TREND MICRO

10.0

Worry-Free™ Business Security Standard Edition i Advanced Edition

Podręcznik instalacji i uaktualniania

Securing Your Journey to the Cloud

Protected Cloud

Web Security

Firma Trend Micro Incorporated zastrzega sobie prawo do wprowadzania, bez wcześniejszej zapowiedzi, zmian w tym dokumencie oraz w opisanych w nim produkt. Przed zainstalowaniem i korzystaniem z produkt należy zapoznać się z plikami „readme", uwagami do wydania oraz najnowszą wersją właściwej dokumentacji, które są dostępne w witrynie internetowej firmy Trend Micro pod adresem:

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

Numer części dokumentu: WFPM108205/180326

Data wydania: Czerwiec 2018 r.

Podlega ochronie patentami USA o numerach: 5 951 698 i 7 188 369

Niniejsza dokumentacja zawiera opis głównych funkcji produkt oraz instrukcje instalacji w środowisku produkcyjnym. Należy ją przeczytać przed zainstalowaniem lub rozpoczęciem użytkowania produkt.

Szczegółowe informacje na temat użycia określonych funkcji w ramach produkt można znaleźć w centrum pomocy online firmy Trend Micro lub w bazie wiedzy firmy Trend Micro.

Firma Trend Micro stara się zawsze ulepszać swoją dokumentację. W przypadku pytań, komentarzy lub sugestii na temat tego lub dowolnego innego dokumentu firmy Trend Micro prosimy o kontakt pod adresem docs@trendmicro.com.

Prosimy o ocenę tego dokumentu w witrynie:

http://www.trendmicro.com/download/documentation/rating.asp

Spis treści

Wstęp

Rozdział 1: Przygotowanie do instalacji i aktualizacji

Rozdział 2: Instalowanie programu Security Server

Rozdział 3: Uaktualnianie programu Security Server i agentów

Dodatek A: Pomoc techniczna

Indeks

Wstęp

Zapraszany do lektury *Podręcznika instalacji i aktualizacji* programu Trend Micro™ Worry-Free™ Business Security. Ten dokument dotyczy następujących wymogów i procedur:

- Instalowanie programu Security Server
- Uaktualnianie programu Security Server i agentów

Informacje na temat instalowania klientów zawiera *Podręcznik administratora*.

Dokumentacja programu Worry-Free Business Security

Dokumentacja programu Worry-Free Business Security obejmuje następujące składniki:

TABELA 1. Dokumentacja programu Worry-Free Business Security

DOKUMENTACJA	OPIS
Podręcznik instalacji oraz uaktualniania	Dokument PDF z omówieniem wymagań i procedur odnoszących się do instalowania programu Security Server oraz instalowania serwera i agentów.
Podręcznik administratora	Dokument PDF z omówieniem informacji wprowadzających, procedur instalacji klienta oraz zarządzania programem Security Server i agentami
Pomoc	Pliki HTML skompilowane w formacie WebHelp lub CHM, zawierające instrukcje korzystania, porady i informacje dotyczące określonych zastosowań programu
plik Readme	Zawiera listę znanych problemów i podstawowych czynności instalacyjnych. Plik ten może również zawierać najnowsze informacje o produkcie, które nie znajdują się w systemie pomocy ani w dokumentacji drukowanej.
Baza wiedzy	Baza danych online zawierająca informacje dotyczące rozwiązywania problemów. Zawiera najnowsze informacje o znanych problemach dotyczących produktu. Aby uzyskać dostęp do bazy wiedzy, odwiedź witrynę internetową http://esupport.trendmicro.com

Najnowsze wersje dokumentów PDF i plików Readme znajdują się pod adresem:

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

Odbiorcy

Dokumentacja programu Worry-Free Business Security jest przeznaczona dla następujących grup użytkowników:

- **Administratorzy zabezpieczeń**: odpowiedzialni za zarządzanie programem Worry-Free Business Security, w tym programem Security Server, oraz za instalację agentów i zarządzanie nimi. Od użytkowników tego typu oczekuje się zaawansowanej wiedzy na temat zarządzania serwerem i siecią.
- **Użytkownicy końcowi**: użytkownicy, którzy mają na komputerach zainstalowane programy Security Agent. Poziom umiejętności takich osób jest różny — od początkujących po zaawansowanych.

Konwencje przyjęte w dokumentacji

Aby ułatwić odnalezienie i zrozumienie informacji, w dokumentacji programu Worry-Free Business Security przyjęto następujące konwencje:

TABELA 2. Konwencje przyjęte w dokumentacji

KONWENCJA	OPIS
WIELKIE LITERY	Akronimy, skróty, nazwy poszczególnych poleceń oraz klawisze klawiatury
Pogrubienie	Nazwy i polecenia menu, przyciski poleceń, karty, opcje oraz nazwy zadań
Kursywa	Odniesienia do innych dokumentacji oraz nowych rozwiązań technologicznych
<Tekst>	Oznacza, że tekst wewnątrz nawiasów ostrych należy zastąpić rzeczywistymi informacjami. Na przykład ścieżkę `C:\Program Files\<nazwa_pliku>` można zmienić na `C:\Program Files\sample.jpg`.
 **Uwaga**	Uwagi lub zalecenia dotyczące konfiguracji
 **Porada**	Informacje o sprawdzonych metodach oraz zaleceniach firmy Trend Micro

KONWENCJA	OPIS
 **OSTRZEŻENIE!**	Ostrzeżenia dotyczące czynności, które mogą stwarzać zagrożenie w sieci

Rozdział 1

Przygotowanie do instalacji i aktualizacji

W tym rozdziale omówiono przygotowania niezbędne przed instalacją lub uaktualnieniem programu Worry-Free™ Business Security.

Edycje produktu

Firma Trend Micro oferuje następujące edycje produktu:

- Worry-Free Business Security**Standard**: Umożliwia ochronę punkty końcowe (komputerów stacjonarnych, przenośnych i serwerów) w sieci lokalnej. Ta edycja zawiera funkcje zapory, skanowania antywirusowego i skanowania antyszpiegowskiego. Obejmuje też pomoc techniczną, pobieranie sygnatur wirusów, skanowanie w czasie rzeczywistym oraz aktualizacje programu przez okres jednego roku.
- Worry-Free Business Security**Advanced**: Umożliwia ochronę punkty końcowe i serwerów Microsoft Exchange w sieci lokalnej. Oprócz funkcji dostępnych w wersji Worry-Free Business Security Standard ta edycja programu obejmuje też funkcje ochrony przed spamem, filtrowania zawartości, zapobiegania utracie danych i blokowania załączników.

Poniższa tabela zawiera listę funkcji obsługiwanych w poszczególnych edycjach.

TABELA 1-1. Dostępne funkcje według edycji produktu

FUNKCJE	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Aktualizacje składników	Tak	Tak
Kontrola urządzeń	Tak	Tak
Oprogramowanie antywirusowe/anty-spyware	Tak	Tak
Zapora	Tak	Tak
Usługa Web Reputation	Tak	Tak
Filtrowanie adresów URL	Tak	Tak
Przewidujące uczenie maszynowe	Tak	Tak
Monitorowanie zachowania	Tak	Tak
Narzędzia użytkownika	Tak	Tak

Funkcje	Worry-Free Business Security Standard	Worry-Free Business Security Advanced
Skanowanie poczty (POP3)	Tak	Tak
Antyspam (POP3)	Tak	Tak
Skanowanie poczty (IMAP)	Nie	Tak
Antyspam (IMAP)	Nie	Tak
Filtrowanie zawartości wiadomości e-mail	Nie	Tak
Zapobieganie utracie danych przez wiadomość e-mail	Nie	Tak
Blokowanie załączników	Nie	Tak

Licencje, rejestracja i aktywacja

Przy zakupie Worry-Free Business Security otrzymujesz licencję na produkt(y) i standardową umowę serwisową. Standardowa umowa serwisowa jest umową pomiędzy organizacją i firmą Trend Micro dotyczącą prawa do uzyskania wsparcia technicznego i aktualizacji produktów pod warunkiem uiszczenia odpowiednich opłat.

Licencja na oprogramowanie firmy Trend Micro obejmuje zazwyczaj prawo do aktualizacji produktu, aktualizacji plików sygnatur i podstawowego wsparcia technicznego tylko przez jeden (1) rok od daty zakupu. Po pierwszym roku umowę serwisową należy corocznie odnawiać po aktualnych cenach obowiązujących w firmie Trend Micro.

Uwaga

Umowa serwisowa wygasa, natomiast nie wygasa umowa licencyjna. Po wygaśnięciu umowy serwisowej skanowanie jest nadal przeprowadzane, ale nie można dokonać aktualizacji plików sygnatur złośliwego oprogramowania / wirusów, silnika skanowania lub plików programu (również ręcznie). Użytkownik nie jest również upoważniony do uzyskania wsparcia technicznego firmy Trend Micro.

Zarejestruj i aktywuj licencję Worry-Free Business Security, aby włączyć wszystkie funkcje produktu.

Klucz rejestracyjny

Klucz rejestracyjny otrzymujesz podczas zakupu Worry-Free Business Security. Składa się z 22 znaków (wraz z myślnikami) i ma następujący format:

Worry-Free Business Security Standard: CS-xxxx-xxxxx-xxxxx-xxxxx

Worry-Free Business Security Advanced: CM-xxxx-xxxxx-xxxxx-xxxxx

Należy użyć klucza rejestracyjnego z pełną licencją, aby zarejestrować Worry-Free Business Security na witrynie internetowej firmy Trend Micro znajdującej się pod adresem https://clp.trendmicro.com.

Kod aktywacyjny

Po dokonaniu rejestracji kod aktywacyjny z pełną licencją zostanie wysłany wiadomością e-mail. Kod aktywacyjny składa się z 37 znaków (wraz z myślnikami) i ma następujący format:

Worry-Free Business Security Standard: CS-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

Worry-Free Business Security Advanced: CM-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

Podczas instalacji Security Server wpisz kod aktywacyjny po wyświetleniu monitu. Jeśli pole nie zostanie wypełnione, Worry-Free Business Security zainstaluje 30-dniową wersję testową. Należy dokonać aktualizacji do wersji z pełną licencją przed wygaśnięciem wersji testowej.

Stan licencji

Poniższa tabela zawiera obsługiwane funkcje w zależności od stanu licencji.

TABELA 1-2. Stan licencji

FUNKCJA	PEŁNA LICENCJA	WERSJA PRÓBNA (30 DNI)	WYGASŁO
Powiadomienie o wygaśnięciu	Tak	Tak	Tak

Funkcja	Pełna licencja	Wersja próbna (30 dni)	Wygasło
Aktualizacje składników	Tak	Tak	Nie
Aktualizacje programu	Tak	Tak	Nie
Pomoc techniczna	Tak	Nie	Nie
Skanowanie w czasie rzeczywistym	Tak	Tak	Tak, ale skanowanie w czasie rzeczywistym będzie używać nieaktualnych składników

Po wygaśnięciu kodu aktywacyjnego z pełną licencją nie można pobrać aktualizacji silnika skanowania lub plików sygnatur. Jednak w odróżnieniu od kodu aktywacyjnego w wersji próbnej, jeśli wygaśnie kod aktywacyjny w wersji z pełną licencją, wszystkie istniejące konfiguracje i pozostałe ustawienia pozostają w mocy. Taka klauzula zapewnia poziom ochrony w przypadku przypadkowego dopuszczenia do wygaśnięcia licencji.

Wersję pełną Worry-Free Business Security można odnowić, wykupując odnowienie usługi. Kod aktywacyjny jest konieczny do zainstalowania wersji pełnych.

W przypadku pytań dotyczących procesu rejestracji należy skorzystać z witryny wsparcia technicznego Trend Micro znajdującej się pod adresem:

http://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

Worry-Free Business Security Network

Rozwiązanie Worry-Free Business Security składa się z następujących elementów:

- *Program Security Server na stronie 1-6*
- *Agenty na stronie 1-7*
- *Konsola internetowa na stronie 1-8*

Program Security Server

Podstawowym elementem pakietu Worry-Free Business Security jest program Security Server. Program Security Server zawiera konsolę internetową — scentralizowaną internetową konsolę do zarządzania programem Worry-Free Business Security. Program Security Server instaluje agenty na klientach w sieci i nawiązuje z tymi agentami relacje typu agent-serwer. Program Security Server umożliwia wyświetlanie informacji o stanie zabezpieczeń, przeglądanie agentów, konfigurowanie zabezpieczeń systemu i pobieranie składników ze scentralizowanej lokalizacji. Program Security Server zawiera także bazę danych, w której przechowywane są dzienniki wykrytych i zgłoszonych przez agenty zagrożeń internetowych.

Program Security Server spełnia następujące ważne funkcje:

- Instaluje i monitoruje agenty oraz zarządza nimi.
- Pobiera składniki, których potrzebują agenty. Domyślnie program Security Server pobiera składniki z serwera Trend Micro ActiveUpdate, a następnie rozsyła je do agentów.

Scan Server

Na serwerze Security Server dostępna jest usługa o nazwie Scan Server, która jest instalowana automatycznie podczas instalacji serwera Security Server. W związku z tym nie ma potrzeby instalowania jej osobno. Usługa Scan Server zostaje uruchomiona w ramach procesu o nazwie `iCRCService.exe` i jest wyświetlana pod nazwą **Usługa Trend Micro Smart Scan** w konsoli Microsoft Management Console.

Gdy programy Security Agent korzystają z metody skanowania o nazwie **Smart Scan**, usługa Scan Server pomaga tym agentom w skuteczniejszym skanowaniu. Proces Smart Scan można opisać w następujący sposób:

- Program Security Agent skanuje klienta pod kątem zagrożeń bezpieczeństwa, korzystając z **Sygnatura agenta usługi Smart Scan**, lżejszej wersji tradycyjnej sygnatury wirusów. W sygnaturze agenta usługi Smart Scan znajduje się większość sygnatur zagrożeń dostępnych w sygnaturze wirusów.
- Program Security Agent, który podczas skanowania nie jest w stanie określić, czy plik stanowi zagrożenie, sprawdza to, wysyłając zapytanie o skanowanie do usługi

Scan Server. Usługa Scan Server sprawdza zagrożenie, korzystając z sygnatury **Smart Scan Pattern**, która zawiera sygnatury zagrożeń niedostępne w sygnaturze agenta usługi Smart Scan.

- Program Security Agent umieszcza wynik zapytania o skanowanie uzyskany od usługi Scan Server w pamięci podręcznej w celu zwiększenia wydajności skanowania.

Dzięki hostowaniu niektórych definicji zagrożeń usługa Scan Server pomaga zmniejszyć obciążenie sieci podczas pobierania składników przez programy Security Agent. Zamiast pobierać sygnaturę wirusów, programy Security Agent pobierają sygnaturę agenta usługi Smart Scan, której rozmiar jest znacznie mniejszy.

Gdy programy Security Agent nie są w stanie uzyskać połączenia z usługą Scan Server, wysyłają żądania skanowania do serwera Trend Micro Smart Protection Network, pełniącego tę samą funkcję, co usługa Scan Server.

Nie ma możliwości odinstalowania usługi Scan Server bez odinstalowywania serwera Security Server. Jeśli nie chcesz korzystać z usługi Scan Server:

1. Na komputerze będącym serwerem Security Server otwórz konsolę Microsoft Management Console i wyłącz opcję **Usługa Trend Micro Smart Scan**.
2. W konsoli internetowej ustaw dla programów Security Agent skanowanie standardowe, przechodząc do karty **Administracja** > **Ustawienia globalne** > **Komputer/serwer** i zaznaczając opcję **Wyłącz usługę skanowania Smart Scan**.

Agenty

Agenty chronią klienty przed zagrożeniami. Klienty to komputery, serwery oraz serwery Microsoft Exchange. Agentami programu Worry-Free Business Security są:

TABELA 1-3. Agenty programu Worry-Free Business Security

AGENT	OPIS
Security Agent	Chroni komputery i serwery przed zagrożeniami i atakami.

AGENT	OPIS
Programy Messaging Security Agent (tylko w wersji Advanced)	Chroni serwery Microsoft Exchange przed zagrożeniami pochodzącymi z wiadomości e-mail.

Agent podlega programowi Security Server, z którego został zainstalowany. Aby dostarczyć programowi Security Server najświeższe informacje o kliencie, agent przesyła w czasie rzeczywistym informacje o stanie zdarzeń. Raportowane są takie zdarzenia, jak wykrycie wirusa, uruchomienie lub zamknięcie agenta, rozpoczęcie skanowania i zakończenie aktualizacji.

Konsola internetowa

Konsola internetowa to centralny punkt monitorowania programów Security Agent w całej sieci firmowej. Zawiera zestaw ustawień domyślnych i wartości, które można skonfigurować zależnie od wymagań zabezpieczeń i specyfikacji. W konsoli Web zastosowano standardowe technologie internetowe, takie jak Java, CGI, HTML i HTTP.

Za pomocą konsoli internetowej można:

- Instalować agentów na punktach końcowych
- Organizować agenty w grupy logiczne w celu ich równoczesnego konfigurowania i zarządzania nimi.
- Konfigurować ustawienia produktu i rozpocząć skanowanie ręczne na punktach końcowych.
- Odbierać powiadomienia i przeglądać raporty dziennika dotyczące działań związanych z zagrożeniami.
- Odbierać powiadomienia i wysyłać alarmy o epidemii za pośrednictwem wiadomości e-mail po wykryciu zagrożeń na punktach końcowych.

Rozdział 2

Instalowanie programu Security Server

W tym rozdziale zamieszczono informacje dotyczące procedury instalacji programu Security Server.

Wymagania dotyczące instalacji i uaktualniania

Pełna lista wymagań dotyczących instalacji i uaktualniania jest dostępna pod adresem:

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

Uwagi dotyczące instalacji programu Security Server

Podczas instalowania programu Security Server należy wziąć pod uwagę następujące kwestie:

Wymagania programu Security Server dotyczące protokołu IPv6

Poniżej przedstawiono wymagania protokołu IPv6 dotyczące serwera Security Server:

- Jeśli serwer ma zarządzać agentami wykorzystującymi protokół IPv4 i IPv6, musi on mieć zarówno adres IPv4, jak i IPv6, oraz być identyfikowany nazwą hosta. Jeśli serwer jest identyfikowany adresem IPv4, nie będzie możliwe nawiązanie połączenia między nim i agentami wykorzystującymi protokół IPv6. Taka sama sytuacja zachodzi między klientami z protokołem IPv4 i serwerem identyfikowanym adresem IPv6.
- Jeśli serwer ma zarządzać tylko agentami wykorzystującymi protokół IPv6, minimalnym wymaganiem jest posiadanie adresu IPv6. Serwer może być

identyfikowany nazwą hosta lub adresem IPv6. Gdy serwer jest identyfikowany nazwą hosta, zalecane jest wprowadzenie pełnej nazwy (FQDN, Fully Qualified Domain Name). Wynika to z faktu, że w środowisku z samym protokołem IPv6 serwer WINS nie może wykonać translacji nazwy hosta na odpowiedni adres IPv6.

- Upewnij się, że adres IPv6 lub IPv4 hosta można uzyskać na przykład przy użyciu polecenia „`ping`" lub „`nslookup`".
- Jeśli instalujesz program Security Server na komputerze z samym protokołem IPv6, skonfiguruj serwer proxy z podwójnym stosem. Umożliwi to zamianę adresów IP (np. DeleGate). Umieść serwer proxy między serwerem Security Server a Internetem, aby umożliwić serwerowi nawiązanie połączenia z usługami obsługiwanymi przez firmę Trend Micro, takimi jak serwer ActiveUpdate, witryna Online Registration i sieć Smart Protection Network.

Lokalizacja programu Security Server

Program Worry-Free Business Security może obsługiwać wiele środowisk sieciowych. Można na przykład umieścić zaporę pomiędzy programem Trend Micro Security Server a klientami z uruchomionym programem Security Agent lub umieścić zarówno program Trend Micro Security Server, jak i wszystkie klienty za pojedynczą zaporą sieciową.

W przypadku zarządzania wieloma ośrodkami zaleca się zainstalowanie programu Security Server w ośrodku głównym i w każdym zarządzanym ośrodku, aby zmniejszyć zużycie przepustowości sieci między ośrodkiem głównym a ośrodkami zarządzanymi, a także przyspieszyć instalację plików sygnatur.

Jeżeli na klientach włączono zaporę systemu Windows, program Worry-Free Business Security automatycznie doda ją do listy wyjątków.

Uwaga

Jeżeli zaporę umieszczono pomiędzy programem Trend Micro Security Server a jego klientami, należy ją skonfigurować tak, aby umożliwić ruch sieciowy pomiędzy portami nasłuchiwania klientów i portem nasłuchiwania programu Trend Micro Security Server.

Liczba klientów

Klient to komputer, na którym planuje się instalację programu Security Agent lub Messaging Security Agent. Dotyczy to komputerów stacjonarnych, przenośnych i serwerów, w tym tych, które używane są do łączności.

Jedna instalacja programu Security Server jest w stanie obsłużyć do 2 500 klientów. W przypadku większej liczby klientów, firma Trend Micro zaleca zainstalowanie następnego programu Security Server.

Ruch sieciowy

Program Worry-Free Business Security generuje ruch sieciowy podczas komunikacji serwera Security Server z agentami.

Program Security Server/Scan Server generuje ruch sieciowy, gdy:

- powiadamia agenty o zmianach w konfiguracji;
- powiadamia agenty o aktualizacjach składników do pobrania;
- łączy się z serwerem ActiveUpdate firmy Trend Micro w celu sprawdzania i pobierania aktualizacji składników;
- odpowiada na żądania skanowania otrzymane od agentów używających funkcji Smart Scan;
- przesyła informacje zwrotne do infrastruktury Trend Micro Smart Protection Network.

Agenty generują ruch, gdy:

- są uruchamiane;
- są zamykane;
- generują dzienniki;
- dokonują zaplanowanej aktualizacji;
- przeprowadzają ręczne aktualizacje („Aktualizuj teraz”);

- łączą się z serwerem skanowania w celu przesłania żądań skanowania.

Uwaga

Inne działania poza aktualizacjami generują nieznaczny ruch sieciowy.

Ruch sieciowy podczas aktualizowania składników

W czasie aktualizowania składników program Security Server generuje znaczny ruch sieciowy. Aby zmniejszyć ruch sieciowy generowany podczas aktualizowania składników, program Security Server przeprowadza duplikację składników. Zamiast pobierać pełny zaktualizowany plik sygnatur program Security Server pobiera tylko „przyrostowe" wzorce sygnatur (mniejsze wersje pełnego pliku sygnatur), a następnie scala je ze starszym plikiem sygnatur.

Program Security Server, który jest aktualizowany regularnie, pobiera tylko sygnaturę przyrostową. W innym przypadku pobiera pełny plik sygnatury.

Firma Trend Micro regularnie publikuje nowe pliki sygnatur. Trend Micro wydaje także nowy plik sygnatur wkrótce po odkryciu szczególnie szkodliwego i aktywnie krążącego wirusa/złośliwego oprogramowania.

Korzystanie z agentów aktualizacji w celu zredukowania zajętości pasma sieciowego

Jeśli obszary sieci między programami Security Agent a programem Security Server są obszarami o „niskiej przepustowości" lub „dużym ruchu", można skonfigurować programy Security Agent w taki sposób, aby pełniły rolę źródeł aktualizacji (agentów aktualizacji) wobec innych agentów. Ułatwia to rozłożenie ciężaru wdrażania składników na wszystkich agentach.

Jeśli na przykład sieć jest podzielona na segmenty według lokalizacji, a łącza sieciowe między segmentami są poddawane dużemu obciążeniu ruchem, firma Trend Micro zaleca, aby przynajmniej jeden program Security Agent w każdym z segmentów działał jako agent aktualizacji.

Serwer dedykowany

Podczas określania komputera klient jako hosta serwera Worry-Free Business Security należy wziąć pod uwagę następujące kwestie:

- Obciążenie procesora, jakie obsługuje klient
- Czy klient pełni inne funkcje

Jeżeli klient docelowy pełni inne funkcje, wybierz klient, który nie obsługuje aplikacji krytycznych lub pochłaniających dużych ilości zasobów.

Problemy ze zgodnością

W niniejszej części opisano problemy ze zgodnością, które mogą wystąpić podczas korzystania z niektórych aplikacji innych firm. Należy zawsze zapoznać się z dokumentacją wszystkich aplikacji innych firm, które są zainstalowane na tym samym komputerze, na którym zostanie zainstalowany program Security Server i inne składniki rozwiązania Worry Free.

Inne oprogramowanie zabezpieczające punkt końcowy

Firma Trend Micro zaleca, aby przed zainstalowaniem programu Security Server ręcznie usunąć inne oprogramowanie zabezpieczające punkt końcowy z komputera docelowego, ponieważ może ono zablokować instalację lub wpływać później na działanie programu Security Server.

Programy związane z zabezpieczeniami w systemach Windows EBS i SBS 2008

Program Worry-Free Business Security jest zgodny z systemami Windows Small Business Server (SBS) 2008 oraz Windows Essential Business Server (EBS) 2008. Jednak niektóre programy zapewniające bezpieczeństwo zainstalowane lub zarządzane w tych systemach operacyjnych mogą wywołać konflikt z programem Worry-Free Business Security. Z tego powodu usunięcie tych programów może okazać się konieczne.

Program Messaging Security Agent a program Forefront

Programu Messaging Security Agent nie można zainstalować na serwerach Microsoft Exchange, na których zainstalowano program Microsoft Forefront Security for Exchange Server (Forefront). Przed zainstalowaniem programu Messaging Security Agent należy odinstalować program Forefront i upewnić się, że uruchomiona jest usługa Microsoft Exchange Information Store.

Program Messaging Security Agent a Microsoft Server Enterprise

Program Messaging Security Agent nie obsługuje niektórych funkcji serwera Microsoft Exchange Server Enterprise, takich jak grupa dostępności danych.

Programy Security Agent i Windows Defender

Zainstalowanie programu Security Agent powoduje wyłączenie programu Windows Defender.

Bazy danych

Skanowanie baz danych może spowodować spadek wydajności aplikacji uzyskujących dostęp do tych baz danych. Firma zaleca wykluczenie baz danych i ich folderów kopii zapasowej ze skanowania w czasie rzeczywistym. Jeśli baza danych wymaga skanowania, należy wykonać tę czynność ręcznie lub zaplanować poza godzinami szczytu, aby zminimalizować wpływ skanowania na jej działanie.

Zapory innych firm

Firma Trend Micro zaleca, aby przed przystąpieniem do instalacji zapory programu Worry-Free Business Security odinstalować lub wyłączyć wszelkie zapory innych firm, w tym następujące aplikacje:

- Zapora połączenia internetowego Windows (ICF)
- Zapora Windows (WF)

Jeżeli jednak konieczne jest uruchomienie zapory połączenia internetowego lub zapory innej firmy, należy dodać porty nasłuchiwania programu Trend Micro Security Server do listy wyjątków zapory (informacje na temat portów nasłuchiwania znajdują się w sekcji *Porty programu Worry-Free Business Security na stronie 2-7*; informacje na temat konfigurowania listy wyjątków zawiera dokumentacja danej zapory).

Porty programu Worry-Free Business Security

W programie Worry-Free Business Security używane są następujące porty:

- **Port nasłuchiwania serwera (port HTTP)**: służy do uzyskiwania dostępu do programu Security Server. Domyślnie program Worry-Free Business Security korzysta z jednego z następujących portów:

- **Domyślna witryna internetowa serwera IIS**: taki sam numer portu jak w przypadku portu TCP serwera HTTP.
- **Wirtualna witryna internetowa serwera IIS**: 8059
- **Serwer Apache**: 8059

- **Port nasłuchiwania klienta**: losowo wygenerowany numer portu, za pośrednictwem którego programy Security Agent i Messaging Security Agent otrzymują polecenia od programu Security Server.

  Porty nasłuchiwania można modyfikować tylko podczas instalacji.

OSTRZEŻENIE!

Duża liczba ataków hakerów i wirusów odbywa się poprzez protokół HTTP i skierowana jest na porty 80 i/lub 8080, które w większości firm używane są jako domyślne porty TCP (Transmission Control Protocol), służące do komunikacji poprzez protokół HTTP. Jeżeli jeden z tych portów jest obecnie używany w firmie jako port HTTP, firma Trend Micro zaleca użycie portu o innym numerze.

Uwaga

Aby ustalić, który port jest używany przez programy Security Agent do łączenia się z serwerem skanowania, należy otworzyć plik SSCFG.ini w katalogu, w którym serwer jest zainstalowany.

- **Porty serwera skanowania**: używane przez serwer skanowania do komunikowania się z programami Security Agent w związku z żądaniami skanowania.

TABELA 2-1. Porty serwera skanowania

TYP PORTU	IIS, DOMYŚLNE	IIS, WIRTUALNE	PREINSTALOWANY SERWER APACHE	NOWA INSTALACJA SERWERA APACHE
Port inny niż SSL	Port inny niż SSL na serwerze internetowym	Pierwszy otwarty port z zakresu od 8082 do 65536	Port inny niż SSL na serwerze internetowym	Port inny niż SSL na serwerze internetowym

Typ portu	IIS, domyślne	IIS, wirtualne	Preinstalowany serwer Apache	Nowa instalacja serwera Apache
port SSL Korzystanie z protokołu SSL	Port SSL na serwerze Web	Pierwszy otwarty port z zakresu od 4345 do 65536	nd.	Port SSL na serwerze Web
port SSL Bez korzystania z protokołu SSL	Pierwszy otwarty port z zakresu od 4345 do 65536	Pierwszy otwarty port z zakresu od 4345 do 65536	nd.	Pierwszy otwarty port z zakresu od 4345 do 65536

- **Port komunikacji Trend Micro Security (for Mac)**: używany przez serwer Trend Micro Security (for Mac) do komunikowania się z klientami Mac. Port domyślny to 61617.
- **Port SMTP**: używany przez program Security Server do wysyłania do administratorów raportów i powiadomień pocztą elektroniczną. Port domyślny to 25.
- **Port serwera proxy**: służy do połączeń za pośrednictwem serwera proxy.

Lista kontrolna instalacji

Po zainstalowaniu programu Security Server program instalacyjny wyświetla monit zawierający następujące informacje:

Tabela 2-2. Lista kontrolna instalacji

Informacje	Wartości domyślne	Wartość użytkownika
Security Server (w tym serwer skanowania)		
Kod aktywacyjny	Dostarczony przez firmę Trend Micro	

Informacje	Wartości domyślne	Wartość użytkownika
Ścieżka instalacji	Jedna z poniższych (w zależności od systemu operacyjnego): • C:\Program Files \TrendMicro\Security Server • C:\Program Files (x86)\Trend Micro \Security Server	
Ścieżka do bazy danych serwera skanowania	Taka sama jak ścieżka instalacji programu Security Server (można ją zmienić)	
Adres IPv4/IPv6	Zdefiniowane przez użytkownika	
W pełni kwalifikowana nazwa domeny (FQDN)	Zdefiniowane przez użytkownika	
Nazwa NetBIOS (host)	Zdefiniowane przez użytkownika	
Serwer sieci Web	Do wyboru: • Apache • IIS (domyślna witryna sieci Web) • IIS (wirtualna witryna sieci Web)	
Port nasłuchiwania (HTTP)	8059	
Port nasłuchiwania (HTTPS)	4343	
Hasło konsoli Web	Zdefiniowane przez użytkownika	

INFORMACJE	WARTOŚCI DOMYŚLNE	WARTOŚĆ UŻYTKOWNIKA
Hasło odinstalowania/ zamknięcia programu Security Agent	Zdefiniowane przez użytkownika	
(Opcjonalnie) Ustawienia SMTP dotyczące wysyłania przez serwer Security Server raportów i powiadomień za pomocą poczty e-mail		
Adres IPv4/IPv6	Zdefiniowane przez użytkownika	
W pełni kwalifikowana nazwa domeny (FQDN)	Zdefiniowane przez użytkownika	
Nazwa NetBIOS (host)	Zdefiniowane przez użytkownika	
Port	25	
Odbiorcy	Zdefiniowane przez użytkownika	
(Opcjonalnie) Ustawienia serwera proxy dotyczące połączenia serwera Security Server z usługami obsługiwanymi przez firmę Trend Micro		
Adres IPv4/IPv6	Zdefiniowane przez użytkownika	
W pełni kwalifikowana nazwa domeny (FQDN)	Zdefiniowane przez użytkownika	
Nazwa NetBIOS (host)	Zdefiniowane przez użytkownika	
Nazwa użytkownika do celów uwierzytelniania	Zdefiniowane przez użytkownika	
Hasło uwierzytelniania	Zdefiniowane przez użytkownika	

Informacje	Wartości domyślne	Wartość użytkownika
Security Agent		
Port nasłuchiwania	Generowany losowo przez program instalacyjny	
Ścieżka instalacji	Jedna z poniższych (w zależności od systemu operacyjnego): • C:\Program Files \TrendMicro\Security Agent • C:\Program Files (x86)\Trend Micro \Security Agent	
(Opcjonalnie) Uwierzytelnianie serwera proxy na potrzeby funkcji programu Security Agent (Monitorowanie zachowania, Web Reputation i Smart Scan) **Uwaga** Programy Security Agent używają ustawień serwera proxy skonfigurowanych w przeglądarce Internet Explorer.		
Nazwa użytkownika do celów uwierzytelniania	Zdefiniowane przez użytkownika	
Hasło uwierzytelniania	Zdefiniowane przez użytkownika	
(Opcjonalnie) Programy Messaging Security Agent		
Adres IPv4/IPv6 serwera Microsoft Exchange	Zdefiniowane przez użytkownika	
W pełni kwalifikowana nazwa domeny (FQDN) serwera Microsoft Exchange	Zdefiniowane przez użytkownika	

INFORMACJE	WARTOŚCI DOMYŚLNE	WARTOŚĆ UŻYTKOWNIKA
Nazwa NetBIOS (host) serwera Microsoft Exchange	Zdefiniowane przez użytkownika	
Konto i hasło administratora domeny używane do logowania się na serwerze Microsoft Exchange	Zdefiniowane przez użytkownika	
Port nasłuchiwania	16372	
Ścieżka instalacji	Jedna z poniższych (w zależności od systemu operacyjnego): • C:\Program Files \TrendMicro\Messaging Security Agent • C:\Program Files (x86)\Trend Micro \Messaging Security Agent	
Folder Temp (program instalacyjny wyodrębnia pliki instalacyjne do tego folderu)	C$	

Instalowanie programu Security Server

Instalowanie programu Security Server obejmuje trzy etapy:

ETAPY	KLUCZOWE ZADANIA

Etap 1: Rozpoczynanie instalacji programu Security Server	• Przeczytaj wstępne wytyczne dotyczące instalacji.
	• Uruchom pakiet instalacyjny.
	• Zaakceptuj warunki umowy licencyjnej.
	• Wybierz typ instalacji.
	  • Standardowa (zalecana)
	  • Minimalna
	  • Niestandardowa
	• Podaj kod aktywacyjny.

ETAPY	KLUCZOWE ZADANIA
Etap 2: Konfigurowanie ustawień zgodnie z wybranym typem instalacji	W przypadku instalacji standardowej lub minimalnej skonfiguruj ustawienia podstawowe, takie jak: • Lokalizacja instalacji programu Security Server • Hasła konta administratora • Ustawienia serwera SMTP i odbiorcy powiadomień • Smart Protection Network

	W przypadku instalacji niestandardowej skonfiguruj wszystkie ustawienia niestandardowe, takie jak:
	• Ustawienia podstawowe
	  • Lokalizacja instalacji programu Security Server
	  • Lokalizacja bazy danych serwera skanowania
	  • Określenie, czy programy Security Agent lub Messaging Security Agent mają być zainstalowane na tym samym komputerze co program Security Server
	• Ustawienia programu Security Server
	  • Serwer sieci Web
	  • Hasło konta administratora
	  • Ustawienia serwera SMTP i odbiorcy powiadomień
	  • Smart Protection Network
	  • Ogólne ustawienia serwera proxy
	• Ustawienia programu Security Agent
	  • Ścieżka instalacji programu Security Agent
	  • Włączone funkcje programu Security Agent
	  • Ustawienia serwera proxy dotyczące usług dodatkowych
	• Ustawienia programu Messaging Security Agent
	  • Ustawienia serwera Microsoft Exchange
	  • Lokalizacja instalacji programu Messaging Security Agent

ETAPY	KLUCZOWE ZADANIA
Etap 3: Proces instalacji	Poczekaj na zakończenie instalacji i zamknij program instalacyjny.

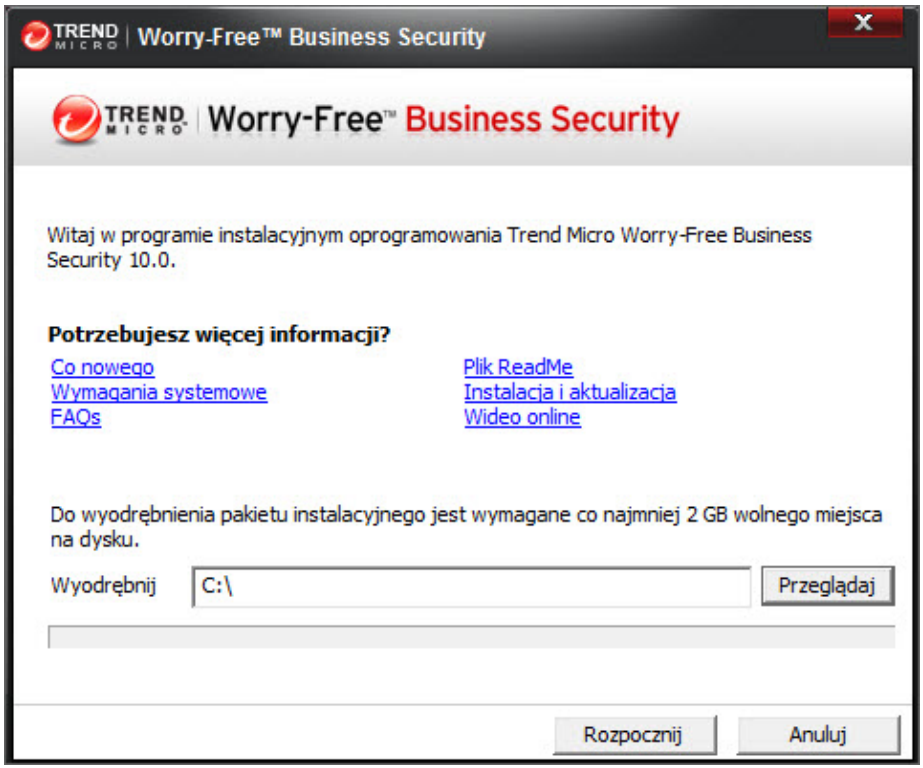
Etap 1: Rozpoczynanie instalacji programu Security Server

Przed rozpoczęciem

- Zaloguj się na komputerze, używając konta z uprawnieniami administratora domeny lub lokalnego.
- Przed rozpoczęciem instalacji programu Worry-Free Business Security zamknij wszystkie uruchomione aplikacje. Jeżeli podczas instalacji są uruchomione inne aplikacje, proces ten może potrwać dłużej.
- Upewnij się, że instalacja serwera Security Server nie jest wykonywana na komputerze, na którym działają aplikacje mogące zablokować usługę IIS. Może to spowodować niepowodzenie instalacji. Więcej informacji zawiera dokumentacja serwera IIS.
- Instalacja programu Trend Micro Security Server nie wymaga ponownego uruchamiania komputera. Po zakończeniu instalacji natychmiast skonfiguruj ustawienia konsoli internetowej, a następnie przejdź do instalowania programów Security Agent na klientach.

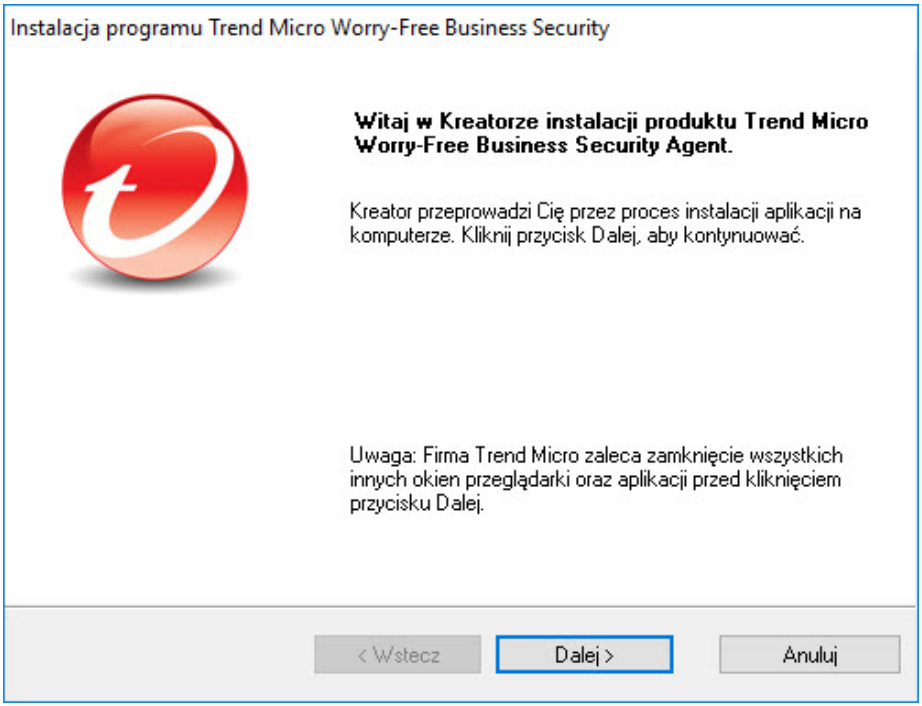
Uruchamianie pakietu instalacyjnego

Dwukrotnie kliknij pakiet instalacyjny (plik `.exe`).

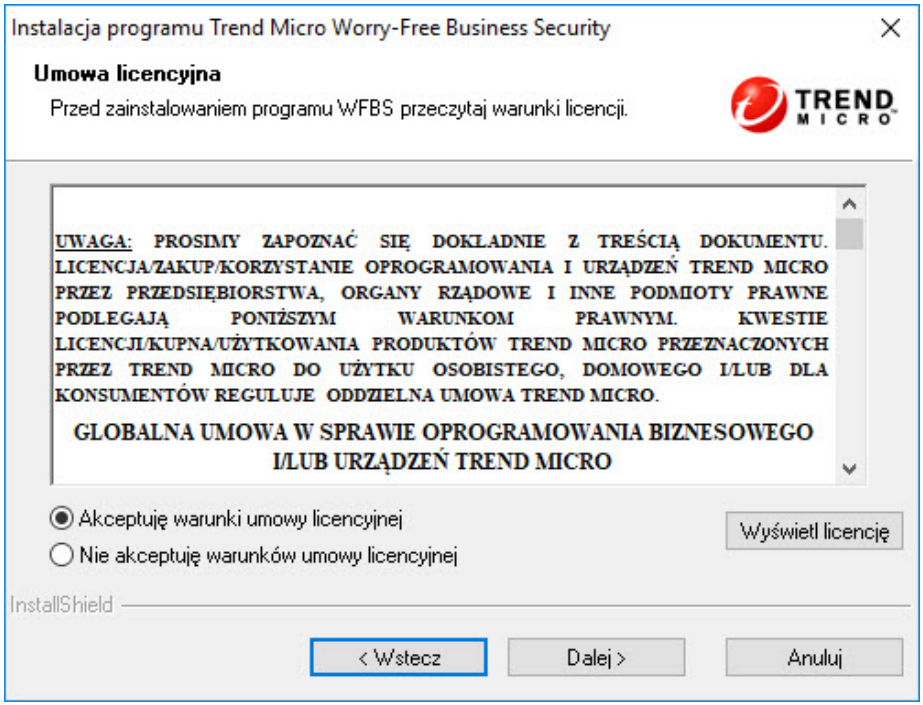


Pliki instalacyjne zostaną wyodrębnione do tego samego katalogu, w którym znajduje się plik `.exe`. Aby zmienić ścieżkę, kliknij przycisk **Przeglądaj** i wskaż odpowiedni katalog.

Po kliknięciu pozycji **Rozpocznij** program instalacyjny zacznie wyodrębniać pliki. Stan wyodrębniania jest wyświetlany na pasku stanu u dołu okna. Po zakończeniu wyodrębniania zostanie wyświetlony ekran powitalny.

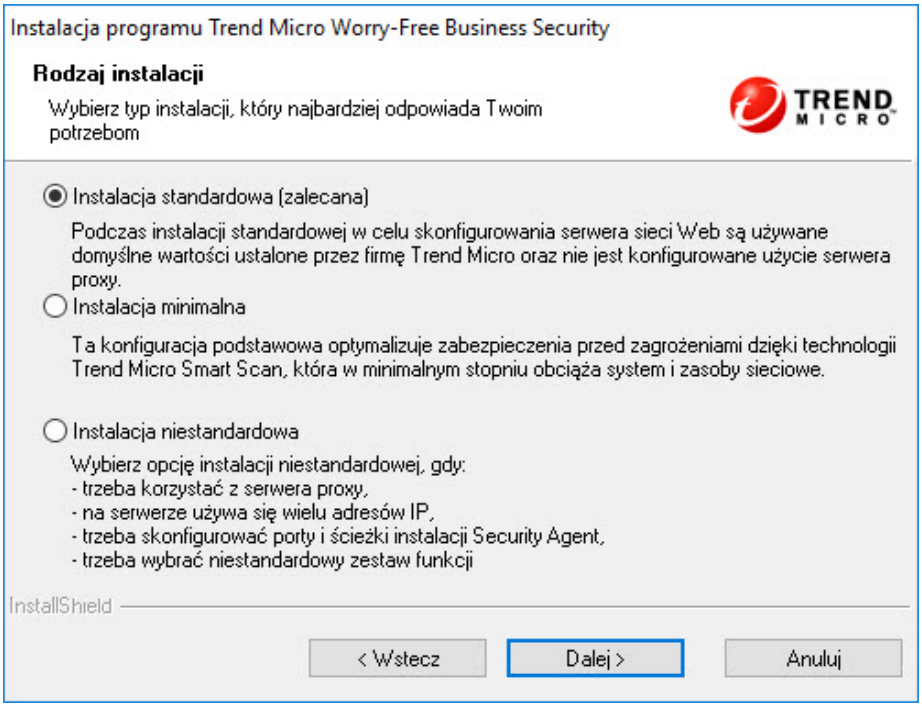

Instalacja programu Trend Micro Worry-Free Business Security
Witaj w Kreatorze instalacji produktu Trend Micro Worry-Free Business Security Agent.
Kreator przeprowadzi Cię przez proces instalacji aplikacji na komputerze. Kliknij przycisk Dalej, aby kontynuować.
Uwaga: Firma Trend Micro zaleca zamknięcie wszystkich innych okien przeglądarki oraz aplikacji przed kliknięciem przycisku Dalej.
< Wstecz
Dalej >
Anuluj

Umowa licencyjna



Przeczytaj umowę licencyjną. Jeśli zgadzasz się z jej warunkami, wybierz pozycję **Akceptuję warunki umowy licencyjnej**.

Rodzaj instalacji



Wybierz jedną z następujących opcji:

Instalacja standardowa (zalecana)

Ta metoda jest odpowiednia dla programu Security Server zarządzającego maksymalnie 100 agentami.

Podczas instalacji standardowej:

- Po instalacji następujące funkcje zostają automatycznie włączone:
  - Oprogramowanie antywirusowe/anty-spyware
  - Monitorowanie zachowania (tylko dla platform komputerowych, takich jak Windows 7)

- Usługa Web Reputation
- Filtrowanie adresów URL
- Smart Scan

Uwaga

Programy Security Agent muszą spełniać minimalne wymagania systemowe niezbędne do uruchomienia funkcji Smart Scan. Lista wymagań jest dostępna pod adresem http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx.

- W przypadku nieobecności programu Security Agent jest on automatycznie instalowany na tym samym komputerze co serwer Security Server.

Uwaga

Program Security Agent można zainstalować na innych klientach w sieci i zarządzać nimi za pomocą konsoli internetowej. Szczegółowe informacje na temat różnych metod instalacji programu Security Agent można znaleźć w Podręczniku administratora.

- Jeśli na komputerze zainstalowane jest inne oprogramowanie zabezpieczające punkt końcowy, program instalacyjny odinstaluje najpierw to oprogramowanie, a następnie zainstaluje program Security Agent.

Uwaga

Niektóre rodzaje oprogramowania zabezpieczającego punkt końcowy można jedynie wykryć, ale nie da się ich odinstalować. W takim przypadku należy najpierw odinstalować oprogramowanie ręcznie.

Listę programów zabezpieczających punkt końcowy, które mogą być odinstalowane lub tylko wykryte bez możliwości odinstalowania, można znaleźć w następującej witrynie internetowej:

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

Instalacja minimalna

Podczas instalacji minimalnej:

- Po instalacji włączona zostaje tylko funkcja ochrony antywirusowej/ antyszpiegowskiej.
- W przypadku nieobecności programu Security Agent jest on automatycznie instalowany na tym samym komputerze co serwer Security Server.

Uwaga

Program Security Agent można zainstalować na innych klientach w sieci i zarządzać nimi za pomocą konsoli internetowej. Szczegółowe informacje na temat różnych metod instalacji programu Security Agent można znaleźć w Podręczniku administratora.

- Jeśli na komputerze zainstalowane jest inne oprogramowanie zabezpieczające punkt końcowy, program instalacyjny odinstaluje najpierw to oprogramowanie, a następnie zainstaluje program Security Agent.

Uwaga

Niektóre rodzaje oprogramowania zabezpieczającego punkt końcowy można jedynie wykryć, ale nie da się ich odinstalować. W takim przypadku należy najpierw odinstalować oprogramowanie ręcznie.

Listę programów zabezpieczających punkt końcowy, które mogą być odinstalowane lub tylko wykryte bez możliwości odinstalowania, można znaleźć w następującej witrynie internetowej:

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

Instalacja niestandardowa

W przypadku instalacji niestandardowej użytkownik ma dodatkowe możliwości konfiguracji serwera Security Server oraz agentów zgodnie ze strategią zabezpieczeń sieci. Ta metoda jest odpowiednia, gdy serwer Security Server ma zarządzać dużą liczbą agentów.

Podczas instalacji niestandardowej następujące ustawienia są **opcjonalne**:

- W przypadku nieobecności programu Security Agent, należy go automatycznie zainstalować na tym samym komputerze co serwer Security Server.

Uwaga

Program Security Agent można zainstalować na innych klientach w sieci i zarządzać nimi za pomocą konsoli internetowej. Szczegółowe informacje na temat różnych metod instalacji programu Security Agent można znaleźć w Podręczniku administratora.

- Jeśli na komputerze zainstalowane jest inne oprogramowanie zabezpieczające punkt końcowy, program instalacyjny odinstaluje najpierw to oprogramowanie, a następnie zainstaluje program Security Agent.

Uwaga

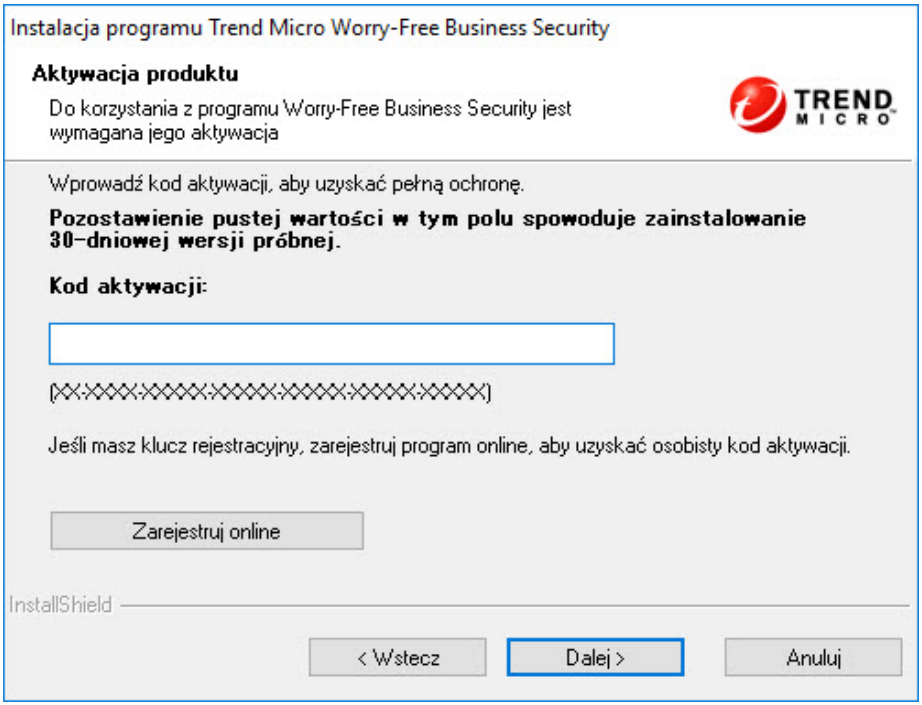
Niektóre rodzaje oprogramowania zabezpieczającego punkt końcowy można jedynie wykryć, ale nie da się ich odinstalować. W takim przypadku należy najpierw odinstalować oprogramowanie ręcznie.

Listę programów zabezpieczających punkt końcowy, które mogą być odinstalowane lub tylko wykryte bez możliwości odinstalowania, można znaleźć w następującej witrynie internetowej:

http://esupport.trendmicro.com/solution/en-US/1060980.aspx

- Program Messaging Security Agent można zainstalować na tym samym komputerze co serwer Security Server (jeśli istnieje serwer Microsoft Exchange) lub na klientach zdalnych.

Aktywacja produktu



Wpisz kod aktywacji w polu **Kod aktywacji**.

W przypadku braku kodu aktywacyjnego, rejestracja tej kopii programu Worry-Free Business Security nie jest możliwa. Kliknij przycisk **Rejestracja w trybie online**, aby otworzyć nowe okno przeglądarki. Postępuj zgodnie z instrukcjami pojawiającymi się na ekranie Rejestracja. Możesz również kliknąć przycisk **Dalej**, aby zainstalować wersję próbną. Jeśli w ciągu 30 dni zostanie ona uaktualniona do pełnej wersji, wszystkie ustawienia pozostaną niezmienione.

Przegląd programu instalacyjnego

Na ekranie Przegląd programu instalacyjnego wyświetlane są składniki wymagające konfiguracji w celu zainstalowania programów Trend Micro Security Server, Security Agent lub Messaging Security Agent.

Po kliknięciu przycisku **Dalej**:

- Jeśli wybrana opcja to Instalacja standardowa/minimalna, przejdź do:
  - *Konfigurowanie ustawień instalacji standardowej lub minimalnej na stronie 2-26*
  - *Etap 3: Proces instalacji na stronie 2-52*
- Jeśli wybrana opcja to Instalacja niestandardowa, przejdź do:

- *Konfigurowanie ustawień instalacji niestandardowej na stronie 2-31*
- *Etap 3: Proces instalacji na stronie 2-52*

Etap 2: konfigurowanie ustawień w zależności od typu instalacji

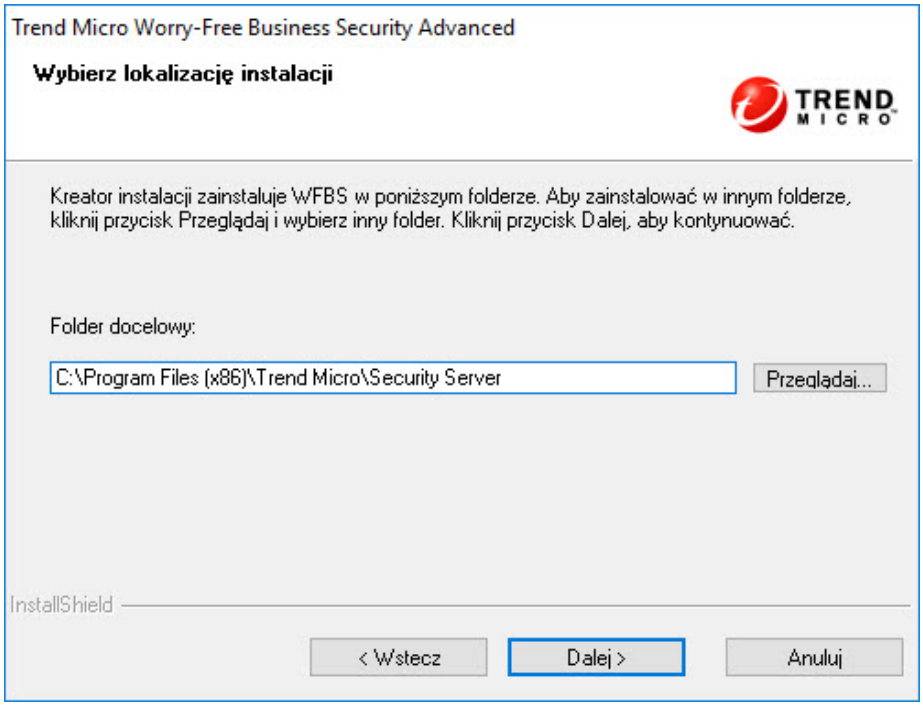
Ustawienia, które należy skonfigurować na etapie 2, zależą od typu instalacji wybranego na etapie 1.

- *Konfigurowanie ustawień instalacji standardowej lub minimalnej na stronie 2-26*
- *Konfigurowanie ustawień instalacji niestandardowej na stronie 2-31*

Konfigurowanie ustawień instalacji standardowej lub minimalnej

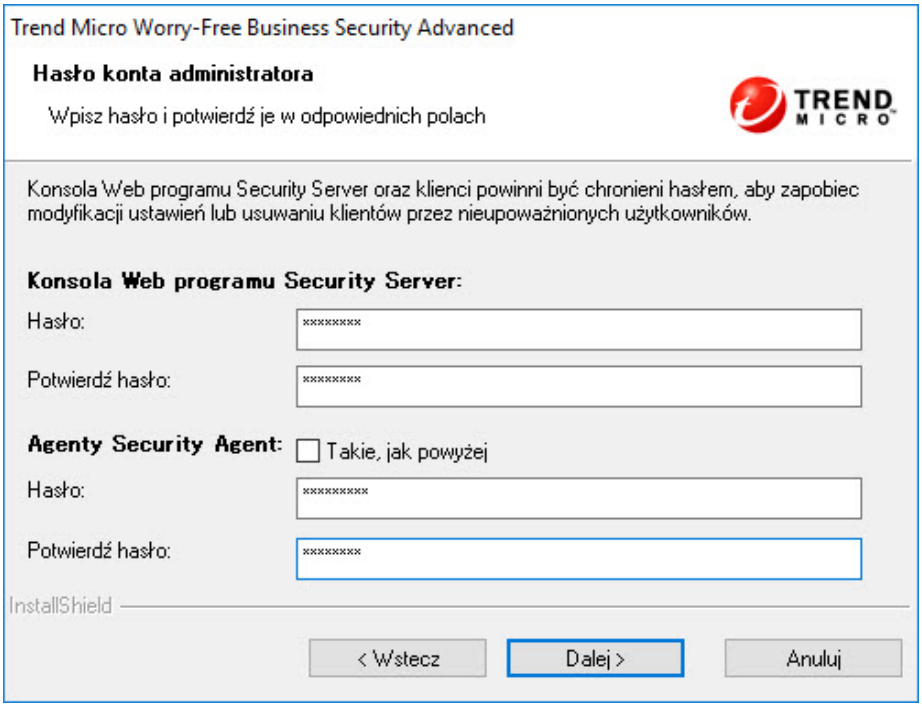
W przypadku przeprowadzania instalacji standardowej lub minimalnej wyświetlane są kolejno następujące ekrany:

Lokalizacja instalacji



Domyślny folder instalacji programu Worry-Free Business Security to `C:\Program Files\Trend Micro\Security Server` lub `C:\Program Files (x86)\Trend Micro\Security Server`. Kliknij przycisk **Przeglądaj**, jeśli chcesz zainstalować program Worry-Free Business Security w innym folderze.

Hasło konta administratora



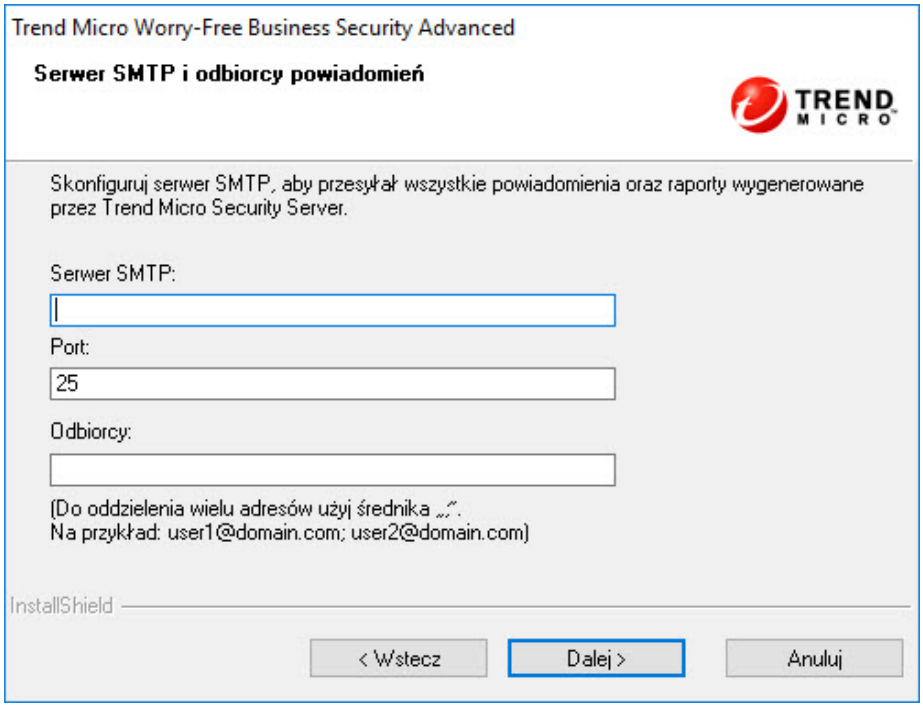
Należy ustalić różne hasła dla konsoli internetowej serwera Security Server i programu Security Agent.

- **Konsola internetowa programu Security Server**: wymagane do zalogowania się do konsoli internetowej.
- **Programy Security Agent**: wymagane do odinstalowania lub zamknięcia programów Security Agent na komputerach klienckich.

Uwaga

W polu hasła rozróżniane są wielkie i małe litery, można w nim wpisać od 1 do 24 znaków.

Serwer SMTP i odbiorcy powiadomień



Określ następujące informacje:

- **Serwer SMTP**: adres serwera SMTP użytkownika.

  Uwaga

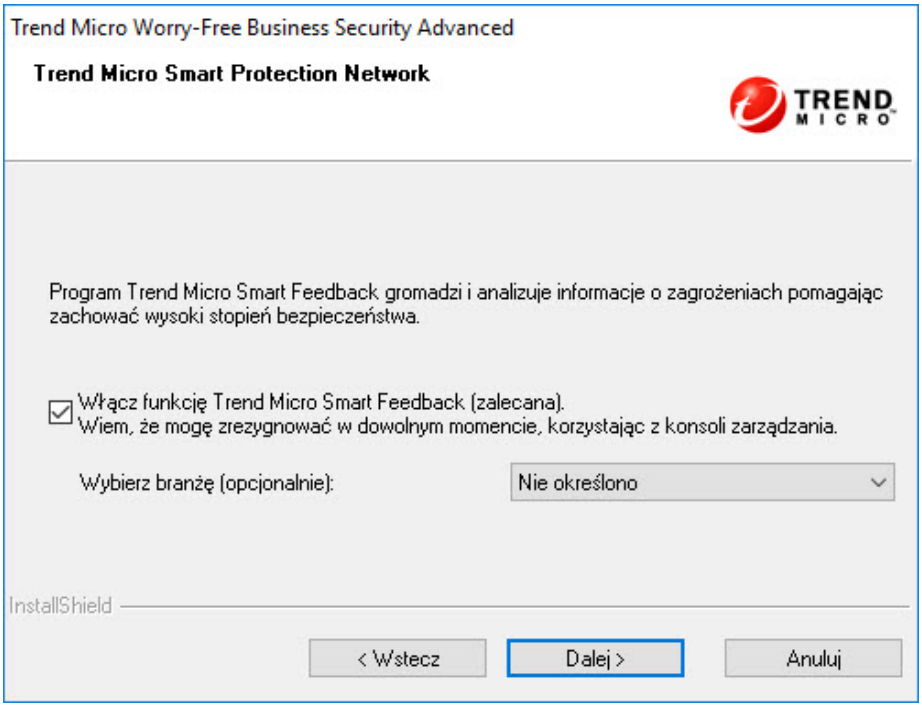
  Jeśli serwer SMTP znajduje się na tym samym komputerze co program WFBS i korzysta z portu 25, program instalacyjny wykrywa nazwę serwera SMTP i aktualizuje pola Serwer SMTP i Port.

- **Port**: port używany przez serwer SMTP do komunikacji.

- **Odbiorcy**: Adresy e-mail używane przez serwer SMTP do wysyłania powiadomień o alarmach. Można wpisać wiele adresów e-mail, jeśli powiadomienia mają byc wysyłane do więcej niż jednej osoby.

Należy sprawdzić ustawienia serwera pocztowego u lokalnego usługodawcy internetowego. Jeżeli nie można uzyskać tych ustawień, należy przejść do następnego kroku. Po zakończeniu instalacji można zaktualizować ustawienia SMTP. Szczegółowe instrukcje zawiera Podręcznik administratora.

Smart Protection Network



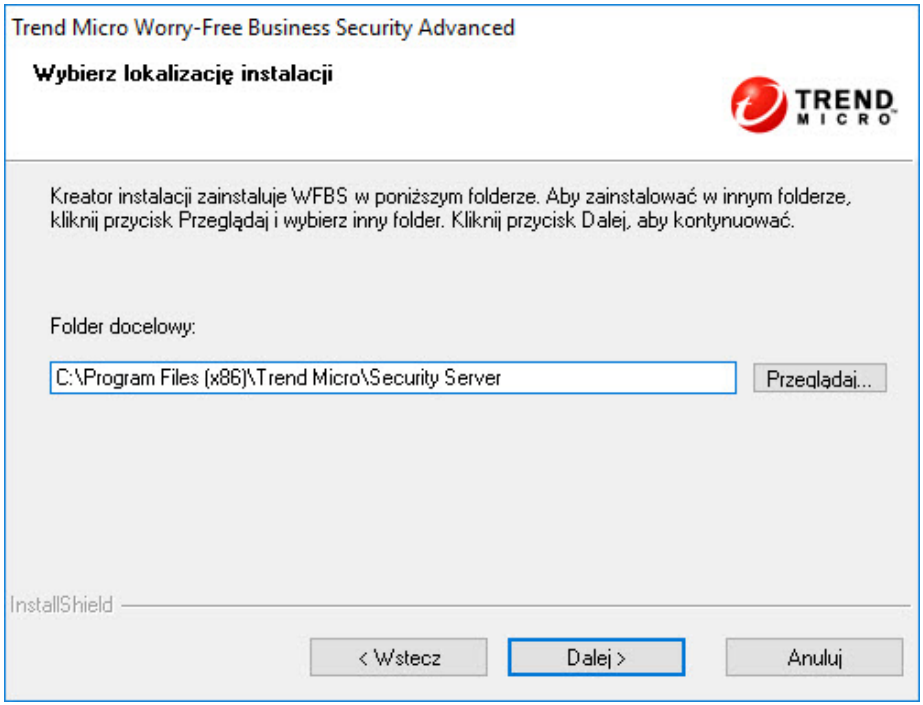
Zdecyduj, czy chcesz uczestniczyć w programie wysyłania informacji Trend Micro Smart Protection Network.

Za pomocą tej opcjonalnej funkcji można przesyłać do firmy Trend Micro informacje dotyczące zarażeń złośliwym oprogramowaniem. Firma Trend Micro zaleca pozostawienie domyślnej wartości, ponieważ dzięki wykorzystaniu informacji programów Worry-Free Business Security podnosi się skuteczność ochrony przed złośliwym oprogramowaniem oferowana przez tę firmę. Można również zrezygnować z uczestnictwa później, korzystając z konsoli internetowej.

Konfigurowanie ustawień instalacji niestandardowej

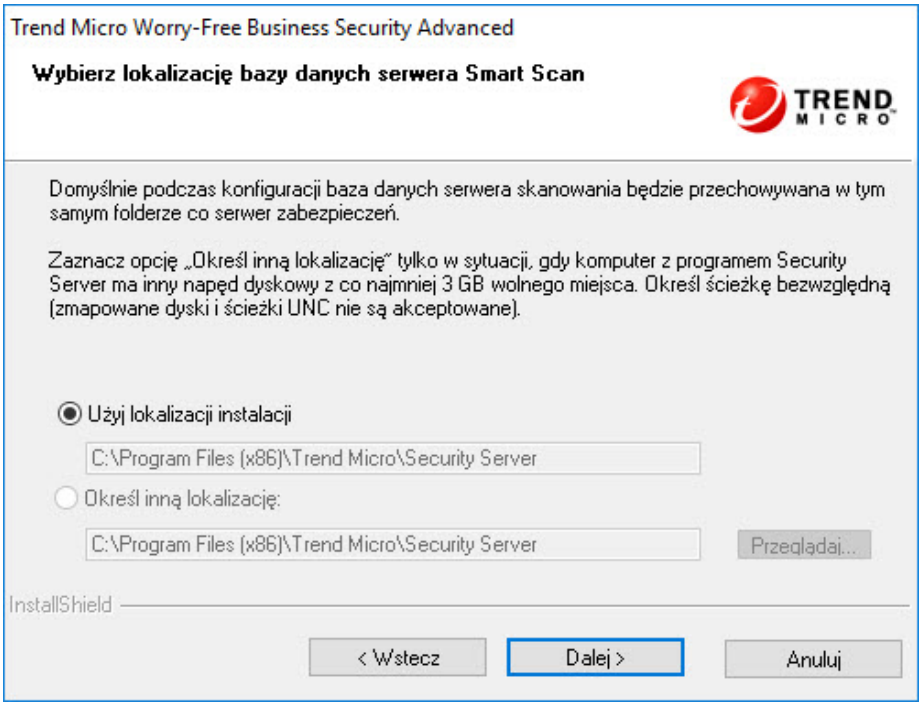
Podczas przeprowadzania instalacji niestandardowej wyświetlane są kolejno następujące ekrany:

Lokalizacja instalacji



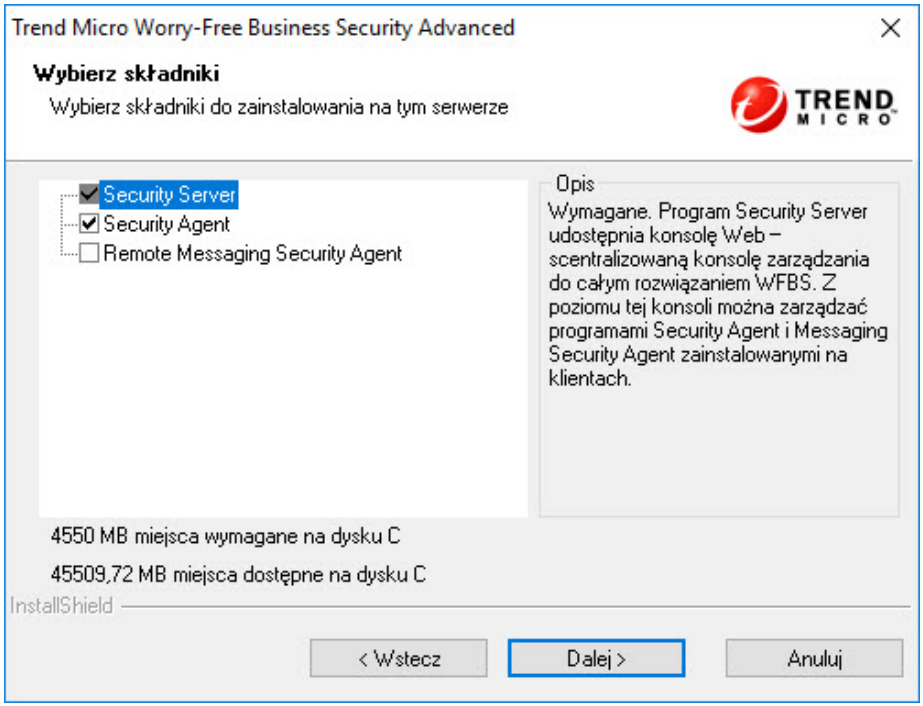
Domyślny folder instalacji programu Worry-Free Business Security to `C:\Program Files\Trend Micro\Security Server` lub `C:\Program Files (x86)\Trend Micro\Security Server`. Kliknij przycisk **Przeglądaj**, jeśli chcesz zainstalować program Worry-Free Business Security w innym folderze.

Lokalizacja bazy danych serwera skanowania



Wybierz opcję **Użyj lokalizacji instalacji**, aby zapisać bazę danych serwera skanowania w tym samym folderze, w którym zainstalowano serwer Security Server, lub opcję **Określ inną lokalizację** i wpisz ścieżkę bezwzględną do innej lokalizacji na serwerze Security Server. Nie można wybrać zmapowanego dysku ani ścieżki UNC.

Wybierz składniki



Wybierz składniki, które mają zostać zainstalowane na komputerze docelowym:

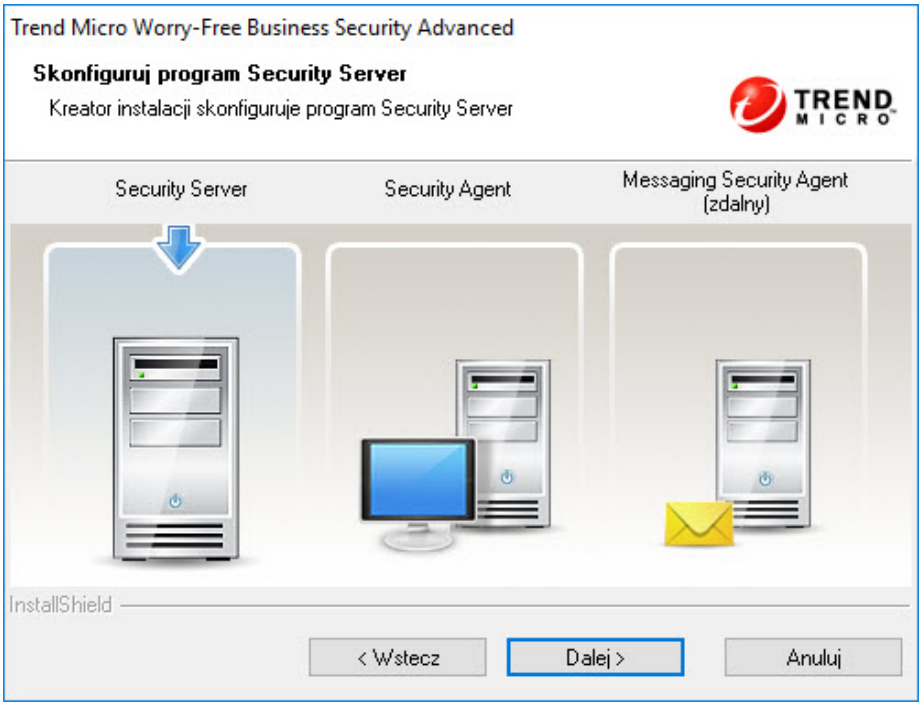
- **Security Server** (wymagany): Na serwerze Security Server znajduje się scentralizowana konsola internetowa.
- **Security Agent** (opcjonalny): Agent zapewniający ochronę komputerom i serwerom.
- **Messaging Security Agent** (opcjonalny): W przypadku instalacji serwera Security Server na komputerze z zainstalowanym serwerem Microsoft Exchange program instalacyjny wyświetla monit o wykonanie instalacji lokalny programu Messaging Security Agent (tylko w wersji Advanced).

- **Remote Messaging Security Agent** (opcjonalny): W przypadku instalacji serwera Security Server na komputerze, który nie wykrywa serwerów Microsoft Exchange, program instalacyjny monituje o zainstalowanie zdalny wersji programu Messaging Security Agent na serwerach zdalnych (tylko wersja Advanced).

Uwaga

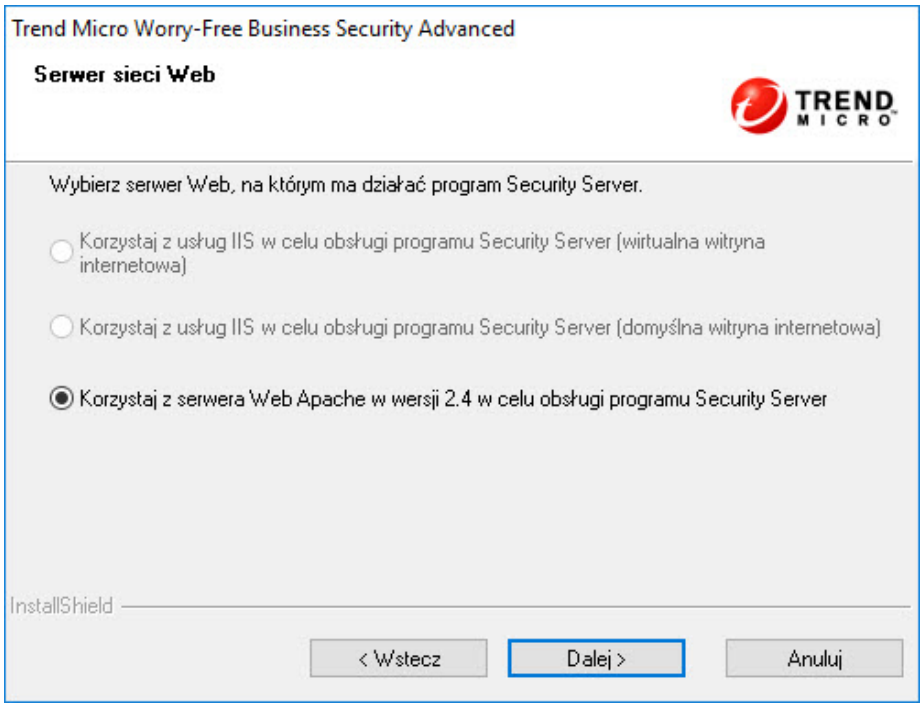
W przypadku instalacji serwera Security Server na komputerze z zainstalowanym serwerem Exchange zdalny program Messaging Security Agent nie zostanie wyświetlony na ekranie wyboru składników. Widoczny będzie wyłącznie lokalny program Messaging Security Agent.

Skonfiguruj program Security Server



Na ekranie konfiguracji serwera Security Server dostępne są ustawienia, które należy skonfigurować.

Serwer sieci Web



W przypadku nowej instalacji program instalacyjny sprawdza, czy na komputerze docelowym istnieje serwer sieci Web.

Scenariusz	Wynik	Uwagi

Program instalacyjny wykrywa zarówno serwer sieci Web IIS, jak i Apache.	• W przypadku instalacji typowej lub minimalnej program instalacyjny automatycznie używa serwera IIS.
	• W przypadku instalacji niestandardowej:
	  • Jeśli dana wersja serwera sieci Web Apache nie jest obsługiwana, program instalacyjny automatycznie używa serwera IIS.
	  • Jeśli dana wersja serwera sieci Web Apache jest obsługiwana, można wybrać dowolny z dwóch serwerów sieci Web.
		Jeśli na komputerze zainstalowany jest system operacyjny Windows 7, 8.1 lub 10, firma Trend Micro zaleca przeprowadzenie instalacji niestandardowej i wybór Apache jako serwera sieci Web.

Program instalacyjny wykrywa tylko serwer sieci Web IIS	• W przypadku instalacji typowej lub minimalnej program instalacyjny automatycznie używa serwera IIS. • W przypadku instalacji niestandardowej można wybrać dowolny z dwóch serwerów sieci Web. W przypadku wybrania serwera Apache automatycznie zainstalowany zostanie serwer Apache w wersji 2.4.	

SCENARIUSZ	WYNIK	UWAGI

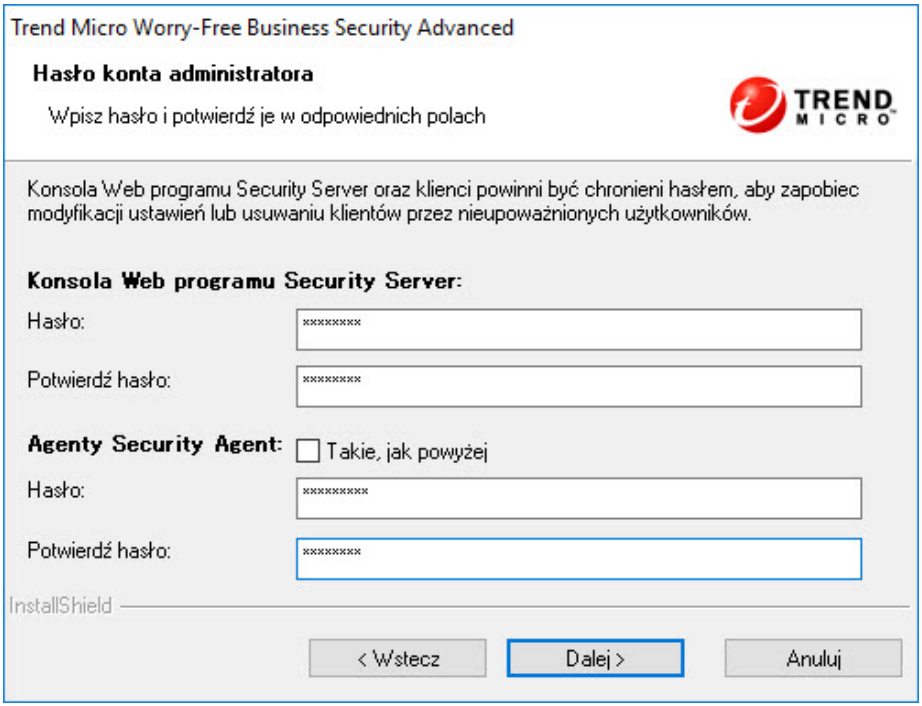
Program instalacyjny wykrywa tylko serwer sieci Web Apache	• Jeśli serwer Apache jest w wersji 2.4, program instalacyjny używa serwera Apache.
	• W przypadku innych wersji serwera Apache nie można kontynuować instalacji. Należy rozważyć wykonanie następujących czynności:
	  • Odinstalować serwer Apache, jeśli żadna aplikacja z niego nie korzysta.
	  • Zaktualizować serwer Apache do wersji 2.4.
	  • Zainstalować program Security Server na innym komputerze.
		Następujące platformy są wyposażone w serwer IIS i współdziałają z programem Security Server:
		• Windows Server 2008/2008 R2
		• Windows SBS 2008
		• Windows EBS 2008
		• Windows SBS 2011 Standard/Essentials
		• Windows Server 2012/2012 R2
		• Windows Server 2016
		Jeśli program instalacyjny nie jest w stanie wykryć serwera IIS na tych platformach, może on być wyłączony (domyślnie lub przez administratora systemu). W takim przypadku należy włączyć serwer IIS.

Program instalacyjny nie wykrywa żadnego serwera sieci Web	Program instalacyjny automatycznie instaluje serwer sieci Web Apache 2.4.	

W przypadku uaktualniania, jeśli aktualnie jako serwer sieci Web używany jest serwer Apache:

- Jeśli serwer sieci Web Apache został zainstalowany przez program instalacyjny produktu Worry-Free Business Security 8.x/9.x, serwer Apache zostanie automatycznie zaktualizowany do wersji 2.4.
- W przypadku zainstalowania przez inne programy program instalacyjny zachowa istniejącą wersję serwera Apache.

Hasło konta administratora



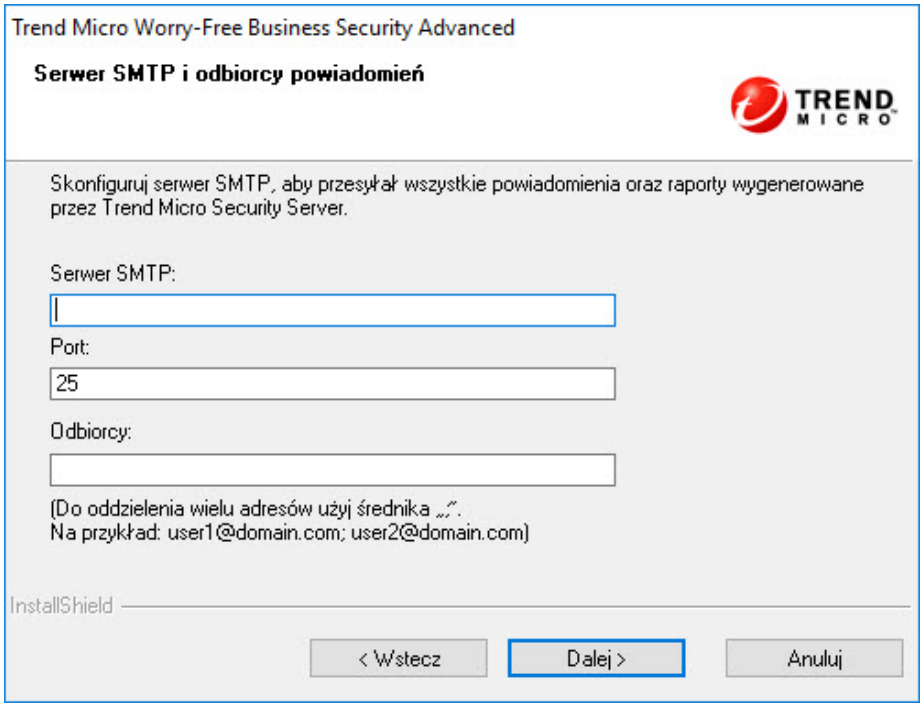
Należy ustalić różne hasła dla konsoli internetowej serwera Security Server i programu Security Agent.

- **Konsola internetowa programu Security Server**: wymagane do zalogowania się do konsoli internetowej.
- **Programy Security Agent**: wymagane do odinstalowania lub zamknięcia programów Security Agent na komputerach klienckich.

Uwaga

W polu hasła rozróżniane są wielkie i małe litery, można w nim wpisać od 1 do 24 znaków.

Serwer SMTP i odbiorcy powiadomień



Określ następujące informacje:

- **Serwer SMTP**: adres serwera SMTP użytkownika.

  Uwaga

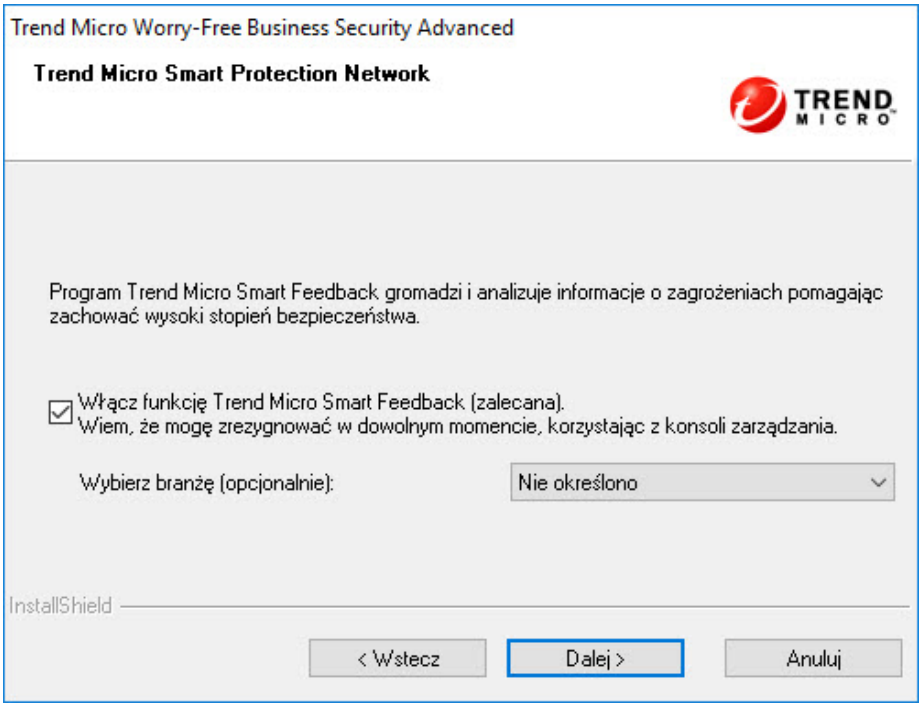
  Jeśli serwer SMTP znajduje się na tym samym komputerze co program WFBS i korzysta z portu 25, program instalacyjny wykrywa nazwę serwera SMTP i aktualizuje pola Serwer SMTP i Port.

- **Port**: port używany przez serwer SMTP do komunikacji.

- **Odbiorcy**: Adresy e-mail używane przez serwer SMTP do wysyłania powiadomień o alarmach. Można wpisać wiele adresów e-mail, jeśli powiadomienia mają byc wysyłane do więcej niż jednej osoby.

Należy sprawdzić ustawienia serwera pocztowego u lokalnego usługodawcy internetowego. Jeżeli nie można uzyskać tych ustawień, należy przejść do następnego kroku. Po zakończeniu instalacji można zaktualizować ustawienia SMTP. Szczegółowe instrukcje zawiera Podręcznik administratora.

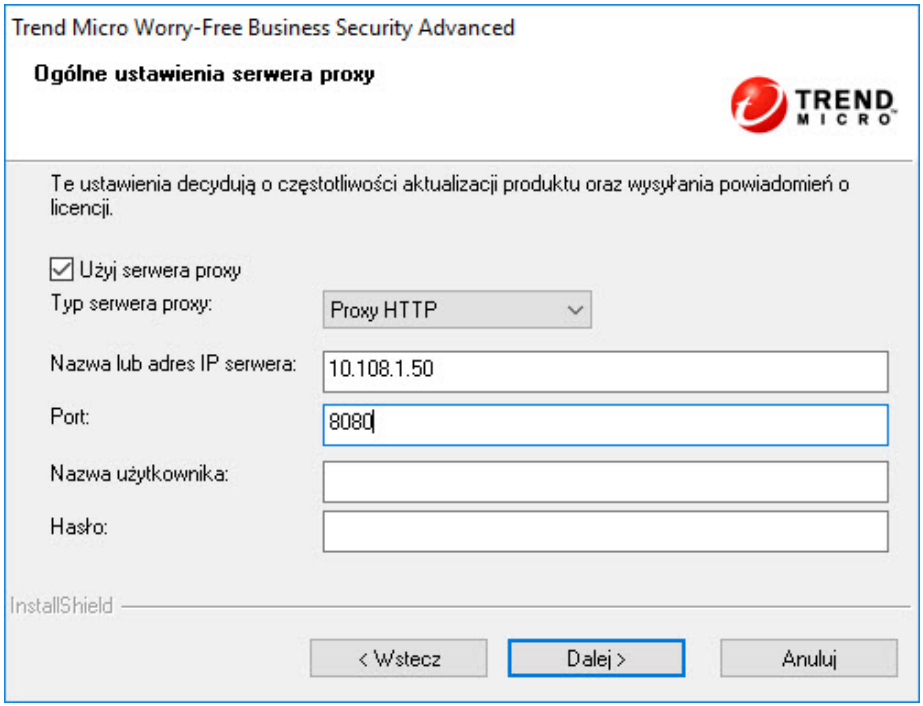
Smart Protection Network



Zdecyduj, czy chcesz uczestniczyć w programie wysyłania informacji Trend Micro Smart Protection Network.

Za pomocą tej opcjonalnej funkcji można przesyłać do firmy Trend Micro informacje dotyczące zarażeń złośliwym oprogramowaniem. Firma Trend Micro zaleca pozostawienie domyślnej wartości, ponieważ dzięki wykorzystaniu informacji programów Worry-Free Business Security podnosi się skuteczność ochrony przed złośliwym oprogramowaniem oferowana przez tę firmę. Można również zrezygnować z uczestnictwa później, korzystając z konsoli internetowej.

Ogólne ustawienia serwera proxy

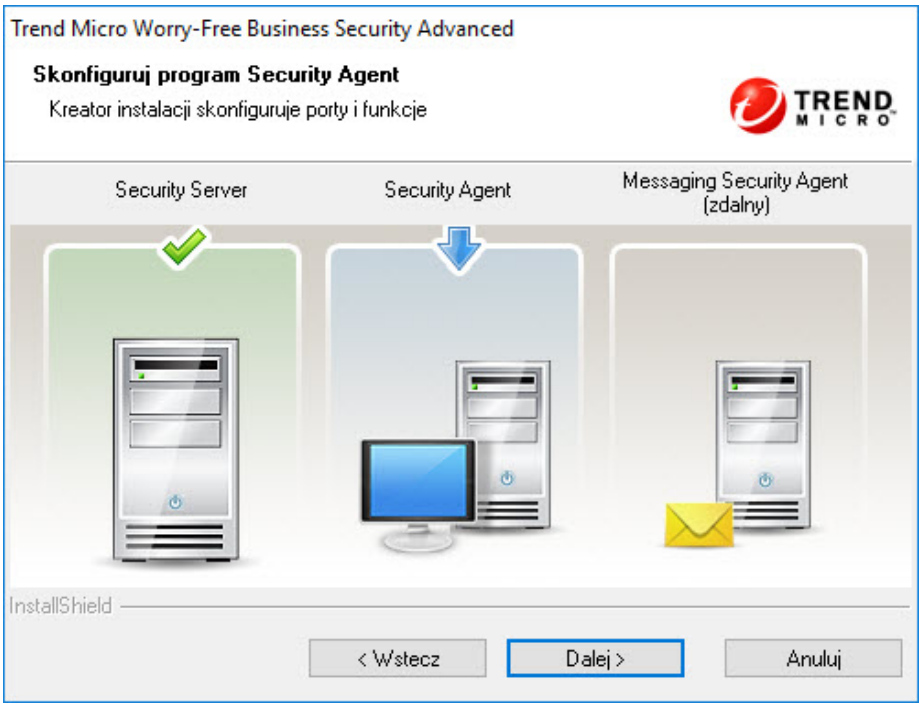


Jeżeli w celu uzyskania dostępu do Internetu wymagany jest serwer proxy, należy zaznaczyć pole wyboru **Użyj serwera proxy** i podać następujące informacje:

- **Typ serwera proxy**

- **Nazwa lub adres IP serwera**
- **Port**
- **Nazwa użytkownika i hasło**: podawane tylko wtedy, gdy serwer proxy wymaga uwierzytelnienia.

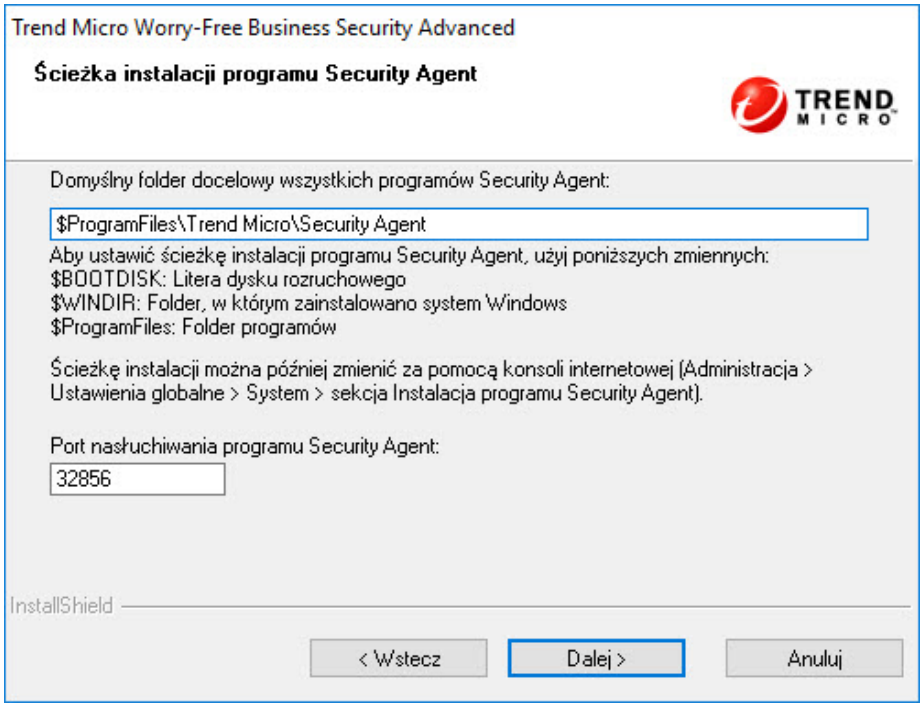
Skonfiguruj program Security Agent



Na ekranie konfiguracji programu Security Agent dostępne są ustawienia, które należy skonfigurować.

Po zainstalowaniu serwera Security Server należy zainstalować program Security Agent na komputerach klienckich w sieci. Szczegółowe informacje na temat różnych metod instalacji programu Security Agent można znaleźć w Podręczniku administratora.

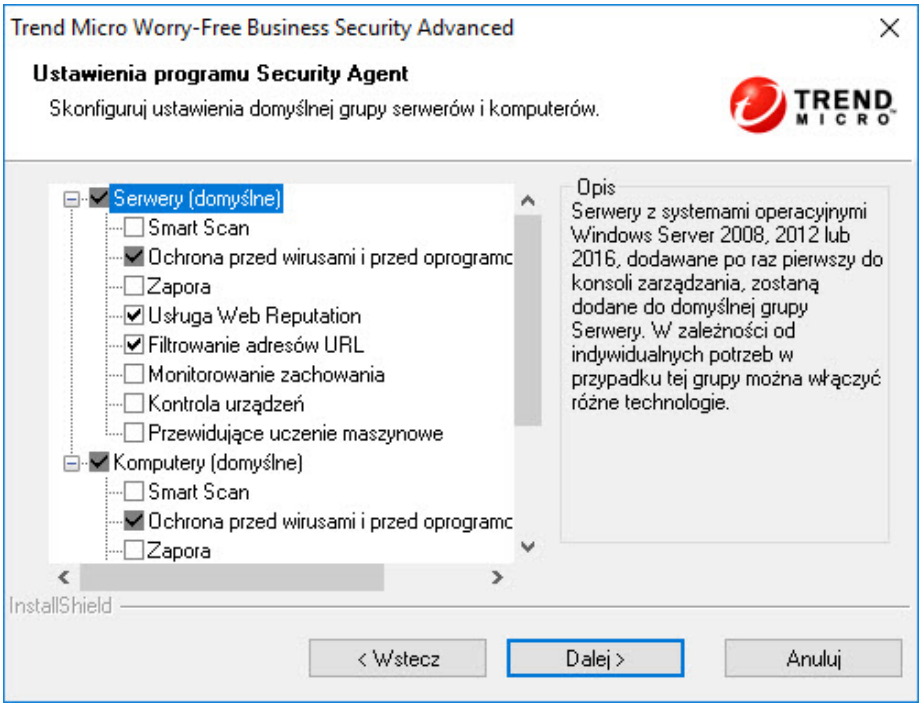
Ścieżka instalacji programu Security Agent



Ustaw następujące elementy:

- **Ścieżka instalacji**: folder docelowy, w którym instalowane są pliki programu Security Agent.
- **port nasłuchiwania programu Security Agent**: Numer portu używanego do komunikacji pomiędzy programem Security Agent i serwerem Security Server.

Ustawienia programu Security Agent



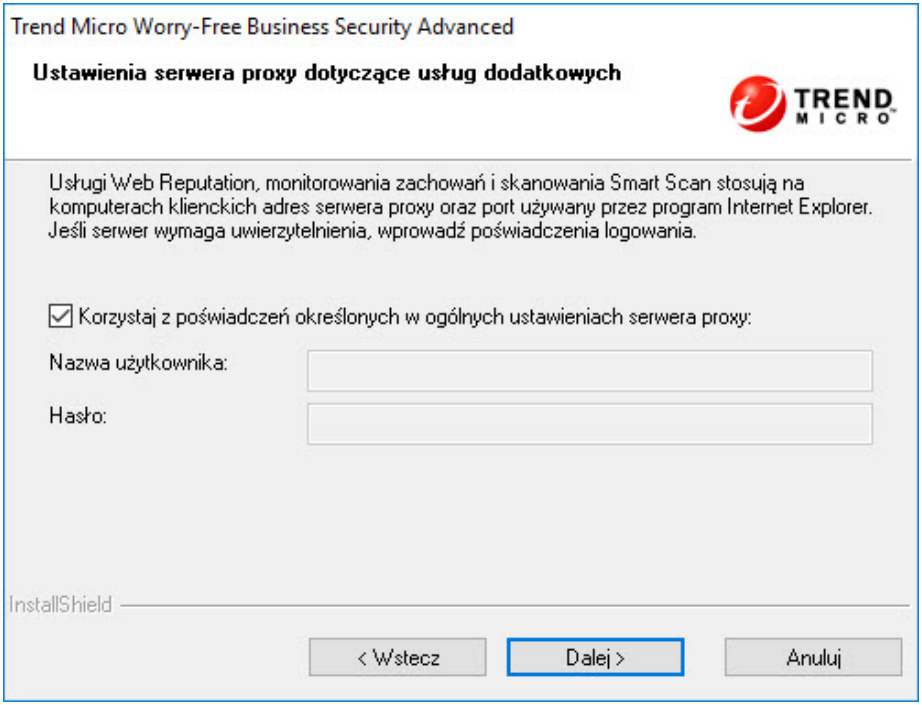
Należy skonfigurować ustawienia programu Security Agent dla serwerów i komputerów.

- **Serwery**: przy dodawaniu do konsoli internetowej nowe programy Security Agent uruchomione na platformach serwerowych Windows (np. Windows Server 2008) zostaną dodane do domyślnej grupy Serwery. W zależności od indywidualnych potrzeb w przypadku tej grupy można włączyć różne technologie.
- **Komputery**: przy dodawaniu do konsoli Web nowe programy Security Agent uruchomione na platformach Windows dla komputerów stacjonarnych (np. Windows 7) zostaną dodane do domyślnej grupy Komputery. W zależności od indywidualnych potrzeb w przypadku tej grupy można włączyć różne technologie.

W każdej grupie można skonfigurować następujące składniki:

- **Smart Scan**: usługa Smart Scan wykorzystuje centralny serwer skanowania w sieci, który przejmuje część obciążenia związanego z zadaniami skanowania otrzymywanymi od klientów.
- **Ochrona przed wirusami i przed oprogramowaniem spyware**: Skanuje pliki podczas otwierania lub tworzenia w poszukiwaniu złośliwego kodu
- **Zapora**: chroni klienty przed atakami złośliwych programów i wirusami sieciowymi, tworząc barierę między komputerami klienckimi a siecią.
- **Usługa Web Reputation**: blokuje złośliwe witryny sieci Web na podstawie informacji dotyczących wiarygodności domen sieci Web oraz przypisuje ocenę reputacji na podstawie różnych czynników.
- **Filtrowanie adresów URL**: blokuje określone kategorie witryn sieci Web (np. pornograficzne lub portale społecznościowe) zgodnie z polityką firmy.
- **Monitorowanie zachowania**: analizuje zachowanie programów, aby aktywnie wykrywać znane i nieznane zagrożenia.
- **Kontrola urządzeń**: nadzoruje dostęp do urządzeń pamięci zewnętrznej i zasobów sieciowych.
- **Przewidujące uczenie maszynowe**: wykorzystuje zaawansowaną technologię uczenia maszynowego w celu kojarzenia informacji o zagrożeniach i wykonywania szczegółowej analizy plików, aby wykrywać pojawiające się nieznane zagrożenia bezpieczeństwa przy użyciu badania cyfrowych odcisków linii papilarnych DNA, mapowania API i innych cech plików.

Ustawienia serwera proxy dotyczące usług dodatkowych



Usługi **Smart Scan**, **Usługa Web Reputation** i **Monitorowanie zachowania** stosują na komputerach klienckich adres serwera proxy oraz port używany przez program Internet Explorer. Jeśli serwer proxy wymaga uwierzytelnienia, należy wprowadzić poświadczenia logowania na tym ekranie.

Konfigurowanie programu Messaging Security Agent

Program Messaging Security Agent należy zainstalować podczas instalacji serwera Security Server.

Przypomnienia i uwagi dotyczące instalacji:

- Nie ma konieczności zatrzymywania lub uruchamiania usług Microsoft Exchange przed rozpoczęciem lub zakończeniem instalacji.
- Jeżeli na komputerze klienckim zapisane są informacje z poprzedniej instalacji programu Messaging Security Agent, instalacja nowej wersji programu nie będzie możliwa. Użyj narzędzia Windows Installer Cleanup Utility do usunięcia pozostałości z poprzedniej instalacji. Aby pobrać narzędzie Windows Installer Cleanup Utility, należy odwiedzić następującą stronę:

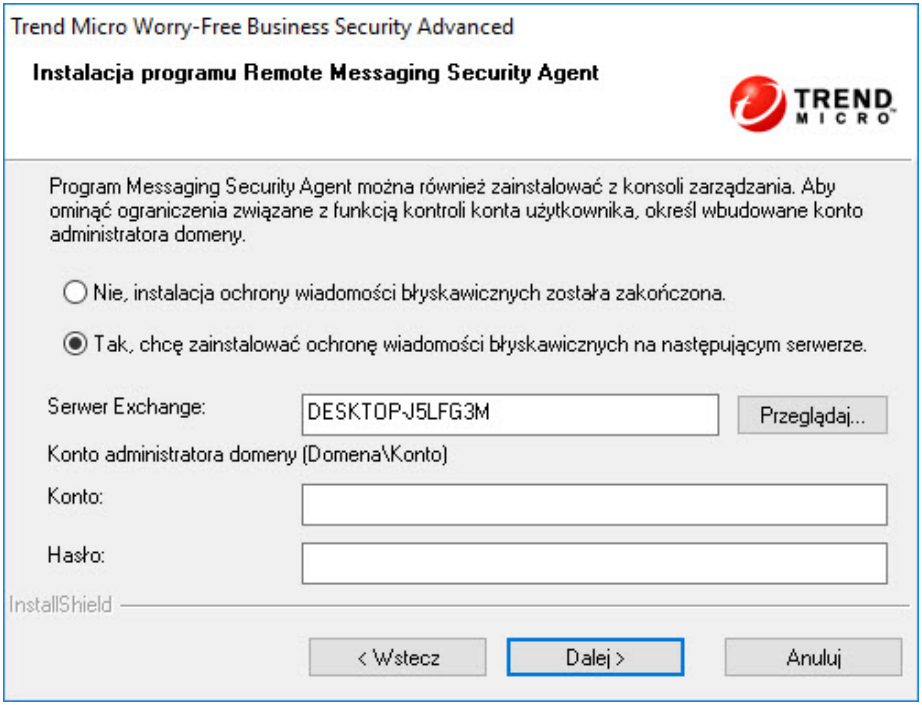
  https://support.microsoft.com/en-us/help/290301
- W przypadku instalowania programu Messaging Security Agent na serwerze, na którym uruchomione są narzędzia blokowania, należy te narzędzia usunąć, aby nie wyłączały usługi IIS, bez której instalacja nie powiodłaby się.
- Program Messaging Security Agent można również zainstalować z poziomu konsoli internetowej po zainstalowaniu serwera Security Server. Szczegółowe informacje, patrz Podręcznik administratora.

Program instalacyjny wyświetla monit o zainstalowanie programu Messaging Security Agent w jednym z dwóch punktów instalacji:

- W przypadku instalacji serwera Security Server na komputerze z zainstalowanym serwerem Microsoft Exchange, program instalacyjny wyświetla monit o wykonanie instalacji **lokalny** programu Messaging Security Agent.

- W przypadku instalacji serwera Security Server na komputerze, który nie wykrywa serwerów Microsoft Exchange, program instalacyjny monituje o zainstalowanie **zdalny** wersji programu Messaging Security Agent na serwerach zdalnych.

Zainstaluj program Messaging Security Agent



Należy podać następujące informacje:

- **Serwer Exchange**

> **Uwaga**
>
> Program instalacyjny automatycznie wykryje nazwę lokalnego serwera Exchange i wypełni pole Serwer Exchange, jeśli serwer Exchange znajduje się na tym samym komputerze, na którym zainstalowany jest program Security Server. Jeśli zainstalowano serwer Exchange na tym samym komputerze, ale jego nazwa nie została wypełniona automatycznie, sprawdź, czy środowisko spełnia minimalne wymagania programu Messaging Security Agent.

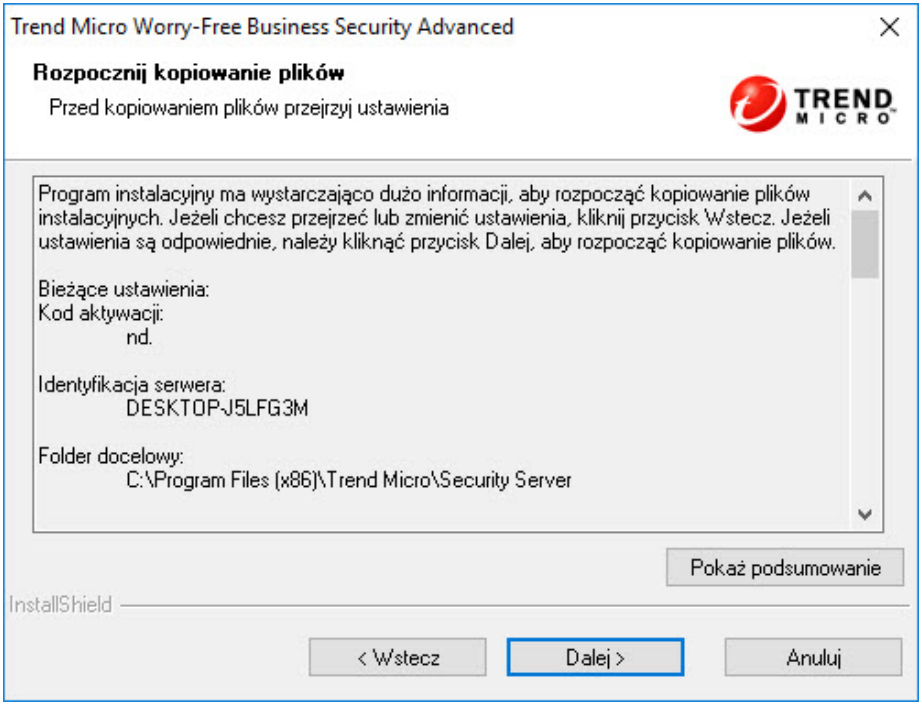
- **Konto administratora domeny**
- **Hasło**

Uwaga

Program instalacyjny może nie przesłać hasła zawierającego znaki specjalne (niealfanumeryczne) do komputera z zainstalowanym serwerem Exchange. Uniemożliwi to instalację programu Messaging Security Agent. Aby rozwiązać ten problem, należy tymczasowo zmienić hasło wbudowanego konta administratora domeny lub zainstalować program Messaging Security Agent bezpośrednio na serwerze Exchange.

Etap 3: Proces instalacji

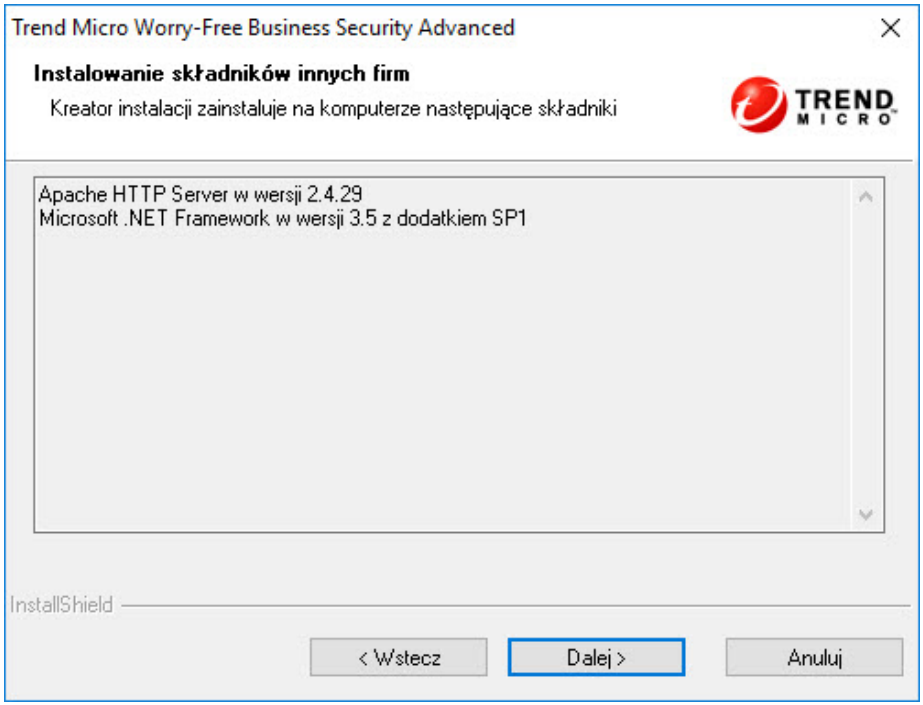
Rozpocznij kopiowanie plików



Na ekranie Rozpocznij kopiowanie plików jest wyświetlane podsumowanie wszystkich parametrów, które będą używane podczas instalacji programu Worry-Free Business Security.

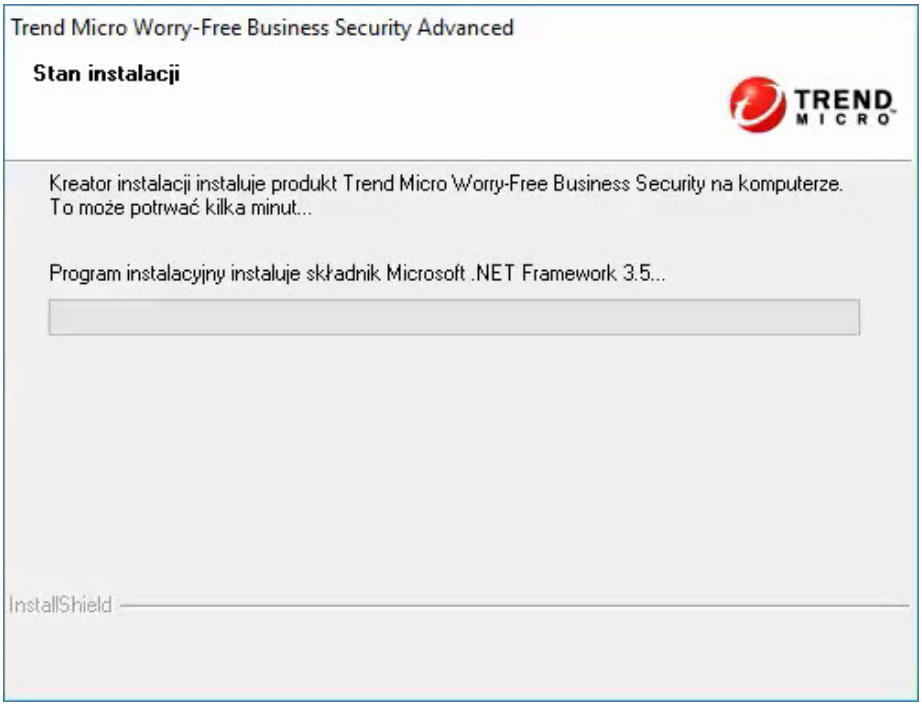
Kliknij przycisk **Wstecz**, jeśli chcesz sprawdzić ustawienia poprzedniej instalacji lub kliknij przycisk **Dalej** , aby kontynuować obecną instalację.

Zainstaluj składniki innych firm



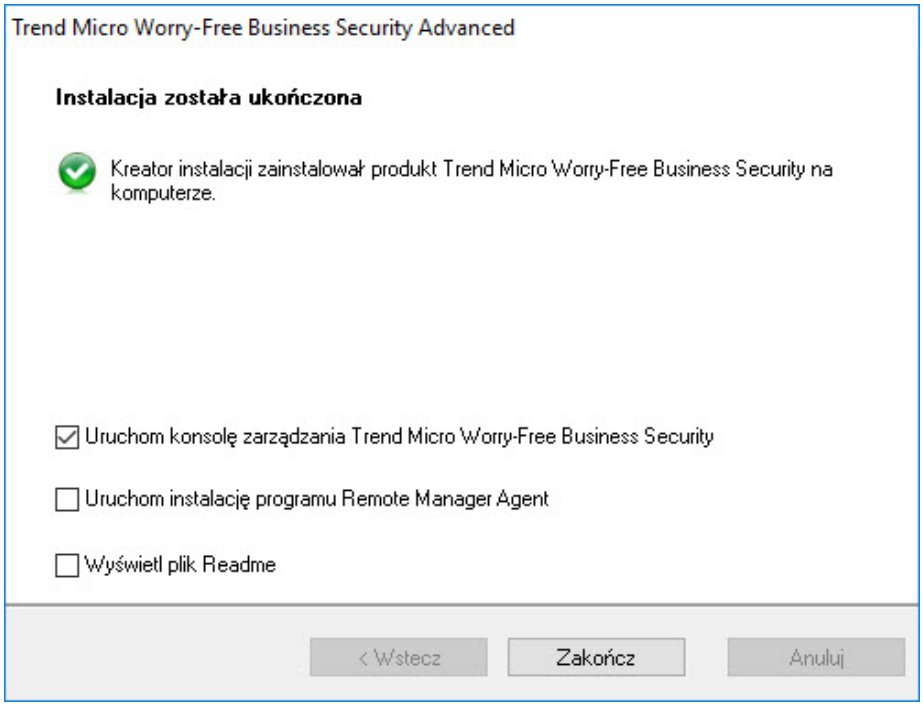
Na tym ekranie wyświetlone są informacje o tym, jakie składniki innych firm zostaną zainstalowane. Kliknij przycisk **Dalej**, aby rozpocząć instalowanie wybranych składników.

Stan instalacji



Instalacja może chwilę potrwać. Podczas instalacji na ekranie stanu będzie wyświetlany postęp instalacji.

Instalacja została ukończona



Można również zaznaczyć pola wyboru w celu wykonania następujących czynności:

- Otwarcia sieciowej konsoli zarządzania (wybranej domyślnie)
- Zainstalowania programu Remote Manager Agent (procedurę przedstawiono w *Podręczniku administratora*)
- Wyświetlenia pliku Readme

Kliknij przycisk **Zakończ**, aby zakończyć instalację.

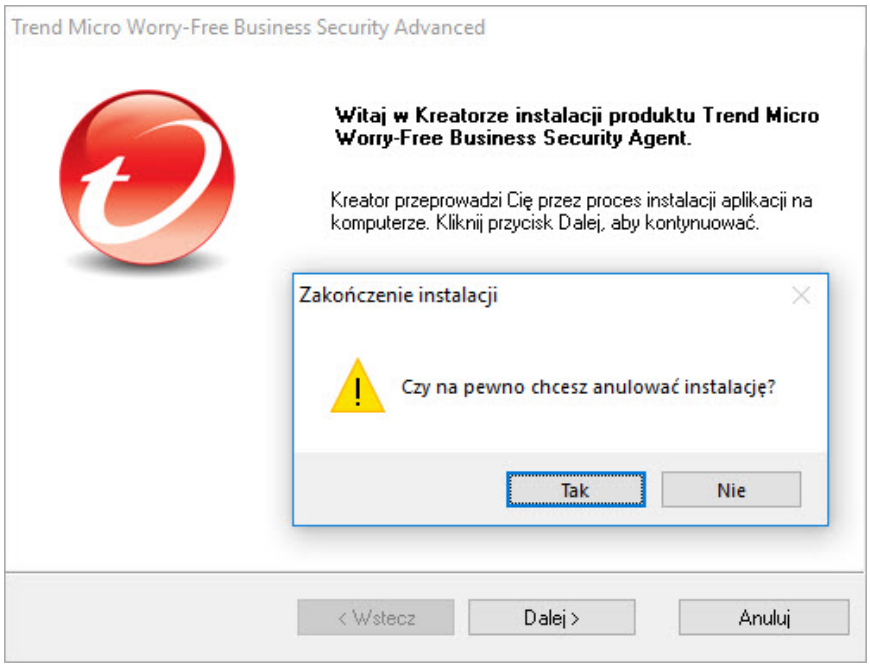
Instalowanie kilku serwerów Security Server w trybie cichej instalacji

Cicha instalacja pozwala przeprowadzić wiele identycznych instalacji w różnych sieciach. Można zarejestrować ustawienia instalacyjne w sesji Kreatora instalacji, a następnie wykorzystać te ustawienia do generowania automatycznych instalacji.

Rejestrowanie sesji instalacji

Procedura

1. Pobierz i wyodrębnij pliki programu WFBS na dysk twardy. Gdy Kreator instalacji rozpocznie zbieranie ustawień instalacyjnych, kliknij kolejno opcje **Anuluj** > **Tak** > **Zakończ**.



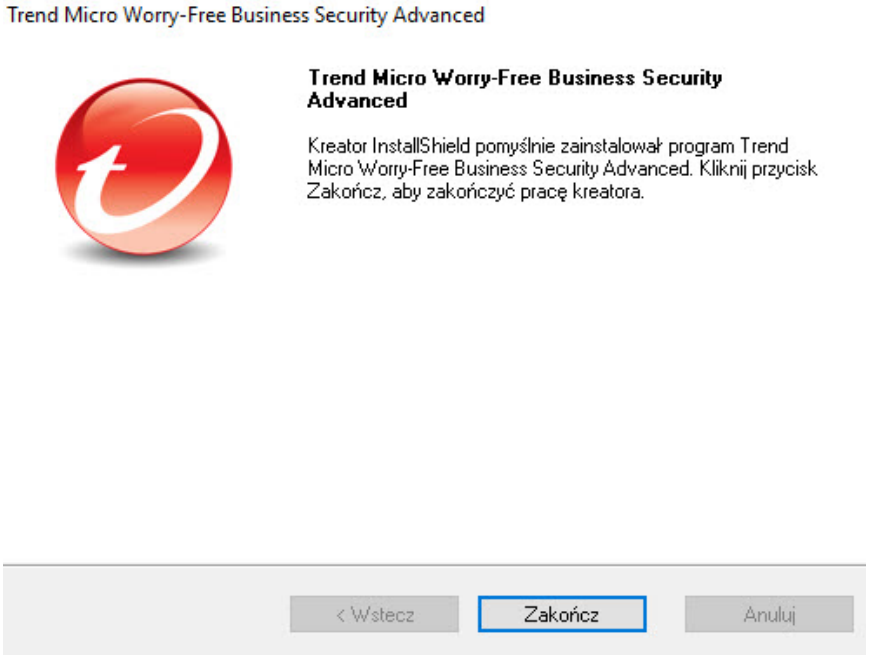
2. W wierszu polecenia przejdź do katalogu, w którym znajdują się wyodrębnione pliki instalacyjne programu WFBS, na przykład: `C:\Extract\WFBS\CSM`

3. Po wyświetleniu odpowiedniego monitu wpisz polecenie `Setup.exe /r /f1"c:\silent-install.iss"` i naciśnij klawisz **Enter**.

   Kreator instalacji zostanie uruchomiony ponownie. Czynności wykonywane przez użytkownika zostaną zapisane w pliku silent-install.iss na dysku C.

4. Postępuj zgodnie z instrukcjami na ekranie. Instrukcje są takie same, jak opisane w sekcji *Instalowanie programu Security Server na stronie 2-13*.

5. Po zakończeniu sesji nagrywania pojawia się następujący ekran potwierdzający. Kliknij przycisk **Zakończ**, aby zakończyć sesję nagrywania i ponownie wyświetlić wiersz polecenia.



Rozpoczęcie cichej instalacji

Procedura

1. W wierszu polecenia przejdź do katalogu, w którym znajdują się wyodrębnione pliki instalacyjne programu WFBS, na przykład: `C:\Extract\WFBS\CSM`
2. Po wyświetleniu odpowiedniego monitu wpisz polecenie `Setup.exe /s /f1"c:\silent-install.iss"` i naciśnij klawisz **Enter**.

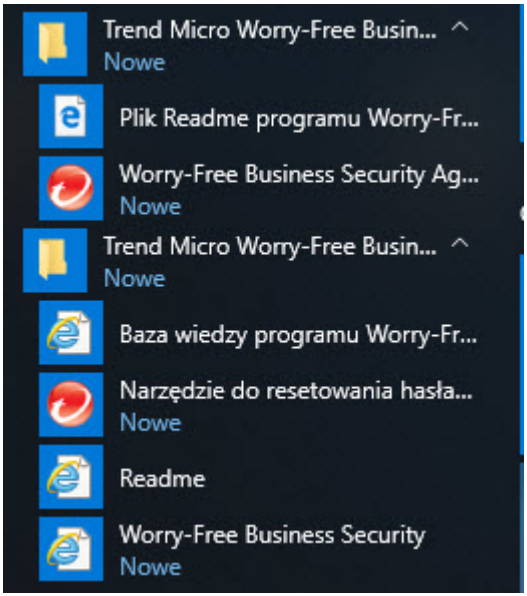
   Czas trwania cichej instalacji programu WFBS, rozpoczynanej automatycznie, jest taki sam, jak w przypadku normalnej instalacji.

   Podczas cichej instalacji na ekranie nie jest wyświetlany postęp instalacji.
3. Aby sprawdzić, czy instalacja zakończyła się powodzeniem, otwórz plik `c:\setup.log`. Jeśli wyświetlony zostanie komunikat `ResultCode=0`, instalacja zakończyła się pomyślnie.
4. Powtórz kroki 1–3 na wszystkich pozostałych komputerach w sieci.

Weryfikacja instalacji

Procedura

- Kliknij **Start** > **Wszystkie programy**, aby sprawdzić, czy programy Security Server i Security Agent pojawiają się na liście.



- Kliknij **Start** > **Panel sterowania** > **Programy** > **Odinstaluj program**, aby sprawdzić, czy programy WFBS i Security Agent pojawiają się na liście.
- Zaloguj się do Konsoli zarządzania przy użyciu adresu URL serwera: `https://{nazwa_serwera}:{numer portu}/SMB`

Uwaga

Jeśli nie jest używany protokół SSL, wpisz ciąg `http` zamiast `https`.

Rozdział 3

Uaktualnianie programu Security Server i agentów

Ten rozdział zawiera informacje niezbędne do zrozumienia procesu uaktualniania programu Security Server i agentów.

Wymagania dotyczące instalacji i uaktualniania

Pełna lista wymagań dotyczących instalacji i uaktualniania jest dostępna pod adresem:

http://docs.trendmicro.com/pl-pl/smb/worry-free-business-security.aspx

Uwagi dotyczące uaktualnienia

Przed uaktualnieniem programu Security Server i agentów należy rozważyć następujące kwestie.

- *Wymagania protokołu IPv6 związane z aktualizacjami na stronie 3-2*
- *Najważniejsze wskazówki dotyczące uaktualniania na stronie 3-3*

Wymagania protokołu IPv6 związane z aktualizacjami

Poniżej przedstawiono wymagania protokołu IPv6 dotyczące serwera Security Server:

- Aktualizowany serwer Security Server musi być zainstalowany w systemie Windows 7, 8.1, 10, Server 2008, 2012, 2012 R2, 2016 i SBS 2008/2011. Serwerów Security Server nie można zainstalować w systemach Windows XP, Server 2003 ani SBS 2003, ponieważ te systemy operacyjne zapewniają tylko częściową obsługę adresowania IPv6.
- Przypisz do serwera Security Server adres IPv6. Ponadto serwer musi zostać zidentyfikowany nazwą hosta; zalecane jest wprowadzenie pełnej nazwy (FQDN, Fully Qualified Domain Name). Jeśli serwer jest identyfikowany przy użyciu adresu IPv6, wszystkie klienty zarządzane obecnie przez ten serwer utracą z nim połączenie. Jeśli serwer jest identyfikowany przy użyciu adresu IPv4, nie będzie możliwe zainstalowanie agenta na komputerach wykorzystujących wyłącznie protokół IPv6.
- Upewnij się, że adres IPv6 lub IPv4 hosta można uzyskać na przykład przy użyciu polecenia ping lub nslookup.

Najważniejsze wskazówki dotyczące uaktualniania

Podczas uaktualniania programu WFBS do najnowszej wersji można zachować ustawienia klienta. Aby zapewnić łatwe przywracanie istniejących ustawień w przypadku problemów z uaktualnieniem, firma Trend Micro zaleca następujące działania:

- Utworzenie kopii zapasowej bazy danych programu Security Server
- Usunięcie wszystkich plików dzienników z serwera Security Server

Tworzenie kopii zapasowej bazy danych programu Security Server

Procedura

1. Zatrzymaj usługę Trend Micro Security Server Master Service.
2. W programie Eksplorator Windows przejdź do folderu programu Security Server i skopiuj zawartość `\PCCSRV\HTTPDB` do innej lokalizacji (na przykład do innego katalogu na tym samym serwerze, na inny komputer lub na dysk wymienny).

Usuwanie plików dzienników z serwera Security Server

Procedura

1. Przejdź do pozycji **Raporty** > **Obsługa** > **Ręczne usuwanie dzienników**.
2. Dla typów dzienników, które chcesz usunąć, zmień wartość ustawienia **Usuń dzienniki starsze niż** na 0.
3. Aby usunąć dzienniki, wybierz jedną z poniższych metod:
   - Kliknij polecenie **Usuń** dla każdego typu dziennika.
   - Kliknij polecenie **Usuń wszystko**, aby usunąć wszystkie dzienniki.

Wcześniejsze uaktualnienia wersji

W tej wersji produktu obsługiwane są uaktualnienia z dowolnej z następujących wersji programu Worry-Free Business Security lub Worry-Free Business Security-Advanced:

- 9.x (z wszystkimi dodatkami Service Pack)
- 8.x (8.0 i 8.0 SP1)

W tej wersji produktu nie są obsługiwane uaktualnienia z żadnej z następujących wersji:

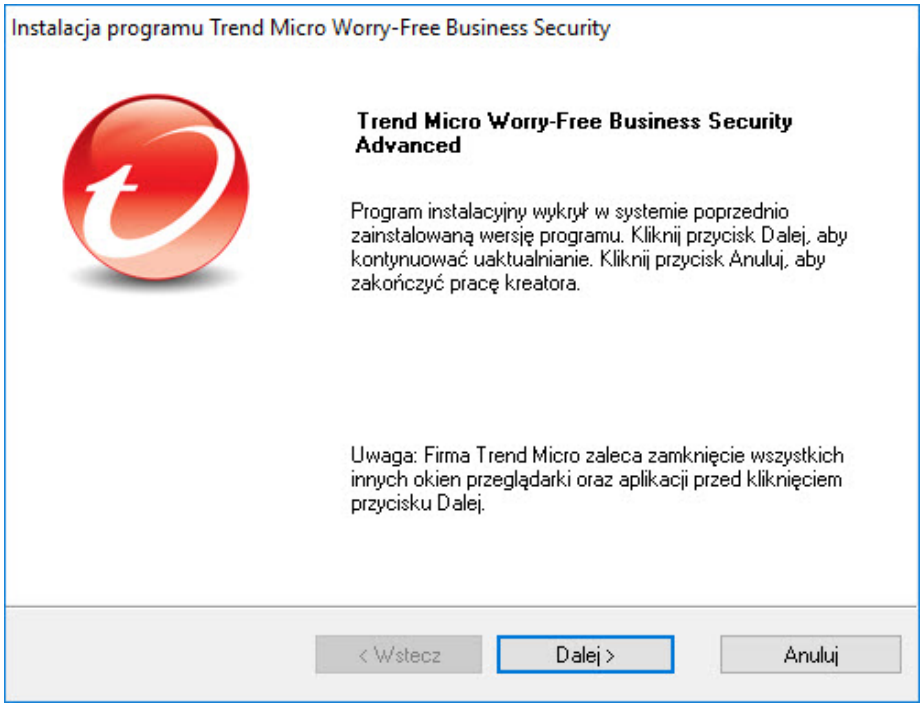
- Worry-Free Business Security lub Worry-Free Business Security-Advanced 7.x
- Worry-Free Business Security lub Worry-Free Business Security-Advanced 6.x
- Worry-Free Business Security lub Worry-Free Business Security-Advanced 5.x
- Wszystkie uaktualnienia obsługujące system Windows 2000
- Client/Server Messaging Security 3.6 (z wyjątkiem wersji japońskiej)
- Client Server Messaging Security 3.5
- Client Server Messaging Security 3.0
- Client/Server Security 3.0
- Client/Server Suite 2.0
- Client/Server/Messaging Suite 2.0
- OfficeScan lub ScanMail for Microsoft Exchange
- Zmiana z jednego języka na inny

Zależnie od przepustowości sieci i liczby agentów, którą zarządza serwer Security Server, można przeprowadzić aktualizację kolejnych grup agentów lub zaktualizować wszystkie agenty jednocześnie po aktualizacji serwera.

1. metoda aktualizacji: aktualizacja za pomocą pakietu instalacyjnego

Pobierz pakiet instalacyjny dla danej wersji produktu i uruchom plik `Setup.exe` na komputerze z programem Security Server. Gdy program instalacyjny wykryje, że na

komputerze istnieje już program Security Server, wyświetlony zostanie monit o jego uaktualnienie pokazany na poniższej ilustracji.



Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby przeprowadzić aktualizację programu Security Server.

Po zakończeniu uaktualniania:

- Programy Security Agent w trybie online są aktualizowane natychmiast.
- Aktualizacja programów Security Agent w trybie offline rozpocznie się w momencie ich przejścia w tryb online.

  Należy poinstruować użytkowników, by połączyli się z siecią, aby oprogramowanie Security Agent mogło przejść w tryb online. Jeśli programy Security Agent pozostają w trybie offline przez dłuższy czas, należy poinstruować użytkowników,

aby odinstalowali to oprogramowanie z klienta, a następnie w celu zainstalowania agenta skorzystali z odpowiedniej metody instalacji agenta (np. programu Client Packager) opisanej w *Przewodniku administratora*.

Uwaga

Wszystkie wcześniejsze ustawienia agentów (poza uprawnieniami agenta aktualizacji) zostaną zachowane po uaktualnieniu do tej wersji. Oznacza to, że po uaktualnieniu agenty aktualizacji zostaną ponownie przekształcone w programy Security Agent. Należy ponownie przydzielić je jako agenty aktualizacji w konsoli zarządzania.

Więcej informacji można znaleźć pod adresem http://esupport.trendmicro.com/solution/en-US/1057531.aspx.

2. metoda aktualizacji: przeniesienie agentów na serwer Security Server 10.0

Przeprowadź nową instalację serwera Security Server, a następnie przenieś programy Security Agent na ten serwer. Po przeniesieniu agenty zostaną automatycznie uaktualnione do wersji 10.0.

Część 1: przeprowadzenie nowej instalacji serwera Security Server 10.0

Procedura

1. Przeprowadź nową instalację serwera Security Server na komputerze. Aby uzyskać więcej informacji, zobacz *Instalowanie programu Security Server na stronie 2-13*.
2. Zapisz następujące informacje dotyczące serwera Security Server 10.0. Podaj te informacje na obsługiwanym serwerze Security Server podczas przenoszenia agentów.
   - nazwa hosta lub adres IP,
   - Port nasłuchiwania serwera

Nazwę hosta i port nasłuchiwania można znaleźć na ekranie Ustawienia zabezpieczeń serwera Security Server, nad panelem Zadania.

Część 2: aktualizacja agentów

Procedura

1. W konsoli internetowej obsługiwanego serwera Security Server przejdź do obszaru **Ustawienia zabezpieczeń**.
2. Aby przenieść programy Security Agent, zaznacz grupę, a następnie zaznacz agenty.

   Porada

   Aby wybrać wiele sąsiadujących programów Security Agent, kliknij pierwszego agenta w zakresie, przytrzymaj klawisz SHIFT i kliknij ostatniego agenta w zakresie. Aby wybrać nieciągły zakres agentów, kliknij pierwszego agenta w zakresie, przytrzymaj klawisz CTRL, a następnie klikaj agenty, które chcesz zaznaczyć.

3. Kliknij polecenie **Zarządzaj drzewem klientów** > **Przenoszenie klienta**.

   Zostanie wyświetlony nowy ekran.

4. Wpisz nazwę hosta i port nasłuchiwania serwera Security Server 10.0, na który agenty zostaną przeniesione.
5. Kliknij opcję **Przenieś**.

Wyniki aktualizacji

- Rozpoczyna się przenoszenie i aktualizacja agentów online. Po uaktualnieniu w zależności od systemu operacyjnego punktu końcowego programy Security Agent zostaną przydzielone na serwerze Security Server 10.0 do grupy **Komputery (domyślne)** lub **Serwery (domyślne)**. Agent dziedziczy ustawienia swojej nowej grupy.
- Aktualizacja agentów offline rozpocznie się w momencie ich przejścia w tryb online. Należy poinstruować użytkowników, by połączyli się z siecią, aby agenty

mogły przejść w tryb online. Jeśli programy Security Agent pozostają w trybie offline przez dłuższy czas, należy poinstruować użytkowników, aby odinstalowali to oprogramowanie z klienta, a następnie w celu zainstalowania agenta skorzystali z odpowiedniej metody instalacji agenta (np. programu Client Packager) opisanej w *Przewodniku administratora*.

Aktualizacja do wersji pełnej lub wersji Advanced

Skorzystaj z ekranu Licencja produktu w konsoli internetowej, aby:

- Zaktualizować produkt z wersji próbnej do wersji pełnej
- Zaktualizować produkt z wersji Standard do wersji Advanced

Wersja próbna i pełna

Na krótko przed wygaśnięciem ważności wersji próbnej na ekranie Stan aktywności konsoli internetowej zostanie wyświetlony komunikat powiadomienia. Wersję próbną można uaktualnić do wersji o pełnej licencji za pomocą konsoli internetowej. Ustawienia konfiguracji zostaną zapisane. Przy zakupie pełnej licencji klient otrzyma klucz rejestracyjny lub kod aktywacyjny.

Wersje Standard i Advanced

Firma Trend Micro udostępnia dwa podobne produkty umożliwiające ochronę komputerów i sieci: Program Worry-Free Business Security Standard i Worry-Free Business Security Advanced.

TABELA 3-1. Wersje produktów

WERSJA PRODUKTU	WORRY-FREE BUSINESS SECURITY STANDARD	WORRY-FREE BUSINESS SECURITY ADVANCED
Rozwiązanie po stronie klienta	Tak	Tak
Rozwiązanie po stronie serwera	Tak	Tak

Wersja produktu	Worry-Free Business Security Standard	Worry-Free Business Security Advanced
Rozwiązanie Microsoft Exchange Server	Nie	Tak

Program można zaktualizować z wersji Worry-Free Business Security Standard do wersji Worry-Free Business Security Advanced po uzyskaniu od firmy Trend Micro kodu aktywacyjnego.

Uaktualnianie do wersji pełnej lub wersji Advanced

Procedura

1. W konsoli internetowej przejdź do pozycji **Administracja** > **Licencja produktu**.
2. Jeśli masz kod aktywacyjny, wybierz opcję **Wprowadź nowy kod**, wpisz go w polu **Nowy kod aktywacyjny** i kliknij przycisk **Aktywuj**.

   Jeśli nie masz kodu aktywacyjnego, przejdź do witryny Trend Micro pod adres http://olr.trendmicro.com, aby zarejestrować się online i uzyskać kod aktywacyjny.

Dodatek A

Pomoc techniczna

W tym rozdziale omówiono następujące zagadnienia:

Zasoby dotyczące rozwiązywania problemów

Przed skontaktowaniem się z działem pomocy technicznej warto rozważyć skorzystanie z następujących zasobów online firmy Trend Micro.

Korzystanie z portalu pomocy technicznej

Portal pomocy technicznej firmy Trend Micro Support jest stale czynnym zasobem sieciowym zawierającym najbardziej aktualne informacje dotyczące typowych i nietypowych problemów.

Procedura

1. Przejdź do witryny http://esupport.trendmicro.com.
2. Wybierz jeden z dostępnych produktów lub kliknij odpowiedni przycisk, aby poszukać rozwiązań.
3. Użyj pola **Przeszukaj pomoc techniczną**, aby znaleźć dostępne rozwiązania.
4. Jeśli rozwiązanie nie zostanie znalezione, kliknij przycisk **Kontakt z pomocą techniczną** i wybierz rodzaj potrzebnej pomocy.

Porada

Aby przesłać zgłoszenie przez Internet, odwiedź stronę o następującym adresie URL:

http://esupport.trendmicro.com/srf/SRFMain.aspx

Pracownik działu pomocy technicznej firmy Trend Micro Support zbada zgłoszenie i udzieli odpowiedzi w ciągu 24 godzin lub szybciej.

Encyklopedia zagrożeń

Większość dzisiejszego złośliwego oprogramowania to zagrożenia hybrydowe, które łączą co najmniej dwie technologie w celu ominięcia protokołów bezpieczeństwa

komputera. Firma Trend Micro zwalcza takie złożone złośliwe oprogramowanie przy użyciu produktów, które tworzą niestandardową strategię ochrony. Encyklopedia zagrożeń zapewnia wszechstronną listą nazw i objawów różnych zagrożeń hybrydowych, włącznie ze znanym złośliwym oprogramowaniem, spamem, złośliwymi adresami URL i znanymi lukami w zabezpieczeniach.

Odwiedź stronę http://about-threats.trendmicro.com/us/threatencyclopedia#malware, aby uzyskać następujące informacje:

- złośliwe oprogramowanie i mobilne kody złośliwe, które są obecnie na wolności lub aktywne;
- strony z informacjami o powiązanych zagrożeniach, które przedstawiają kompleksowo atak internetowy;
- poradniki poświęcone zagrożeniom internetowym, które przedstawiają ukierunkowane ataki i zagrożenia bezpieczeństwa;
- informacje o atakach internetowych i trendach online;
- cotygodniowe raporty o złośliwym oprogramowaniu.

Kontakt z firmą Trend Micro

Z przedstawicielami firmy Trend Micro można skontaktować się telefonicznie lub pocztą e-mail:

Adres	Trend Micro (EMEA) Limited - Central Eastern Europe, Office in Warsaw Warsaw Trade Tower Floor 30, Chłodna 51 00-867 Warszawa
Telefon	+48 (22)486 34 50
Witryna internetowa	http://www.trendmicro.pl

Adres e-mail	biuro@trendmicro.com

- Lista biur pomocy technicznej na całym świecie:

  http://www.trendmicro.com/us/about-us/contact/index.html

- Kontakt z firmą Trend Micro:

  http://www.trendmicro.pl/about/contact/index.html

- Dokumentacja produktu firmy Trend Micro:

  http://docs.trendmicro.com/pl-pl/home.aspx

Przyspieszanie przyjęcia zgłoszenia serwisowego

Aby usprawnić procedurę rozwiązywania problemów, należy przygotować następujące informacje:

- procedura odtworzenia problemu.
- informacje o urządzeniu lub sieci;
- Marka i model komputera oraz wszystkie dodatkowe podłączone urządzenia lub sprzęt
- ilość pamięci RAM i wolnego miejsca na dysku twardym;
- wersje systemu operacyjnego i dodatku Service Pack;
- Wersja zainstalowanego agenta
- Numer seryjny lub kod aktywacji
- szczegółowy opis środowiska instalacji;
- dokładny tekst komunikatu o błędzie.

Przesyłanie podejrzanej zawartości do firmy Trend Micro

Dostępnych jest wiele opcji przesyłania podejrzanej zawartości do firmy Trend Micro w celu przeprowadzenia dalszej analizy.

Email Reputation Services

Istnieje możliwość sprawdzenia reputacji określonego adresu IP i określenia agenta przesyłania wiadomości w celu dołączenia do globalnej listy dozwolonych:

https://ers.trendmicro.com/

Zapoznaj się z następującym wpisem Bazy wiedzy, aby wysłać próbki wiadomości do firmy Trend Micro:

http://esupport.trendmicro.com/solution/en-US/1112106.aspx

Usługi File Reputation Services

Zgromadź informacje systemowe i prześlij zawartość podejrzanego pliku do firmy Trend Micro:

http://esupport.trendmicro.com/solution/en-us/1059565.aspx

Zanotuj numer zgłoszenia, aby można było je śledzić.

Usługi Web Reputation Services

Istnieje możliwość zapytania o ocenę bezpieczeństwa i typ zawartości adresu URL, odnośnie którego istnieje podejrzenie, że jest to witryna phishingowa lub inny tzw. „wektor infekcji" (celowo utworzone źródło zagrożeń internetowych, takich jak spyware i wirusy):

http://global.sitesafety.trendmicro.com/

Jeśli przypisana ocena jest nieprawidłowa, można wysłać prośbę o ponowne sklasyfikowanie do firmy Trend Micro.

Inne zasoby

W witrynie internetowej oprócz rozwiązań i pomocy technicznej dostępnych jest wiele innych pomocnych zasobów, które pozwalają uzyskać aktualne informacje oraz poznawać innowacje i najnowsze trendy dotyczące bezpieczeństwa.

Centrum pobierania

Od czasu do czasu firma Trend Micro może udostępnić poprawkę dla znanego problemu, który został zgłoszony, lub uaktualnienie określonego produktu albo usługi. Aby sprawdzić dostępność poprawek, odwiedź witrynę:

http://www.trendmicro.com/download/emea/?lng=emea

Jeśli poprawka nie została zastosowana (poprawki są oznaczone datą), otwórz plik Readme w celu sprawdzenia, czy poprawka ma zastosowanie do danego środowiska. Plik Readme zawiera także instrukcje instalacji.

Opinie o dokumentacji

Firma Trend Micro stara się zawsze ulepszać swoją dokumentację. W przypadku pytań, komentarzy lub sugestii dotyczących tego albo innego dokumentu firmy Trend Micro należy odwiedzić witrynę:

http://www.trendmicro.com/download/documentation/rating.asp

Indeks

TREND MICRO INCORPORATED

Trend Micro (EMEA) Limited - Central Eastern Europe, Office in Warsaw Warsaw
Trade Tower Floor 30, Chłodna 5100-867 Warszawa
Telefon: +48 (22)486 34 50 Faks: +48 (22) 486 34 49 info@trendmicro.com

www.trendmicro.com

Item Code: WFPM108205/180326