Poznámky k verzi aplikace Symantec™ Endpoint Protection 14.3

Poslední aktualizace: červen 2020

Table of Contents

Prohlášení o autorských právech 3
Novinky v aplikaci Symantec Endpoint Protection 14.3 4
Známé problémy a jejich řešení 6
Systémové požadavky na aplikaci Symantec Endpoint Protection (SEP) 10
Podporované možnosti upgradu na nejnovější verzi aplikace Symantec Endpoint Protection 14.x 17
Další zdroje informací 19

Prohlášení o autorských právech

Novinky v aplikaci Symantec Endpoint Protection 14.3

Tato část popisuje nové funkce pro vydání 14.3.

Funkce ochrany

- Vývojáři aplikací třetích stran mohou chránit své zákazníky před dynamickým malwarem založeným na skriptech a před netradičními cestami kybernetického útoku. Aplikace jiného výrobce volá rozhraní Windows AMSI a požaduje prověření skriptu poskytnutého uživatelem, který je směrován do klienta Symantec Endpoint Protection. Klient odpoví verdiktem o tom, zda je chování skriptu škodlivé. Pokud chování není škodlivé, spuštění skriptu pokračuje. Pokud je chování skriptu škodlivé, aplikace ho nespustí. V klientovi se v dialogovém okně Výsledky zjišťování zobrazí stav „Přístup byl odepřen“. Ke skriptům jiných výrobců patří například Windows PowerShell, JavaScript a VBScript. Je třeba povolit funkci Auto-Protect. Tato funkce pracuje v počítačích se systémem Windows 10 a novějšími.
  Jak pomáhá rozhraní AMSI (Antimalware Scan Interface) s obranou proti malwaru
  Antimalware Scan Interface (AMSI)

Symantec Endpoint Protection Manager

- Vzdálená konzole aplikace Symantec Endpoint Protection nyní podporuje jazyk Java 11 namísto Java 8.Chcete-li získat přístup ke vzdálené konzoli, otevřete podporovaný webový prohlížeč, do adresního řádku zadejte následující adresu: `http://SEPMServer:9090/symantec.html` a stáhněte nový balíček vzdálené konzole. Postupujte podle uvedených pokynů. Předchozí verze vzdálené konzole Symantec Endpoint Protection Manager již není podporována.
  Přihlášení k aplikaci Symantec Endpoint Protection
- Jednu z aplikací Symantec Endpoint Protection Manager v umístění můžete nakonfigurovat jako hlavní server protokolování pro předávání protokolů na server syslog. Pokud hlavní protokolovací server přejde do režimu offline, druhý server pro správu převezme a předá protokoly na server syslog. Když se hlavní protokolovací server vrátí do režimu online, obnoví předávání protokolů.
  Konfigurace serveru s podporou převzetí služeb při selhání pro externí protokolování
- Zásady integrace mají novou možnost přesměrování provozu služby WSS, **Povolit vlastní soubor PAC služby LPS**.Tato možnost umožňuje nahradit výchozí soubor PAC, který je hostován serverem LPS v klientovi, vlastním souborem PAC. Vlastní soubor PAC řeší problém kompatibility s aplikacemi jiných výrobců, které nefungují s místním serverem proxy, který naslouchá na adaptéru zpětné smyčky.
  Konfigurace přesměrování přenosů služby WSS
- Podpora databáze Microsoft SQL Server 2019.
- Proces antivirové kontroly nyní používá samostatnou službu oddělenou od hlavní služby nesouvisející se zabezpečením. Tento nový prověřovací proces přináší efektivnější využití paměti, nepřetržitou ochranu a menší závislost na problémech s hlavní službou.
- Databázové schéma obsahuje nové sloupce jako součást funkce pro budoucí vydání. (tabulky AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2, SEM_AGENT)
- Rozhraní Rest API obsahuje v JSON odpovědi rozhraní API /sepm/api/v1/computers pro volání a stahování zprávy o stavu počítače následující pole: quarantineStatus, quarantineCode, wssStatus, pskVersion.
- Následující komponenty třetích stran byly upgradovány na novější verze: Apache Tomcat, knihovny Boost C++, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, ovladač Microsoft JDBC pro SQL Server, OpenSC, OpenSSL, Spring Security, rozhraní spring-framework, sqlite.
- Chcete-li zaregistrovat doménu Symantec Endpoint Protection Manager v cloudové konzoli, musíte nejprve získat registrační token prostřednictvím konzole Symantec Endpoint Security. Registrační token jste získali dříve kliknutím na tlačítko **Začínáme** na stránce **Cloud**.

Aktualizace klienta a platformy

- Klient systému Windows podporuje Windows 10 20H1 (Windows 10 verze 2004)
- Klient systému Linux nyní podporuje verzi Ubuntu 18.04, RHEL 8 a CentOS 8.
- Nástroj AppRemover byl aktualizován na novější verzi. Nástroj AppRemover odebere před instalací klienta systému Windows aplikace jiných výrobců. Další informace o tom, které aplikace odebere, naleznete v tématu: Odstranění bezpečnostního softwaru jiných výrobců v aplikaci Endpoint Protection 14.3

Funkce odstraněny

- Následující oznámení již nezobrazují pole **Závažnost rizika** a **Typ rizika**: Incident rizika, Jedna událost rizika, Nová zjištěná rizika.

Novinky ve všech vydáních aplikace Symantec Endpoint Protection

Známé problémy a jejich řešení

Položky uvedené v této části se týkají této verze aplikace Symantec Endpoint Protection.

Table 1: Problémy s upgradem

Problém	Popis a řešení
Upgrade serveru SQL Server z verze 2017 na verzi 2019 se nezdaří s povoleným režimem FIPS [14.3]	Může se zobrazit chyba: „Došlo k následující chybě. Při instalaci rozšiřující funkce došlo k chybě s chybovou zprávou: Vytvoření AppContainer se nezdařilo s chybovou zprávou NONE, state. Tato implementace není součástí ověřených kryptografických algoritmů FIPS na platformě Windows.“ K tomu dochází, pokud máte aplikaci Symantec Endpoint Protection Manager 14.3 s podporou FIPS a upgradujete z Microsoft SQL Server 2017 na 2019. [SEP-61473] Chcete-li tento problém vyřešit, zakažte FIPS na úrovni operačního systému: 1. Ve složce `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools` klikněte na možnost **Místní zásady zabezpečení** > **Místní zásady** > **Možnosti zabezpečení** a deaktivujte možnost **Systémová kryptografie: Používat algoritmy kompatibilní s FIPS k šifrování, hashování a podepisování** 2. Upgrade SQL Serveru z verze 2017 na verzi 2019. 3. Po úspěšném upgradu SQL Serveru znovu povolte FIPS. Upgrade SQL z verze 2017 na 2019 se nezdaří s povoleným režimem FIPS
Vlastní názvy mohou během upgradu na verzi 14.2 nebo novější zabránit dokončení aktualizace zásad brány firewall	V případě upgradu na aplikaci Symantec Endpoint Protection verze 14.2 nebo novější nemohou zásady brány firewall při změně některých výchozích názvů řádně reagovat na změny IPv6. Výchozím názvem je myšlen název výchozích zásad a výchozích pravidel. Pokud během upgradu nedojde k aktualizaci pravidel, možnosti IPv6 se nezobrazí. Na pravidla nově vytvořená po upgradu se tento problém nevztahuje. Pokud to bude možné, vraťte veškeré upravené názvy zpět do výchozí podoby. V opačném případě se ujistěte, že žádná vlastní pravidla, která přidáte do výchozí zásady, nebudou žádným způsobem blokovat komunikaci IPv6. To samé platí pro nově přidané zásady a pravidla.

Table 2: Problémy s aplikací Symantec Endpoint Protection Manager

Problém	Popis a řešení
Pokud používáte funkci hybridní správy a servery proxy [14.2.2.1 a novější], je nutné v aplikaci Symantec Endpoint Security přidat další adresy URL na seznam povolených položek.	V důsledku nedávné akvizice produktu Symantec Enterprise Security společností Broadcom se změnily ve verzi 14.2.2.1 adresy URL ke komunikaci mezi klienty a cloudy. [CDM-42467] Klienty je nutné upgradovat na verzi sestavení 14.2.5569.2100 nebo novější v následující situaci • Používáte produkt Symantec Endpoint Security ke správě svých klientů a zásad, když jsou vaše místní domény Symantec Endpoint Protection Manager zaregistrované v cloudové konzoli. • Používáte servery proxy. Chcete-li tyto adresy URL přidat na seznam povolených položek v agentech s plnou cloudovou správou nebo hybridní správou, je nutné je přidat na seznam povolených položek v aplikaci Symantec Endpoint Security: 1. V aplikaci Symantec Endpoint Security přejděte na možnost **Koncový bod > Zásady > Zásady seznamu povolených položek [název zásad]**. 2. V zásadách seznamu povolených položek vedle položky **Vyloučeno doménou** vyberte možnost **Přidat**, přidejte postupně následující adresy URL a vyberte možnost **Přidat**: `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (přidejte, pokud máte zařízení v Evropě). Pokud budete dále spravovat klienty v novější verzi, ponechte spoc.norton.com. 3. Výběrem možnosti **Uložit zásady** a pak **Ano** aktualizujte zásady a použijte je pro existující skupiny. Viz část Adresy URL na seznam povolených položek pro Symantec Endpoint Security. Viz část Upgrade agentů Symantec s cloudovou správou na verzi 14.2 RU2 MP1 nebo novější ke 4. květnu 2020.
Vzdálená konzole aplikace Symantec Endpoint Protection Manager již nepodporuje 32bitovou platformu Windows [14.3]	Od verze 14.3 se nelze přihlásit k vzdálené konzole aplikace Symantec Endpoint Protection Manager, pokud používáte 32bitovou verzi systému Windows. Prostředí Oracle Java SE Runtime Environment již nepodporuje 32bitové verze systému Microsoft Windows. [SEP-61106] Pokud se zobrazí následující zpráva, přihlaste se k aplikaci Symantec Endpoint Protection Manager z místního počítače: „Tato verze programu C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe není kompatibilní s verzí systému Windows, kterou používáte. Zkontrolujte informace o systému počítače a obraťte se na vydavatele softwaru.“ Přihlášení k aplikaci Symantec Endpoint Protection Manager
Při instalaci aplikace Symantec Endpoint Protection Manager [14.3] se zobrazí chyba „Instalace modulu Microsoft Visual C++ Runtime se nezdařila“	Při instalaci aplikace Symantec Endpoint Protection Manager v systému Windows 2012 R2 se může zobrazit následující chyba: „Nepodařilo se nainstalovat modul Microsoft Visual C++ Runtime“ [SEP-60396] Chcete-li tento problém vyřešit, aktivujte systém Windows a nainstalujte aktualizace systému Windows. Aktualizace Windows nainstaluje balíček Visual C++ 2017 Redistributable, což je předpokladem k instalaci aplikace Symantec Endpoint Protection Manager 14.3 v systému Windows 2012 R2.

Problém	Popis a řešení
Nelze povolit TLS 1.1 a TLS 1.2 jako výchozí zabezpečovací protokoly ve WinHTTP v systému Windows [14.3]	Po upgradu nebo instalaci aplikace Symantec Endpoint Protection Manager verze 14.3, která je zaregistrovaná do cloudové konzole, již server pro správu nenahrává úspěšně protokoly do cloudu. V souboru uploader.log se může zobrazit následující chyba: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Tento problém je způsoben chybějící aktualizací společnosti Microsoft, která poskytuje podporu pro TLS 1.1 a 1.2. Chcete-li tento problém vyřešit, nainstalujte aktualizaci společnosti Microsoft: KB3140245. Další informace naleznete zde: Nelze povolit TLS 1.1 a TLS 1.2 jako výchozí zabezpečovací protokoly ve WinHTTP v systému Windows
Poté, co klient obdrží aktualizované zásady ochrany proti hrozbám v aplikaci Endpoint pro službu AD [14.2 RU1 MP1 a novější] se v aplikaci Symantec Endpoint Protection Manager stále zobrazuje zpráva „Zavedení probíhá“.	Toto chování je běžné. Zásady aplikace Ochrana proti hrozbám v aplikaci Endpoint pro AD 3.3 jsou podporovány na straně klienta od verze 14.2 RU1 MP1. Použijete zásady ochrany proti hrozbám v aplikaci Symantec Endpoint pro službu Active Directory 3.3 na skupinu. Tato skupina obsahuje některé klienty, kteří používají aplikaci Symantec Endpoint Protection 14.2 RU1 nebo starší. Tito klienti přijímají a používají zásady podle očekávání, ale stav v aplikaci Symantec Endpoint Protection Manager stále zobrazuje zprávu Zavedení probíhá.

Table 3: Problémy s klienty systému Windows, Mac a Linux

Problém	Popis a řešení
Instalace klienta aplikace Symantec Endpoint Protection 14.3 pro systém Windows může selhat, pokud nejprve nenainstalujete podporu SHA-2 [14.3]	Pokud používáte starší verze operačního systému (Windows 7 RTM nebo SP1, Windows Server 2008 R2 nebo R2 SP1 nebo R2 SP2), je nutné mít na svých zařízeních nainstalovanou podporu podepisování kódu SHA-2, abyste mohli instalovat aktualizace systému Windows vydané od července 2019. Bez podpory SHA-2 se instalace klienta systému Windows občas nezdaří. Instalace může selhat bez ohledu na to, zda klienty instalujete poprvé nebo provádíte automatický upgrade z předchozí verze. [SEP-61175/61403] Chcete-li získat podporu podepisování kódu SHA-2 společnosti Microsoft, přečtěte si následující informace: Požadavky na podporu podepisování kódu SHA-2 od roku 2019 pro Windows a WSUS Instalace klienta Symantec Endpoint Protection 14.3 pro systém Windows může selhat, pokud není nainstalována podpora SHA-2
Klient Symantec Endpoint Protection pro systém Windows při instalaci v systému Windows 10 1803 s povolenou technologií UWF [14.3] se nespouští	Pokud je klient Symantec Endpoint Protection spuštěn v 32bitovém operačním systému Windows 10 RS4 1803, když je povolena technologie UWF (Unified Write Filter) a používá se k ochraně jednotky, na které je nainstalován klient systému Windows, nepracuje klient správně. Tento operační systém Windows obsahuje závadu UWF, která brání spuštění klienta systému Windows. Chcete-li tento problém vyřešit: • Proveďte upgrade na jinou verzi operačního systému, která neobsahuje vadu. • Zakažte UWF. Další informace: Aplikace Endpoint Protection nefunguje správně, když je nainstalovaná v systému Windows 10 1803 s povolenou technologií UWF
Klienti pro systém Mac, kteří povolují přesměrování přenosů služby WSS, nerespektují uživatelské nastavení proxy pro službu LiveUpdate [14.2 RU1 MP1 a novější]	Své spravované klienty systému Mac jste nakonfigurovali pro aplikaci Symantec Endpoint Protection 14.2 RU1 MP1 nebo novější tak, aby používali uživatelské nastavení proxy pro službu LiveUpdate pomocí možnosti Nastavení externí komunikace. Po povolení přesměrování přenosů služby WSS (WTR) pro své klienty systému Mac pomocí zásad aplikace Symantec Endpoint Protection Manager nicméně zjistíte, že přenos služby LiveUpdate nadále nerespektuje vaše uživatelské nastavení proxy. Místo toho se služba LiveUpdate pokouší o přímé připojení. Chcete-li tento problém vyřešit, použijte pouze uživatelské nastavení serveru proxy pro službu LiveUpdate při zakázaném přesměrování přenosů služby WSS.

Problém	Popis a řešení
Prohlížeč Microsoft Edge neočekávaně umožňuje stahovat soubory PDF při povoleném posílení zabezpečení [14.2 RU1 MP1 a novější]	Při použití prohlížeče Microsoft Edge můžete v klientovi Symantec Endpoint Protection s povoleným posílením zabezpečení neočekávaně stahovat soubory PDF. Při používání ostatních prohlížečů funguje prevence stahování souborů PDF očekávaným způsobem. Oprava tohoto problému bude k dispozici v další verzi.

V souvislosti nedávným oznámením společnosti Broadcom, že se společnost Symantec Enterprise Protection oficiálně připojila k společnosti Broadcom, společnost Symantec provedla migraci dokumentace na portál Broadcom Symantec Security Tech Docs Portal.

Pokud hledáte dokumentaci produktu Endpoint Protection, klikněte na kartu **Symantec Security Software** a potom na tlačítko **Endpoint Security and Management** > **Endpoint Protection**.

Table 4: Problémy s dokumentací

Problém	Popis a řešení
Články s postupy vypršely.	Články s postupy, které tvořily duplicitní témata v nápovědě aplikace Symantec Endpoint Protection Manager, byly znovu publikovány na webu Endpoint Protection a nyní mají jinou adresu URL. Chcete-li článek vyhledat, použijte **vyhledávací pole**.
Soubory PDF	Společnost Symantec zveřejnila všechny soubory PDF v článcích DOC. Platnost těchto stránek vypršela. Chcete-li najít nejnovější verzi souboru PDF, přejděte na stránku Související dokumenty. V budoucnu bude společnost Broadcom přidávat starší soubory PDF a přeložené soubory PDF.

Vyřešené problémy najdete v tématu: Nové opravy a součásti aplikace Symantec Endpoint Protection 14.3

Systémové požadavky na aplikaci Symantec Endpoint Protection (SEP)

Obecně jsou požadavky na systém následující aplikace stejné jako požadavky na operační systémy, ve kterých jsou tyto aplikace podporovány.

NOTE
Starší verze aplikace Symantec Endpoint Protection Manager nemusí být schopna správně spravovat klienta s novější verzí. Mohou nastat problémy s aktualizacemi obsahu a správou klienta.Například aplikace Symantec Endpoint Protection Manager 14.0.1 nebo starší nemůže správně poskytovat klientovi verze 14.2 jeho zástupné názvy specifické pro danou verzi. Aplikace Symantec Endpoint Protection Manager pro verze starší než 14 MP2 nemůže správně poskytovat klientům s verzí novější než 14.0.1 jejich zástupné názvy specifické pro danou verzi.

Následující tabulky obsahují požadavky na software a hardware pro aplikaci Symantec Endpoint Protection.

Table 5: Systémové požadavky softwaruSymantec Endpoint Protection Manager (SEPM)

Součást	Požadavky
Operační systém	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** Operační systémy pro stolní počítače nejsou podporovány. **Note:** Verze Windows Server Core není podporována. Verze Windows Server Core nezahrnuje prohlížeč Internet Explorer, který aplikace Symantec Endpoint Protection Manager požaduje, aby mohla fungovat.
Webový prohlížeč	Pro přístup k webové konzole aplikace Symantec Endpoint Protection Manager a zobrazení nápovědy aplikace Symantec Endpoint Protection Manager jsou podporovány následující prohlížeče: • Microsoft Edge Poznámka: 32bitová verze systému Windows 10 nepodporuje v prohlížeči Edge přístup k webové konzole. • Microsoft Internet Explorer 11 • Mozilla Firefox 5.x až 68.x • Google Chrome 75.x

Součást	Požadavky
Databáze	**Aplikace Symantec Endpoint Protection Manager obsahuje vestavěnou databázi. Místo toho můžete použít databázi z jedné z následujících verzí serveru Microsoft SQL Server:** • SQL Server 2008, SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012, RTM – SP4 • SQL Server 2014, RTM – SP3 • SQL Server 2016, RTM, SP1, SP2 • SQL Server 2017, RTM • SQL Server 2019, RTM (od verze 14.3) **Note:** Databáze verze SQL Server Express Edition není podporována. Podporovány jsou databáze SQL Server hostované ve službě Amazon RDS (od verze 14.0.1 MP2). **Note:** Pokud aplikace Symantec Endpoint Protection využívá databázi SQL Server a vaše prostředí využívá pouze protokol TLS 1.2, ověřte, zda SQL Server podporuje protokol TLS 1.2. Možná budete muset použít opravu systému SQL Server. Toto doporučení se vztahuje na SQL Server 2008, 2012, a 2014. Bez opravy systému SQL Server pro účely podpory protokolu TLS 1.2 může dojít k problémům při provádění upgradu z aplikace Symantec Endpoint Protection verze 12.1 na verzi 14. **Note:** Podpora TLS 1.2 pro Microsoft SQL Server
Další požadavky na prostředí	V sítích, kde se používá pouze protokol IPv6, musí být také nainstalován a deaktivován zásobník IPv4. Pokud je zásobník IPv4 odinstalován, nebude aplikace Symantec Endpoint Protection Manager fungovat.

Table 6: Hardwarové požadavky aplikace Symantec Endpoint Protection Manager

Součást	Požadavky
Procesor	Minimálně procesor Intel Pentium Dual-Core nebo obdobný, doporučen alespoň osmijádrový procesor **Note:** Procesory Intel Itanium IA-64 podporovány nejsou.
Fyzická paměť RAM	Minimálně 2 GB volné paměti RAM, doporučeno 8 GB nebo více **Note:** V závislosti na požadavcích ostatních již nainstalovaných aplikací na paměť RAM může server aplikace Symantec Endpoint Protection Manager vyžadovat další volnou paměť RAM. Pokud je na serveru aplikace Symantec Endpoint Protection Manager nainstalován například systém Microsoft SQL Server, mělo by být na serveru k dispozici minimálně 8 GB paměti.
Displej	1024 x 768 nebo více
Pevný disk v případě instalace na systémovou jednotku	**S vestavěnou databází nebo místní databází serveru SQL Server:** • Minimálně 40 GB volného místa (doporučeno 200 GB) pro server pro správu a databázi **Se vzdálenou databází serveru SQL Server:** • Minimálně 40 GB volného místa (doporučeno 100 GB) pro server pro správu • Další volné místo na disku vzdáleného serveru pro databázi
Pevný disk v případě instalace na alternativní jednotku:	**S vestavěnou databází nebo místní databází serveru SQL Server:** • Minimálně 15 GB volného místa na systémové jednotce (doporučeno 100 GB) • Minimálně 25 GB volného místa na instalační jednotce (doporučeno 100 GB) **Se vzdálenou databází serveru SQL Server:** • Minimálně 15 GB volného místa na systémové jednotce (doporučeno 100 GB) • Minimálně 25 GB volného místa na instalační jednotce (doporučeno 100 GB) • Další volné místo na disku vzdáleného serveru pro databázi

Pokud používáte databázi SQL Server, může být potřeba více volného místa na disku. Množství dalšího požadovaného místa a jeho umístění závisí na jednotce používané serverem SQL Server, požadavcích na údržbu databáze a dalších nastaveních databáze.

Table 7: Požadavky na systém klienta Symantec Endpoint Protection pro systém Windows

Součást	Požadavky
Operační systém (stolní počítač)	• Windows 7 (32bitová verze, 64bitová verze, RTM a SP1) • Windows Embedded 7 Standard, POSReady a Enterprise (32bitová a 64bitová verze) • Windows 8 (32bitová verze, 64bitová verze) • Windows Embedded 8 Standard (32bitová a 64bitová verze) • Windows 8.1 (32bitová verze, 64bitová verze), včetně funkce Windows To Go • Windows 8.1, aktualizace z dubna 2014 (32bitová verze, 64bitová verze) • Windows 8.1, aktualizace ze srpna 2014 (32bitová verze, 64bitová verze) • Windows Embedded 8.1 Pro, Industry Pro a Industry Enterprise (32bitová a 64bitová verze) • Windows 10 (1507) (32bitová verze, 64bitová verze), včetně systému Windows 10 Enterprise 2015 LTSB • Windows 10 November Update (1511) (32bitová verze, 64bitová verze) • Windows 10 Anniversary Update (1607) (32bitová verze, 64bitová verze), včetně systému Windows 10 Enterprise 2016 LTSB • Windows 10 Creators Update (1703) (32bitová verze, 64bitová verze) • Windows 10 Fall Creators Update (1709) (32bitová verze, 64bitová verze) • Windows 10 April 2018 Update (1803) (32bitová verze, 64bitová verze) • Windows 10, aktualizace z října 2018 (1809) (32bitová verze, 64bitová verze), včetně systému Windows 10 Enterprise 2019 LTSC • Windows 10, aktualizace z května 2019 (1903) (32bitová verze, 64bitová verze) • Windows 10, aktualizace z listopadu 2019 (1909) (32bitová verze, 64bitová verze) (14.2 RU1 a novější) • Windows 10 20H1 (Windows 10 verze 2004) (od 14.3)
Operační systém (server)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2, aktualizace z dubna 2014 • Windows Server 2012 R2, aktualizace ze srpna 2014 • Windows Server 2016 • Windows Server 2019 • Windows Server, verze 1803 (Server Core) (14.2 a novější) • Windows Server, verze 1809 (Server Core) • Windows Server, verze 1903 (Server Core) (14.2 RU1 a novější) • Windows Server, verze 1909 (Server Core) (14.2 RU1 a novější)
Prevence narušení prohlížeče	Podpora prevence narušení prohlížeče závisí na verzi systému zjištění narušení klienta (CIDS). Viz téma Supported browsers for Browser Intrusion Prevention in Endpoint Protection (Podporované prohlížeče pro prevenci narušení prohlížeče v aplikaci Endpoint Protection).

Table 8: Požadavky na systém klienta Symantec Endpoint Protection pro systém Windows

Součást	Požadavky
Procesor (fyzické počítače)	• 32bitový procesor: 2 GHz Intel Pentium 4 nebo ekvivalent (Intel Pentium 4 nebo ekvivalent) • 64bitový procesor: 2 GHz Pentium 4 s podporou x86-64 nebo ekvivalent **Note:** Nejsou podporovány procesory Itanium.
Procesor (virtuální počítače)	Minimálně jeden virtuální soket a jedno jádro na soket s frekvencí 1 GHz (doporučuje se jeden virtuální soket a dvě jádra na soket s frekvencí 2 GHz) **Note:** Je nutné povolit vyhrazení prostředků hypervisoru.
Fyzická paměť RAM	1 GB paměti (doporučeno 2 GB) nebo více, pokud to vyžaduje operační systém
Displej	800 x 600 nebo více
Pevný disk	Požadavky na místo na disku závisí na typu instalovaného klienta, instalační jednotce a umístění dat programu. Složka dat programu se obvykle nachází na systémové jednotce ve výchozím umístění C:\ProgramData. Bez ohledu na zvolenou instalační jednotku je vždy potřeba volné místo na systémové jednotce. **Požadavky na pevný disk:** • Požadavky klienta Symantec Endpoint Protection pro systém Windows na volné místo na pevném disku v případě instalace na systémovou jednotku uvádí požadavky na pevný disk v případě instalace aplikace Symantec Endpoint Protection na systémovou jednotku. • Požadavky klienta Symantec Endpoint Protection pro systém Windows na volné místo na pevném disku v případě instalace na alternativní jednotku uvádí požadavky na pevný disk v případě instalace aplikace Symantec Endpoint Protection na alternativní jednotku. **Note:** Požadavky na prostor vycházejí ze souborových systémů NTFS. Další místo je potřeba pro aktualizace obsahu a protokoly.

Table 9: Požadavky klienta Symantec Endpoint Protection pro systém Windows na volné místo na pevném disku v případě instalace na systémovou jednotku

Typ klienta	Požadavky
Standardní klient	**V případě umístění složky dat programu na systémové jednotce:** • 395 MB* **V případě umístění složky dat programu na alternativní jednotce:** • Systémová jednotka: 180 MB • Alternativní instalační jednotka: 350 MB
Klient Embedded nebo VDI	**V případě umístění složky dat programu na systémové jednotce:** • 245 MB* **V případě umístění složky dat programu na alternativní jednotce:** • Systémová jednotka: 180 MB • Alternativní instalační jednotka: 200 MB
Klient vnitřní sítě	**V případě umístění složky dat programu na systémové jednotce:** • 545 MB* **V případě umístění složky dat programu na alternativní jednotce:** • Systémová jednotka: 180 MB • Alternativní instalační jednotka: 500 MB

* Během instalace je vyžadováno dalších 135 MB místa.

Table 10: Požadavky klienta Symantec Endpoint Protection pro systém Windows na volné místo na pevném disku v případě instalace na alternativní jednotku

Typ klienta	Požadavky
Standardní klient	**V případě umístění složky dat programu na systémové jednotce:** • Systémová jednotka: 380 MB • Alternativní instalační jednotka: 15 MB* **V případě umístění složky dat programu na alternativní jednotce:**** • Systémová jednotka: 30 MB • Jednotka se složkou dat programu: 350 MB • Alternativní instalační jednotka: 150 MB
Klient Embedded nebo VDI	**V případě umístění složky dat programu na systémové jednotce:** • Systémová jednotka: 230 MB • Alternativní instalační jednotka: 15 MB* **V případě umístění složky dat programu na alternativní jednotce:**** • Systémová jednotka: 30 MB • Jednotka se složkou dat programu: 200 MB • Alternativní instalační jednotka: 150 MB
Klient vnitřní sítě	**V případě umístění složky dat programu na systémové jednotce:** • Systémová jednotka: 530 MB • Alternativní instalační jednotka: 15 MB* **V případě umístění složky dat programu na alternativní jednotce:**** • Systémová jednotka: 30 MB • Jednotka se složkou dat programu: 500 MB • Alternativní instalační jednotka: 150 MB

* Během instalace je vyžadováno dalších 135 MB místa.

** Pokud se složka dat programu nachází na alternativní instalační jednotce, připočítejte v celkovém součtu 15 MB k jednotce se složkou dat programu. Instalační program však bude během instalace stále potřebovat 150 MB volného místa na alternativní instalační jednotce.

Table 11: Požadavky na systém klienta Symantec Endpoint Protection pro systém Windows Embedded

Součást	Požadavky
Procesor	Intel Pentium 1 GHz
Fyzická paměť RAM	256 MB **Note:** Tato cifra je určena pro instalaci vloženého klienta Symantec Endpoint Protection. Pokud současně implementujete dodatečné funkce z integrovaného řešení, jako je služba EDR, může být zapotřebí více fyzické paměti RAM.
Pevný disk	Klient Symantec Endpoint Protection Embedded a VDI vyžaduje následující množství volného místa na pevném disku: • V případě instalace na systémovou jednotku: 245 MB • V případě instalace na alternativní jednotku: 230 MB na systémové jednotce a 15 MB na alternativní jednotce Během instalace je potřeba dalších 135 MB místa. Tyto údaje předpokládají umístění složky dat programu na systémové jednotce. Podrobnější informace a požadavky jiných typů klientů naleznete v požadavcích na systém klienta Symantec Endpoint Protection pro systém Windows.

Součást	Požadavky
Operační systém Embedded	• Windows Embedded Standard 7 (32bitová a 64bitová verze) • Windows Embedded POSReady 7 (32bitová a 64bitová verze) • Windows Embedded Enterprise 7 (32bitová a 64bitová verze) • Windows Embedded 8 Standard (32bitová a 64bitová verze) • Windows Embedded 8.1 Industry Pro (32bitová a 64bitová verze) • Windows Embedded 8.1 Industry Enterprise (32bitová a 64bitová verze) • Windows Embedded 8.1 Pro (32bitová a 64bitová verze)
Minimální požadované součásti systému	• Správce filtrů (FltMgr.sys) • Podpora sledování výkonu (pdh.dll) • Instalační služba systému Windows
Šablony	• Application Compatibility (výchozí) • Digital Signage • Industrial Automation • IE, Media Player, RDP • Set Top Box • Thin Client Šablona Minimum Configuration není podporována. Sjednocený filtr zápisu (UWF) ani rozšířený filtr zápisu (EWF) nejsou podporovány. Doporučuje se, aby souborový filtr zápisu (FBWF) byl nainstalován spolu s filtrem registru.

Table 12: Požadavky na systém klienta Symantec Endpoint Protection pro systém Mac

Součást	Požadavky
Procesor	64bitový procesor Intel Core 2 Duo nebo novější
Fyzická paměť RAM	2 GB paměti RAM
Pevný disk	500 MB volného místa na pevném disku pro instalaci
Displej	800 x 600
Operační systém	• macOS 10.13 • macOS 10.14 • macOS 10.15 až 10.15.5 macOS 10.14.5 a novější podporují požadavky na notářskou úpravu kext. Viz Endpoint Protection 14.2 RU1 a notarizace kext pro systém macOS 10.14.5. Seznam podporovaných operačních systémů u předchozích vydání najdete v tématu Kompatibilita počítače Mac s klientem Endpoint Protection

Table 13: Požadavky na systém klienta Symantec Endpoint Protection pro systém Linux

Součást	Požadavky
Hardware	• Procesor Intel Pentium 4 (2 GHz) nebo novější • 1 GB paměti RAM • 7 GB volného místa na pevném disku
Operační systémy	• Amazon Linux • CentOS 6U3–6U9, 7–7U7, 8; 32bitová a 64bitová verze • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32bitová a 64bitová verze • Fedora 16, 17; 32bitová a 64bitová verze • 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, 32bitová a 64bitová verze; 12, 12 SP1, 12 SP3, 64bitová verze • SUSE Linux Enterprise Desktop (SLED) 11 SP1 – 11 SP4, 32bitová a 64bitová verze; 12 SP3, 64bitová verze • Ubuntu 12.04, 14.04, 16.04, 18.04 (od verze 14.3); 32bitová a 64bitová verze Seznam podporovaných jader operačních systémů u předchozích vydání najdete v tématu Supported Linux kernels for Symantec Endpoint Protection (Podporovaná jádra systému Linux pro aplikaci Symantec Endpoint Protection).
Grafická počítačová prostředí	K zobrazení klienta Symantec Endpoint Protection pro systém Linux můžete použít následující grafická prostředí: • KDE • Gnome • Unity

Další požadavky na prostředí	• Glibc
	Nejsou podporovány operační systémy, které používají knihovnu glibc verze 2.6 nebo starší.
	• Závislé balíčky i686 na 64bitových počítačích
	Řada spustitelných souborů v klientovi pro systém Linux jsou 32bitové programy. U 64bitových počítačů je třeba před instalací klienta pro systém Linux nainstalovat závislé balíčky i686.
	Pokud jste závislé balíčky i686 ještě nenainstalovali, můžete tak učinit z příkazového řádku. Tato instalace vyžaduje oprávnění superuživatele, jak ukazují následující příkazy `sudo`:
	– Distribuce založené na systému Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Distribuce založené na systému Debian: `sudo apt-get install ia32-libs`
	– Distribuce založené na systému Ubuntu:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`
	• net-tools nebo iproute2
	Aplikace Symantec Endpoint Protection používá jeden z těchto nástrojů podle toho, který je již nainstalován v počítači.
	• Vývojářské nástroje
	Funkce automatické kompilace a ruční kompilace modulu jádra funkce Auto-Protect vyžadují instalaci určitých nástrojů pro vývojáře. Mezi tyto vývojářské nástroje patří gcc, zdrojový kód jádra a hlavičkové soubory. Podrobné informace o tom, co a jak je třeba instalovat pro konkrétní verze systému Linux, naleznete v dokumentu:
	Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux (Ruční kompilace modulů jádra funkce Auto-Protect aplikace Endpoint Protection pro systémy Linux)

Poznámky k verzi a systémové požadavky pro všechny verze aplikace Symantec Endpoint Protection

Podporované možnosti upgradu na nejnovější verzi aplikace Symantec Endpoint Protection 14.x

NOTE

V případě verzí aplikace Symantec Endpoint Protection starších, než je nejnovější verze, je zpravidla podporována každá verze před touto verzí uvedená v seznamu. Tuto možnost byste si však měli u své konkrétní verze ověřit v poznámkách k verzi.

Poznámky k verzi, nové opravy a systémové požadavky pro všechny verze aplikace Endpoint Protection

Aplikace Symantec Endpoint Protection Manager a klient pro systém Windows

Následující verze aplikace Symantec Endpoint Protection Manager a klienta Symantec Endpoint Protection pro systém Windows lze upgradovat přímo na aktuální verzi:

- 11.x a Small Business Edition 12.0 (pouze klienti aplikace Symantec Endpoint Protection, v podporovaných operačních systémech)
- 12.1.x, až do verze 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

Klient pro systém Mac

Následující verze klienta Symantec Endpoint Protection pro systém Mac lze upgradovat přímo na aktuální verzi:

- 12.1.4 – 12.1.6 MP9
  Klient systému Mac nebyl aktualizován na verzi 12.1.6 MP10.
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

NOTE

Klient Symantec Endpoint Protection pro systém Mac nebyl aktualizován na verzi 14.0.1 MP2.

Klient pro systém Linux

Následující verze klienta Symantec Endpoint Protection pro systém Linux lze upgradovat přímo na aktuální verzi:

- 12.1.x, až do verze 12.1.6 MP9
  Klient systému Linux nebyl aktualizován na verzi 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

Aplikace Symantec AntiVirus pro systém Linux 1.0.14 je jediná verze, kterou můžete převést přímo na aplikaci Symantec Endpoint Protection. Nejprve je třeba odinstalovat všechny ostatní verze aplikace Symantec AntiVirus pro systém Linux. Nelze převést spravovaného klienta na nespravovaného.

Nepodporované cesty upgradu

Migraci do produktu Symantec Endpoint Protection nelze provádět ze všech produktů společnosti Symantec. Před instalací klienta aplikace Symantec Endpoint Protection je nutné odinstalovat následující produkty:

- Nepodporované produkty společnosti Symantec: Symantec AntiVirus a Symantec Client Security
- Všechny produkty Symantec Norton™
- Aplikace Symantec Endpoint Protection pro systém Windows XP Embedded 5.1
- Všechny verze aplikace Symantec Endpoint Protection pro systém Mac do verze 12.1.4

Aplikaci Symantec Endpoint Protection Manager 11.0.x nebo Symantec Endpoint Protection Manager Small Business Edition 12.0.x nelze přímo upgradovat na žádnou verzi aplikace Symantec Endpoint Protection Manager 14. Nejprve je nutné tyto verze odinstalovat nebo provést upgrade na verzi 12.1.x a teprve poté na verzi 14.x.

Aplikaci Symantec Endpoint Protection Manager 12.1.6 MP7 nelze upgradovat na verzi 14, protože verze schématu databáze ve verzi 12.1.6 MP7 je novější než ve verzi 14. Z verze 12.1.6 MP7 je nutné upgradovat na verzi 14 MP1 nebo novější.

Upgrade z verze 14 MP1 (14.0.2332.0100) na verzi 14 MP1 Refresh Build (14.0.2349.0100) není podporován.

Downgrade není povolen. Pokud například chcete přejít z aplikace Symantec Endpoint Protection 14.2.1.1 na verzi 12.1.6 MP10, je nejprve nutné aplikaci Symantec Endpoint Protection MP14.2.1.1 odinstalovat.

Pokud máte číslo sestavení, ale nejste si jistí, o jakou verzi vydání se jedná, viz:

- Vydané verze aplikace Symantec Endpoint Protection
- Informace o typech a verzích vydání aplikace Endpoint Protection

Další zdroje informací

Informace o aplikaci Endpoint Protection zobrazují webové stránky, na kterých se nachází osvědčené postupy, informace o řešení potíží a další zdroje, které vám pomohou s použitím produktu.

Table 14: Informace o webu aplikace Endpoint Protection

Typ informací	Odkaz na webové stránky
Zkušební verze	Obraťte se na zástupce účtu.
Aktuální příručky a dokumentace	• Produktové příručky pro nejnovější verzi (anglicky) • Produktové příručky pro nejnovější verzi (jiné jazyky) • Příručky ke všem verzím aplikace Symantec Endpoint Protection 14.x (anglicky) **Ostatní jazyky:**
Technická podpora	Technická podpora aplikace Endpoint Protection Obsahuje články databáze znalostí, podrobné informace k vydání produktu, aktualizace a opravy a kontakty na podporu.
Informace a novinky o hrozbách	Symantec Security Center
Školení	Education Services Přístup k výukovým kurzům, knihovně eLibrary a dalším zdrojům
Fóra Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom