

Versionshinweise zu Symantec™ Endpoint Protection 12.1.6 MP10

Symantec Endpoint Protection – Versionshinweise

Produktversion: 12.1.6 MP10

Dokumentationsversion: 1

Dieses Dokument wurde zuletzt aktualisiert am: April 06, 2018

Rechtlicher Hinweis

Copyright © 2018 Symantec Corporation. Alle Rechte vorbehalten.

Symantec, das Symantec-Logo, das Checkmark-Logo, LiveUpdate sowie Norton sind Marken oder eingetragene Marken der Symantec Corporation oder ihrer verbundenen Unternehmen in den USA und anderen Ländern. Andere Namen sind möglicherweise Marken ihrer Inhaber.

Das in diesem Dokument beschriebene Produkt wird unter Lizenzen bereitgestellt, die seine Nutzung, Vervielfältigung, Verteilung und Dekompilierung/Reverse Engineering einschränken. Kein Teil dieses Dokuments darf ohne vorherige schriftliche Zustimmung von Symantec Corporation und ihrer Lizenzgeber, sofern vorhanden, in irgendeiner Form reproduziert werden.

DIE DOKUMENTATION WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN VORAUSSETZUNGEN, DARSTELLUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHT-BEEINTRÄCHTIGUNG, SIND AUSGESCHLOSSEN, AUSSER IN DEM UMFANG, IN DEM SOLCHE HAFTUNGS AUSSCHLÜSSE ALS NICHT RECHTSGÜLTIG ANGESEHEN WERDEN. SYMANTEC CORPORATION IST NICHT FÜR BEILÄUFIG ENTSTANDENE SCHÄDEN ODER FÜR FOLGESCHÄDEN VERANTWORTLICH, DIE IN VERBINDUNG MIT DER BEREITSTELLUNG, LEISTUNG ODER DER VERWENDUNG DIESER DOKUMENTATION STEHEN. DIE IN DIESER DOKUMENTATION ENTHALTENEN INFORMATIONEN KÖNNEN JEDERZEIT OHNE ANKÜNDIGUNG GEÄNDERT WERDEN.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043, USA

<http://www.symantec.de>

Technischer Support

Der technische Support von Symantec betreibt Supportcenter in aller Welt. Hauptaufgabe des technischen Supports ist es, auf Anfragen zu Produktmerkmalen und Funktionalität zu reagieren. Die Gruppe "Technischer Support" erstellt auch Inhalt für unsere Online-Supportdatenbank. Die Gruppe "Technischer Support" arbeitet kooperativ mit den anderen Funktionsbereichen innerhalb Symantec, um Ihre Fragen rechtzeitig zu beantworten. Beispielsweise arbeitet die Gruppe "Technischer Support" mit der Produktentwicklung und Symantec Security Response, um Warnmeldungsdienste und Aktualisierungen der Virendefinitionen zur Verfügung zu stellen.

Die Supportangebote von Symantec bieten Folgendes:

- Verschiedene Supportoptionen, die Ihnen die Flexibilität geben, die richtige Anzahl von Diensten für Unternehmen aller Größen auszuwählen
- Telefon- und/oder webbasierter Support, der schnell reagiert und aktuelle Informationen bietet
- Upgrade-Versicherung, die Software-Upgrades liefert
- Globaler Support, der auf Basis regionaler Geschäftszeiten oder rund um die Uhr erworben werden kann
- Erstklassige Serviceangebote einschließlich Kontoverwaltungsdienste

Informationen zu den Supportangeboten von Symantec finden Sie auf unserer Website unter folgender URL:

www.symantec.com/business/support/

Alle Support-Dienste werden in Übereinstimmung mit Ihrer Supportvereinbarung und der zu dem Zeitpunkt geltenden technischen Enterprise-Support-Richtlinie bereitgestellt.

Kontaktaufnahme mit dem technischen Support

Kunden mit einer aktuellen Supportvereinbarung können unter folgender URL auf technische Support-Informationen zugreifen:

www.symantec.com/business/support/

Bevor Sie sich an den technischen Support wenden, prüfen Sie, ob die in der Produktdokumentation aufgeführten Systemanforderungen erfüllt sind. Sie sollten auch am Computer sein, auf dem das Problem auftrat, falls es notwendig ist, das Problem zu replizieren.

Wenn Sie sich an den technischen Support wenden, halten Sie folgende Informationen bereit:

- Produktversion
- Hardware-Daten
- Verfügbarer Arbeitsspeicher, Speicherplatz und NIC-Informationen

- Betriebssystem
- Version und Patch-Level
- Netzwerktopologie
- Router, Gateway und IP-Adressinformationen
- Problembeschreibung:
 - Fehlermeldungen und Protokolldateien
 - Durchgeführte Fehlerbehebung, vor Kontaktierung von Symantec
 - Aktuelle Software-Konfigurationsänderungen und Netzwerkänderungen

Lizenzierung und Registrierung

Wenn Ihr Symantec-Produkt die Registrierung oder einen Lizenzschlüssel erfordert, konsultieren Sie die Webseite unseres technischen Supports unter folgender URL:

www.symantec.com/business/support/

Kundendienst

Informationen zum Kundenservice sind unter folgender URL verfügbar:

www.symantec.com/business/support/

Der Kundendienst steht Ihnen bei nicht-technischen Fragen zur Verfügung, die beispielsweise folgende Probleme betreffen:

- Fragen bezüglich der Produktlizenzierung oder Zuweisung von Seriennummern
- Produktregistrierung-Updates, wie Adress- oder Namensänderungen
- Allgemeine Produktinformationen (Funktionen, verfügbare Sprachen, lokale Händler)
- Neueste Informationen über Produktaktualisierungen und Upgrades
- Informationen über Upgrade-Versicherung und Supportverträge
- Informationen über die Symantec Buying Programs
- Rat über technische Support-Optionen von Symantec
- Nicht technische Presales-Fragen
- Probleme mit Datenträgern (CD-ROM, DVD) oder Handbüchern

Informationsquellen zur Supportvereinbarung

Wenn Sie Symantec bezüglich einer vorhandenen Supportvereinbarung kontaktieren möchten, wenden Sie sich bitte an das für Supportvereinbarungen zuständige Team für Ihre Region:

Asien-Pazifik und Japan customercare_apj@symantec.com

Europa, Naher Osten und Afrika semea@symantec.com

Nordamerika und Lateinamerika [supportolutions@symantec.com](mailto:supportsolutions@symantec.com)

Versionshinweise

In diesem Dokument werden folgende Themen behandelt:

- [Informationen zu diesem Dokument](#)
- [Neue Funktionen in Symantec Endpoint Protection 12.1.6 MP10](#)
- [Bekannte Probleme und Problemumgehungen](#)
- [Systemanforderungen für Symantec Endpoint Protection](#)
- [Unterstützte Aktualisierungspfade auf Symantec Endpoint Protection](#)
- [Weitere Informationsquellen](#)

Informationen zu diesem Dokument

Dieses Dokument enthält Informationen zu Symantec Endpoint Protection.

Lesen Sie dieses Dokument, bevor Sie das Produkt installieren oder sich an den technischen Support wenden. Die Versionshinweise beschreiben bekannte Probleme und deren Behebung, die nicht in der Standarddokumentation oder in der Online-Hilfe enthalten sind.

Siehe "[Bekannte Probleme und Problemumgehungen](#)" auf Seite 7.

Siehe "[Systemanforderungen für Symantec Endpoint Protection](#)" auf Seite 10.

Neue Funktionen in Symantec Endpoint Protection 12.1.6 MP10

Diese Version von Symantec Endpoint Protection enthält neue Funktionen, Änderungen oder Verbesserungen in den folgenden Bereichen:

- Kundendefekte

- Aktualisierte Komponenten anderer Hersteller

[Neue Funktionen in allen Versionen von Symantec Endpoint Protection 12.1.x](#)

Siehe "[Bekannte Probleme und Problemumgehungen](#)" auf Seite 7.

Bekannte Probleme und Problemumgehungen

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

- Siehe "[Installieren des Produkts](#)" auf Seite 7.
- Siehe "[Informationen zu Symantec Endpoint Protection Manager](#)" auf Seite 7.
- Siehe "[Informationen zu Dokumentation und Hilfe](#)" auf Seite 9.

Hier finden eine Liste behobener Probleme für diese Version:

[Neue Behebungen und Komponentenversionen in Symantec Endpoint Protection 12.1.6 MP10](#)

Installieren des Produkts

Dieser Abschnitt enthält Informationen zum Installieren des Produkts.

Installation von oder Upgrade auf Symantec Endpoint Protection Manager 12.1.6 MP10 wird unter Windows XP/Server 2003 blockiert.

Da PHP auf eine neue Version aktualisiert wurde, wird Symantec Endpoint Protection Manager unter Windows XP/Server 2003 nicht mehr unterstützt. PHP 5.6.27 enthält Sicherheitsverbesserungen im Vergleich zu vorherigen Versionen. Keine Problemumgehung ist verfügbar. Stattdessen müssen Sie entweder den Computer aktualisieren oder Symantec Endpoint Protection Manager auf einen neuen Computer verschieben, der ein unterstütztes Windows-Betriebssystem ausführt.

Informationen zum Verschieben von Symantec Endpoint Protection Manager 12.1.x auf einen neuen Server finden Sie unter [Verschieben von Symantec Endpoint Protection Manager auf einen anderen Server ohne Beeinträchtigung der Clientkommunikation oder Datenverlust](#).

Informationen zu Symantec Endpoint Protection Manager

Dieser Abschnitt enthält Informationen zu Symantec Endpoint Protection Manager.

HTTPS-Kommunikationen mit Symantec Endpoint Protection-Clients unter Windows XP/Server 2003 schlagen fehl

Clientkommunikationen mit Windows XP-/Server 2003-Computern schlagen fehl, wenn die HTTPS-Kommunikation in Symantec Endpoint Protection 12.1.6 MP10 aktiviert ist. Dieser Fehler tritt aufgrund nicht übereinstimmenden Chiffren auf.

Verwenden Sie das Verfahren auf der nächsten Seite, um dieses Problem zu umgehen:

[HTTPS-Kommunikationen mit Endpoint Protection-Clients unter Windows XP/Server 2003 schlagen fehl](#)

Webkonsolenzugriff funktioniert nicht mit Internet Explorer 8-10

Da JRE aktualisiert wurde, unterstützt Symantec Endpoint Protection Manager ab Version 12.1.6 MP9 Internet Explorer 8, 9 oder 10 nicht mehr. Der Webkonsolenzugriff auf Symantec Endpoint Protection Manager 12.1.6 MP10 schlägt fehl, wenn Internet Explorer 8, 9 oder 10 installiert ist. Verwenden Sie stattdessen Internet Explorer 11 oder einen anderen unterstützten Browser.

Siehe "[Systemanforderungen für Symantec Endpoint Protection Manager](#)" auf Seite 11.

Der Remote-Zugriff auf Symantec Endpoint Protection Manager über die Java-Konsole schlägt fehl, wenn FIPS aktiviert ist.

In einer FIPS-kompatiblen Umgebung schlägt der Zugriff auf Symantec Endpoint Protection Manager 12.1.6 MP10 fehl und meldet, dass das Zertifikat nicht validiert werden konnte, und die Anwendung nicht ausgeführt wird. Dieser Fehler wird von einer Inkompatibilität zwischen Crypto-J und JRE 8 verursacht. Um dieses Problem zu umgehen, greifen Sie auf Symantec Endpoint Protection Manager unter Verwendung der Webkonsole zu.

[Der Remote-Zugriff auf Endpoint Protection Manager über die Java-Konsole schlägt fehl, wenn FIPS aktiviert ist](#)

"Firewall" wird in der Symantec Endpoint Protection Manager-Webkonsole als "Fire..." angezeigt

Wenn Sie sich über die Webkonsole bei Symantec Endpoint Protection Manager einloggen, wird auf der Registerkarte "Richtlinien" "Firewall" als "Fire..." angezeigt. Dies ist ein kosmetisches Problem. Eine Fehlerbehebung ist für eine zukünftige Version geplant.

Windows LiveUpdate zeigt englischen Text für lokalisierte Versionen von Symantec Endpoint Protection Manager an.

Symantec Endpoint Protection Manager enthält Windows LiveUpdate, das Inhalte herunterlädt und auf verwalteten Clients bereitstellt. In lokalisierten Versionen von Symantec Endpoint Protection Manager werden die Dialogfelder von Windows LiveUpdate nur auf Englisch angezeigt.

Dieses Verhalten ist derzeit erwartet. Windows LiveUpdate soll in einer zukünftigen Version von Symantec Endpoint Protection lokalisiert werden.

Informationen zu Dokumentation und Hilfe

Dieser Abschnitt enthält Änderungen oder Ergänzungen zur Dokumentation und zur kontextbezogenen Hilfe.

Die Hilfe gibt irrtümlich an, dass Warnmeldungen nicht für alle SONAR-Aktionstypen erzeugt werden.

Das Hilfethema "SONAR: SONAR" gibt irrtümlich an, dass für Bei Erkennung keine Warnmeldung angezeigt wird, wenn die Aktion "Nur protokollieren" ist. Eine Warnmeldung wird für alle Aktionstypen ausgegeben, wenn eine SONAR-Erkennung erfolgt, nicht nur für "Isolieren" und "Entfernen". Der korrigierte Text für "Bei Erkennung" lautet:

Der Benutzer erhält eine Warnmeldung, wenn SONAR ein Problem erkennt.

Die Hilfe enthält keine Informationen zur maximalen Bandbreite zum Herunterladen von Clients vom Group Update Provider (GUP).

In Symantec Endpoint Protection Manager enthält das Thema "Group Update Provider" der kontextbezogenen Hilfe keine Anweisungen zum Festlegen der Option "Maximale Bandbreite für Group Update Provider zum Herunterladen von Clients". Die Beschreibung lautet:

Maximale Bandbreite für Group Update Provider zum Herunterladen von Clients : Verwenden Sie diese Option zum Einrichten eines GUP, um mehrere Standorte zu versorgen, die nur wenige Clients haben. Sie sollten die Bandbreite für Standorte verringern, die eine geringere Konnektivität haben und auf denen Inhaltsfluten vermieden werden sollen, wenn ein vollständiger Satz Inhaltsdefinitionen bereitgestellt wird.

Korrekturen und Ergänzungen zur Datenbankschemareferenz für 12.1.6

Die folgenden Elemente fehlen in der Datenbankschemareferenz für Symantec Endpoint Protection 12.1.6 oder sind falsch.

Tabelle 1-1 Updates der Datenbankschemareferenz für 12.1.6

Element	Update
Einträge in Agent-Verhaltensprotokollen zeigen die falsche Maßeinheit an	<p>Schemaeinträge in Agent-Verhaltensprotokollen zu Anwendungssteuerungsverletzungen listen die Dateigrößen in Megabyte (MB) auf. Die Dateigröße sollte stattdessen in Byte angegeben werden, sowohl in der Datenbank als auch in den Clientprotokollen.</p> <p>Betroffen sind folgende:</p> <ul style="list-style-type: none"> ■ AGENT_BEHAVIOR_LOG_1 ■ AGENT_BEHAVIOR_LOG_2 ■ BEHAVIOR_REPORT
Fehlende Werte in der ACTUALACTION-Tabelle	<p>Die ACTUALACTION-Tabelle lässt irrtümlich die folgenden Werte aus:</p> <ul style="list-style-type: none"> ■ 24 - RepairFailedPowerEraser Ein Power Eraser-Scan wird empfohlen. Symantec Endpoint Protection kann die Bedrohung nicht entfernen oder bereinigen. Symantec Endpoint Protection kann die Bedrohung nur blockieren. ■ 25 - RepairFailedPowerEraser2 Ein Power Eraser-Scan wird empfohlen. Symantec Endpoint Protection kann die Bedrohung nicht entfernen oder bereinigen. Symantec Endpoint Protection kann nicht bestätigen, dass die Bedrohung blockiert wurde. ■ 100 - IDS block ■ 101 - Firewall violation ■ 102 - Allowed by user ■ 200 - Attachment stripped
Werte für Agent-Verhaltensprotokolle für die Spalte DESCRIPTION (Beschreibung)	<p>In der Tabelle AGENT_BEHAVIOR_LOG_1 gilt für die Spalte DESCRIPTION ein Limit von 256 Zeichen. Deshalb sind möglicherweise tatsächliche Werte aus dem Client länger als die, die in Protokollen oder Berichten von Symantec Endpoint Protection Manager angezeigt werden. Bestätigen Sie den Vorgang auf dem Client.</p>

Die Datenbankschemareferenz für 12.1.6 finden Sie unter [Symantec Endpoint Protection 12.1.6 – Datenbankschema](#).

Systemanforderungen für Symantec Endpoint Protection

Im Allgemeinen sind die Systemanforderungen für Symantec Endpoint Protection Manager- und Symantec Endpoint Protection-Clients mit denen für die Betriebssysteme identisch, unter denen sie unterstützt werden.

Die aktuellen Systemanforderungen finden Sie unter:

[Systemanforderungen für Symantec Endpoint Protection 12.1.6 MP10](#)

- Siehe ["Systemanforderungen für Symantec Endpoint Protection Manager"](#) auf Seite 11.
- Siehe ["Systemanforderungen für den Symantec Endpoint Protection-Client für Windows"](#) auf Seite 13.
- Siehe ["Systemanforderungen für den Symantec Endpoint Protection-Client für Windows Embedded"](#) auf Seite 15.
- Siehe ["Systemanforderungen für den Symantec Endpoint Protection-Client für Mac"](#) auf Seite 16.
- Siehe ["Systemanforderungen für den Symantec Endpoint Protection-Client für Linux"](#) auf Seite 17.

Siehe ["Unterstützte virtuelle Installationen und Virtualisierungsprodukte"](#) auf Seite 18.

Systemanforderungen für Symantec Endpoint Protection Manager

Hinweis: Diese Version von Symantec Endpoint Protection Manager verwaltet 11.0.x- und 12.0.x-Clients, unabhängig vom Client-Betriebssystem. Die Unterstützung von Symantec Endpoint Protection 11.0.x und 12.0.x wurde jedoch am 5. Januar 2015 eingestellt.

Tabelle 1-2 Systemanforderungen für Symantec Endpoint Protection Manager

Komponente	Anforderungen
Prozessor	Mindestens Intel Pentium Dual-Core oder Äquivalent Hinweis: Intel Itanium IA-64-Prozessoren werden nicht unterstützt.
Arbeitsspeicher	Mindestens 2 GB verfügbar; 4 GB oder mehr werden empfohlen Hinweis: Für den Symantec Endpoint Protection Manager-Server ist eventuell zusätzlicher Arbeitsspeicher erforderlich. Dies hängt von den Anforderungen anderer bereits installierter Anwendungen ab.
Festplatte	Mindestens 16 GB (100 GB empfohlen) für den Management-Server Mindestens 40 GB (200 GB empfohlen) für den Management-Server und eine lokal installierte Datenbank
Anzeige	1024 x 768 oder besser

Komponente	Anforderungen
Betriebssystem (Desktop)	<ul style="list-style-type: none"> ■ Windows 7 (32 Bit, 64 Bit; RTM und SP1; alle Editions außer Starter und Home) ■ Windows 8 (32 und 64 Bit) ■ Windows 8.1 (32 Bit, 64 Bit) ■ Windows 8.1 Update (April 2014) (32 Bit, 64 Bit) ■ Windows 8.1 Update (August 2014) (32 Bit, 64 Bit) <p>Hinweis: Windows 7 lässt nur 20 gleichzeitige Verbindungen zu. Die Installation von Symantec Endpoint Protection Manager unter Windows 7 wird nur in kleineren Umgebungen empfohlen. Konfigurationsempfehlungen finden Sie unter Best Practices beim Installieren von Endpoint Protection Manager unter Windows 7 oder XP.</p>
Betriebssystem (Server)	<ul style="list-style-type: none"> ■ Windows Server 2008 (32 und 64 Bit, R2, RTM, SP1 und SP2) ■ Windows Small Business Server 2008 (64-Bit) ■ Windows Essential Business Server 2008 (64-Bit) ■ Windows Small Business Server 2011 (64-Bit) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Server 2012 R2 Update (April 2014) ■ Windows Server 2012 R2 Update (August 2014) ■ Windows Server 2016 <p>Hinweis: Windows Server Core Edition wird nicht unterstützt. Windows Server Core enthält Internet Explorer nicht, der zum Einsatz von Symantec Endpoint Protection Manager erforderlich ist.</p>
Webbrowser	<p>Die folgenden Browser werden für den Webkonsolenzugriff auf Symantec Endpoint Protection Manager und für das Anzeigen der Symantec Endpoint Protection Manager-Hilfe unterstützt:</p> <ul style="list-style-type: none"> ■ Microsoft Internet Explorer 11 Siehe "Webkonsolenzugriff funktioniert nicht mit Internet Explorer 8-10" auf Seite 8. ■ Mozilla Firefox 5.x bis 59.x ■ Google Chrome 65.x

Komponente	Anforderungen
Datenbank	<p>Symantec Endpoint Protection Manager enthält eine eingebettete Datenbank. Sie können auch eine Datenbank aus einer der folgenden Versionen von Microsoft SQL Server verwenden:</p> <ul style="list-style-type: none"> ■ SQL Server 2005, SP4 ■ SQL Server 2008, RTM - SP4 ■ SQL Server 2008 R2, RTM - SP3 ■ SQL Server 2012, RTM - SP3 ■ SQL Server 2014, RTM - SP2 ■ SQL Server 2016 <p>Hinweis: Die SQL Server Express Edition-Datenbank wird nicht unterstützt.</p> <p>Hinweis: 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.</p> <p>Weitere Informationen: Unterstützung für Microsoft SQL Server TLS 1.2</p>

Hinweis: 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.

Siehe "[Unterstützte virtuelle Installationen und Virtualisierungsprodukte](#)" auf Seite 18.

Systemanforderungen für den Symantec Endpoint Protection-Client für Windows

Tabelle 1-3 Systemanforderungen für den Symantec Endpoint Protection-Client für Windows

Komponente	Anforderungen
Prozessor	<ul style="list-style-type: none"> ■ 32-Bit-Prozessor: Mindestens 1 GHz Intel Pentium III oder gleichwertig (Intel Pentium 4 oder gleichwertig empfohlen) ■ 64-Bit-Prozessor: Mindestens 2 GHz Pentium 4 mit x86-64-Unterstützung oder gleichwertig <p>Hinweis: Itanium-Prozessoren werden nicht unterstützt.</p>
Arbeitsspeicher	512 MB RAM (1 GB empfohlen) oder mehr, falls vom Betriebssystem erfordert

Komponente	Anforderungen
Festplatte	<p>1,8 GB verfügbarer Festplattenspeicher für die Installation sowie Speicherplatz für Content und Protokolle</p> <p>Hinweis: Platzbedarf basiert auf NTFS-Dateisystemen.</p>
Anzeige	800 x 600 oder besser
Betriebssystem (Desktop)	<ul style="list-style-type: none"> ■ Windows XP Home oder Professional (32 Bit, SP3; 64 Bit, SP2) ■ Windows XP Embedded (SP3) ■ Windows Vista (32 Bit, 64 Bit) ■ Windows 7 (32 Bit, 64 Bit, RTM und SP1) ■ Windows Embedded 7 Standard, POSReady und Enterprise (32 und 64 Bit) ■ Windows 8 (32 und 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, Industry Enterprise (32 und 64 Bit) ■ Windows 10 (32 Bit, 64 Bit) ■ Windows 10 November Update (2015) (32 und 64 Bit) ■ Windows 10 Anniversary Update (2016) (32 und 64 Bit) (grundlegende Kompatibilität) ■ Windows 10 Creator Update (2017) (32 und 64 Bit) (grundlegende Kompatibilität) ■ Windows 10 Fall Creators Update (2017) (32 und 64 Bit) (grundlegende Kompatibilität) <p>Wichtige Informationen zur grundlegenden Kompatibilität finden Sie unter Unterstützung von Endpoint Protection unter Windows 10-Updates und Windows Server 2016.</p> <p>Siehe "Systemanforderungen für den Symantec Endpoint Protection-Client für Windows Embedded" auf Seite 15.</p>
Betriebssystem (Server)	<ul style="list-style-type: none"> ■ Windows Server 2003 (32 und 64 Bit, R2, SP1 und höher) ■ Windows Small Business Server 2003 (32-Bit) ■ Windows Server 2008 (32 Bit, 64 Bit, R2, SP1 und SP2) ■ Windows Small Business Server 2008 (64-Bit) ■ Windows Essential Business Server 2008 (64-Bit) ■ Windows Small Business Server 2011 (64-Bit) ■ Windows Server 2012 ■ Windows Server 2012 R2 ■ Windows Server 2012 R2 Update (April 2014) ■ Windows Server 2012 R2 Update (August 2014) ■ Windows Server 2016 (grundlegende Kompatibilität) <p>Wichtige Informationen zur grundlegenden Kompatibilität finden Sie unter Unterstützung von Endpoint Protection unter Windows 10-Updates und Windows Server 2016.</p>

Komponente	Anforderungen
Browser-Angriffsschutz	Browser-Angriffsschutz-Unterstützung basiert auf der Version der Client-Intrusion Detection-System-Engine (CIDS). Vom Browser-Angriffsschutz in Endpoint Protection unterstützte Browser.

Siehe "[Unterstützte virtuelle Installationen und Virtualisierungsprodukte](#)" auf Seite 18.

Systemanforderungen für den Symantec Endpoint Protection-Client für Windows Embedded

Tabelle 1-4 Systemanforderungen für den Symantec Endpoint Protection-Client für Windows Embedded

Komponente	Anforderungen
Prozessor	1 GHz Intel Pentium
Arbeitsspeicher	256 MB
Festplatte	450 MB freier Festplattenspeicher
Version von Windows Embedded	<ul style="list-style-type: none"> ■ Windows Embedded Standard (WES) 2009 (32 Bit, SP3) ■ Windows Embedded POSReady 2009 (32 Bit, SP3) ■ Windows Embedded Point of Service (WEPOS) (32 Bit, SP3) ■ 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	<ul style="list-style-type: none"> ■ Filter-Manager (FitMgr.sys) ■ Performance Data Helper (pdh.dll) ■ Windows Installer-Dienst ■ FBA: Treibersignierung (gilt nur für XP-basiertes Embedded) ■ WinLogon (gilt nur für XP-basiertes Embedded)

Komponente	Anforderungen
Vorlagen	<ul style="list-style-type: none"> ■ Anwendungscompatibilität (Standard) ■ Digitale Beschilderung ■ Industrielle Automatisierung ■ IE, Media Player, RDP ■ Set-Top-Box ■ Thin Client <p>Die minimale Konfigurationsvorlage wird nicht unterstützt.</p> <p>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.</p>

Weitere Informationen finden Sie unter [Unterstützung von Symantec Endpoint Protection unter Windows Embedded](#).

Siehe "[Unterstützte virtuelle Installationen und Virtualisierungsprodukte](#)" auf Seite 18.

Systemanforderungen für den Symantec Endpoint Protection-Client für Mac

Tabelle 1-5 Systemanforderungen für den Symantec Endpoint Protection-Client für Mac

Komponente	Anforderungen
Prozessor	64 Bit Intel Core 2 Duo oder besser
Arbeitsspeicher	2 GB RAM
Festplatte	500 MB freier Speicherplatz für die Installation
Anzeige	800 x 600
Betriebssystem	Mac OS X 10.8, 10.9, 10.10, 10.11 und macOS 10.12 Hinweis: 12.1.6 MP10 wird unter macOS 10.13 nicht unterstützt.

Systemanforderungen für den Symantec Endpoint Protection-Client für Linux

Tabelle 1-6 Systemanforderungen für den Symantec Endpoint Protection-Client für Linux

Komponente	Anforderungen
Hardware	<ul style="list-style-type: none"> ■ Prozessor: Intel Pentium 4 (2 GHz) oder neuerer Prozessor ■ 1 GB RAM ■ 7 GB freier Festplattenspeicher
Betriebssysteme	<ul style="list-style-type: none"> ■ Amazon Linux ■ CentOS 9U4, 6U5, 6U6, 6U6, 7, 7U1, 7U2, 7U3 (32 und 64 Bit) ■ Debian 6.0.5 Squeeze, Debian 8 Jessie; 32 und 64 Bit ■ Fedora 16, 17; 32 und 64 Bit ■ Novell Open Enterprise Server (OES) 2 SP2 und 2 SP3 mit SUSE Linux Enterprise Server (SLES) 10 SP3; 32 und 64 Bit ■ Novell Open Enterprise Server (OES) 11 und 11 SP1 mit SUSE Linux Enterprise Server (SLES) 11 SP1 und SP2; 64 Bit ■ Oracle Linux (OEL) 5U8, 5U9, 6U2, 6U4, 6U5; 64 Bit ■ Red Hat Enterprise Linux Server (RHEL) 5U7 - 5U11, 6U2 - 6U9, 7 - 7U3 (32 and 64 Bit) ■ SUSE Linux Enterprise Server (SLES) 10 SP3, 10 SP4, 11 SP1 – 11 SP3 (32 und 64 Bit) ■ SUSE Linux Enterprise Desktop (SLED) 10 SP3, 10 SP4, 11 SP1 - 11 SP3 (32 und 64 Bit) ■ Ubuntu 11.10, 12.04, 12.04.02, 14.04, 16.04; 32 und 64 Bit <p>Eine Liste der unterstützten Betriebssystemkernel finden Sie unter Unterstützte Linux-Kernel für Symantec Endpoint Protection.</p>
Grafische Benutzeroberflächen	<p>Sie können die folgenden grafischen Benutzeroberflächen für den Einsatz des Symantec Endpoint Protection-Client für Linux verwenden:</p> <ul style="list-style-type: none"> ■ KDE ■ Gnome ■ Unity

Komponente	Anforderungen
Andere Umgebungsbedingungen	<ul style="list-style-type: none"> ■ Oracle Java 1.5 oder höher; Java 7 oder höher empfohlen Für diese Installation sind Super-User-Rechte erforderlich. ■ Unlimited Strength Java Cryptography Extension (JCE) Sie müssen die Richtliniendateien für "Unlimited Strength Java Cryptography Extension" installieren, damit diese Ihrer Version von Java entsprechen. Für diese Installation sind Super-User-Rechte erforderlich. Sie können die Installationsdateien unter "Zusätzliche Ressourcen" von der folgenden Oracle-Website herunterladen: http://www.oracle.com/technetwork/java/javase/downloads/ ■ 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 <code>sudo</code>: Red Hat-Distributionen:<code>sudo yum install glibc.i686 libgcc.i686 libX11.i686</code> Debian-Distributionen:<code>sudo apt-get install ia32-libs</code> Ubuntu-Distributionen:<code>sudo apt-get install libx11-6:i386 libgcc1:i386 libc6:i386</code> ■ net-tools Zum Installieren von Symantec Endpoint Protection unter Red Hat Enterprise Linux Server (RHEL) 7.1 oder höher müssen Sie zuerst "net-tools" installieren. ■ XFS-Dateisysteme, die Inode64-Attribute enthalten, werden nicht unterstützt.

Siehe "[Unterstützte virtuelle Installationen und Virtualisierungsprodukte](#)" auf Seite 18.

Unterstützte virtuelle Installationen und Virtualisierungsprodukte

Sie können Symantec Endpoint Protection unter unterstützten Betriebssystemen installieren, die in einer virtuellen Umgebung ausgeführt werden. Installieren Sie Symantec Endpoint Protection auf dem Gastbetriebssystem, nicht dem Host.

Die folgenden Virtualisierungsprodukte unterstützen Symantec Endpoint Protection Manager, die Konsole und die eingebettete Datenbank sowie die Symantec Endpoint Protection-Clientsoftware für Windows und Linux:

- Windows Azure
- Amazon WorkSpaces
- VMware WS 5.0 (Workstation) oder höher

- VMware GSX 3.2 (Enterprise) oder höher
- VMware ESX 2.5 (Workstation) oder höher
- VMware ESXi 4.1 - 5.5
- VMware ESXi 6.0
- VMware ESXi 6.0 Update 1
- VMware ESXi 6.0 Update 2
- Microsoft Virtual Server 2005
- Microsoft Enterprise Desktop Virtualization (MED-V) mit Windows XP-Modus
- Windows Server 2008 Hyper-V
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Citrix XenServer 5.6 oder höher
- Virtual Box von Oracle

Unterstützte Aktualisierungspfade auf Symantec Endpoint Protection

Symantec Endpoint Protection Manager und Windows-Client

Die folgenden Versionen von Symantec Endpoint Protection Manager und Symantec Endpoint Protection Windows-Client können direkt auf 12.1.6 MP10 aktualisiert werden:

- 11.0.x und Small Business Edition 12.0.x
 Weitere Informationen finden Sie unter [Unterstützte Aktualisierungs- und Migrationspfade auf Symantec Endpoint Protection 12.1.x](#).
- 12.1 RTM (12.1.671.4971)
- 12.1.1 (12.1.1000.157)
- 12.1.1 MP1 (12.1.1101.401)
- 12.1.2 (12.1.2015.2015)
- 12.1.2 MP1 (12.1.2100.2093)
- 12.1.3 (12.1.3001.165)
- 12.1.4 (12.1.4013.4013)
- 12.1.4a (12.1.4023.4080)

- 12.1.4 MP1 (12.1.4100.4126)
- 12.1.4 MP1a (12.1.4104.4130)
- 12.1.4 MP1b (12.1.4112.4156b)
- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)
- 12.1.6 MP1 (12.1.6306.6100)
- 12.1.6 MP1a (12.1.6318.6100)
- 12.1.6 MP2 (12.1.6465.6200)
- 12.1.6 MP3 (12.1.6608.6300)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP5 (12.1.7004.6500)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP7 (12.1.7166.6700)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9a (12.1.7385.6900)

Mac OS-Client

Die folgenden Versionen des Symantec Endpoint Protection-Clients für Mac können direkt auf die Version 12.1.6 MP10 aktualisiert werden:

- 12.1 RTM (12.1.671.4971)
- 12.1.1 (12.1.1000.157)
- 12.1.2 (12.1.2015.2015)
- 12.1.4 (12.1.4013.4013)
- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)
- 12.1.6 MP2 (12.1.6465.6200)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9 (12.1.7369.6900)

Hinweis: Der Symantec Endpoint Protection-Client für Mac wurde für 12.1.3, 12.1.6 MP1/MP1a/MP3/MP5 und MP7 nicht aktualisiert.

Linux-Client

Die folgenden Versionen des Symantec Endpoint Protection-Client für Linux können direkt auf die Version 12.1.6 MP10 aktualisiert werden:

- 12.1.5 (12.1.5337.5000)
- 12.1.6 (12.1.6168.6000)
- 12.1.6 MP3 (12.1.6608.6300)
- 12.1.6 MP4 (12.1.6867.6400)
- 12.1.6 MP5 (12.1.7004.6500)
- 12.1.6 MP6 (12.1.7061.6600)
- 12.1.6 MP7 (12.1.7166.6700)
- 12.1.6 MP8 (12.1.7266.6800)
- 12.1.6 MP9 (12.1.7369.6900)

Symantec AntiVirus für Linux 1.0.14 ist die einzige Version, die Sie direkt auf Symantec Endpoint Protection migrieren können. Sie müssen alle anderen Versionen von Symantec AntiVirus für Linux zuerst 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 12.1.6 MP10-Client installieren:

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

Downgrade-Pfade werden nicht unterstützt. Beispiel: Wenn Sie eine Migration von Symantec Endpoint Protection 14.0.1 MP1 auf Version 12.1.6 MP10 durchführen, müssen Sie zuerst Symantec Endpoint Protection 14.0.1 MP1 deinstallieren.

Unterstützte Upgrades auf Windows 10, wenn der Symantec Endpoint Protection-Client installiert ist

Sie können auf Windows 10 bei installiertem Symantec Endpoint Protection-Client wie folgt aktualisieren:

- Aktualisieren Sie auf Windows 10, wenn 12.1.6 MP1 oder höher installiert ist.
- Aktualisieren Sie auf Windows 10 Anniversary Update bzw. Creators Update, wenn 12.1.6 MP5 oder höher installiert ist.
- Aktualisieren Sie auf Windows 10 Fall Creators Update, wenn 12.1.6 MP9 oder höher installiert ist.

Vor dem Windows-Upgrade müssen Sie sicherstellen, dass die Viren- und Spyware-Schutz-Definitionen vom 27. Juli 2015 oder später stammen. Die Definitionen enthalten ein Update auf Eraser Engine (115.1.1.10), das für die Kompatibilität mit Windows 10 erforderlich ist.

Sie müssen Versionen des Symantec Endpoint Protection-Client installieren, die niedriger als die bereits angegebenen sind. Das Upgrade des Betriebssystems wird beendet, wenn es eine frühere Version von Symantec Endpoint Protection erkennt.

Die folgenden Betriebssystem-Aktualisierungspfade werden unterstützt, wenn die entsprechende kompatible Clientversion installiert ist:

- Windows 8.1 auf Windows 10
- Windows 8 auf Windows 10
- Windows 7 auf Windows 10

Hinweis: Windows 7 enthält Early Launch-Anti-Malware (ELAM) nicht. Deshalb ist die ELAM-Komponente von Symantec Endpoint Protection nicht aktiviert und wird nicht aktiviert, nachdem Sie auf Windows 10 aktualisiert haben, wenn Symantec Endpoint Protection installiert ist. Die Schutzstufe ist mit der unter Windows 7 identisch.

Damit der Symantec Endpoint Protection-Client ELAM erkennen und die ELAM-Komponente von Symantec Endpoint Protection aktivieren kann, müssen Sie Symantec Endpoint Protection deinstallieren und erneut installieren. Sie können aus 12.1.6 MP1 auf die neueste Version von Symantec Endpoint Protection aktualisieren, damit die ELAM-Komponente erkannt wird. Das Reparieren der Clientinstallation aktiviert die ELAM-Komponente nicht.

Weitere Informationsquellen

[Tabelle 1-7](#) zeigt die Website an, auf der Sie Informationen zu Best Practices, Fehlerbehebung und andere Ressourcen zum Einsatz des Produkts finden.

Tabelle 1-7 Symantec-Website

Art der Informationen	Link zur Website
Testversionen	Testversion (14.x)
Aktualisierte Handbücher und Dokumentation	<p>Englisch :</p> <ul style="list-style-type: none"> ■ Symantec Product Documentation ■ Produkt Handbücher für alle Versionen von Symantec Endpoint Protection 12.1.x ■ Produkt Handbücher für alle Versionen von Symantec Endpoint Protection 14 <p>Andere Sprachen:</p> <ul style="list-style-type: none"> ■ Portugiesisch (Brasilien) ■ Chinesisch (vereinfacht) ■ Chinesisch (traditionell) ■ Französisch ■ Deutsch ■ Italienisch ■ Japanisch ■ Koreanisch ■ Spanisch <p>*Die Dateien für Tschechisch, Polnisch und Russisch finden Sie auf der Seite "Englisch".</p>
Technischer Support	<p>Technischer Support für Endpoint Protection</p> <p>Schließt Supportdatenbankartikel, Produktversionsdetails, Updates und Patches sowie Kontaktoptionen für den Support ein.</p>
Bedrohungsinformationen und -Updates	Symantec Security Center
Schulung	<ul style="list-style-type: none"> ■ Symantec Education Services <p>Greifen Sie auf Schulungen, die eLibrary und mehr zu.</p>
Symantec Connect-Foren	Endpoint Protection