server 2008, 2012 e 2014. Senza la patch di SQL Server per il supporto a TLS 1.2 possono verificarsi problemi durante l'aggiornamento da Symantec Endpoint Protection 12.1 a 14. **Note:** Supporto TLS 1.2 per Microsoft SQL Server
Altri requisiti di ambiente	Nelle reti IPv6 pure, è comunque necessario installare e disattivare lo stack IPv4. Se lo stack IPv4 viene disinstallato, Symantec Endpoint Protection Manager non funziona.

Table 6: Requisiti di sistema dell'hardware per Symantec Endpoint Protection Manager

Componente	Requisiti
Processore	Almeno Intel Pentium Dual-Core o equivalente, consigliati 8 core o più **Note:** I processori Intel Itanium IA-64 non sono supportati.
RAM fisica	Almeno 2 GB di RAM disponibili; consigliati almeno 8 GB **Note:** Il server Symantec Endpoint Protection Manager potrebbe necessitare di ulteriore RAM a seconda dei requisiti RAM di altre applicazioni già installate. Ad esempio, se Microsoft SQL Server è installato sul server Symantec Endpoint Protection Manager, sul server devono essere disponibili almeno 8 GB.
Schermo	1024 x 768 o superiore
Unità disco rigido quando si installa nell'unità di sistema	Con un database SQL Server locale: • Almeno 40 GB disponibili (200 GB consigliati) per il server di gestione e il database Con un database SQL Server remoto: • Almeno 40 GB disponibili (100 GB consigliati) per il server di gestione e il database • Ulteriore spazio su disco disponibile sul server remoto per il database

Componente	Requisiti
Unità disco rigido quando si installa in un'unità alternativa	Con un database SQL Server locale: • L'unità di sistema richiede almeno 15 GB disponibili (100 GB consigliati) • L'unità di installazione richiede almeno 25 GB disponibili (100 GB consigliati) Con un database SQL Server remoto: • L'unità di sistema richiede almeno 15 GB disponibili (100 GB consigliati) • L'unità di installazione richiede almeno 25 GB disponibili (100 GB consigliati) • Ulteriore spazio su disco disponibile sul server remoto per il database
Altro	Una scheda di interfaccia di rete abilitata

Se si utilizza un database SQL Server potrebbe essere necessaria una quantità maggiore di spazio su disco. La quantità e la posizione dello spazio aggiuntivo dipendono dall'unità utilizzata da SQL Server, dai requisiti di manutenzione del database e da altre impostazioni del database.

Table 7: Requisiti di sistema del software per il client Symantec Endpoint Protection per Windows

Componente	Requisiti
Sistema operativo (desktop)	• Windows 7 (a 32 e a 64 bit; RTM e SP1) • Windows Embedded 7 Standard, POSReady e Enterprise (a 32 e 64 bit) • Windows 8 (a 32 e 64 bit) • Windows Embedded 8 Standard (a 32 e 64 bit) • Windows 8.1 (a 32 e 64 bit), compreso Windows To Go • Aggiornamento di Windows 8.1 di aprile 2014 (a 32 e 64 bit) • Aggiornamento di Windows 8.1 di agosto 2014 (a 32 e 64 bit) • Windows Embedded 8.1 Pro, Industry Pro, Industry Enterprise (a 32 e 64 bit) • Windows 10 (versione 1507) (a 32 e 64 bit), compreso Windows 10 Enterprise 2015 LTSB • Windows 10 November Update (versione 1511) (a 32 e 64 bit) • Windows 10 Anniversary Update (versione 1607) (a 32 e 64 bit), compreso Windows 10 Enterprise 2016 LTSB • Windows 10 Creators Update (versione 1703) (a 32 e 64 bit) • Windows 10 Fall Creators Update (versione 1709) (a 32 e 64 bit) • Windows 10 April 2018 Update (versione 1803) (a 32 e 64 bit) • Windows 10 October 2018 Update (versione 1809) (a 32-bit e 64-bit), compreso Windows 10 Enterprise 2019 LTSC. • Windows 10 May 2019 Update (versione 1903) (a 32 bit e 64 bit) • Windows 10 November 2019 Update (versione 1909) (a 32 bit e a 64 bit) (a partire dalla versione 14.2 RU1) • Windows 10 20H1 (Windows 10 versione 2004) (a partire dalla versione 14.3) • Windows 10 20H2 (Windows 10 versione 2009) (a partire dalla versione 14.3 RU1)
Sistema operativo (server)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Aggiornamento di Windows Server 2012 R2 di aprile 2014 • Aggiornamento di Windows Server 2012 R2 di agosto 2014 • Windows Server 2016 • Windows Server 2019 • Windows Server, versione 1803 (Server Core) (a partire dalla versione 14.2) • Windows Server, versione 1809 (Server Core) • Windows Server, versione 1903 (Server Core) (a partire dalla versione 14.2 RU1) • Windows Server, versione 1909 (Server Core) (a partire dalla versione 14.2 RU1) • Windows Server, versione 2004 • Windows Server, versione 20H2 (14.3 RU1)
Prevenzione contro le intrusioni del browser	Il supporto della prevenzione contro le intrusioni del browser è basato sulla versione del motore del sistema di rilevazione delle intrusioni del client (CIDS). Consultare la sezione Browser supportati per la prevenzione contro le intrusioni del browser in Endpoint Protection.

Table 8: Requisiti di sistema dell'hardware per il client Symantec Endpoint Protection per Windows

Componente	Requisiti
Processore (per i computer fisici)	• Processore a 32 bit: Intel Pentium da almeno 2 GHz o equivalente (consigliato Intel Pentium 4 o equivalente) • Processore a 64 bit: Pentium 4 da almeno 2 GHz o equivalente con supporto x86-64 **Note:** I processori Itanium non sono supportati.
Processore (per i computer virtuali)	Minimo un socket virtuale e un core per socket a 1 GHz (consigliati un socket virtuale e due core per socket a 2 GHz) **Note:** La prenotazione di risorsa hypervisor deve essere attivata.
RAM fisica	1 GB (2 GB consigliato) o più, se richiesto dal sistema operativo
Schermo	800 x 600 o superiore
Unità disco rigido	I requisiti di spazio su disco dipendono dal tipo di client che si installa, dall'unità in cui viene installato e dalla posizione dei file di dati del programma. La cartella dei dati del programma si trova solitamente nell'unità di sistema, nella posizione predefinita C:\ProgramData. Lo spazio su disco disponibile nell'unità di sistema è sempre richiesto, indipendentemente dall'unità di installazione scelta. **Note:** I requisiti di spazio sono basati sui file system NTFS. È inoltre richiesto spazio aggiuntivo per gli aggiornamenti dei contenuti e i registri.

Table 9: Requisiti di sistema dell'unità disco rigido per il client Symantec Endpoint Protection per Windows quando viene installato nell'unità di sistema

Tipo di client	Requisiti
Standard	Con la cartella dei dati del programma situata nell'unità di sistema: • 395 MB* Con la cartella dei dati del programma situata in un'unità alternativa: • Unità di sistema: 180 MB • Unità di installazione alternativa: 350 MB
Incorporato/VDI	Con la cartella dei dati del programma situata nell'unità di sistema: • 245 MB* Con la cartella dei dati del programma situata in un'unità alternativa: • Unità di sistema: 180 MB • Unità di installazione alternativa: 200 MB
Dark network	Con la cartella dei dati del programma situata nell'unità di sistema: • 545 MB* Con la cartella dei dati del programma situata in un'unità alternativa: • Unità di sistema: 180 MB • Unità di installazione alternativa: 500 MB

* Durante l'installazione sono richiesti 135 MB aggiuntivi.

Table 10: Requisiti di sistema dell'unità disco rigido per il client Symantec Endpoint Protection per Windows quando viene installato in un'unità alternativa

Tipo di client	Requisiti
Standard	Con la cartella dei dati del programma situata nell'unità di sistema: • Unità di sistema: 380 MB • Unità di installazione alternativa: 15 MB* Con la cartella dei dati del programma situata in un'unità alternativa:** • Unità di sistema: 30 MB • Unità dei dati del programma: 350 MB • Unità di installazione alternativa: 150 MB
Incorporato/VDI	Con la cartella dei dati del programma situata nell'unità di sistema: • Unità di sistema: 230 MB • Unità di installazione alternativa: 15 MB* Con la cartella dei dati del programma situata in un'unità alternativa:** • Unità di sistema: 30 MB • Unità dei dati del programma: 200 MB • Unità di installazione alternativa: 150 MB
Dark network	Con la cartella dei dati del programma situata nell'unità di sistema: • Unità di sistema: 530 MB • Unità di installazione alternativa: 15 MB* Con la cartella dei dati del programma situata in un'unità alternativa:** • Unità di sistema: 30 MB • Unità dei dati del programma: 500 MB • Unità di installazione alternativa: 150 MB

* Durante l'installazione sono richiesti 135 MB aggiuntivi.

** Se la cartella dei dati del programma si trova nell'unità di installazione alternativa, aggiungere 15 MB all'unità dei dati del programma. Tuttavia, il programma di installazione richiede sempre 150 MB disponibili nell'unità di installazione alternativa durante l'installazione.

Table 11: Requisiti di sistema del client Symantec Endpoint Protection per Windows Embedded

Componente	Requisiti
Processore	Intel Pentium da 1 GHz
RAM fisica	256 MB **Note:** Questa cifra si riferisce all'installazione del client incorporato Symantec Endpoint Protection. Se si implementano anche funzionalità aggiuntive di una soluzione integrata come ad esempio EDR, è necessaria una quantità di RAM fisica aggiuntiva.
Unità disco rigido	Il client Symantec Endpoint Protection VDI/incorporato richiede il seguente spazio su disco rigido disponibile: • Installato nell'unità di sistema: 245 MB • Installato in un'unità alternativa: 230 MB nell'unità di sistema e 15 MB nell'unità alternativa Durante l'installazione sono richiesti 135 MB aggiuntivi. Questi valori presumono che la cartella dei dati del programma si trovi nell'unità di sistema. Per ulteriori informazioni o per i requisiti degli altri tipi di client, vedere i requisiti di sistema del client Symantec Endpoint Protection per Windows.

Componente	Requisiti
Sistema operativo Embedded	• Windows Embedded Standard 7 (a 32 e a 64 bit) • Windows Embedded POSReady 7 (a 32 e a 64 bit) • Windows Embedded Enterprise 7 (a 32 e a 64 bit) • Windows Embedded 8 Standard (a 32 e 64 bit) • Windows Embedded 8.1 Industry Pro (a 32 e a 64 bit) • Windows Embedded 8.1 Industry Enterprise (a 32 e a 64 bit) • Windows Embedded 8.1 Pro (a 32 e a 64 bit)
Componenti minimi necessari	• Filter Manager (FltMgr.sys) • Performance Data Helper (pdh.dll) • Servizio Windows Installer
Modelli	• Compatibilità delle applicazioni (impostazione predefinita) • Segnaletica digitale • Automazione industriale • IE, Media Player, RDP • Decoder • Thin client Il modello di configurazione minima non è supportato. Il filtro di scrittura avanzato (EWF) e il filtro di scrittura unificato (UWF) non sono supportati. Il filtro di scrittura consigliato è il Filtro di scrittura basato su file (FBWF) installato con il filtro del registro.

Table 12: Requisiti di sistema del client Symantec Endpoint Protection per Mac

Componente	Requisiti
Processore	Intel Core 2 Duo a 64 bit o versioni successive
RAM fisica	2 GB di RAM
Unità disco rigido	1 GB di spazio disponibile su disco rigido per l'installazione
Schermo	800 x 600
Sistema operativo	• macOS 10.14 macOS 10.14.5 e le versioni sucessive supportano i requisiti di autenticazione kext. Consultare la sezione Endpoint Protection 14.2 RU1 e autenticazione kext per MacOS 10.14.5. • macOS da 10.15 a 10.15.7 Per un elenco dei sistemi operativi supportati per le versioni precedenti, consultare la sezione Compatibilità Mac con il client Endpoint Protection.

Table 13: Requisiti di sistema del client Symantec Endpoint Protection per Linux

Componente	Requisiti
Hardware	• Intel Pentium 4 (2 GHz) o superiore • 500 MB di RAM • 2 GB di spazio disponibile su disco se /var, /opt e /tmp condividono lo stesso volume o filesystem • 500 MB di spazio disponibile su disco in ogni /var, /opt e /tmp su volumi differenti
Sistemi operativi	Sistemi operativi supportati a partire dalla versione 14.3 RU1: • Amazon Linux 2 • CentOS 6.x, 7.x, 8.x • Oracle Enterprise Linux 6.x, 7.x, 8.x • Red Hat Enterprise Linux 6.x, 7.x, 8.x • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Sistemi operativi supportati per la versione 14.3 e le versioni precedenti: • Amazon Linux • CentOS 6U3 - 6U9, 7 - 7U7; 8; 32 bit e 64 bit • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32 bit e 64 bit • Fedora 16, 17; 32 bit e 64 bit • Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32 bit e 64 bit; 12, 12 SP1, 12 SP3, 64 bit • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32 bit e 64 bit; 12 SP3, 64 bit • Ubuntu 12.04, 14.04, 16.04, 18.04 (a partire della versione 14.3); 32 bit e 64 bit Per un elenco dei kernel del sistema operativo supportati per le release precedenti, consultare la sezione Elenco delle distribuzioni e dei kernel Linux con driver/moduli precompilati di Auto-Protect per Symantec Endpoint Protection per Linux 14.x.
Ambienti desktop grafici	È possibile utilizzare i seguenti ambienti desktop grafici per visualizzare il client Symantec Endpoint Protection per Linux: • KDE • Gnome • Unity L'agente Symantec per Linux 14.3 RU1 non dispone di un'interfaccia utente grafica.

Componente	Requisiti

Altri requisiti di ambiente (14.3 MP1 e versioni precedenti)	• Glibc
	Non è supportato alcun sistema operativo che esegue glibc in una versione precedente alla 2.6.
	• net-tools o iproute2
	Symantec Endpoint Protection utilizza uno di questi due strumenti, a seconda di quanto è già installato sul computer.
	• OpenSSL 1.0.2k-fips o versioni successive
	• Strumenti per sviluppatori
	Il processo di compilazione automatica e di compilazione manuale per il modulo Auto-Protect del kernel richiedono l'installazione di determinati strumenti per sviluppatori. Questi strumenti includono gcc e i file di origine e intestazione del kernel. Per dettagli sui componenti da installare e sulla modalità di installazione per versioni specifiche di Linux, consultare:
	Compilazione manuale dei moduli Auto-Protect del kernel per Endpoint Protection per Linux
	• Pacchetti dipendenti basati su i686 nei computer a 64 bit
	Molti dei file eseguibili nel client Linux sono programmi a 32 bit. Per i computer a 64 bit è necessario installare i pacchetti basati su i686 dipendenti prima di installare il client per Linux.
	Se i pacchetti basati su i686 dipendenti non sono stati installati, è possibile installarli dalla riga di comando. L'installazione richiede i privilegi di utente avanzato, dimostrabili con `sudo` mediante i seguenti comandi:
	– Per le distribuzioni basate su Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Per le distribuzioni basate su Debian: `sudo apt-get install ia32-libs`
	– Per le distribuzioni basate su Ubuntu:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`

Versioni di rilascio, note, nuove correzioni e requisiti di sistema per Endpoint Security e per tutte le versioni di Endpoint Protection

Percorsi di aggiornamento supportati e non supportati alla versione più recente di Symantec Endpoint Protection 14.x

In genere, per le versioni di Symantec Endpoint Protection precedenti alla versione più recente, è supportata ogni versione che precede nell'elenco. Verificare consultando le note di rilascio fornite con la versione specifica.

Versioni di rilascio, note, nuove correzioni e requisiti di sistema per Endpoint Security e per tutte le versioni di Endpoint Protection

Percorsi di aggiornamento supportati

- Symantec Endpoint Protection Manager versione 12.1.6 MP10 e versioni successive con il database integrato esegue l'aggiornamento in modo trasparente al database Microsoft SQL Server Express, versione 14.3 RU1. Gli aggiornamenti da 12.1.6 MP9 e versioni precedenti a 14.3 RU1 sono bloccati.
- Symantec Endpoint Protection Manager 14.x esegue l'aggiornamento in modo trasparente su 12.1.x, ad eccezione dei casi in cui il supporto è stato rimosso, come ad esempio Windows Server 2003, i sistemi operativi desktop e i sistemi operativi a 32 bit, nonché alcune versioni di SQL Server.
- Il client Symantec Endpoint Protection 14.x esegue l'aggiornamento in modo trasparente su tutte le versioni precedenti del client 12.1 e 11 installate sui sistemi operativi supportati. L'eccezione riguarda il fatto che per client Mac di versioni precedenti alla 12.1.4, sia necessario eseguire l'aggiornamento a 12.1.4 (o versioni successive) oppure eseguire la disinstallazione.

Considerazioni sulla migrazione di Symantec Endpoint Protection 14

Symantec Endpoint Protection Manager e client Windows

È possibile eseguire l'upgrade delle seguenti versioni di Symantec Endpoint Protection Manager e del client Windows Symantec Endpoint Protection direttamente alla versione corrente:

- 11.x e Small Business Edition 12.0 (solo per i client Symantec Endpoint Protection, per i sistemi operativi supportati)
- 12.1.x, fino a 12.1.6 MP10
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

Client Mac

È possibile eseguire l'upgrade delle seguenti versioni del client Symantec Endpoint Protection per Mac direttamente alla versione corrente:

- 12.1.4 - 12.1.6 MP9
  Il client Mac non è stato aggiornato per la versione 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

NOTE

Il client Symantec Endpoint Protection per Mac non è stato aggiornato in 14.0.1 MP2.

Client Linux

NOTE
L'agente Symantec per Linux 14.3 RU1 rileva e disinstalla il client Symantec Endpoint Protection precedente per Linux, quindi esegue una nuova installazione. Le configurazioni precedenti non verranno conservate.

È possibile eseguire l'upgrade delle seguenti versioni del client Symantec Endpoint Protection per Linux direttamente alla versione corrente:

- 12.1.x, fino a 12.1.6 MP9
  Il client Linux non è stato aggiornato per la versione 12.1.6 MP10.
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

Symantec AntiVirus per Linux 1.0.14 è la sola versione di cui è possibile eseguire la migrazione direttamente a Symantec Endpoint Protection. È necessario prima disinstallare tutte le altre versioni di Symantec AntiVirus per Linux. Non è possibile eseguire la migrazione di un client gestito a un client non gestito.

Percorsi di upgrade non supportati

Non è possibile eseguire la migrazione a Symantec Endpoint Protection da tutti i prodotti Symantec. È necessario disinstallare i seguenti prodotti prima di installare il client Symantec Endpoint Protection:

- Symantec AntiVirus e Symantec Client Security, i quali non sono supportati.
- Tutti i prodotti Symantec Norton
- Symantec Endpoint Protection per Windows XP Embedded 5.1
- Qualsiasi versione di Symantec Endpoint Protection per il client Mac precedente a 12.1.4. In alternativa, è possibile eseguire l'aggiornamento a 12.1.4 o versioni successive.

Note:

- Qualsiasi migrazione del client Symantec Endpoint Protection per la versione precedente alla versione 12.1.x non è supportata.
- Non è possibile eseguire l'aggiornamento diretto di Symantec Endpoint Protection Manager 11.0.x o Symantec Endpoint Protection Manager Small Business Edition 12.0.x su qualsiasi versione di Symantec Endpoint Protection Manager 14. È necessario disinstallare prima queste versioni oppure eseguire l'aggiornamento a 12.1.x prima dell'aggiornamento della versione più recente di 14.x.
- Non è possibile eseguire l'upgrade di Symantec Endpoint Protection Manager 12.1.6 MP7 alla versione 14 perché la versione dello schema del database di 12.1.6 MP7 è successiva alla 14. Eseguire l'upgrade di 12.1.6 MP7 a 14 MP1 o versione successiva.
- Il supporto per la versione 14.0.x è stato interrotto per Windows XP, Server 2003 e qualsiasi sistema operativo Windows integrato basato su Windows XP. Symantec Endpoint Protection Manager 14.2 RU1 è in grado di gestire questi computer come legacy dei client 12.1.x client, sebbene i client 12.1.x siano EOL. Per questi client, è possibile

utilizzare un prodotto Symantec che supporta ancora questi sistemi operativi legacy, come ad esempio Data Center Security (DCS).

- L'upgrade da 14 MP1 (14.0.2332.0100) a 14 MP1 Refresh Build (14.0.2349.0100) non è supportato.
- I percorsi di downgrade non sono supportati. Ad esempio, se si desidera eseguire la migrazione dalla versione 14.2.1.1 di Symantec Endpoint Protection alla versione 12.1.6 MP10, è necessario in primo luogo disinstallare Symantec Endpoint Protection 14.2.1.1.
- Se si conosce il numero di build ma non si è certi della versione della distribuzione a cui corrisponde, vedere: Informazioni sui tipi di release e sulle versioni di Endpoint Protection

Dove ottenere ulteriori informazioni

La seguente tabella visualizza i siti Web in cui è possibile consultare best practice, informazioni per la risoluzione degli errori e altre risorse utili per l'uso del prodotto.

Table 14: Informazioni sul sito Web di Endpoint Protection

Tipi di informazioni	Collegamento al sito Web
Versioni di prova	Contattare il rappresentante dell'account.
Manuali e aggiornamenti della documentazione	• Guide di prodotto per la versione più recente (inglese) • Guide di prodotto per la versione più recente (altre lingue) • Guide di prodotto per tutte le versioni di Symantec Endpoint Protection 14.x (inglese)
Supporto tecnico	Supporto tecnico di Endpoint Protection Include articoli della knowledge base, dettagli della versione del prodotto, aggiornamenti, patch e opzioni di contatto del supporto.
Informazioni e aggiornamenti relativi alle minacce	Symantec Security Center
Formazione	Servizi di formazione Consente di accedere ai corsi di formazione, eLibrary e altro ancora.
Forum di Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom