Note di rilascio di Symantec™ Endpoint Protection 14.3

Ultimo aggiornamento: giugno 2020

Table of Contents

Dichiarazione sul copyright

Novità di Symantec Endpoint Protection 14.3

In questa sezione vengono descritte le nuove funzionalità per la release 14.3.

Funzionalità di protezione

- Gli sviluppatori di applicazioni di terze parti possono proteggere i propri clienti da malware basati su script dinamici e da modalità non tradizionali di cyberattack.L'applicazione di terze parti richiama l'interfaccia AMSI di Windows per richiedere un'analisi degli script forniti dall'utente, indirizzati al client di Symantec Endpoint Protection. Il client risponde con un verdetto per indicare se il comportamento dello script è dannoso. Se il comportamento non è dannoso, l'esecuzione dello script procede. Se il comportamento dello script è dannoso, l'applicazione non viene eseguita.Sul client, la finestra di dialogo Risultati di rilevamento visualizza lo stato "Accesso negato".Esempi di script di terze parti includono Windows PowerShell, JavaScript e VBScript. Auto-Protect deve essere attivato. Questa funzionalità funziona per i computer Windows 10 e versioni successive.
  Come il componente Antimalware Scan Interface (AMSI) consente di difendersi da malware
  Antimalware Scan Interface (AMSI)

Symantec Endpoint Protection Manager

- La console remota di Symantec Endpoint Protection ora supporta Java 11 invece di Java 8.Per accedere alla console remota, aprire un browser Web supportato e digitare il seguente indirizzo nella casella corrispondente: `http://SEPMServer:9090/symantec.html` e scaricare il nuovo pacchetto della console remota. Seguire le istruzioni riportate. La versione precedente della console remota di Symantec Endpoint Protection Manager non è più supportata.
  Accesso a Symantec Endpoint Protection
- È possibile configurare una delle utilità di gestione di Symantec Endpoint Protection sul sito come server di registrazione principale per inoltrare i registri al server syslog. Se il server di registrazione principale non è in linea, verrà sostituito da un secondo server di gestione, il quale inoltra i registri al server syslog. Quando il server di registrazione principale torna in linea, riprende l'inoltro dei registri.
  Configurazione di un server di failover per la registrazione esterna
- La politica Integrazioni dispone di una nuova opzione per il reindirizzamento del traffico WSS, **Abilita file PAC personalizzato di LPS.**Questa opzione consente di sostituire il file PAC predefinito ospitato dal server LPS sul client con un file PAC personalizzato. Il file PAC personalizzato risolve i problemi di compatibilità con applicazioni di terze parti che non funzionano con un server proxy locale in ascolto sulla scheda di loopback.
  Configurazione di WSS Traffic Redirection
- Supporto per il database Microsoft SQL Server 2019.
- Il processo di scansione antivirus ora utilizza un servizio differente dal servizio principale non di protezione. Questo nuovo processo di scansione garantisce un utilizzo più efficiente della memoria, una protezione continua e una minore dipendenza dai problemi relativi al servizio principale.
- Lo schema del database include nuove colonne come parte di una funzionalità per una release futura. (tabelle AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2, SEM_AGENT)
- L'API REST contiene i seguenti campi nel JSON di risposta API di sepm/api/v1/computers per richiamare e scaricare il report Stato del computer: quarantineStatus, quarantineCode, wssStatus, pskVersion.
- Aggiornamento dei seguenti componenti di terze parti alle versioni più recenti: Apache Tomcat, Boost C++ Libraries, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, Microsoft JDBC Driver for SQL Server, OpenSC, OpenSSL, Spring Security, spring-framework, sqlite.
- Per registrare il dominio di Symantec Endpoint Protection Manager nella console cloud, è necessario innanzitutto ricevere il token di registrazione tramite la console di Symantec Endpoint Security. In precedenza, era possibile ottenere il token di registrazione facendo clic su **Introduzione** nella pagina **Cloud**.

Aggiornamenti di client e piattaforme

- Il client Windows supporta Windows 10 20H1 (Windows 10 versione 2004)
- Il client Linux ora supporta Ubuntu 18.04, RHEL 8 e CentOS 8.
- Lo strumento AppRemover è stato aggiornato a una versione più recente.Lo strumento AppRemover rimuove le applicazioni di terze parti prima di poter installare il client Windows.Per ulteriori informazioni su quali applicazioni vengono rimosse, consultare la sezione Rimozione del software di protezione di terze parti in Endpoint Protection 14.3

Funzionalità rimosse

- Le seguenti notifiche non mostrano più i campi **Gravità rischio** e **Tipo di rischio**: Rischio epidemia, Evento rischio singolo e Nuovo rischio rilevato.

Novità di tutte le release di Symantec Endpoint Protection

Risoluzione di problemi noti

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

Table 1: Problemi di aggiornamento

Problema	Descrizione e soluzione
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. L'aggiornamento SQL da 2017 a 2019 non viene eseguito correttamente e la modalità FIPS è abilitata
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
Whitelist di URL aggiuntivi in Symantec Endpoint Security se si utilizzano l'opzione di gestione ibrida e i server proxy [14.2.2.1 o versione successiva]	Con l'acquisizione recente 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. Per inserire gli URL in whitelist in agenti completamente gestiti da cloud o ibridi, è necessario eseguire inserirli nella whitelist in Symantec Endpoint Security: 1. In Symantec Endpoint Security, accedere a **Endpoint > Politiche > Politica Whitelist [nome politica]**. 2. Nella politica Whitelist, accanto a **Escluso dal dominio**, selezionare **Aggiungi**, aggiungere uno alla volta gli URL seguenti e selezionare **Aggiungi**: `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (aggiungere i dispositivi presenti in Europa). Mantenere spoc.norton.com se si continua a gestire i client con una versione successiva. 3. Selezionare **Salva politica**, quindi fare clic su **Sì** per aggiornare la politica e applicarla ai gruppi esistenti. Consultare la sezione URL per l'inserimento in whitelist per Symantec Endpoint Security. Consultare la sezione Aggiornamento degli agenti Symantec gestiti da cloud alla versione 14.2 RU2 MP1 (o versione successiva) del 4 maggio 2020.
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 compatibile con la versione di Windows in esecuzione. Verificare le informazioni sul sistema del computer e contattare l'autore del software." Accesso a Symantec Endpoint Protection Manager
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.

Problema	Descrizione e soluzione
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
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 di 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.

Problema	Descrizione e soluzione
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. Una correzione per questo problema è pianificata per una versione 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 un elenco dei problemi risolti, consultare la sezione: 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. Windows Server Core non include Internet Explorer, che Symantec Endpoint Protection Manager richiede per funzionare.
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: • 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 • Mozilla Firefox da 5.x a 68.x • Google Chrome 75.x

Componente	Requisiti
Database	**Symantec Endpoint Protection Manager include un database incorporato. 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 (dalla versione 14.3) **Note:** L'edizione del database SQL Server Express non è supportata.I database di 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 di TLS 1.2, possono verificarsi problemi durante l'aggiornamento da Symantec Endpoint Protection 12.1 alla versione 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 incorporato o 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
Unità disco rigido quando si installa in un'unità alternativa	**Con un database incorporato o 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

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 64 bit) (a partire dalla versione 14.2 RU1) • Windows 10 20H1 (Windows 10 versione 2004) (a partire dalla versione 14.3)
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)
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. **Requisiti di sistema dell'unità disco rigido:** • I requisiti di sistema per i dischi rigidi del client Symantec Endpoint Protection per Windows sono installati sull'unità di sistema descrivono i requisiti di sistema del disco rigido quando Symantec Endpoint Protection è installato sull'unità di sistema. • I requisiti di sistema per i dischi rigidi del client Symantec Endpoint Protection per Windows installati su un'unità alternativa descrivono i requisiti di sistema del disco rigido quando Symantec Endpoint Protection è installato su un'unità alternativa. **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: Client Symantec Endpoint Protection per i requisiti di sistema di Mac

Componente	Requisiti
Processore	Intel Core 2 Duo a 64 bit o versioni successive
RAM fisica	2 GB di RAM
Unità disco rigido	500 MB di spazio disponibile su disco rigido per l'installazione
Schermo	800 x 600
Sistema operativo	• macOS 10.13 • macOS 10.14 • macOS da 10.15 a 10.15.5 macOS 10.14.5 e le versioni successive supportano i requisiti di autenticazione kext. Consultare la sezione Endpoint Protection 14.2 RU1 e autenticazione kext per MacOS 10.14.5. 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 • 1 GB di RAM • 7 GB di spazio disponibile su disco rigido
Sistemi operativi	• 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 dei sistemi operativi supportati per le release precedenti, consultare la sezione Kernel Linux supportati per Symantec Endpoint Protection.
Ambienti desktop grafici	È possibile utilizzare i seguenti ambienti desktop grafici per visualizzare il client Symantec Endpoint Protection per Linux: • KDE • Gnome • Unity

Altri requisiti ambientali	• Glibc
	Non è supportato alcun sistema operativo che esegue glibc in una versione precedente alla 2.6.
	• 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`
	• net-tools o iproute2
	Symantec Endpoint Protection utilizza uno di questi due strumenti, a seconda di quanto è già installato sul computer.
	• 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

Note di rilascio e requisiti di sistema per tutte le versioni di Symantec Endpoint Protection

Percorsi di aggiornamento supportati per la versione più recente di Symantec Endpoint Protection 14.x

NOTE

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.

Note di rilascio, nuove correzioni e requisiti di sistema per tutte le versioni di Endpoint Protection

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

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
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

NOTE

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

Client Linux

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

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:

- Prodotti non supportati Symantec AntiVirus e Symantec Client Security
- Tutti i prodotti Symantec Norton™
- Symantec Endpoint Protection per Windows XP Embedded 5.1
- Versioni di Symantec Endpoint Protection per Mac precedenti alla 12.1.4

Non è possibile eseguire l'upgrade di Symantec Endpoint Protection Manager 11.0.x o Symantec Endpoint Protection Manager Small Business Edition 12.0.x direttamente a qualunque versione di Symantec Endpoint Protection Manager 14. È necessario disinstallare queste versioni oppure eseguire l'upgrade a 12.1.x prima dell'upgrade a 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.

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:

- Versioni rilasciate di Symantec Endpoint Protection
- Informazioni sui tipi di release e sulle versioni di Endpoint Protection

Dove ottenere ulteriori informazioni

Le informazioni su Endpoint Protection mostrano i siti Web in cui è possibile consultare best practice, informazioni per la risoluzione dei problemi 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) **Altre lingue:**
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