Versionshinweise zu Symantec™ Endpoint Protection 14.3

Zuletzt aktualisiert: Juni 2020

Table of Contents

Copyright-Erklärung

Neue Funktionen in Symantec Endpoint Protection 14.3

In diesem Abschnitt werden die neuen Funktionen für Version 14.3 beschrieben.

Schutzfunktionen

- Anwendungsentwickler von Drittanbietern können ihre Kunden vor dynamischer, skriptbasierter Malware und außergewöhnlichen Cyberangriffen schützen.Die Drittanbieteranwendung ruft die Windows AMSI-Schnittstelle auf, um einen Scan des vom Benutzer bereitgestellten Skripts anzufordern, der an den Symantec Endpoint Protection-Client weitergeleitet wird. Der Client sendet eine Antwort, in der angegeben ist, ob das Skriptverhalten bösartig ist. Wenn das Verhalten nicht bösartig ist, wird die Ausführung des Skripts fortgesetzt. Wenn das Verhalten des Skripts bösartig ist, wird es von der Anwendung nicht ausgeführt.Im Client wird im Dialogfeld "Erkennungsergebnisse" der Status "Zugriff verweigert" angezeigt.Beispiele für Skripte von Drittanbietern sind Windows PowerShell, JavaScript und VBScript. Auto-Protect muss aktiviert sein. Diese Funktion ist für Windows 10 und höhere Computer geeignet.
  How the Antimalware Scan Interface (AMSI) helps you defend against malware (nur auf Englisch verfügbar)
  Antimalware Scan Interface (AMSI) (nur auf Englisch verfügbar)

Symantec Endpoint Protection Manager

- Die Remote-Konsole von Symantec Endpoint Protection unterstützt jetzt Java 11 anstelle von Java 8.Um auf die Remote-Konsole zuzugreifen, öffnen Sie einen unterstützten Webbrowser und geben Sie die folgende Adresse in das Adressfeld ein: `http://SEPMServer:9090/symantec.html` und laden Sie das Paket für die neue Remote Console herunter. Befolgen Sie die Anweisungen. Die Vorgängerversion der Remote-Konsole für Symantec Endpoint Protection Manager wird nicht mehr unterstützt.
  Einloggen bei Symantec Endpoint Protection
- Sie können einen der Symantec Endpoint Protection Manager am Standort als Master-Protokollierungs-Server konfigurieren, um Protokolle an den Syslog-Server weiterzuleiten. Wenn der Master-Protokollierungs-Server offline geht, übernimmt der zweite Management-Server und leitet die Protokolle an den Syslog-Server weiter. Wenn der Master-Protokollierungs-Server wieder online ist, wird die Weiterleitung der Protokolle auf diesem fortgesetzt.
  Konfigurieren von Failover-Servern für die externe Protokollierung
- Die Integrationsrichtlinie verfügt über eine neue Option für die WSS-Datenverkehrsumleitung: **Benutzerdefinierte PAC-Datei des LPS aktivieren**.Mit dieser Option können Sie die PAC-Standarddatei, die vom LPS-Server auf dem Client gehostet wird, durch eine benutzerdefinierte PAC-Datei ersetzen. Die benutzerdefinierte PAC-Datei löst Kompatibilitätsprobleme mit Anwendungen von Drittanbietern, die nicht mit einem lokalen Proxy-Server funktionieren, der den Loopback-Adapter überwacht.
  Konfigurieren der WSS-Datenverkehrsumleitung
- Unterstützung für die Microsoft SQL Server 2019-Datenbank
- Der Antivirusscan-Prozess verwendet jetzt einen Dienst, der vom nicht-sicherheitsbezogenen Hauptdienst getrennt ist. Dieser neue Scan-Prozess ermöglicht eine effizientere Speicherauslastung, kontinuierlichen Schutz und eine geringere Abhängigkeit von Problemen mit dem Hauptdienst.
- Das Datenbankschema enthält neue Spalten als Teil einer Funktion für eine zukünftige Version. (Tabellen AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2, SEM_AGENT)
- Die Rest-API enthält die folgenden Felder in der API-Antwort-JSON "/sepm/api/v1/computers" zum Aufrufen und Herunterladen des Berichts "Computerstatus": quarantineStatus, quarantineCode, wssStatus, pskVersion.
- Aktualisierung der folgenden Drittanbieterkomponenten auf neuere Versionen: Apache Tomcat, Boost C++-Bibliotheken, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, Microsoft JDBC-Treiber für SQL Server, OpenSC, OpenSSL, Spring Security, Spring Framework, SQLite.
- Um die Symantec Endpoint Protection Manager-Domäne in der Cloud-Konsole anzumelden, müssen Sie zuerst das Anmelde-Token über die Symantec Endpoint Security-Konsole abrufen. In der Vergangenheit haben Sie das Anmelde-Token erhalten, indem Sie auf der Seite **Cloud** auf **Erste Schritte** geklickt haben.

Client- und Plattform-Updates

- Der Windows-Client unterstützt Windows 10 20H1 (Windows 10 Version 2004).
- Der Linux-Client unterstützt jetzt Ubuntu 18.04, RHEL 8 und CentOS 8.
- Das AppRemover-Tool wurde auf eine neuere Version aktualisiert.Das AppRemover-Tool entfernt Anwendungen von Drittanbietern, bevor Sie den Windows-Client installieren können.Weitere Informationen darüber, welche Anwendungen entfernt werden, finden Sie unter Entfernen von Sicherheitssoftware von Drittanbietern in Endpoint Protection 14.3.

Entfernte Funktionen

- In den folgenden Benachrichtigungen werden die Felder **Risikoschweregrad** und **Risikotyp** nicht mehr angezeigt: Risikoausbruch, Einzelnes Risikoereignis, Neues Risiko erkannt.

Neue Funktionen in allen Versionen von Symantec Endpoint Protection

Bekannte Probleme und Problemumgehungen

Die Probleme in diesem Abschnitt gelten für diese Version von Symantec Endpoint Protection.

Table 1: Probleme mit Upgrades

Problem	Beschreibung und Lösung
Ein SQL Server-Upgrade von Version 2017 auf Version 2019 schlägt mit aktiviertem FIPS-Modus fehl [14.3]	Möglicherweise wird folgender Fehler angezeigt: "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." Dieser Fehler tritt auf, wenn Sie einen FIPS-aktivierten Symantec Endpoint Protection Manager 14.3 haben und ein Upgrade von Microsoft SQL Server 2017 auf 2019 durchführen. [SEP-61473] Um dieses Problem zu umgehen, deaktivieren Sie FIPS auf Betriebssystemebene: 1. Klicken Sie in `C:\ProgramData\Microsoft\Windows\Startmenü \Programme\Verwaltungs-Programme` auf **Lokale Sicherheitsrichtlinie** > **Lokale Richtlinien** > **Sicherheitsoptionen** und deaktivieren Sie die Option **Systemkryptografie: FIPS-konformen Algorithmus für Verschlüsselung, Hashing und Signatur verwenden**. 2. Führen Sie ein Upgrade von SQL Server Version 2017 auf Version 2019 durch. 3. Nachdem SQL Server erfolgreich aktualisiert wurde, aktivieren Sie FIPS erneut. SQL-Upgrade von 2017 auf 2019 schlägt mit aktiviertem FIPS-Modus fehl
Benutzerdefinierte Namen verhindern möglicherweise, dass die Firewall-Richtlinie beim Aktualisieren auf 14.2 aktualisiert wird.	Beim Aktualisieren auf Symantec Endpoint Protection 14.2 oder höher können Firewall-Richtlinien die Änderungen für IPv6 nicht übernehmen, wenn bestimmte Standardnamen geändert wurden. Dazu gehören die Namen von Standardrichtlinien und Standardregeln. Wenn die Regeln während des Upgrades nicht aktualisiert werden können, werden die IPv6-Optionen nicht angezeigt. Alle neuen Richtlinien oder Regeln, die Sie nach dem Upgrade erstellen, sind nicht betroffen. Wenn möglich, ändern Sie alle geänderten Namen auf den Standardwert zurück. Stellen Sie andernfalls sicher, dass benutzerdefinierte Regeln, die Sie einer Standardrichtlinie hinzugefügt haben, die IPv6-Kommunikation nicht blockieren. Stellen Sie dies auch für neue Richtlinien oder Regeln sicher, die Sie hinzufügen.

Table 2: Probleme mit Symantec Endpoint Protection Manager

Problem	Beschreibung und Lösung
Weitere URLs in Symantec Endpoint Security auf die Positivliste setzen, wenn Sie die Option für Hybrid-Management und Proxy-Server verwenden [14.2.2.1 oder höher]	Mit der Übernahme von Symantec Enterprise Security durch Broadcom wurde die URL für die Kommunikation zwischen Client und Cloud in 14.2.2.1 geändert. [CDM-42467] In den folgenden Situationen müssen Sie Ihre Clients auf Version-Build 14.2.5569.2100 oder höher aktualisieren: • Sie verwenden Symantec Endpoint Security, um Ihre Clients und Richtlinien zu verwalten, wenn Ihre On-Premise-Domänen von Symantec Endpoint Protection Manager in der Cloud-Konsole angemeldet sind. • Sie verwenden Proxy-Server. Um URLs entweder in vollständig Cloud-verwalteten oder hybrid verwalteten Agenten zu Positivlisten hinzuzufügen, müssen Sie diese in Symantec Endpoint Security auf eine Positivliste setzen: 1. Gehen Sie in Symantec Endpoint Security zu **Endgerät > [Name der Richtlinie] Richtlinie für die Positivliste**. 2. Wählen Sie in "Richtlinie für die Positivliste" neben **Excluded by Domain** die Option **Hinzufügen** aus, fügen Sie die folgenden URLs nacheinander hinzu und wählen Sie **Hinzufügen** aus: `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (fügen Sie diese URL hinzu, wenn Sie Geräte in Europa haben) Behalten Sie spoc.norton.com bei, wenn Sie weiterhin Clients mit einer höheren Version verwalten. 3. Klicken Sie auf **Richtlinie speichern** und dann auf **Ja**, um die Richtlinie zu aktualisieren und auf vorhandene Gruppen anzuwenden. Weitere Informationen finden Sie unter URLs für die Positivliste von Symantec Endpoint Security. Weitere Informationen finden Sie unter Aktualisieren von Cloud-verwalteten Symantec-Agenten auf Version 14.2 RU2 MP1 oder höher bis zum 4. Mai 2020.
Die 32-Bit-Windows-Plattform wird von der Remote-Konsole von Symantec Endpoint Protection Manager nicht mehr unterstützt [14.3]	Ab Version 14.3 können Sie sich nicht bei der Remote-Konsole von Symantec Endpoint Protection Manager einloggen, wenn Sie eine 32-Bit-Version von Windows ausführen. Die 32-Bit-Version von Microsoft Windows wird nicht mehr von Oracle Java SE Runtime Environment unterstützt. [SEP-61106] Wenn die folgende Meldung angezeigt wird, loggen Sie sich lokal bei Symantec Endpoint Protection Manager ein: "Diese Version von C:\Benutzer\Administrator\Downloads\Symantec Endpoint Protection Manager-Konsole\bin\javaw.exe ist mit der von Ihnen ausgeführten Windows-Version nicht kompatibel. Überprüfen Sie die Systeminformationen Ihres Computers und wenden Sie sich an den Softwareherausgeber." Einloggen bei Symantec Endpoint Protection Manager
Fehler "Microsoft Visual C++ Runtime konnte nicht installiert werden" wird bei der Installation von Symantec Endpoint Protection Manager angezeigt [14.3]	Möglicherweise wird bei der Installation von Symantec Endpoint Protection Manager unter Windows 2012 R2 folgender Fehler angezeigt: "Microsoft Visual C++ Runtime konnte nicht installiert werden". [SEP-60396] Um dieses Problem zu umgehen, aktivieren Sie Windows und installieren Sie die Windows-Updates. Mit dem Windows-Update wird Visual C++ 2017 Redistributable installiert. Dies ist eine Voraussetzung für die Installation von Symantec Endpoint Protection Manager 14.3 unter Windows 2012 R2.

Problem	Beschreibung und Lösung
Update, um TLS 1.1 und TLS 1.2 als standardmäßige sichere Protokolle in WinHTTP unter Windows zu aktivieren [14.3]	Nachdem Sie ein Upgrade auf Symantec Endpoint Protection Manager Version 14.3 durchgeführt oder diese Version installiert haben und wenn diese Version in der Cloud-Konsole angemeldet ist, lädt der Management-Server die Protokolle nicht mehr erfolgreich in die Cloud hoch. In der Datei "uploader.log" wird möglicherweise der folgende Fehler angezeigt: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Dieses Problem wird durch ein fehlendes Microsoft-Update verursacht, das Unterstützung für TLS 1.1 und 1.2 bietet. Um das Problem zu lösen, installieren Sie das Microsoft-Update KB3140245. Weitere Informationen finden Sie hier: Update, um TLS 1.1 und TLS 1.2 als standardmäßige sichere Protokolle in WinHTTP unter Windows zu aktivieren
Die Meldung "Bereitstellung läuft..." wird weiterhin in Symantec Endpoint Protection Manager angezeigt, nachdem der Client eine aktualisierte Richtlinie für Endpoint Threat Defense for AD [14.2 RU1 MP1 und höher] erhalten hat.	Dies ist ein zu erwartendes Verhalten. Richtlinien für Endpoint Threat Defense for AD 3.3 werden auf dem Client nur ab Version 14.2 RU1 MP1 unterstützt. Sie wenden eine Richtlinie für Symantec Endpoint Threat Defense for Active Directory 3.3 auf eine Gruppe an. Diese Gruppe enthält einige Clients, auf denen Symantec Endpoint Protection 14.2 RU1 oder früher ausgeführt wird. Diese Clients erhalten die Richtlinie und wenden sie wie erwartet an, aber der Status in Symantec Endpoint Protection Manager lautet weiterhin "Bereitstellung läuft...".

Table 3: Probleme mit Windows-, Mac- und Linux-Clients

Problem	Beschreibung und Lösung
Die Installation des Windows-Clients für Symantec Endpoint Protection 14.3 kann fehlschlagen, wenn Sie vorher nicht die SHA-2-Unterstützung installieren [14.3]	Wenn Sie ältere Betriebssystemversionen (Windows 7 RTM oder SP1, Windows Server 2008 R2 oder R2 SP1 oder R2 SP2) ausführen, müssen Sie auf Ihren Geräten die Unterstützung der SHA-2-Codesignierung installiert haben, um Windows-Updates zu installieren, die im Juli 2019 oder später veröffentlicht wurden. Ohne die SHA-2-Unterstützung schlägt die Installation des Windows-Clients manchmal fehl. Die Installation kann fehlschlagen, wenn Sie Clients zum ersten Mal installieren oder ein automatisches Upgrade von einer Vorgängerversion durchführen. [SEP-61175/61403] Um die von Microsoft erzwungene Unterstützung der SHA-2-Codesignierung zu erhalten, finden Sie weitere Informationen unter: Unterstützung der SHA-2-Codesignierung für Windows und WSUS (2019) Die Installation des Windows-Clients für Symantec Endpoint Protection 14.3 kann fehlschlagen, wenn keine SHA-2-Unterstützung installiert ist
Der Windows-Client für Symantec Endpoint Protection wird nicht ausgeführt, wenn er unter Windows 10 1803 mit aktiviertem UWF installiert ist [14.3]	Wenn der Symantec Endpoint Protection-Client auf dem Windows 10 RS4 1803 32-Bit-Betriebssystem ausgeführt wird und der einheitliche Schreibfilter (Unified Write Filter, UWF) aktiviert ist und das Laufwerk schützt, auf dem der Windows-Client installiert ist, wird der Client nicht ordnungsgemäß ausgeführt. Dieses Windows-Betriebssystem enthält einen UWF-Fehler, der verhindert, dass der Windows-Client ausgeführt wird. Um dieses Problem zu umgehen, gehen Sie wie folgt vor: • Führen Sie ein Upgrade auf eine andere Version des Betriebssystems durch, die den Fehler nicht enthält. • Deaktivieren Sie UWF.Weitere Informationen finden Sie unter Endpoint Protection funktioniert bei einer Installation auf Windows 10 1803 mit aktiviertem UWF nicht ordnungsgemäß.

Problem	Beschreibung und Lösung
Mac-Clients, auf denen die WSS-Datenverkehrsumleitung aktiviert ist, berücksichtigen die benutzerdefinierten Proxy-Einstellungen für LiveUpdate nicht [14.2 RU1 MP1 und höher]	Sie haben Ihre verwalteten Mac-Clients für Symantec Endpoint Protection 14.2 RU1 MP1 oder höher so konfiguriert, dass benutzerdefinierte Proxy-Einstellungen für LiveUpdate über externe Kommunikationseinstellungen verwendet werden können. Nachdem Sie die WSS-Datenverkehrsumleitung (WDU) für Mac-Clients über die Symantec Endpoint Protection Manager-Richtlinie aktiviert haben, werden Ihre benutzerdefinierten Proxy-Einstellungen für den LiveUpdate-Datenverkehr jedoch nicht mehr berücksichtigt. Stattdessen versucht LiveUpdate, eine Direktverbindung herzustellen. Verwenden Sie zum Umgehen dieses Problems nur benutzerdefinierte Proxy-Einstellungen für LiveUpdate, wenn die WSS-Datenverkehrsumleitung deaktiviert ist.
Microsoft Edge lässt das Herunterladen von PDFs zu, obwohl die Anwendungshärtung aktiviert ist [14.2 RU1 MP1 und höher]	Wenn die Anwendungshärtung auf dem Symantec Endpoint Protection-Client aktiviert ist, ist der Download von PDF-Dateien unerwartet möglich, wenn Sie den Microsoft Edge-Browser verwenden. Unter anderen Browsern wird das Herunterladen von PDFs wie erwartet verhindert. Eine Fehlerbehebung für dieses Problem ist für eine zukünftige Version geplant.

Mit der Ankündigung von Broadcom, dass Symantec Enterprise Protection offiziell zu Broadcom gehört, wurde die Dokumentation von Symantec zum Tech Docs-Portal für Symantec Security von Broadcom migriert.

Um die Dokumentation für Endpoint Protection zu finden, klicken Sie auf die Registerkarte **Symantec Security Software** und dann auf **Endpoint Security and Management** > **Endpoint Protection**.

Table 4: Probleme mit der Dokumentation

Problem	Beschreibung und Lösung
Die HOWTO-Artikel sind abgelaufen.	Die HOWTO-Artikel, bei denen es sich um Duplikate der Themen in der Symantec Endpoint Protection Manager-Hilfe handelte, wurden auf der Site für Endpoint Protection erneut veröffentlicht und haben jetzt eine andere URL. Um einen Artikel zu finden, verwenden Sie das **Suchfeld**.
PDF-Dateien	Symantec hat alle PDF-Dateien zu Dokumentationsartikeln veröffentlicht. Diese Seiten sind abgelaufen. Um die aktuellste Version der PDF-Datei zu finden, gehen Sie zur Seite Zugehörige Dokumente. In der Zukunft wird Broadcom ältere PDF-Dateien und übersetzte PDF-Dateien hinzufügen.

Gelöste Probleme finden Sie unter Neue Fehlerbehebungen und Komponenten für Symantec Endpoint Protection 14.3.

Systemanforderungen für Symantec Endpoint Protection (SEP)

Im Allgemeinen sind die Systemanforderungen für die folgenden Produkte mit denen für die Betriebssysteme identisch, unter denen sie unterstützt werden.

> **NOTE**
> Eine ältere Version von Symantec Endpoint Protection Manager kann einen Client mit einer neueren Version möglicherweise nicht ordnungsgemäß verwalten. Probleme mit Content-Updates und Clientverwaltung können auftreten.Beispiel: Symantec Endpoint Protection Manager 14.0.1 oder früher kann einen Client der Version 14.2 mit seinen versionsspezifischen Monikern nicht korrekt bereitstellen. Symantec Endpoint Protection Manager für ältere Versionen als 14 MP2 kann Client-Versionen mit 14.0.1 oder höher nicht ordnungsgemäß mit ihren versionsspezifischen Monikern bereitstellen.

In den folgenden Tabellen werden die Software- und Hardwareanforderungen für Symantec Endpoint Protection beschrieben.

Table 5: Softwareanforderungen für Symantec Endpoint Protection Manager (SEPM)

Komponente	Anforderungen
Betriebssystem	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** Desktop-Betriebssysteme werden nicht unterstützt. **Note:** Windows Server Core Edition wird nicht unterstützt. Windows Server Core enthält Internet Explorer nicht, der zum Einsatz von Symantec Endpoint Protection Manager erforderlich ist.
Webbrowser	Die folgenden Browser werden für den Webkonsolenzugriff auf Symantec Endpoint Protection Manager und für das Anzeigen der Symantec Endpoint Protection Manager-Hilfe unterstützt: • Microsoft Edge Hinweis: Die 32-Bit-Version von Windows 10 unterstützt keinen Webkonsolenzugriff im Edge-Browser. • Microsoft Internet Explorer 11 • Mozilla Firefox 5.x bis 68.x • Google Chrome 75.x

Komponente	Anforderungen
Datenbank	**Symantec Endpoint Protection Manager enthält eine eingebettete Datenbank. Sie können auch eine Datenbank aus einer der folgenden Versionen von Microsoft SQL Server verwenden:** • 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 (ab 14.3) **Note:** Die SQL Server Express Edition-Datenbank wird nicht unterstützt.SQL Server-Datenbanken, die auf Amazon RDS gehostet werden, werden unterstützt (ab 14.0.1 MP2). **Note:** Wenn Symantec Endpoint Protection eine SQL Server-Datenbank verwendet und die Umgebung nur TLS 1.2 nutzt, vergewissern Sie sich, dass SQL Server TLS 1.2 unterstützt. Sie benötigen eventuell einen Patch für SQL Server. Diese Empfehlung gilt für SQL Server 2008, 2012 und 2014.Wenn das SQL Server-Patch für die Unterstützung von TLS 1.2 nicht installiert ist, kann es beim Aktualisieren von Symantec Endpoint Protection 12.1 auf 14 zu Problemen kommen. **Note:** Unterstützung für Microsoft SQL Server TLS 1.2
Andere Umgebungsbedingungen	Der IPv4-Stapel muss auch in reinen IPv6-Netzwerken installiert und dann deaktiviert werden. Wenn der IPv4-Stapel deinstalliert wird, funktioniert Symantec Endpoint Protection Manager nicht.

Table 6: Hardware-Anforderungen für Symantec Endpoint Protection Manager

Komponente	Anforderungen
Prozessor	Mindestens Intel Pentium Dual-Core oder Äquivalent, 8-Core oder besser empfohlen **Note:** Intel Itanium IA-64-Prozessoren werden nicht unterstützt.
Arbeitsspeicher	2 GB frei verfügbar; 8 GB werden empfohlen **Note:** Der Symantec Endpoint Protection Manager-Server kann zusätzlichen Arbeitsspeicher erfordern. Das hängt von den Arbeitsspeicheranforderungen anderer bereits installierter Anwendungen ab.Beispiel: Wenn Microsoft SQL Server auf dem Symantec Endpoint Protection Manager-Server installiert ist, sollten auf dem Server mindestens 8 GB verfügbar sein.
Anzeige	1.024 x 768 oder höher
Festplatte bei Installation auf dem Systemlaufwerk	**Mit einer integrierten oder lokalen SQL Server-Datenbank:** • 40 GB mindestens (200 GB empfohlen) für den Management-Server und Datenbank **Mit einer Remote-SQL Server-Datenbank:** • 40 GB mindestens (100 GB empfohlen) für den Management-Server • Zusätzlicher Speicherplatz auf dem Remote-Server für die Datenbank
Festplatte bei der Installation auf einem anderen Laufwerk	**Mit einer integrierten oder lokalen SQL Server-Datenbank:** • Auf dem Systemlaufwerk sind mindestens 15 GB erforderlich (100 GB empfohlen) • Auf dem Installationslaufwerk sind mindestens 25 GB erforderlich (100 GB empfohlen) **Mit einer Remote-SQL Server-Datenbank:** • Auf dem Systemlaufwerk sind mindestens 15 GB erforderlich (100 GB empfohlen) • Auf dem Installationslaufwerk sind mindestens 25 GB erforderlich (100 GB empfohlen) • Zusätzlicher Speicherplatz auf dem Remote-Server für die Datenbank

Wenn Sie eine SQL Server-Datenbank verwenden, müssen Sie möglicherweise mehr Speicherplatz zur Verfügung stellen. Die Menge und der Speicherort des zusätzlichen Speicherplatzes hängt davon ab, auf welchem Laufwerk SQL Server genutzt wird, den Wartungsanforderungen der Datenbank und anderen Datenbankeinstellungen.

Table 7: Systemanforderungen für den Symantec Endpoint Protection-Client für Windows

Komponente	Anforderungen
Betriebssystem (Desktop)	• Windows 7 (32 Bit, 64 Bit, RTM und SP1) • Windows Embedded 7 Standard, POSReady und Enterprise (32 und 64 Bit) • Windows 8 (32 Bit, 64 Bit) • Windows Embedded 8 Standard (32 und 64 Bit) • Windows 8.1 (32 und 64 Bit), einschließlich Windows To Go • Windows 8.1 Update (April 2014) (32 und 64 Bit) • Windows 8.1 Update (August 2014) (32 und 64 Bit) • Windows Embedded 8.1 Pro, Industry Pro und Industry Enterprise (32 und 64 Bit) • Windows 10 (Version 1507) (32 und 64 Bit), einschließlich Windows 10 Enterprise 2015 LTSB • Windows 10 November Update (Version 1511) (32 und 64 Bit) • Windows 10 Anniversary Update (Version 1607) (32 und 64 Bit), einschließlich Windows 10 Enterprise 2016 LTSB • Windows 10 Creator Update (Version 1703) (32 und 64 Bit) • Windows 10 Fall Creators Update (Version 1709) (32 und 64 Bit) • Windows 10 April 2018 Update (Version 1803) (32 und 64 Bit) • Windows 10 Oktober 2018 Update (Version 1809) (32 und 64 Bit), einschließlich Windows 10 Enterprise 2019 LTSB • Windows 10 Mai 2019 Update (Version 1903) (32 und 64 Bit) • Windows 10 November 2019 Update (Version 1909) (32 Bit und 64 Bit) (ab 14.2 RU1) • Windows 10 20H1 (Windows 10 Version 2004) (ab 14.3)
Betriebssystem (Server)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2 Update (April 2014) • Windows Server 2012 R2 Update (August 2014) • Windows Server 2016 • Windows Server 2019 • Windows Server, Version 1803 (Server Core) (ab 14.2) • Windows Server, Version 1809 (Server Core) • Windows Server, Version 1903 (Server Core) (ab 14.2 RU1) • Windows Server, Version 1909 (Server Core) (ab 14.2 RU1)
Browser-Angriffsschutz	Browser-Angriffsschutz-Unterstützung basiert auf der Version der Client-Intrusion Detection-System-Engine (CIDS). Weitere Informationen finden Sie unter Unterstützte Browser für den Browser-Angriffsschutz in Endpoint Protection.

Table 8: Hardware-Anforderungen für den Symantec Endpoint Protection-Client für Windows

Komponente	Anforderungen
Prozessor (für physische Computer)	• 32-Bit-Prozessor: 2 GHz Intel Pentium 4 oder gleichwertig (Intel Pentium 4 oder gleichwertig empfohlen) • 64-Bit-Prozessor: 2 GHz Pentium 4 mit x86-64-Unterstützung oder gleichwertig **Note:** Itanium-Prozessoren werden nicht unterstützt.
Prozessor (für virtuelle Computer)	Ein virtuelles Socket und ein Kern pro Socket mit mindestens 1 GHz (ein virtuelles Socket und zwei Kerne pro Socket mit 2 GHz empfohlen) **Note:** Die Ressourcenreservierung für Hypervisor muss aktiviert sein.
Arbeitsspeicher	1 GB (2 GB empfohlen) oder mehr, falls vom Betriebssystem erfordert
Anzeige	800 x 600 oder höher
Festplatte	Speicherplatzanforderungen hängen vom Typ des zu installierenden Client, dem Laufwerk und dem Speicherort des Programmdatenordners ab. Der Programmdatenordner befindet sich normalerweise auf dem Systemlaufwerk unter "C:\ProgramData". Auf dem Systemlaufwerk ist immer Speicherplatz erforderlich, unabhängig davon, auf welchem Laufwerk die Software installiert wird. **Anforderungen an die Festplatte:** • Client für Windows verfügbare Festplattensystem Voraussetzungen: Wenn auf dem Systemlaufwerk installiert, werden die Systemvoraussetzungen für das Festplattenlaufwerk beschrieben, wenn auf dem Systemlaufwerk installiert wird. Symantec Endpoint Protection Symantec Endpoint Protection • Anforderungen an die Festplatte, wenn Symantec Endpoint Protection auf einem anderen Laufwerk installiert wird beschreibt die Anforderungen an die Festplatte, wenn Symantec Endpoint Protection auf einem anderen Laufwerk installiert wird. **Note:** Platzbedarf basiert auf NTFS-Dateisystemen. Weitere Speicherplatz ist auch für Content-Updates und Protokolle erforderlich.

Table 9: Anforderungen an die Festplatte, wenn Symantec Endpoint Protection auf dem Systemlaufwerk installiert wird

Clienttyp	Anforderungen
Standard	**Programmdatenordner auf dem Systemlaufwerk:** • 395 MB* **Programmdatenordner auf einem anderen Laufwerk:** • Systemlaufwerk: 180 MB • Anderes Laufwerk: 350 MB
Eingebettet/VDI	**Programmdatenordner auf dem Systemlaufwerk:** • 245 MB* **Programmdatenordner auf einem anderen Laufwerk:** • Systemlaufwerk: 180 MB • Anderes Laufwerk: 200 MB
Dark Network	**Programmdatenordner auf dem Systemlaufwerk:** • 545 MB* **Programmdatenordner auf einem anderen Laufwerk:** • Systemlaufwerk: 180 MB • Anderes Laufwerk: 500 MB

* Weitere 135 MB sind während der Installation erforderlich.

Table 10: Anforderungen an die Festplatte, wenn Symantec Endpoint Protection auf einem anderen Laufwerk installiert wird.

Clienttyp	Anforderungen
Standard	**Programmdatenordner auf dem Systemlaufwerk:** • Systemlaufwerk: 380 MB • Anderes Laufwerk: 15 MB* **Programmdatenordner auf einem anderen Laufwerk:**** • Systemlaufwerk: 30 MB • Programmdatenlaufwerk: 350 MB • Anderes Laufwerk: 150 MB
Eingebettet/VDI	**Programmdatenordner auf dem Systemlaufwerk:** • Systemlaufwerk: 230 MB • Anderes Laufwerk: 15 MB* **Programmdatenordner auf einem anderen Laufwerk:**** • Systemlaufwerk: 30 MB • Programmdatenlaufwerk: 200 MB • Anderes Laufwerk: 150 MB
Dark Network	**Programmdatenordner auf dem Systemlaufwerk:** • Systemlaufwerk: 530 MB • Anderes Laufwerk: 15 MB* **Programmdatenordner auf einem anderen Laufwerk:**** • Systemlaufwerk: 30 MB • Programmdatenlaufwerk: 500 MB • Anderes Laufwerk: 150 MB

* Weitere 135 MB sind während der Installation erforderlich.

** Wenn sich der Programmdatenordner auf dem anderen Installationslaufwerk befindet, erweitern Sie den Speicherplatz auf dem Programmdatenlaufwerk um 15 MB. Zum Installieren sind 150 MB Speicherplatz auf dem anderen Installationslaufwerk erforderlich.

Table 11: Systemanforderungen für den Symantec Endpoint Protection-Client für Windows Embedded

Komponente	Anforderungen
Prozessor	Intel Pentium (1 GHz)
Arbeitsspeicher	256 MB **Note:** Diese Angabe ist für eine Installation des eingebetteten Symantec Endpoint Protection-Clients. Wenn Sie zusätzliche Funktionen einer integrierten Lösung wie EDR implementieren, ist mehr Arbeitsspeicher erforderlich.

Komponente	Anforderungen
Festplatte	Der eingebettete/VDI-Client von Symantec Endpoint Protection benötigt den folgenden freien Speicherplatz: • Bei der Installation auf dem Systemlaufwerk: 245 MB • Bei der Installation auf einem anderen Laufwerk: 230 MB auf dem Systemlaufwerk und 15 MB auf dem anderen Laufwerk Weitere 135 MB sind während der Installation erforderlich. Diese Zahlen gehen davon aus, dass sich der Programmdatenordner auf dem Systemlaufwerk befindet. Ausführliche Informationen sowie die Systemanforderungen für die anderen Clienttypen finden Sie unter "Systemanforderungen für den Symantec Endpoint Protection-Client für Windows".
Version von Windows Embedded	• Windows Embedded Standard 7 (32 und 64 Bit) • Windows Embedded POSReady 7 (32 und 64 Bit) • Windows Embedded Enterprise 7 (32 und 64 Bit) • Windows Embedded 8 Standard (32 und 64 Bit) • Windows Embedded 8.1 Industry Pro (32 und 64 Bit) • Windows Embedded 8.1 Industry Enterprise (32 und 64 Bit) • Windows Embedded 8.1 Pro (32 und 64 Bit)
Mindestens erforderliche Komponenten	• Filter-Manager (FltMgr.sys) • Performance Data Helper (pdh.dll) • Windows Installer-Dienst
Vorlagen	• Anwendungskompatibilität (Standard) • Digitale Beschilderung • Industrielle Automatisierung • IE, Media Player, RDP • Set-Top-Box • Thin Client Die minimale Konfigurationsvorlage wird nicht unterstützt. Der erweiterte Schreibfilter (EWF) und der vereinheitlichte Schreibfilter (UWF) werden nicht unterstützt. Der empfohlene Schreibfilter ist der dateibasierte (FBWF), der zusammen mit dem Registrierungs-Filter installiert wird.

Table 12: Systemanforderungen für den Symantec Endpoint Protection-Client für Mac

Komponente	Anforderungen
Prozessor	64 Bit Intel Core 2 Duo oder höher
Arbeitsspeicher	2 GB RAM
Festplatte	500 MB freier Speicherplatz für die Installation
Anzeige	800 x 600
Betriebssystem	• macOS 10.13 • macOS 10.14 • macOS 10.15 bis 10.15.5 macOS 10.14.5 und höher unterstützt die Anforderungen für kext-Beglaubigungen. Weitere Informationen finden Sie unter Endpoint Protection 14.2 RU1 und kext-Beglaubigung für macOS 10.14.5. Eine Liste der unterstützten Betriebssysteme für frühere Versionen finden Sie unter Mac-Kompatibilität mit dem Endpoint Protection-Client.

Table 13: Systemanforderungen für den Symantec Endpoint Protection-Client für Linux

Komponente	Anforderungen
Hardware	• Prozessor: Intel Pentium 4 (2 GHz) oder neuerer Prozessor • 1 GB RAM • 7 GB freier Festplattenspeicher
Betriebssysteme	• Amazon Linux • CentOS 6U3 – 6U9, 7 – 7U7, 8; 32 Bit und 64 Bit • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32 und 64 Bit • Fedora 16, 17; 32 und 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 und 64 Bit); 12, 12 SP1 - 12 SP3 (64 Bit) • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4 (32 und 64 Bit); 12 SP3 (64 Bit) • Ubuntu 12.04, 14.04, 16.04, 18.04 (ab 14.3); 32 Bit und 64 Bit Eine Liste der unterstützten Betriebssystemkernel für frühere Versionen finden Sie unter Von Symantec Endpoint Protection unterstützte Linux-Kernel.
Grafische Benutzeroberflächen	Sie können die folgenden grafischen Benutzeroberflächen für den Einsatz des Symantec Endpoint Protection-Client für Linux verwenden: • KDE • Gnome • Unity

Andere Umgebungsbedingungen	• Glibc
	Betriebssysteme, die glibc unter 2.6 ausführen, werden nicht unterstützt.
	• i686-basierte abhängige Pakete auf 64-Bit-Computern
	Viele der ausführbaren Dateien im Linux-Client sind 32-Bit-Programme. Bei 64-Bit-Computern müssen Sie vor der Installation des Linux-Client die i686-basierten abhängigen Pakete installieren.
	Wenn Sie die i686-basierten abhängigen Pakete nicht bereits installiert haben, können Sie sie über die Befehlszeile installieren. Für diese Installation sind Super-User-Rechte erforderlich. Beispiel für Befehle mit `sudo`:
	– Red Hat-Distributionen: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Debian-Distributionen: `sudo apt-get install ia32-libs`
	– Ubuntu-Distributionen:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`
	• net-tools oder iproute2
	Symantec Endpoint Protection verwendet eines dieser beiden Tools, abhängig davon, was bereits auf dem Computer installiert ist.
	• Tools für Programmierer
	Zum automatischen und manuellen Kompilieren des Auto-Protect-Kernelmoduls müssen bestimmte Tools installiert werden. Erforderlich sind gcc sowie die Kernel-Quellcode- und Header-Dateien. Ausführliche Anweisungen zum Installieren unter bestimmten Linux-Versionen finden Sie unter:
	Manuelles Kompilieren der Auto-Protect-Kernelmodule für Endpoint Protection für Linux

Versionshinweise und Systemanforderungen für alle Versionen von Symantec Endpoint Protection

Unterstützte Aktualisierungspfade auf die neueste Version von Symantec Endpoint Protection 14.x

NOTE

Im Allgemeinen wird jeweils die vorherige Version von Symantec Endpoint Protection in der Liste unterstützt. Jedoch sollten Sie dies bestätigen, indem Sie die Versionshinweise für die installierte Version prüfen.

Versionshinweise, neue Fehlerbehebungen und Systemanforderungen für alle Versionen von Endpoint Protection

Symantec Endpoint Protection Manager und Windows-Client

Die folgenden Versionen von Symantec Endpoint Protection Manager und des Symantec Endpoint Protection-Windows-Client können direkt auf die neueste Version aktualisiert werden:

- 11.x und Small Business Edition 12.0 (nur Symantec Endpoint Protection-Clients für unterstützte Betriebssysteme)
- 12.1.x, bis 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

macOS-Client

Die folgenden Versionen des Symantec Endpoint Protection-Client für Mac können direkt auf die aktuelle Version aktualisiert werden:

- 12.1.4 - 12.1.6 MP9
  Der macOS-Client wurde für Version 12.1.6 MP10 nicht aktualisiert.
- 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

Der Symantec Endpoint Protection-Client für Mac wurde für 14.0.1 MP2 nicht aktualisiert.

Linux-Client

Die folgenden Versionen des Symantec Endpoint Protection-Client für Linux können direkt auf die neueste Version aktualisiert werden:

- 12.1.x, bis 12.1.6 MP9
  Der Linux-Client wurde für Version 12.1.6 MP10 nicht aktualisiert.
- 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 für Linux 1.0.14 ist die einzige Version, die Sie direkt auf Symantec Endpoint Protection migrieren können. Sie müssen zuerst alle anderen Versionen von Symantec AntiVirus für Linux deinstallieren. Sie können verwaltete Clients nicht auf einen nicht verwalteten Client migrieren.

Nicht unterstützte Aktualisierungspfade

Das Migrieren auf Symantec Endpoint Protection ist nicht aus allen Symantec-Produkten möglich. Sie müssen die folgenden Produkte deinstallieren, bevor Sie den Symantec Endpoint Protection-Client installieren:

- Die nicht unterstützten Symantec-Produkte "Symantec AntiVirus" und "Symantec Client Security"
- Alle Symantec Norton™ Produkte
- Symantec Endpoint Protection für Windows XP Embedded 5.1
- Versionen von Symantec Endpoint Protection für Mac unter 12.1.4

Das direkte Aktualisieren von Symantec Endpoint Protection Manager 11.0.x oder Symantec Endpoint Protection Manager Small Business Edition 12.0.x auf Symantec Endpoint Protection Manager 14 ist nicht möglich. Sie müssen diese Versionen zuerst deinstallieren oder auf Version 12.1.x aktualisieren, bevor Sie auf Version 14.x aktualisieren.

Das Aktualisieren von Symantec Endpoint Protection Manager 12.1.6 MP7 auf Version 14 ist nicht möglich, da die Version des Datenbankschemas in 12.1.6 MP7 höher ist als in 14. Stattdessen müssen Sie 12.1.6 MP7 auf 14 MP1 oder höher aktualisieren.

Das Aktualisieren von 14 MP1 (14.0.2332.0100) auf 14 MP1 Refresh Build (14.0.2349.0100) wird nicht unterstützt.

Downgrade-Pfade werden nicht unterstützt. Beispiel: Wenn Sie aus Symantec Endpoint Protection 14.2.1.1 auf 12.1.6 MP10 aktualisieren, müssen Sie zuerst Symantec Endpoint Protection 14.2.1.1 deinstallieren.

Sie finden die Build-Nummern und die relevanten Versionen hier:

- Veröffentlichte Versionen von Symantec Endpoint Protection
- Info zu den verschiedenen Versionen von Endpoint Protection

Weitere Informationsquellen

Unter Informationen zu Endpoint Protection werden die Websites aufgeführt, auf der Sie Informationen zu Best Practices und Fehlerbehebung sowie andere Ressourcen zum Einsatz des Produkts finden.

Table 14: Website-Informationen zu Endpoint Protection

Art der Informationen	Link zur Website
Testversionen	Wenden Sie sich an Ihren Kundenbetreuer.
Aktualisierte Handbücher und Dokumentation	• Produkthandbücher für die neueste Version (Englisch) • Produkthandbücher für die neueste Version (andere Sprachen) • Produkthandbücher für alle Versionen von Symantec Endpoint Protection 14.x (Englisch) **Andere Sprachen:**
Technischer Support	Technischer Support für Endpoint Protection Schließt Supportdatenbankartikel, Produktversionsdetails, Updates und Patches sowie Kontaktoptionen für den Support ein.
Bedrohungsinformationen und -Updates	Symantec Security Center
Schulung	Education Services Greifen Sie auf Schulungen, die eLibrary und mehr zu.
Symantec Connect-Foren	Endpoint Protection


Symantec
A Division of Broadcom