Uwagi o wydaniu programu Symantec™ Endpoint Protection 14.3

Ostatnia aktualizacja: czerwiec 2020 r.

Table of Contents

Informacja o prawach autorskich

Nowości w programie Symantec Endpoint Protection 14.3?

W tej sekcji opisano nowe funkcje wersji 14.3.

Funkcje ochrony

- Deweloperzy aplikacji innych firm mogą chronić swoich klientów przed dynamicznym złośliwym oprogramowaniem opartym na skryptach i przed nietradycyjnymi sposobami cyberataku.Aplikacja innej firmy wywołuje interfejs AMSI systemu Windows, aby zażądać skanowania skryptu dostarczonego przez użytkownika, który jest kierowany do klienta programu Symantec Endpoint Protection. Klient odpowiada werdyktem, aby wskazać, czy zachowanie skryptu jest złośliwe. Jeśli zachowanie nie jest złośliwe, wówczas wykonanie skryptu postępuje. Jeśli zachowanie skryptu jest złośliwe, aplikacja nie uruchamia go.Na kliencie w oknie dialogowym Wyniki wykrywania wyświetlany jest stan „Odmowa dostępu".Przykłady skryptów innych firm obejmują programy Windows PowerShell, JavaScript i VBScript. Funkcja Auto-Protect musi być włączona. Ta funkcja działa na komputerach z systemem Windows 10 i nowszych.
  Jak Interfejs skanowania złośliwego oprogramowania (AMSI) pomaga chronić przed złośliwym oprogramowaniem
  Interfejs skanowania złośliwego oprogramowania (AMSI)

Symantec Endpoint Protection Manager

- Konsola zdalna programu Symantec Endpoint Protection obsługuje teraz technologię Java 11 zamiast Java 8.Aby uzyskać dostęp do konsoli zdalnej, otwórz obsługiwaną przeglądarkę internetową i wpisz w polu adresu następujący adres: `http://SEPMServer:9090/symantec.html` i pobierz nowy pakiet konsoli zdalnej. Wykonaj wymienione instrukcje. Poprzednia wersja konsoli zdalnej programu Symantec Endpoint Protection Manager nie jest już obsługiwana.
  Logowanie do programu Symantec Endpoint Protection
- Można skonfigurować jeden z menedżerów programu Symantec Endpoint Protection w lokacji jako główny serwer rejestrowania do przekazywania dzienników do serwera syslog. Jeśli główny serwer rejestrowania przejdzie w tryb offline, drugi serwer zarządzania przejmuje i przekazuje dzienniki do serwera syslog. Gdy główny serwer rejestrowania powraca do trybu online, wznawia przekazywanie dzienników.
  Konfigurowanie serwera przełączania awaryjnego do rejestrowania zewnętrznego
- Zasady integracji mają nową opcję dla Przekierowania ruchu sieciowego WSS, **Włącz niestandardowy plik PAC LPS**.Ta opcja umożliwia zastąpienie domyślnego pliku PAC hostowanego przez serwer LPS na kliencie z niestandardowym plikiem PAC. Niestandardowy plik PAC rozwiązuje problemy ze zgodnością z aplikacjami innych firm, które nie działają z lokalnym serwerem proxy nasłuchującym z karty pętli zwrotnej.
  Konfiguracja przekierowania ruchu sieciowego WSS
- Obsługa bazy danych programu Microsoft SQL Server 2019.
- Proces skanowania antywirusowego używa teraz usługi oddzielnej od głównej usługi niezwiązanej z zabezpieczeniami. Ten nowy proces skanowania zapewnia bardziej efektywne użycie pamięci, ciągłą ochronę i mniejszą zależność od problemów z usługą główną.
- Schemat bazy danych zawiera nowe kolumny jako część funkcji dla przyszłej wersji. (AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2, SEM_AGENT tables)
- Interfejs Rest API zawiera następujące pola odpowiedzi interfejsu API /sepm/api/v1/computers JSON do wywołania i pobrania raportu o stanie komputera: quarantineStatus, quarantineCode, wssStatus, pskVersion.
- Uaktualniono następujące składniki innych firm do nowszych wersji: Apache Tomcat, Boost C++ Libraries, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, sterownik JDBC Microsoft SQL Server, OpenSC, OpenSSL, Spring Security, spring-framework, sqlite.
- Aby zarejestrować domenę menedżera Symantec Endpoint Protection w konsoli w chmurze, należy najpierw uzyskać token rejestracji za pośrednictwem konsoli Symantec Endpoint Protection. Wcześniej uzyskasz token rejestracji, klikając przycisk **Zacznijmy** na stronie **Chmury**.

Aktualizacje klientów i platform

- Klient systemu Windows obsługuje system Windows 10 20H1 (Windows 10 wersja 2004)
- Klient Linux obsługuje teraz Ubuntu 18.04, RHEL 8 i CentOS 8.
- Narzędzie AppRemover zostało zaktualizowane do nowszej wersji.Narzędzie AppRemover usuwa aplikacje innych firm przed zainstalowaniem klienta systemu Windows.Aby uzyskać więcej informacji na temat aplikacji, które są usuwane, zobacz: Usuwanie oprogramowania zabezpieczającego innych firm w programie Endpoint Protection 14.3

Funkcje usunięte

- Następujące powiadomienia: Infekcja zagrożeniami, Pojedyncze zdarzenie zagrożenia, Wykryto nowe zagrożenie nie wyświetlają już pól: **Nasilenie ryzyka** i **Typ ryzyka**.

Nowości we wszystkich wersjach programu Symantec Endpoint Protection

Znane problemy i ich rozwiązania

Zagadnienia w tej sekcji dotyczą bieżącej wersji programu Symantec Endpoint Protection.

Table 1: Problemy z uaktualnieniem

Problem	Opis i rozwiązanie
Uaktualnienie programu SQL Server z wersji 2017 do wersji 2019 kończy się niepowodzeniem z włączonym trybem FIPS [14.3]	Może zostać wyświetlony błąd: „Wystąpił następujący błąd". Wystąpił błąd podczas instalowania funkcji rozszerzalności z komunikatem o błędzie: utworzenie aplikacji AppContainer nie powiodło się z komunikatem o błędzie BRAK, stan. Ta implementacja nie jest częścią algorytmów kryptograficznych zweryfikowanych przez platformę Windows FIPS. Dzieje się tak, jeśli włączono tryb FIPS programu Symantec Endpoint Protection Manager 14.3 i dokonano aktualizacji z programu Microsoft SQL Server 2017 do 2019.[SEP-61473] Aby uniknąć tego problemu, wyłącz tryb FIPS na poziomie systemu operacyjnego: 1. W `C:\ProgramData\Microsoft\Windows\Menu Start\Programy \Narzędzia administracyjne` kliknij pozycję **Lokalne zasady zabezpieczeń** > **Zasady lokalne** > **Opcje zabezpieczeń** i wyłącz **Kryptografię systemu: Użyj algorytmów zgodnych ze standardem FIPS do szyfrowania, mieszania i podpisywania** 2. Uaktualnienie z programu SQL Server w wersji 2017 do wersji 2019. 3. Po pomyślnym uaktualnieniu programu SQL Server ponownie włącz tryb FIPS. Uaktualnienie SQL z 2017 do 2019 kończy się niepowodzeniem z włączonym trybem FIPS
Niestandardowe nazwy mogą uniemożliwiać aktualizację zasad zapory podczas uaktualniania programu do wersji 14.2 lub nowszej	W przypadku uaktualniania programu Symantec Endpoint Protection do wersji 14.2 lub nowszej, zasady zapory nie mogą uwzględniać zmian w przypadku adresów IPv6, jeśli niektóre nazwy domyślne zostały zmienione. Nazwy domyślne obejmują nazwy zasad domyślnych i nazwy reguł domyślnych. Jeśli reguł nie można zaktualizować podczas uaktualniania oprogramowania, opcje IPv6 nie są wyświetlane. Nie dotyczy to żadnych nowych reguł lub zasad tworzonych po uaktualnieniu. Jeśli to możliwe, należy przywrócić wszystkie nazwy domyślne. W przeciwnym razie należy się upewnić, że żadne reguły niestandardowe dodane do zasady domyślnej nie blokują komunikacji IPv6. Analogiczne działania należy podjąć w przypadku wszystkich nowych dodawanych zasad lub reguł.

Table 2: Problemy dotyczące programu Symantec Endpoint Protection Manager

Problem	Opis i rozwiązanie
Można umieścić dodatkowe adresy URL na białej liście w programie Symantec Endpoint Security, jeśli zostanie wybrana opcja zarządzania hybrydowego i serwery proxy [14.2.2.1 lub nowszych]	Wraz z niedawnym przejęciem przez Broadcom firmy Symantec Enterprise Security adresy URL komunikacji klient-chmura uległy zmianie w 14.2.2.1.[CDM-42467] Należy uaktualnić klientów do wersji kompilacji 14.2.5569.2100 lub nowszej w następującej sytuacji • Program Symantec Endpoint Security służy do zarządzania klientami i zasadami podczas rejestrowania lokalnych domen programu Symantec Endpoint Protection Manager w konsoli w chmurze • Serwery proxy są używane. Aby wpisać adresy URL na białą listę w pełni zarządzanych w chmurze lub hybrydowo zarządzanych agentach, należy umieścić je na białej liście w programie Symantec Endpoint Security: 1. W programie Symantec Endpoint Security przejdź do pozycji **Endpoint > Zasady > [nazwa zasady] Zasada listy dozwolonych**. 2. W obszarze Zasada listy dozwolonych obok pozycji **Wykluczone według domeny**wybierz pozycję **Dodaj**, dodaj po jednym naraz następujące adresy URL i wybierz pozycję **Dodaj**: `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (dodaj, jeśli posiadasz urządzenia w Europie). Zachowaj spoc.norton.com, jeśli kontynuujesz zarządzanie klientami w nowszej wersji. 3. Wybierz pozycję **Zapisz zasady**, a następnie pozycję **Tak**, aby zaktualizować zasadę i zastosować ją do istniejących grup. Zobacz Adresy URL do uwzględnienia na liście dozwolonych programu Symantec Endpoint Security. Zobacz Uaktualnianie agentów zarządzanych w chmurze firmy Symantec do wersji 14.2 RU2 MP1 lub nowszych do 4 maja 2020 r.
Konsola zdalna programu Symantec Endpoint Protection Manager nie obsługuje już 32-bitowej platformy Windows [14.3]	Od wersji 14.3 nie można zalogować się do konsoli zdalnej programu Symantec Endpoint Protection Manager, jeśli pracuje się na 32-bitowej wersji systemu Windows. Środowisko Oracle Java SE Runtime nie obsługuje już 32-bitowych wersji systemu Microsoft Windows. [SEP-61106] Jeśli zostanie wyświetlony następujący komunikat, zaloguj się lokalnie do programu Symantec Endpoint Protection Manager: „Ta wersja programu C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe nie jest zgodna z używanym systemem Windows. Sprawdź informacje o systemie komputera, a następnie skontaktuj się z wydawcą oprogramowania.” Logowanie do programu Symantec Endpoint Protection Manager
Podczas instalowania programu Symantec Endpoint Protection Manager [14.3] wyświetlony jest błąd „Niepowodzenie instalacji środowiska Microsoft Visual C++ Runtime”	Podczas instalowania programu Symantec Endpoint Protection Manager w systemie Windows 2012 R2 może wystąpić następujący błąd: „Nie można zainstalować środowiska Microsoft Visual C++ Runtime” [SEP-60396] Aby uniknąć tego problemu, należy aktywować system Windows i zainstalować aktualizacje systemu Windows. Aktualizacja systemu Windows instaluje redystrybucyjny program Visual C++ 2017, który jest niezbędny do instalacji programu Symantec Endpoint Protection Manager 14.3 w systemie Windows 2012 R2.

Problem	Opis i rozwiązanie
Aktualizuj, aby umożliwić włączenie protokołów TLS 1.1 i TLS 1.2 jako domyślnych bezpiecznych protokołów w WinHTTP w systemie Windows [14.3]	Po zainstalowaniu lub uaktualnieniu do programu Symantec Endpoint Protection Manager w wersji 14.3, która jest zarejestrowana w konsoli w chmurze, serwer zarządzania nie przekazuje już pomyślnie dzienników do chmury. W pliku uploader.log może pojawić się następujący błąd: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Ten problem jest spowodowany brakującą aktualizacją systemu Microsoft, która zapewnia obsługę protokołu TLS 1.1 i 1.2. W celu rozwiązania tego problemu należy zainstalować aktualizację systemu Microsoft: KB3140245. Więcej informacji: Aktualizuj, aby umożliwić włączenie protokołów TLS 1.1 i TLS 1.2 jako domyślnych bezpiecznych protokołów w WinHTTP w systemie Windows
Komunikat „Wdrażanie w toku” wciąż pojawia się w programie Symantec Endpoint Protection Manager, gdy klient otrzyma aktualizowane zasady dla programu Endpoint Threat Defense dla usługi AD [14.2 RU1 MP1 i nowsze wersje]	Jest to oczekiwany sposób działania. Zasady programu Endpoint Threat Defense 3.3 dla usługi AD są obsługiwane tylko w wersji klienta 14.2 RU1 MP1 lub nowszej. Zastosuj zasadę dla programu Symantec Endpoint Threat Defense for Active Directory 3.3 do grupy. Grupa zawiera klienty używające programu Symantec Endpoint Protection w wersji 14.2 RU1 lub starszej. Takie klienty poprawnie otrzymują i stosują zasady, ale ich status w programie Symantec Endpoint Protection Manager nadal zawiera komunikat Wdrażanie w toku.

Table 3: Problemy z klientami systemu Windows, Mac i Linux

Problem	Opis i rozwiązanie
Instalacja klienta systemu Windows programu Symantec Endpoint Protection 14.3 może zakończyć się niepowodzeniem, chyba że po raz pierwszy zostanie zainstalowana obsługa programu SHA-2 [14.3]	W przypadku uruchamiania starszych wersji systemu operacyjnego (Windows 7 RTM lub SP1, Windows Server 2008 R2 lub R2 SP1 lub R2 SP2) wymagana jest zainstalowana na urządzeniach obsługa podpisywania kodu SHA-2 w celu zainstalowania aktualizacji systemu Windows wydanych w lipcu 2019 r. lub później. Bez obsługi algorytmu SHA-2 instalacja klienta systemu Windows czasami kończy się niepowodzeniem. Instalacja może zakończyć się niepowodzeniem, niezależnie od tego, czy klienty zostaną zainstalowane po raz pierwszy, czy automatycznie uaktualnione z poprzedniej wersji.[SEP-61175/61403] Aby uzyskać egzekwowaną przez firmę Microsoft obsługę podpisywania kodu SHA-2, zobacz: 2019 Wymagania dotyczące obsługi podpisywania kodu SHA-2 dla systemów Windows i WSUS Instalacja klienta systemu Windows programu Symantec Endpoint Protection 14.3 może zakończyć się niepowodzeniem, chyba że zainstalowana jest obsługa algorytmu SHA-2
Klient systemu Windows programu Symantec Endpoint Protection nie jest uruchamiany po zainstalowaniu w systemie Windows 10 1803 z włączoną funkcją UWF [14.3]	Jeśli klient programu Symantec Endpoint Protection działa w 32-bitowym systemie operacyjnym Windows 10 RS4 1803 po włączeniu ujednoliconego filtru zapisu (UWF) i przy ochronie dysku, na którym jest zainstalowany klient systemu Windows, klient nie działa poprawnie. Ten system operacyjny Windows zawiera wadę UWF, która uniemożliwia uruchomienie klienta systemu Windows. Aby uniknąć tego problemu: • Uaktualij do innej wersji systemu operacyjnego, która nie zawiera wady. • Wyłącz UWF.Zobacz: Program Endpoint Protection działa nieprawidłowo po zainstalowaniu w systemie Windows 10 1803 z włączoną obsługą UWF

Problem	Opis i rozwiązanie
Klienty Mac, które włączają przekierowanie ruchu sieciowego WSS, nie stosują się do ustawień niestandardowych serwera proxy dla usługi LiveUpdate [14.2 RU1 MP1 i nowsze wersje]	Skonfigurowano zarządzane klienty Mac dla programu Symantec Endpoint Protection 14.2 RU1 MP1 lub nowszego w celu używania ustawień niestandardowych serwera proxy dla usługi LiveUpdate poprzez ustawienia komunikacji zewnętrznej. Jednak po włączeniu przekierowania ruchu sieciowego WSS (WTR) w klientach Mac za pośrednictwem zasady programu Symantec Endpoint Protection Manager, ruch sieciowy usługi LiveUpdate nie stosuje się już do ustawień niestandardowych serwera proxy. Zamiast tego usługa LiveUpdate próbuje nawiązać bezpośrednie połączenie. Aby obejść ten problem, należy używać ustawień niestandardowych serwera proxy dla usługi LiveUpdate tylko, gdy przekierowanie ruchu sieciowego WSS jest wyłączone.
Przeglądarka Microsoft Edge nieoczekiwanie zezwala na pobieranie plików PDF z włączonym Zabezpieczaniem [14.2 RU1 MP1 i nowsze wersje]	Po włączeniu funkcji Zabezpieczania aplikacji w kliencie Symantec Endpoint Protection można nieoczekiwanie pobierać pliki PDF przy użyciu przeglądarki Microsoft Edge. Zapobieganie pobieraniu plików PDF działa poprawnie w innych przeglądarkach. Poprawka tego problemu jest planowana w przyszłym wydaniu.

Z niedawnym ogłoszeniem Broadcom, że firma Symantec Enterprise Protection oficjalnie dołączyła do Broadcom, firma Symantec przeniosła dokumentację do portalu Broadcom Symantec Security Tech Docs Portal.

Aby znaleźć dokumentację programu Endpoint Protection, kliknij kartę **Oprogramowanie zabezpieczające firmy Symantec**, a następnie kliknij pozycję **Zabezpieczenia i zarządzanie programu Endpoint** > **Endpoint Protection**.

Table 4: Problemy dotyczące dokumentacji

Problem	Opis i rozwiązanie
Artykuły HOWTO wygasły.	Artykuły HOWTO, które były duplikatami tematów w Pomocy programu Symantec Endpoint Protection Manager, zostały ponownie opublikowane w witrynie Endpoint Protection i mają teraz inny adres URL. W celu wyszukania artykułu, użyj pola **Wyszukaj**.
Pliki PDF	Symantec opublikował wszystkie pliki PDF w artykułach DOC. Te strony wygasły. Aby znaleźć najnowszą wersję pliku PDF, przejdź do strony Dokumenty pokrewne. W przyszłości firma Broadcom doda starsze i przetłumaczone pliki PDF.

Aby sprawdzić problemy rozwiązane, zobacz: Nowe poprawki i składniki programu Symantec Endpoint Protection 14.3

Wymagania systemowe programu Symantec Endpoint Protection dla (SEP)

Wymagania systemowe dla poniższych produktów są przeważnie takie same, jak systemów operacyjnych, na których są obsługiwane.

NOTE
Wcześniejsza wersja programu Symantec Endpoint Protection Manager może nie być w stanie poprawnie zarządzać klientem w nowszej wersji. Mogą wystąpić problemy z aktualizacjami zawartości i zarządzaniem klientami.Na przykład program Symantec Endpoint Protection Manager 14.0.1 lub wcześniejszy nie może poprawnie dostarczać klientowi w wersji 14.2 swoich specyficznych dla wersji monikerów. Program Symantec Endpoint Protection Manager dla wersji wcześniejszych niż 14 MP2 nie może poprawnie dostarczać wersji klienta wersji późniejszych niż 14.0.1 z ich specyficznymi dla wersji monikerami.

W poniższych tabelach opisano wymagania dotyczące oprogramowania i sprzętu dla programu Symantec Endpoint Protection.

Table 5: Wymagania systemowe oprogramowania programu Symantec Endpoint Protection Manager (SEPM)

Składnik	Wymagania
System operacyjny	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** Systemy operacyjne dla komputerów stacjonarnych nie są obsługiwane. **Note:** Wersja Windows Server Core nie jest obsługiwana. System Windows Server Core nie obejmuje przeglądarki internetowej Internet Explorer, której do działania wymaga program Symantec Endpoint Protection Manager.
Przeglądarka internetowa	Następujące przeglądarki są obsługiwane pod względem dostępu internetowego z konsoli do programu Symantec Endpoint Protection Manager oraz do wyświetlania Pomocy Symantec Endpoint Protection Manager: • Microsoft Edge Uwaga: System Windows w wersji 32-bitowej nie obsługuje dostępu konsoli internetowej w przeglądarce Edge. • Microsoft Internet Explorer 11 • Mozilla Firefox 5.x do wersji 68.x • Google Chrome 75.x

Składnik	Wymagania
Baza danych	**Program Symantec Endpoint Protection Manager zawiera wbudowaną bazę danych. Można również używać bazy danych z jednej z następujących wersji programu 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 wersji 14.3) **Note:** Baza danych programu SQL Server Express Edition nie jest obsługiwana.Obsługiwane są bazy danych serwera SQL hostowane w serwisie Amazon RDS (od wersji 14.0.1 MP2). **Note:** Jeśli Symantec Endpoint Protection wykorzystuje bazę danych SQL Server i środowisko użytkownika wykorzystuje tylko TLS 1.2; upewnij się, że SQL Server obsługuje TLS 1.2. Może być konieczna instalacja poprawki do programu SQL Server. To zalecenie dotyczy SQL Server 2008, 2012 i 2014.Bez poprawki do SQL Server obsługującej TLS 1.2, podczas uaktualnienia z Symantec Endpoint Protection 12.1 do 14 mogą wystąpić problemy. **Note:** Obsługa protokołu TLS 1.2 dla programu Microsoft SQL Server
Inne wymagania dotyczące środowiska	Stos IPv4 musi być nadal zainstalowany i wyłączony tylko w sieciach IPv6. Po odinstalowaniu stosu IPv4 program Symantec Endpoint Protection Manager nie działa.

Table 6: wymagania systemowe oprogramowania Symantec Endpoint Protection Manager

Składnik	Wymagania
Procesor	Intel Pentium Dual-Core lub równoważny, zalecany co najmniej 8-rdzeniowy procesor **Note:** Procesory Intel Itanium IA-64 nie są obsługiwane.
Fizyczna pamięć RAM	Minimum 2 GB dostępnej pamięci RAM, zalecane 8 GB lub więcej **Note:** Serwer Symantec Endpoint Protection Manager może wymagać dodatkowej pamięci RAM w zależności od wymogów innych, już zainstalowanych aplikacji.Na przykład, jeśli program Microsoft SQL Server jest zainstalowany na serwerze Symantec Endpoint Protection Manager, to serwer powinien mieć co najmniej 8 GB wolnego miejsca w pamięci.
Wyświetlacz	1024 x 768 lub więcej
Dysk twardy podczas instalowania na dysku systemowym	**W przypadku wbudowanej bazy danych lub lokalnej bazy danych programu SQL Server:** • Co najmniej 40 GB dostępnego miejsca (zalecane 200 GB) dla serwera zarządzania i bazy danych **Ze zdalną bazą danych programu SQL Server:** • Co najmniej 40 GB dostępnego miejsca (zalecane 100 GB) dla serwera zarządzania. • Dodatkowe miejsce na dysku serwera zdalnego dla bazy danych
Miejsce na dysku w przypadku instalowania programu na innym dysku:	**W przypadku wbudowanej bazy danych lub lokalnej bazy danych programu SQL Server:** • Minimum 15 GB dostępnego miejsca (zalecane 100 GB) na dysku systemowym • Minimum 25 GB dostępnego miejsca (zalecane 100 GB) na dysku instalacji **Ze zdalną bazą danych programu SQL Server:** • Minimum 15 GB dostępnego miejsca (zalecane 100 GB) na dysku systemowym • Minimum 25 GB dostępnego miejsca (zalecane 100 GB) na dysku instalacji • Dodatkowe miejsce na dysku serwera zdalnego dla bazy danych

Jeśli używana jest baza danych SQL Server, może być konieczne zwolnienie dodatkowego miejsca na dysku. Ilość i lokalizacja dodatkowego miejsca na dysku zależy od dysków używanych przez SQL Server, wymagań dotyczących konserwacji bazy danych oraz innych ustawień bazy danych.

Table 7: Wymagania systemowe dotyczące programu Symantec Endpoint Protection klienta systemu Windows

Składnik	Wymagania
System operacyjny (komputery stacjonarne)	• Windows 7 (32-bitowy, 64-bitowy, RTM i SP1) • Windows Embedded 7 Standard, POSReady i Enterprise (32- i 64-bitowy) • Windows 8 (32-bitowy, 64-bitowy) • Windows Embedded 8 Standard (32- i 64-bitowy) • Windows 8.1 (32-bitowy, 64-bitowy), włącznie z funkcją Windows To Go • Windows 8.1, aktualizacja z kwietnia 2014 (32-bitowy, 64-bitowy) • Windows 8.1, aktualizacja z sierpnia 2014 (32-bitowy, 64-bitowy) • Windows Embedded 8.1 Pro, Industry Pro, Industry Enterprise (wersje 32- i 64-bitowe) • Windows 10 (1507) (wersje 32- i 64-bitowe), włącznie z wersją Windows 10 Enterprise 2015 LTSB • Windows 10 November Update (1511) (wersje 32- i 64-bitowe) • Windows 10 Anniversary Update (1607) (wersje 32- i 64-bitowe), włącznie z wersją Windows 10 Enterprise 2016 LTSB • Windows 10 Creators Update (1703) (wersje 32- i 64-bitowe) • Windows 10 Fall Creators Update (1709) (wersje 32- i 64-bitowe) • Windows 10 April 2018 Update (1803) (wersje 32- i 64-bitowe) • Windows 10 October 2018 Update (wersja 1809) (wersje 32- i 64-bitowe), w tym Windows 10 Enterprise 2019 LTSC. • Windows 10 May 2019 Update (wersja 1903) (wersje 32- i 64-bit) • Windows 10 November Update 2019 (wersja 1909) (wersje 32- i 64-bitowe) (14.2 RU1 i nowsze wersje) • Windows 10 20H1 (Windows 10 wersja 2004) (od wersji 14.3)
System operacyjny (serwer)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012, aktualizacja R2 z kwietnia 2014 • Windows Server 2012, aktualizacja R2 z sierpnia 2014 • Windows Server 2016 • Windows Server 2019 • Windows Server, wersja 1803 (Server Core) (od wersji 14.2 i nowsze wersje) • Windows Server, wersja 1809 (Server Core) • Windows Server, wersja 1903 (Server Core) (od wersji 14.2 RU1 i nowsze wersje) • Windows Server, wersja 1909 (Server Core) (od wersji 14.2 RU1 i nowsze wersje)
Zapobieganie włamaniom do przeglądarki	Obsługa funkcji zapobiegania włamaniom do przeglądarki zależy od wersji mechanizmu Systemu wykrywania włamań klienta (CIDS). Zobacz Przeglądarki obsługiwane przez funkcję ochrony przeglądarki przed włamaniami w programie Endpoint Protection.

Table 8: Wymagania systemowe dotyczące programu Symantec Endpoint Protection klienta systemu Windows

Składnik	Wymagania
Procesor (na komputerach fizycznych)	• Procesor 32-bitowy: co najmniej Intel Pentium o szybkości 2 GHz lub równoważny (zalecany Intel Pentium 4 lub równoważny) • Procesor 64-bitowy: co najmniej Pentium 4 o szybkości 2 GHz z obsługą architektury x86-64 lub równoważny **Note:** Procesory Itanium nie są obsługiwane.
Procesor (dla komputerów wirtualnych)	Jedno gniazdo wirtualne i minimum jeden rdzeń na gniazdo przy 1 GHz (przy 2 GHz zaleca się jedno gniazdo wirtualne i dwa rdzenie na gniazdo) **Note:** Rezerwacja zasobów warstwy hypervisor musi być włączona.
Fizyczna pamięć RAM	1 GB (zalecany 2 GB) lub więcej, jeśli wymaga tego system operacyjny
Wyświetlacz	800 x 600 lub więcej
Dysk twardy	Wymagania dotyczące miejsca na dysku zależą od rodzaju instalowanego klienta, dysku instalacji oraz lokalizacji przechowywania plików z danymi programu. Folder danych programu zwykle znajduje się na dysku systemowym, w domyślnej lokalizacji C:\ProgramData. Wolne miejsce na dysku systemowym jest zawsze wymagane, niezależnie od wyboru dysku instalacji. **Wymagane miejsce na dysku:** • Wymagane miejsce na dysku twardym w przypadku programu klienta Symantec Endpoint Protection dla systemu Windows instalowanego na dysku systemowym opisuje wymagania systemowe dysku twardego w sytuacji, gdy program Symantec Endpoint Protection jest zainstalowany na innym dysku. • Wymagane miejsce na dysku twardym w przypadku programu klienta Symantec Endpoint Protection dla systemu Windows instalowanego na innym dysku opisuje wymagania systemowe dysku twardego w sytuacji, gdy program Symantec Endpoint Protection jest zainstalowany na dysku systemowym. **Note:** Wymagania dotyczące miejsca dotyczą systemu plików NTFS. Dodatkowe miejsce na dysku jest także wymagane dla aktualizacji i dzienników.

Table 9: Wymagane miejsce na dysku twardym w przypadku programu Symantec Endpoint Protection klienta systemu Windows instalowanego na dysku systemowym

Typ klienta	Wymagania
Standardowe	**Jeśli folder danych programu znajduje się na dysku systemowym:** • 395 MB* **Jeśli folder danych programu znajduje się na innym dysku:** • Dysk systemowy: 180 MB • Inny dysk instalacji: 350 MB
Wbudowane / VDI	**Jeśli folder danych programu znajduje się na dysku systemowym:** • 245 MB* **Jeśli folder danych programu znajduje się na innym dysku:** • Dysk systemowy: 180 MB • Inny dysk instalacji: 200 MB
Ciemna sieć	**Jeśli folder danych programu znajduje się na dysku systemowym:** • 545 MB* **Jeśli folder danych programu znajduje się na innym dysku:** • Dysk systemowy: 180 MB • Inny dysk instalacji: 500 MB

* W trakcie instalacji wymagane jest dodatkowe 135 MB wolnego miejsca.

Table 10: Wymagane miejsce na dysku twardym w przypadku programu Symantec Endpoint Protection klienta systemu Windows instalowanego na innym dysku

Typ klienta	Wymagania
Standardowe	**Jeśli folder danych programu znajduje się na dysku systemowym:** • Dysk systemowy: 380 MB • Inny dysk instalacji: 15 MB* **Jeśli folder danych programu znajduje się na innym dysku: **** • Dysk systemowy: 30 MB • Dysk danych programu: 350 MB • Inny dysk instalacji: 150 MB
Wbudowane / VDI	**Jeśli folder danych programu znajduje się na dysku systemowym:** • Dysk systemowy: 230 MB • Inny dysk instalacji: 15 MB* **Jeśli folder danych programu znajduje się na innym dysku: **** • Dysk systemowy: 30 MB • Dysk danych programu: 200 MB • Inny dysk instalacji: 150 MB
Ciemna sieć	**Jeśli folder danych programu znajduje się na dysku systemowym:** • Dysk systemowy: 530 MB • Inny dysk instalacji: 15 MB* **Jeśli folder danych programu znajduje się na innym dysku: **** • Dysk systemowy: 30 MB • Dysk danych programu: 500 MB • Inny dysk instalacji: 150 MB

* W trakcie instalacji wymagane jest dodatkowe 135 MB wolnego miejsca.

** Jeśli folder danych programu jest taki sam, jak dane na innym dysku instalacji, należy dodać 15 MB do dysku danych programu, aby uzyskać łączną wymaganą ilość miejsca. W trakcie instalacji instalator potrzebuje jednak 150 MB wolnego miejsca na innym dysku instalacji.

Table 11: Wymagania systemowe dotyczące klienta programu Symantec Endpoint Protection dla systemu Windows Embedded

Składnik	Wymagania
Procesor	Intel Pentium o szybkości 1 GHz
Fizyczna pamięć RAM	256 MB **Note:** Ta liczba dotyczy instalacji klienta wbudowanego Symantec Endpoint Protection. Jeśli zastosowano również dodatkowe funkcje z zintegrowanego rozwiązania, takiego jak EDR, wymagana jest dodatkowa pamięć fizyczna RAM.

Składnik	Wymagania
Dysk twardy	Klienty wbudowane / VDI programu Symantec Endpoint Protection wymagają następującej ilości wolnego miejsca na dysku: • Instalacja na dysku systemowym: 245 MB • Instalacja na innym dysku: 230 MB na dysku systemowym oraz 15 MB na innym dysku W trakcie instalacji wymagane jest dodatkowe 135 MB. Podane ilości obowiązują w przypadku instalacji foldera danych programu na dysku systemowym. Aby uzyskać szczegółowe informacje lub informacje o wymaganiach dotyczących innych rodzajów klientów, patrz wymagania systemowe klienta programu Symantec Endpoint Protection dla systemu Windows.
System operacyjny Embedded	• Windows Embedded Standard 7 (32- i 64-bitowy) • Windows Embedded POSReady 7 (32- i 64-bitowy) • Windows Embedded Enterprise 7 (32- i 64-bitowy) • Windows Embedded 8 Standard (32- i 64-bitowy) • Windows Embedded 8.1 Industry Pro (32- i 64-bitowy) • Windows Embedded 8.1 Industry Enterprise (32- i 64-bitowy) • Windows Embedded 8.1 Pro (32- i 64-bitowy)
Wymagane minimalne składniki	• Menedżer filtrów (FltMgr.sys) • Pomoc danych wydajności (pdh.dll) • Usługa instalator Windows
Szablony	• Zgodność aplikacji (domyślnie) • Oznaczenie cyfrowe • Automatyzacja przemysłowa • IE, Media Player, RDP • Dekoder • Zubożony klient Szablon minimalnej konfiguracji nie jest obsługiwany. Rozszerzony filtr zapisu (EWF) i Ujednolicony filtr zapisu (UWF) nie są obsługiwane. Zalecanym filtrem zapisu jest Filtr zapisu oparty na plikach (FBWF) instalowany wraz z Filtrem rejestru.

Table 12: Wymagania systemowe dotyczące programu Symantec Endpoint Protection klienta systemu Mac

Składnik	Wymagania
Procesor	64-bitowy procesor Intel Core 2 Duo lub nowszy
Fizyczna pamięć RAM	2 GB pamięci RAM
Dysk twardy	500 MB dostępnego miejsca na dysku twardym na instalację
Wyświetlacz	800 x 600
System operacyjny	• macOS 10.13 • macOS 10.14 • macOS 10.15 do 10.15.5 macOS 10.14.5 i nowsze obsługują wymagania dotyczące notaryzacji rozszerzeń kext. Zobacz Endpoint Protection 14.2 RU1 i notaryzacja rozszerzeń kext dla systemu macOS 10.14.5. Aby uzyskać listę obsługiwanych systemów operacyjnych dla poprzednich wersji, zobacz: Zgodność komputerów Mac z klientem programu Endpoint Protection

Table 13: Wymagania systemowe programu Symantec Endpoint Protection klienta systemu Linux

Składnik	Wymagania
Sprzęt	• Procesor Intel Pentium 4 (o szybkości 2 GHz) lub nowszy • 1 GB pamięci RAM • 7 GB wolnego miejsca na dysku twardym
Systemy operacyjne	• Amazon Linux • CentOS 6U3 - 6U9, 7 - 7U7, 8; wersje 32- i 64-bitowe • Debian 6.0.5 Squeeze, Debian 8 Jessie; wersje 32- i 64-bitowe • Fedora 16, 17; wersje 32- i 64-bitowe • 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-bitowy i 64-bitowy; 12, 12 SP1 - 12 SP3, 64-bitowy • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32- i 64-bitowe; 12 SP3, 64-bitowe • Ubuntu 12.04, 14.04 16.04, 18.04 (od wersji 14.3); wersje 32- i 64-bitowe Listę obsługiwanych jąder systemu operacyjnego poprzednich wersji zawiera artykuł pod adresem: Jądra systemu Linux obsługiwane przez program Symantec Endpoint Protection.
Środowiska graficzne pulpitu	Do wyświetlania interfejsu programu Symantec Endpoint Protection klienta systemu Linux można używać następujących środowisk graficznych pulpitu: • KDE • Gnome • Unity

Inne wymagania dotyczące środowiska	• Glibc
	System operacyjny z bibliotekami glibc 2.6 lub wcześniejszą ich wersją nie jest obsługiwany.
	• Pakiety zależności w wersji i686 na komputerach 64-bitowych
	Wiele plików wykonywalnych w kliencie dla systemu Linux to programy 32-bitowe. W przypadku komputerów 64-bitowych przed zainstalowaniem klienta systemu Linux należy zainstalować pakiety zależności w wersji i686.
	Jeśli na komputerze nie zainstalowano pakietów zależności w wersji i686, można to zrobić za pomocą wiersza polecenia. Ta instalacja wymaga uprawnień administratora, na co wskazuje użycie polecenia `sudo` w poniższych poleceniach:
	– W przypadku dystrybucji opartych na systemie Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– W przypadku dystrybucji opartych na systemie Debian: `sudo apt-get install ia32-libs`
	– W przypadku dystrybucji opartych na systemie Ubuntu:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`
	• net-tools lub iproute2
	Program Symantec Endpoint Protection wykorzystuje te narzędzia w zależności od tego, jakie oprogramowanie zainstalowano na komputerze.
	• Narzędzia programisty
	Proces automatycznej kompilacji dla modułu jądra Auto-Protect wymaga instalacji niektórych narzędzi programisty. Te narzędzia programistyczne obejmują pliki nagłówka, źródło jądra i gcc. Szczegółowe instrukcje dotyczące instalacji na określonych wersjach systemu Linux:
	Ręczna kompilacja modułów jądra Auto-Protect dla programu Endpoint Protection for Linux

Informacje o wersji i wymagania systemowe dla wszystkich wersji programu Symantec Endpoint Protection

Obsługiwane ścieżki uaktualnienia najnowszej wersji Symantec Endpoint Protection 14.x

NOTE

Zazwyczaj w przypadku wersji programu Symantec Endpoint Protection wcześniejszych niż najnowsza wersja, obsługiwana jest każda wersja znajdująca się na liście przed tą wersją. Należy to jednak potwierdzić, sprawdzając informacje o wydaniu dołączone do konkretnej wersji.

Informacje o wersji, nowe poprawki i wymagania systemowe dla wszystkich wersji programu Endpoint Protection

Symantec Endpoint Protection Manager oraz klient systemu Windows

Następujące wersje programu Symantec Endpoint Protection Manager oraz klienta Symantec Endpoint Protection systemu Windows można uaktualnić bezpośrednio do najnowszej wersji:

- Wersje 11.x oraz Small Business Edition 12.0 (dotyczy wyłącznie klientów Symantec Endpoint Protection i obsługiwanych systemów operacyjnych)
- 12.1.x, maksymalnie do wersji 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 systemu Mac

Następujące wersje klienta Symantec Endpoint Protection systemu Mac można uaktualnić bezpośrednio do najnowszej wersji:

- 12.1.4 – 12.1.6 MP9
  Klient dla systemu Mac nie został aktualizowany do wersji 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

Klienta programu Symantec Endpoint Protection systemu macOS nie zaktualizowano do wersji 14.0.1 MP2.

Klient systemu Linux

Następujące wersje klienta Symantec Endpoint Protection systemu Linux można uaktualnić bezpośrednio do najnowszej wersji:

- 12.1.x, maksymalnie do wersji 12.1.6 MP9
  Klient dla systemu Linux nie został aktualizowany do wersji 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

Wersja programu Symantec AntiVirus for Linux 1.0.14 jest jedyną wersją, którą można migrować bezpośrednio do programu Symantec Endpoint Protection. Najpierw należy odinstalować wszystkie inne wersje programu Symantec AntiVirus for Linux. Nie można migrować klienta zarządzanego na klienta niezarządzanego.

Nieobsługiwane ścieżki uaktualnienia

Migracji do programu Symantec Endpoint Protection nie można wykonać ze wszystkich produktów firmy Symantec. Przed instalacją klienta programu Symantec Endpoint Protection należy odinstalować następujące produkty:

- Nieobsługiwane produkty firmy Symantec, takie jak Symantec AntiVirus i Symantec Client Security.
- Wszystkie produkty Symantec Norton™
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Program Symantec Endpoint Protection for Mac w wersji starszej niż 12.1.4

Nie można uaktualnić programu Symantec Endpoint Protection Manager 11.0.x lub programu Symantec Endpoint Protection Manager Small Business Edition 12.0.x bezpośrednio do programu Symantec Endpoint Protection Manager 14. Przed uaktualnieniem do wersji 14.x należy w pierwszej kolejności odinstalować te wersje programu lub dokonać uaktualnienia do wersji 12.1.x.

Nie można uaktualnić programu Symantec Endpoint Protection Manager 12.1.6 MP7 do wersji 14, ponieważ wersja schematu bazy danych w 12.1.6 MP7 jest nowsza niż w wersji 14. Należy jednak uaktualnić wersję 12.1.6 MP7 do wersji 14 MP1 lub nowszej.

Nie jest obsługiwane uaktualnienie z wersji 14 MP1 (14.0.2332.0100) do wersji 14 MP1 Refresh Build (14.0.2349.0100).

Ścieżki zmiany wersji na niższą nie są obsługiwane. Na przykład, aby możliwa była migracja z najnowszej wersji programuSymantec Endpoint Protection 14.2.1.1 do wersji 12.1.6 MP10, należy najpierw odinstalować program Symantec Endpoint Protection 14.2.1.1.

Jeśli masz numer kompilacji, ale nie wiesz, jak przekłada się on na numer wersji, przeczytaj artykuł:

- Wydane wersje programu Symantec Endpoint Protection
- Informacje dotyczące typów i wersji wydań oprogramowania Endpoint Protection

Dodatkowe źródła informacji

Informacje o witrynie internetowej programu Endpoint Protection przedstawiają witryny internetowe, w których można uzyskać informacje o sprawdzonych metodach i rozwiązywaniu problemów oraz inne informacje ułatwiające używanie produktu.

Table 14: Informacje o witrynie internetowej programu Endpoint Protection

Typy informacji	Łącze do witryny
Wersje próbne	Skontaktuj się z przedstawicielem swojego konta.
Aktualizacje podręczników i dokumentacji	• Podręczniki produktu dla najnowszej wersji wydań (j. angielski) • Podręczniki produktu dla najnowszej wersji wydań (inne języki) • Podręczniki produktu do wszystkich wersji programu Symantec Endpoint Protection 14.x (j. angielski) **Inne języki:**
Pomoc techniczna	Pomoc techniczna programu Endpoint Protection Pomoc techniczna obejmuje bazę wiedzy, szczegółowe informacje o wersjach produktu, aktualizacje i poprawki oraz dane kontaktowe działu pomocy technicznej.
Informacje o zagrożeniach oraz aktualizacje	Centrum zabezpieczeń firmy Symantec
Szkolenie	Usługi edukacyjne Uzyskaj dostęp do kursów szkoleniowych, zasobów eLibrary i nie tylko.
Fora Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom