Versionshinweise zu Symantec™ Endpoint Protection 14.3 RU1

Aktualisiert: Dezember 2020

Table of Contents

Copyright-Erklärung

Neuheiten bei Symantec Endpoint Protection 14.3 RU1

In diesem Abschnitt werden die neuen Funktionen dieser Version beschrieben.

Schutzfunktionen

- Die neuen Agents Symantec Mac Agent und Symantec Linux Agent können entweder über den lokalen Symantec Endpoint Protection Manager oder die Integrated Cyber Defense Manager-Cloud-Konsole installiert und verwaltet werden.
  Installieren des Symantec Endpoint Protection-Clients für Mac
  Installieren des Symantec-Agent für Linux 14.3 RU1
- Verhindert neue und unbekannte Bedrohungen auf macOS durch die Überwachung von fast 1.400 Dateiverhaltensweisen in Echtzeit. Der neue Mac-Agent enthält diese Verhaltensschutzfunktionen. Der Verhaltensschutz (SONAR) nutzt künstliche Intelligenz und Advanced Machine Learning für Zero-Day-Schutz, um neue Bedrohungen effektiv zu stoppen.
  Verwalten von SONAR
- Blockiert nicht vertrauenswürdige, nicht portable ausführbare Dateien (PE) wie PDF-Dateien und Skripte, die noch nicht als Bedrohung identifiziert werden. Klicken Sie in der Ausnahmerichtlinie auf **Windows-Ausnahmen** > **Dateizugriff**.
- Verhindert Webbedrohungen basierend auf der Reputationswertung einer Webseite. Die Angriffsschutzrichtlinie enthält URL-Reputationsfilterung, die Webseiten mit Reputationswerten unter einem bestimmten Schwellenwert blockiert. Die Reputationsbewertungen reichen von -10 (schlecht) bis +10 (gut). Die Option **URL-Reputation aktivieren** ist standardmäßig aktiviert.
- Sie können erzwingen, dass Symantec Endpoint Protection sich eine Anwendung basierend auf dem Hash-Wert der Anwendung merkt. Klicken Sie in der Ausnahmerichtlinie auf **Windows-Ausnahmen** > **Anwendung** > **Anwendung nach Fingerabdruck hinzufügen**.
- Schützt Endgeräte und Benutzer vor webbasierten Angriffen auf bösartige Websites mit der Funktion "Umleitung des Netzwerkdatenverkehrs". Die Funktion "Umleitung des Netzwerkdatenverkehrs" leitet den gesamten Netzwerkverkehr (beliebiger Port) oder nur webbasierten Datenverkehr (Ports 80 und 443) an den Symantec Web Security Service um, der Netzwerkverkehr und SaaS-Anwendungszugriff abhängig von der Unternehmensrichtlinie zulässt oder blockiert. Für die Umleitung des Netzwerkdatenverkehrs gibt es eine neue Umleitungsmethode namens "Tunnelmethode". Mit der Tunnelmethode wird der gesamte Internetverkehr an den Symantec Web Security Service (WSS) weitergeleitet. Dort wird der Verkehr anhand der Richtlinien für den Symantec WSS entweder zugelassen oder blockiert. Die Tunnelmethode gilt als Beta-Funktion. Sie sollten dafür gründliche Tests mit Ihren Anwendungen für Ihre WSS-Richtlinien durchführen. Broadcom bietet eine Beta-Website mit einem Testleitfaden und der Möglichkeit, Feedback zu hinterlassen. Melden Sie sich mit Ihren Broadcom-Zugangsdaten auf der folgenden Website an:
  Validate.broadcom.com
  Konfigurieren von Network Traffic Redirection
- Die Integrationsrichtlinie wurde in "Richtlinie für Network Traffic Redirection" umbenannt.
- Unterstützt MITRE-angereicherte Ereignisse in Symantec EDR. Diese Verbesserung ermöglicht es Ihnen, das MITRE ATT&CK-Framework zu verwenden, um Kontext für Vorgänge in Ihrer Umgebung zu erhalten.
- Unterstützung für die folgenden Symantec EDR-Ereignisse, die mehr Einblick in die Endgeräte erlauben:
  – AMSI-Ereignisse bieten Einblick in Angriffsmethoden, die herkömmliche Abfragemethoden für Befehlszeilen umgehen können.
  – ETW-Ereignisse bieten Einblick in Ereignisse auf verwalteten Windows-Endgeräten.
- Sie können Windows Defender und Symantec Endpoint Protection auf demselben Computer ausführen. Der Auto-Protect-Scan wird nach Windows Defender ausgeführt und kann alle Bedrohungen erkennen, die Windows Defender nicht erkannt hat. Die Option **Kann mit Windows Defender zusammen verwendet werden** stellt sicher, dass Auto-

Protect ausgeführt wird, wenn Microsoft Defender deaktiviert ist. Zum Deaktivieren der Option klicken Sie auf die Richtlinie für Viren- und Spyware-Schutz und auf die Registerkarte **Verschiedenes** > **Verschiedenes**.

- Die Angriffskettenverhinderung wird jetzt für hybrid-verwaltete Clients unterstützt.

Symantec Endpoint Protection Manager

- Die eingebettete Datenbank wurde auf die Microsoft SQL Express-Datenbank aktualisiert. Die SQL Server Express-Datenbank speichert Richtlinien und Sicherheitsereignisse effizienter als die eingebettete Standarddatenbank und wird automatisch mit Symantec Endpoint Protection Manager installiert.
  Best Practices für das Upgrade von der eingebetteten Datenbank auf die Microsoft SQL Server Express-Datenbank
- Während der Installation oder des Upgrades von Symantec Endpoint Protection Manager führt der Management-Server-Konfigurationsassistent Folgendes durch:
  - Installiert LiveUpdate-Content automatisch.
  - Stellt eine Option zur Verwendung eines TLS-Zertifikats für die sichere Kommunikation zwischen SQL Server und dem Symantec Endpoint Protection Manager bereit.
- LiveUpdate nutzt eine neue Engine in Symantec Endpoint Protection Manager, die für die Ausführung auf der Cloud-Konsole optimiert ist.
  Versionshinweise und neue Fixes für LiveUpdate Administrator
- Die Option **Vorhandene Sicherheitssoftware anderer Hersteller automatisch deinstallieren**, die in 14.3 MP1 nicht verfügbar war, ist in 14.3 RU1 in einer aktualisierten Version wieder verfügbar. Diese Option wird verwendet, um Sicherheitssoftware von Drittanbietern zu deinstallieren. Klicken Sie zum Aufrufen dieser Option auf die Seite **Admin** > **Pakete** > **Einstellungen für Clientinstallationen**.
  Entfernen der Sicherheitssoftware von Drittanbietern in Endpoint Protection 14
  Entfernen von Sicherheitssoftware von Drittanbietern in Endpoint Protection 14.3 RU1
- Der Client-Bereitstellungsassistent, der zum Bereitstellen von Clientpaketen verwendet wird, muss über verifizierte Zugangsdaten verfügen und eine Verbindung zum Symantec Endpoint Protection Manager herstellen können. Wenn die Überprüfung fehlschlägt, wird der Client-Bereitstellungsprozess angehalten, um zu verhindern, dass Active Directory-Benutzerkonten gesperrt werden.
  Installieren von Symantec Endpoint Protection-Clients mit Remote-Push
- Über die Computerstatus-Protokolle und -Berichte können Sie jetzt einen Bereich für die Felder **Client-Version** und **IPS-Version** auswählen. Der Filter **Produktversion** wurde in **Client-Version** umbenannt.
- Die Option **Taskleistensymbol deaktivieren** ist für Clients verfügbar, die auf einem Terminalserver ausgeführt werden und zu einer hohen CPU-Auslastung und Speicherauslastung führen. Sie können nun das Symbol für den Benachrichtigungsbereich (auch als Taskleistensymbol bezeichnet) deaktivieren, um zu verhindern, dass mehrere Instanzen von Benutzersitzungsprozessen (wie SmcGui.exe und ccSvcHost.exe) ausgeführt werden. Sie aktivieren diese Option über die Registerkarten **Clients** > **Richtlinien** > **Sicherheitseinstellungen** > **Allgemein**.
- Der Positivlistenmodus und Blacklist-Modus wurden entsprechend der Zulassen- und Blockierungsfunktionen aktualisiert. Auf der Seite **Clients** auf der Registerkarte **Richtlinien** im Dialogfeld **Systemsperre** haben sich die Listen der Anwendungsdateien von **Positivlistenmodus** und **Blacklist-Modus** zu **Zulassungsmodus** und **Verweigerungsmodus** geändert.
- Auf der Seite **Admin** auf der Registerkarte **Server** > **Externe Protokollierung konfigurieren** > **Allgemein** hat sich die Option **Master-Protokollierungs-Server** zu **Primärer Protokollierungs-Server** geändert.
- Der Protokolltyp **System** > das Protokoll **Administrativ** und das Protokoll **Prüfung** listet den Computernamen auf.
- Client-Firewall-Protokolle werden erfasst, damit Sie weniger Benachrichtigungen in der Cloud-Konsole erhalten.
- Oracle Java SE wurde durch OpenJDK ersetzt.
- Die Drittanbieterkomponenten von JQuery wurden auf eine neuere Version aktualisiert.

Client- und Plattform-Updates

- Der Windows-Client unterstützt Windows 10 20H2 (Windows 10-Version 2009).
- Der Mac-Client unterstützt macOS 10.15.7.
- Die veralteten Mac-Clientinstallationspakete wurden in den Ordner "Additional Packages" verschoben.

Entfernte Funktionen

- Die Optionen **Risikoschweregrad** und **Risikoverteilung nach Schweregrad** wurden aus Benachrichtigungen und Berichten entfernt.
- Die Registerkarte **CASMA** und der Befehl **Analysieren** wurden entfernt, da diese Funktion in 14.3 nicht mehr unterstützt wird.
- Der Mac-Client unterstützt macOS 10.13 nicht mehr.

Dokumentation

Die Symantec Endpoint Protection Manager-Hilfe finden Sie jetzt online: Symantec Endpoint Protection – Installations- und Administratorhandbuch

Datenbankschema

Das Datenbankschema umfasst die folgenden Änderungen.

Tabelle	Spaltenänderung
ALERTS	Die Spalte ENRICHED_DATA wurde hinzugefügt.
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	Die folgenden Spalten wurden aus jeder Tabelle entfernt: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Tabelle	Spaltenänderung
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	• Die Spalte CONTENT wurde vom Typ "image" zu "varbinary" geändert. • Die indizierte Spalte FILESTREAM_ID wurde hinzugefügt. • Der Index FILESTREAM_ID wurde hinzugefügt. • Folgende Spalten wurden entfernt: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
INVENTORYREPORT	Die folgenden Spalten wurden hinzugefügt: • PRODUCTVERSIONFROM • PRODUCTVERSIONTO • IDS_VERSIONFROM • IDS_VERSIONTO
SEM_AGENT	• Die Spalte NTR_MESSAGE wurde hinzugefügt. • Folgende Spalten wurden entfernt: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
SEM_AGENT_VERSION	Die folgenden Spalten wurden hinzugefügt: • VERSION • FORMATTED_VERSION • REFRESH_USN • AGENT_VERSION_FORMAT_REFRESH • VERSION1 • VERSION2 • VERSION3 • VERSION4
SEM_SVA	Folgende Spalten wurden entfernt: • RESERVED_INT1 • RESERVED_INT2 • RESERVED_BIGINT1 • RESERVED_BIGINT2 • RESERVED_CHAR1 • RESERVED_CHAR2 • RESERVED_VARCHAR1
V_ALERTS	Die Spalte ENRICHED_DATA wurde hinzugefügt.

Neue Funktionen in allen Versionen von Symantec Endpoint Protection

Bekannte Probleme und Problemumgehungen für Symantec Endpoint Protection

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

Table 1: Probleme mit Upgrades

Problem	Beschreibung und Lösung
Ein Symantec Endpoint Protection Manager in einem Dark Network lädt alten CIDS-Content (Client Intrusion Detection System) auf neue Clients herunter, weil LiveUpdate während eines Upgrades [14.3 RU1] nicht ausgeführt wird.	Wenn ein Symantec Endpoint Protection Manager 14.3 RU1 weder auf das Internet noch auf einen LUA-Server (LiveUpdate Administrator) zugreifen kann, wird alter und inkompatibler Content im Cache behalten. Dieser alte Content wird normalerweise für die neuen Clients bereitgestellt. Um den Content im Cache des Management-Servers zu aktualisieren, laden Sie die zertifizierten Virendefinitionen und .jdb-Dateien des CIDS manuell herunter. [SEP-69125] Um sicherzustellen, dass die neuen Clients keinen alten Content erhalten, installieren Sie manuell eine .jdb-Datei des CIDS auf SEPM, bevor Sie neue Clients installieren oder alte Clients aktualisieren. Herunterladen von JDB-Dateien zum Aktualisieren von Definitionen für Endpoint Protection Manager
Einloggen bei Symantec Endpoint Protection Manager (SEPM) nicht möglich, wenn die Netzwerk-Schnittstellenkarte deaktiviert ist [14.3 RU1]	Nach der Installation von Symantec Endpoint Protection Manager können Sie sich nicht in der Konsole einloggen, und die folgende Fehlermeldung wird angezeigt: `Unerwarteter Server-Fehler` Dieses Problem kann auftreten, wenn zum Zeitpunkt der SEPM-Installation die Netzwerk-Schnittstellenkarte des Computers deaktiviert ist. Dies führt dazu, dass das Serverzertifikat nicht generiert wird. [SEP-67040] Prüfen Sie das Serverzertifikat, wenn Sie herausfinden möchten, ob SEPM mit einer deaktivierten Netzwerk-Schnittstellenkarte installiert wurde. Weitere Informationen finden Sie unter: SEPM install will fail if no network connections are available (Die SEPM-Installation schlägt fehl, wenn keine Netzwerkverbindungen verfügbar sind).
Wenn Sie SEPM deinstallieren und die Option verwenden, um die Standarddatenbank zu entfernen und die SQL Server Express-Instanz zu verlassen, wird der folgende Fehler angezeigt: "`Beim Herstellen der Verbindung zum Datenbankserver ist ein Fehler aufgetreten`".	Wenn Sie den Symantec Endpoint Protection Manager deinstallieren und die Option **Nur die Datenbank entfernen und die mit SEPM installierte SQL Server Express-Instanz beibehalten** auswählen, wird möglicherweise folgender Fehler angezeigt: "`Beim Herstellen der Verbindung zum Datenbankserver ist ein Fehler aufgetreten`". Dieses Problem tritt auf, nachdem Sie die Anmeldeinformationen für den Standardbenutzer-DBA hinzugefügt haben, und kann sich auf Benutzerrechte beziehen. [SEP-68670] Um dieses Problem zu umgehen, führen Sie die Deinstallation durch, indem Sie die SEPM-Datei setup.exe ausführen, und klicken Sie bei der Deinstallation auf die Option **Nur die Datenbank entfernen und die mit SEPM installierte SQL Server Express-Instanz beibehalten**.

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
Einige EDR-Ereignisse werden nicht auf dem Client [14.3 RU1] angezeigt	Der Symantec Endpoint Protection-Client muss Windows 10 Build 14393 oder höher ausführen, um Symantec EDR Event Tracing für Windows (ETW)-Ereignisse zu erfassen. [SEP-67175]
Die Funktion zur Network Traffic Redirection hat einige Einschränkungen [14.3 RU1]	• Der Symantec Web Security Service wird unter IPv4 und nicht IPv6 bereitgestellt. [SEP-68700] • Die Umleitung per Tunnel: – Kann nur auf Windows 10 64-Bit-Version 1703 und höher ausgeführt werden (halbjährlicher Wartungskanal) Diese Methode unterstützt keine anderen Windows-Betriebssysteme oder den Mac-Client. [SEP-67927] – Unterstützt keine HVCI-fähigen Geräte unter Windows 10 (64 Bit). [SEP-67648] – Leitet ausgehenden Datenverkehr vom Symantec Endpoint Protection-Client zum WSS um, bevor er durch die Firewall des Clients oder die Regeln zur URL-Reputation ausgewertet wird. Stattdessen wird der Datenverkehr anhand der WSS-Firewall und der URL-Regeln ausgewertet. Beispiel: Wenn eine SEP-Client-Firewall-Regel google.com blockiert und eine WSS-Regel google.com zulässt, ermöglicht der Client Benutzern den Zugriff auf google.com. Eingehender lokaler Datenverkehr zum Client wird weiterhin von der Symantec Endpoint Protection-Firewall verarbeitet. [SEP-67488] – Das WSS Captive Portal ist nicht für die Tunnel-Methode verfügbar, und der Client ignoriert die Abfrage der Zugangsdaten. In einer zukünftigen Version ersetzt die SAML-Authentifizierung im WSS-Agent das Captive Portal und ist im Symantec Endpoint Protection-Client verfügbar. – Wenn ein Clientcomputer mithilfe der Tunnel-Methode eine Verbindung zum WSS herstellt und virtuelle Computer hostet, muss jeder Gastbenutzer das im WSS-Portal bereitgestellte SSL-Zertifikat installieren. – Datenverkehr für ein lokales Netzwerk wie Ihr Startverzeichnis oder die Active Directory-Authentifizierung wird nicht umgeleitet. Die Tunnelmethode wird derzeit als Beta-Funktion betrachtet.
Doppelte Agent-Anmeldeeinträge nach dem Upgrade von 14.2.x auf 14.3 MP1 und höher [14.3 RU1]	Beim Aktualisieren von Symantec Endpoint Protection-Clients von 14.2.x auf 14.3 MP1 und höher werden doppelte Agent-Anmeldeeinträge für diese Clients auf der Seite **Geräte** in Symantec Endpoint Protection Manager erstellt. Es gibt keine funktionellen Auswirkungen und Sie können weiterhin mit den neuen Einträgen für Clients der Version 14.3 RU1 arbeiten. Symantec Endpoint Protection Manager entfernt ältere Agent-Einträge.
URLs in Symantec Endpoint Security zulassen, wenn Sie die Option für Hybrid-Management, Proxy-Server oder eine Perimeter-Firewall [14.3] verwenden	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. Sie lassen die URLs entweder in vollständig Cloud-verwalteten oder hybrid verwalteten Agents sowie in Ihrem Proxy-Server und/oder in der Perimeter-Firewall zu. Weitere Informationen finden Sie unter: URLs, die SEP und SES das Verbinden mit Symantec-Servern erlauben Weitere Informationen finden Sie unter Aktualisieren von Cloud-verwalteten Symantec-Agenten auf Version 14.2 RU2 MP1 oder höher.

Problem	Beschreibung und Lösung
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."
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.
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
Falsche Meldungen im Installationsprotokoll des Symantec-Agents für Linux. [14.3 RU1]	In einigen Fällen protokolliert das Agent-Installationsprogramm falsche Meldungen zu einer nicht übereinstimmenden Treiberversion oder einem erforderlichen Neustart. Diese Meldungen wirken sich nicht auf die Funktionalität des Agent aus.
Auf einem SuSe Linux-Gerät entfernt zypper die SEP Linux-Clientpakete, während das Paket "at" entfernt wird. [14.3 RU1]	Auf einem SuSe Linux-Gerät entfernt der Befehl "zypper remove at" die SEP Linux-Clientpakete, da das "at"-Paket als erforderliches abhängiges Paket hinzugefügt wird und die zypper-Befehle automatisch versuchen, die SEP-Clientpakete "sdcss-kmod" und "sdcss-sepagent" als Pakete mit nicht genutzten Abhängigkeiten zu entfernen. **Problemumgehung:** Um das "at"-Paket zu entfernen, führen Sie den folgenden Befehl aus: rpm -e --nodeps at

Problem	Beschreibung und Lösung
Upgrade-Problem unter macOS 10.15 und höher [14.3 MP1]	Unter macOS 10.15 und höher aktualisiert die Funktion **Symantec Endpoint Protection auf Remote-Computern installieren** im Clientbereitstellungsassistenten den Symantec Endpoint Protection-Client nicht von älteren Versionen auf Version 14.3 MP1. **Problemumgehung:** Verwenden Sie das **automatische Upgrade von Symantec Endpoint Protection Manager**, um das Upgrade des Symantec Endpoint Protection-Client unter macOS 10.15 und höher durchzuführen.
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.
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 RU1

Neue Fehlerbehebungen und Komponenten für Symantec Endpoint Protection 14.3 MP1

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 für 14.2x und frühere Versionen nicht unterstützt.
Webbrowser	Die folgenden Browser werden für den Webkonsolenzugriff auf Symantec Endpoint Protection Manager und für das Anzeigen der Symantec Endpoint Protection Manager-Hilfe unterstützt: • Chromium-basierter Edge-Browser von Microsoft (ab 14.3) • Microsoft Edge Hinweis: Die 32-Bit-Version von Windows 10 unterstützt keinen Webkonsolenzugriff im Edge-Browser. • Microsoft Internet Explorer 11 (14.2.x und früher) • Mozilla Firefox 5.x bis 83 • Google Chrome 87

Komponente	Anforderungen
Datenbank	Symantec Endpoint Protection Manager enthält eine Standarddatenbank: • Microsoft SQL Server Express 2014 (für Windows Server 2008 R2) • Microsoft SQL Server Express 2017 • Eingebettete Sybase-Datenbank (nur bis 14.3 MP.x) 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 (14.3 und höher) **Note:** 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. Ist das SQL Server-Patch für die Unterstützung von TLS 1.2 nicht installiert, kann es beim Aktualisieren aus 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 sind.
Anzeige	1.024 x 768 oder höher
Festplatte bei Installation auf dem Systemlaufwerk	Mit einer 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

Komponente	Anforderungen
Festplatte bei der Installation auf einem anderen Laufwerk	Mit einer 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
Andere	Eine aktivierte Netzwerk-Schnittstellenkarte

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 Bit, 64 Bit), inkl. 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) • Windows 10 20H2 (Windows 10 Version 2009) (ab 14.3 RU1)
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) • Windows Server, Version 2004 • Windows Server, Version 20H2 (14.3 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. **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.
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".

Komponente	Anforderungen
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	1 GB freier Speicherplatz für die Installation
Anzeige	800 x 600
Betriebssystem	• macOS 10.14 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. • macOS 10.15 bis 10.15.7 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 • 500 MB RAM • 2 GB verfügbarer Speicherplatz, wenn /var, /opt und /tmp das gleiche Dateisystem bzw. den gleichen Datenträger verwenden • 500 MB verfügbarer Speicherplatz in jedem /var, /opt und /tmp, wenn diese auf verschiedenen Datenträgern sind
Betriebssysteme	Unterstützte Betriebssysteme ab Version 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 Unterstützte Betriebssysteme für Versionen bis 14.3: • 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 Betriebssystem-Kernels für frühere Versionen finden Sie unter List of Linux Distributions and Kernels with Precompiled Auto-Protect Drivers/Modules for Symantec Endpoint Protection for Linux 14.x.
Grafische Benutzeroberflächen	Sie können die folgenden grafischen Benutzeroberflächen für den Einsatz des Symantec Endpoint Protection-Client für Linux verwenden: • KDE • Gnome • Unity Symantec-Agent für Linux 14.3 RU1 verfügt über keine grafische Benutzeroberfläche.

Komponente	Anforderungen

Andere Umgebungsanforderungen (bis 14.3 MP1)	• Glibc
	Betriebssysteme, die glibc unter 2.6 ausführen, werden nicht unterstützt.
	• net-tools oder iproute2
	Symantec Endpoint Protection verwendet eines dieser beiden Tools, abhängig davon, was bereits auf dem Computer installiert ist.
	• OpenSSL 1.0.2k-FIPS oder höher
	• 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
	• 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`

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

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

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 Endpoint Security und alle Versionen von Endpoint Protection

Unterstützte Aktualisierungspfade

- Symantec Endpoint Protection Manager Version 12.1.6 MP10 und höher mit der integrierten Datenbank kann nahtlos auf die Microsoft SQL Server Express-Datenbank Version 14.3 RU1 aktualisiert werden. Aktualisierungen von 12.1.6 MP9 und früher auf 14.3 RU1 werden blockiert.
- Symantec Endpoint Protection Manager 14.x lässt sich nahtlos über 12.1.x aktualisieren, es sei denn, der Support wurde eingestellt, wie z. B. für Windows Server 2003, Desktop-Betriebssysteme und 32-Bit-Betriebssysteme sowie einige Versionen von SQL Server.
- Der Symantec Endpoint Protection 14.x-Client lässt sich nahtlos über alle 12.1- und 11-Clientversionen aktualisieren, die auf unterstützten Betriebssystemen installiert sind. Die Ausnahme ist der Mac-Client bis zur Version 12.1.4, den Sie auf 12.1.4 oder höher aktualisieren oder deinstallieren müssen.

Hinweise zur Migration von Symantec Endpoint Protection 14

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
- 14.3, 14.3 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 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

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

Linux-Client

NOTE
Symantec-Agent für Linux 14.3 RU1 erkennt und deinstalliert den älteren Symantec Endpoint Protection-Client für Linux und führt dann eine neue Installation aus. Alte Konfigurationen werden nicht beibehalten.

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
- 14.3, 14.3 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:

- Symantec AntiVirus und Symantec Client Security, die nicht unterstützt werden.
- Alle Norton-Produkte
- Symantec Endpoint Protection für Windows XP Embedded 5.1
- Alle Symantec Endpoint Protection für Mac-Clients, die älter als 12.1.4 sind. Sie können auch auf 12.1.4 oder eine höhere Version aktualisieren.

Hinweise:

- Die Migration von Symantec Endpoint Protection-Clients mit einer älteren Version als 12.1.x wird nicht unterstützt.
- Das direkte Aktualisieren von Symantec Endpoint Protection Manager 11.0.x oder Symantec Endpoint Protection Manager Small Business Edition 12.0.x auf eine Version von Symantec Endpoint Protection Manager 14 ist nicht möglich. Sie müssen diese Versionen zuerst deinstallieren oder auf Version 12.1.x aktualisieren, bevor Sie auf die aktuellste Version von 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.
- Die Unterstützung von Windows XP, Server 2003 und Windows Embedded basierend auf Windows XP wurde in 14.0.x eingestellt. Symantec Endpoint Protection Manager 14.2 RU1 kann diese Computer als veraltete 12.1.x-Clients verwalten, obwohl 12.1.x-Clients nicht mehr unterstützt werden. Für diese Clients sollten Sie ein Produkt von Symantec verwenden, das noch diese veralteten Betriebssysteme unterstützt, wie zum Beispiel Data Center Security (DCS).
- 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 Symantec Endpoint Protection 14.2.1.1 auf 12.1.6 MP10 aktualisieren, müssen Sie zuerst Symantec Endpoint Protection 14.2.1 deinstallieren.
- Sie finden die Build-Nummern und die relevanten Versionen hier:

Info zu den verschiedenen Versionen von Endpoint Protection

Weitere Informationsquellen

Folgende Tabelle zeigt die Website an, auf der Sie Informationen zu Best Practices, Fehlerbehebung und 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)
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