



## **Uwagi o wydaniu programu Symantec<sup>™</sup> Endpoint Protection 14.3 RU1**

**Aktualizacja: grudzień 2020 r.**

## Table of Contents

Informacja o prawach autorskich.....	3
Nowości w programie Symantec Endpoint Protection 14.3 RU1.....	4
Znane problemy i rozwiązania zastępcze dla programu Symantec Endpoint Protection.....	9
Wymagania systemowe programu Symantec Endpoint Protection dla (SEP).....	14
Obsługiwane i nieobsługiwane ścieżki uaktualnienia do najnowszej wersji Symantec Endpoint Protection 14.x.....	22
Dodatkowe źródła informacji.....	25

## Informacja o prawach autorskich

---

Informacja o prawach autorskich

Broadcom, logo Pulse, Connect Everything oraz Symantec są znakami towarowymi firmy Broadcom.

Copyright © 2020 Broadcom. Wszelkie prawa zastrzeżone.

Termin „Broadcom” odnosi się do firmy Broadcom Inc. i/lub jej podmiotów zależnych. Więcej informacji można znaleźć na stronie [www.broadcom.com](http://www.broadcom.com).

Firma Broadcom zastrzega prawo do wprowadzania bez uprzedniego powiadomienia zmian do produktów lub danych, w celu poprawy wydajności, funkcji lub jakości. Informacje dostarczone przez firmę Broadcom są uważane za dokładne i wiarygodne. Firma Broadcom nie przyjmuje jednak odpowiedzialności za konsekwencje stosowania tych informacji lub opisywanych tutaj produktów i urządzeń. Nie przyznaje też licencji na swoje patenty lub patenty innych osób lub firm.

## Nowości w programie Symantec Endpoint Protection 14.3 RU1

Ta sekcja opisuje nowe funkcje w tej wersji.

### Funkcje ochrony

- Zawiera nowe agenty dla systemu Mac i Linux, które można zainstalować i zarządzać z poziomu lokalnego programu Symantec Endpoint Protection Manager lub zintegrowanej konsoli w chmurze Cyber Defense Manager.
  - [Instalowanie klienta programu Symantec Endpoint Protection dla komputerów Mac](#)
  - [Instalowanie Symantec Agent dla systemu Linux 14.3 RU1](#)
- Zapobiega nowym i nieznanym zagrożeniom w systemie macOS, monitorując prawie 1400 zachowań plików w czasie rzeczywistym. Nowy agent dla systemu Mac zawiera funkcje ochrony opartej na sposobach działania. Ochrona oparta na sposobach działania (SONAR) wykorzystuje sztuczną inteligencję i zaawansowane uczenie maszynowe do ochrony typu „godzina zero”, aby skutecznie powstrzymać nowe zagrożenia.
  - [Zarządzanie funkcją SONAR](#)
- Blokuje niezauważane nieprzenośne pliki wykonywalne (PE), takie jak pliki PDF i skrypty, które nie zostały jeszcze zidentyfikowane jako zagrożenie. W zasadach wyjątków kliknij pozycję **Wyjątki systemu Windows > Dostęp do plików**.
- Zapobiega zagrożeniom internetowym na podstawie oceny reputacji strony internetowej. Zasady funkcji Zapobieganie włamaniom obejmuje filtrowanie reputacji adresów URL, które blokuje strony internetowe z oceną reputacji poniżej określonego progu. Oceny reputacji wahają się od -10 (źle) do +10 (dobrze). Opcja **Włącz reputację adresu URL** jest domyślnie włączona.
- Można wymusić, aby program Symantec Endpoint Protection zapamiętywał aplikacje na podstawie wartości skrótu aplikacji. W zasadach wyjątków kliknij pozycję **Wyjątki systemu Windows > Aplikacja > Dodaj aplikację opartą na niepowtarzalnym identyfikatorze**.
- Chroni punkty końcowe i użytkowników przed atakami pochodzącymi z Internetu na destruktorych witrynach za pomocą funkcji Przekierowania ruchu sieciowego. Przekierowanie ruchu sieciowego przekierowuje cały ruch sieciowy (dowolny port) lub tylko ruch internetowy (porty 80 i 443) do usługi Symantec Web Security, która zezwala lub blokuje ruch sieciowy i dostęp do aplikacji SaaS na podstawie polityki firmy. Zasada Przekierowania ruchu sieciowego ma nową metodę przekierowania zwaną metodą tunelu. Metoda tunelu automatycznie przekierowuje cały ruch internetowy do usługi Symantec WSS, gdzie ruch jest dozwolony lub blokowany na podstawie zasad Symantec Web Security Service. Metoda tunelu jest uznawana za funkcję w wersji beta. Należy przeprowadzić dokładne testowanie aplikacji w odniesieniu do zasad WSS. Broadcom posiada stronę internetową w wersji beta, która oferuje przewodnik po testach oraz miejsce, gdzie można zostawić opinie na temat własnych doświadczeń. Zaloguj się do następującej witryny sieci Web przy użyciu poświadczeń Broadcom: [Validate.broadcom.com](https://validate.broadcom.com)
  - [Konfiguracja Przekierowania ruchu sieciowego](#)
- Nazwa Zasada integracji została zmieniona na Zasadę przekierowania ruchu sieciowego.
- Umożliwia obsługę zdarzeń wzbogaconych o rozwiązania MITRE w programie Symantec EDR. Wykorzystanie frameworka MITRE ATT&CK w celu dostarczenia informacji o tym, co aktualnie dzieje się w danym środowisku.
- Umożliwia obsługę następujących zdarzeń EDR firmy Symantec, które zapewniają szczegółowy wgląd w punktach końcowych:
  - Zdarzenia AMSI zapewniają widoczność metod złoźcy, które mogą omijać tradycyjne metody sprawdzania z wiersza poleceń.
  - Zdarzenia ETW zapewniają wgląd w zdarzenia występujące w zarządzanych punktach końcowych systemu Windows.
- Obejmuje możliwość uruchamiania programu Windows Defender, jak i Symantec Endpoint Protection na tym samym komputerze. Skanowanie Automatycznej ochrony jest uruchamiane po programie Windows Defender i może wykryć wszelkie zagrożenia, które nie zostaną rozpoznane przez Windows Defender. Opcja **Wspólne działanie z Windows Defender** gwarantuje, że funkcja Automatycznej ochrony działa w przypadku wyłączenia programu Microsoft

Defender. Aby wyłączyć tę opcję, przejdź do zasady Ochrony przed wirusami i programami typu spyware > **Różne** > karta **Różne**.

- Ograniczanie łańcucha ataku jest teraz obsługiwane dla klientów zarządzanych hybrydowo.

## Symantec Endpoint Protection Manager

- Wbudowana baza danych została zaktualizowana do bazy danych programu Microsoft SQL Express. Baza danych programu SQL Server Express przechowuje zasady i zdarzenia zabezpieczeń bardziej efektywnie niż domyślna wbudowana baza danych i jest instalowana automatycznie z Symantec Endpoint Protection Manager.

[Najważniejsze wskazówki dotyczące uaktualniania z osadzonej niniejszej bazy danych do bazy danych programu Microsoft SQL Server Express](#)

- Podczas instalacji lub uaktualnienia programu Symantec Endpoint Protection Manager, Kreator konfiguracji serwera zarządzania:
  - Automatycznie instaluje zawartość usługi LiveUpdate.
  - Udostępnia opcję używania certyfikatu TLS do bezpiecznej komunikacji między programem SQL Server a Symantec Endpoint Protection Manager.
- Usługa LiveUpdate używa nowego silnika w programie Symantec Endpoint Protection Manager, o nazwie LUX, który jest zoptymalizowany do pracy na konsoli w chmurze.

[Uwagi o wersji LiveUpdate Administrator i nowe poprawki](#)

- Opcja **Automatycznie odinstaluj istniejące oprogramowanie zabezpieczające innych firm**, która nie była dostępna w wersji 14.3 MP1, jest ponownie dostępna w wersji 14.3 RU1 z wersją zaktualizowaną. Ta opcja służy do odinstalowywania oprogramowania zabezpieczającego innych firm. Aby uzyskać dostęp do tej opcji, kliknij stronę **Administrator > Pakiety > Ustawienia instalacji klienta**.

[Usuwanie oprogramowania zabezpieczającego innych firm w programie Endpoint Protection 14](#)

[Usuwanie oprogramowania zabezpieczającego innych firm w programie Endpoint Protection 14.3 RU1](#)

- Kreator wdrażania klientów, używany do wdrażania pakietów klienckich, musi mieć zweryfikowane poświadczenia i możliwość nawiązania połączenia z programem Symantec Endpoint Protection Manager. Jeśli proces weryfikacji zakończy się niepowodzeniem, proces wdrażania klienta zostaje zatrzymany, aby uniemożliwić zablokowanie kont użytkowników Active Directory.

[Instalowanie klientów programu Symantec Endpoint Protection za pomocą zdalnego wypychania](#)

- Dzienniki i raporty o stanie komputera umożliwiają teraz wybór zakresu dla pól **Wersja klienta** i **Wersja IPS**. Nazwa filtra **Wersja produktu** została zmieniona na **Wersja klienta**.
- Opcja **Wyłącz ikonę obszaru powiadomień** jest dostępna dla klientów, którzy działają na serwerze terminalowym i powodują wysokie zużycie procesora i pamięci. Można teraz wyłączyć ikonę w obszarze powiadomień, zwanej również ikoną zasobnika systemu, aby zapobiec uruchamianiu wielu wystąpień procesów sesji użytkownika (takich jak SmcGui.exe i ccSvcHost.exe). Ta opcja jest włączona na karcie **Klienci > Zasady > Ustawienia zabezpieczeń > Ogólne**.
- Zaktualizowano tryb listy dozwolonych i listy niedozwolonych zgodnie z funkcjonalnością zezwalania i blokowania. Na stronie **Klienci > karta Zasady > okno dialogowe Blokada systemu** listy plików aplikacji zmieniły się z **Whitelist Mode** (Tryb listy dozwolonych) i **Blacklist Mode** (Tryb listy niedozwolonych) na **Allow Mode** (Tryb zezwalania) i **Deny Mode** (Tryb odmowy).
- Na stronie **Administrator > karta Serwery > Skonfiguruj rejestrowanie zewnętrzne > karta Ogólne**, opcja **Serwer główny rejestrowania** została zmieniona na **Podstawowy serwer logowania**.
- Typ dziennika **systemu > dziennik administracyjny** i dziennik **inspekcji** wyświetla nazwę komputera.
- Dzienniki zapory sieciowej klienta są gromadzone, dzięki czemu użytkownik otrzymuje mniej powiadomień na konsoli w chmurze.
- Oprogramowanie Oracle Java SE zastąpiono OpenJDK.
- Zaktualizowano składniki zewnętrzne JQuery do nowszej wersji.

## Aktualizacje klientów i platform

- Klient systemu Windows obsługuje system Windows 10 20H2 (Windows 10 wersja 2009)
- Klient systemu Mac obsługuje system macOS 10.15.7.
- Przeniesiono starsze pakiety instalacyjne klienta systemu Mac do folderu Dodatkowe pakiety.

#### **Funkcje usunięte**

- Opcje **Dotkliwość zagrożenia** i **Rozkład ryzyka według kryterium dotkliwości** zostały usunięte z powiadomień i raportów.
- Karta **CASMA** i polecenie **Analizuj** zostały usunięte, ponieważ ta funkcja jest nieobsługiwana w wersji 14.3.
- Klient dla systemu Mac nie obsługuje już systemu macOS 10.13.

#### **Dokumentacja**

Pomoc programu Symantec Endpoint Protection Manager jest teraz dostępna online i znajduje się pod adresem: [Podręcznik instalacji i podręcznik administratora programu Symantec Endpoint Protection](#)

#### **Schemat bazy danych**

Schemat bazy danych zawiera następujące zmiany:

Tabela	Zmiana kolumny
ALERTS	Dodano kolumnę ENRICHED_DATA
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA COMMAND COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG REPORTS SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2 SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG <del>V_ENFORCER_SYSTEM_LOG</del> V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER	Usunięto następujące kolumny z każdej tabeli: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Tabela	Zmiana kolumny
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	<ul style="list-style-type: none"> <li>• Typ danych kolumny CONTENT zmieniony z image na 'varbinary'</li> <li>• Dodano kolumnę indeksowaną FILESTREAM_ID</li> <li>• Dodano indeks FILESTREAM_ID</li> <li>• Usunięto następujące kolumny:               <ul style="list-style-type: none"> <li>– RESERVED_INT1</li> <li>– RESERVED_INT2</li> <li>– RESERVED_BIGINT1</li> <li>– RESERVED_BIGINT2</li> <li>– RESERVED_CHAR1</li> <li>– RESERVED_CHAR2</li> <li>– RESERVED_VARCHAR1</li> <li>– RESERVED_BINARY</li> </ul> </li> </ul>
INVENTORYREPORT	Dodano następujące kolumny: <ul style="list-style-type: none"> <li>• PRODUCTVERSIONFROM</li> <li>• PRODUCTVERSIONTO</li> <li>• IDS_VERSIONFROM</li> <li>• IDS_VERSIONTO</li> </ul>
SEM_AGENT	<ul style="list-style-type: none"> <li>• Dodano kolumnę NTR_MESSAGE</li> <li>• Usunięto następujące kolumny:               <ul style="list-style-type: none"> <li>– RESERVED_INT1</li> <li>– RESERVED_INT2</li> <li>– RESERVED_BIGINT1</li> <li>– RESERVED_BIGINT2</li> <li>– RESERVED_CHAR1</li> <li>– RESERVED_CHAR2</li> <li>– RESERVED_VARCHAR1</li> <li>– RESERVED_BINARY</li> </ul> </li> </ul>
SEM_AGENT_VERSION	Dodano następujące kolumny: <ul style="list-style-type: none"> <li>• VERSION</li> <li>• FORMATTED_VERSION</li> <li>• REFRESH_USN</li> <li>• AGENT_VERSION_FORMAT_REFRESH</li> <li>• VERSION1</li> <li>• VERSION2</li> <li>• VERSION3</li> <li>• VERSION4</li> </ul>
SEM_SVA	Usunięto następujące kolumny: <ul style="list-style-type: none"> <li>• RESERVED_INT1</li> <li>• RESERVED_INT2</li> <li>• RESERVED_BIGINT1</li> <li>• RESERVED_BIGINT2</li> <li>• RESERVED_CHAR1</li> <li>• RESERVED_CHAR2</li> <li>• RESERVED_VARCHAR1</li> </ul>
V_ALERTS	Dodano kolumnę ENRICHED_DATA

Nowości we wszystkich wersjach programu Symantec Endpoint Protection



## Znane problemy i rozwiązania zastępcze dla programu Symantec Endpoint Protection

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

**Table 1: Problemy z uaktualnieniem**

Problem	Opis i rozwiązanie
Symantec Endpoint Protection Manager w ciemnej sieci pobiera starą zawartość Systemu wykrywania włamań klienta (Client Intrusion Detection System) do nowych klientów, ponieważ usługa LiveUpdate nie jest uruchamiana podczas uaktualniania [wersja 14.3 RU1]	Gdy wersja 14.3 RU1 Symantec Endpoint Protection Manager nie może uzyskać dostępu do Internetu ani serwera LiveUpdate Administrator (LUA), przechowuje starą, niezgodną zawartość w swojej pamięci podręcznej. Ta stara zawartość jest zwykle dostarczana do nowych klientów. Aby zaktualizować zawartość w pamięci podręcznej serwera zarządzania, należy ręcznie pobrać certyfikowane definicje wirusów i pliki .jdb CIDS. [SEP-69125] Aby upewnić się, że nowi klienci nie otrzymają starej zawartości, należy ręcznie zainstalować plik CIDS .jdb na SEPM przed zainstalowaniem nowych lub aktualizacją starych klientów. <a href="#">Pobieranie plików .jdb w celu aktualizacji definicji programu Endpoint Protection Manager</a>
Nie można zalogować się do programu Symantec Endpoint Protection Manager (SEPM) po wyłączeniu karty interfejsu sieciowego [wersja 14.3 RU1]	Jeśli po zainstalowaniu programu Symantec Endpoint Protection Manager nie można zalogować się do konsoli i zostanie wyświetlony następujący komunikat o błędzie: Nieoczekiwany błąd serwera Ten problem może wystąpić, jeśli karta interfejsu sieciowego komputera jest wyłączona po zainstalowaniu modułu SEPM, który uniemożliwia wygenerowanie certyfikatu serwera. [SEP-67040] Aby dowiedzieć się, czy program SEPM został zainstalowany z wyłączoną kartą interfejsu sieciowego, zapoznaj się z certyfikatem serwera. Zobacz: <a href="#">Instalacja SEPM zakończy się niepowodzeniem, jeśli nie będzie dostępnych połączeń sieciowych</a>
Po odinstalowaniu SEPM i skorzystaniu z opcji usunięcia domyślnej bazy danych i pozostawieniu instancji SQL Server Express, pojawia się następujący błąd: „Wystąpił błąd podczas próby połączenia z serwerem bazy danych”.	Jeśli podczas dezinstalacji programu Symantec Endpoint Protection Manager wybrana zostanie opcja <b>Usuń tylko bazę danych i pozostaw zainstalowaną instancję SQL Server Express z opcją SEPM</b> , może pojawić się następujący błąd: „Wystąpił błąd podczas próby połączenia z serwerem bazy danych”. Ten problem występuje po dodaniu poświadczeń dla domyślnego użytkownika DBA i może być związany z uprawnieniami użytkownika. [SEP-68670] Aby obejść ten problem, należy wykonać dezinstalację, uruchamiając instalatora SEPM.exe plik i klikając opcję <b>Usuń tylko bazę danych i pozostaw opcję SQL Server Express zainstalowaną z opcją SEPM</b> podczas dezinstalacji.
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 BRACK, 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 <b>Lokalne zasady zabezpieczeń &gt; Zasady lokalne &gt; Opcje zabezpieczeń</b> i wyłącz <b>Kryptografię systemu: Użyj algorytmów zgodnych ze standardem FIPS do szyfrowania, mieszania i podpisywania</b> 2. Uaktualnienie z programu SQL Server w wersji 2017 do wersji 2019. 3. Po pomyślnym uaktualnieniu programu SQL Server ponownie włącz tryb FIPS. <a href="#">Uaktualnienie SQL z 2017 do 2019 kończy się niepowodzeniem z włączonym trybem FIPS</a>

Problem	Opis i rozwiązanie
Niestandardowe nazwy mogą uniemożliwiać aktualizację zasad zapory podczas uaktualniania programu do wersji 14.2 lub nowszej	<p>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.</p> <p>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.</p>

Table 2: Problemy dotyczące programu Symantec Endpoint Protection Manager

Problem	Opis i rozwiązanie
Niektóre zdarzenia EDR nie pojawiają się na kliencie [wersja 14.3 RU1]	Klient programu Symantec Endpoint Protection musi uruchomić system Windows 10 kompilacja 14393 lub nowszej do zbierania zdarzeń usługi Symantec EDR Event Tracing dla systemu Windows (ETW). [SEP-67175]
Funkcja Przekierowanie ruchu sieciowego ma pewne ograniczenia [14.3 RU1]	<ul style="list-style-type: none"> <li>• Usługa Symantec Web Security Service uwzględnia protokoły IPv4, ale nie IPv6. [SEP-68700]</li> <li>• Przekierowanie za pomocą metody tunelu: <ul style="list-style-type: none"> <li>– Działa tylko w systemie Windows 10 x64 w wersji 1703 i nowszych (opcja Semi-Annual Servicing Channel). Ta metoda nie obsługuje żadnych innych systemów operacyjnych Windows ani klienta systemu Mac. [SEP-67927]</li> <li>– Nie obsługuje urządzeń 64-bitowych z systemem Windows 10 z obsługą interfejsu HVCI. [SEP-67648]</li> <li>– Przekierowuje ruch wychodzący z klienta programu Symantec Endpoint Protection do WSS, zanim zostanie sprawdzony przez zaporę klienta lub reguły reputacji adresu URL. Zamiast tego ruch ten jest analizowany pod kątem zapory sieciowej WSS i reguł adresów URL. Na przykład, jeśli reguła zapory klienta SEP blokuje google.com, a reguła WSS pozwala na dostęp do google.com, klient pozwala użytkownikom na dostęp do google.com. Przychodzący ruch lokalny do klienta jest nadal przetwarzany przez zaporę Symantec Endpoint Protection. [SEP-67488]</li> <li>– Portal WSS Captive nie jest dostępny dla metody tunelu, a klient ignoruje poświadczenia wezwania. W nowszym wydaniu oprogramowania uwierzytelnianie SAML dla agenta WSS zastąpi Captive Portal i będzie dostępne w kliencie Symantec Endpoint Protection.</li> <li>– Jeśli komputer kliencki łączy się z usługą WSS przy użyciu metody tunelu i obsługuje maszyny wirtualne, każdy użytkownik-gość musi zainstalować certyfikat SSL podany w portalu WSS.</li> <li>– Ruch w sieci lokalnej, na przykład w katalogu domowym lub uwierzytelnianiu Active Directory, nie jest przekierowywany.</li> </ul> </li> </ul> <p>Metoda tunelu jest obecnie uznawana za funkcję w wersji beta.</p>
Zduplikowane wpisy rejestracji agenta po uaktualnieniu z wersji 14.2.x do 14.3 MP1 i nowszych [14.3 RU1]	<p>Uaktualnienie klientów programu Symantec Endpoint Protection z wersji 14.2.x do 14.3 MP1 i nowszych tworzy zduplikowane wpisy rejestracji agenta dla tych klientów na stronie <b>Urządzenia</b> w programie Symantec Endpoint Protection Manager.</p> <p>Nie ma to wpływu na funkcjonalność i można kontynuować pracę z nowymi wpisami dla klientów w wersji 14.3 RU1. Symantec Endpoint Protection Manager usunie starsze wpisy agenta.</p>

Problem	Opis i rozwiązanie
<p>Zezwalaj na adresy URL w programie Symantec Endpoint Security, jeśli używasz opcji zarządzania hybrydowego, serwerów proxy lub zapory obwodowej [wersja 14.3]</p>	<p>Wraz z przejściem 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</p> <ul style="list-style-type: none"> <li>• Program Symantec Endpoint Security służy do zarządzania klientami i zasadami podczas rejestracji lokalnych domen programu Symantec Endpoint Protection Manager w konsoli w chmurze</li> <li>• Serwery proxy są używane.</li> </ul> <p>Adresy URL są zezwalane na agentach w pełni zarządzanych w chmurze lub hybrydowo, a następnie serwerze proxy i/lub zaporze obwodowej. Zobacz: <a href="#">Adresy URL umożliwiające SEP i SES łączenie się z serwerami Symantec</a> Zobacz <a href="#">Uaktualnianie agentów zarządzanych w chmurze firmy Symantec do wersji 14.2 RU2 MP1 lub nowszych</a>.</p>
<p>Konsola zdalna programu Symantec Endpoint Protection Manager nie obsługuje już 32-bitowej platformy Windows [14.3]</p>	<p>W wersji 14.3 i nowszych 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.”</p>
<p>Podczas instalowania programu Symantec Endpoint Protection Manager [14.3] wyświetlony jest błąd „Niepowodzenie instalacji środowiska Microsoft Visual C++ Runtime”</p>	<p>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.</p>
<p>Aktualizuj, aby umożliwić włączenie protokołów TLS 1.1 i TLS 1.2 jako domyślnych bezpiecznych protokołów w WinHTTP w systemie Windows [14.3]</p>	<p>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: &lt;SEVERE&gt; WinHttpSendRequest: 12175: A security error occurred Ten problem jest spowodowany brakuącą 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: <a href="#">Aktualizuj, aby umożliwić włączenie protokołów TLS 1.1 i TLS 1.2 jako domyślnych bezpiecznych protokołów w WinHTTP w systemie Windows</a></p>
<p>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]</p>	<p>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.</p>

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

Problem	Opis i rozwiązanie
Nieprawidłowe komunikaty w dzienniku instalatora agenta Symantec dla systemu Linux. [14.3 RU1]	W niektórych przypadkach instalator agenta rejestruje niepoprawne komunikaty związane z niepasującą wersją sterownika lub wymaganym ponownym uruchomieniem. Te komunikaty nie wpływają na funkcjonalność agenta.
Na urządzeniu SuSe Linux zypper usuwa pakiety klientów SEP systemu Linux podczas usuwania pakietu 'at'. [14.3 RU1]	Na urządzeniu SuSe Linux polecenie 'zypper remove at' usuwa pakiety klientów SEP Linux, ponieważ pakiet 'at' jest dodawany jako wymagany pakiet zależny, a polecenia zypper automatycznie próbują usunąć pakiety klientów SEP 'sdcss-kmod' i 'sdcss-sepagent' jako pakiety z nieużywanymi zależnościami. <b>Rozwiązanie zastępcze:</b> Aby usunąć pakiet 'at', uruchom następujące polecenie: rpm -e --nodeps at
Problem z uaktualnieniem w systemie macOS 10.15 i nowszych [14.3 MP1]	W systemie macOS 10.15 lub nowszym funkcja <b>Zainstaluj program Symantec Endpoint Protection na komputerach zdalnych</b> w Kreatorze wdrażania klientów nie może uaktualnić klienta programu Symantec Endpoint Protection ze starszych wersji do wersji 14.3 MP1. <b>Rozwiązanie:</b> Użyj <b>Automatycznego uaktualnienia programu Symantec Endpoint Protection Manager</b> , aby wykonać uaktualnienie klienta programu Symantec Endpoint Protection w systemie macOS 10.15 lub nowszym.
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: <a href="#">2019 Wymagania dotyczące obsługi podpisywania kodu SHA-2 dla systemów Windows i WSUS</a> 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 ujednoczonego filtra 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: <ul style="list-style-type: none"> <li>• Uaktualnij do innej wersji systemu operacyjnego, która nie zawiera wady.</li> <li>• Wyłącz UWF. Zobacz: <a href="#">Program Endpoint Protection działa nieprawidłowo po zainstalowaniu w systemie Windows 10 1803 z włączoną obsługą UWF</a></li> </ul>
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.

Problem	Opis i rozwiązanie
Przeglądarka Microsoft Edge nieoczekiwanie zezwala na pobieranie plików PDF z włączonym Zabezpieczeniem [14.2 RU1 MP1 i nowsze wersje]	Po włączeniu funkcji Zabezpieczenia 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 programem 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 <a href="#">Endpoint Protection</a> i mają teraz inny adres URL. W celu wyszukania artykułu, użyj pola <b>Wyszukaj</b> .
Pliki PDF	Symantec opublikował wszystkie pliki PDF w artykułach DOC. Te strony wygasły. Aby znaleźć najnowszą wersję pliku PDF, przejdź do strony <a href="#">Dokumenty pokrewne</a> . 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 RU1](#)

[Nowe poprawki i składniki programu Symantec Endpoint Protection 14.3 MP1](#)

[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	<ul style="list-style-type: none"> <li>• Windows Server 2008 R2</li> <li>• Windows Server 2012</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2016</li> <li>• Windows Server 2019</li> </ul> <p><b>Note:</b> Systemy operacyjne dla komputerów stacjonarnych nie są obsługiwane.</p> <p><b>Note:</b> Wersja Windows Server Core nie jest obsługiwana w wersji 14.2x i wcześniejszej.</p>
Przeglądarka internetowa	<p>Następujące przeglądarki są obsługiwane pod względem dostępu internetowego z konsoli do programu Symantec Endpoint Protection Manager oraz do wyświetlania Pomocy Symantec Endpoint Protection Manager:</p> <ul style="list-style-type: none"> <li>• Przeglądarka Microsoft Edge oparta na oprogramowaniu Chromium (14.3 i nowsze)</li> <li>• Microsoft Edge</li> </ul> <p>Uwaga: System Windows w wersji 32-bitowej nie obsługuje dostępu konsoli internetowej w przeglądarce Edge.</p> <ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 11 (wersja 14.2.x i wcześniejsze)</li> <li>• Mozilla Firefox 5.x do wersji 83</li> <li>• Google Chrome 87</li> </ul>



Składnik	Wymagania
Baza danych	<p>Program Symantec Endpoint Protection Manager zawiera domyślną bazę danych:</p> <ul style="list-style-type: none"> <li>• Microsoft SQL Server Express 2014 (dla systemu Windows Server 2008 R2)</li> <li>• Microsoft SQL Server Express 2017</li> <li>• Wbudowana baza danych Sybase (tylko wersja 14.3 MP.x i wcześniejsze)</li> </ul> <p>Można również używać bazy danych z jednej z następujących wersji programu Microsoft SQL Server:</p> <ul style="list-style-type: none"> <li>• SQL Server 2008 SP4</li> <li>• SQL Server 2008 R2, SP3</li> <li>• SQL Server 2012 RTM - SP4</li> <li>• SQL Server 2014 RTM - SP3</li> <li>• SQL Server 2016 RTM, SP1, SP2</li> <li>• SQL Server 2017 RTM</li> <li>• SQL Server 2019 RTM (wersja 14.3 lub nowsze)</li> </ul> <p><b>Note:</b> Obsługiwane są bazy danych serwera SQL hostowane w serwisie Amazon RDS (od wersji 14.0.1 MP2).</p> <p><b>Note:</b> 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.</p> <p><b>Note:</b> <a href="#">Obsługa protokołu TLS 1.2 dla programu Microsoft SQL Server</a></p>
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	<p>Intel Pentium Dual-Core lub równoważny, zalecany co najmniej 8-rdzeniowy procesor</p> <p><b>Note:</b> Procesory Intel Itanium IA-64 nie są obsługiwane.</p>
Fizyczna pamięć RAM	<p>Minimum 2 GB dostępnej pamięci RAM, zalecane 8 GB lub więcej</p> <p><b>Note:</b> 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.</p>
Wyświetlacz	1024 x 768 lub więcej
Dysk twardy podczas instalowania na dysku systemowym	<p>Z lokalną bazą danych programu SQL Server:</p> <ul style="list-style-type: none"> <li>• Co najmniej 40 GB dostępnego miejsca (zalecane 200 GB) dla serwera zarządzania i bazy danych</li> </ul> <p>Ze zdalną bazą danych programu SQL Server:</p> <ul style="list-style-type: none"> <li>• Co najmniej 40 GB dostępnego miejsca (zalecane 100 GB) dla serwera zarządzania.</li> <li>• Dodatkowe miejsce na dysku serwera zdalnego dla bazy danych</li> </ul>
Miejsce na dysku w przypadku instalowania programu na innym dysku:	<p>Z lokalną bazą danych programu SQL Server:</p> <ul style="list-style-type: none"> <li>• Minimum 15 GB dostępnego miejsca (zalecane 100 GB) na dysku systemowym</li> <li>• Minimum 25 GB dostępnego miejsca (zalecane 100 GB) na dysku instalacji</li> </ul> <p>Ze zdalną bazą danych programu SQL Server:</p> <ul style="list-style-type: none"> <li>• Minimum 15 GB dostępnego miejsca (zalecane 100 GB) na dysku systemowym</li> <li>• Minimum 25 GB dostępnego miejsca (zalecane 100 GB) na dysku instalacji</li> <li>• Dodatkowe miejsce na dysku serwera zdalnego dla bazy danych</li> </ul>

Składnik	Wymagania
Inne	Włączona karta interfejsu sieciowego

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)	<ul style="list-style-type: none"> <li>• Windows 7 (32-bitowy, 64-bitowy, RTM i SP1)</li> <li>• Windows Embedded 7 Standard, POSReady i Enterprise (32- i 64-bitowy)</li> <li>• Windows 8 (32-bitowy, 64-bitowy)</li> <li>• Windows Embedded 8 Standard (32- i 64-bitowy)</li> <li>• Windows 8.1 (32-bitowy, 64-bitowy), włącznie z funkcją Windows To Go</li> <li>• Windows 8.1, aktualizacja z kwietnia 2014 (32-bitowy, 64-bitowy)</li> <li>• Windows 8.1, aktualizacja z sierpnia 2014 (32-bitowy, 64-bitowy)</li> <li>• Windows Embedded 8.1 Pro, Industry Pro, Industry Enterprise (wersje 32- i 64-bitowe)</li> <li>• Windows 10 (1507) (wersje 32- i 64-bitowe), włącznie z wersją Windows 10 Enterprise 2015 LTSC</li> <li>• Windows 10 November Update (1511) (wersje 32- i 64-bitowe)</li> <li>• Windows 10 Anniversary Update (1607) (wersje 32- i 64-bitowe), włącznie z wersją Windows 10 Enterprise 2016 LTSC</li> <li>• Windows 10 Creators Update (1703) (wersje 32- i 64-bitowe)</li> <li>• Windows 10 Fall Creators Update (1709) (wersje 32- i 64-bitowe)</li> <li>• Windows 10 April 2018 Update (1803) (wersje 32- i 64-bitowe)</li> <li>• Windows 10 October 2018 Update (wersja 1809) (wersje 32- i 64-bitowe), w tym Windows 10 Enterprise 2019 LTSC.</li> <li>• Windows 10 May 2019 Update (wersja 1903) (wersje 32- i 64-bit)</li> <li>• Windows 10 November Update 2019 (wersja 1909) (wersje 32- i 64-bitowe) (14.2 RU1 i nowsze wersje)</li> <li>• Windows 10 20H1 (Windows 10 wersja 2004) (wersja 14.3 i nowsze)</li> <li>• Windows 10 20H2 (Windows 10 wersja 2009) (od wersji 14.3)</li> </ul>
System operacyjny (serwery)	<ul style="list-style-type: none"> <li>• Windows Server 2008 R2</li> <li>• Windows Small Business Server 2011</li> <li>• Windows Server 2012</li> <li>• Windows Server 2012 R2</li> <li>• Windows Server 2012, aktualizacja R2 z kwietnia 2014</li> <li>• Windows Server 2012, aktualizacja R2 z sierpnia 2014</li> <li>• Windows Server 2016</li> <li>• Windows Server 2019</li> <li>• Windows Server, wersja 1803 (Server Core) (od wersji 14.2 i nowsze wersje)</li> <li>• Windows Server, wersja 1809 (Server Core)</li> <li>• Windows Server, wersja 1903 (Server Core) (od wersji 14.2 RU1 i nowsze wersje)</li> <li>• Windows Server, wersja 1909 (Server Core) (wersja 14.2 RU1 i nowsze wersje)</li> <li>• Windows Server, wersja 2004</li> <li>• Windows Server, wersja 20H2 (wersja 14.3 RU1)</li> </ul>
Zapobieganie włamaniom do przeglądarki	<p>Obsługa funkcji zapobiegania włamaniom do przeglądarki zależy od wersji mechanizmu Systemu wykrywania włamań klienta (CIDS).</p> <p>Zobacz: <a href="#">Przeglądarki obsługiwane przez funkcję ochrony przeglądarki przed włamaniami w programie Endpoint Protection</a></p>



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

Składnik	Wymagania
Procesor (na komputerach fizycznych)	<ul style="list-style-type: none"> <li>Procesor 32-bitowy: co najmniej Intel Pentium o szybkości 2 GHz lub równoważny (zalecany Intel Pentium 4 lub równoważny)</li> <li>Procesor 64-bitowy: co najmniej Pentium 4 o szybkości 2 GHz z obsługą architektury x86-64 lub równoważny</li> </ul> <p><b>Note:</b> Procesory Itanium nie są obsługiwane.</p>
Procesor (dla komputerów wirtualnych)	<p>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)</p> <p><b>Note:</b> Rezerwacja zasobów warstwy hypervisor musi być włączona.</p>
Fizyczna pamięć RAM	1 GB (zalecany 2 GB) lub więcej, jeśli wymaga tego system operacyjny
Wyświetlacz	800 x 600 lub więcej
Dysk twardy	<p>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.</p> <p>Wolne miejsce na dysku systemowym jest zawsze wymagane, niezależnie od wyboru dysku instalacji.</p> <p><b>Note:</b> Wymagania dotyczące miejsca dotyczą systemu plików NTFS. Dodatkowe miejsce na dysku jest także wymagane dla aktualizacji i dzienników.</p>

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

Typ klienta	Wymagania
Standardowe	<p>Jeśli folder danych programu znajduje się na dysku systemowym:</p> <ul style="list-style-type: none"> <li>395 MB*</li> </ul> <p>Jeśli folder danych programu znajduje się na innym dysku:</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 180 MB</li> <li>Inny dysk instalacji: 350 MB</li> </ul>
Wbudowane / VDI	<p>Jeśli folder danych programu znajduje się na dysku systemowym:</p> <ul style="list-style-type: none"> <li>245 MB*</li> </ul> <p>Jeśli folder danych programu znajduje się na innym dysku:</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 180 MB</li> <li>Inny dysk instalacji: 200 MB</li> </ul>
Ciemna sieć	<p>Jeśli folder danych programu znajduje się na dysku systemowym:</p> <ul style="list-style-type: none"> <li>545 MB*</li> </ul> <p>Jeśli folder danych programu znajduje się na innym dysku:</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 180 MB</li> <li>Inny dysk instalacji: 500 MB</li> </ul>

\* 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	<p>Jeśli folder danych programu znajduje się na dysku systemowym:</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 380 MB</li> <li>Inny dysk instalacji: 15 MB*</li> </ul> <p>Jeśli folder danych programu znajduje się na innym dysku:**</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 30 MB</li> <li>Dysk danych programu: 350 MB</li> <li>Inny dysk instalacji: 150 MB</li> </ul>
Wbudowane / VDI	<p>Jeśli folder danych programu znajduje się na dysku systemowym:</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 230 MB</li> <li>Inny dysk instalacji: 15 MB*</li> </ul> <p>Jeśli folder danych programu znajduje się na innym dysku:**</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 30 MB</li> <li>Dysk danych programu: 200 MB</li> <li>Inny dysk instalacji: 150 MB</li> </ul>
Ciemna sieć	<p>Jeśli folder danych programu znajduje się na dysku systemowym:</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 530 MB</li> <li>Inny dysk instalacji: 15 MB*</li> </ul> <p>Jeśli folder danych programu znajduje się na innym dysku:**</p> <ul style="list-style-type: none"> <li>Dysk systemowy: 30 MB</li> <li>Dysk danych programu: 500 MB</li> <li>Inny dysk instalacji: 150 MB</li> </ul>

\* 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**

Składnik	Wymagania
Procesor	Intel Pentium o szybkości 1 GHz
Fizyczna pamięć RAM	<p>256 MB</p> <p><b>Note:</b> 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.</p>

Składnik	Wymagania
Dysk twardy	<p>Klienci wbudowane / VDI programu Symantec Endpoint Protection wymagają następującej ilości wolnego miejsca na dysku:</p> <ul style="list-style-type: none"> <li>Instalacja na dysku systemowym: 245 MB</li> <li>Instalacja na innym dysku: 230 MB na dysku systemowym oraz 15 MB na innym dysku</li> </ul> <p>W trakcie instalacji wymagane jest dodatkowe 135 MB.</p> <p>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.</p>
System operacyjny Embedded	<ul style="list-style-type: none"> <li>Windows Embedded Standard 7 (32- i 64-bitowy)</li> <li>Windows Embedded POSReady 7 (32- i 64-bitowy)</li> <li>Windows Embedded Enterprise 7 (32- i 64-bitowy)</li> <li>Windows Embedded 8 Standard (32- i 64-bitowy)</li> <li>Windows Embedded 8.1 Industry Pro (32- i 64-bitowy)</li> <li>Windows Embedded 8.1 Industry Enterprise (32- i 64-bitowy)</li> <li>Windows Embedded 8.1 Pro (32- i 64-bitowy)</li> </ul>
Wymagane minimalne składniki	<ul style="list-style-type: none"> <li>Menedżer filtrów (FitMgr.sys)</li> <li>Pomoc danych wydajności (pdh.dll)</li> <li>Usługa instalator Windows</li> </ul>
Szablony	<ul style="list-style-type: none"> <li>Zgodność aplikacji (domyślnie)</li> <li>Oznaczenie cyfrowe</li> <li>Automatyzacja przemysłowa</li> <li>IE, Media Player, RDP</li> <li>Dekoder</li> <li>Zubożony klient</li> </ul> <p>Szablon minimalnej konfiguracji nie jest obsługiwany.</p> <p>Rozszerzony filtr zapisu (EWF) i Ujednoczony filtr zapisu (UWF) nie są obsługiwane. Zalecanym filtrem zapisu jest Filtr zapisu oparty na plikach (FBWF) instalowany wraz z Filtrem rejestru.</p>

**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	1 GB dostępnego miejsca na dysku twardym na instalację
Wyświetlacz	800 x 600
System operacyjny	<ul style="list-style-type: none"> <li>macOS 10.14</li> <li>macOS 10.14.5 i nowsze obsługują wymagania dotyczące notaryzacji rozszerzeń kext. Zobacz <a href="#">Endpoint Protection 14.2 RU1 i notaryzacja rozszerzeń kext dla systemu macOS 10.14.5</a>.</li> <li>macOS 10.15 do 10.15.7</li> </ul> <p>Aby uzyskać listę obsługiwanych systemów operacyjnych dla poprzednich wersji, zobacz: <a href="#">Zgodność komputerów Mac z klientem programu Endpoint Protection</a></p>

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

Składnik	Wymagania
Sprzęt	<ul style="list-style-type: none"> <li>• Procesor Intel Pentium 4 (o szybkości 2 GHz) lub nowszy</li> <li>• 500 MB pamięci RAM</li> <li>• 2 GB dostępnej przestrzeni dyskowej, jeśli /var, /opt i /tmp współdzielą ten sam system plików/rozmiar</li> <li>• 500 MB dostępnego miejsca na dysku w każdym /var, /opt, i /tmp jeśli na różnych rozmiarach</li> </ul>
Systemy operacyjne	<p>Obsługiwane systemy operacyjne od wersji 14.3 RU1:</p> <ul style="list-style-type: none"> <li>• Amazon Linux 2</li> <li>• CentOS 6.x, 7.x, 8.x</li> <li>• Oracle Enterprise Linux 6.x, 7.x, 8.x</li> <li>• Red Hat Enterprise Linux 6.x, 7.x, 8.x</li> <li>• SuSE Linux Enterprise Server 12.x, 15.x</li> <li>• Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS</li> </ul> <p>Obsługiwane systemy operacyjne dla wersji 14.3 i wcześniejszych:</p> <ul style="list-style-type: none"> <li>• Amazon Linux</li> <li>• CentOS 6U3 - 6U9, 7 - 7U7, 8; wersje 32- i 64-bitowe</li> <li>• Debian 6.0.5 Squeeze, Debian 8 Jessie; wersje 32- i 64-bitowe</li> <li>• Fedora 16, 17; wersje 32- i 64-bitowe</li> <li>• Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8, 7, 7U1, 7U2, 7U3, 7U4</li> <li>• Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2</li> <li>• SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bitowy i 64-bitowy; 12, 12 SP1 - 12 SP3, 64-bitowy</li> <li>• SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32- i 64-bitowe; 12 SP3, 64-bitowe</li> <li>• Ubuntu 12.04, 14.04 16.04, 18.04 (od wersji 14.3); wersje 32- i 64-bitowe</li> </ul> <p>Aby uzyskać listę obsługiwanych jąder systemu operacyjnego dla poprzednich wersji, zobacz <a href="#">Lista dystrybucji i jąder systemu Linux z wstępnie skompilowanymi sterownikami/modułami Automatycznej ochrony dla programu Symantec Endpoint Protection dla systemu Linux 14.x.</a></p>
Środowiska graficzne pulpitu	<p>Do wyświetlania interfejsu programu Symantec Endpoint Protection klienta systemu Linux można używać następujących środowisk graficznych pulpitu:</p> <ul style="list-style-type: none"> <li>• KDE</li> <li>• Gnome</li> <li>• Unity</li> </ul> <p>Symantec Agent dla systemu Linux 14.3 RU1 nie ma graficznego interfejsu użytkownika.</p>

Składnik	Wymagania
Inne wymagania dotyczące środowiska (wersja 14.3 MP1 i wcześniejsze)	<ul style="list-style-type: none"> <li>• Glibc System operacyjny z bibliotekami glibc 2.6 lub wcześniejszą ich wersją nie jest obsługiwany.</li> <li>• net-tools lub iproute2 Program Symantec Endpoint Protection wykorzystuje te narzędzia w zależności od tego, jakie oprogramowanie zainstalowano na komputerze.</li> <li>• Biblioteka OpenSSL 1.0.2k-fips lub nowsza</li> <li>• 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: <a href="#">Ręczna kompilacja modułów jądra Auto-Protect dla programu Endpoint Protection for Linux</a></li> <li>• 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 <code>sudo</code> w poniższych poleceniach: <ul style="list-style-type: none"> <li>– W przypadku dystrybucji opartych na systemie Red Hat: <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686</code></li> <li>– W przypadku dystrybucji opartych na systemie Debian: <code>sudo apt-get install ia32-libs</code></li> <li>– W przypadku dystrybucji opartych na systemie Ubuntu: <pre>sudo dpkg --add-architecture i386 sudo apt-get update sudo apt-get install gcc-multilib libx11-6:i386</pre> </li> </ul> </li> </ul>

[Wersje wydań, uwagi, nowe poprawki i wymagania systemowe dotyczące programu Endpoint Security i wszystkich wersji programu Endpoint Protection](#)

## Obsługiwane i nieobsługiwane ścieżki uaktualnienia do najnowszej wersji Symantec Endpoint Protection 14.x

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.

[Wersje wydań, uwagi, nowe poprawki i wymagania systemowe dotyczące programu Endpoint Security i wszystkich wersji programu Endpoint Protection](#)

### Obsługiwane ścieżki uaktualnienia

- Program Symantec Endpoint Protection Manager w wersji 12.1.6 MP10 i nowszych z wbudowaną bazą danych bezproblemowo uaktualnia się do bazy danych Microsoft SQL Server Express w wersji 14.3 RU1. Aktualizacje z wersji 12.1.6 MP9 i wcześniejszych do wersji 14.3 RU1 są blokowane.
- Symantec Endpoint Protection Manager w wersji 14.x uaktualnia bezproblemowo od wersji 12.1.x, z wyjątkiem przypadków, w których usunięto obsługę techniczną, takich jak np: Windows Server 2003, systemy operacyjne dla komputerów stacjonarnych oraz 32-bitowe systemy operacyjne, a także niektóre wersje SQL Server.
- Klient programu Symantec Endpoint Protection w wersji 14.x bezproblemowo uaktualnia wszystkie poprzednie wersje klienta 12.1 i 11 zainstalowane w obsługiwanych systemach operacyjnych. Wyjątkiem jest wersja klienta Mac wcześniejsza niż 12.1.4, którą należy uaktualnić do 12.1.4 lub nowszej, albo odinstalować.

[Zagadnienia dotyczące migracji w programie Symantec Endpoint Protection 14](#)

### 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
- 14.3, 14.3 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 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

**NOTE**

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

**Klient systemu Linux****NOTE**

Symantec Agent dla systemu Linux 14.3 RU1 wykrywa i odinstalowuje starszego klienta Symantec Endpoint Protection systemu Linux, a następnie wykonuje nową instalację. Stare konfiguracje nie zostaną zachowane.

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
- 14.3, 14.3 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:

- Program Symantec AntiVirus i Symantec Client Security, które nie są obsługiwane.
- Wszystkie produkty Symantec Norton
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Dowolna wersja programu Symantec Endpoint Protection dla klienta Mac wcześniejszego niż 12.1.4. Możesz też uaktualnić do wersji 12.1.4 lub nowszej.

**Uwagi:**

- Migracja klienta programu Symantec Endpoint Protection dla wersji wcześniejszej niż 12.1.x nie jest obsługiwana.
- Nie można uaktualnić programu Symantec Endpoint Protection Manager 11.0.x ani programu Symantec Endpoint Protection Manager Small Business Edition 12.0.x bezpośrednio do dowolnej wersji programu Symantec Endpoint Protection Manager 14. Przed uaktualnieniem do wersji 14.x należy w pierwszej kolejności odinstalować te wersje programu lub dokonać uaktualnienia do najnowszego wydania 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.
- W wersji 14.0.x odrzucono obsługę systemów Windows XP, Server 2003 oraz wszelkich systemów operacyjnych Windows Embedded opartych na Windows XP. Program Symantec Endpoint Protection Manager 14.2 RU1 może zarządzać tymi komputerami jako starszymi wersjami klientów 12.1.x, chociaż klienci 12.1.x nie będą już obsługiwane.

Dla tych klientów można użyć produktu firmy Symantec, który nadal obsługuje starsze systemy operacyjne, takie jak Data Center Security (DCS).

- 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 programu Symantec Endpoint Protection 14.2.1.1 do wersji 12.1.6 MP10, należy najpierw odinstalować program Symantec Endpoint Protection 14.2.1.
- Jeśli masz numer kompilacji, ale nie wiesz, jak przekłada się on na numer wersji, przeczytaj artykuł: [Informacje dotyczące typów i wersji wydań oprogramowania Endpoint Protection](#)



## Dodatkowe źródła informacji

Poniższa tabela przedstawia 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	<ul style="list-style-type: none"> <li><a href="#">Podręczniki produktu dla najnowszej wersji wydań</a> (j. angielski)</li> <li><a href="#">Podręczniki produktu dla najnowszej wersji wydań</a> (inne języki)</li> <li><a href="#">Podręczniki produktu do wszystkich wersji programu Symantec Endpoint Protection 14.x</a> (j. angielski)</li> </ul>
Pomoc techniczna	<a href="#">Pomoc techniczna programu Endpoint Protection</a> Pomoc techniczna obejmuje bazę wiedzy, szczegółowe informacje o wersjach produktu, aktualizacje i poprawki oraz dane kontaktowe działu pomocy technicznej.
Informacje o zagrożeniach oraz aktualizacje	<a href="#">Centrum zabezpieczeń firmy Symantec</a>
Szkolenie	<a href="#">Usługi edukacyjne</a> Uzyskaj dostęp do kursów szkoleniowych, zasobów eLibrary i nie tylko.
Fora Symantec Connect	<a href="#">Endpoint Protection</a>

