Bitdefender

GravityZone

PODRĘCZNIK INSTALACJI

Bitdefender GravityZone
Podręcznik instalacji

Data publikacji 2017.01.25

Uwagi prawne

Bitdefender

Spis treści

Wstęp

Podręcznik ten jest przeznaczony dla administratorów sieci, którzy poszukują pomocy we wdrażaniu GravityZone w formie konsoli on-premise, a także dla managerów IT poszukujących informacji na temat wymagań i dostępnej ochrony modułowej GravityZone.

Niniejszy dokument ma na celu wyjaśnienie, jak zainstalować i skonfigurować rozwiązanie GravityZone i jego agentów bezpieczeństwa na wszystkich typach punktów końcowych w firmie.

1. Znaki umowne stosowane w przewodniku

Konwencje Typograficzne

Podręcznik ten wykorzystuje kilka stylów formatowania tekstu dla polepszonej czytelności. Dowiesz się o ich postaci i znaczeniu z poniższej tabeli.

Wygląd	Opis
`wzorzec`	Zgodne nazwy poleceń i składnia ścieżki, nazwy plików, konfiguracja punktu wejścia i wyjścia dla wyświetlanego tekstu są drukowane przy `stałej szerokości` znaków.
http://www.bitdefender.com	Nawiązania (linki) URL odnoszą do innych miejsc takich jak serwery http czy ftp.
documentation@bitdefender.com	Adresy Email zostały umieszczone w tekście dla informacji kontaktowych.
„Wstęp” (p. v)	To odnośnik do linka wewnętrznego umiejscowionego w dokumencie.
opcja	Wszystkie opcje produktu są napisane z użyciem **pogrubionych** znaków.
słowo kluczowe	Ważne słowa kluczowe lub frazy są wyróżniane poprzez użycie **pogrubionych** znaków.

Uwagi

Uwagi, są to notatki graficznie wyróżnione, zwracające Państwa uwagę na dodatkowe informacje odnoszące się do aktualnego paragrafu.

Notatka
Wskazówka jest krótką poradą. Chociaż można by ją ominąć, jednak wskazówki zawierają użyteczne informacje, takie jak specyficzne działanie lub powiązania z podobnym tematem.

WAŻNE
Ten znak wymaga Państwa uwagi i jego pomijanie nie jest zalecane. Zazwyczaj nie są to wiadomości krytyczne, ale znaczące.

Ostrzeżenie
To jest krytyczna informacja, którą należy traktować ze zwiększoną ostrożnością. Nic złego się nie stanie jeśli podążasz za tymi wskazówkami. Powinieneś to przeczytać i zrozumieć, ponieważ opisuje coś ekstremalnie ryzykowanego.

1. O GRAVITYZONE

GravityZone jest biznesowym rozwiązaniem bezpieczeństwa zaprojektowanym od podstaw z myślą o wirtualizacji i chmurze by dostarczać usługę ochrony dla fizycznych punktów końcowych i maszyn wirtualnych opartych na prywatnej, publicznej chmurze oraz serwerów pocztowych Exchange.

GravityZone to pojedynczy produkt który posiada ujednoliconą konsolę administracyjną dostępną w chmurze, zarządzaną przez Bitdefender lub jako urządzenie wirtualne zainstalowane w siedzibie umożliwiające nam z tego punktu egzekwowanie i zarządzanie polityką bezpieczeństwa dla dowolnej ilości punktów końcowych, ich rodzaju oraz lokalizacji.

GravityZone dostarcza wielowarstwową ochronę dla punktów końcowych, łącznie z serwerami poczty Microsoft Exchange: antymalware wraz z monitorowaniem zachowań, ochronę przed zagrożeniami dnia zero, kontrolę aplikacji, sandboxa, zaporę sieciowej, kontrolę urządzeń, kontrolę treści, antyphishing i antyspam.

1.1. Usługi bezpieczeństwa GravityZone

GravityZone oferuje następujące usługi ochrony:

- Security for Endpoints
- Security for Virtualized Environments
- Security for Exchange
- Security for Amazon Web Services

Security for Amazon Web Services

Chociaż chmura obliczeniowa jest szeroko uznawaną technologią bezpieczeństwa, firmy nadal potrzebują maksymalnej ochrony przed wycelowanymi atakami malware. Aby w pełni wykorzystać potencjał chmury obliczeniowej bez utraty bezpieczeństwa, rozwiązania antymalware powinny mieć minimalny wpływ na wydajność systemu.

Security for Amazon Web Services adresuje wszystkie te wyzwania z wysoko-skalowalną, innowacyjną technologią. Rozwiązanie Bitdefender zostało zaprojektowane specjalnie dla środowisk wirtualnych i spełnia wymagania najbardziej dynamicznych infrastruktur cloud. Zintegrowana z Amazon Web Services (AWS) dla dostępność w chmurze Bitdefender. Security for Amazon Web Services

chroni zwirtualizowany system Windows i Linux pozostawiając mały odcisk i generując natychmiastowe oszczędności dla użytkowników Amazon.

Security for Endpoints

Chroni dyskretnie dowolną liczbę laptopów, komputerów stacjonarnych i serwerów Windows, Linux i Mac OS X, za pomocą nagradzanej technologii Antymalware. Dodatkowo, systemy Windows korzystają z jeszcze większego bezpieczeństwa dzięki dwukierunkowej zaporze sieciowej, wykrywaniu włamań, kontroli dostępu, filtrowaniu stron internetowych, ochronie wrażliwych danych, kontroli aplikacji i urządzeń. Niskie wykorzystanie systemu zapewnia wzrost wydajności. Rozwiązanie stanowi alternatywę dla klasycznych systemów antimalware łącząc w sobie uznane branżowo technologie zabezpieczeń z prostotą wdrożenia i potężnym narzędziem do zarządzania GravityZone Control Center. Proaktywna heurystyka zobowiązana jest do klasyfikacji złośliwych procesów w oparciu o ich zachowanie, wykrywając zagrożenia w czasie rzeczywistym.

Security for Virtualized Environments

Security for Virtualized Environments jest pierwszym uniwersalnym rozwiązaniem bezpieczeństwa dla zwirtualizowanych centrów danych, ochraniając wirtualne serwery i komputery stacjonarne w systemach Windows i Linux. Wspierane nowatorską technologią buforowania, rozwiązanie przynosi korzyści w stosunku do wydajności i zwiększa konsolidację serwerów nawet o 30% w porównaniu do tradycyjnych rozwiązań antymalware.

Security for Exchange

Bitdefender Security for Exchange zapewnia antymalware, antyspam, antyphishing, filtrowanie załączników i treści płynnie zintegrowane z Microsoft Exchange Server, aby zapewnić bezpieczne środowisko komunikacji i współpracy oraz zwiększenie wydajności. Korzystając z wielokrotnie nagradzanych technologii antymalware i antyspamowych, chroni użytkowników Exchange przed najnowszym, najbardziej zaawansowanym złośliwym oprogramowaniem i przed próbami kradzieży cennych i poufnych danych użytkowników.

1.2. Architektura GravityZone

Rozwiązanie GravityZone zawiera następujące składniki:

- Konsola Webowa (Control Center)

- Security Server
- Agenci Bezpieczeństwa

1.2.1. Konsola Webowa (Control Center)

Rozwiązania ochrony Bitdefender zarządzane za pomocą GravityZone z pojedynczego punktu zarządzania, Control Center konsoli webowej, która zapewnia łatwiejsze zarządzanie i dostępu całościowego stanu zabezpieczenia, globalnych zagrożeń ochrony oraz kontrolę nad wszystkimi modułami bezpieczeństwa chroniącymi wirtualne i fizyczne stacje robocze, serwery i instancje Amazon. Zasilana przez Architekturę Gravity, Control Center jest w stanie odpowiedź na potrzeby nawet największych organizacji.

Control Center interfejs oparty na przeglądarce integruje się z istniejącym systemem zarządzania i monitoringu systemu co upraszcza nam automatyczne zastosowanie ochrony na niezarządzanych stacjach i serwerach.

1.2.2. Security Server

Security Server jest dedykowaną maszyną wirtualną, która deduplikuje i centralizuje większość funkcjonalności antymalware dla agentów, działających jako serwer.

Notatka
Twoja licencja produktu może nie zawierać tej funkcji.

Security Server musi być zainstalowany na jednym lub kilku hostach tak, aby pomieścić wiele chronionych maszyn wirtualnych.

Dla instancji Amazon EC2, nie musisz instalować Security Server. W tym wypadku, maszyna Security Server jest hostowana przez Bitdefender, a instancja EC2 będzie automatycznie łączyła się do Bitdefender Security Server hostowanego w odpowiednim regionie AWS.

1.2.3. Agenci Bezpieczeństwa

Aby chronić Twoją sieć z Bitdefender, musisz zainstalować właściwych agentów bezpieczeństwa GravityZone na punktach końcowych sieci.

- Bitdefender Endpoint Security Tools
- Endpoint Security for Mac

Bitdefender Endpoint Security Tools

GravityZone zapewnia dzięki Bitdefender Endpoint Security Tools ochronę fizycznych oraz maszyn wirtualnych. Jest to inteligentne środowisko eksploatacji świadomości użyte jako środek zdolny do automatycznej samo-konfiguracji w zależności od rodzaju punktu końcowego. Bitdefender Endpoint Security Tools może zostać rozmieszczony na dowolnych urządzeniach, fizycznych oraz wirtualnych dostarczając elastyczny system skanowania będący idealnym rozwiązaniem dla mieszanych środowisk (fizycznych, wirtualnych i w chmurze).

Dodatkowo, system ochrony plików, Bitdefender Endpoint Security Tools obejmuje również ochronę serwera poczty dla serwerów Microsoft Exchange.

Bitdefender Endpoint Security Tools wykorzystuje pojedynczy szablon zasad dla maszyn fizycznych i wirtualnych i jedno źródło zestawu instalacyjnego dla wszelkich środowisk (fizycznych czy wirtualnych). Bitdefender Endpoint Security Tools jest dostępny również dla końcówek fizycznych Linux (serwery i stacje robocze).

Silniki Skanowania

Silniki skanowania są ustawione automatycznie podczas tworzenia paczek Bitdefender Endpoint Security Tools, pozwalając agentowi punktu końcowego na wykrycie konfiguracji maszyny i zaadoptowanie odpowiedniej technologii skanowania. Administrator może również dostosować silniki skanowania wybierając pośród kilku technologii skanowania:

1. **Skanowanie Lokalne**, gdy skanowanie jest wykonywane na lokalnym punkcie końcowym. Tryb Skanowania Lokalnego nadaje się do potężnych maszyn, posiadających wszystkie sygnatury i silniki przechowywane lokalnie.
2. **Hybrydowe Skanowanie z Lekkimi Silnikami (Chmura Publiczna)** z umiarkowanym odwzorowaniem, wykorzystując skanowanie w chmurze i, częściowo, lokalne sygnatury. Ten tryb skanowania przynosi korzyści z lepszego wykorzystania zasobów oraz angażuje poza przesłankowe skanowanie.
3. **Centralne skanowanie w osobistej chmurze** przy pomocy niewielkiego odwzorowania wymagającego serwera ochrony do skanowania. W tym przypadku żadna sygnatura nie jest przechowywana lokalnie, a skanowanie jest wykonywane na zabezpieczonym serwerze.

Notatka
Jest to minimalny zestaw silników przechowywanych lokalnie potrzebnych do rozpakowywania skompresowanych plików.

4. **Centralne Skanowanie (Prywatna Chmura skanowanie z Security Server)z awaryjnym* Skanowaniem Lokalnym (Pełne Silniki)**
5. **Centralne Skanowanie (Prywatna Chmura skanowanie z Security Server) z awaryjnym* Skanowaniem Hybrydowym (Publiczna Chmura z Lekkimi Silnikami)**

* Podczas wykorzystania podwójnego silnika skanowania, gdy pierwszy silnik jest niedostępny, zostanie użyty silnik awaryjny. Zużycie zasobów oraz wykorzystanie sieci będzie bazowało względnie do użytych silników.

POKAŻ MODUŁY

Następujące moduły ochrony są dostępne z Bitdefender Endpoint Security Tools:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- Zapora Sieciowa
- Kontr. Zawart.
- Kontrola Urządzenia
- Super Użytkow.

Antymalware

Moduł ochrony antymalware bazuje na skanowaniu sygnatur i heurystycznej analizy (B-HAVE) przeciwko: wirusom, robakom, trojanom, spyware, adaware, keyloggerami, rootkitami i innymi typami złośliwego oprogramowania.

Technologia skanowania antymalware Bitdefender opiera się na następujących warstwach ochrony:

- Po pierwsze, tradycyjna metoda skanowania jest wykorzystywana, gdzie zeskanowana treść jest dopasowana do bazy sygnatur. Baza sygnatur zawiera wzory bajtów charakterystycznych dla znanych zagrożeń i jest regularnie aktualizowana przez Bitdefender. Ta metoda skanowania jest skuteczna przeciwko potwierdzonym zagrożeniom, które były badane i udokumentowane. Jakkolwiek bez względu na to jak szybko baza sygnatur jest aktualizowana, zawsze istnieje luka pomiędzy czasem gdy nowe zagrożenie zostaje odkryte a tym kiedy zostaje wydana poprawka.
- Przeciwko najnowszym, nieudokumentowanym zagrożeniom stosowana jest druga warstwa ochrony której dostarcza nam **B-HAVE**, heurystyczny silnik Bitdefender. Algorytmy heurystyczne wykrywają szkodliwe oprogramowanie na podstawie cech behawioralnych. B-HAVE uruchamia podejrzany malware w środowisku wirtualnym, aby sprawdzić jego wpływ na system i upewnić się, że

nie stanowi zagrożenia. Jeśli zagrożenie zostało wykryte, uniemożliwione jest uruchomienie programu.

Zaawansowana Kontrola Zagrożeń

Dla zagrożeń, które wymykają się nawet silnikowi heurystycznemu, trzecia warstwa ochrony występuje w formie Zaawansowanej Kontroli Zagrożeń (ATC).

Zaawansowana Kontrola Zagrożeń stale monitoruje procesy i ocenia podejrzane zachowania, takie jak próby: ukrycia typu procesu, wykonanie kodu w innej przestrzeni procesowej (HJ pamięci procesu dla przekroczenia uprawnień), replikacji, upuszczenia plików, ukrycia aplikacji wyliczeń procesowych, itp. Każde podejrzane zachowanie podnosi rating procesu. Gdy próg zostanie osiągnięty, wyzwalany jest alarm.

WAŻNE

Moduł ten jest dostępny wyłącznie dla komputerów stacjonarnych i serwerów obsługiwanych systemów operacyjnych Windows, z wyjątkiem:

- Windows XP (64-bit)
- Windows Server 2003 / Windows Server 2003 R2 (32-bit, 64-bit)

Zapora Sieciowa

Firewall kontroluje dostęp aplikacji do sieci i do Internetu. Dostęp jest automatycznie dopuszczony do obszernej bazy danych znanych, uzasadnionych wniosków. Ponadto zapora sieciowa chroni system przed skanowaniem portów, ograniczeniami ICS i ostrzega gdy nowe węzły dokonują połączenia przez Wi-Fi.

WAŻNE

Ten moduł jest dostępny tylko dla wspieranych stacji roboczych Windows, z wyjątkiem starszych systemów operacyjnych. Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne” (p. 14).

Kontr. Zawart.

Moduł Kontroli Zawartości pomaga w egzekwowaniu polityki firmy dla dozwolonego ruchu, dostępu do sieci, ochrony danych i kontroli aplikacji. Administratorzy mogą definiować opcje skanowania ruchu i wykluczeń, harmonogram dostępu do stron internetowych, podczas blokowania lub dopuszczania niektórych kategorii stron internetowych lub adresów URL, mogą konfigurować zasady ochrony danych i zdefiniować uprawnienia do korzystania z określonych aplikacji.

WAŻNE
Ten moduł jest dostępny tylko dla wspieranych stacji roboczych Windows, z wyjątkiem starszych systemów operacyjnych. Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne" (p. 14).

Kontrola Urządzenia

Moduł Kontroli Urządzeń umożliwia zapobieganie wyciekom poufnych danych i infekcjom malware za pośrednictwem urządzeń zewnętrznych podłączanych do urządzeń końcowych poprzez zastosowanie reguł i wyjątków przez polityki szerokiego zakresu typów (takich jak urządzenia USB, Bluetooth, napędy CD/DVD, Urządzenia pamięci masowej, itp.).

WAŻNE
Ten Moduł jest dostępny tylko dla komputerów stacjonarnych i serwerów obsługiwanych systemów operacyjnych Windows, z wyjątkiem tych starszych systemów. Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne" (p. 14).

Super Użytkow.

Administratorzy Control Center mogą przyznawać prawa Power User użytkownikom punktów końcowych poprzez ustawienia polityk. Moduł Power User umożliwia uprawnienia administratora na poziomie użytkownika, umożliwiając użytkownikowi dostęp do punktów końcowych i modyfikację ustawień zabezpieczeń za pomocą lokalnej konsoli. Control Center jest powiadamiana, gdy punkt końcowy jest w trybie Power User i administrator Control Center zawsze może nadpisać ustawienia lokalnych zabezpieczeń.

WAŻNE
Ten Moduł jest dostępny tylko dla komputerów stacjonarnych i serwerów obsługiwanych systemów operacyjnych Windows, z wyjątkiem tych starszych systemów. Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne" (p. 14).

Role Punktów Końcowych

Rola Relay

Agenci Endpoint z rolą Bitdefender Endpoint Security Tools Relay służącą jako serwer komunikacji proxy i aktualizacji dla innych punktów końcowych w sieci. Agenci Endpoint z rolą relay są szczególnie potrzebni w organizacjach z sieciami

zamkniętymi, gdzie cały ruch odbywa się za pośrednictwem jednego punktu dostępu.

W firmach z dużym rozproszeniem sieci, agenci relay pomagają obniżenie wykorzystania pasma, zapobiegając bezpośredniemu łączeniu się chronionych punktów końcowych i serwerów bezpieczeństwa za każdym razem bezpośrednio z konsolą zarządzającą GravityZone.

Gdy agent Bitdefender Endpoint Security Tools Relay jest zainstalowany w sieci, inne punkty końcowe mogą być skonfigurowane za pomocą polityki do komunikacji przez agenta relay z Control Center.

Agenci Bitdefender Endpoint Security Tools Relay służą do następujących czynności:

- Wykrywanie wszystkich niezabezpieczonych punktów końcowych w sieci.

  Funkcjonalność ta jest niezbędna do wdrażania agenta bezpieczeństwa w środowisku chmury GravityZone.
- Wdrażanie agenta endpoint w sieci lokalnej.
- Aktualizacja chronionych punktów końcowych w sieci.
- Zapewnienie komunikacji pomiędzy Control Center i podłączonymi punktami końcowymi.
- Działa jako serwer proxy dla chronionych punktów końcowych.
- Optymalizowanie ruchu sieciowego podczas aktualizacji, wdrożenia, skanowania i innych konsumujących zasoby zadań.

WAŻNE
Rola ta jest dostępna wyłącznie dla komputerów stacjonarnych i serwerów obsługiwanych systemów operacyjnych Windows.

Rola Ochrony Exchange

Bitdefender Endpoint Security Tools z rolą Exchange może być zainstalowany na serwerach Microsoft Exchange w celu ochrony użytkowników Exchange przed zagrożeniami pochodzącymi z wiadomości e-mail.

Bitdefender Endpoint Security Tools z wolą Exchange chroni zarówno urządzenie serwera oraz rozwiązanie Microsoft Exchange.

Endpoint Security for Mac

Endpoint Security for Mac jest potężnym skanerem antymalware, który wykrywa i usuwa wszystkie rodzaje złośliwego oprogramowania, wirusów, spyware, konie

trojańskie, keyloggery, robaki i adware na komputerach Macintosh z procesorami Intel, stacjach roboczych i laptopach z systemem Mac OS X w wersja 10.8.5 lub nowszą.

Endpoint Security for Mac zawiera tylko moduł Antymalware, podczas gdy dostępna jest technologia skanowania **Skanowanie Lokalne**, ze wszystkimi sygnaturami i silnikami przechowywanymi lokalnie.

2. WYMAGANIA DOTYCZĄCE INSTALACJI

Wszystkie rozwiązania GravityZone są instalowane i zarządzane przez Control Center.

2.1. Wymagania Ochrony Punktu Końcowego

Aby chronić Twoją sieć z Bitdefender, musisz zainstalować agentów bezpieczeństwa GravityZone na punktach końcowych sieci. Aby zoptymalizować ochronę, możesz także zainstalować Security Server. W tym celu, potrzebujesz użytkownika z prawami administracyjnymi Control Center nad usługami jakie potrzebujesz zainstalować i nad punktami końcowymi sieci, którą zarządzasz.

2.1.1. Wymagania Agenta Bezpieczeństwa

Wymagania Sprzętowe

Procesor kompatybilny z Intel® Pentium

Systemy operacyjne stacji roboczych

- 1 GHZ lub szybszy dla Microsoft Windows XP SP3 i Windows XP SP2 64 bit
- 2 GHz lub szybszy dla Microsoft Windows Vista SP1 lub wyższy (32 i 64 bit), Microsoft Windows 7 (32 i 64 bit), Microsoft Windows 7 SP1 (32 i 64bit), Windows 8, Windows 8.1, Windows 10, Windows 10 TH2, Windows 10 Anniversary Update "Redstone"
- 800 MHZ lub szybszy dla Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded z Service Pack 2, Microsoft Windows XP Tablet PC Edition

Systemy operacyjne serwera

- Minimalnie: 2.4 GHz jednordzeniowy CPU
- Rekomandowane: 1.86 GHz lub szybszy Intel Xeon wielordzeniowy CPU

Wolna pamięć RAM

Wymagana do instalacji pamięć RAM (MB)

OS	POJEDYNCZY SILNIK					
	Skan. Lokalne		Skan. Hybrydowe		Scentraliz. Skan.	
	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje
Windows	1024	1200	512	660	256	400
Linux	1024	1024	512	512	256	256
Mac	1024	1024	n/d	n/d	n/d	n/d

Pamięć RAM do codziennego użycia (MB)*

OS	Antywirus (Poj. Silnik)			Moduły Ochrony				
	Lokal.	Hybryda	Scentraliz.	Skanowanie Behaw.	Zapora Sieciowa	Kontrola Zaw.	Power User	Serwer Aktual.
Windows	75	55	30	+13	+17	+41	+29	+76
Linux	200	180	90	-	-	-	-	-
Mac	300	-	-	-	-	-	-	-

* Pomiar pokrycia dziennego użycia klientów punktów końcowych, bez brania pod uwagę dodatkowych zadań, takich jak skanowanie na żądanie lub aktualizacje produktu.

Wymagania HDD

Wolna Przestrzeń HDD Wymagana do Instalacji (MB)

OS	POJEDYNCZY SILNIK						PODWÓJNY SILNIK			
	Skan. Lokalne		Skan. Hybrydowe		Scentraliz. Skan.		Scentraliz. + Lokalne Skan.		Scentraliz. + Hybrydowe Skan.	
	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje
Windows	1024	1200	500	700	350	570	1024	1200	500	700
Linux	1024	1024	400	400	250	250	1024	1024	400	400
Mac	1024	1024	n/d	n/d	n/d	n/d	n/d	n/d	n/d	n/d

Notatka

- Wymagane jest co najmniej 10 GB dodatkowego wolnego miejsca na dysku dla podmiotów z rolą Bitdefender Endpoint Security Tools Relay, gdyż będą one przechowywać wszystkie aktualizacje i paczki instalacyjne.
- Kwarantanna dla Serwerów Exchange wymaga dodatkowej przestrzeni dyskowej na partycji gdzie zainstalowano agenta bezpieczeństwa.

  Rozmiar kwarantanny zależy od liczby elementów przechowywanych oraz ich wielkości.

  Domyślnie, agent jest instalowany na systemowej partycji.

Wolne Miejsce na HDD dla Codziennego Użytkowania (MB)*

OS	Antywirus (Poj. Silnik)			Moduły Ochrony				
	Lokal.	Hybryda	Scentraliz.	Skanowanie Behaw.	Zapora Sieciowa	Kontrola Zaw.	Power User	Serwer Aktual.
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
Mac	1024	-	-	-	-	-	-	-

* Pomiar pokrycia dziennego użycia klientów punktów końcowych, bez brania pod uwagę dodatkowych zadań, takich jak skanowanie na żądanie lub aktualizacje produktu.

Wykorzystanie Ruchu

- **Ruch aktualizacji produktu pomiędzy punktem końcowym klienta a serwerem aktualizacji**

  Każda periodyczna aktualizacja produktu Bitdefender Endpoint Security Tools podczas pobierania generuje następujący ruch dla każdego klienta punktu końcowego:

  - Dla systemu operacyjnego Windows: ~20 MB
  - Dla systemu operacyjnego Linux: ~26 MB
  - Dla Mac OS: ~25 MB

- **Ruch aktualizacji pobranych sygnatur, pomiędzy klientem punktu końcowego a serwerem aktualizacji**

Typ Serwera Aktualizacji	Typ Silnika Skanowania		
	Lokal.	Hybryda	Scentraliz.
Relay (MB / dzień)	65	58	55
Bitdefender Serwer Aktualizacji (MB / dzień)	3	3.5	3

- **Ruch Centralnego Skanowania pomiędzy klientem punktu końcowym i Security Server**

Przeskanowane Obiekty	Typ Ruchu		Pobrano (MB)	Przesłano (MB)
Pliki*	Pierwsze skanowanie		27	841
	Skanowanie buforowane		13	382
Strony internetowe**	Pierwsze skanowanie	Ruch sieciowy	621	Niedostępny
		Security Server	54	1050
	Skanowanie buforowane	Ruch sieciowy	654	Niedostępny
		Security Server	0.2	0.5

* Dostarczone dane zostały zmierzone na 3.49 GB plików (6'658 plików), z których 1.16 GB to przenośne pliki wykonywalne (PE).

** Dostarczone dane zostały wyliczone z najwyższych pozycji rankingów 500 stron internetowych.

- **Ruch hybrydowego skanowania pomiędzy klientem punktu końcowego a Usługą Chmury Bitdefender**

Przeskanowane Obiekty	Typ Ruchu	Pobrano (MB)	Przesłano (MB)
Pliki*	Pierwsze skanowanie	1.7	0.6
	Skanowanie buforowane	0.6	0.3
Ruch sieciowy**	Ruch sieciowy	650	Niedostępny
	Usługi w Chmurze Bitdefender	2.6	2.7

* Dostarczone dane zostały zmierzone na 3.49 GB plików (6'658 plików), z których 1.16 GB to przenośne pliki wykonywalne (PE).

** Dostarczone dane zostały wyliczone z najwyższych pozycji rankingów 500 stron internetowych.

Notatka
Letencja sieciowa pomiędzy klientem punktu końcowego i Serwerem Chmury Bitdefender muszi wynosić poniżej 1 sekundy.

- **Ruch sygnatur pobierania pomiędzy klientami Bitdefender Endpoint Security Tools Relay i serwerem aktualizacji**

  Klient z rolą Bitdefender Endpoint Security Tools Relay pobiera ~16 MB / na dzień* z serwera aktualizacji.

  * Dostępne wraz z klientem Bitdefender Endpoint Security Tools zaczynając od wersji 6.2.3.569.

- **Ruch pomiędzy klientami punktów końcowych i konsolą webowoą Control Center**

  przeciętny ruch to 618 KB / dzień jest generowany pomiędzy punktem końcowym klienta i webowej konsoli Control Center.

Wspierane systemy operacyjne

System Operacyjny Windows

Systemy Operacyjne Komputerów

- Windows 10 Anniversary Update "Redstone"(2)
- Windows 10 TH2(2)
- Windows 10(2)
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista z dodatkiem Service Pack 1
- Windows XP z Service Pack 2 64 bit(1)
- Windows XP z Service Pack 3(1)

Tablety i Wbudowane Systemy Operacyjne

- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009 (1)
- Windows Embedded Standard 2009 (1)
- Windows XP z wbudowanym Service Pack 2(1)(3)
- Windows XP Tablet PC Edition(1)(3)

Systemy operacyjne serwera

- Windows Server 2016
- Windows Server 2012 / Windows Server 2012 R2
- Windows Server 2008 / Windows Server 2008 R2
- Windows Server 2003(1) / Windows Server 2003 R2(1)
  Windows Server 2003(1)(9) / Windows Server 2003 R2(1)
- Windows Small Business Server (SBS) 2011
- Windows Small Business Server (SBS) 2008
- Windows Small Business Server (SBS) 2003(1)
- Windows Home Server(1)

WAŻNE
Bitdefender Endpoint Security Tools obsługuje technologię Windows Server Failover Cluster (WSFC).

Ostrzeżenie
(1) Wraz z 30-tym stycznia 2017 roku, Bitdefender ogranicza ochronę do Antymalware i Zaawansowanej Kontroli Zagrożeń (jeśli wspierana) dla starszych systemów operacyjnych.

(2) Tylko Bitdefender Endpoint Security Tools i Endpoint Security oferują wsparcie dla Windows 10. Aby sprawdzić wersje, z których jest to dostępne, przejdź do specyfiki produktu Informacji o Wydaniu.
(3) Te specyficzne wbudowane komponenty systemów operacyjnych muszą być zainstalowane:

- Sieci TCP/IP z klientem dla sieci Microsoft
- Wsparcie Baz Binarnych
- Manager Filtra
- Wsparcie DNS Cache
- Instalator Windows
- WMI Windows Installer Provider
- Usługa Stacji roboczej
- WinHTTP
- Windows XP Service Pack 2 Resource DLL
- Windows Logon (Standard)
- Powłoka Explorer
- Format NTFS

Systemy Operacyjne Linux

- Red Hat Enterprise Linux / CentOS 5.6 lub wyższy
- Ubuntu 12.04 lub wyższy

WAŻNE
Proszę zanotować, że repozytorium Ubuntu 12.04 będzie niedostępne z początkiem Kwietnia 2017 roku. Mocno zachęcamy do podniesienia Ubuntu do wersji 14.04.

- SUSE Linux Enterprise Server 11 lub wyższy
- OpenSUSE 11 lub wyższy
- Fedora 16 lub wyższy
- Debian 7.0 lub wyższy
- Amazon Linux AMI
- Oracle Linux 6.3 lub nowszy

Skanowanie dostępowe jest dostępne dla wszystkich gościnnych systemów operacyjnych. Na systemach Linux, skanowanie dostępowe jest dostarczane w następujących sytuacjach:

Wersja Kernel	Dystrybucja Linux	Wsparcie skanowania dostępowego
2.6.38 lub wyższe	Wszystkie wspierane	Opcja jądra fanotify musi być włączona. Dla systemów Debian 8, przejdź do tego artykułu.
2.6.18 - 2.6.37	Debian 5.0, 6.0 CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender zapewnia wsparcie poprzez DazukoFS z prekombilowanymi modułami kernela.

Dla innych dystrybucji oraz wersji kernela potrzebujesz manualnie skompilować moduł DazukoFS. Aby zobaczyć procedurę manualnej komplikacji DazukoFS, zobacz:„Ręcznie skompiluj moduł DazukoFS." (p. 43)

Notatka
Fanotify i DazukoFS włącza trzecią część aplikacji aby kontrolowały dostęp do plików w systemie Linux. Aby uzyskać więcej informacji, odwołaj się do:

- Strony podręcznika fanotify: http://www.xypron.de/projects/fanotify-manpages/man7/fanotify.7.html.
- Strona projektu Dazuko project: http://dazuko.dnsalias.org/wiki/index.php/About.

Systemy Operacyjne Mac OS X

- Mac OS X Sierra (10.12.x)
- Mac OS X El Capitan (10.11.x)
- Mac OS X Yosemite (10.10.5)
- Mac OS X Mavericks (10.9.5)
- Mac OS X Mountain Lion (10.8.5)

Obsługiwane systemy plików

Bitdefender instaluje się na i chroni następujące systemy plików:

AFS, BTRFS, ext2, ext3, ext4, FAT, FAT16, FAT32, VFAT, exFAT, NTFS, UFS, ISO 9660 / UDF, NFS, CIFS/SMB, VXFS, XFS.

Notatka
Skanowanie dostępowe nie wspiera NFS i CIFS/SMB.

Obsługiwane przeglądarki

Przeglądarka bezpieczeństwa Endpoint jest weryfikowana do pracy z następującymi przeglądarkami:

- Internet Explorer 8+
- Mozilla Firefox 30+
- Google Chrome 34+
- Safari 4+
- Microsoft Edge 20+
- Opera 21+

2.1.2. Wymagania Security Server

Security Server jest wstępnie skonfigurowaną wirtualną maszyną działającą na Ubuntu Server 16.04 LTS (4.4 kernel).

Notatka
Twoja licencja produktu może nie zawierać tej funkcji.

Bitdefender Security Server może zostać zainstalowany na następujących platformach wirtualizacyjnych:

- VMware vSphere 6.0, 5.5, 5.1, 5.0, 4.1 wraz z VMware vCenter Server 6.0, 5.5, 5.0, 4.1
- VMware View 5.3, 5.2, 5.1, 5.0
- VMware Workstation 8.0.6, 9.x, 10.x, 11.x
- VMware Player 5.x, 6.x, 7.x
- Citrix XenServer 7.0, 6.5, 6.2, 6.0, 5.6 lub 5.5 (zawierający Xen Hypervisor)
- Citrix XenDesktop 7.9, 7.8, 7.7, 7.6, 7.5, 7.1, 7, 5.6, 5.5, 5.0
- Citrix XenApp 7.9, 7.8, 7.6, 7.5, 6.5
- Citrix VDI-in-a-Box 5.x

- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2 lub Windows Server 2008 R2, 2012, 2012 R2 (zawierający Hyper-V Hypervisor)
- Red Hat Enterprise Virtualization 3.0 (zawierający KVM Hypervisor)
- Oracle VM 3.0

Notatka
Wsparcie dla innych platform wirtualizacji może być dostarczone na życzenie.

Przydział zasobów pamięci i procesora dla Security Server zależy od liczby i rodzaju maszyn wirtualnych uruchomionych na komputerze. Poniższa tabela zawiera zalecane zasoby, które mają być przyznane:

Liczb chronionych VMs	RAM	CPU
1-50 maszyn wirtualnych	2 GB	2 CPU
51-100 maszyn wirtualnych	2 GB	4 CPU
101-200 maszyn wirtualnych	4 GB	6 CPU

2.2. Wymagania Ochrony Exchange

Security for Exchange jest dostarczany przez Bitdefender Endpoint Security Tools, który jest w stanie chronić zarówno system plików jak i serwer pocztowy Microsoft Exchange.

2.2.1. Obsługiwane Środowiska Microsoft Exchange

Security for Exchange wspiera następujące wersje i role Microsoft Exchange:

- Exchange Server 2016 z rolą Edge Transport lub Mailbox
- Exchange Server 2013 z rolą Edge Transport lub Mailbox
- Exchange Server 2010 z rolą Edge Transport, Hub Transport lub Mailbox
- Exchange Server 2007 z rolą Edge Transport, Hub Transport lub Mailbox

Security for Exchange jest kompatybilny z Microsoft Exchange Database Availability Groups (DAG).

2.2.2. Wymagania systemowe

Security for Exchange jest kompatybilny z dowolnym fizycznym lub wirtualnym 64- bitowym serwerem (Intel lub AMD) uruchamiając obsługiwaną wersję serwera Microsoft Exchange i rolę. Aby uzyskać więcej informacji na temat wymagań systemowych Bitdefender Endpoint Security Tools, odwołaj się do „Wymagania Agenta Bezpieczeństwa" (p. 10).

Zalecana dostępność zasobów serwera:

- Wolna pamięć RAM: 1 GB
- Wolne miejsce na dysku: 1 GB

2.2.3. Inne Wymagania Oprogramowania

- Dla Microsoft Exchange Server 2013 z Service Pack 1: KB2938053 od Microsoft.
- Dla Microsoft Exchange Server 2007: .NET Framework 3.5 Service Pack 1 lub wyższy

2.3. Porty Komunikacji GravityZone

Poniższa tabela zawiera informacje na temat portów używanych przez składniki GravityZone:

Port	Użycie
80 (HTTP) / 443 (HTTPS)	Port używany do uzyskania dostępu do konsoli webowej Control Center. Bitdefender Cloud Antispam Detection Service
80	Port serwera aktualizacji:.
443 (HTTPS)	Port używany przez klienta oprogramowania do połączenia z Serwerem Komunikacji.
7074 (HTTP)	Port serwera aktualizacji: Komunikacja z Relay* (jeśli jest dostępna)
53 (UDP)	Port wykorzystany dla Listy RBL (RBLs)

* Relay jest serwerem aktualizacji, który musi cały czas nasłuchiwać portu, Bitdefender zapewnia mechanizm zdolny do automatycznego otwierania losowego

portu na hoście lokalnym (127.0.0.1) tak, że serwer aktualizacji może otrzymać odpowiednie szczegóły konfiguracji. Mechanizm ten ma zastosowanie, gdy domyślny port 7074 jest używany przez inny program. W tym przypadku, serwer aktualizacji próbuje otworzyć port 7075 do nasłuchiwania na lokalnym hoście. Jeśli port 7075 jest również niedostępny, serwer aktualizacji będzie szukać innego portu, który jest wolny (w przedziale od 1025 do 65535) i skutecznie będzie nasłuchiwał połączenia z lokalnym hostem.

Aby otrzymać więcej informacji na temat portów GravityZone, patrz ten artykuł KB.

3. INSTALOWANIE OCHRONY

Poniższa tabela przedstawia typy punktów końcowych, każda usługa ma chronić:

Usługa	Punkty końcowe
Security for Endpoints	Komputery fizyczne (stacje robocze, laptopy i serwery) z systemami Microsoft Windows, Linux i Mac OS X
Security for Virtualized Environments	Maszyny wirtualne Microsoft Windows lub Linux
Security for Exchange	Serwery Microsoft Exchange
Security for Amazon Web Services	Instancja EC2 uruchomiona na Microsoft Windows i Linux

3.1. Zarządzanie Licencjami

GravityZone jest licencjonowany za pomocą jednego klucza dla wszystkich usług bezpieczeństwa z wyjątkiem Security for Amazon Web Services, które są subskrybowane za pomocą usług Płatności Amazon. Aby uzyskać więcej informacji na temat licencjonowania Security for Amazon Web Services, przejdź do „Integracja z Usługami Amazon EC2" (p. 53).

Możesz wypróbować GravityZone za darmo przez 30 dni. W okresie próbnym wszystkie funkcje są w pełni dostępne i można korzystać z usługi na dowolnej liczbie komputerów. Przed zakończeniem okresu próbnego, jeśli chcesz nadal korzystać z usług, należy zdecydować się na płatną subskrypcję i dokonać zakupu.

Notatka
Możesz zobaczyć czerwoną wstążkę w górnej części strony internetowej, informującą o wygasłej wersji trial. Jeśli używasz tylko Security for Amazon Web Services, proszę zignorować to ostrzeżenie, gdyż odnosi się ono do usług Security for Endpoints i Security for Virtualized Environments.

Aby kupić licencje, skontaktuj się z sprzedawcą Bitdefender lub skontaktuj sie z nami poprzez e-mail enterprisesales@bitdefender.com.

Twoja subskrypcja jest zarządzana przez Bitdefender lub przez partnera Bitdefender który sprzeda ci usługę. Niektórzy partnerzy Bitdefender są dostawcy usług bezpieczeństwa. W zależności od ustaleń subskrypcyjnych, GravityZone operacje

dzień w dzień mogą być obsługiwane zarówno wewnętrznie lub przez firmę zewnętrzną przez dostawcę usługi bezpieczeństwa.

3.1.1. Szukanie sprzedawcy

Nasi sprzedawcy przekażą Ci potrzebne informacje i pomogą wybrać licencje najlepiej pasującą do twoich potrzeb.

Aby znaleźć sprzedawcę Bitdefender w twoim państwie:

1. Przejdź do strony Lokalizacja Partnerów na stronie Bitdefender.
2. Wybierz kraj w którym mieszkasz, aby zobaczyć dostępne informacje kontaktowe partnerów Bitdefender.
3. Jeśli w swoim kraju nie możesz znaleźć sprzedawcy Bitdefender, skontaktuj się z nami, wysyłając e-mail na adres enterprisesales@bitdefender.com.

3.1.2. Aktywowanie licencji

Przy zakupie płatnego abonamentu po raz pierwszy, klucz licencyjny jest wydawane dla Ciebie. Subskrypcja GravityZone jest włączona przez aktywowanie tego klucza licencyjnego.

Ostrzeżenie
Aktywacja licencji nie dołącza jej możliwości do aktywnej licencji. Zamiast tego, nowa licencja zastępuje starą. Na przykład, aktywowanie 10 licencji punktów końcowych, na działającą wcześniej licencje dla 100 punktów końcowych, NIE da wyniku subskrypcji dla 110 punktów końcowych Wręcz przeciwnie, to zmniejszy liczbę określonych punktów końcowych ze 100 do 10.

Klucz licencyjny zostanie wysłany do Ciebie w wiadomości e-mail po zakupieniu. W zależności od umowy o świadczenie usług, gdy Twój klucz licencyjny jest wydawany, usługodawca może aktywować go dla Ciebie. Alternatywnie, możesz aktywować twoja licencję ręcznie, dzięki poniższym krokom:

1. Zaloguj się do Control Center korzystając ze swojego konta.
2. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moja Firma**.
3. Sprawdź szczegóły obecnej licencji w sekcji **Licencja**.
4. W sekcji **Licencja**, wybierz typ **Licencja**.
5. W polu **Klucz licencyjny** podaj klucz licencyjny.

6. Naciśnij przycisk **Sprawdź** i poczekaj zanim Control Center prześle informacje o wpisanym kluczu licencyjnym.
7. Kliknij **Zapisz**.

3.1.3. Sprawdzanie szczegółów aktualnej licencji

zobacz szczegóły twojej licencji:

1. Zaloguj się do Control Center używając twojego adresu e-mail i hasła otrzymanych w wiadomości e-mail.
2. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moja Firma**.
3. Sprawdź szczegóły obecnej licencji w sekcji **Licencja**. Możesz nacisnąć również przycisk **Sprawdź** i poczekaj zanim Control Center prześle informacje o posiadanym kluczu licencyjnym.

3.2. Instalowanie Ochrony Endpoint

W zależności od konfiguracji maszyn i środowiska sieci, możesz wybrać, aby zainstalować tylko agenty bezpieczeństwa lub aby użyć także Security Server. W tym ostatnim przypadku, trzeba najpierw zainstalować Security Server, a następnie agenty bezpieczeństwa.

Zaleca się, aby użyć Security Server jeśli maszyny mają mało zasobów sprzętowych.

WAŻNE
Tylko Bitdefender Endpoint Security Tools i Bitdefender Tools wspierają połączenie do Security Server. Aby uzyskać więcej informacji, odwołaj się do „ Architektura GravityZone" (p. 2).

3.2.1. Instalowanie Security Server

Notatka
Twoja licencja produktu może nie zawierać tej funkcji.

Instalowanie Security Server na Hostach

Musisz zainstalować Security Server na jednym lub więcej hostach tak, aby dostosować liczbę wirtualnych maszyn, które będą chronione.

Musisz wziąć pod uwagę liczbę chronionych maszyn wirtualnych, zasoby dostępne dla Security Server na hoście, tak jak połączenie sieciowe pomiędzy Security Server i chronionymi maszynami wirtualnymi.

Notatka
Security Server musi zostać zainstalowany jedynie w lokalnych sieciach, w celu ochrony maszyn wirtualnych zainstalowanych po stronie firmy. Przy zarządzaniu intancjami Amazon EC2, nie ma potrzeby instalowania maszyny Security Server, gdy te są już hostowane przez Bitdefender dla każdego regionu AWS.

Agent bezpieczeństwa zainstalowany na maszynach wirtualnych łączy się do Security Server za pośrednictwem protokołu TCP/IP, używając szczegółów podczas instalacji szczegółów lub poprzez polityki.

Instalacja lokalna

Pakiet Security Server jest dostępny dla pobierania z Control Center w kilku różnych formatach, kompatybilne z głównymi wirtualnymi platformami.

Pobieranie Pakietów Instalacyjnych Security Server

Aby pobrać pakiety instalacyjne Security Server:

1. Przejdź do strony **Sieć > Pakiety**.
2. Wybierz Domyślny Pakiet Security Server.
3. Kliknij przycisk **Pobierz** w górnej części tabeli i wybierz typ pakietu z menu.
4. Zapisz wybrany pakiet w odpowiedniej lokalizacji.

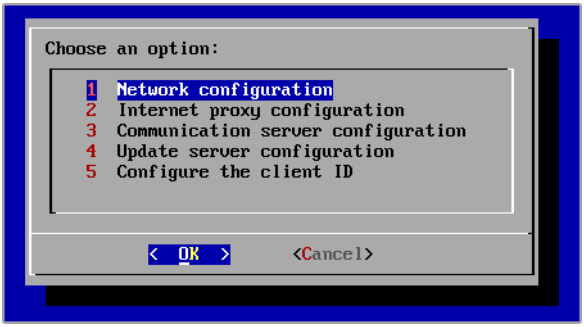
Wdrażanie Paczek instalacyjnych Security Server

Gdy masz pakiet instalacyjny, wdróż go na hosta używając preferowanego narzędzia do instalacji maszyny wirtualnej.

Po wdrożeniu, ustawSecurity Server w ten sposób:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere). Alternatywnie, możesz połączyć się z urządzeniem przez SSH.
2. Zaloguj się używając domyślnych poświadczeń.
   - Nazwa użytkownika: `root`
   - Hasło:`sve`

3. Uruchom komendę `sva-setup`. Będziesz miał dostęp do interfejsu konfiguracyjnego urządzenia.



Security Server interfejs konfiguracji (menu główne)

Aby poruszać się po menu i opcjach, użyj klawisza `Tab` i strzałek. Aby wybrać konkretną opcję, naciśnij `Enter`.

4. Konfiguruj ustawienia sieciowe.

   Security Server wykorzystuje protokół TCP/IP do komunikowania się z innym komponentem GravityZone. Możesz skonfigurować urządzenie, aby automatycznie uzyskiwało ustawienia sieciowe z serwera DHCP lub możesz ręcznie skonfigurować ustawienia, tak jak opisano w następującym dokumencie:

   a. Z głównego menu, wybierz **Konfiguracja Sieci**.

   b. Wybierz interfejs sieciowy.

   c. Wybierz tryb konfiguracji IP:

      - **DHCP**, jeśli chcesz aby Security Server automatycznie pozyskiwał ustawienia sieci z serwera DHCP.
      - **Statyczny**, jeśli serwer DHCP jest niedostępny lub rezerwacja IP dla tego urządzenia została dokonana na serwerze DHCP. W tym przypadku, musisz ręcznie skonfigurować ustawienia sieci.

        i. Wprowadź nazwę hosta, adres IP, maskę sieci, bramę i DNS serwera w odpowiednich polach.

        ii. Wybierz **OK** aby zapisać zmiany.

Notatka
Jeżeli łączysz się z urządzeniem przez klienta SSH, zmieniając ustawienia sieci, natychmiast zostanie zakończona twoja sesja.

5. Konfiguruj ustawienia proxy.

   Jeżeli serwer proxy jest używany wewnątrz sieci, musisz dostarczyć jego szczegóły tak by Security Server mógł komunikować się z Control Center GravityZone.

   Notatka
   Tylko proxy z podstawowym uwierzytelnianiem są obsługiwane.

   a. Z głównego menu, wybierz **Konfiguracja Internetowego proxy**.
   b. Wprowadź nazwę hosta, nazwę użytkownika, hasło i domenę w odpowiednim polu.
   c. Wybierz **OK** aby zapisać zmiany.
6. Skonfiguruj adres Serwera Komunikacyjnego.
   a. Z głównego menu, wybierz **Konfiguracja serwera Komunikacyjnego**.
   b. Wprowadź jeden z następujących adresów dla Serwera Komunikacji:
      - `https://cloud-ecs.gravityzone.bitdefender.com:443/hydra`
      - `https://cloudgz-ecs.gravityzone.bitdefender.com:443/hydra`

      WAŻNE
      Ten adres musi być taki sam jak ten, który pojawia się w ustawieniach polityki Control Center. Aby sprawdzić link, idź do strony **Polityki**, dodaj lub otwórz politykę niestandardową, nawiguj do sekcji **Ogólne > Komunikacja > Przypisanie Komunikacji Punktu Końcowego** sekcji i wprowadź nazwę serwera komunikacyjnego w polu nagłówka kolumny. Prawidłowy serwer pojawi się w wynikach wyszukiwania.

   c. Wybierz **OK** aby zapisać zmiany.
7. Konfiguruj ID klienta.
   a. Z menu głównego wybierz **Konfiguruj ID klienta**.
   b. Wprowadź ID firmy.

ID składa się z 32 znaków, które można znaleźć poprzez wejście na stronę szczegółów firmy w Control Center.

c. Wybierz **OK** aby zapisać zmiany.

3.2.2. Instalowanie Agentów Bezpieczeństwa

Aby dowiedzieć się więcej o dostępnych agentach bezpieczeństwa, przejdź do „Agenci Bezpieczeństwa" (p. 3).

Aby chronić swoje fizyczne i wirtualne punkty końcowe, a także instacje Amazon EC2, musisz zainstalować agenta bezpieczeństwa na każdym z nich. Poza zarządzaniem ochroną na lokalnym punkcie końcowym, agent bezpieczeństwa komunikuje się także z Control Center, aby otrzymywać polecenia administratora i wysyłać wyniki swoich działań.

Na maszynach z systemem Windows, agenty bezpieczeństwa mogą mieć dwie role i możesz je zainstalować następująco:

1. Jako prosty agent bezpieczeństwa dla Twoich punktów końcowych.
2. Jako Relay działający jako agent bezpieczeństwa, a takze jako serwer komunikacyjny, proxy i serwer aktualizacji dla innych punktów końcowych w sieci.

Ostrzeżenie

- Pierwszy punkt końcowy, na którym zainstalujesz ochronę musi posiadać rolę Relay, w innym wypadku nie będziesz w stanie zdalnie zainstalować agenta bezpieczeństwa na innym punkcie końcowym w tej samej sieci.
- Relay punktu końcowego musi być włączony i online w celu komunikacji i łączności agentów z Control Center.

Możesz zainstalować agenty bezpieczeństwa na fizycznym lub wirtualnym punkcie końcowym poprzez uruchomienie pakietów lokalnie lub poprzez uruchomienie zadania zdalnie z Control Center.

To bardzo ważne żeby dokładnie czytać i śledzić instrukcje aby przeprowadzić instalacje.

W trybie normalnym, agenty bezpieczenstwa mają minimalny interfejs użytkownika. Dopuszcza tylko użytkowników aby sprawdzić status ochrony i uruchomić podstawowe zadania bezpieczeństwa (aktualizacje i skanowanie), bez zapewnienia dostępu do ustawień.

Jeśli został włączony przez administratora sieci poprzez paczkę instalacyjną i polityki bezpieczeństwa, agent bezpieczeństwa może również uruchomić Tryb Power User na punktach końcowych z systemem Windows, pozwalając użytkownikowi punktu końcowego wyświetlać i modyfikować ustawienia polityk. Niemniej jednak administrator Control Center może zawsze kontrolować, zawsze ustawienia polityk są stosowane, zastępując tryb Power User.

Domyślnie, wyświetlany język interfejsu użytkownika na chronionych punktach końcowych jest ustawiony w czasie instalacji na język Twojego konta. Aby zainstalować interfejs użytkownika w innym języku na wybranych punktach końcowych, możesz stworzyć pakiet instalacyjny i ustawić preferowany język w opcjach konfiguracyjnych. Aby uzyskać więcej informacji o tworzeniu paczek instalacyjnych, odwołaj się do „Tworzenie pakietów instalacyjnych" (p. 31).

Przygotowywanie do Instalacji

Przed instalacja, wykonaj poniższe kroki przygotowawcze, aby upewnić się, że wszystko się uda:

1. Upewnij się, że docelowe punkty końcowe spełniają minimalne wymagania sprzętowe. Dla niektórych punktów końcowych, możesz potrzebować zainstalować ostatni dostępny service pack dla systemu operacyjnego lub wolne miejsce na dysku. Sprządź listę punktów końcowych, które nie spełniają niezbędnych wymogów, aby można było je wykluczyć z zarządzania.
2. Odinstaluj (nie tylko wyłącz) każde oprogramowanie antymalware, firewall lub ochronę Internetu z docelowych punktów końcowych. Uruchomienie agenta bezpieczeństwa jednocześnie z innym oprogramowaniem ochronnym na punkcie końcowym, może wpływać na ich działanie i spowodować problemy z systemem.

   Wiele niekompatybilnych programów bezpieczeństwa jest automatycznie wykrywanych i usuwanych w czasie instalacji. Aby nauczyć się wiecej i sprawdzić liste wykrytych programów ochronnych, odwołaj się do tego artykułu KB.

   WAŻNE
   Nie musisz się bac o funkcje bezpieczeństwa Windows (Windows Defender, Windows Firewall), zostaną one wyłączone automatycznie przez rozpoczęciem instalacji.

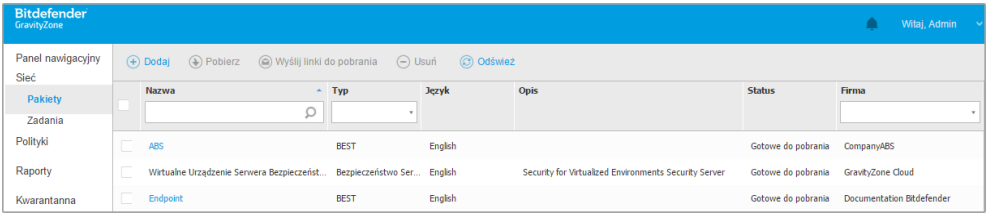
3. Instalacja wymaga praw administracyjnych i dostępu do internetu. Upewnij się, że posiadasz niezbędne poświadczenia dla wszystkich punktów końcowych.
4. Punkty końcowe muszą mieć połączenie z Control Center.

5. Zaleca się, aby używać statycznego adresu IP dla serwera relay. Jeśli nie ustawiłeś statycznego adresu IP, użyj nazwy hosta maszyny.

Instalacja lokalna

Jednym sposobem na instalację agenta bezpieczeństwa na punkcie końcowym jest lokalne uruchomienie pakietów instalacyjnych.

Możesz tworzyć i zarządzać pakietami instalacyjnymi na stronie **Sieć > Pakiety** .



Strona Pakietów

Ostrzeżenie

- Pierwsza maszyna, na której zainstalujesz zabezpieczenie musi mieć rolę Relay, w przeciwnym razie nie będziesz w stanie wdrożyć agenta bezpieczeństwa na innych punktach końcowych w sieci.
- Maszyna Relay musi być włączona i widoczna online, aby klienci mieli połączenie z Control Center.

Gdy pierwszy klient zostanie zainstalowany, zostanie on wykorzystany do wykrycia innych punktów końcowych w tej samej sieci, bazując na mechanizmie wykrywania sieci. Aby uzyskać więcej informacji o wykrywaniu sieci, odwołaj się do „Jak działa wyszukiwanie sieci” (p. 45).

Aby lokalnie zainstalować agenta bezpieczeństwa na punkcie końcowym, należy wykonać następujące kroki:

1. Utwórz pakiet instalacyjny według swoich potrzeb.

   Notatka
   Ten krok nie jest obowiązkowym, jeśli pakiet już został stworzony dla sieci w ramach twojego konta.

2. Pobierz pakiet instalacyjny na docelowy punkt końcowy.

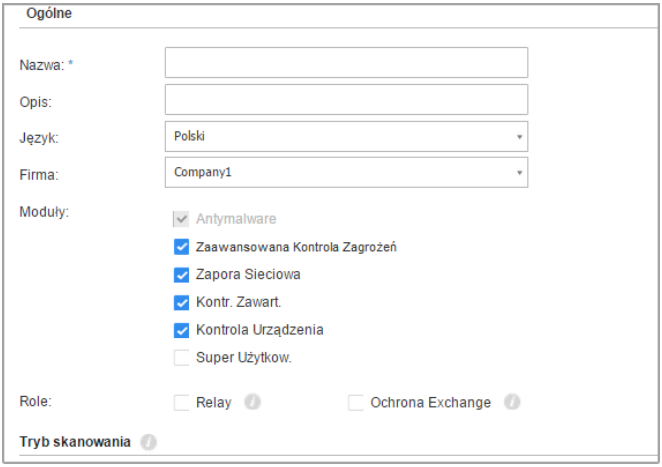
Alternatywnie możesz wysłać linki do pobrania pakietów instalacyjnych w wiadomości e-mail do kilku użytkowników sieci.

3. Uruchom pakiet instalacyjny na docelowym punkcie końcowym.

Tworzenie pakietów instalacyjnych

Aby utworzyć pakiet instalacyjny:

1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć > Pakiety**.
3. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Wyświetlone zostanie okno konfiguracji.



Tworzenie Paczek - Opcje

4. Wpisz sugestywną nazwę i opis dla pakietów instalacyjnych, które chcesz stworzyć.
5. Z pola **Języki**, wybierz żądany język dla interfejsu klienta.
6. Wybierz moduły ochrony, które chcesz zainstalować.

Notatka
Zostaną zainstalowane tylko obsługiwane moduły dla każdego z systemów operacyjnych. Aby uzyskać więcej informacji, odwołaj się do „POKAŻ MODUŁY” (p. 5).
W instancjach Amazon EC2, tylko moduły Antymalware, Kontrola Aktywności Wirusów i Kontrola Urządzeń są wspierane.

7. Wybierz docelową rolę punktu końcowego:
   - **Relay**, aby stworzyć pakiet dla punktu końcowego z rolą Relay. Aby uzyskać więcej informacji, odwołaj się do „Rola Relay” (p. 7)
   - **Ochrona Exchange**, aby zainstalować moduły zabezpieczeń dla Serwerów Microsoft Exchange, w tym antymalware, antyspam, filtrowanie treści i załączników dla ruchu pocztowego Exchange i skanowania antymalware na żądanie baz danych programu Exchange. Aby uzyskać więcej informacji, odwołaj się do „Instalowanie Ochrony Exchange” (p. 49).
8. **Tryb skanowania**. Wybierz technologię skanowania, która najlepiej pasuje do Twojego środowiska sieciowego i zasobów punktów końcowych. Możesz zdefiniować tryb skanowania, poprzez wybranie jednego z następujących typów:
   - **Automatyczne**. W tym przypadku, agent bezpieczeństwa będzie automatycznie wykrywał konfigurację punktu końcowego i odpowiednio dostosuje technologię skanowania:
     - Centralne Skanowanie w Prywatnej Chmurze (z Security Server) z awaryjnym Skanowaniem Hybrydowym (Lekkie Silniki) dla fizycznych komputerów o niskiej wydajności sprzętu.
     - Lokalne Skanowanie (z Pełnymi Silnikami) na fizycznych komputerach z wysokimi wymaganiami sprzętowymi.
     - Centralne Skanowanie w Prywatnej Chmurze (z Security Server)z awaryjnym Skanowaniem Hybrydowym (z Lekkimi Silnikami) dla maszyn wirtualnych. Sprawa ta wymaga co najmniej jednego wdrożonego Security Server w sieci.
     - Centralne Skanowanie w Prywatnej Chmurze (Security Server)z awaryjnym Skanowaniem Hybrydowym (z Lekkimi Silnikami) dla EC2. W tym przypadku, instancje EC2 automatycznie połączą się z Security Server Bitdefender hostowanym w odpowiednim regionie AWS.

Notatka
Zaleca się korzystanie z domyślnych trybów skanowania dla instancji EC2, ponieważ są one specjalnie zaprojektowane dla małych footprint'ów i niskiego zużycia zasobów.

- **Użytkownika**. W tym przypadku, można skonfigurować tryb skanowania, wybierając spośród kilku technologii skanowania dla maszyn fizycznych i wirtualnych:
  - Centralne Skanowanie w Chmurze Prywatnej (z Security Server)
  - Hybrydowe Skanowanie (z Lekkimi Silnikami)
  - Lokalne Skanowanie (z Pełnymi Silnikami)
  - Centralne Skanowanie w Prywatnej Chmurze (z Security Server)z awaryjnym* Skanowaniem Hybrydowym (z Lekkimi Silnikami)
  - Centralne Skanowanie w Prywatnej Chmurze (z Security Server)z awaryjnym* Skanowaniem Lokalnym (z Pełnymi Silnikami)

  Dla instancji EC2, można wybrać pomiędzy następującymi trybami niestandardowego skanowania:
  - Centralne Skanowanie w Prywatnej Chmurze (z Security Server)z awaryjnym* Skanowaniem Hybrydowym (z Lekkimi Silnikami)
  - Centralne Skanowanie w Prywatnej Chmurze (Security Server)z awaryjnym* Skanowaniem Lokalnym (z Pełnymi Silnikami)

  * Podczas wykorzystania podwójnego silnika skanowania, gdy pierwszy silnik jest niedostępny, zostanie użyty silnik awaryjny. Zużycie zasobów oraz wykorzystanie sieci będzie bazowało względnie do użytych silników.

  Aby uzyskać więcej informacji na temat dostępnych technologii skanowania, zapoznaj się z „Silniki Skanowania" (p. 4)

Ostrzeżenie

9. **Przyporządkowanie Security Server**.

   Podczas dostosowywania silników lokalnego skanowania sieci przy użyciu Private Cloud (Security Server), musimy wybrać lokalnie zainstalowane serwery ochrony, które chcemy wykorzystać i skonfigurować ich priorytetowanie w sekcji **Przypisane Security Server**:

- Kliknij listę Security Server w nagłówku tabeli. Wyświetlono listę wykrytych Security Server.
- Wybierz jednostkę.
- Naciśnij przycisk ⊕ **Dodaj** z nagłówka kolumny **Akcje**.

  Security Server został dodany do listy.
- Zrób te same kroki, aby dodać kilka serwerów bezpieczeństwa, jeżeli jest to możliwe. W tym przypadku, możesz skonfigurować priorytet używając strzałek ⌃ góra i ⌄ dół dostępnych po prawej stronie każdego wpisu. Gdy pierwszy Security Server nie jest dostępny, następny zostanie wykorzystany i tak dalej.
- Aby usunąć wpis z listy, naciśnij przycisk ⊗ **Usuń** w górnej części tabeli.

Możesz wybrać opcję szyfrowania połączenia z Security Server wybierając opcję **Użyj SSL**.

Dla instancji EC2, hostowany w odpowiednim regionie Security Server Bitdefender jest automatycznie przypisywany, tak by nie było konieczności konfigurowania sekcji **Przypisanie Security Server**.

10. Wybierz **Skanuj przed instalacją** jeżeli chcesz się upewnić, że maszyny są czyste przed instalacją na nich klienta. Szybkie skanowanie w chmurze zostanie przeprowadzone na docelowych maszynach przed rozpoczęciem instalacji.
11. Na punktach końcowych Windows, Bitdefender Endpoint Security Tools jest zainstalowany w domyślnym katalogu instalacyjnym. Wybierz **Użyj niestandardowej ścieżki instalacyjnej** jeżeli chcesz zainstalować Bitdefender Endpoint Security Tools w innej lokalizacji. W tym przypadku, podaj ścieżkę docelową w odpowiednim polu. Użyj konwencji Windows podczas wprowadzania ścieżki (np. `D:\folder`). Jeżeli folder docelowy nie istnieje, zostanie stworzony podczas instalacji.
12. Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.
13. Jeśli docelowe punkty końcowe są w Inwentaryzacji Sieci w **Grupy Niestandardowe**, możesz wybrać, aby przenieść je do określonego folderu od razu po zakończeniu wdrażania agenta bezpieczeństwa.

    Zaznacz **Użyj foldera niestandardowego** i wybierz folder w odpowiedniej tabeli.

14. W sekcji **Wdrożeniowiec**, wybierz podmiot, do którego będzie podłączony docelowy punkt końcowy do instalacji i aktualizacji klienta:
    - **Bitdefender Cloud**, jeśli chcesz aktualizować klientów bezpośrednio z Internetu.:

      W tym przypadku, można również zdefiniować ustawienia serwera proxy, jeśli docelowe punkty końcowe są połączone z Internetem za pośrednictwem serwera proxy. Wybierz **Użyj proxy do komunikacji** i wprowadź wymagane ustawienia proxy w polach poniżej.
    - **Endpoint Security Relay**, jeśli chcesz połączyć punkty końcowe z zainstalowanym w Twojej sieci klientem relay. Wszystkie maszyny z rolą relay wykryte w Twojej sieci pokażą się w tabeli poniżej. Wybierz maszynę relay, którą chcesz. Połączone punkty końcowe będą komunikować się z Control Center tylko przez określonego relay.

      WAŻNE
      Port 7074 musi być otwarty dla wdrożeń przez Bitdefender Endpoint Security Tools Relay do pracy.

15. Kliknij **Zapisz**.

Nowoutworzony pakiet zostanie dodany do listy pakietów.

Notatka
Ustawienia skonfigurowane w ramach pakietu instalacyjnego będą stosowane do punktów końcowych natychmiast po instalacji. Tak szybko, jak polityka jest stosowana do klienta, ustawienia skonfigurowane w ramach polityki będą egzekwowane, zastępując niektóre ustawienia pakietu instalacyjnego (takie jak serwery komunikacyjne lub ustawienia proxy).

Pobieranie pakietów instalacyjnych

Aby pobrać pakiety instalacyjne agentów bezpieczeństwa:

1. Zaloguj się do Control Center z punktu końcowego, na którym chcesz zainstalować ochronę.
2. Przejdź do strony **Sieć > Pakiety**.
3. Wybierz pakiety instalacyjne , które chcesz pobrać.
4. Naciśnij przycisk **Pobierz** w górnej części tabeli i wybierz typ instalacji, który chcesz. Dwa typy plików instalacyjnych są dostępne.

- **Pobieranie**. Downloader najpierw pobiera pełny zestaw instalacyjny z serwerów w chmurze Bitdefender, a następnie rozpoczyna instalacje. Plik ma mały rozmiar i może być uruchomiony w systemach 32-bit i 64-bit (co czyni to łatwym w dystrybucji). Z drugiej strony, wymaga aktywnego połączenia z Internetem.
- **Pełen Zestaw**. Pełne zestawy instalacyjne są większe i muszą być uruchomione na odpowiedniej wersji systemu operacyjnego.

  Pełny zestaw jest używany do instalacji ochrony na punktach końcowych z wolnym łączem lub brakiem połączenia z Internetem. Pobierz ten plik na połączony z Internetem punkt końcowy, następnie rozprowadź go na innych punktach końcowych używając zewnętrznych nośników pamięci lub udostępniając w sieci.

  Notatka
  Dostępne pełne wersje narzędzi:
  - **Windows OS:** systemy 32-bit i 64-bit
  - **System Operacyjny Linux:** dla systemów 32-bit i 64-bit
  - **Mac OS X:** tylko systemy 64-bit

  Upewnij się, że instalujesz poprawną dla systemu wersję.

5. Zapisz plik na punkcie końcowym.

Ostrzeżenie
Nie należy zmieniać nazwy wykonywalnego pliku downloadera, w przeciwnym wypadku nie będzie on w stanie porać plików instalacyjnych z serwera Bitdefender.

Wyślij linki do pobrania pakietów instalacyjnych w wiadomości e-mail.

Możesz potrzebować szybko poinformować innych użytkowników o dostępności pakietów instalacyjnych do pobrania. W tym przypadku, wykonaj kroki opisane poniżej:

1. Przejdź do strony **Sieć > Pakiety**.
2. Wybierz pakiety instalacyjne, które potrzebujesz.
3. Kliknij przycisk **Wyślij linki pobierania** z górnej strony tabeli. Wyświetlone zostanie okno konfiguracji.

4. Wpisz adres e-mail dla każdego użytkownika, który chce otrzymać link do pobrania pakietu instalacyjnego. Naciśnij `Enter` po każdym adresu e-mail.

   Upewnij się, że każdy wpisany adres e-mail jest prawidłowy.
5. Jeżeli chcesz zobaczyć linki pobierania przed wysłaniem ich w wiadomości e-mail, naciśnij na przycisk **Linki instalacyjne**.
6. Kliknij **Wyślij**. E-mail zawierający link instalacyjny jest wysyłany do każdego podanego adresu e-mail.

Uruchamianie Pakietów Instalacyjnych

Aby instalacja została uruchomiona, pakiet instalacyjny musi być uruchamiany przy użyciu uprawnień administratora.

Pakiet instaluje się inaczej na każdym systemie operacyjnym, jak następuje:

- Na systemach operacyjnych Windows i MAC:
  1. Na docelowy punkt końcowy, pobierz plik instalacyjny z Control Center lub skopiuj go z udziału sieciowego.
  2. Jeżeli pobrałeś pełny zestaw, wyodrębnij pliki z archiwum.
  3. Uruchom plik wykonywalny.
  4. Postępuj według instrukcji na ekranie.
- Na systemach operacyjnych Linux:
  1. Połącz się i zaloguj do Control Center.
  2. Pobierz lub kopiuj plik instalacyjny do docelowego punktu końcowego.
  3. Jeżeli pobrałeś pełny zestaw, wyodrębnij pliki z archiwum.
  4. Uzyskaj uprawnienia roota przez uruchomienie polecenia `sudo su`.
  5. Zmień uprawnienia do pliku instalacyjnego, aby można było go wykonać:

     ```
     # chmod +x installer
     ```

  6. Uruchom plik instalacyjny:

     ```
     # ./installer
     ```

7. Aby sprawdzić, czy agent został zainstalowany na punkcie końcowym, uruchom polecenie:

```
$ service bd status
```

Gdy agent bezpieczeństwa zostanie zainstalowany, punkt końcowy pokaże się w zarządzaniu w Control Center (Strona **Sieć**) w ciągu kilku minut.

Instalacja Zdalna

Control Center dopuszcza zdalną instalację agenta bezpieczeństwa na punktach końcowych wykrytych w sieci przez użycie zadań instalacji.

Kiedy już zainstalowano lokalnie pierwszego klienta z rolą relay, może upłynąć kilka minut, zanim reszta punktów końcowych sieci, stanie się widoczna w Control Center. Od tego momentu, możesz zdalnie zainstalować agenta bezpieczeństwa na punktach końcowych zarządzanych przez Ciebie przy użyciu zadania instalacji z Control Center.

Bitdefender Endpoint Security Tools zawiera mechanizm automatycznego wykrywania sieci, która umożliwia wykrywanie innych punktów końcowych, w tej samej sieci. Wykryte punkty końcowe są wyświetlane jako **niezarządzane** na stronie **Sieci**.

Wymagania zdalnej instalacji

Aby zdalna instalacja działała:

- Bitdefender Endpoint Security Tools Relay musi być zainstalowany w Twojej sieci.
- Każdy docelowy punkt końcowy musi pozwolić na zdalne połączenie, jak opisano tutaj:
  - Na systemach operacyjnych Windows: `admin$` udziały administracyjne muszą być włączone. Skonfiguruj każdą docelową stacje roboczą do używania zaawansowanej wymiany plików.
  - Na systemach operacyjnych Linux: SSH musi być włączone.
  - Na systamach operacyjnych MAC: zdalne logowanie musi być włączone.
- Tymczasowo wyłącz Kontrolę Konta użytkownika na wszystkich punktach końcowych z systemami operacyjnymi Windows, które zawierają tej funkcji

zabezpieczeń (Windows Vista, Windows 7, Windows Server 2008, itp.). Jeśli punkty końcowe wchodzą w skład domeny, za pomocą polityki możesz zdalnie wyłączyć Kontrolę Użytkownika.

- Wyłącz lub zamknij zaporę sieciową na punktach końcowych. Jeśli punkty końcowe wchodzą w skład domeny, za pomocą polityki możesz wyłączyć zdalnie zaporę sieciową Windows.

Uruchamianie Zadania Zdalnej Instalacji

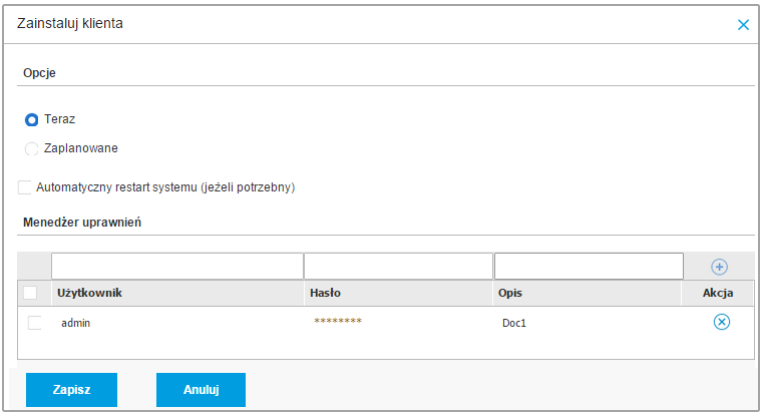
Aby uruchomić zdalną instalacje:

1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć**.
3. Wybierz żądaną grupę z lewego panelu bocznego. Jednostki należące do wybranej grupy są wyświetlone w prawym panelu bocznym tabeli.

   Notatka
   Opcjonalnie, możesz zastosować filtry, aby wyświetlić tylko punkty końcowe niezarządzane. Naciśnij menu **Filtry** i wybierz poniższe opcje: **Niezarządzane** z zakładki **Bezpieczeństwo** i **Wszystkie elementy rekurencyjnie** z zakładki **Głębokość**.
   Gdy pracując z instancjami EC2, można również dodać opcję **Instancja EC2** w zakładce **Typ** podczas zastosowywania wszystkich innych wspomnianych wcześniej kryteriów.

4. Wybierz wpisy (punkty końcowe lub grupy punktów końcowych), na których chcesz zainstalować ochronę.
5. Kliknij przycisk **Zadanie** z górnej strony tabeli i wybierz **Instaluj**.

   Kreator **Klienta Instalacji** został wyświetlony.



Instalowanie Bitdefender Endpoint Security Tools z menu zadań

6. W sekcji **Opcje** skonfiguruj czas instalacji:
   - **Teraz**, aby rozpocząć wdrożenie natychmiast.
   - **Zaplanowane**, aby ustawić przedział czasu na rozpoczęcie wdrożenia. W tym przypadku, wybierz przedział czasu jaki chcesz (godziny, dni lub tygodnie) i skonfiguruj go tak jak potrzebujesz.

   Notatka
   Na przykład, gdy określone operacje są wymagane na maszynach docelowych przed instalowaniem klienta (takie jak odinstalowanie innego oprogramowania albo ponowne uruchomienie systemu), możesz zaplanować zadanie wdrożenia aby uruchamiało się co 2 godziny. Zadanie rozpocznie się dla każdej maszyny docelowej w ciągu 2 godzin od udanego wdrożenia.

7. Jeśli chcesz, by docelowe punkty końcowe samoczynnie się uruchamiały, aby zakończyć instalację, wybierz **Automatyczny restart (w razie potrzeby)**.
8. W sekcji **Menadżer poświadczeń**, wybierz poświadczenia administracyjne potrzebne do zdalnego uwierzytelnienia na docelowych punktach końcowych. Możesz dodać poświadczenia wprowadzając użytkownika i hasło dla każdego docelowego systemu operacyjnego. Dla systemów Linux możesz również użyć klucza prywatnego zamiast hasła.

WAŻNE
Dla Windows 8.1 musisz podać poświadczenia wbudowanego konta administratora lub konta administratora domeny. Aby nauczyć się więcej, odwołaj się do tego artykułu KB.

Aby dodać wymagane poświadczenia OS:

a. Wprowadź nazwę użytkownika konta administratora w odpowiednie pola z nagłówka tabeli.

   Użyj konwencji systemu Windows podczas wprowadzania nazwy konta użytkownika domeny np. `user@domain.com` lub `domain\user`. Aby upewnić się, że podane poświadczenia będę działać, dodaj je w obu formach (`user@domain.com` i `domain\user`).

   Notatka
   Jeżeli komputery są w domenie, wystarczy wprowadzić poświadczenia administratora domeny.
   Użyj konwencji systemu Windows podczas wprowadzania nazwy konta użytkownika domeny np. `user@domain.com` lub `domain\user`. Aby upewnić się, że podane poświadczenia będę działać, dodaj je w obu formach (`user@domain.com` i `domain\user`).

b. Wybierz rodzaj uwierzytelniania z menu:
   - **Hasło**, aby użyć hasła administratora.
   - **Załaduj plik .pem**, aby użyć prywatnego klucza.

c. Jeśli uwierzytelniasz za pomocą hasła, wprowadź hasło w polu obok menu.

d. Jeśli uwierzytelniasz za pomocą prywatnego klucza, kliknij przycisk **Przeglądaj** i wybierz plik `.pem` zawierający odpowiedni klucz prywatny.

e. Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto.

f. Kliknij przycisk ⊕ **Dodaj** . Konto jest dodane do listy poświadczeń.

   Notatka
   Określone poświadczenia, zostaną automatycznie zapisane w Menadżer Poświadczeń tak, by nie trzeba było wprowadzać ich następnym razem. Aby uzyskać dostęp do Menedżera Poświadczeń wskaż tylko swoją nazwę użytkownika w prawym górnym rogu konsoli.

WAŻNE
Jeżeli dostarczone poświadczenia są nieważne, instalacja klienta nie powiedzie się na odpowiednich punktach końcowych. Upewnij się, że zaktualizowałeś wprowadzone poświadczenia OS w Menedżerze Poświadczeń, gdy są one zmieniane na docelowych punktach końcowych.

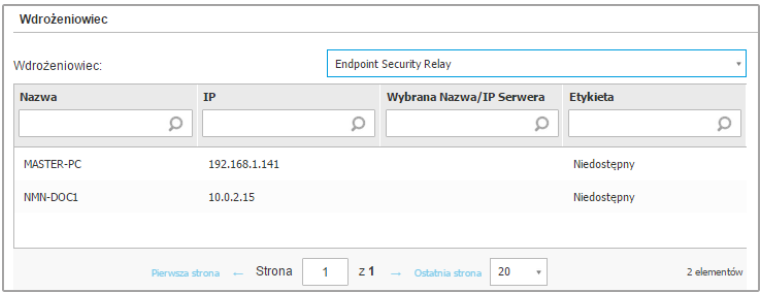
9. Zaznacz pola odpowiadające kontom, które chcesz używać.

Notatka
Ostrzeżenie jest wyświetlane tak długo jak nie wybierzesz żadnych poświadczeń. Ten krok jest obowiązkowy, aby zdalnie zainstalować agenta bezpieczeństwa na punktach końcowych.

10. W sekcji **Wdrożeniowiec**, skonfiguruj relay, do którego będzie podłączony docelowy punkt końcowy do instalacji i aktualizacji klienta:

- Wszystkie maszyny z rolą relay wykryte w twojej sieci pokażą się w tabeli **Relay Endpoint Security**. Każdy nowy klient musi być połączony z przynajmniej jednym klientem relay z tej samej sieci, który będzie służyć do komunikacji i aktualizacji serwera. Wybierz relay, który chcesz połączyć z docelowym punktem końcowym. Połączone punkty końcowe będą komunikować się z Control Center tylko przez określonego relay.

WAŻNE
Port 7074 musi być otwarty dla wdrożenia poprzez agenta relay aby mógł działać.



- Jeżeli docelowy punkt końcowy komunikuje się z agentem relay poprzez proxy, musisz również zdefiniować ustawienia proxy. W tym przypadku, wybierz **Użyj proxy do komunikacji** i wprowadź wymagane ustawienia proxy w polach poniżej.

11. Musisz wybrać jeden pakiet instalacyjny dla aktualnego wdrożenia. Kliknij listę **Użyj pakietu** i wybierz pakiet instalacyjny, który chcesz. Można tu znaleźć wszystkie pakiety instalacyjne wcześniej utworzone dla Twojego konta, a także domyślny pakiet instalacyjny dostępny z Control Center.
12. Jeśli to potrzebne, można zmienić niektóre ustawienia wybranego pakietu instalacyjnego, klikając przycisk **Dostosuj** obok pola **Użycie pakietu**.

    Ustawienia pakietu instalacyjnego pojawią się poniżej i możesz wprowadzić zmiany, które potrzebujesz. Aby dowiedzieć się więcej o edycji pakietów instalacyjnych, patrz „Tworzenie pakietów instalacyjnych" (p. 31).

    Jeśli chcesz zapisać zmiany jako nowy pakiet, wybierz opcję **Zapisz jako pakiet** umieszczoną na dole listy ustawień pakietów, a następnie wpisz nazwę dla nowego pakietu instalacyjnego.
13. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

Możesz zobaczyć i zarządzać zadaniem na stronie **Sieć > Zadania**.

Wsparcie dla skanowania zależnego od dostępu w Wirtualnych maszynach Linux

Wersja Bitdefender Endpoint Security Tools dla Linux zawiera możliwości skanowania dostępowego, które pracują z określoną dystrybucją Linux i wersjami jądra. Sprawdź wymagania systemu aby zweryfikować skanowanie zależne od dostępu, funkcjonujące na maszynie Linux. Następnie musisz nauczyć się jak ręcznie skompilować moduł DazukoFS.

Ręcznie skompiluj moduł DazukoFS.

Postępuj według poniższych kroków aby skompilować DazukoFS dla wersji jądra systemy i załaduj moduły:

1. Pobierz odpowiednie nagłówki jądra.
   - W systemie **Ubuntu**, uruchom komendę:

```
$ sudo apt-get install linux-headers-'uname -r'
```

- W systemach **UbuntuRHEL/CentOS**, uruchom komendę:

```
$ sudo yum install kernel-devel kernel-headers-'uname -r'
```

2. W systemach **Ubuntu**. potrzebujesz `build-essential`:

```
$ sudo apt-get install build-essential
```

3. kopiuj i wyodrębnij kod źródłowy DazukoFS w wybranym katalogu:

```
# mkdir temp
# cd temp
# cp /opt/BitDefender/share/src/dazukofs-source.tar.gz
# tar -xzvf dazukofs-source.tar.gz
# cd dazukofs-3.1.4
```

4. Skompiluj moduł:

```
# make
```

5. Zainstaluj i załaduj moduł:

```
# make dazukofs_install
```

Wymagania dotyczące korzystania ze skanowania dostępowego z DazukoFS

Aby DazukoFS i skanowaniu zależne od dostępu mogły razem pracować musi być spełniony szereg warunków. Proszę sprawdzić, czy którekolwiek z oświadczeń poniżej stosuje się do systemu Linux i postępuj zgodnie ze wskazówkami, aby uniknąć problemów.

- polityka SELinux musi być włączona i ustawiona na **zezwolono**. Sprawdź i dopasuj ustawienia polityki SELinux, edytując plik `/etc/selinux/config`.
- Bitdefender Endpoint Security Tools jest wyłącznie zgodny z wersją DazukoFS zawartą w pakiecie instalacyjnym. Jeżeli DazukoFS jest zainstalowany w systemie, usuń go przed instalacja Bitdefender Endpoint Security Tools.

- DazukoFS wspiera niektóre wersje jądra. Jeżeli pakiety DazukoFS dostarczone z Bitdefender Endpoint Security Tools nie są kompatybilne z wersją jądra systemu, moduł się nie załaduje. W danym przypadku, możesz zaktualizować jądro do obsługiwanej wersji lub przekompilować moduł DazukoFS do twojej wersji jądra. Możesz znaleźć pakiet DazukoFS w katalogu instalacyjnym Bitdefender Endpoint Security Tools:

  `/opt/BitDefender/share/modules/dazukofs/dazukofs-modules.tar.gz`

- Kiedy udostępniasz pliki używając dedykowanych serwerów takich jak NFS, UNFSv3 lub Samba, musisz uruchomić usługi w poniższej kolejności:

  1. Włącz skanowanie na wejściu przy pomocy polityki z Control Center.

     Aby uzyskać więcej informacji, zapoznaj się z Podręcznikiem Administratora GravityZone.

  2. Uruchom usługę udostępniania w sieci.

     Dla NFS:

     ```
     # service nfs start
     ```

     Dla UNFSv3:

     ```
     # service unfs3 start
     ```

     Dla Samba:

     ```
     # service smbd start
     ```

WAŻNE
Dla usługi NFS, DazukoFS jest kompatybilny tylko z Użytkownikiem Serwera NFS.

Jak działa wyszukiwanie sieci

Security for Endpoints zawiera mechanizm automatycznego wykrywania sieci przeznaczonej do wykrywania komputerów grupy roboczej.

Security for Endpoints opiera się na **Usłudze Microsoft Computer Browser** do wyszukiwania sieci. Usługa przeglądania komputera jest technologia sieciową,

która jest używana przez komputery z systemem operacyjnym Windows do aktualizacji listy domen, grup roboczych i komputerów w ich obrębie i dostarcza te listy do komputerów klienta na żądanie. Komputery wykryte w sieci przez usługę przeglądania komputerów można zobaczyć uruchamiając komendę **zobacz sieć** w oknie wiersza poleceń.

Polecenie zobacz sieć

Aby włączyć wyszukiwanie sieci, musisz mieć zainstalowany Bitdefender Endpoint Security Tools przynajmniej na jednym komputerze w sieci. Ten komputer będzie używany do skanowania sieci.

WAŻNE

Control Center nie używa informacji sieciowych z Active Directory ani z funkcji mapy sieci dostępnej w Windows Vista i późniejszych. Mapa sieci zależy od innych technologi wykrywania sieci: protokołu Link Layer Topology Discovery (LLTD).

Control Center nie jest aktywnie zaangażowany w operację serwisową Computer Browser. Bitdefender Endpoint Security Tools wysyła jedynie zapytanie do usługi Computer Browser w celu uzyskania listy stacji roboczych i serwerów widocznych aktualnie w sieci (znanych jako lista przeglądania) następnie wysyła je do Control Center. Control Center przetwarza listy przeglądania, dołączając nowo wykryte komputery do listy **Niezarządzane Komputery**. Wcześniej wykryte komputery nie są usunięte po ponownym zapytaniu wykrywania sieci, musisz wyłączyć & ręcznie; usuń komputery, które nie są już w sieci.

Początkowe zapytanie na liście przeglądania przeprowadzane jest po raz pierwszy podczas instalacji Bitdefender Endpoint Security Tools w sieci.

- Jeżeli Bitdefender Endpoint Security Tools jest zainstalowany na komputerze grupy roboczej, tylko komputery z grupy roboczej będą widoczne w Control Center.

- Jeżeli Bitdefender Endpoint Security Tools jest zainstalowany na komputerze domeny, tylko komputery z domeny będą widoczne w Control Center. Komputery z innej domeny zostaną wykryte jeżeli mają zaufane połączenie z domeną, na której jest zainstalowany Bitdefender Endpoint Security Tools.

Kolejne pytania wyszukiwania sieci są wykonywane regularnie co godzinę. Dla każdego nowego zapytania, Control Center dzieli zarządzanie przestrzenią komputerów w widocznym obszarze i następnie wyznacza jeden Bitdefender Endpoint Security Tools w każdym obszarze, aby wykonać zadanie. Widocznym obszarem jest grupa komputerów, które wykrywają siebie nawzajem. Zazwyczaj, widoczny obszar jest definiowany przez grupę robocza lub domenę, ale to zależy od topologii sieci i konfiguracji. W niektórych przypadkach, widoczność obszaru może zależeć od wielu domen i grup roboczych.

Jeżeli wybrany Bitdefender Endpoint Security Tools wyświetli błąd podczas wykonywania zapytania, Control Center poczeka do następnego zaplanowanego zapytania, aby spróbować ponownie, bez wybierania innego Bitdefender Endpoint Security Tools.

Dla pełnej widoczności sieci Bitdefender Endpoint Security Tools musi być zainstalowany na przynajmniej jednym komputerze każdej grupy roboczej lub domeny w twojej sieci. W idealnym przypadku Bitdefender Endpoint Security Tools powinien być zainstalowany co najmniej na jednym komputerze w każdej podsieci.

Więcej o usłudze przeglądania komputerów Microsoft

Szybka charakterystyka usługi przeglądania komputerów:

- Działa niezależnie od usługi Active Directory.
- Działa wyłącznie w sieci IPv4 i działa niezależnie w granicach grupy LAN (grupy roboczej lub domeny). Przeglądanie listy jest opracowane i utrzymywane dla każdej grupy LAN.
- Zazwyczaj używa bezpołączeniowych transmisji Serwera do komunikacji między węzłami.
- Używa NetBIOS nad TCP/IP (NetBT).
- Wymaga nazwy rozdzielczości NetBIOS. Jest zalecane posiadanie infrastruktury Windows Internet Name Service (WINS) i działanie w sieci.
- Domyślnie nie jest włączone w Windows Serwer 2008 i 2008 R2.

Dla szczegółowych informacji usługa Przeglądania Komputera, sprawdź Dane Techniczne usługi Przeglądania komputerów w Microsoft Technet.

Wymagania wyszukiwania sieci

Aby poprawnie wykryć wszystkie komputery (serwery i stacje robocze) które będą zarządzane przez Control Center, wymagane są:

- Komputery muszą być przyłączone do grupy roboczej lub domeny i połączone przez lokalną sieć IPv4. Usługa Przeglądarki komputerowej nie działa w sieci IPv6.
- Kilka komputerów w każdej grupie LAM (stacje robocze lub domeny) muszą uruchamiać usługę Przeglądarki Komputerów. Podstawowe kontrolery domeny muszą również uruchomić usługę.
- NetBIOS nad TCP/IP (NetBT) musi być włączony na komputerach. Lokalny firewall musi dopuszczać ruch NetBT.
- Udostępnianie plików musi być włączone na komputerach. Lokalny firewall musi dopuszczać udostępnianie plików.
- Infrastruktura Windows Internet Name Service (WINS) musi zostać ustawiona i działać poprawnie.
- Dla Windows Vista lub wyższych wersji, wykrywanie sieci musi być włączone (**Panel Kontrolny > Centrum Wykrywania i Udostępniania > Zmień Zaawansowane Ustawienia udostępniania**).

  Aby móc włączyć tę funkcję, musisz najpierw uruchomić poniższe usługi:
  - Klient DNS
  - Funkcja wykrywania zasobów publikacji
  - Wykrywanie SSDP
  - Host UPnP Urządzenia
- W środowiskach z wieloma domenami, jest rekomendowane aby ustawić zaufaną relację pomiędzy domenami, dzięki czemu komputery będą miały dostęp do przeglądania listy z innych domen.

Komputery, z których Bitdefender Endpoint Security Tools wysyła zapytania do usługi Przeglądarki Komputerowej muszą mieć możliwość rozpoznawania nazw NetBIOS.

Notatka
Mechanizm wyszukiwania sieci działa dla wszystkich obsługiwanych systemów operacyjnych, włączając wersję wbudowaną w Windows, pod warunkiem, że wymagania są spełnione.

3.3. Instalowanie Ochrony Exchange

Security for Exchange automatycznie integruje się z Serwerami Exchange, w zależności od roli serwera. Dla każdej z ról tylko kompatybilne funkcje są instalowane, co opisano tutaj:

Funkcje	Microsoft Exchange 2016/2013		Microsoft Exchange 2010/2007		
	Krawędź	Skrzynka pocztowa	Krawędź	Hub	Skrzynka pocztowa
Poziom Transport					
Filtrowanie Antymalware	x	x	x	x	
Filtrowanie Antyspam	x	x	x	x	
Filtrowanie zawartości	x	x	x	x	
Filtrowanie załączników	x	x	x	x	
Exchange Store					
Skanowanie na żądanie przeciw malware		x			x

3.3.1. Przygotowywanie do Instalacji

Zanim zainstalujesz Security for Exchange, upewnij się, że wszystkie wymagania są spełnione, inaczej Bitdefender Endpoint Security Tools może zostać zainstalowany bez modułu ochrony Exchange.

Dla płynnego działania modułu Ochrony Exchange i zapobiegania konfliktom oraz niepożądanym efektom, usuń agentów antymalware i filtrowania wiadomości e-mail.

Bitdefender Endpoint Security Tools automatycznie wykrywa i usuwa większość produktów antymalware i wyłącza wbudowanego agenta antymalware w Exchange

Server od wersji 2013. Szczegółowe informacje dotyczące listy wykrytych oprogramowań zabezpieczających, patrz ten artykuł KB.

Możesz ręcznie ponownie włączyć wbudowanego agenta antymalware Exchange w dowolnym czasie, jednak nie jest to zalecane, aby to robić.

3.3.2. Instalowanie Ochrony na Serwerach Exchange

Aby chronić swoje Serwery Exchange, musisz zainstalować Bitdefender Endpoint Security Tools z rolą Ochrona Exchange na każdym z nich.

Masz kilka opcji wdrożenia Bitdefender Endpoint Security Tools na Serwerach Exchange:

- Instalacja lokalna, przez pobranie i uruchomienie pakietu instalacyjnego na serwerze.
- Zdalna instalacja, uruchamiając zadanie **Zainstaluj**.
- Zdalnie, uruchamiając zadanie **Rekonfiguruj Klienta**, jeśli Bitdefender Endpoint Security Tools oferuje już ochronę systemu na serwerze.

Szczegółowe kroki instalacji, odwołaj się do „Instalowanie Agentów Bezpieczeństwa" (p. 28).

3.4. Menedżer uprawnień

Menadżer Poświadczeń pomaga zdefiniować poświadczenia wymagane dla zdalnego uwierzytelniania na różnych systemach operacyjnych w twojej sieci.

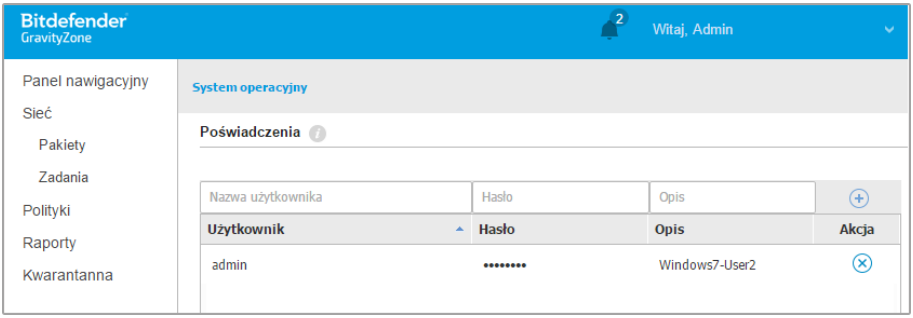
Aby otworzyć Menadżera Poświadczeń, kliknij nazwę użytkownika w górnym prawym rogu strony i wybierz **Menadżer Poświadczeń**.

Menu menadżera poświadczeń

3.4.1. Dodaj Poświadczenia to Menadżera Poświadczeń

Za poocą Menadżera Poświadczeń możesz zarządzać poświadczeniami administratora wymaganymi do zdalnego uwierzytelniania podczas instalacji zadań wysyłanych do komputerów i maszyn wirtualnych w twojej sieci.

Aby dodać zestaw poświadczeń:



Menedżer uprawnień

1. Wprowadź nazwę użytkownika i hasło konta administratora dla każdego docelowego systemu operacyjnego w odpowiednim polu z górnej strony nagłówka tabeli. Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto. Jeżeli komputery są w domenie, wystarczy wprowadzić poświadczenia administratora domeny.

   Użyj konwencji Windows podczas wprowadzania nazwy użytkownika konta

   - Dla maszyn Active Directory użyj tych składni: `username@domain.com` i `domain\username`. Aby upewnić się że wprowadzone poświadczenia będą działać, dodaj je w obu formach (`username@domain.com` i `domain\username`).
   - Dla maszyn z grupy roboczej, wystarczy wprowadzić tylko nazwę użytkownika, bez nazwy grupy roboczej.

2. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli. Nowe ustawienia poświadczeń zostały dodane do tabeli.

Notatka
Jeżeli nie określiłeś poświadczeń uwierzytelniania, będziesz musiał podać je podczas uruchamiania zadania instalacyjnego. Określone poświadczenia, zostaną zapisane automatycznie w menadżerze poświadczeń, więc nie będziesz musiał wprowadzać ich ponownie następnym razem.

3.4.2. Usuwanie Poświadczeń z Menadżera Poświadczeń

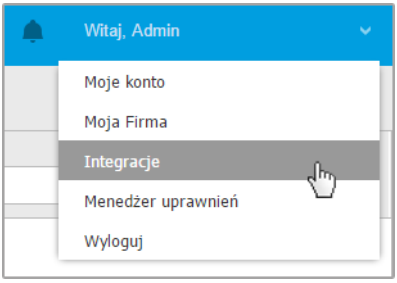
aby usunąć nieaktualne poświadczenia z Menadżera Poświadczeń:

1. Wskaż wiersz w tabeli zawierający dane uwierzytelniające, które chcesz usunąć.
2. Kliknij przycisk **Usuń** po prawej stronie odpowiedniego wiersza w tabeli. Wybrane konto zostanie usunięte.

4. INTEGRACJE

Jako klient Bitdefender używający Control Center w celu zarządzania bezpieczeństwem własnej firmy, posiadasz możliwość integracji Control Center z rozwiązaniami firm trzecich takich jak Amazon EC2 Services.

Możesz skonfigurować integrację rozwiązań firm trzecich na stronie **Integracje**, do której dostęp można uzyskać poprzez wskazanie swojej nawy użytkownika w prawym górnym rogu konsoli i wybierając **Integracje**.



4.1. Integracja z ConnectWise

Control Center stanowi specyficzną funkcjonalność integracji dla partnerów z kontami ConnectWise, umożliwiając sprawne monitorowanie usług bezpieczeństwa Bitdefender dostarczonych do firm klienckich za pośrednictwem platformy ConnectWise, na podstawie zautomatyzowanych procedur biletowych i rozliczeniowych.

Aby uzyskać pełne informacje na temat integracji GravityZone Control Center z ConnectWise, patrz Przewodnik Integracji ConnectWise.

4.2. Integracja z Usługami Amazon EC2

4.2.1. O Integracji Amazon EC2 w Control Center

Z Control Center GravityZone, administratorzy mają możliwość integracji z usłgą Amazon Elastic Compute Cloud (EC2) i centralne wdrożenie, zarządzanie i monitorowanie ochrony Bitdefender na przykładzie ich zasobów. Posiadane serwery skanowania są hostowane przez Bitdefender wewnątrz chmury AWS Cloud w celu zapewnienia optymalnego odcisku na chronionych przypadkach by wyeliminować

skanowanie napowietrznego występującego w tradycyjnym oprogramowaniu ochrony.

Bitdefender Control Center zarządza instancjami Amazon EC2 za pośrednictwem specjalnych funkcji, takich jak:

- Zintegrowany spis EC2 pogrupowany według regionów Amazon i Dostępności Stref.

  Po tym jak integracja Amazon EC2 została skonfigurowana, instancje Amazon należące do określonych poświadczeń konta użytkownika są importowane do Control Center w ramach inwentaryzacji sieci. Niestandardowa grupa **Amazon EC2** zostanie wyświetlona, zawierając wszystkie regiony Amazon i swoich stref dostępności, zawierających instancje.

  Można rozróżnić przypadki online i offline dzięki ich ikonom:

  – Instancje offline

  – Instancje online

- Specyficzne filtrowanie EC2 w widoku sieci:

  – Filtrowanie punktów końcowych wg typu instancji EC2

  – Filtrowanie punktów końcowych według tagów EC2 określone w konsoli zarządzania Amazon

  – Filtrowanie instancji EC2 po ich statusie (uruchomione, zatrzymane, zakończone)

- Automatyczne (domyślne) tryby skanowania dla instancji EC2 ustawianych na Central Scan przy użyciu Security Server Bitdefender gospodarowane w odpowiednim regionie AWS, w odwrocie Hybrydowego skanowania (z lekkimi silnikami używającymi skanowanie wewnątrz chmury i częściowe lokalne sygnatury).

Notatka

Zaleca się korzystanie z domyślnych trybów skanowania dla instancji EC2, ponieważ są one specjalnie zaprojektowane dla małych footprint'ów i niskiego zużycia zasobów.
Dla instancji z potężnymi zasobami, możesz również skonfigurować instancje EC2 w celu uruchomienia za pomocą Bitdefender Security Server prywatnego skanowania w chmurze wygospodarowanego w odpowiednim regionie AWS wraz z awaryjnym skanowaniem lokalnym (Pełne silniki wykorzystujące sygnatury i silniki przechowywane lokalnie).

- Grupowanie zakończonych instancji w określonym folderze drzewa sieci. Wcześniej zarządzane (chronione) instancje które zostały wyłączone z konsoli zarządzania Amazon, są przechowywane w grupie **Zakończonych Zarządzeń Instancji** znajdującej się w katalogu **Amazon EC2**. Nadal możesz uzyskać informacje o tych przypadkach za pośrednictwem raportów. Jeśli nie są już potrzebne, zakończone instancje mogą być usuwane z inwentaryzacji sieci.

4.2.2. Konfigurowanie Integracji Amazon EC2 w Control Center

Integracja Security for Amazon Web Services wymaga ID klucza dostępu oraz tajnego klucza dostępu twojego konta AWS lub AWS Zarządzania tożsamością i dostępem (IAM) użytkownika.

Aby skonfigurować Twoją integrację Amazon EC2:

1. Połącz się i zaloguj do Control Center.
2. Kliknij swoją nazwę użytkownika w górnym, prawym rogu konsoli i wybierz **Integracje**. Strona integracji pojawi się.
3. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli.
4. Kliknij link **Dodaj Integrację Amazon EC2**. Wyświetlone zostanie okno konfiguracji.
5. Wpisz klucze dostępu użytkowników Amazon w dostępnych polach.

   Notatka
   Zaleca się, aby skonfigurować integrację z kontem AWS za pomocą klucza dostępu z użytkownikiem IAM stworzonym specjalnie do tego celu.
   Twój użytkownik Amazon jest podłączony do dostarczonych list uwierzytelniających i musi posiadać przynajmniej możliwość samego odczytu w Amazon EC2.

6. Kliknij **Zapisz**.
7. Wyświetlana jest Umowa Licencyjna AWS. Musisz przeczytać i zgodzić się z warunkami licencji, aby móc kontynuować.
8. Control Center sprawdzi, czy dostarczone klucze AWS są ważne. Jeśli tak, Twoje instancje Amazon będą zaimportowane w Control Center i integracja zostanie wykonana.

   Od tego momentu, możesz przeglądać i zarządzać instancjami Amazon ze strony **Sieć** pod węzłem **Niestandardowe Grupy > Amazon EC2**. Tutaj instancje

Amazon EC2 są zgrupowane w swoich regionach Amazon i odpowiadających im Strefach Dostępności. Control Center automatycznie synchronizuje się z inwentaryzacją Amazon EC2 co 15 minut. Możesz również ręcznie zsynchronizować z inwentaryzacją Amazon za pomocą przycisku **Synchronizuj z Amazon EC2** umieszczonego w górnej części strony **Sieć**.

Jeżeli wprowadzone poświadczenia dostępu Amazon nie są ważne, zostaniesz o tym powiadomiony i poproszony o podanie ich ponownie.

4.2.3. Subskrybuj do Security for Amazon Web Services

Jako bezpośredni klient Bitdefender, możesz w każdej chwili skonfigurować swoje Security for Amazon Web Services na stronie **Integracja**.

Kiedy Integracja Amazon EC2 została skonfigurowana, możesz zacząć korzystać z tej usługi w trybie próbnym przez 30 dni. Otrzymasz e-mailem potwierdzenie Twojej 30-dniowej próbnej subskrypcji usług Amazon EC2. Podczas okresu próbnego, możesz mógł w pełni chronić i zarządzać każdą iloscią instancji wykorzystując usługę bezpieczeństwa dostępną wraz z GravityZone Control Center.

Jeśli chcesz nadal korzystać z tej usługi po okresie próbnym, musisz licencjonować swoją subskrypcję AWS autoryzując płatności do Bitdefender z konta Płatności Amazon. To jest operacja w jednym czasie w okresie ważności karty kredytowej i spełnia dwie funkcje: licencjonowanie subskrypcji AWS i autoryzacja płatności z kontem Płatności Amazon dla kolejnych miesięcznych rozliczeń.

Po licencjonowaniu subskrypcji AWS, będzie pobierana opłata miesięczna na podstawie użytkowania.

Ostrzeżenie
Jeżeli nie dokonasz zakupu subskrypcji po upływie okresu próbnego, twoje zarządzane instancje przestaną być ważne po upływie 30 dni od twojej ostatniej subskrypcji i nie będą one już więcej chronione.

Licencjonowanie Twojej Subskrypcji AWS

1. Zaloguj się do Control Center korzystając ze swojego konta.
2. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moja Firma**.
3. W sekcji **Subskrypcja AWS**, kliknij widget **Płać z Amazon**.

4. Będziesz przekierowany do strony **Logowanie Amazon**. Zaloguj się używając konta Płatności Amazon.

> **Notatka**
> Musisz skonfigurować przeglądarkę, żeby zaakceptować pliki cookies firm trzecich, aby widget Amazon zadziałał.

5. Konfiguruj swoje metody Płatności Amazon wybierając ważną kartę kredytową i włączyć opcję **Użyj wybranej metody płatności dla przyszłych zakupów i płatności dla tego sklepu**.
6. Kliknij **Zapisz**. Twoja subskrypcja AWS jest teraz **Licencjonowana**.

> **Notatka**
> Jeśli wybrana karta kredytowa wygasła, trzeba będzie ponownie licencjonować subskrypcję AWS, wykonując wyżej wymienione czynności.

Anulowanie Twojej Subskrypcji AWS

Możesz anulowac swoją subskrypcję AWS, w każdej chwili, bezpośrednio ze swojego konta firmowego Control Center. Kiedy anulujesz subskrypcję AWS:

- Wszystkie agenty bezpieczeństwa Bitdefender zainstalowane na Twoich instancjach wygasły i te instancje pozostały natychmiast bez ochrony.
- Autoryzacja płatności za subskrypcję na Płatnościach Amazon jest automatycznie anulowana. Jednakże, pobierana będzie opłata za bieżące miesięczne zużycie, aż do czasu, kiedy zrezygnujesz z subskrypcji.

Aby zrezygnować z subskrypcji:

1. Zaloguj się do Control Center korzystając ze swojego konta.
2. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moja Firma**.
3. W sekcji **Subskrypcja AWS**, kliknij przycisk **Anuluj Subskrypcję**.
4. Czynności należy potwierdzić, klikając **Tak**. Twoja subskrypcja AWS jest teraz **Anulowana**.

Możesz w każdej chwili ponownie subskrybować usługę, wykonując procedurę licencjonowania.

Edytowanie Twojej Subskrypcji AWS

1. Zaloguj się do Control Center korzystając ze swojego konta.
2. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moja Firma**.
3. W sekcji **Subskrypcja AWS**, kliknij widget **Płać z Amazon**.
4. Zaloguj się używając konta Płatności Amazon.
5. Wprowadź zmiany, które potrzebujesz.
6. Kliknij **Zapisz**.

Notatka
Po edycji subskrypcji AWS, otrzymasz dwa e-maile z Płatności Amazon, które potwierdzą anulowanie poprzedniej autoryzacji oraz ustawią nowy sposób płatności.

4.3. Usuwanie Integracji

Aby usunąć integrację już nie potrzebujesz:

1. Na stronie **Integracje**, zaznacz pole wyboru odpowiadające rozwiązaniu, którą chcesz usunąć.
2. Kliknij przycisk ⊖ **Usuń** w górnej części tabeli. Po zatwierdzeniu akcji, wybrana integracja zostanie usunięta z Control Center.

WAŻNE
Po usunięciu integracji, wszystkie twoje klienty zainstalowane na odpowiednich platformach wygasną, w znaczeniu, że przestaną komunikować się z Usługami Cloud Bitdefender i Control Center oraz zostaną usunięci z Control Center.

5. ODINSTALOWYWANIE OCHRONY

Możesz odinstalować i zainstalować komponenty GravityZone w takich przypadkach, gdy trzeba użyć klucza licencyjnego na innej maszynie, aby naprawić błędy lub podczas aktualizacji.

Aby poprawnie odinstalować ochronę Bitdefender z punktów końcowych w Twojej sieci, podążaj za opisanymi instrukcjami w tym rozdziale.

- Odinstalowywanie Ochrony Endpoint
- Odinstalowywanie Ochrony Exchange

5.1. Odinstalowywanie Ochrony Endpoint

Aby bezpiecznie usunąć ochronę Bitdefender, musisz najpierw odinstalować agenty bezpieczeństwa, a następnie Security Server, jeśli jest to potrzebne. Jeśli chcesz odinstalować tylko Security Server, upewnij się, że najpierw połączyłeś jego agenty do innego Security Server.

- Odinstalowywanie Agentów Bezpieczeństwa
- Odinstalowywanie Security Server

5.1.1. Odinstalowywanie Agentów Bezpieczeństwa

Masz dwie opcje na odinstalowanie agentów bezpieczeństwa:

- Zdalnie w Control Center
- Manualnie na maszynie docelowej

Ostrzeżenie
Agenty bezpieczeństwa i Serwery Bezpieczeństwa są niezbędne dla utrzymania punktów końcowych bezpiecznych przed wszelkiego rodzaju zagrożeniami, a tym samym ich odinstalowanie może umieścić całą sieć w niebezpieczeństwie.

Zdalne Odinstalowywanie

Aby zdalnie odinstalować ochronę Bitdefender z jakiegokolwiek zarządzanego punktu końcowego:

1. Przejdź do strony **Sieć**.

2. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie komputery z wybranego kontenera są wyświetlane w prawym panelu bocznym tabeli.
3. Zaznacz punkty końcowe, z których chcesz dokonać odinstalowania agenta bezpieczeństwa Bitdefender.
4. Kliknij **Zadania** w górnej części tabeli i wybierz **Odinstaluj klienta**. Wyświetlono okno konfiguracji.
5. W oknie zadania **Odinstaluj agenta** możesz wybrać czy zachować pliki poddane kwarantannie na punkcie końcowym czy je usunąć.
6. Naciśnij **Zapisz** aby utworzyć zadanie. Pojawia się wiadomość potwierdzająca.

Możesz zobaczyć i zarządzać zadaniem w **Sieć > Zadania**.

Jeśli chcesz przeinstalować agenty bezpieczeństwa, przejdź do „Instalowanie Ochrony Endpoint" (p. 24).

Deinstalacja Lokalna

Aby ręcznie odinstalować agenta bezpieczeństwa Bitdefender z maszyny Windows:

1. W zależności od Twojego systemu operacyjnego:
   - W Windows 7, idź do **Start > Panel Kontrolny > Odinstaluj program** w kategorii **Programy**.
   - W Windows 8, idź do **Ustawienia > Panel Kontrolny > Odinstaluj program** w kategorii **Program**.
   - W Windows 8.1, kliknij prawym przyciskiem myszy na przycisk **Start**, a następnie wybierz **Panel Kontrolny > Programy & funkcje**.
   - W Windows 10, idź do **Start > Ustawienia > System > Aplikacje & funkcje**.
2. Wybierz agenta Bitdefender z listy programów.
3. Kliknij **Odinstaluj**.
4. Wprowadź hasło Bitdefender, jeśli jest włączone w polityce bezpieczeństwa. Podczas deinstalacji, możesz zobaczyć postęp zadania.

Aby ręcznie odinstalować agenta bezpieczeństwa Bitdefender z maszyny Linux:

1. Otwórz terminal.
2. Zdobądź dostęp do roota poprzez komendy `su` lub `sudo su`

3. Nawigacja za pomocą polecenia `cd` do następującej ścieżki: `/opt/BitDefender/bin`
4. Uruchom skrypt:

```
# ./remove-sve-client
```

5. Wprowadź hasło Bitdefender, aby kontynuować, jeśli jest włączone w polityce bezpieczeństwa.

Aby manualnie odinstalować agenta Bitdefender z Mac:

1. PRzejdź do **Finder > Aplikacje**.
2. Otwórz folder Bitdefender.
3. Kliknij dwukrotnie **Bitdefender Mac Uninstall**.
4. W oknie potwierdzającym, kliknij oba **Sprawdź** i **Odinstaluj**, aby kontynuować.

Jeśli chcesz przeinstalować agenty bezpieczeństwa, przejdź do „Instalowanie Ochrony Endpoint" (p. 24).

5.1.2. Odinstalowywanie Security Server

Możesz odinstalować Security Server tak samo jak go zainstalowałeś, albo przez Control Center albo przez wiersz poleceń (CLI) wirtualnego interfejsu GravityZone.

Aby odinstalować Security Server w Control Center:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Wybierz centrum danych lub folder zawierający host na którym Security Server jest zainstalowany. Punkty końcowe są wyświetlane po prawej stronie panelu.
4. Zaznacz pole zawierające host na którym Security Server jest zainstalowany.
5. W menu **Zadania**, wybierz **Odinstaluj Security Server**.

Możesz zobaczyć i zarządzać zadaniem w **Sieć > Zadania**.

Kiedy Security Server jest zainstalowany na tym samym wirtualnym urządzeniu co role GravityZone, możesz go usunąć korzystając z wiersza poleceń tego urządzenia. Aby to zrobić:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).

   Użyj klawiszy strzałek i przycisku `Tab` do nawigacji w menu i opcjach. Naciśnij `Enter`, aby wybrać konkretną opcję.

2. W menu **Opcje Urządzenia**, idź do **Zaawansowane Ustawienia**.
3. Wybierz **Odinstaluj Serwer Bezpieczeństwa**. Okno potwierdzające jest wyświetlane.
4. Naciśnij klawisz `Y` lub naciśnij `Enter` mając wybraną opcję **Tak**, aby kontynuować. Poczekaj na zakończenie deinstalacji.

5.2. Odinstalowywanie Ochrony Exchange

Możesz usunąć Ochronę Exchange z jakiegokolwiek Serwera Microsoft Exchange mając Bitdefender Endpoint Security Tools z tą rolą zainstalowaną. Możesz wykonać odinstalowywanie w Control Center.

1. Przejdź do strony **Sieć**.
2. Wybierz pożądany kontener z lewego panelu bocznego. Wpisy będą wyświetlane po prawej stronie panelu tabeli.
3. Wybierz punkt końcowy, z którego chcesz odinstalować Ochronę Exchange.
4. Kliknij **Rekonfiguruj Klienta** w menu **Zadania**, w górnym panelu tabeli. Wyświetlono okno konfiguracji.
5. W sekcji **Ogólne** wyczyść pole wyboru **Ochrona Exchange**.

   Ostrzeżenie
   W oknie konfiguracji, upewnij się, że wybrałeś wszystkie inne role, które są aktywne na punkcie końcowym. W przeciwnym razie będą one także odinstalowane.

6. Naciśnij **Zapisz** aby utworzyć zadanie.

Możesz zobaczyć i zarządzać zadaniem w **Sieć > Zadania**.

Jeśli chcesz przeinstalować Ochronę Exchange, przejdź do „Instalowanie Ochrony Exchange" (p. 49).

6. OTRZYMYWANIE POMOCY

Bitdefender stara się zapewnić swoim klientom najwyższy poziom szybkiej i dokładnej pomocy technicznej. Jeżeli męczy cię jakiś problem lub masz pytania dotyczące produktu Bitdefender, przejdź do naszego Centrum Wsparcia Online. Oferuje kilka zasobów, które możesz użyć do szybkiego znalezienia rozwiązania lub odpowiedzi. Jeśli wolisz, możesz skontaktować się z Obsługą Klienta Bitdefender. Nasi przedstawiciele ds. pomocy technicznej szybko odpowiedzą na twoje pytania oraz zapewnią ci niezbędną pomoc.

Notatka
Możesz dowiedzieć się więcej na temat usług wsparcia jakie oferujemy i sposobów jej udzielania w Centrum pomocy.

6.1. Bitdefender Wsparcie Techniczne

Bitdefender Centrum Pomocy, to miejsce gdzie uzyskasz wszelką pomoc dla Twoich produktów Bitdefender.

Możesz użyć kilku źródeł, aby szybko znaleźć rozwiązanie problemu lub odpowiedź:

- Znana baza artykułów
- Bitdefender forum pomocy
- Dokumentacja produktu

Możesz również użyć ulubionej wyszukiwarki, aby znaleźć więcej informacji o ochronie komputera, produktach Bitdefender i firmie.

Znana baza artykułów

Bazą wiedzy Bitdefender jest dostępne w internecie repozytorium informacji na temat produktów Bitdefender produktów. Przechowuje czytelne raporty z trwających działań zespołu Bitdefender odnośnie pomocy technicznej i naprawiania błędów oraz bardziej ogólne artykuły dotyczące ochrony antywirusowej, szczegółowego zarządzania rozwiązaniami produktu Bitdefender oraz wielu innych zagadnień.

Baza wiedzy Bitdefender jest publiczna i bezpłatna. Informacje, które zawiera, stanowią kolejny sposób na dostarczenie klientom Bitdefender, potrzebnej wiedzy technicznej i wsparcia. Prawidłowe żądania informacji lub raportów o błędach, pochodzące od klientów Bitdefender, w końcu znajdują drogę do Bazy Wiedzy

Bitdefender. jako raporty informujące o poprawkach, sposoby ominięcia problemów czy pliki pomocy produktu i teksty informacyjne.

Baza Wiedzy Bitdefender dla produktów biznesowych jest dostepna w każdej chwili na http://bitdefender.pl/dla-biznesu/uzyteczne-linki/wsparcie-techniczne.

Bitdefender forum pomocy

Forum pomocy technicznej Bitdefender pozwala użytkownikom Bitdefender uzyskać pomoc oraz pomagać innym osobom korzystającym z produktu. Możesz tu opublikować dowolny problem lub pytanie dotyczące twoich produktów Bitdefender.

Pracownicy ds. pomocy technicznej Bitdefender monitorują forum sprawdzając nowe wpisy i zapewniając pomoc. Odpowiedź lub rozwiązanie można także uzyskać od bardziej zaawansowanego użytkownika programu Bitdefender.

Przed zamieszczeniem problemu lub pytania przeszukaj forum, w celu znalezienie podobnych lub powiązanych tematów.

Forum pomocy technicznej Bitdefender jest dostępne pod adresem http://forum.bitdefender.com w 5 językach: angielskim, niemieckim, francuskim, hiszpańskim i rumuńskim. Aby uzyskać dostęp do sekcji poświęconej produktom biznesowym, kliknij łącze **Ochrona dla biznesu**.

Dokumentacja produktu

Dokumentacja produktu jest najbardziej kompletnym źródłem informacji o produkcie.

Możesz sprawdzić i pobrać najnowszą wersję dokumentacji dla produktów firmy Bitdefender na Centrum pomocy, w sekcji **Dokumentacja** dostępnej na każdej stronie pomocy technicznej produktu.

6.2. Prośba o pomoc

Prosimy o kontakt w celu uzyskania pomocy za pośrednictwem naszego Centrum pomocy online:

1. Odwiedź serwis@marken.com.pl.
2. Skorzystaj z formularza kontaktowego, aby otworzyć pomoc e-mail lub uzyskać dostęp do innych dostępnych opcji kontaktu.

6.3. Używanie Narzędzi Pomocy

Narzędzie wsparcia GravityZone jest stworzone żeby pomagać użytkownikom i łatwo uzyskać potrzebne informacje ze wsparcia technicznego. Uruchom Narzędzie Wsparcia na zagrożonych komputerach i wyślij otrzymane archiwum z informacjami o problemach do wsparcia przedstawiciela Bitdefender.

6.3.1. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Windows

1. pobierz Narzędzie wsparcia i prześlij je do zagrożonych komputerów. Aby pobrać narzędzie wsparcia:
   a. Połącz się z Control Center używając twojego konta.
   b. Kliknij link **Pomoc i Wsparcie** w lewym dolnym rogu konsoli.
   c. Linki do pobrania są dostępne w sekcji **Wsparcie**. Dwie wersje są dostępne: jedna dla systemu 32-bit i druga dla systemu 64-bit. Upewnij się, że używasz odpowiedniej wersji gdy uruchamiasz Narzędzie wsparcia na komputerze.
2. Uruchom Narzędzie wsparcia lokalnie na każdym zarażonym komputerze.
   a. Zaznacz pole wyboru oznaczające zgodę, a następnie kliknij **„Dalej”**.
   b. Wypełnij pola formularza niezbędnymi danymi:
      i. Wpisz swój adres e-mail.
      ii. Podaj swoje imię.
      iii. Z odpowiedniego menu wybierz swój kraj.
      iv. Opisz problem, który napotkałeś.
      v. opcjonalnie, możesz spróbować odtworzyć problem przed rozpoczęciem zbierania danych. W tym przypadku, należy postępować w następujący sposób:
         A. Włącz opcje **Spróbuj odtworzyć problem przed wysłaniem**.
         B. Kliknij **Dalej**.
         C. Wybierz rodzaj napotkanego problemu.
         D. Kliknij **Dalej**.

E. Odtwórz problem na swoim komputerze. Kiedy zrobione, wróć do Narzędzi wsparcia i wybierz opcje **Powielanie problemu**.

c. Kliknij **Dalej**. Narzędzie pomocy zbiera informacje o produkcie, innych zainstalowanych aplikacjach oraz o konfiguracji sytemu (sprzętowej i programowej).

d. Poczekaj na zakończenie działania.

e. Aby zamknąć to okno, kliknij **Zakończ**. Archiwum plików zostało utworzone na twoim pulpicie.

   Wyślij archiwum zip razem z twoją prośbą do wsparcia przedstawiciela Bitdefender używając formularza pomocy technicznej dostępnego na stronie **Pomoc i Wsparcie** w konsoli.

6.3.2. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Linux

Dla systemów operacyjnych Linux, Narzędzie Wsparcia jest zintegrowane wraz z agentem bezpieczeństwa Bitdefender.

Aby zebrać informacje na temat systemu Linux przy pomocy Narzędzia Wsparcia, uruchom następujące polecenia:

```
# /opt/BitDefender/bin/bdconfigure
```

korzystając z następujących dostępnych opcji:

- `--help` aby wyświetlić listę wszystkich poleceń Narzędzia Wsparcia
- `enablelogs` aby włączyć produkt i dziennik modułu komunikacyjnego (wszystkie usługi zostaną automatycznie uruchomione ponownie)
- `disablelogs` aby wyłączyć produkt i dzienniki modułu komunikacyjnego (wszystkie usługi zostaną automatycznie uruchomione ponownie)
- `deliverall` aby stworzyć archiwum zawierające produkt i dzienniki modułu komunikacji, dostarczane do folderu `/tmp` w następującym formacie: `bitdefender_machineName_timeStamp.tar.gz`.

  1. Zostanie wyświetlony monit, jeżeli zachcesz wyłączyć dzienniki. W razie potrzeby, usługi są automatycznie ponownie uruchamiane.

2. Zostanie wyświetlony monit, czy chcesz usunąć dzienniki.

- `deliverall -default` dostarcza pewne informacje jak w poprzedniej opcji, lecz domyślne akcje nie będą uwzględniane w dzienniku bez potwierdzenia ze strony użytkownika (dzienniki zostają wyłączone i skasowane).

Aby zaraportować zdarzenie GravityZone dotyczące twojego systemu Linux, przejdź do kolejnego kroku, wykorzystując wsześniej opisane opcje:

1. Uruchom produkt oraz dziennik modułu komunikacyjnego.
2. Spróbuj odtworzyć problem.
3. Wyłącz dzienniki.
4. Utwórz archiwum dzienników.
5. Odbierz bilet mailowego wsparcia używając formularza dostępnego na stronie **Pomoc & Wsparcie** Control Center, wraz z opisem zdarzenia i załączonym archiwum dziennika.

Narzędzie Wsparcia dla Linux dostarcza następujące informacje:

- `etc`, `var/log`, `/var/crash` (jeśli dostępne) oraz foldery `var/epag` z `/opt/BitDefender`, zawierają dzienniki i ustawienia Bitdefender
- Plik `/tmp/bdinstall.log` zawierający informacje dotyczące instalacji
- Plik `network.txt`, zawierający ustawienia sieci / informacje połączenia maszyny
- Plik `system.txt` zawiera ogólne informacje systemowe (dystrybucja, wersja jądra, dostępna pamięć RAM, wolna przestrzeń dyskowa)
- Plik `users.txt`, zawierający informacje o użytkowniku
- Pozostałe informacje dotyczące produktu związane z systemem, takie jak zewnętrzne połączenia procesów i wykorzystanie procesora
- Logi systemowe

6.3.3. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Mac

Składając zapytanie do Zespołu Wsparcia Technicznego Bitdefender należy podać następujące informacje:

- Szczegółowy opis problemu, który napotkałeś.
- Zrzut ekranu (jeśli dotyczy) dokładnego błędu wiadomości, która się pojawi.
- Log Narzędzia Wsparcia.

Aby zebrać informacje o systemie Mac przy użyciu Narzędzia Wsparcia:

1. Pobierz archiwum ZIP zawierające narzędzie pomocy technicznej.
2. Rozpakuj archiwum. To wyodrębni plik **BDProfiler.tool**.
3. Otwórz okno Terminala.
4. Przejdź do lokalizacji pliku **BDProfiler.tool**.

   Na przykład:

   ```
   cd /Users/Bitdefender/Desktop;
   ```

5. Dodaj uprawnienia do wykonywania do pliku:

   ```
   chmod +x BDProfiler.tool;
   ```

6. Uruchom narzędzie.

   Na przykład:

   ```
   /Users/Bitdefender/Desktop/BDProfiler.tool;
   ```

7. Naciśnij `Y` i wprowadź hasło, gdy zostaniesz poproszony o podanie hasła administratora.

   Poczekaj kilka minut, aż narzędzie zakończy generowanie logu. Znajdziesz plik archiwum wyników (**Bitdefenderprofile_output.zip**) w tym samym folderze z narzędziem.

6.4. Informacje o produkcie

Skuteczna komunikacja jest kluczem do udanej współpracy. Przez ostatnie 10 lat Bitdefender uzyskał niekwestionowaną reputację dzięki ciągłemu dążeniu do poprawy komunikacji z klientami, aby przewyższyć oczekiwania partnerów oraz

klientów. Jeśli miałbyś jakiekolwiek problemy czy pytania, bez wahania skontaktuj się z nami.

6.4.1. Adresy Internetowe

Dział sprzedaży: enterprisesales@bitdefender.com
Centrum pomocy:http://bitdefender.pl/dla-biznesu/uzyteczne-linki/wsparcie-techniczne
Dokumentacja: documentation@bitdefender.com
Lokalni Dystrybutorzy:http://www.bitdefender.com/partners
Program partnerski: partners@bitdefender.com
Rzecznik prasowy: pr@bitdefender.com
Wysyłanie Próbek Wirusów: virus_submission@bitdefender.com
Wysyłanie Próbek Spamu: spam_submission@bitdefender.com
Raportowanie Abuse: abuse@bitdefender.com

6.4.2. Lokalni Dystrybutorzy

Lokalni dystrybutorzy Bitdefender są gotowi odpowiedzieć na wszelkie zapytania dotyczące ich obszaru działań, zarówno w sprawach handlowych, jak i ogólnych.

Wyszukiwanie dystrybutora Bitdefender w danym kraju:

1. Odwiedź http://www.bitdefender.com/partners.
2. Przejdź do **Lokalizator Partnera**.
3. Informacje kontaktowe lokalnych dystrybutorów Bitdefender powinny wyświetlić się automatycznie. Jeśli to się nie stanie, wybierz kraj, w którym mieszkasz, aby wyświetlić te informacje.
4. Jeśli w swoim kraju nie możesz znaleźć dystrybutora Bitdefender, skontaktuj się z nami, wysyłając e-mail na adres enterprisesales@bitdefender.com.

6.4.3. Biura Bitdefender

Biura Bitdefender są gotowi odpowiedzieć na wszelkie zapytania dotyczące ich obszaru działań, zarówno w sprawach handlowych, jak i ogólnych. Ich adresy oraz dane kontaktowe są wypisane poniżej.

Stany Zjednoczone

Bitdefender, LLC
PO Box 667588

Pompano Beach, Fl 33066
United States
Telefon (sprzedaż&pomoc techniczna): 1-954-776-6262
Sprzedaż: sales@bitdefender.com
Internet: http://www.bitdefender.com
Centrum pomocy: http://www.bitdefender.com/support/business.html

Francja

PROFIL TECHNOLOGY
49, Rue de la Vanne
92120 Montrouge
Faks: +33 (0)1 47 35 07 09
Telefon: +33 (0)1 47 35 72 73
Adres e-mail: supportpro@profiltechnology.com
Strona: http://www.bitdefender.fr
Centrum pomocy: http://www.bitdefender.fr/support/professionnel.html

Hiszpania

Bitdefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
España
Faks: (+34) 93 217 91 28
Telefon (biuro i sprzedaż): (+34) 93 218 96 15
Telefon (pomoc techniczna): (+34) 93 502 69 10
Sprzedaż: comercial@bitdefender.es
Strona: http://www.bitdefender.es
Centrum pomocy: http://www.bitdefender.es/support/business.html

Niemcy

Bitdefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Telefon (biuro i sprzedaż): +49 (0)2301 91 84 222
Telefon (pomoc techniczna): +49 (0)2301 91 84 444

Sprzedaż: vertrieb@bitdefender.de
Strona: http://www.bitdefender.de
Centrum pomocy: http://www.bitdefender.de/support/business.html

Anglia i Irlandia

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
UK
Telefon (sprzedaż&pomoc techniczna): (+44) 203 695 3415
Adres e-mail: info@bitdefender.co.uk
Sprzedaż: sales@bitdefender.co.uk
Strona: http://www.bitdefender.co.uk
Centrum pomocy: http://www.bitdefender.co.uk/support/business.html

Rumunia

BITDEFENDER SRL
DV24 Offices, Building A
24 Delea Veche Street
024102 Bucharest, Sector 2
Faks: +40 21 2641799
Telefon (sprzedaż&pomoc techniczna): +40 21 2063470
Sprzedaż: sales@bitdefender.ro
Strona: http://www.bitdefender.ro
Centrum pomocy: http://www.bitdefender.ro/support/business.html

Zjednoczone Emiraty Arabskie

Bitdefender FZ-LLC
Dubai Internet City, Building 17
Office # 160
Dubai, UAE
Telefon (sprzedaż&pomoc techniczna): 00971-4-4588935 / 00971-4-4589186
Faks: 00971-4-44565047
Sprzedaż: sales@bitdefender.com
Internet: http://www.bitdefender.com/world
Centrum pomocy: http://www.bitdefender.com/support/business.html

A. Aneksy

A.1. Wspierane Typy Plików

Antymalwarowe silniki skanowania załączone w rozwiązaniu ochrony Bitdefender mogą skanować wszystkie typy plików, które mogą zawierać zagrożenia. Lista poniżej zawiera najbardziej pospolite typy plików, które są analizowane.

{*; 386; 3g2; 3gg; 7z; a6p; ac; accda; accdb; accdc; accde; accdr; accdt; accdu; acl; acm; acr; action; ade; adp; ain; air; app; ar; arc; arj; as; asd; asf; asp; au; avi; awk; ax; bas; bat; bin; bmp; boo; bz; bz2; bzip2; cab; cal; cgi; chm; cla; class; cmd; cnv; com; cpio; cpl; cru; crush; csc; csh; dat; dcx; deb (with gzip, bzip2, xz); dek; dld; dll; dmg (with HFS); doc; docm; docx; dot; dotm; dotx; drv; drw; ds; ds4; dtd; ebm; emf; eml; eps; esh; exe; ezs; fky; frs; fxp; gadget; gif; grv; gx2; gz; gzip; hap; hlp; hms; hta; htm; html; htt; iaf; icd; ico; img; inf; ini; inx; ipf; iso; isu; jar; jfif; jpe; jpeg; jpg; js; jse; jsx; kix; laccdb; lha; lzh; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mid; mmf; mov; mp3; mpd; mpeg; mpg; mpp; mpt; mpx; ms; msg; msi; mso; msp; mst; msu; nws; oab; obd; obi; obs; obt; ocx; odt; oft; ogg; ole; one; onepkg; osci; ost; ovl; pa; paf; pak; pat; pci; pcx; pdf; pex; pfd; pgm; php; pif; pip; png; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; ppz; prc; prf; prg; ps1; psd; psp; pst; pub; puz; pvd; pwc; pwz; py; pyc; pyo; qpx; qt; qxd; ra; ram; rar; rbx; rgb; rgs; rm; rox; rpj; rpm (with cpio, gzip, bzip2, xz); rtf; scar; scr; script; sct; sdr; sh3; shb; shs; shw; sit; sldm; sldx; smm; snp; snt; spr; src; svd; swf; sym; sys; tar; tar.z; tb2; tbz2; td0; tgz; thmx; tif; tiff; tlb; tms; tsp; tt6; u3p; udf; ufa; url; vb; vbe; vbs; vbscript; vwp; vxd; wav; wbk; wbt; wcm; wdm; wiz; wks; wll; wmf; wml; wpc; wpf; wpg; wpk; wpl; ws; ws2; wsc; wsf; wsh; xar; xl; xla; xlam; xlb; xlc; xll; xlm;

xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp; xz; z; zip; zl?; zoo