Bitdefender

GravityZone

PODRĘCZNIK INSTALACJI

Bitdefender GravityZone
Podręcznik instalacji

Data publikacji 2017.02.10

Uwagi prawne

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. vi)	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, a chmura by dostarczać usługę ochrony dla fizycznych punktów końcowych, urządzeń mobilnych, 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 Mobile
- Hypervisor Memory Introspection

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 obciążenie systemowe zapewnia wzrost wydajności, a integracja z Microsoft Active Directory ułatwia automatyczne zastosowanie ochrony na niezarządzanych komputerach stacjonarnych oraz serwerach. 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

GravityZone stanowi dziś pierwsze niezależne od platformy rozwiązanie do ochrony dymanicznych centrów danych. Zgodność z każdym znanym środowiskiem, zaczynając od VMware ESXi do Citrix Xen lub Microsoft Hyper-V, Bitdefender Security for Virtualized Environments wykorzystuje zbiorczą charakterystykę wirtualizacji, przenosząc główne procesy bezpieczeństwa na scentralizowane urządzenia wirtualne. Wspierane nowatorską technologią buforowania, rozwiązanie przynosi korzyści w stosunku do wydajności i zwiększa konsolidację serwerów nawet o 30% w porównaniu do tradycyjnych rozwiązań antymalware. Z poziomu zarządzania, Security for Virtualized Environments integruje się z platformami trzecich firm takich jak VMware, vCenter i XenSerwer dla automatyzacji zadań administracyjnych i zmniejszenia kosztów operacyjnych.

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.

Hypervisor Memory Introspection (HVI)

Powszechnie wiadomo, że dobrze zorganizowani, napędzani profitami napastnicy poszukują nieznanych luk (luk zero-day), albo używają jednorazowych, specjalnie zbudowanych exploitów (exploity zero-day) oraz innych narzędzi. Atakujący również korzystają z zaawansowanych technik w celu opóźnienia i ładowności sekwencji ataku do maskowania szkodliwej aktywności. Nowsze, napędzane dochodami ataki są budowane by być cichymi i by pokonywały tradycyjne narzędzia bezpieczeństwa.

W środowiskach zwirtualizowanych, problem jest rozwiązany, HVI chroni centra danych o wysokim zagęszczeniu maszyn wirtualnych przeciwko zaawansowanym i nadzwyczajnym zagrożeniom, których silniki oparte na sygnaturach nie mogą

pokonać. To wymusza silną izolację, zapewniając w czasie rzeczywistym wykrywanie ataków, blokując te, które się zdarzą i natychmiast usuwane jest zagrożenie.

Gdy chronioną maszyną jest Windows lub Linux, serwer lub komputer, HVI zapewnia wgląd na poziomie, który jest niemożliwy do osiągnięcia z poziomu systemu operacyjnego gościa. Podobnie jak hypervisor kontroluje dostęp do sprzętu w imieniu każdej maszyny wirtualnej gościa, HVI posiada dogłębną wiedzę zarówno w trybie użytkownika, jak i jądra pamięci gościa. W rezultacie [HIV] zawiera kompletny wgląd w pamięć gościa, a więc pełny kontekst. Jednocześnie HVI jest izolowany od chronionych gości, tak samo jak hypervisor jest izolowany. Operując na poziomie hypervisor i wykorzystując funkcjonalności hypervisor'a, HVI przezwycięża problemy techniczne tradycyjnego bezpieczeństwa ujawniając szkodliwą aktywność w centrach danych.

HVI identyfikuje techniki ataku zamiast wzorców ataków. W ten sposób, technologia jest w stanie identyfikować, raportować i zapobiegać wspólnym technikom exploitów. Jądro jest chronione przed technikami hookowania rootkitami, które są wykorzystywane podczas łańcucha zabicia ataku, aby dostarczyć stealth. Procesy trybu użytkownika są również chronione przed wstrzyknięciem kodu, funkcji detouring i wykonaniem kodu ze stosu lub sterty.

Security for Mobile

Ujednolica w całym przedsiębiorstwie ochronę i zarządzanie oraz zgodność w kontroli urządzeń iPhone, iPad i systemem Android poprzez dostarczenie niezawodnego oprogramowania i dystrybucji aktualizacji za pośrednictwem firmy Apple oraz sklepów Android. Rozwiązanie zostało zaprojektowane tak by umożliwić kontrolowaną adaptację rozwiązania bring-your-own-device (BYOD) poprzez zainicjowanie i konsekwentne egzekwowanie zasad użytkowania na wszystkich urządzeniach przenośnych. Funkcje bezpieczeństwa zawierają blokadę ekranu, kontrolę uwierzytelnienia, lokalizowanie urządzenia, zdalne czyszczenie pamięci, wykrywanie zrootowanych i odblokowanych urządzeń oraz kontroli profili bezpieczeństwa. W przypadku urządzeń z Android poziom bezpieczeństwa jest wyższy dzięki skanowaniu w czasie rzeczywistym i szyfrowaniu karty pamięci. W rezultacie kontrolujemy urządzenia i chronimy znajdujące się na nich poufne dane firmowe.

1.2. Architektura GravityZone

Unikatowa architektura GravityZone dostarcza nam ułatwione skalowanie i zabezpieczenie dowolnej ilości systemów. GravityZone może zostać skonfigurowany do korzystania z wielu urządzeń wirtualnych w wielu przypadkach i z zastosowaniem określonych ról (Baza danych, serwery komunikacyjne, serwery aktualizacyjne i konsola WWW) by zapewnić skalowalność i niezawodność.

Każda rola instancji może zostać zainstalowana na innym urządzeniu. Wbudowany równoważnik ról zapewnia GravityZone ochronę nawet największych sieci korporacyjnych, nie powodując efektu spowolnienia ani zawężenia przepustowości. Istniejące sprzętowe lub programowe rozwiązania kompensacyjne mogą zastąpić wbudowany stabilizator, jeżeli taki jest używany w danej sieci.

Dostarczany w kontenerze wirtualnym, GravityZone może być zaimportowany do pracy na dowolnej platformie wirtualizacji, w tym VMware, Citrix, Microsoft Hyper-V.

Integracja z VMware vCenter, Citrix XenServer oraz Microsoft Active Directory zmniejszają nasz wysiłek związany z wdrażaniem ochrony dla stacji fizycznych i wirtualnych punktów końcowych.

Rozwiązanie GravityZone zawiera następujące składniki:

- GravityZone Virtual Appliance z dostępnymi rolami:
  - Baza danych
  - Serwer aktual.
  - Serwer komunikacji
  - Konsola Webowa (Control Center)
- Kreator Raportów z wirtualnego urządzenia z dostępnymi rolami:
  - Baza danych
  - Procesory
- Security Server
- Agenci Bezpieczeństwa

1.2.1. Urządzenie Wirtualne GravityZone

Rozwiązanie GravityZone instalowane w siedziebie jest dostarczane jako samo-konfigurująca się publikacjaLinux Ubuntu utwardzonego urządzenia wirtualnego wbudowanego w obraz maszyny wirtualnej, łatwy do instalacji i konfiguracji przy użyciu interfejsu wiersza poleceń (CLI). Wirtualne urządzenia są dostępne w kilku formatach kompatybilnych z platformami wirtualizacji (OVA, XVA, VHD, OVF, RAW).

1.2.2. Baza danych GravityZone

Centralna logika architektury GravityZone. Bitdefender używa nie-relacyjnej bazy danych MongoDB, prostej w skalowaniu i replikacji.

1.2.3. Serwer Aktualizacji GravityZone

Serwer aktualizacyjny posiada istotną rolę przy uaktualnianiu rozwiązania GravityZone oraz agentów zainstalowanych na końcówkach poprzez replikowanie i publikowanie potrzebnych paczek oraz plików instalacyjnych.

1.2.4. Serwer Komunikacji GravityZone

Serwer komunikacyjny jest łącznikiem pomiędzy agentami bezpieczeństwa i bazą danych, przekazują polityki i zadania do chronionych urządzeń końcowych oraz zdarzeniowych raportów do agentów bezpieczeństwa.

1.2.5. Konsola Webowa (Control Center)

Bitdefender rozwiązania ochrony są zarządzane przez GravityZone z poziomu pojedynczego punktu zarządzania, Control Center konsoli WWW, która umożliwia nam łatwiejsze zarządzanie i dostęp całościowego stanu zabezpieczeń, globalnego poziomu zagrożenia oraz kontrolę nadrzędnego zabezpieczenia modułów chroniących wirtualne i fizyczne stanowiska, serwery oraz urządzenia mobilne. Zasilana przez Architekturę Gravity, Control Center jest w stanie odpowiedź na potrzeby nawet największych organizacji.

Control Center zintegrowana z istniejącym systemem zarządzania i monitorowaniem systemu, aby łatwo automatycznie zatwierdzać ochronę niezarządzanych komputerów stacjonarnych, serwerów i urządzeń przenośnych, które pojawiają się w Microsoft Active Directory, VMware vCenter i Citrix XenServer lub są po prostu wykrywane w sieci.

1.2.6. Kreator Raportu

Kreator Raportów pozwala na tworzenie i zarządzanie kompleksowymi bazami zapytań, korzystając z wielu filtrów. Oparte na zapytaniach raporty dostarczają wszystkie informacje, których potrzebujesz do zrozumienia każdego zdarzenia lub zmiany, która wydarzyła się kiedykolwiek w twojej sieci.

1.2.7. Security Server

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

Są trzy wersje Security Server dla każdego typu środowisk wirtualnych:

- **Security Server dla VMware NSX.** Ta wersja jest automatycznie instalowana na każdym hoście w klastrze, gdzie Bitdefender została wdrożona.
- **Security Server dla VMware vShield Endpoint.** Ta wersja musi być zainstalowana na każdym hoście, aby był chroniony.
- **Wieloplatformowy Security Server.** Ta wersja jest dla różnych innych zwirtualizowanych środowisk i to musi być zainstalowane na jednym lub wielu hostach tak, aby pomieścić liczbę chronionych maszyn wirtualnych. Gdy korzystasz z HVI, Security Server musi być zainstalowany na każdym hoście, który zawiera maszyny wirtualne do ochrony.

1.2.8. Pakiet Uzupełniający HVI

Pakiet HVI zapewnia powiązanie pomiędzy hypervisor'em i Security Server na tym hoście. W ten sposób, Security Server jest w stanie monitorować pamięć wykorzystaną na hoście, na którym jest zainstalowany, w oparciu o polityki bezpieczeństwa GravityZone.

1.2.9. 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 Tools (vShield)
- GravityZone Mobile Client

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 aplikacji
- 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. 21).

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. 21).

Kontrola aplikacji

Moduł Kontroli Aplikacji zapobiega malware, atakom 0-day i zwiększa ochronę bez wpływu na wydajność. Kontrola aplikacji wymusza elastyczne zasady białej listy aplikacji, które identyfikują i zapobiegają instalację i wykonanie jakichkolwiek niepożądanych, niezaufanych lub złośliwych aplikacji.

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

- Windows Vista
- serwery Windows
- Starsze systemy operacyjne Windows Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne" (p. 21).

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. 21).

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. 21).

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.
- 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.

Bitdefender Tools (vShield)

Bitdefender Tools jest lekkim agentem dla środowisk zwirtualizowanych VMware, które są zintegrowane z vShield Endpoint. Agent bezpieczeństwa instalowany na maszynach wirtualnych chronionych przez Security Server, aby pozwolić skorzystać z dodatkowej funkcjonalności to prowadzi:

- Dopuszcza uruchomienie zadań skanowania pamięci i procesów na maszynie.
- Informuje użytkownika o wykrytych infekcjach i akcjach zastosowanych na nich.
- Dodaje więcej opcji dla wyjątków skanowania antymalware.

GravityZone Mobile Client

GravityZone Mobile Client rozszerza z łatwością polityki zabezpieczeń na dowolnej liczbie urządzeń z systemem Android oraz iOS, chroniąc je przed nieautoryzowanym użyciem i ryzykiem utraty poufnych danych. Funkcje bezpieczeństwa zawierają blokadę ekranu, kontrolę uwierzytelnienia, lokalizowanie urządzenia, zdalne czyszczenie pamięci, wykrywanie zrootowanych i odblokowanych urządzeń oraz kontroli profili bezpieczeństwa. W przypadku urządzeń z Android poziom bezpieczeństwa jest wyższy dzięki skanowaniu w czasie rzeczywistym i szyfrowaniu karty pamięci.

Aplikacja GravityZone Mobile Client jest dystrybuowana wyłącznie poprzez Apple App Store i Google Play.

2. WYMAGANIA DOTYCZĄCE INSTALACJI

Wszystkie rozwiązania GravityZone są instalowane i zarządzane przez Control Center.

2.1. Wymagania GravityZone Appliance

GravityZone jest dostarczany jako urządzenie wirtualne. Urządzenie GravityZone dostępne jet w następujących formatach:

- OVA (kompatybilny z VMware vSphere, View, VMware Player)
- XVA (kompatybilny z Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (kompatybilny z Microsoft Hyper-V)
- OVF (kompatybilny z Red Hat Enterprise Virtualization)*
- OVF (kompatybilny z Oracle VM)*
- RAW (kompatybilny z Kernel-based Virtual Machine lub KVM)*

*pakiety OVF i RAW są archiwizowane w formacie tar.bz2.

Dla zgodności platformy Oracle VM VirtualBox, patrz ten artykuł KB.

Wsparcie dla innych formatów i platform wirtualizacji może być dostarczone na życzenie.

2.1.1. Wymagania Sprzętowe

Wdraża urządzenie GravityZone posiadające poniższą konfigurację sprzętową:

Wymagany vCPU

Składnik	Ilość Punktów Końcowych						
	250	1000	5000	10000	25000	25000*	50000*
Serwer aktual.	1	1	1	1	1	1	1
Konsola internetowa	1	1	2	4	6	6	8
Serwer komunikacji	1	1	2	4	6	6	8
Baza danych*	1	2	2	2	3	3	6
Całkowity**	4	5	7	11	16	20	30

* - pomnóż przez dwa dla środowisk GravityZone używających zestawu repliki baz danych
** - łączna dla środowisk GravityZone bez zestawu repliki bazy danych

Wymagana Pamięć RAM (GB)

Składnik	Ilość Punktów Końcowych						
	250	1000	5000	10000	25000	25000*	50000*
Serwer aktual.	1	1	1	1	2	2	2
Konsola internetowa	2	2	3	5	7	7	9
Serwer komunikacji	1	1	2	4	6	6	8
Baza danych*	2	4	5	6	8	8	8
Całkowity**	6	8	11	16	23	32	36

* - pomnóż przez dwa dla środowisk GravityZone używających zestawu repliki baz danych
** - łączna dla środowisk GravityZone bez zestawu repliki bazy danych

Wymagana Powierzchnia Dysku Twardego (GB)

Składnik	Ilość Punktów Końcowych						
	250	1000	5000	10000	25000	25000*	50000*
Serwer aktual.							
Konsola internetowa	40	40	40	40	40	40	40
Serwer komunikacji							
Baza danych*	10	20	20	20	40	40	80
Całkowity**	50	60	60	60	80	120	200

* - jedynie dla rozproszonych środowisk GravityZone używających zestawów replik baz danych
*** - łączna dla środowisk GravityZone bez zestawu repliki bazy danych
** - pomnóż przez dwa dla środowisk GravityZone używających zestawy repliki baz danych

2.1.2. Połączenie z Internetem

Urządzenie GravityZone wymaga dostępu do Internetu.

2.1.3. Control Center wymagania konsoli webowej

Dostęp do konsoli webowej Control Center, wymagane jest co następuje:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+, Microsoft Edge 20+, Opera 12+
- Zalecana rozdzielczość ekranu: 1280x800 lub wyższa
- Komputer, z którego chcesz się połączyć, musi mieć połączenie sieciowe do Control Center.

Ostrzeżenie
Control Center nie pracuje / wyświetla poprawnie w Internet Explorer 9+ z włączoną funkcją zgodności, co jest równoznaczne z wykorzystaniem nieobsługiwanych wersji przeglądarki.

2.2. Wymagania Ochrony Punktu Końcowego

Aby chronić swoją sieć z Security for Endpoints lub Security for Virtualized Environments, musisz zainstalować agenty 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 wdrożyć i nad punktami końcowymi sieci, którą zarządzasz.

2.2.1. 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.

- **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.

Wymagania dla Środowisk VMware vShield

To są wymagania i footprint Bitdefender Tools dla zintegrowanych systemów w środowiskach VMware zawierających vShield Endpoint.

Platforma	RAM	Miejsce na Dysku
Windows	6-16* MB (~ 10 MB dla GUI)	24 MB
Linux	9-10 MB	10-11 MB

*5 MB, gdy Tryb Cichy jest włączony i 10 MB, gdy jest wyłączony. W trybie Cichym, Bitdefender Tools graficzny interfejs użytkownika (GUI) nie ładuje się automatycznie podczas startu systemu, zwalniając zasoby.

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(3)(6)
- Windows 8(7)
- Windows 7
- Windows Vista z dodatkiem Service Pack 1(4)
- Windows XP z Service Pack 2 64 bit(1)(4)
- Windows XP z Service Pack 3(1)(4)

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][5]
- Windows XP Tablet PC Edition[1][5]

Systemy operacyjne serwera

- Windows Server 2016
- Windows Server 2012[7][8] / Windows Server 2012 R2[6]
- Windows Server 2008 / Windows Server 2008 R2[8]
- 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) Platforma VMware vShield (Wersja Bezagentowa) wspiera Windows 8.1 (32/64 bit) i Windows Server 2012 R2 (64 bit) dostępne rozpoczynając z VMware vSphere 5.5 - ESXi build 1892794 lub nowszy.
(4) NSX VMware i VMware vShield Endpoint nie obsługuje wersji 64- bitowej systemów Windows XP i Vista.
(5) 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

(6) W VMware NSX, wersja OS jest obsługiwana zaczynając od vSphere 5.5 Patch 2.
(7) VMware NSX, wersja OS jest obsługiwana zaczynając od vSphere 5.5.
(8) VMware ESX nie obsługuje wersji 32- bitowych systemów Windows 2012 i Windows Server 2008 R2.
(9) W VMware ESX, Windows Server 2003 jest obsługiwany z SP2.

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
- Oracle Solaris 11, 10 (tylko w środowiskach VMware vShield)
- Oracle Linux 6.3 lub nowszy

WAŻNE
W środowiskach NSX, wsparcie dla systemów Linux jest zapewnione poprzez Bitdefender Endpoint Security Tools, zainstalowane na maszynach wirtualnych i skonfigurowane do korzystania z lokalnych silników skanowania.

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. 109)

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+

2.2.2. Wspierane platformy wirtualizacyjne

Security for Virtualized Environments zapewnia wsparcie dla następujących platform wirtualizacji:

- 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.

Integracja z wymaganiami VMware vShield Endpoint

- ESXi 6.0, 5.5, 5.1, 5.0 (wersja 474610 lub wyższa), 4.1 (wersja 433742 lub wyższa)
- vCenter Server 6.0, 5.5, 5.1, 5.0, 4.1
- vCloud Networking and Security 5.5.4, 5.5.3, 5.5.2, 5.5.1
- vShield Manager 5.5.4-3953973 lub wyższy
- vShield Endpoint zainstalowany przez vShield Manager na hoście/hostach chronionych przez Security for Virtualized Environments
- VMware Tools 8.6.0 wersja 446312 lub wyższa zainstalowane na chronionych maszynach wirtualnych w trybie pełnym lub z kierowcą vShield Endpoint wybrany pod VMCI w trybie niestandardowym.

WAŻNE
Zaleca się, aby utrzymywać wszystkie produkty VMware zaktualizowane z najnowszymi poprawkami.

- Jeżeli używasz ESXi 5.5 do wsparcia gości systemów operacyjnych Windows 2012 R2 i Windows 8.1 wymagane jest zastosowanie VMware ESXi 5.5, Patch ESXi550-201407401-BG: Aktualizacja esx-base (2077407).
- Jeżeli używasz ESXi 5.0, jest wysoce zalecane zastosowanie VMware ESXi 5.0 Patch ESXi500-201204401-BG: Updates tools-light, który rozwiązuje krytyczne problemy ze sterownikami gościa vShield Endpoint. Aktualizauj patch Narzędzi VMware do wersji 8.6.5 build 652272.
- Jeżeli używasz ESXi 4,1 P3, musisz uzyskać zaktualizowaną wersje Narzędzi VMware i zainstalować ją na wirtualnych maszynach. Więcej informacji, szukaj w artykule KB

Integracja z Wymaganiami VMware NSX

- ESXi 5.5 lub nowszy dla każdego serwera
- vCenter Server 5.5 lub nowszy
- NSX Menedżer 6.2.4 lub nowszy
- Narzędzia VMware 9.1.0 lub nowsze.

WAŻNE
Zaleca się, aby utrzymywać wszystkie produkty VMware zaktualizowane z najnowszymi poprawkami.

2.2.3. Wspierane Narzędzia Zarządzania Wirtualizacjami

Control Center aktualnie integruje się z następującymi narzędziami do zarządzania wirtualizacją:

- Serwer VMware vCenter
- Citrix XenServer

aby skonfigurować integrację, musisz podać nazwę użytkownika i hasło administratora.

2.2.4. Wymagania Security Server

Security Server jest wstępnie skonfigurowaną maszyną wirtualną działającą na Ubuntu Server w następujących wersjach:

- 12.04 LTS (VMware vShield i Multi-Platforma)
- 16.04 (VMware NSX)

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

Security Server przez NSX pochodzi z predefiniowanych konfiguracji sprzętowej (CPU i RAM), które można dostosować w VMware vSphere Web Client przez włączenie i wyłączenie urządzenia, edytując jego ustawienia, a następnie poprzez jego ponowne włączenie. Aby uzyskać szczegółowe informacje, odwołaj się do „Instalowanie Security Server zintegrowanego z VMware NSX" (p. 85).

Inne wymagania zależą od tego, czy urządzenie integruje się z VMware VSHIELD Endpoint lub NSX:

- W środowiskach VMware z vShield Endpoint:
  - Security Server musi być zainstalowany na każdym hoście ESXi, aby był chroniony.
  - Musisz mieć 80 GB miejsca na dysku na każdym hoście.
- W środowiskach VMware z NSX:
  - Security Server automatycznie instaluje na każdym hoście ESXi, które w klastrze mają być chronione, w czasie Bitdefender wdrożenia usługi.
  - Musisz mieć 80 GB miejsca na dysku na każdym hoście.
- W innych środowiskach:
  - Chociaż nie jest to obowiązkowe, Bitdefender rekomenduje zainstalowanie Security Server na każdym fizycznym hoście w celu poprawy wydajności.
  - Musisz mieć 8 GB miejsca na dysku na każdym hoście Security Server.

2.3. Wymagania Ochrony Mobile

2.3.1. Wspierane platformy

Security for Mobile wspiera następujące typy urządzeń mobilnych i systemy operacyjne:

- Apple iPhone i tablety iPad (iOS 5.1+)
- Smartfony i tablety z Google Android (2.3+)

2.3.2. Wymagania Połączeń

Urządzenia mobilne muszą mieć aktywne dane komórkowe lub połączenie Wi-Fi oraz połączenie z serwerem komunikacji.

2.3.3. Powiadomienia Push

Security for Mobile używa powiadomień push do informowania klientów mobilnych o aktualizacjach polityki i dostępnych zadaniach. Powiadomienia Push są wysyłane przez Serwer komunikacji przez usługę dostarczaną przez producenta systemu operacyjnego:

- Usługi Wiadomości Chmury Google (GCM) dla urządzeń Android. Do pracy GCM wymagane jest co następuje:

  - Google Play Store musi być zainstalowany.
  - Urządzenia działające na wersji niższej niż Android 4.0.4 muszą przynajmniej raz zalogować się do konta Google.
  - Żeby wysłać powiadomienia push, liczba portów musi być otwarta.
- Usługi Powiadomienia Push Apple (APNs) dla urządzeń iOS. Więcej informacji, szukaj w artykule Apple KB

Możesz sprawdzić, czy powiadomienia Mobile Push działają poprawnie w sekcji **Sprawdź Powiadomienia Mobile Push** w **Konfiguracja > Różne**.

Aby nauczyć się więcej o GravityZone Zarządzaniu urządzeń przenośnych, zobacz ten artykuł KB.

2.3.4. Certyfikaty Zarządzania iOS

Aby skonfigurować infrastrukturę zarządzania urządzeniami przenosnymi iOS, należy podać liczbę certyfikatów bezpieczeństwa.

Aby uzyskać więcej informacji, odwołaj się do „Certyfikaty" (p. 64).

2.4. 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.

2.4.1. 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).

2.4.2. 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. 16).

Zalecana dostępność zasobów serwera:

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

2.4.3. 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

2.5. Wymagania HVI

HVI działa za pomocą dwóch komponentów: Security Server i Paczki Uzupełniającej HVI. Produkty te muszą być zainstalowane na hostach w Twoim środowisku wirtualnym, gdzie masz maszyny wirtualne, które chcesz ochronić.

Zanim wdrożysz HVI na hostach, upewnij się, że następujące wymagania są spełnione:

Wspierane platformy wirtualizacyjne

- Citrix XenServer 7 Edycja Enterprise ze wszystkimi poprawkami włącznie XS70E023.

  Dodatkowe pakiety poprawek następujące XS70E023 są opcjonalne.

Wspierane gościnne systemy operacyjne

Maszyny wirtualne, które chcesz chronić z HVI muszą być uruchomione na następujących systemach operacyjnych:

Windows Desktop Operating Systems

- Windows 10

- Windows 8.1
- Windows 8
- Windows 7

Serwerowe Systemy Operacyjne Windows

- Windows Server 2016
- Windows Server 2012 / Windows Server 2012 R2
- Windows Server 2008/ Windows Server 2008 R2

Systemy Operacyjne Linux

- Debian 8, 64-bit
- Ubuntu 16.04 LTS, 64-bit
- Ubuntu 15.04, 64-bit
- Ubuntu 14.04 LTS 64-bit
- CentOS 7, 64-bit
- Red Hat Enterprise Linux 7, 64-bit
- SUSE Linux Enterprise Server 12, 64-bit

Wymagania Sprzętowe Hosta

- **Mikroarchitektura CPU:**
  - Jakikolwiek procesor Intel® Sandy Bridge lub nowszy, ze wsparciem dla Technologii Wirtualizacji Intel®.
  - Rozszerzenia VT- x lub VT- d muszą być włączone w BIOSie.
- **Wolne miejsce na dysku:** Oprócz miejsca wymaganego przez Security Server, HVI wymaga dodatkowych 9 MB dla Pakietu Uzupełniającego na każdym hoście.

Wymagania Security Server

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	4 GB	4 CPU
51-100 maszyn wirtualnych	8 GB	6 CPU
101-200 maszyn wirtualnych	16 GB	8 CPU

Wolne miejsce na dysku: Musisz przeznaczyć 8 GB miejsca na dysku na każdym hoście dla Security Server.

Wymagania Maszyn Wirtualnych Gościa

W zwykłej konfiguracji środowiska, dla optymalnej wydajności i wskaźnika konsolidacji VM, zaleca się, aby mieć następującą minimalną konfigurację sprzętową dla maszyn wirtualnych gościa:

- **vCPU:** 2 x vCPU
- **RAM:** 3 GB

2.6. Wymagania Kreatora Raportu

Konstruktor Raportów jest dostarczany jako urządzenie wirtualne, w następujących formatach:

- OVA (kompatybilny z VMware vSphere, View, VMware Player)
- XVA (kompatybilny z Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (kompatybilny z Microsoft Hyper-V)
- OVF (kompatybilny z Red Hat Enterprise Virtualization)*
- OVF (kompatybilny z Oracle VM)*
- RAW (kompatybilny z Kernel-based Virtual Machine lub KVM)*

*pakiety OVF i RAW są archiwizowane w formacie tar.bz2.

Konstruktor Raportów wymaga, aby uruchomić dwie instancje Kreatora Raportu Virtual Appliance, jeden dla każdej roli Bazodanowej i Procesorów.

2.6.1. Wymagania Sprzętowe

Wdrażaj urządzenie Konstruktora Raportów z następującą konfiguracją sprzętową:

Wymagane CPU

Virtual Appliance	Ilość Punktów Końcowych					
	250	1000	5000	10000	25000	50000
Baza danych	4	4	4	4	6	8
Procesory	6	6	6	6	6	6

Wymagana Pamięć RAM (GB)

Virtual Appliance	Ilość Punktów Końcowych					
	250	1000	5000	10000	25000	50000
Baza danych	8	8	8	8	16	16
Procesory	8	8	8	8	8	8

Wymagana Powierzchnia Dysku Twardego (GB)

Virtual Appliance	Ilość Punktów Końcowych					
	250	1000	5000	10000	25000	50000
Baza danych*	15	20	50	90	210	400
Procesory**	50	200	1000	1950	4800	9500

* Narzędzie Wirtualne Kreatora Raportów z Bazy danych dostarcza zdarzenia z zużycia dysku zebrane przez jeden rok.
*Dysk wykorzystania Urządzenia Wirtualnego Konstruktor Reportów Procesorów jest dostarczany biorąc pod uwagę średnio 10 raportów miesięcznie, z podzbiorem 15 kolumn każdego z nich.

2.6.2. Wymagania Systemowe

Kreator Raportu wymaga następująco:

- Konsola:
  - GravityZone 6.1.27-537+
- Agenty bezpieczeństwa na punkty końcowe:

- Bitdefender Endpoint Security Tools 6.2.10.829+
- Endpoint Security dla Maca 4.0.0.167123+

2.7. 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
443 (HTTPS)	Integracja vCenter Server i XenServer Komunikacja pomiędzy GravityZone i hypervisor
8443 (HTTPS)	Port używany przez klienta oprogramowania do połączenia z Serwerem Komunikacji.
7074 (HTTP)	Port serwera aktualizacji: Komunikacja z Relay* (jeśli jest dostępna)
7077	Port Server Staging dla pobierania aktualizacji produktu i pakietów. Komunikacja z Relay* (jeśli jest dostępna)
7075	Obsługuje komunikację pomiędzy usługami GravityZone i światem zewnętrznym.
4369 / 6150	Porty wykorzystywane w celu umożliwienia komunikacji pomiędzy Control Center i serwerem komunikacji.
27017	Domyślny port wykorzystywany przez Serwer Komunikacji i Control Center, aby mieć dostęp do bazy danych.
32002	Port używany przez konsole Control Center do wysyłania i odbierania informacji dotyczących raportów, powiadomień, e-maili, których na ogół przetworzenie trwa dłużej.
7081 / 7083 (SSL)	Porty używane przez agentów punktów końcowych do połączenia z Security Server.

Port	Użycie
48651	Port komunikacyjny pomiędzy agentem Bitdefender Endpoint Security Tools dla Linux i Security Server w środowisku VMware z punktem końcowym vShield.
48652	Port komunikacyjny pomiędzy hipernadzorcąBitdefender Tools(vmkernel) i Security Server w środowisku VMware z punktem końcowym vShield.
5228, 5229, 5230	Porty Wiadomości Chmury Google (GCM). Serwer komunikacji używa GCM do wysyłania powiadomień push do zarządzanych urządzeń Android.
2195, 2196, 5223	Porty Usługi Powiadomień Push Apple (APNs). Porty 2195 i 2196 są używane przez Serwer komunikacji do komunikacji z serwerami APNs. Port 5223 jest używany do zarządzania urządzeniami iOS do komunikacji z serwerami APNs poprzez Wi-Fi w określonych warunkach. Więcej informacji, szukaj w artykule Apple KB
123 (UDP)	Port dla protokołu pakietów użytkownika (UDP) używany przez GravityZone urządzenia do synchronizacji z serwerem NTP.
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

Aby chronić Twoją sieć z Bitdefender, musisz zainstalować agenty bezpieczeństwa GravityZone na punktach końcowych. W tym celu, potrzebujesz użytkownika z prawami administracyjnymi Control Center nad usługami jakie potrzebujesz zainstalować i nad punktami końcowymi, którymi zarządzasz.

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 uruchomione na dowolnej platformie wirtualizacji.
Security for Mobile	iPhone, iPad i urządzenia z systemem Android
Security for Exchange	Serwery Microsoft Exchange
Hypervisor Memory Introspection	Maszyny wirtualne Microsoft Windows i Linux uruchomione na Citrix XenServer

3.1. Instalacja i konfiguracja GravityZone

Aby upewnić się, że instalacja idzie gładko, wykonaj następujące kroki:

1. Przygotowanie do instalacji
2. Wdróż i skonfiguruj urządzenie wirtualne GravityZone
3. Połącz się z Control Center i ustaw pierwsze konto użytkownika
4. Konfiguruj ustawienia Control Center

3.1.1. Przygotowanie do Instalacji

Do instalacji, potrzebujesz obrazu urządzenia wirtualnego GravityZone. Po wdrożeniu i skonfigurowaniu urządzenia GravityZone, możesz zdalnie zainstalować klienta lub pobrać potrzebne pakiety instalacyjne dla wszystkich elementów usług bezpieczeństwa z webowego interfejsu Control Center.

Obraz urządzenia GravityZone jest dostępny w kilku różnych formatach, kompatybilnych z głównymi platformami wirtualizacyjnymi. Możesz uzyskać linki do pobrania przez rejestracje dla wersji trial na stronie Bitdefender Enterprise .

Do instalacji i wstępnej konfiguracji, potrzebujesz:

- Nazwy DNS lub stałe adresy IP (przez konfigurację statyczną lub przez rezerwacje DHCP) dla urządzeń GravityZone
- Nazwa użytkownika i hasło administratora domeny
- Serwer vCenter, Manager vShield, szczegóły XenServer (nazwa hosta lub adres IP, port komunikacyjny, nazwa użytkownika i hasła dla administratora)
- Klucz licencyjny dla GravityZone usług bezpieczeństwa (sprawdź wersję próbną lub zakup email)
- Ustawienia serwera poczty wychodzącej
- Jeżeli potrzebne, ustawienia serwera proxy
- Certyfikaty bezpieczeństwa

Dodatkowe warunki muszą być spełnione aby zainstalować usługi.

3.1.2. Wdróż Urządzenie GravityZone

Aplikacje GravityZone mogą uruchamiać jedną, kilka lub wszystkie z poniższych ról:

- **Serwer bazodanowy**
- **Serwer aktual.**
- **Konsola internetowa**
- **Serwer komunikacji**

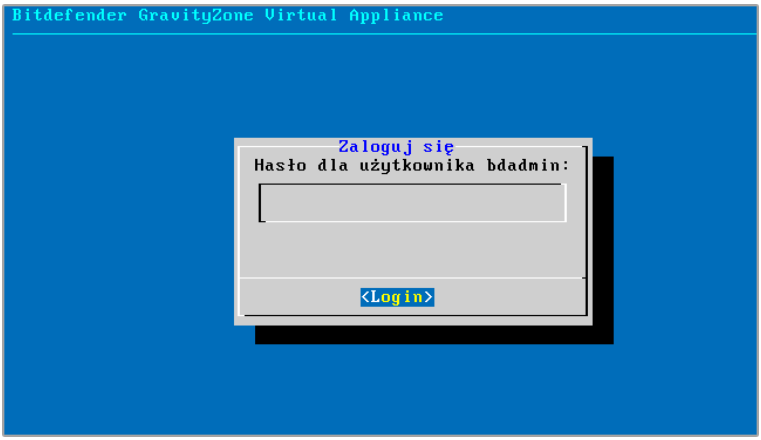
WdrożenieGravityZone wymaga uruchomienia jednej instancji każdej roli. W zależności od tego w jaki sposób chcesz dystrybuować role GravityZone, możesz wdrożyć jedną z czterech GravityZone urządzeń. Rola Serwera bazy danych jest pierwszym krokiem instalacji. W scenariuszu z wielu urządzeń GravityZone, możesz zainstalować rolę dla bazy danych serwera na pierwszym urządzeniu i skonfigurować wszystkie inne urządzenia do podłączenia do istniejących instancji bazy danych.

Wdrożyć i skonfigurować urządzenie GravityZone

1. Importuj obraz urządzenia wirtualnego GravityZone w środowisku wirtualnym.
2. Zasilanie urządzenia.
3. Z narzędzia do zarządzania wirtualizacją, dostęp do interfejsu konsoli urządzenia GravityZone.
4. Ustaw hasło dla wbudowanego `bdadmin` administratora systemu.

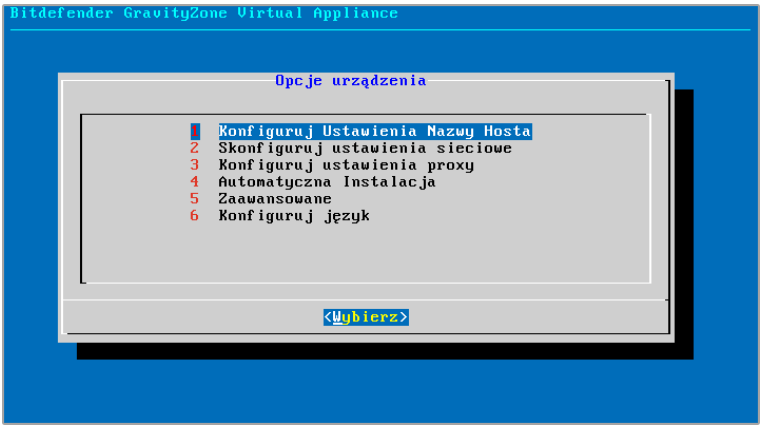
Interfejs konsoli urządzenia: podaj nowe hasło.

5. Zaloguj używając ustawionego hasła.



Interfejs konsoli urządzenia: login

6. Będziesz miał dostęp do interfejsu konfiguracyjnego urządzenia. Użyj klawiszy strzałek i przycisku `Tab` do nawigacji w menu i opcjach. Naciśnij `Enter`, aby wybrać konkretną opcję.



Interfejs konsoli urządzenia: główne menu

Początkowo, interfejs konfiguracji urządzenia jest po angielsku.

Aby zmienić język interfejsu:

a. Wybierz **Konfiguracja Języka** z menu głównego.

b. Wybierz język z dostępnych opcji. Pojawi się nowa wiadomość potwierdzająca.

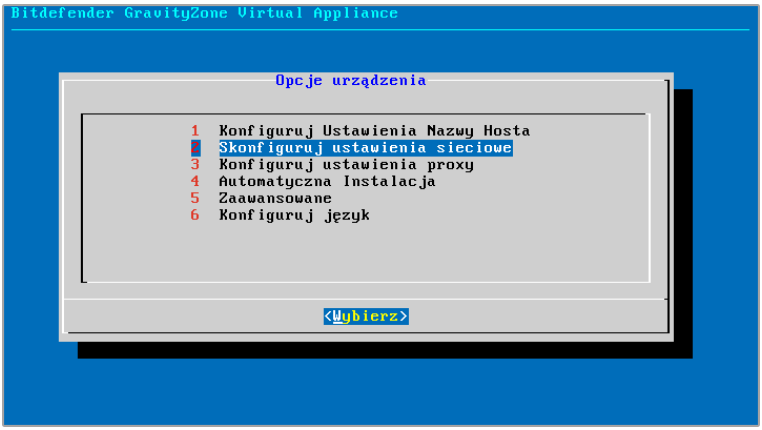
> **Notatka**
> Być może trzeba przewinąć w dół, aby zobaczyć swój język.

c. Wybierz **OK** aby zapisać zmiany.

7. Konfiguruj ustawienia sieciowe.

Można skonfigurować urządzenie, aby automatycznie uzyskać ustawienia sieciowe z serwera DHCP lub ręcznie skonfigurować ustawienia sieciowe. Jeśli zdecydujesz się skorzystać z DHCP, należy skonfigurować serwer DHCP, aby zarezerwować konkretny adres IP dla urządzenia.

a. Z menu głównego wybierz **Konfiguruj ustawienia sieciowe**.

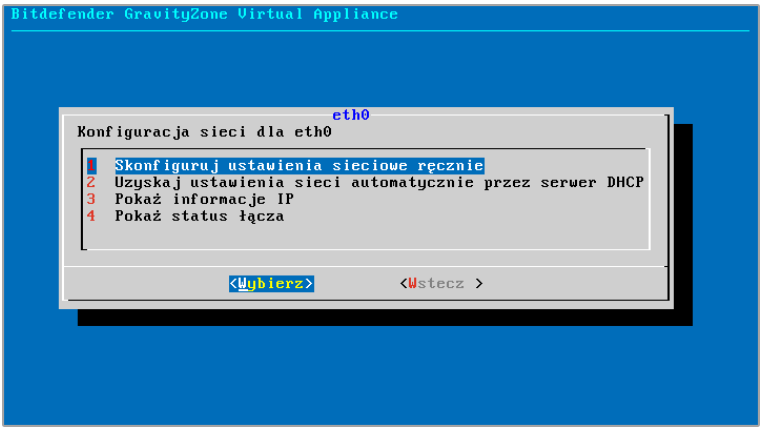


Interfejs konsoli urządzenia: opcja ustawień sieciowych

b. Wybierz interfejs sieciowy.

c. Wybierz metodę konfiguracji:

- **Skonfiguruj ustawienia sieciowe ręcznie.** Musisz określić adres IP, maskę sieci, adres bramy i adres serwera DNS.
- **Uzyskaj ustawienia sieci automatycznie przez serwer DHCP.** Użyj tej opcji tylko jeżeli masz skonfigurować serwer DHCP do zarezerwowania konkretnego adres IP dla urządzenia.



Interfejs konsoli urządzenia: ustawienia sieciowe

d. Możesz sprawdzić szczegóły dotyczące konfiguracji IP lub aktualny status połączenia, wybierając odpowiednie opcje.

8. Konfiguruj ustawienia nazwy hosta.

   Komunikacja z rolami GravityZone odbywa się za pomocą adresów IP lub nazwy DNS zainstalowanych urządzeń. Domyślnie, GravityZone elementy komunikują się używając adresu IP. Jeżeli chcesz włączyć komunikację przez nazwy DNS, musisz skonfigurowaćGravityZone urządzenia z nazwami DNS i upewnić się, że poprawnie rozpoznaje skonfigurowany adres IP urządzenia.

   Warunki wstępne:

   - Skonfiguruj rekord DNS na serwerze DNS.
   - Nazwa DNS musi być poprawie przypisana do skonfigurowanego adresu IP urządzenia. Dlatego należy upewnić się, że urządzenie jest skonfigurowane z prawidłowym adresem IP.

   Aby skonfigurować ustawienia nazwy hosta:

   a. Z menu głównego wybierz **Konfiguruj ustawienia nazwy hosta**.

   b. Wprowadź nazwę hosta urządzenia i nazwę domeny usługi Active Directory (w razie potrzeby).

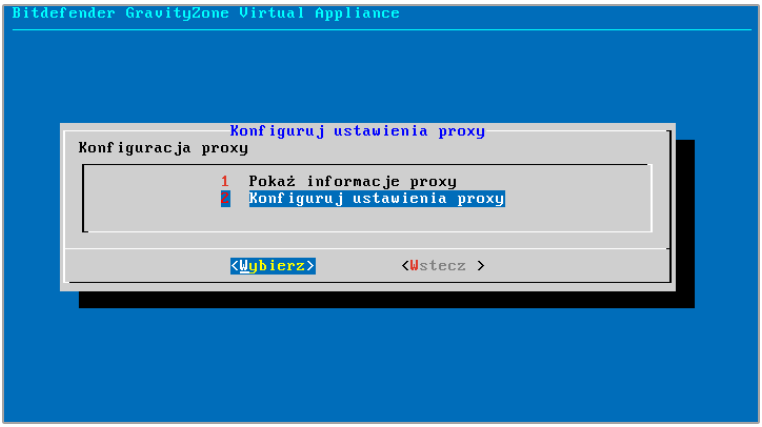
   c. Wybierz **OK** aby zapisać zmiany.

9. Konfiguruj ustawienia proxy.

   Jeśli urządzenie łączy się z Internetem przez serwer proxy, musisz skonfigurować ustawienia proxy:

   a. Z menu głównego wybierz **Konfiguruj ustawienia Proxy**.

   b. Wybierz **Konfiguruj ustawienia proxy**.



Interfejs konsoli urządzenia: skonfiguruj ustawienia proxy

   c. Podaj adres serwera proxy. Użyj poniższej składni:

   - Jeżeli serwer proxy nie wymaga uwierzytelniania:

     `http(s)://<IP/hostname>:<port>`

   - Jeżeli serwer proxy wymaga uwierzytelnianie:

     `http(s)://<username>:<password>@<IP/hostname>:<port>`

   d. Wybierz **OK** aby zapisać zmiany.

10. Zainstaluj role GravityZone. Możesz wybrać, czy chcesz zainstalować role ręcznie lub automatycznie. Podczas automatycznej instalacji wszystkie role są instalowane na tym samym urządzeniu. Podczas ręcznego instalowania urządzenia GravityZone, możesz je skonfigurować, na przykład, aby zainstalować tylko role, które potrzebujesz lub podłączyć do istniejącej instancji bazy danych.

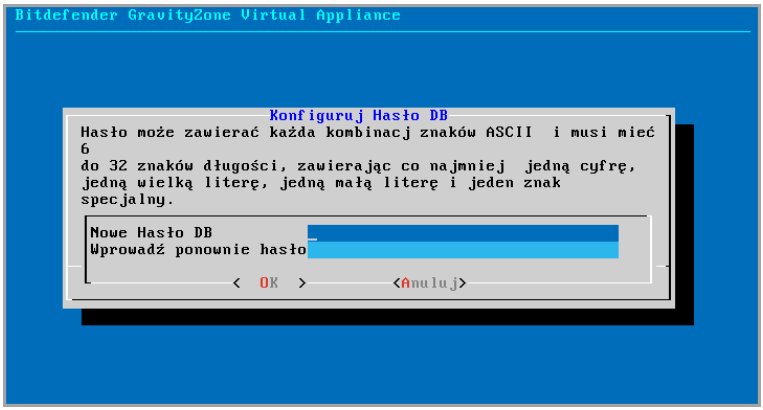
    - Aby automatycznie zainstalować role:

a. Z głównego menu, wybierz **Automatyczna Instalacja**. Zostaniesz poproszony, aby przeczytać i zaakceptować umowę EULA i pojawi się komunikat potwierdzenia, informujący o rolach, które zostaną zainstalowane.

> **Notatka**
> Security Server zostanie również zainstalowany, ale to będzie dostępne do użycia tylko wtedy, gdy pozwali na to klucz licencyjny.

b. Zaznacz **Tak**, aby potwierdzić.

c. Zostaniesz poproszony, aby skonfigurować hasło bazy danych. Hasło może zawierać każda kombinacj znaków ASCII i musi mieć 6 do 32 znaków długości, zawierając co najmniej jedną cyfrę, jedną wielką literę, jedną małą literę i jeden znak specjalny.

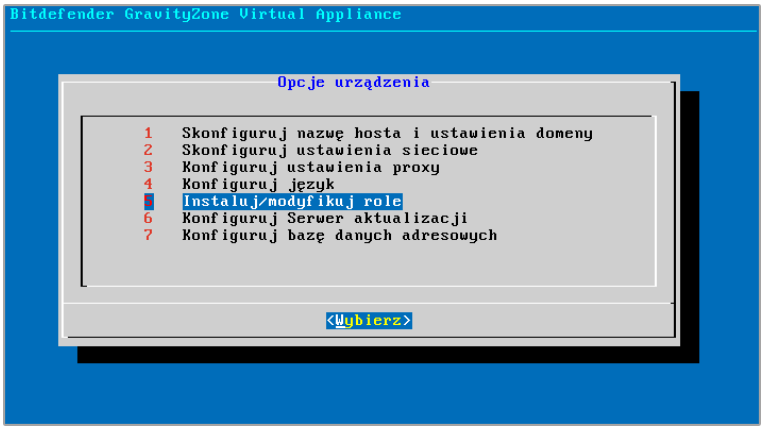


Interfejs konsoli urządzenia: skonfiguruj hasło bazy danych

> **Notatka**
> Ta opcja jest dostępna tylko w początkowej konfiguracji urządzenia GravityZone.

- Aby ręcznie zainstalować role:

  a. Z głównego menu, wybierz **Zaawansowane Ustawienia**.



Interfejs konsoli urządzenia: instalowanie ról

b. Wybierz **Zainstaluj/Odinstaluj Role**, aby zainstalować urządzenie w środowisku GravityZone z pojedynczym serwerem bazy danych.

> **Notatka**
> Jeśli zainstalowałeś urządzenie, aby rozszerzyć swoje środowisko GravityZone, patrz „Połącz z Istniejącą Bazą Danych" (p. 76).

c. Wybierz **Dodaj lub usuń role**. Pojawi się nowa wiadomość potwierdzająca.

d. Naciśnij `Enter`, aby kontynuować.

e. Naciśnij `Spację`, a następnie `Enter`, aby zainstalować rolę bazy danych serwera. Musisz potwierdzić swój wybór naciskając ponownie `Enter`.

f. Konfiguruj hasło bazy danych. Hasło może zawierać każda kombinacj znaków ASCII i musi mieć 6 do 32 znaków długości, zawierając co najmniej jedną cyfrę, jedną wielką literę, jedną małą literę i jeden znak specjalny.

g. Naciśnij `Enter` i poczekaj na zakończenie instalacji.

h. Zainstaluj inne role wybierając **Dodaj lub usuń role** z menu **Instaluj/Odinstaluj Role** i wybierz role do instalacji. Naciśnij `Spację`, aby wybrać rolę, a następnie `Enter`, aby kontynuować. Musisz potwierdzić

swój wybór klikając ponownie `Enter` i następnie zaczekać na zakończenie instalacji.

Notatka

Instalowanie każdej roli trwa kilka minut. Podczas instalacji, wymagane pliki są sciągane z internetu. instalacja może zająć więcej czasu jeżeli połączenie internetowe jest wolne. Jeżeli instalacja zawiesza się, przesuń urządzenie.

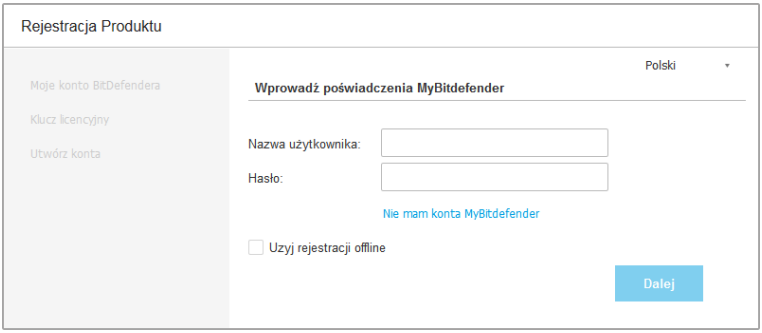
Podczas wdrażania i zakładania urządzenia GravityZone, możesz w każdej chwili edytować ustawienia urządzenia używając interfejsu konfiguracji. Aby uzyskać więcej informacji na temat GravityZone konfiguracji urządzenia, zobacz „Zarządzanie Urządzeniem GravityZone" (p. 70).

3.1.3. Control Center Ustawienia początkowe

Po wdrożeniu i ustawieniu urządzenia GravityZone, należy uzyskać dostęp do interfejsu WWW Control Center i skonfigurować konto administratora firmy.

1. W pasku adresu przeglądarki internetowej wpisz adres IP lub nazwę hosta DNS Control Center urządzenia (używając `https://` prefiks). Wyświetlone zostanie kreator konfiguracji.
2. Musisz najpierw zarejestrować wdrożenie GravityZone do konta Bitdefender. Podaj nazwę użytkownika i hasła dla twojego konta Bitdefender. Jeżeli jeszcze nie masz konta Bitdefender, naciśnij na odpowiedni link, aby utworzyć.

   Jeśli połączenie z Internetem nie jest dostępne, wybierz **Użyj rejestracji offline**. W tym przypadku, konto Bitdefender nie jest wymagane.

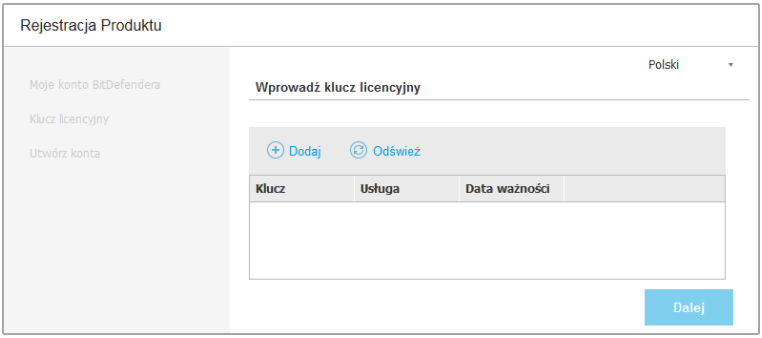


Ustawienia początkowe - konta MyBitdefender

3. Kliknij **Dalej** aby kontynuować.
4. Dostarczone klucze licencyjne potrzebne do zatwierdzenia zakupionych usług bezpieczeństwa GravityZone. Sprawdź rejestracje wersji próbnej lub email zakupu aby znaleźć twoje klucze licencyjne.
   a. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli. Wyświetlone zostanie okno konfiguracji.
   b. Wybierz typ rejestracji licencji (online lub offline).
   c. Podaj klucz licencyjny w polu **Klucz licencyjny**. Dla rejestracji offline, będzie wymagane podanie kodu rejestracyjnego.
   d. Poczekaj chwilę aż klucz licencyjny zostanie zatwierdzony. Kliknij **Dodaj**, aby zakończyć.

   Klucz licencyjny pojawi się w tabeli licencyjnej. Możesz zobaczyć usługi bezpieczeństwa, status, datę wygaśnięcia i aktualne zużycie każdego klucza licencyjnego w odpowiedniej kolumnie.

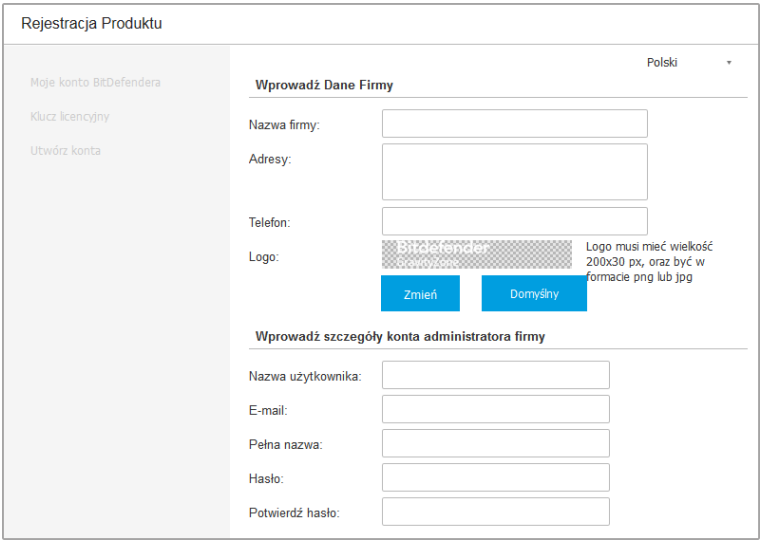
   Notatka
   Podczas ustawień poczatkowych, ostatni ważny klucz licencyjny musi być uzuyty do rozpoczęcia użytkowania GravityZone. Możesz później dodać więcej kluczy licencyjnych lub modyfikować istniejące.



Ustawienia początkowe - Zapewnienie kluczy licencyjnych

5. Kliknij **Dalej** aby kontynuować.
6. Uzupełnij informacje Twojej firmy, takie jak nazwa firmy, adres i telefon.

7. Możesz zmienić logo wyświetlane w Control Center jak również w raporcie twojej firmy i powiadomieniach e-mail, według poniższych:
   - Naciśnij **Zmiana** aby przeglądać obrazy logo na twoim komputerze. Obraz musi być w formacie .png lub .jpg i wielkość obrazu musi wynosić 200x30 pikseli.
   - Naciśnij **Domyślne** aby usunąć obraz i zresetować obraz do domyślnie dostarczonego przez Bitdefender.
8. Podać wymagane dane do konta administratora firmy: nazwa użytkownika, adres e-mail i hasło. Hasło musi zawierać co najmniej jedną wielką liter, co najmniej jedną małą literę i co najmniej jedną cyfrę lub jeden znak specjalny.



Wstępna konfiguracja - Skonfiguruj swoje konto

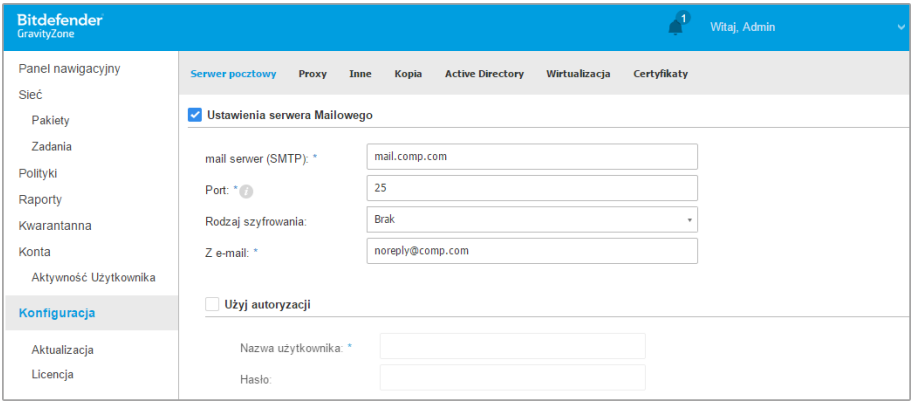
9. Kliknij **Utwórz konto**.

Konto administracyjne firmy zostanie stworzone i automatycznie zostaniesz zalogowany do nowego konta Bitdefender Control Center.

3.1.4. Konfiguruj ustawienia Control Center

Po ustawieniach początkowych, potrzebujesz skonfigurować ustawienia Control Center Jako Administrator Firmy, możesz zrobić poniższe:

- Skonfiguruj mail, proxy i inne ogólne ustawienia.
- Uruchom i zaplanuj Control Center zapasowe bazy danych.
- skonfiguruj integracje z Active Directory oraz narzędzia zarządzania wirtualizacją (vCenter Serwer, XenServer).
- Zainstaluj certyfikaty bezpieczeństwa.



Ustawienia serwera Mailowego

Serwer pocztowy

Control Center wymaga zewnętrznego serwera poczty do wysyłania komunikatów e-mail.

Notatka
Zaleca się utworzenie specjalnego konta pocztowego używanego przez Control Center.

Włącz Control Center, aby wysłać e-maile:

1. Przejdź do strony **Konfiguracja**.
2. Wybierz zakładkę **Mail Serwer**.

3. Wybierz **Ustawienia Serwera Poczty** i skonfiguruj wymagane ustawienia:
   - **mail serwer (SMTP).** Wpisz adres IP lub nazwę host serwera mailowego, który będzie wysyłał e-maile.
   - **Port.** Wpisz port używany do połączenia z serwerem poczty.
   - **Rodzaj szyfrowania.** Jeśli serwer poczty wymaga zaszyfrowanego połączenia, wybierz odpowiedni typ z menu (SSL, TLS lub STARTTLS).
   - **E-mail.** Wpisz adres e-mail, który ma się pojawiać w wiadomości e-mail w polu Od (adres e-mail nadawcy).
   - **Użyj autoryzacji.** Zaznacz to pole wyboru, jeśli serwer poczty wymaga uwierzytelniania. Musisz podać prawidłową nazwę użytkownika / adres e-mail i hasło.
4. Kliknij **Zapisz**.

Control Center automatyczne sprawdza ustawienia poczty podczas zapisu. Jeżeli dostarczone ustawienia nie mogą zostać potwierdzone, komunikat błędu informuje o niepoprawnych ustawieniach. Popraw ustawienia i spróbuj ponownie.

Proxy

Jeśli Twoja firma łączy się z Internetem przez serwer proxy, musisz skonfigurować ustawienia proxy:

1. Przejdź do strony **Konfiguracja**.
2. Wybierz zakładkę **Proxy**.
3. Wybierz **Używaj ustawień Proxy** i skonfiguruj wymagane ustawienia:
   - **Adres** - wpisz adres IP serwera proxy.
   - **Port** – wpisz port używany do łączenia z serwerem proxy.
   - **Nazwa użytkownika** - wpisz nazwę użytkownika rozpoznawanego przez proxy.
   - **Hasło proxy** - wpisz poprawne hasło dla wcześniej podanego użytkownika.
4. Kliknij **Zapisz**.

Inne

Na stronach **Konfiguracja** > **Różne** możesz skonfigurować poniższe ustawienia ogólne:

- **Gdy potrzebny jest niedostępny obraz Security Server.** Urządzenie GravityZone nie zawiera domyślnie obrazów maszyn wirtualnych Security Server. Jeśli administrator próbuje pobrać obraz Security Server lub uruchomić zadanie instalacji Security Server, działanie nie powiedzie się. Możesz skonfigurować automatyczną działanie dla tej sytuacji, wybierając jedną z następujących opcji:
  - **Automatycznie pobierz obraz**
  - **Powiadom administratora i nie pobieraj**

  Notatka

  Aby uniknąć zakłóceń w pracy administratora, można ręcznie pobrać niezbędne paczki Security Server ze strony **Aktualizacja**, w zakładce **Aktualizacja Produktu**. Aby uzyskać więcej informacji, odwołaj się do „Pobieranie Aktualizacji Produktu" (p. 134).

- **Gdy potrzebna jest niedostępna paczka.** Możesz skonfigurować automatyczną działanie dla tej sytuacji, wybierając jedną z następujących opcji:
  - **Pobierz paczkę automatycznie**
  - **Powiadom administratora i nie pobieraj**
- **Współbieżne wdrożenia.** Administratorzy mogą zdalnie wdrożyć komponenty bezpieczeństwa uruchamiając zadania instalacji. Użyj tej opcji aby określić maksymalną liczne jednoczesnych wdrożeń, które mogą być wykonywane w tym samym czasie.

  Na przykład, jeżeli maksymalna liczna aktualnych wdrożeń to 10 i zdalna instalacja klienta jest przypisana do 100 komputerów, Control Center zainicjuje wysłanie 10 pakietów instalacyjnych w sieci. W tym przypadku, instalacja klienta jest wykonywana jednocześnie na maksymalnie 10 komputerach, wszystkie inne podzadania będą czekać na swoją kolej. Tak długo jak pod zadania są wykonane, inny pakiet instalacyjny jest wysłany i tak dalej.
- **Użyj wdrożenia SSH zamiast określonych metod integracji.** Wybierz tę opcję jeśli preferujesz używanie wdrożenia SSH zamiast innych określonych metod integracji, takich jak VIX API.

- **Ustawienia serwera NTP**. Serwer NTP jest używany do synchronizacji czasu pomiędzy wszystkimi urządzeniami GravityZone. Domyślny adres serwera NTP jest zapewniony, możesz go zmienić w polu **Adres Serwera NTP**.

  Notatka
  Dla urządzeń GravityZone do komunikacji z Serwerem NTP, 123 (UDP) port musi byc otwarty.

- **Włączone Syslog**. Przez włączenie tej funkcji, zezwolisz GravityZone wysyłać powiadomienia do zalogowanych serwerów o używanym protokole Syslog. W ten sposób masz możliwość, aby lepiej monitorować zdarzenia GravityZone.

  Aby wyświetlić lub skonfigurować listę powiadomień wysyłaną do Syslog server, odwołaj się do rozdziału **Powiadomienia** z Przewodnika Administratora GravityZone.

  Aby włączyć logowanie do zdalnego serwera Syslog:

  1. Zaznacz pole wyboru **Włącz Syslog**.
  2. Podaj nazwę serwera lu IP, preferowany protokół i port nasłuchiwania Syslog.
  3. Naciśnij przycisk ⊕ **dodaj**a kolumny **Działanie**.

Naciśnij **Zapisz** aby zastosować zmiany.

Kopia

Upewnij się, że twoje Control Center dane są bezpieczne, możesz chcieć zrobić kopie zapasową bazy danych GravityZone. Możesz uruchomić tyle ile chcesz kopii zapasowych bazy danych jak, lub zaplanować okresowe tworzenie kopii zapasowych automatycznie w określonych przedziałach czasu.

Każda komenda tworzy tworzy kopie bazy danych w pliku `tgz` (GZIP Skompresowany plik archiwum Tar) w lokalizacji określonej w ustawieniach kopii zapasowej.

Kiedy kilku administratorów zarządza przywilejami w ustawieniach Control Center, możesz skonfigurować **Ustawienia Powiadomień** aby otrzymywać powiadomienia, za każdym razem jak kopia zapasowa bazy danych zostanie utworzona. Aby uzyskać więcej informacji, zajrzyj do rozdziału **Powiadomienia** w Przewodniku Administratora GravityZone.

Tworzenie Backupów Baz Danych

Aby uruchomić kopię zapasową Bazy Danych

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Backup**.
2. Kliknij przycisk **Kopia Zapasowa Teraz** w górnej części tabeli. Wyświetlone zostanie okno konfiguracji.
3. Wybierz gdzie ma zostać zapisana kopia zapasowa:
   - **Lokalnie**, dla zapisu kopi zapasowej archiwum dla urzadzenia GravityZone. W tym przypadku, nalezy okreslić ścieżkę do konkretnego katalogu z urządzenia GravityZone w którym zostanie zapisane archiwum.

     Urządzenie GravityZone ma strukturę katalogów Linux. Na przykład, możesz wybrać żeby utworzyć kopie zapasową w katalogu `tmp`. W tym przypadku, wpisz `/tmp` w polu **Ścieżka**.
   - **FTP**, dla zapisu kopi archiwum na serwerze FTP. W tym przypadku, wpisz szczegóły FTP w poniższych polach.
   - **FTP**, dla zapisu kopi archiwum na serwerze w sieci. W tym przypadku, wpisz ścieżkę do lokalizacji w sieci, które potrzebujesz (np. `\\computer\folder`), nazwa domeny i dane logowania użytkownika.
4. Kliknij przycisk **Ustawienia testowe**. Powiadomienie tekstowe poinformuje Cię, czy określone ustawienia są ważne lub nieważne.

   aby utworzyć kopie zapasową, wszystkie ustawienia muszą być ważne.
5. Kliknij **Wygeneruj**. Strona **Backup** będzie wyświetlana. Nowy wpis kopi zapasowej zostanie dodany do listy. Sprawdź **Status** nowej kopii zapasowej. Gdy backup będzie zakończony, znajdziesz archiwum `tgz` w określonej lokalizacji.

> **Notatka**
> Lista dostępna na stronie **Backup** zawiera logi wszystkich utworzonych backup'ów. Te logi nie zapewniają dostępu do archiwów kopii zapasowych, wyświetlają one tylko szczegóły tworzonych kopii zapasowych.

Aby zaplanować kopię zapasową Bazy Danych:

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Backup**.
2. Kliknij przycisk **Ustawiania Kopii Zapasowej** w górnej części tabeli. Wyświetlone zostanie okno konfiguracji.

3. Wybierz **Harmonogram Kopi Zapasowej**.
4. Skonfiguruj częstotliwość tworzenia kopii zapasowych (dzienny, tygodniowy, miesięczny) i czas rozpoczęcia.

   Na przykład, możesz zaplanować tworzenie kopii zapasowych co tydzień, w każdy piątek, począwszy od 22:00.
5. Konfiguruj zaplanowaną lokalizację kopii zapasowych.
6. Wybierz gdzie ma zostać zapisana kopia zapasowa:
   - **Lokalnie**, dla zapisu kopi zapasowej archiwum dla urzadzenia GravityZone. W tym przypadku, nalezy okreslić ścieżkę do konkretnego katalogu z urządzenia GravityZone w którym zostanie zapisane archiwum.

     Urządzenie GravityZone ma strukturę katalogów Linux. Na przykład, możesz wybrać żeby utworzyć kopie zapasową w katalogu `tmp`. W tym przypadku, wpisz `/tmp` w polu **Ścieżka**.
   - **FTP**, dla zapisu kopi archiwum na serwerze FTP. W tym przypadku, wpisz szczegóły FTP w poniższych polach.
   - **FTP**, dla zapisu kopi archiwum na serwerze w sieci. W tym przypadku, wpisz ścieżkę do lokalizacji w sieci, które potrzebujesz (np. `\\computer\folder`), nazwa domeny i dane logowania użytkownika.
7. Kliknij przycisk **Ustawienia testowe**. Powiadomienie tekstowe poinformuje Cię, czy określone ustawienia są ważne lub nieważne.

   aby utworzyć kopie zapasową, wszystkie ustawienia muszą być ważne.
8. Kliknij **Zapisz**, aby zaplanować kopię zapasową.

Przywracanie Kopii Zapasowej Bazy Danych

Gdy z różnych powodów Twoja instancja GravityZone pracuje nieprawidłowo (nieudana aktualizacja, dysfunkcyjny interfejs, uszkodzone pliki, błędy, itp.), możesz przywrócić bazy danych GravityZone z kopii zapasowej używając:

- To samo urządzenie
- Świeży obraz GravityZone
- Funkcja Replica Set

Wybierz opcję, która najbardizej pasuje do sytuacji i kontynuuj procedurę przywracania dopiero po uważnym przeczytaniu przesłanek opisanych poniżej.

Przywracanie bazy danych do tego samego VA GravityZone

Warunki wstępne

- Połączenie SSH do urządzenia GravityZone, za pomocą uprawnień **roota**.

  Możesz użyć poświadczeń **putty** i **dadmin**, aby połączyć się z urządzeniem przez SSH, a następnie uruchomić polecenie `sudo su`, aby przejść do konta **root**.
- Infrastruktura GravityZone nie zmieniła się od backupu.
- Oba pliki backupu (**.json** i **.tgz**) są dostępne.
- W architekturze rozproszonej, GravityZone nie został skonfigurowany do korzystania z replikacji bazy danych (Replica Set).

  Aby zweryfikować konfigurację, wykonaj następujące kroki:

  1. Otwórz plik `/etc/mongodb.conf`.
  2. Sprawdź, `replSet` nie jest skonfigurowany, tak jak w poniższym przykładzie:

     ```
     # replSet = setname
     ```

  Notatka
  Aby przywrócić bazę danych, gdy włączony jest w Replica Set, przejdź do „Przywracanie bazy danych w środowisku Replica Set" (p. 59).

- Żaden proces CLI nie jest uruchomiony.

  Aby się upewnić, że wszystkie procesy CLI są zatrzymane, uruchom następującą komendę.

  ```
  # killall -9 perl
  ```

- Pakiet **mongoconsole** jest zainstalowany na urządzeniu.

  Aby sprawdzić, czy warunek jest spełniony, należy uruchomić polecenie:

  ```
  # /opt/bitdefender/bin/mongoshellrestore --version
  ```

Komenda nie powinna zwracać żadnych błędów, w przeciwnym razie wykonaj:

```
# apt-get update
# apt-get install --upgrade mongoconsole
```

Przywracanie bazy danych

1. Wyodrębnij pliki z archiwum kopii zapasowych:

```
# cd /directory-z kopią zapasową
# tar -xvf gz-backup.tgz
```

, gdzie **directory-bez-kopii zapasowej** jest ścieżką do miejsca, w którym zostały zapisane pliki kopii zapasowych i **gz-backup.tgz** jest plikiem archiwum **.tgz** z wybranej kopii zapasowej.

Pliki są rozpakowywane w nowym folderze o tej samej nazwie co plik **.tgz** w bieżącym katalogu. Pliki są rozpakowywane w nowym folderze o tej samej nazwie co plik **.tgz** w bieżącym katalogu.

Na przykład:

```
# cd /tmp/backup
# tar -xvf gz-backup-2014-11-24_16h20m.tgz
# ls
gz-backup-2014-11-24_16h20m.json gz-backup-2014-11-24_16h20m.tgz
gz-backup-2014-11-24_16h20m
```

2. Przywróć bazę danych.

```
# nohup /opt/bitdefender/bin/mongoshellrestore --drop -u bd -p \
Twoje _hasłodirectory-z kopią zapasowągz-backup
/directory-z kopią zapasową
/directory-z kopią zapasową
/directory-z kopią zapasową
```

, gdzie **twoje_hasło** jest hasłem bazy danych, które ustawiasz w Interfejsie Wiersza Poleceń Urządzenia GravityZone.

Polecenie przywrócenia tworzy dwa pliki dziennika w katalogu z kopią zapasową: **restore.log**, **restore-err.log**.

Na przykład:

```
# nohup /opt/bitdefender/bin/mongoshellrestore --drop -u bd -p \
Twoje _hasłotmp/backupgz-backup-2014-11-24_16h20m
/tmp/backuptmp/backup
/tmp/backup
```

3. Poczekaj, aż żadna nowa wiadomość nie będzie wyświetlana na ekranie, a następnie naciśnij `CTRL + C`.
4. Restartuj urządzenie(a) GravityZone. Przywrócenie bazy danych zostało zakończone.

Przywracanie bazy danych z wycofanego z użytku VA GravityZone

Warunki wstępne

- Świeża instalacja VA GravityZone:
  - Z tym samym IP, co stare urządzenie
  - Mając **tylko** zainstalowaną rolę Serwera Bazodanowego.

  Możesz pobrać obraz VA GravityZone stąd.
- Połączenie SSH do urządzenia wirtualnego GravityZone, za pomocą uprawnień **roota**.
- Infrastruktura GravityZone nie zmieniła się od wykonania backupu.
- Oba pliki backupu (**.json** i **.tgz**) są dostępne.
- W architekturze rozproszonej, GravityZone nie został skonfigurowany do korzystania z replikacji bazy danych (Replica Set).

  Jeśli używasz Replica Set, w swoim środowisku GravityZone, masz również zainstalowaną rolę Serwera Bazodanowego na innych instancjach urządzenia.

  Aby przywrócić bazę danych, gdy włączony jest w Replica Set, przejdź do „Przywracanie bazy danych w środowisku Replica Set” (p. 59).

Przywracanie bazy danych

1. Przerwij VASync.

```
# stop vasync
```

2. Wyodrębnij pliki z archiwum kopii zapasowych:

```
# cd /directory-z kopią zapasową
# tar -xvf gz-backup.tgz
```

, gdzie **directory-bez-kopii zapasowej** jest ścieżką do miejsca, w którym zostały zapisane pliki kopii zapasowych i **gz-backup.tgz** jest plikiem archiwum **.tgz** z wybranej kopii zapasowej.

Pliki są rozpakowywane w nowym folderze o tej samej nazwie co plik **.tgz**, (**gz-backup**), w bieżącym katalogu.

Na przykład:

```
# cd /tmp/backup
# tar -xvf gz-backup-2014-11-24_16h20m.tgz
```

3. Przywróć bazę danych.

```
# nohup /opt/bitdefender/bin/mongoshellrestore --drop -u bd \
-p Twoje _hasłodirectory-z kopią zapasowągz-backup
/directory-z kopią zapasową
/directory-z kopią zapasową
/directory-z kopią zapasową
```

, gdzie **twoje_hasło** jest hasłem bazy danych, które ustawiasz w Interfejsie Wiersza Poleceń Urządzenia GravityZone.

Polecenie przywrócenia tworzy dwa pliki dziennika w katalogu z kopią zapasową: **restore.log**, **restore-err.log**.

Na przykład:

```
# nohup /opt/bitdefender/bin/mongoshellrestore --drop -u bd -p \
Twoje _hasłotmp/backup/gz-backup-2014-11-24_16h20m
/tmp/backuptmp/backup
tail -f /tmp/backup
```

4. Poczekaj, aż żadna nowa wiadomość nie będzie wyświetlana na ekranie, a następnie naciśnij `CTRL + C`.
5. Przywrócenia ID starego urządzenia:

```
# /opt/bitdefender/bin/mongoshell -u bd -p Twoje _hasło
--eval print(db.applianceInstalls.findOne({name:'db'}).\
applianceId)" --quiet > /opt/bitdefender/etc/applianceid
```

, gdzie **twoje_hasło** jest hasłem bazy danych, które ustawiasz w Interfejsie Wiersza Poleceń Urządzenia GravityZone.

6. Zanotuj jakiekolwiek inne role, które zostały zainstalowane z kopii zapasowej.
7. Usuń stare role z bazy danych.

```
# /opt/bitdefender/bin/mongoshell -u bd -p Twoje _hasło
--eval "db.applianceInstalls.remove({ip:db.applianceInstalls.\
findOne({name:'db'}).ip,name:{'$ne': 'db'}});" --quiet
```

, gdzie **twoje_hasło** jest hasłem bazy danych, które ustawiasz w Interfejsie Wiersza Poleceń Urządzenia GravityZone.

8. Rozpocznij VASync.

```
# start vasync
```

9. Przeinstaluj pozostałe role, które wcześniej były na urządzeniu.
10. Restartuj urządzenie(a) GravityZone. Przywrócenie bazy danych zostało zakończone.

Przywracanie bazy danych w środowisku Replica Set

Jeżeli wdrożyłeś bazę danych w środowisku Replica Set możesz znaleźć oficjalną procedurę przywracania w podręczniku online mongoDB (tylko w języku angielskim).

Notatka
Procedura wymaga zaawansowanych umiejętności technicznych i powinna być wykonywana jedynie przez wykwalifikowanego inżyniera. Jeśli napotkasz trudności, prosimy o kontakt z naszym Wsparciem Technicznym, aby pomóc Ci w przywróceniu bazy danych.

Domeny Active Directory

Poprzez integracje z Active Directory, istniejące zasoby Active Directory są importowane do Control Center, uproszczone jest wdrażanie bezpieczeństwa, zarządzanie monitorowaniem i raportowaniem. Dodatkowo, użytkownikom usługi Active Directory mogą być przypisane różne role w Control Center.

Jeśli jest potrzeba, możesz wybrać, w których Kontrolerach Domeny Active Directory jest wykonana integracja.

Żeby zintegrować i zsynchronizować Control Center z domeny Active Directory:

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Active Directory**.
2. Wybierz **Synchronizuj z usługą Active Directory** i skonfiguruj wymagane ustawienia:
   - Interwał synchronizacji (w godzinach)
   - Nazwa domeny Active Directory (łącznie z rozszerzeniem domeny)
   - Nazwa użytkownika i hasło administratora domeny
   - Opcjonalnie, wyświetlono jeden lub więcej Kontroler Domeny z tabeli **Żądaj Kontrolera Domeny**
3. Kliknij **Zapisz**.

WAŻNE
Kiedy hasło użytkownika zostanie zmienione, pamiętaj aby uaktualnić to w Control Center.

Wirtualizacja

Control Center jest zintegrowana z VMware vCenter Serwer i Citrix XenServer.

- „Integracja z Serwerem vCenter" (p. 60)

- „Integracja z Serwerem XenServer" (p. 63)

WAŻNE
Kiedy ustawiasz nowa integracje z innym serwerem vCenter lub systemem XenServer, pamiętaj aby przejrzeć i uaktualnić przywileje dostępu dla istniejących użytkowników.

Integracja z Serwerem vCenter

Możesz zintegrować Control Center z jednym albo wieloma Systemami serwera vCenter. Systemy serwera vCenter w trybie powiązań muszą być dodawane oddzielnie do Control Center.

aby ustawić integracje z Serwerem vCenter:

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Wirtualizacja**.
2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli i wybierz **vCenter Serwer** z menu. Wyświetlone zostanie okno konfiguracji.
3. Określ szczegóły vCenter Serwer.
   - Nazwa systemu vCenter Server w Control Center
   - Nazwa Hosta lub adresu IP systemu serwera vCenter
   - port Servera vCenter (domyślny `443`)
4. Określ dane logowania, które maja zostać użyte do uwierzytelnienia z serwerem vCenter. Możesz wybrać, aby korzystanie z danych dostarczonych do integracji z Active Directory lub innego zestawu poświadczeń. Użytkownik, którego poświadczenia dostarczasz musi mieć uprawnienia administratora lub roota na serwerze vCenter.
5. Wybierz platformę VMware zainstalowaną w Twoim środowisku i skonfiguruj odpowiednio ustawienia:
   - **Brak**. Wybierz tę opcję, jeśli nie ma zainstalowanej konkretnej platformy VMware.
   - **vShield**. Określ szczegóły systemu vShield Menedżer zintegrowanego z serwerem vCenter.
     - Nazwa Hosta lub adresu IP systemu menadżera vShield
     - port vShield Menadżer (domyślny `443`)
   - **NSX**. Określ szczegóły Managera NSX zintegrowanego z vCenter Server.
     - Nazwa hosta lub adres IP Managera NSX
     - port NSX Menadżer (domyślny `443`)

– Nazwa użytkownika i hasło używane do uwierzytelniania na NSX Manager.

  Te poświadczenia będą zapisane na chronionym wpisie, nie w Managerze Poświadczeń.

– Zaznacz pole wyboru **dodaj etykietę jeśli wirus został znaleziony** aby korzystać z domyślnych etykiet ochrony NSXa, kiedy malware jest znaleziony na wirtualnej maszynie.

  Maszyna może być tagowana przez trzy różne tagi bezpieczeństwa, w zależności od poziomu ryzyka zagrożenia.

  - `ANTI_VIRUS.VirusFound.threat=low`, stosowana na maszynie, gdy Bitdefender wyszukuje szkodliwe oprogramowanie niskiego ryzyka, które może usunąć.
  - `ANTI_VIRUS.VirusFound.threat=medium`, stosowanie na maszynie jeżeli Bitdefender nie może usunąć zainfekowanych pliki, ale zamiast tego dezynfekuje je.
  - `ANTI_VIRUS.VirusFound.threat=high`, zastosowanie na maszynie jeżeli Bitdefender nie może ani usunąć ani wyleczyć zainfekowanych pliki, ale blokuje dostęp do nich.

  Gdy zagrożenia o różnym stopniu ryzyka są wykrywane na tej samej maszynie, wszystkie powiązane tagi będą zastosowane. Na przykład, maszyna, na której stwierdzono wysokie i niskie ryzyko szkodliwego oprogramowania będą miały oba znaczniki bezpieczeństwa.

  Notatka
  Można znaleźć tagi bezpieczeństwa w VMware vSphere, pod **Networking & Bezpieczeństwo > NSX Managers >** `NSX Manager` **> Manage > Tagi bezpieczeństwa** tab.
  Chociaż można utworzyć tak wiele tagów ile chcesz, to tylko trzy wymienione tagi działają z Bitdefender.

6. **Ogranicz przypisanie polityki z widoku sieci**. Użyj tej opcji w celu kontrolowania dostępu administratora sieci mającego na celu zmianę polityk maszyn wirtualnych poprzez **Komputery i Maszyny Wirtualne** wyświetlane na stronie **Sieci**. Gdy ta opcja jest zaznaczona, administratorzy mogą zmienić politykę maszyn wirtualnych tylko z widoku inwentaryzacji sieci **Maszyny Wirtualne**.

7. Kliknij **Zapisz**. Zostaniesz poproszony, aby zaakceptować certyfikaty bezpieczeństwa vCenter Server i NSX Manager. Certyfikaty te zapewniają bezpieczną komunikację pomiędzy GravityZone oraz komponenty VMware, rozwiązanie ryzyko an-in-the-middle attacks.

   Możesz sprawdzić, czy poprawne certyfikaty zostały zainstalowane poprzez sprawdzenie informacji w witrynie przeglądarki dla każdego komponentu VMware na podstawie informacji certyfikatu wyświetlonego w polu Control Center.

8. Zaznacz pola wyboru, aby zaakceptować używane certyfikaty.
9. Kliknij **Zapisz**. Będziesz mógł zobaczyć vCenter Server na liście aktywnych integracji.
10. Jeśli korzystasz z platformy NSX:
    a. Przejdź do zakładki **Aktualizacja > Komponenty**.
    b. Pobierz i następnie opublikuj paczkę **Security Server (VMware z NSX)**. Aby uzyskać więcej informacji jak aktualizować komponenty GravityZone, przejdź do „Aktualizowanie GravityZone" (p. 132).
    c. Przejdź do zakładki **Konfiguracja > Wirtualizacja**.
    d. W kolumnie **Akcja**, Kliknij przycisk **Zarejestruj** odpowiadający za vCenter zintegrowany z NSX zarejestrować usługę Bitdefender z VMware NSX Manager.

Ostrzeżenie
Gdy certyfikat bezpieczeństwa wygasł i vCenter próbuje zsynchronizować, Pop-up poprosi o aktualizacje. Otwórz okno konfiguracji integracji vCenter Serwer, kliknij **Zapisz**, zaakceptuj nowe certyfikaty, a następnie kliknij **Zapisz** ponownie.

Po rejestracji Bitdefender dodaje się do konsoli VMware vSphere:
- Usługa Bitdefender
- Manager usług Bitdefender
- Trzy nowe domyślne profile dla tolerancyjnych, normalnych i agresywnych trybów skanowania.

Notatka
Możesz zobaczyć te profile usług także na stronie **Polityki** Control Center. Kliknij przycisk **Kolumny** po prawej stronie prawego panelu, aby zobaczyć dodatkowe informacje.

Na końcu, możesz zobaczyć, że Serwer vCenter synchronizuje się. Odczekaj kilka minut, aż do zakończenia synchronizacji.

Integracja z Serwerem XenServer

Możesz zintegrować Control Center z jednym albo wieloma Systemami serwera XenServer.

aby ustawić integracje z Serwerem XenServer:

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Wirtualizacja**.
2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli i wybierz **XenServer** z menu. Wyświetlone zostanie okno konfiguracji.
3. Określ szczegóły XenServer Serwer.
   - Nazwa systemu XenServer w Control Center
   - Nazwa Hosta lub adresu IP systemu XenServer
   - port XenServer (domyślny `443`)
4. Określ dane logowania, które maja zostać użyte do uwierzytelnienia z serwerem XenServer. Możesz wybrać, aby korzystanie z danych dostarczonych do integracji z Active Directory lub innego zestawu poświadczeń.
5. **Ogranicz przypisanie polityki z widoku sieci**. Użyj tej opcji w celu kontrolowania dostępu administratora sieci mającego na celu zmianę polityk maszyn wirtualnych poprzez **Komputery i Maszyny Wirtualne** wyświetlane na stronie **Sieci**. Gdy ta opcja jest zaznaczona, administratorzy mogą zmienić politykę maszyn wirtualnych tylko z widoku inwentaryzacji sieci **Maszyny Wirtualne**.
6. Kliknij **Zapisz**. Będziesz mógł zobaczyć vCenter Server na liście aktywnych integracji i że jest w trakcie synchronizacji. Odczekaj kilka minut, aż do zakończenia synchronizacji.

Zarządzanie Integracjami

Aby edytować i aktualizować szczegóły integracji:

1. W Control Center, przejdź do zakładki **Konfiguracja > Wirtualizacja**.
2. Naciśnij przycisk ✎ **Edytuj** w kolumnie **Działanie**.
3. Skonfiguruj ustawienia reguł według potrzeb. Aby uzyskać więcej informacji, przejdź do następującej sekcji, zależnie od sytuacji:
   - „Integracja z Serwerem vCenter” (p. 60)
   - „Integracja z Serwerem XenServer” (p. 63)

4. Kliknij **Zapisz**. Poczekaj kilka minut, aż do ponownej synchronizacji serwera.

Aby usunąć integrację vShield:

1. W Control Center, przejdź do zakładki **Konfiguracja > Wirtualizacja**.
2. Kliknij przycisk ⊖ **Usuń** w kolumnie **Akcja**, odpowiadający integracji, która ma być usunięta.
3. Kliknij **Tak**, aby potwierdzić akcję.

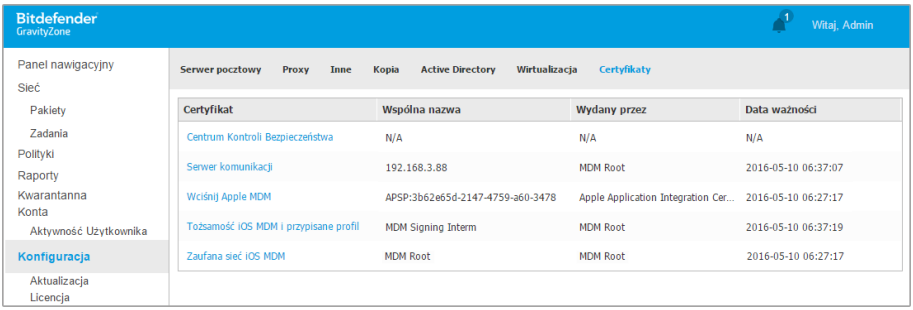
Aby usunąć integrację NSX:

1. Zaloguj się do konsoli VMware vSphere i usuń wszystkie polityki Bitdefender i Security Server.
2. W Control Center, przejdź do zakładki **Konfiguracja > Wirtualizacja**.
3. W kolumnie **Akcja**, odpowiadającej integracji, która ma zostać usunięta, kliknij ⊗ **Wyrejestruj** a następnie ⊖ **Usuń**.
4. Kliknij **Tak**, aby potwierdzić akcję.

Aby upewnić się, że zostają wyświetlane najnowsze informacje, kliknij przycisk **Odśwież** z górnej części tabeli.

Certyfikaty

Aby umożliwić GravityZone wdrożenie do prawidłowego działania i w bezpieczny sposób, musisz utworzyć i dodać liczbę certyfikatów bezpieczeństwa w Control Center.



Strona certyfikatów

Control Center dostarcza poniższe formaty certyfikatów:

- PEM (.pem, .crt, .cer, .key)
- DER (.der, .cer)
- PKCS#7 (.p7b, .p7c)
- PKCS#12 (.p12, .pfx)

Notatka

Następujące certyfikaty są potrzebne wyłącznie do zarządzania bezpieczeństwem na urządzeniach Apple iOS:

- Certyfikaty serwera komunikacji
- Certyfikat Apple MDM Push
- Certyfikat Tożsamość iOS MD i Przypisywanie Profili
- Certyfikat iOS MDM Trust Chain

Jeżeli nie planujesz wdrożyć zarządzania urządzeniem przenośnym iOS, nie musisz dostarczać tych certyfikatów.

Control Center Certyfikaty Bezpieczeństwa

Control Center Certyfikat bezpieczeństwa jest potrzebny, żeby zidentyfikować konsole internetową Control Center jako zaufaną stronę w przeglądarce internetowej. Control Center używa domyślnego certyfikatu SSL podpisanego przez Bitdefender. Ten wbudowany certyfikat nie jest rozpoznawany przez przeglądarki internetowe i wyzwala ostrzeżenie bezpieczeństwa. Aby uniknąć ostrzeżeń zabezpieczeń przez przeglądarki, dodaj certyfikat SSL podpisany przez spółkę lub przez zewnętrzny urząd certyfikacji (CA).

Aby dodać lub zamienić certyfikaty Control Center:

1. Przejdź do strony **Konfiguracja** i kliknij zakładkę **Certyfikaty**.
2. Kliknij nazwę certyfikatu.
3. Wybierz typ certyfikatu (z oddzielnym lub wbudowanym kluczem prywatnym).
4. Naciśnij przycisk **Dodaj** obok pola **Certyfikat** i wgraj certyfikat.
5. Dla certyfikatów z oddzielnymi kluczami prywatnymi, naciśnij przycisk **Dodaj** obok pola **Klucz prywatny** i wgraj klucz prywatny.
6. Jezeli certyfikat jest chroniony hasłem, wpisz hasło w odpowiednim polu.
7. Kliknij **Zapisz**.

Punkt końcowy - Security Server Certyfikat Komunikacji Bezpieczeństwa

Certyfikat ten gwarantuje bezpieczną komunikację między agentami bezpieczeństwa a Security Server (Wieloplatformowy), który mają przypisany.

Podczas jego wdrażania, Security Server generuje domyślny samopodpisany certyfikat. Możesz zastąpić ten wbudowany certyfikat dodając jeden ze swoich wyborów w Control Center.

Aby dodać lub zastąpić Punkt koncowy - Security Server Certyfikat Komunikacji:

1. Przejdź do strony **Konfiguracja** i kliknij zakładkę **Certyfikaty**.
2. Kliknij nazwę certyfikatu.
3. Wybierz typ certyfikatu (z oddzielnym lub wbudowanym kluczem prywatnym).
4. Naciśnij przycisk **Dodaj** obok pola **Certyfikat** i wgraj certyfikat.
5. Dla certyfikatów z oddzielnymi kluczami prywatnymi, naciśnij przycisk **Dodaj** obok pola **Klucz prywatny** i wgraj klucz prywatny.
6. Jezeli certyfikat jest chroniony hasłem, wpisz hasło w odpowiednim polu.
7. Kliknij **Zapisz**. Komunikat ostrzegawczy może się pojawić, jeśli certyfikat jest samopodpisany lub wygasł. Jeśli wygasł, należy odnowić certyfikat.
8. Kliknij **Tak**, aby kontynuować ładowanie certyfikatu. Natychmiast po zakończeniu przesyłania Control Center wysyła certyfikat bezpieczeństwa do Security Server.

W razie potrzeby można przywrócić oryginalny wbudowany certyfikat każdego Security Server, w następujący sposób:

1. Kliknij nazwę certyfikatu na stronie **Certyfikaty**.
2. Wybierz **Brak certyfikatów (użyj domyślnie)** jako typ certyfikatu.
3. Kliknij **Zapisz**.

Certyfikaty serwera komunikacji

Certyfikat serwera komunikacji jest używany do zabezpieczenia komunikacji pomiędzy serwerem komunikacji, a urządzeniami przenośnymi iOS.

Wymagania:

- Ten certyfikat SSL może być podpisany zarówno przez Twoją firmę, jak i przez zewnętrzny urząd certyfikacji.

- Nazwa wspólna certyfikatu musi zawierać dokładnie nazwę domeny lub adres IP używany przez klientów mobilnych do komunikacji z Serwerem Komunikacji. To jest skonfigurowane jako zewnętrzny adres MDM w interfejsie konfiguracyjnym konsoli urządzenia GravityZone.
- Klienci mobilni muszą ufać temu certyfikatowi. Dlatego, musisz również dodać iOS MDM Trust Chain.

Aby dodać lub zamienić certyfikaty serwera komunikacji:

1. Przejdź do strony **Konfiguracja** i kliknij zakładkę **Certyfikaty**.
2. Kliknij nazwę certyfikatu.
3. Wybierz typ certyfikatu (z oddzielnym lub wbudowanym kluczem prywatnym).
4. Naciśnij przycisk **Dodaj** obok pola **Certyfikat** i wgraj certyfikat.
5. Dla certyfikatów z oddzielnymi kluczami prywatnymi, naciśnij przycisk **Dodaj** obok pola **Klucz prywatny** i wgraj klucz prywatny.
6. Jezeli certyfikat jest chroniony hasłem, wpisz hasło w odpowiednim polu.
7. Kliknij **Zapisz**.

Certyfikat Apple MDM Push

Certyfikat Apple MDM Push jest potrzebny w celu bezpiecznej komunikacji pomiędzy serwerem komunikacji i usługą powiadomień Apple Push (APNs) do wysyłania powiadomień push. Powiadomienia push są używane do monitowania urządzeń o połączeniu z Serwerem komunikacji, kiedy nowe zadania lub zmiany polityki są dostępne.

Apple wystawia ten certyfikat specjalnie dla twojej firmy, ale wymaga, aby żądanie podpisania twojego certyfikatu (CSR) zostało podpisane przez Bitdefender. Control Center dostarcza kreator, który pomoże Ci łatwo uzyskać certyfikat Push Apple MDM.

WAŻNE

- Będziesz potrzebować Apple ID żeby uzyskać i zarządzać certyfikatami. Jeżeli nie posiadasz Apple ID, możesz stworzyć go na stronie Mój Apple ID Użyj ogólnego adresu, a nie adresu pracownika do rejestracji Apple ID, jeżeli będziesz potrzebować odnowić później certyfikat.
- Strona Apple nie działać poprawnie w przeglądarce Internet Explorer. Zalecamy korzystanie z najnowszych wersji Safari lub Chrome.

- Certyfikat Apple MDM Push jest ważny tylko przez rok. kiedy certyfikat jest bliski wygaśnięciu, musisz odnowić go i zaimportować odnowiony certyfikat do Control Center. Jeżeli pozwolisz certyfikatowi wygasnąć, musisz stworzyć nowy i reaktywować wszystkie swoje urządzenia.

Dodawanie certyfikatu Apple MDM Push

Aby uzyskać certyfikat Apple MDM Push i zaimportować go do Control Center:

1. Przejdź do strony **Konfiguracja** i kliknij zakładkę **Certyfikaty**.
2. Naciśnij nazwę certyfikatu i postępuj zgodnie z kreatorem poniżej:

Krok 1 - Zdobądź certyfikat podpisany przez Bitdefender

Wybierz odpowiednią opcję:

- **Muszę wygenerować prośbę o certyfikat podpisany przez Bitdefender** (Zalecane)
  a. Podaj nazwę firmy, pełną nazwa i adres e-mail w odpowiednim polu.
  b. Naciśnij **Wygeneruj** aby pobrać plik CSR przypisany do Bitdefender.
- **Mam już żądanie podpisania certyfikatu i potrzebuję, aby był on podpisany przez Bitdefender**
  a. Wgraj twój plik CSR i przypisany klucz prywatny przez naciśnięcie przycisku **Dodaj** obok odpowiednich pól.

     Serwer komunikacji potrzebuje klucza prywatnego do autoryzacji z serwerami APN.
  b. Określ ochronę hasłem klucza prywatnego, jeżeli potrzeba.
  c. Naciśnij przycisk **Przypisz** aby pobrać plik CSR przypisany do Bitdefender.

Krok 2 - Żądanie certyfikatu Push firmy Apple

a. Naciśnij link **Portal Certyfikatów Apple Push** i przypisz używanie twojego Apple ID i hasła.
b. Naciśnij przycisk **Utwórz Certyfikat** i zaakceptować Warunki użytkowania.
c. Naciśnij **Wybierz plik**, zaznacz plik CSR i naciśnij **Wgraj**.

> **Notatka**
> Możesz znaleźć przycisk **Wybierz plik** z inną nazwą poprzez **Wybierz** lub **Przeglądaj**, zależnie od przeglądarki, której używasz.

d. Ze strony potwierdzenia, naciśnij przycisk **Pobierz** aby otrzymać certyfikat MDM Push.

e. Wróć do kreatora z Control Center.

Krok 3 - Importuj certyfikat push Apple

Naciśnij **Dodaj Certyfikat** i wgraj plik certyfikatu ze swojego komputera.

Możesz sprawdzić szczegóły certyfikatu w polu poniżej.

3. Kliknij **Zapisz**.

Odnawianie Certyfikatu Apple MDM Push

Aby odnowić certyfikat Apple MDM i zaktualizować go w Control Center:

1. Przejdź do strony **Konfiguracja** i kliknij zakładkę **Certyfikaty**.
2. Kliknij nazwę certyfikatu, aby otworzyć kreatora importu.
3. Uzyskaj certyfikat podpisany przez Bitdefender. Procedura jest taka sama jak dla uzyskania nowego certyfikatu.
4. Naciśnij odnośnik **Portal Certyfikatów Apple Push** i przypisz z tym samym Apple ID używanym do stworzenia certyfikatu.
5. Zlokalizuj certyfikat MDM Push dla Bitdefender i naciśnij odpowiadający przycisk **Odnów**.
6. Naciśnij **Wybierz plik**, zaznacz plik CSR i naciśnij **Wgraj**.
7. Naciśnij **Pobierz** aby zapisać certyfikat na twoim komputerze.
8. Wróć do Control Center i zaimportuj nowy certyfikat Apple push.
9. Kliknij **Zapisz**.

Certyfikat Tożsamość iOS MD i Przypisywanie Profili

iOS MDM Tożsamość i podpisywanie Profili.Certyfikat używany przez Serwer komunikacji do podpisania certyfikatu tożsamości i skonfigurowania profili wysłano do urządzeń mobilnych.

Wymagania:

- Musi to być pośredni albo łączony certyfikat, podpisany przez twoją firmę lub przez zewnętrzny urząd certyfikacji.
- Klienci mobilni muszą ufać temu certyfikatowi. Dlatego, musisz również dodać iOS MDM Trust Chain.

Aby dodać lub zamienić certyfikat Tożsamość iOS MD i Przypisywanie Profili:

1. Przejdź do strony **Konfiguracja** i kliknij zakładkę **Certyfikaty**.
2. Kliknij nazwę certyfikatu.
3. Wybierz typ certyfikatu (z oddzielnym lub wbudowanym kluczem prywatnym).

4. Naciśnij przycisk **Dodaj** obok pola **Certyfikat** i wgraj certyfikat.
5. Dla certyfikatów z oddzielnymi kluczami prywatnymi, naciśnij przycisk **Dodaj** obok pola **Klucz prywatny** i wgraj klucz prywatny.
6. Jezeli certyfikat jest chroniony hasłem, wpisz hasło w odpowiednim polu.
7. Kliknij **Zapisz**.

Certyfikat iOS MDM Trust Chain

Certyfikaty iOS MDM Trust Chain są wymagane na urządzeniach przenośnych aby upewnić się, że zaufanie dla Serwera Komunikacji i Identyfikacji iOS MDM i certyfikatu przypisania profilu. Serwer Komunikacji wysyła ten certyfikat do urządzeń przenośnych podczas aktywacji.

iOS MDM Trust Chain musi zawierać wszystkie certyfikaty pośrednie di certyfikatu głównego firmy lub certyfikat pośredni wydany rzez urząd certyfikacji zewnętrznej.

Aby dodać lub zamienić certyfikaty iOS MDM Trust Chain:

1. Przejdź do strony **Konfiguracja** i kliknij zakładkę **Certyfikaty**.
2. Kliknij nazwę certyfikatu.
3. Naciśnij przycisk **Dodaj** obok pola **Certyfikat** i wgraj certyfikat.
4. Kliknij **Zapisz**.

3.1.5. Zarządzanie Urządzeniem GravityZone

Urządzenie GravityZone posiada podstawowy interfejs konfiguracyjny, dostępny z narzędzia zarządzania używanego do zarządzania środowiskiem wirtualnym, gdzie możesz wdrażać urządzenie.

Oto dostępne opcje po wdrożeniu urządzenia GravityZone:

- Konfiguruj Ustawienia Nazwy Hosta
- Skonfiguruj ustawienia sieciowe
- Konfiguruj ustawienia proxy
- Serwer Komunikacji MDM
- Role Instalowania/Odinstalowywania
- Zainstaluj Security Server
- Połącz z Istniejącą Bazą Danych

- Serwer aktual.
- Konfiguruj role balancerów
- Replica Set
- Konfiguruj język

Notatka
Zauważ, że **Automatyczna Instalacja** nie jest już dostępna.

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

Konfiguruj nazwę hosta i ustawienia

Komunikacja z rolami GravityZone odbywa się za pomocą adresów IP lub nazwy DNS zainstalowanych urządzeń. Domyślnie, GravityZone elementy komunikują się używając adresu IP. Jeżeli chcesz włączyć komunikację przez nazwy DNS, musisz skonfigurowaćGravityZone urządzenia z nazwami DNS i upewnić się, że poprawnie rozpoznaje skonfigurowany adres IP urządzenia.

Warunki wstępne:

- Skonfiguruj rekord DNS na serwerze DNS.
- Nazwa DNS musi być poprawie przypisana do skonfigurowanego adresu IP urządzenia. Dlatego należy upewnić się, że urządzenie jest skonfigurowane z prawidłowym adresem IP.

Aby skonfigurować ustawienia nazwy hosta:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z menu głównego wybierz **Konfiguruj ustawienia nazwy hosta**.
3. Wprowadź nazwę hosta urządzenia i nazwę domeny usługi Active Directory (w razie potrzeby).
4. Wybierz **OK** aby zapisać zmiany.

Skonfiguruj ustawienia sieciowe

Można skonfigurować urządzenie, aby automatycznie uzyskać ustawienia sieciowe z serwera DHCP lub ręcznie skonfigurować ustawienia sieciowe. Jeśli zdecydujesz

się skorzystać z DHCP, należy skonfigurować serwer DHCP, aby zarezerwować konkretny adres IP dla urządzenia.

Żeby skonfigurować ustawienia sieciowe:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z menu głównego wybierz **Konfiguruj ustawienia sieciowe**.
3. Wybierz interfejs sieciowy (domyślny `ath0`).
4. Wybierz metodę konfiguracji:
   - **Skonfiguruj ustawienia sieciowe ręcznie.** Musisz określić adres IP, maskę sieci, adres bramy i adres serwera DNS.
   - **Uzyskaj ustawienia sieci automatycznie przez serwer DHCP.** Użyj tej opcji tylko jeżeli masz skonfigurować serwer DHCP do zarezerwowania konkretnego adres IP dla urządzenia.
5. Możesz sprawdzić szczegóły dotyczące konfiguracji IP lub aktualny status połączenia, wybierając odpowiednie opcje.

Konfiguruj ustawienia proxy

Jeśli urządzenie łączy się z Internetem przez serwer proxy, musisz skonfigurować ustawienia proxy.

Notatka
Ustawienie proxy można skonfigurować z Control Center, Strona **Konfiguracja > Proxy**. Zmiana ustawień proxy w jednym miejscu automatycznie aktualizuje je w innym miejscu też

Konfigurowanie ustawień proxy:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z menu głównego wybierz **Konfiguruj ustawienia Proxy**.
3. Wybierz **Konfiguruj ustawienia proxy**.
4. Podaj adres serwera proxy. Użyj poniższej składni:
   - Jeżeli serwer proxy nie wymaga uwierzytelniania:

     ```
     http(s)://<IP/hostname>:<port>
     ```

- Jeżeli serwer proxy wymaga uwierzytelnianie:

  `http(s)://<username>:<password>@<IP/hostname>:<port>`

5. Wybierz **OK** aby zapisać zmiany.

Wybierz **Pokaż informacje proxy**, aby sprawdzić ustawienia serwera proxy.

Serwer Komunikacji MDM

Notatka
Ta konfiguracja jest przeznaczona tylko do zarządzania urządzeniami przenośnymi i dostępna po zainstalowaniu rola Serwera Komunikacji.

W domyślnych ustawieniach GravityZone, urządzenia przenośne mogą być zarządzane tylko wtedy gdy są one przyłączone bezpośrednio do sieci korporacyjnej (przez Wi-Fi lub VPN). Dzieje się tak, ponieważ podczas rejestracji urządzeń przenośnych są one skonfigurowane by łączyć się z lokalnym adresem urządzenia Serwera komunikacji.

Aby móc zarządzać urządzeniami przenośnymi za pośrednictwem internetu bez względu na to gdzie się znajdują, należy skonfigurować serwer komunikacji używając publicznego adresu.

Aby móc zarządzać urządzeniami mobilnymi, gdy nie są podłączone do sieci firmy, dostępne są następujące opcje:

- Skonfigurować przekierowanie portów na bramie firmowej na urządzenia z rolą serwera komunikacyjnego.
- Dodaj kartę sieciową do urządzenia z działającego w roli serwera komunikacyjnego i przypisz mu publiczny adres IP.

W obu przypadkach, należy skonfigurować serwer komunikacyjny z adresem zewnętrznym by mógł być wykorzystywany do zarządzania urządzeniem mobilnym:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z menu głównego wybierz **Serwer Komunikacyjny MDM**.
3. wybierz **Konfiguruj zewnętrzny adres serwera MDM**
4. Podaj adres zewnętrzny.

   Użyj następującej składni: `https://<IP/Domain>:<Port>`.

- Jeśli używasz przekierowania portów, musisz wpisać publiczny adres IP lub nazwę domeny oraz port otwarty na bramce.
- Jeśli korzystasz z publicznego adresu dla serwera komunikacyjnego, należy wprowadzić publiczny adres IP lub nazwę domeny oraz port komunikacyjny serwera. Domyślny port `8443`.

5. Wybierz **OK** aby zapisać zmiany.
6. Wybierz **Pokaż zewnętrzny adres Serwera MDM**, aby sprawdzić ustawienia.

Role Instalowania/Odinstalowywania

Aplikacje GravityZone mogą uruchamiać jedną, kilka lub wszystkie z poniższych ról:

- **Serwer bazodanowy**
- **Serwer aktual.**
- **Konsola internetowa**
- **Serwer komunikacji**

WdrożenieGravityZone wymaga uruchomienia jednej instancji każdej roli. W zależności od tego w jaki sposób chcesz dystrybuować role GravityZone, możesz wdrożyć jedną z czterech GravityZone urządzeń. Rola Serwera bazy danych jest pierwszym krokiem instalacji. W scenariuszu z wielu urządzeń GravityZone, możesz zainstalować rolę dla bazy danych serwera na pierwszym urządzeniu i skonfigurować wszystkie inne urządzenia do podłączenia do istniejących instancji bazy danych.

Notatka

Możesz zainstalować dodatkowe instancje określonych ról, za pomocą równoważenia ról. Aby uzyskać więcej informacji, odwołaj się do „Konfiguruj role balancerów” (p. 78).

Aby zainstalować role GravityZone:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z głównego menu, wybierz **Zaawansowane Ustawienia**.
3. Wybierz **Zainstaluj/Odinstaluj Role**.
4. Wybierz **Dodaj lub usuń role**.

5. Postępuj zgodnie z obecną sytuacją:
   - Jeśli jest to wstępne wdrożenie urządzenia GravityZone, naciśnij klawisz `Spacja`, a następnie `Enter`, aby zainstalować rolę Serwera Bazy Danych. Musisz potwierdzić swój wybór naciskając ponownie `Enter`. Skonfiguruj hasło bazy danych, a następnie zaczekaj aż instalacja zostanie zakończona.
   - Jeśli już wdrożyłeś inne urządzenie z rolą serwera bazy danych, wybierz **Anuluj** i wrócisz do menu **Dodaj lub usuń role**. Musisz wybrać **Konfiguracja Adresu Bazy danych** i wpisać adres bazy danych serwera. Upewnij się, że ustawiłeś hasło bazy danych zanim uzyskasz dostęp do tych opcji. Jeśli nie znasz hasła bazy danych, skonfiguruj nowe, wybierając **Ustawienia Zaawansowane > Ustaw nowe hasło bazy danych** z menu głównego.

     Użyj następującej składni: `http://<IP/Hostname>:<Port>`. Domyślny port bazy danych `27017`. Wprowadź główne hasło bazy danych.
6. Zainstaluj inne role wybierając **Dodaj lub usuń role** z menu **Instaluj/Odinstaluj Role** i wybierz role do instalacji. Dla każdej roli, którą chcesz zainstalować lub odinstalować, naciśnij przycisk `Spacja`, aby zaznaczyć lub odznaczyć rolę, a następnie naciśnij `Enter`, aby kontynuować. Musisz potwierdzić swój wybór klikając ponownie `Enter` i następnie zaczekać na zakończenie instalacji.

Notatka

Instalowanie każdej roli trwa kilka minut. Podczas instalacji, wymagane pliki są sciągane z internetu. instalacja może zająć więcej czasu jeżeli połączenie internetowe jest wolne. Jeżeli instalacja zawiesza się, przesuń urządzenie.

Możesz zobaczyć zainstalowane role i ich adresy IP, wybierając jedną z następujących opcji z menu **Zainstaluj/Odinstaluj Role**:

- **Pokaż lokalnie zainstalowane role**, aby wyświetlić tylko role zainstalowane na tym urządzeniu.
- **Pokaż wszystkie zainstalowane role**, aby wyświetlić wszystkie role zainstalowane w środowisku GravityZone.

Zainstaluj Security Server

Notatka
Security Server będzie dostępny do użytku tylko, jeśli Twój klucz licencyjny na to pozwala.

Możesz zainstalować Security Serverz interfejsu konfiguracji urządzenia GravityZone, bezpośrednio na urządzeniu GravityZone lub z Control Center jako samodzielne urządzenie. Zalety instalowania Security Server z urządzenia to:

- Odpowiedni dla wdrożeń GravityZone z jednego urządzenia posiadającego wszystkie role.
- Możesz przeglądać i korzystać z Security Server, bez konieczności integracji GravityZone z platformą wirtualizacji.
- Mniej operacji wdrażania do wykonania.

Warunki wstępne:

Urządzenie GravityZone musi mieć zainstalowaną rolę Serwera Bazy Danych lub musi być skonfigurowane tak, aby podłączyć się do istniejącej bazy danych.

Aby zainstalować Security Server z interfejsu urządzenia:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z głównego menu, wybierz **Zaawansowane Ustawienia**.
3. Wybierz **Zainstaluj Security Server**. Pojawi się nowa wiadomość potwierdzająca.
4. Wciśnij `Enter`, aby kontynuować i czekaj aż instalacja zakończy się.

Notatka
Możesz odinstalować ten Security Server tylko z menu **Zaawansowanych Ustawień** interfejsu urządzenia.

Połącz z Istniejącą Bazą Danych

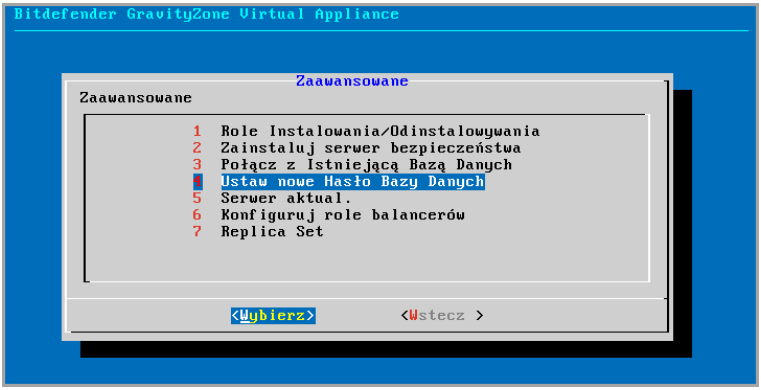
W scenariuszu z wielu urządzeń GravityZone, możesz zainstalować rolę dla bazy danych serwera na pierwszym urządzeniu i skonfigurować wszystkie inne urządzenia do podłączenia do istniejących instancji bazy danych.

Notatka
Jeżeli twoje ustawienia składają się z pojedynczych urządzeń GravityZone, nie potrzebujesz ustawiać tej opcji.

Żeby skonfigurować urządzenie GravityZone do połączenia z istniejącą bazą danych:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z głównego menu, wybierz **Zaawansowane Ustawienia**.
3. Wybierz **Połącz z Istniejącą Bazą Danych**.

Notatka
Upewnij się, że ustawiłeś hasło bazy danych zanim uzyskasz dostęp do tych opcji. Jeśli nie znasz hasła bazy danych, ustaw nowe, uzyskując dostęp do **Ustawienia Zaawansowane > Ustaw nowe hasło bazy danych** z menu głównego.

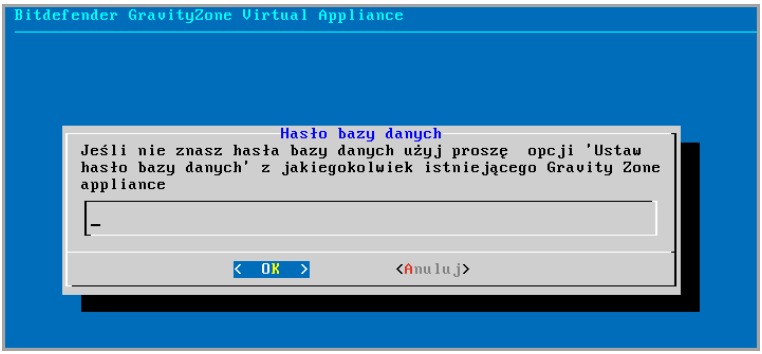


Interfejs konsoli urządzenia: menu Ustawień Zaawansowanych

4. Wybierz **Konfiguruj adres Serwera bazodanowego**.
5. Wpisz adres bazy danych, używając następującej składni:

   `<IP/Nazwa Hosta>:<Port>`

   Określanie portu jest opcjonalne. Domyślny port `27017`.
6. Wprowadź główne hasło bazy danych.



Interfejs konsoli urządzenia: wprowadź hasło bazy danych

7. Wybierz **OK** aby zapisać zmiany.
8. Wybierz **Pokaż adres serwera bazy danych** aby upewnić się, ze adres jest poprawnie skonfigurowany.

Konfiguruj Serwer aktualizacji

Urządzenie GravityZone domyślnie jest skonfigurowane aby aktualizować się przez Internet. Jeśli wolisz, możesz ustawić zainstalowane urządzenie do aktualizacji z lokalnego serwera aktualizacji Bitdefender (w urządzeniu GravityZone z zainstalowaną rolą serwera aktualizacji).

Żeby ustawić adres aktualizacji serwera:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z głównego menu, wybierz **Zaawansowane Ustawienia**.
3. Wybierz **Serwer Aktualizacji**.
4. Zaznacz **Skonfiguruj adres aktualizacji**.
5. Wpisz adres IP lub nazw hosta urządzenia działającego z rola Serwera Aktualizacji. Domyślny porty Serwera aktualizacji to `7074`.

Konfiguruj role balancerów

Aby zapewnić niezawodność i skalowalność, możesz zainstalować wiele instancji poszczególnych ról (Serwer komunikacji, konsola sieciowa).

Każda rola instalowana jest na innym urządzeniu.

Każdy przypadek zdefiniowanej roli musi być połączony do innej roli poprzez role balancer.

Urządzenie GravityZone zawiera wbudowany balancer, który możesz zainstalować i używać. Jeżeli posiadasz już oprogramowanie balansujące lub sprzęt poza siecią, możesz użyć ich zamiast wbudowanych balancerów.

Wbudowane role balancerów nie mogą być zainstalowane razem z rolami w urządzeniach GravityZone

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z głównego menu, wybierz **Zaawansowane Ustawienia**.
3. Zaznacz **Skonfiguruj Role Balancerów**.
4. Wybierz jedną z opcji:
   - **Użyj zewnętrznych balancerów.** Wybierz tą opcje jeżeli twoja infrastruktura sieciowa zawiera oprogramowanie balansujące lub sprzęt, który je dostarcza. Musisz podać adres balancera dla każdej roli, którą chcesz zrównoważyć. Użyj poniższej składni:

     `http(s)://<IP/Hostname>:<Port>`.
   - **Użyj wbudowanych balancerów.** Wybierz tą opcje jeżeli chcesz zainstalować i użyć wbudowanego oprogramowania balancera.
5. Wybierz **OK** aby zapisać zmiany.

Replica Set

Z ta opcją możesz włączyć używanie repliki zestawu replik zmaiast pojedynczego serwera instancji bazy danych. Ten mechanizm zezwala na stworzenie wielu instancji baz danych poprzez dystrybucje środowiska GravityZone, zapewnia bazy danych o wysokiej dostepności w przypadku awarii.

WAŻNE
Replikacja bazy danych jest dostępna tylko dla świeżych instalacji urządzeń GravityZone rozpoczynających się od wersji 5.1.17-441.

Konfiguracja Zestawu Replik

Na początek, musisz włączyć Zestaw Replik na pierwszym zainstalowanym urządzeniu GravityZone. Następnie, będziesz mógł dodać członków zestawu replik poprzez zainstalowanie roli bazy danych na innych instancjach GravityZone w tym samym środowisku.

WAŻNE

- Replica Set wymaga więcej niż trzech członków, aby działać.
- możesz dodać siedem instancji ról bazy danych jako zestaw replik członków (ograniczenie MongoDB).
- Zaleca się, aby korzystać z nieparzystej liczby instancji baz danych. Parzysta liczba członków będzie zużywać więcej zasobów dla tych samych rezultatów.

Aby włączyć replikację bazy danych w swoim środowisku GravityZone:

1. Zainstaluj rolę Serwera Bazy Danych na pierwszym urządzeniu GravityZone Aby uzyskać więcej informacji, odwołaj się do „Role Instalowania/Odinstalowywania” (p. 74).
2. Skonfiguruj inne urządzenia, aby połączyć się z pierwszą instancją bazy danych. Aby uzyskać więcej informacji, odwołaj się do „Połącz z Istniejącą Bazą Danych” (p. 76).
3. Przejdź do głównego menu pierwszego urządzenia, wybierz **Ustawienia Zaawansowane**, a następnie wybierz **Replica Set**, aby to włączyć. Pojawi się nowa wiadomość potwierdzająca.
4. Zaznacz **Tak**, aby potwierdzić.
5. Zainstaluj rolę Serwera Bazy danych na każdym z urządzeń GravityZone.

Tak szybko, jak powyższe czynności zostaną zakończone, wszystkie instancje bazy danych rozpoczną pracę jako zestawu replik:

- Podstawowa instancja jest wybrana, jako jedyna do zaakceptowania operacji zapisu.
- Podstawowa instancja zapisuje wszystkie zmiany zastosowane na zestawach danych w dzienniku.
- Drugorzędne instancje replikują ten dziennik i stosują te same zmiany do swoich zbiorów danych.

- Kiedy podstawowa instancja stanie się niedostępna, zestaw replik wybiera jedną z następnych instancji jako podstawowa.
- Kiedy podstawowa instancja nie komunikuje się z innymi członkami przez więcej niż 10 sekund, zestaw replik podejmie próbę wybrania innego członka do stania się nową podstawową instancją.

Usuwanie Zestawu replik członków

Aby usunąć zestaw replik członków, musisz wybrać ich menu CLI **Zainstaluj/Odinstaluj Role > Dodaj lub Usuń Role** i odznacz **Serwer Bazy Danych**.

Notatka
możesz usunąć zestaw replik członków tylko jeżeli ostatnie cztery instancje bazy danych zostały zainstalowane w sieci.

Konfiguruj język

Aby zmienić język interfejsu konfiguracji urządzenia:

1. Wybierz **Konfiguracja Języka** z menu głównego.
2. Wybierz język z dostępnych opcji. Pojawi się nowa wiadomość potwierdzająca.

   Notatka
   Być może trzeba przewinąć w dół, aby zobaczyć swój język.

3. Wybierz **OK** aby zapisać zmiany.

3.2. Zarządzanie Licencjami

Usługi bezpieczeństwa GravityZone są licencjonowane i sprzedawane osobno. Każda usługa bezpieczeństwa GravityZone wymaga prawidłowego klucza licencyjnego. Co najmniej jeden ważny klucz licencyjny musi być dostarczony, aby korzystać z GravityZone.

Aby zarejestrować produkt offline, musisz posiadać kod rejestracji offline przypisany do twojego klucza licencyjnego.

Możesz wybrać do testów GravityZone i zdecydować czy jest to odpowiednie rozwiązanie dla Twojej firmy. Aby aktywować twój okres próbny, należy wprowadzić klucze licencyjne z rejestracyjnej maila rejestracyjnego w Control Center.

Notatka
Control Center jest za darmo z każdą usługą bezpieczeństwa GravityZone

Aby kontynuować używanie usług bezpieczeństwa po wygaśnięciu wersji próbnej, musisz kupić klucz licencyjny do rejestracji usługi.

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

Klucze licencyjne GravityZone mogą być zarządzane na stronie **Konfiguracja > Licencja** w Control Center. Kiedy twój aktualny klucz licencyjny będzie bliski wygaśnięcia, pojawi się wiadomość w konsoli, że musisz go odnowić. Aby wpisać nowy klucz licencyjny albo zobaczyć szczegóły aktualnej licencji, idź do strony **Konfiguracja > Licencja**.

3.2.1. 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.

3.2.2. Wprowadzanie Twoich kluczy licencyjnych

Rejestracja licencji GravityZone może być przeprowadzona online lub offline (gdy połączenie internetowe nie jest możliwe). W obu przypadkach, potrzebujesz wprowadzić poprawny klucz licencyjny dla każdej usługi bezpieczeństwa jaką chcesz używać.

Możesz wpisać kilka kluczy licencyjnych dla tej samej usługi, ale tylko ostatni wprowadzony klucz będzie aktywny.

Aby zarejestrować produkt offline, musisz posiadać kod rejestracji offline przypisany do twojego klucza licencyjnego.

Aby przypisać licencję dla twoich usług bezpieczeństwa GravityZone lub zmienić istniejący klucz licencyjny:

1. Zaloguj się do Control Center używając konta administratora firmy.

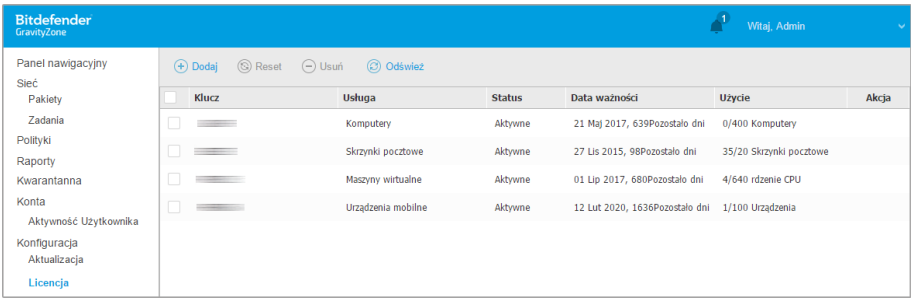
2. Przejdź do strony **Konfiguracja > Licencja**
3. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli.
4. Wybierz rodzaj rejestracji:
   - **Online**. W tym przypadku, wprowadź ważny klucz licencyjny w pole **Klucz licencyjny**. Klucz licencyjny zostanie sprawdzony i zatwierdzony online.
   - **Offline**, gdy połączenie z interetem nie jest dostępne. W tym przypadku, potrzebujesz wprowadzić klucz licencyjny, jak również kod rejestracyjny.

   Jeżeli klucz licencyjny nie jest ważny, zostanie wyświetlony błąd weryfikacji jako podpowiedź w polu **Klucz Licencyjny**.
5. Kliknij **Dodaj**. Klucz licencyjny zostanie dodany do strony **Licencja**, gdzie możesz wybrać jego szczegóły.
6. Naciśnij **Zapisz** aby zastosować zmiany. Control Center uruchamia się ponownie i trzeba znów się zalogować, aby zobaczyć zmiany.

3.2.3. Sprawdzanie szczegółów aktualnej licencji

zobacz szczegóły twojej licencji:

1. Zaloguj się do Control Center używając konta administratora firmy.
2. Przejdź do strony **Konfiguracja > Licencja**



Strona Licencji

3.
   - Klucz licencyjny
   - Usługi bezpieczeństwa których dotyczą klucze licencyjne
   - Status klucza licencji

WAŻNE
Tylko jeden klucz licencyjny może być aktywny w tym samym czasie dla poszczególnych usług.

- Czas wygaśnięcia i czas pozostały do końca licencji

WAŻNE
Po wygaśnięciu licencji, moduły ochronne z zainstalowanymi agentami są wyłączone. Jako rezultat, punkty końcowe nie są już chronione i nie możesz wykonać żadnego zadania skanowania. Nowo zainstalowany agent będzie w okresie trial.

- Ilość licencji

3.2.4. Resetowanie licznika zużycia licencji

Możesz znaleźć informacje o liczbie wykorzystania kluczy licencyjnych na stronie **Licencja** w kolumnie **Wykorzystanie**.

Jeśli chcesz zaktualizować informacje o użytkowaniu, wybierz klucz licencyjny, który Ciebie interesuje i kliknij przycisk **Resetuj** w górnej części tabeli.

3.2.5. Usuwanie kluczy licencyjnych

Możesz wybrać czy usunąć nieprawidłowe lub nieważne klucze licencyjne ze strony **Licencja**

Ostrzeżenie
Usuwanie kluczy licencyjnych usunie przypisane usługi bezpieczeństwa z Control Center. Nie będziesz mógł zainstalować i zarządzać ochroną oferowaną przez tę usługę, na punktach końcowych w swojej sieci. Niemniej jednak, punkty końcowe są chronione tak długo, jak klucz licencyjny jest ważny.
Jeśli wprowadzisz nowy ważny klucz licencyjny, który zawiera wcześniej usuniętą usługę, ponownie uaktywnią się wszystkie funkcje tej usługi w Control Center.

Aby usunąć klucz licencyjny:

1. Zaloguj się do Control Center używając konta administratora firmy.
2. Przejdź do strony **Konfiguracja > Licencja**
3. Zaznacz klucz licencyjny, który chcesz usunąć i kliknij przycisk **Usuń** w górnej części tabeli.

3.3. 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 w środowiskach wirtualnych, takich jak VMware lub Citrix Xen lub jeśli komputery 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. 4).

3.3.1. Instalowanie Security Server

Security Server jest dedykowana maszyną wirtualną, która deduplikuje i centralizuje większość fikcjonalności antymalware dla klientów, działających jako serwer.

Security Server rozmieszczenie jest specyficzne dla środowiska w którym jest zainstalowany. Procedury instalacyjne opisane są tu:

Instalowanie Security Server zintegrowanego z VMware NSX

W środowiskach VMware z zainstalowanym NSX, należy wdrożyć Bitdefender obsługę w każdym klastrze, który ma być chroniony. Specjalnie zbudowane urządzenie będzie automatycznie wdrażać we wszystkich hostach w klastrze. Wszystkie maszyny wirtualne na hoście są automatycznie połączone przez Introspekcję Gościa do Security Server instancji serwera zainstalowanego na tym komputerze.

Wdrożenie Security Server jest wykonywane wyłącznie od klienta vSphere Web.

Aby zainstalować Bitdefender usługę:

1. Zaloguj się do sieci klienta vSphere.
2. Idź do **Sieć & Bezpieczeństwo > Instalacja** i kliknij zakładkę **Wdrożenia usług**.
3. Kliknij przycisk **Nowe rozmieszczenie usług** (ikona znaku plus). Otwiera się okno konfiguracji.
4. Wybierz **Introspekcja gości** i kliknij **Następny**.

5. Wybierz centrum danych i klastry, na których można wdrożyć usługę, a następnie kliknij **Dalej**.
6. Wybierz pamięć i zarządzanie siecią, kliknij **Następny**, a następnie **Zakończ**.
7. Powtórz kroki od 3 do 6, tym razem wybierając **Bitdefender** usługę.

   Przed przystąpieniem do instalacji należy upewnić się, że masz połączenie sieciowe pomiędzy wybraną siecią i GravityZone Control Center.

   Gdy Bitdefender usługa jest zainstalowana, zostanie ona automatycznie wdrożona Security Server na wszystkie hosty ESXi w wybranych klastrów.

Ostrzeżenie
Aby usługi działały prawidłowo, należy zainstalować je w następującej kolejności, najpierw Introspekcja gości, a następnie Bitdefender, a nie oba jednocześnie.

Notatka
Aby uzyskać więcej informacji na temat dodawania usług partnerskich NSX, patrz VMware NSX Documentation Center.
Jeśli zdecydujesz się na **określono na hosta** do przechowywanie i zarządzanie siecią, sprawdź, czy agent VM jest ustawiony na komputerach zarówno dla gości introspekcji i usług Bitdefender.

Security Server ma określone wymagania, które są zależne od liczby maszyn wirtualnych jakie ma chronić. Aby ustawić domyślną konfigurację sprzętową Security Server:

1. Zaloguj się do sieci klienta VMware vSphere.
2. Idź do **Hostów i Klasterów**.
3. Wybierz klaster gdzie Security Server zostanie wdrożony, a następnie wybierz **Podobne obiekty> Maszyny Wirtualne** tab.
4. Wyłącz **Bitdefender** urządzenie.
5. Kliknij prawym przyciskiem myszy nazwę urządzenia i następnie wybierz **Edytuj ustawienia...** z menu kontekstowego.
6. W zakładce **sprzęt wirtualny**, ustaw wartości procesora i pamięć RAM do swoich potrzeb, a następnie kliknij przycisk **OK**, aby zapisać zmiany.
7. Zasil urządzenie ponownie.

Notatka
Aby aktualizować VMWare vShield do NSX, odnieś się do artykułu.

Instalacja Security Server zintegrowanego z VMware VSHIELD i Security Server Multi-Platformą

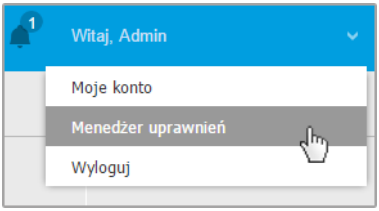
1. Połącz z platformą wirtualizacji
2. Zainstaluj Security Server na hostach

Łączenie z Platformą Wirtualizacyjną

Aby mieć dostęp do zwirtualizowanej struktury zintegrowanej z Control Center musisz podać swoje poświadczenia użytkownika dla każdego dostępnego systemu serwera wirtualizacji. Control Center używa twoich poświadczeń aby połączyć z wirtualną infrastrukturą, pokazywanie tylko zasobów do których masz dostęp (jak określono vCenter Serwer).

Aby określić poświadczenia do połączenia z systemami serwera wirtualizacji:

1. Kliknij nazwę użytkownika w prawym górnym rogu konsoli i wybierz stronę **Zarządzanie Poświadczeniami**.



Sieć > Menu Pakietów

2. Przejdź do zakładki **Wirtualne Środowisko**.
3. Określ niezbędne poświadczenia uwierzytelniania.
   a. Wybierz serwer z odpowiedniego menu.

Notatka
Jeżeli menu jest niedostępne, albo nie została jeszcze skonfigurowana integracja lub wszystkie niezbędne poświadczenia zostały już skonfigurowane.

b. Podaj swoją nazwę użytkownika, hasło i sugestywny opis.

c. Kliknij przycisk ⊕ **Dodaj** . Nowe ustawienia poświadczeń pokazały się w tabeli.

Notatka

Jeżeli nie określiłeś poświadczeń uwierzytelnienia, będziesz musiał podać je podczas próby przeglądania spisu dowolnego systemu Serwera vCenter. Po wprowadzeniu swoich poświadczeń, zostaną one zapisane w Menadżerze Poświadczeń tak, by nie było potrzeby wprowadzania ich ponownie.

Instalowanie Security Server na Hostach

Musisz zainstalować Security Server na komputerach w następujący sposób:

- W środowiskach VMware z vShield Endpoint, musisz zainstalować specjalnie zbudowane urządzenie na każdym hoście, który ma być chroniony. Wszystkie wirtualne maszyny na hoście automatycznie łączą się przez vShield Endpoint z Security Server zainstalowanym na hoście.
- W środowiskach Citrix, musisz zainstalować Security Server na każdym hoście, który chcesz chronić z HVI, poprzez zadanie zdalnej instalacji.
- We wszystkich środowiskach musisz zainstalować Security Server na więcej niż jednym hoście 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. Agent bezpieczeństwa zainstalowany na maszynach wirtualnych łączy się do Security Server za pośrednictwem protokołu TCP/IP, używając szczegółów podczas instalacji szczegółów lub poprzez polityki.

Jeżeli Control Center jest zintegrowana z Serwerem vCenter i XenServer, możesz automatycznie wdrożyć Security Server na hoście z Control Center. Możesz ściągnąć pakiety Security Server do samodzielnej instalacji z Control Center

Notatka

-
  - Dla środowisk VMware z vShield Endpoint, możesz wdrożyć Security Server na hoście wyłącznie poprzez zadanie instalacji.

Instalacja lokalna

We wszystkich wirtualnych środowiskach, które nie są zintegrowane z Control Center musisz zainstalować Security Server ręcznie na hoście, używając pakietów instalacyjnych. 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:

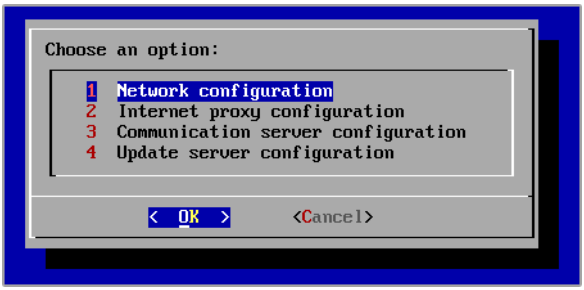
1. Przejdź do strony **Sieć > Pakiety**.
2. Wybierz Domyślny Pakiet Security Server.
3. Kliknij przycisk **Pobierz** w górnej części tabeli i wybierz typ pakietu z menu.
4. Zapisz wybrany pakiet w odpowiedniej lokalizacji.

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. Wpisz adres Serwera Komunikacyjnego, w tym numer portu 8443, w następującym formacie:

      `https://Communication-Server-IP:8443`

      Alternatywnie, można użyć nazwy hosta Serwera Komunikacyjnego zamiast adresu IP.
   c. Wybierz **OK** aby zapisać zmiany.

Instalacja Zdalna

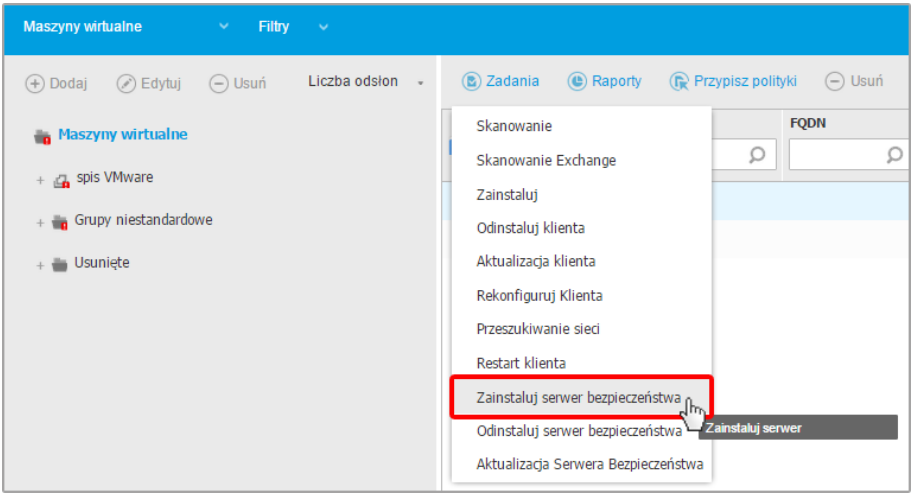
Control Center dopuszcza zdalna instalację Security Server na widocznych hostach przez użycie zadań instalacji.

Aby zainstalować zdanie Security Server na jednym lub kilku hostach:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Przeglądaj zasoby VMware lub Citrix i wybierz pole wyboru odpowiadające wybranym hostom lub kontenerom (serwer vCenter, XenServer lub centrum danych). Dla szybkiej selekcji, możesz bezpośrednio wybrać główny kontener (VMware Inventory or Citrix Inventory). Będziesz mógł wybrać hosty indywidualnie z kreatora instalacji.

Notatka
Nie możesz wybrać hostów z różnych folderów.

4. Kliknij przycisk **Zadania** w górnej części tabeli i wybierz **Zainstaluj Security Server** z menu. Okno **Instalacja Security Server** zostało wyświetlone.



Instalowanie Security Server z menu zadań

5. Wybierz hosty na których chcesz zainstalować Security Server.
6. Wybierz ustawienia konfiguracji jakich chcesz używać.

WAŻNE
Korzystanie z ustawień wspólnych podczas wdrażania wieloplatformowego Security Server jednocześnie wymaga hostów udostępniających tą sama ilość pamięci, których adresy IP są przypisane do serwerów DHCP i będą częścią tej samej sieci.

Przy wyborze konfiguracji każdego innego Security Server, będziesz w stanie określić ustawienia, takie jakie chcesz dla każdego hosta w kolejnym kroku kreatora. Czynności opisane dalej stosuje się w przypadku, gdy używana jest opcja **Skonfiguruj każdy Security Server**.

7. Kliknij **Dalej**.

8. Podaj sugestywną nazwę dla Security Server.
9. Wybierz pojemnik w który ma zawierać Security Server z menu **Wdrożenie Kontenera**.
10. Wybierz dysk docelowy.
11. Wybierz rodzaj dysku rezerwowego. Jest zalecane aby wdrożyć urządzenie używając dysku rezerwowego.

    WAŻNE
    Jeżeli używasz małego dysku rezerwowego i miejsce na dysku się skończyło, Security Server zamrozi się, w konsekwencji host pozostanie niechroniony.

12. Skonfiguruj pamięć i zasoby procesora alokacji na podstawie wskaźnika konsolidacji VM na hoście. Wybierz **Niskie**, **Średnie** lub **Wysokie** aby załadować zalecane ustawienia alokacji zasobów lub **Ręczne** do konfiguracji zasobów ręcznej alokacji.
13. Opcjonalnie możesz wybrać żeby ustawić hasło administracyjne dla konsoli Security Server. Ustaw hasło administracyjne nadpisując domyślne hasło ("sve").
14. Ustaw strefę czasową urządzenia.
15. Wybierz typ konfiguracji sieci z sieci Bitdefender. Adres IP Security Server nie może się zmienić w czasie gdy jest używany przez Linuksowych agentów do komunikacji.

    Jeśli zdecydujesz się wybrać DHCP, upewnij się, że skonfigurowałeś serwer DHCP, aby zarezerwował adres IP dla urządzenia.

    Jeżeli wybierzesz statyczne, musisz podać adres IP, maska subnet, bramę i informacje DNS.
16. Wybierz sieć vShield i podaj poświadczenia vShield. Domyślna etykieta dla sieci vShield to `vmservice-vshield-pg`.
17. Kliknij **Zapisz**.

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

Notatka
Aby aktualizować VMWare vShield do NSX, odnieś się do artykułu KB.

3.3.2. Instalowanie Agentów Bezpieczeństwa

Aby chronić swoje fizyczne i wirtualne punkty końcowe, 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.

Aby dowiedzieć się więcej o dostępnych agentach bezpieczeństwa, przejdź do „Agenci Bezpieczeństwa" (p. 6).

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.

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. 96).

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.

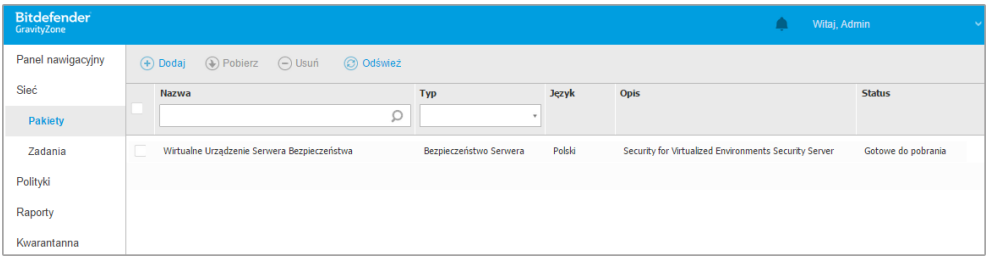
   WAŻNE
   Nie musisz się bac o funkcje bezpieczeństwa Windows (Windows Defender, Windows Firewall), zostaną one wyłączone automatycznie przez rozpoczęciem instalacji.

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 sieciowe z urządzeniem GravityZone.
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

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. 111).

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

1. Utwórz pakiet instalacyjny według swoich potrzeb.

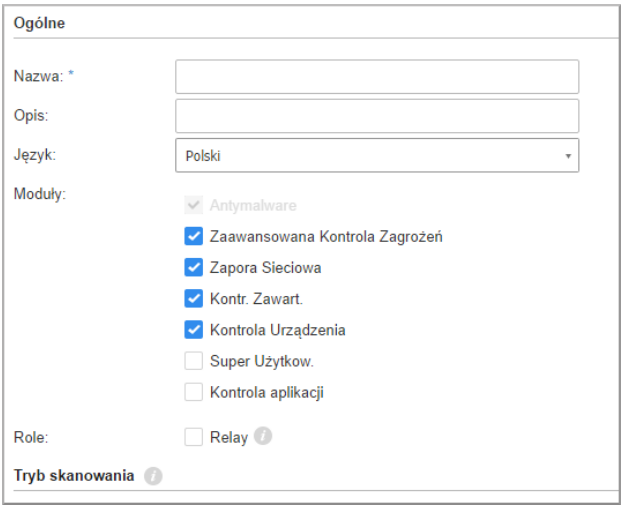
   Notatka
   Ten krok nie jest obowiązkowym, jeśli pakiet już został stworzony dla sieci w ramach twojego konta.

2. Pobierz pakiet instalacyjny na docelowy punkt końcowy.
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. 8).

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. 11)
   - **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. 114).

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 (Security Server) dla maszyn wirtualnych. Sprawa ta wymaga co najmniej jednego wdrożonego Security Server w sieci.
   - **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)

   * 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. 7)

Ostrzeżenie
Dostępność trybów skanowania jest ograniczona na agentach ochrony dziedziczenia. Endpoint Security wspiera tylko Lokalne Skanowanie, gdy Bitdefender Tools wspiera tylko Centralne Skanowanie.

9. **Wdrożenie punktu końcowego z vShield po wykryciu środowiska VMware zintegrowanego z vShield**. Opcja ta może być używana, gdy pakiet instalacyjny jest zainstalowany na maszynie wirtualnej w środowisku VMware zintegrowanym z vShield. W tym przypadku, VMware vShield Endpoint zostanie zainstalowany na komputerze docelowym, zamiast agenta bezpieczeństwa Bitdefender.

   WAŻNE
   Ta opcja jest tylko dla zdalnych wdrożeń, nie dla lokalnych instalacji. Podczas lokalnej instalacji w środowisku VMware zintegrowanym z vShield, masz możliwość pobrania pakietu vShield-Integrated.

10. Podczas dostosowywania silników skanowania przy użyciu skanowania 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**.

11. **Różne**. Możesz skonfigurować następujące opcje dla różnych typów plików z docelowego punktu końcowego:

    - **Zatwiedź crash dumps**. Wybierz tę opcję, żeby pliki memory dump zostały przesłane do Laboratorium analizy Bitdefender jeżeli agent bezpieczeństwa ulegnie awarii. Crash dumps pomogą naszym inżynierom znaleźć co jest powodem problemu i zapobiec jego wystąpieniu następnym razem. Żadne prywatne informacje nie zostaną wysłane.

- **Przesyła pliki objęte kwarantanną do laboratorium Bitdefender co (godziny)**. domyślnie, pliki kwarantanny są automatycznie wysyłane do laboratorium Bitdefender co godzinę. Możesz edytować przedziały czasu pomiędzy plikami kwarantanny, które zostały wysłane. Przykładowe pliki będą przeanalizowane przez badaczy szkodliwego oprogramowania firmy Bitdefender. Jeśli obecność szkodliwego oprogramowania zostanie potwierdzona, odpowiednia sygnatura umożliwi usunięcie tego oprogramowania.
- **Wyślij podejrzane pliki wykonywalne do Bitdefender**. Wybierz tę opcję, aby pliki, które wydają się niegodne zaufania lub podejrzanie się zachowują będą wysyłane do Laboratoriów Bitdefender do analizy.

12. 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.
13. 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.
14. Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.
15. 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.
16. W sekcji **Wdrożeniowiec**, wybierz podmiot, do którego będzie podłączony docelowy punkt końcowy do instalacji i aktualizacji klienta:
    - **Urządzenie GravityZone**, gdy punkty końcowe łączą się bezpośrednio do Urządzenia GravityZone.

      W tym przypadku, możesz także zdefiniować:

      – Niestandardowy Communication Server wpisując jego adres IP lub nazwę hosta, jeśli jest to wymagane.

– Ustawienia proxy, jeśli docelowy punkt końcowy komunikuje się z Urządzeniem GravityZone poprzez proxy. W tym przypadku, 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.

17. 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.

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 pozwala na zdalną instalację agenta bezpieczeństwa na punkcie końcowym dla integracji środowiska z Control Center i na innych punktach końcowych wykrytych w sieci poprzez użycie zadania instalacyjnego. W środowiskach VMware, zdalna instalacja polega na VMware Tools, natomiast w środowiskach Citrix XenServer, opiera się ona na akcjach administracyjnych Windows i SSH.

Gdy agent bezpieczenstwa jest zainstalowany na punkcie końcowym, może zająć kilka minut zanim reszta punktów końcowych w sieci pojawi się w Control Center.

Bitdefender Endpoint Security Tools zawiera mechanizm automatycznego wykrywania sieci, która umożliwia wykrywanie punktów końcowych, które nie są w usłudze Active Directory. Wykryte punkty końcowe są widoczne jako

niezarządzane na stronie **Sieć**, w widoku **Komputery**, w **Grupa Niestandardowa**. Control Center automatycznie usuwa punkty końcowe Active Directory z listy wykrytych punktów końcowych.

Aby włączyć wyszukiwanie sieci, musisz mieć zainstalowany Bitdefender Endpoint Security Tools przynajmniej na jednym punkcie końcowym w sieci. Ten punkt końcowy będzie używany do skanowania sieci i instalacji Bitdefender Endpoint Security Tools na niechronionych punktach końcowych.

Aby uzyskać więcej informacji o wykrywaniu sieci, odwołaj się do „Jak działa wyszukiwanie sieci" (p. 111).

Wymagania zdalnej instalacji

Aby zdalna instalacja działała:

- 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:

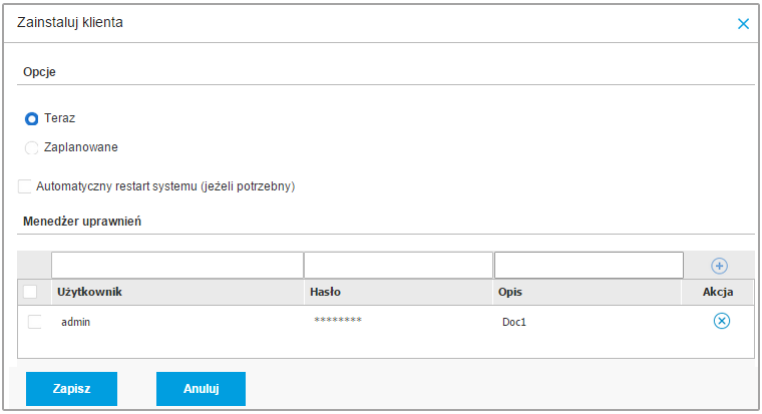
1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć**.
3. Wybierz **Komputery i Wirtualne Maszyny** z selektora widoku.

4. 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**.

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

   Kreator **Klienta Instalacji** został wyświetlony.



Instalowanie Bitdefender Endpoint Security Tools z menu zadań

7. 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.

8. Jeśli chcesz, by docelowe punkty końcowe samoczynnie się uruchamiały, aby zakończyć instalację, wybierz **Automatyczny restart (w razie potrzeby)**.
9. W sekcji **Menadżer poświadczeń**, wybierz poświadczenia administracyjne potrzebne do zdalnego uwierzytelnienia na docelowych punktach końcowych. Możesz dodać poświadczenia przez wpisanie użytkownika i hasła dla docelowego systemu operacyjnego.

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 i hasło konta administratora w odpowiednie pola z nagłówka tabeli.

   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.

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

b. 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.

10. 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.

11. W sekcji **Wdrożeniowiec**, wybierz podmiot, do którego będzie podłączony docelowy punkt końcowy do instalacji i aktualizacji klienta:

- **Urządzenie GravityZone**, gdy punkty końcowe łączą się bezpośrednio do Urządzenia GravityZone.

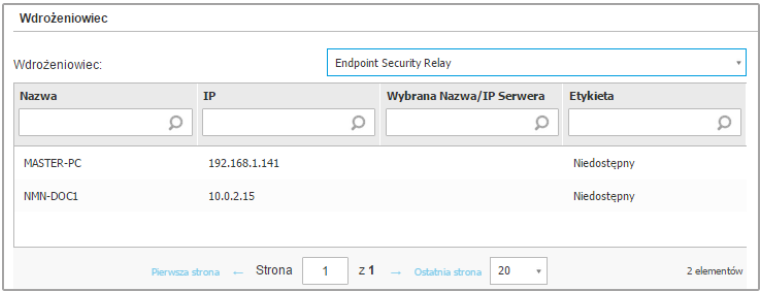
  W tym przypadku, możesz także zdefiniować:

  – Niestandardowy Communication Server wpisując jego adres IP lub nazwę hosta, jeśli jest to wymagane.

  – Ustawienia proxy, jeśli docelowy punkt końcowy komunikuje się z Urządzeniem GravityZone poprzez proxy. W tym przypadku, 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 wdrożenia poprzez agenta relay aby mógł działać.



12. Użyj sekcji **Dodatkowe cele** jeśli chcesz wdrożyć klienta do konkretnych maszyn w sieci, które nie są widoczne w zasobach sieci. Rozwiń sekcję i podaj adres IP lub nazwy hostów tych maszyn w odpowiednich polach, oddzielone przecinkiem. Możesz dodać dowolną liczbę adresów IP.
13. 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.
14. 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. 96).

    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.
15. 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

Oprócz integracji z usługa Active Directory, Security for Endpoints zawiera również mechanizm automatycznego wykrywania sieci, przeznaczony 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.

3.4. 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

3.4.1. 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.

3.4.2. 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. 94).

3.5. Instalowanie HVI

Aby móc korzystać z HVI na maszynach wirtualnych od swoich hostów Xen, należy wykonać następujące kroki:

1. Sprawdź wstępne wymagania instalacji
2. Zainstaluj Security Server
3. Zainstaluj Pakiet Uzupełniający HVI

Warunki wstępne

- XenServer jest zintegrowany z GravityZone.
- XenCenter jest zainstalowany na Twojej maszynie.

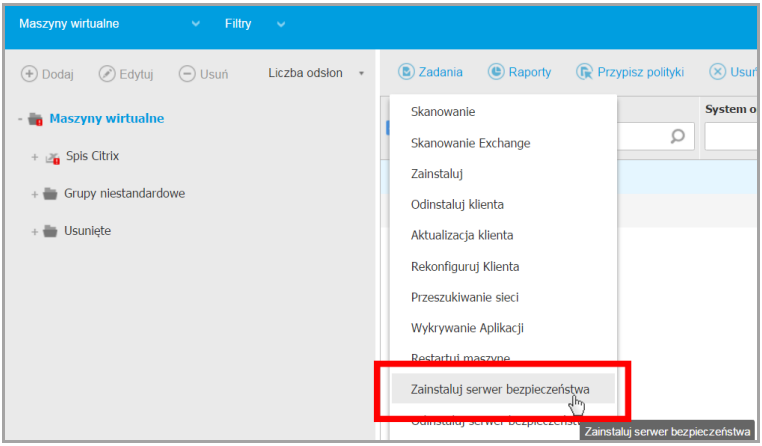
Instalowanie Security Server

Aby zainstalować Security Server na jednym lub kilku hostach:

1. Przejdź do strony **Sieć**.
2. Wybierz **Maszynę Wirtualną** z selektora widoku.
3. Przejrzyj inwentaryzację Citrix i zaznacz pola wyboru odpowiadające żądanym hostom. Dla szybkiej selekcji, możesz bezpośrednio wybrać główny kontener (Citrix Inventory). Będziesz mógł wybrać hosty indywidualnie z kreatora instalacji.

Notatka
Nie możesz wybrać hostów z różnych folderów.

4. Kliknij przycisk **Zadania** w górnej części tabeli i wybierz **Zainstaluj Security Server** z menu. Okno **Instalacja Security Server** zostało wyświetlone.



Instalowanie Security Server

5. Wybierz hosty na których chcesz zainstalować Security Server.
6. Wybierz ustawienia konfiguracji jakich chcesz używać.

WAŻNE
Korzystanie z ustawień wspólnych podczas wdrażania wieloplatformowego Security Server jednocześnie wymaga hostów udostępniających tą sama ilość pamięci, których adresy IP są przypisane do serwerów DHCP i będą częścią tej samej sieci.

Przy wyborze konfiguracji każdego innego Security Server, będziesz w stanie określić ustawienia, takie jakie chcesz dla każdego hosta w kolejnym kroku kreatora. Czynności opisane dalej stosuje się w przypadku, gdy używana jest opcja **Skonfiguruj każdy Security Server**.

7. Kliknij **Dalej**.

Notatka
W zależności od wcześniej wykonanego wyboru, niektóre funkcje opisane w niniejszym dokumencie mogą nie mieć zastosowania do Twojej sytuacji.

8. Podaj sugestywną nazwę dla Security Server.
9. Wybierz kontener, w których chcesz zawrzeć Security Server z menu **Kontener**.
10. Wybierz dysk docelowy.
11. Wybierz rodzaj dysku rezerwowego. Jest zalecane aby wdrożyć urządzenie używając dysku rezerwowego.

    WAŻNE
    Jeżeli używasz małego dysku rezerwowego i miejsce na dysku się skończyło, Security Server zamrozi się, w konsekwencji host pozostanie niechroniony.

12. Skonfiguruj pamięć i zasoby procesora alokacji na podstawie wskaźnika konsolidacji VM na hoście. Wybierz **Niskie**, **Średnie** lub **Wysokie** aby załadować zalecane ustawienia alokacji zasobów lub **Ręczne** do konfiguracji zasobów ręcznej alokacji.
13. Ustaw strefę czasową urządzenia.
14. Ustaw hasło administratora dla konsoli Security Server. Ustaw hasło administracyjne nadpisując domyślne hasło ("sve").
15. Wybierz typ konfiguracji sieci z sieci Bitdefender. Adres IP Security Server nie może się zmienić w czasie gdy jest używany przez Linuksowych agentów do komunikacji.

    Jeśli zdecydujesz się wybrać DHCP, upewnij się, że skonfigurowałeś serwer DHCP, aby zarezerwował adres IP dla urządzenia.

    Jeżeli wybierzesz statyczne, musisz podać adres IP, maska subnet, bramę i informacje DNS.

16. Kliknij **Zapisz**.

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

Instalowanie Pakietu Uzupełniającego HVI

1. Przejdź do strony **Konfiguracja > Aktualizacja**.
2. Wybierz Pakiet Uzupełniający HVI z listy **Komponenty** i kliknij przycisk **Pobierz** w górnej części tabeli.
3. Przejdź do strony **Sieć** i wybierz **Maszyny Wirtualne** z selektora widoków.
4. Wybierz **Serwer** z menu **Widoki** w lewym panelu.

5. Wybierz jeden lub więcej hostów Xen z inwentaryzacji sieci. Możesz łatwo zobaczyć dostępne hosty zaznaczając opcję **Wpisz > Hosty** z menu **Filtry**.
6. Kliknij przycisk **Zadania** po prawej stronie panelu i wybierz **Zainstaluj Pakiet Uzupełniający HVI**. Otwiera się okno instalacyjne.
7. Zaplanuj kiedy zadanie instalacyjne powinno się rozpocząć. Możesz wybrać czy uruchomić zadanie natychmiast po zapisaniu zadania, czy w określonym czasie. W przypadku, gdy instalacja nie może zostać wykonana w określonym czasie, zadanie automatycznie powtarza się zgodnie z ustawieniami powtarzania. Na przykład, jeśli zaznaczyłeś więcej hostów i jeden host nie jest dostępny, gdy pakiet jest zaplanowany do instalacji, zadanie zostanie uruchomione ponownie w określonym czasie.
8. Host musi zostać zrestartowany, aby zastosować zmiany i zakończyć instalację. Jeśli chcesz, aby ponownie uruchomić hosta bez nadzoru, wybierz **Automatycznie uruchom ponownie hosta**.
9. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

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

3.6. Instalowanie Ochrony Urządzeń Mobilnych

Security for Mobile to mobilne rozwiązanie do zarządzania urządzeniami przenośnymi iPhone, iPad i Android. Żeby uzyskać pełną listę wspieranych wersji systemów operacyjnych, sprawdź Wymagania systemu.

Aby zarządzać Security for Mobile z Control Center, musisz dodać urządzenie do Active Directory lub niestandardowego użytkownika, następnie zainstaluj aplikacje GravityZone Mobile Client na urządzeniu. Po ustawieniu usług, możesz uruchomić zadania administracyjne na urządzeniach przenośnych.

Przed rozpoczęciem, upewnij się, że Skonfigurowano publiczny (zewnętrzny) adres dla Serwera komunikacji.

Zainstaluj Security for Mobile:

1. Jeżeli nie zintegrowałeś Active Directory, musisz utwórz użytkowników dla urządzeń mobilnych właścicieli.
2. Dodaj urządzenia do użytkowników.
3. Zainstaluj GravityZone Mobile Client na urządzeniu i aktywuj je.

3.6.1. Skonfiguruj zewnętrzny adres dla serwera komunikacji

W domyślnych ustawieniach GravityZone, urządzenia przenośne mogą być zarządzane tylko wtedy gdy są one przyłączone bezpośrednio do sieci korporacyjnej (przez Wi-Fi lub VPN). Dzieje się tak, ponieważ podczas rejestracji urządzeń przenośnych są one skonfigurowane by łączyć się z lokalnym adresem urządzenia Serwera komunikacji.

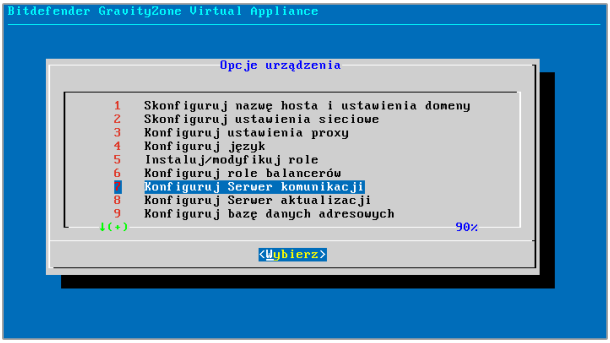
Aby móc zarządzać urządzeniami przenośnymi za pośrednictwem internetu bez względu na to gdzie się znajdują, należy skonfigurować serwer komunikacji używając publicznego adresu.

Aby móc zarządzać urządzeniami mobilnymi, gdy nie są podłączone do sieci firmy, dostępne są następujące opcje:

- Skonfigurować przekierowanie portów na bramie firmowej na urządzenia z rolą serwera komunikacyjnego.
- Dodaj kartę sieciową do urządzenia z działającego w roli serwera komunikacyjnego i przypisz mu publiczny adres IP.

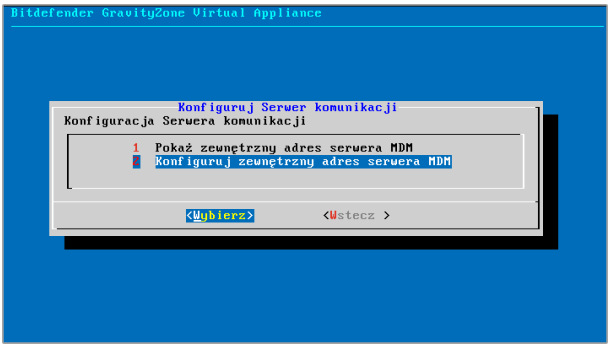
W obu przypadkach, należy skonfigurować serwer komunikacyjny z adresem zewnętrznym by mógł być wykorzystywany do zarządzania urządzeniem mobilnym:

1. Dostęp do konsoli urządzeń z narzędzia zarządzającego wirtualizacją (np. Klient vSphere).
2. Z menu głównego wybierz **Konfiguruj Serwer Komunikacyjny**.



Okno opcji aplikacji

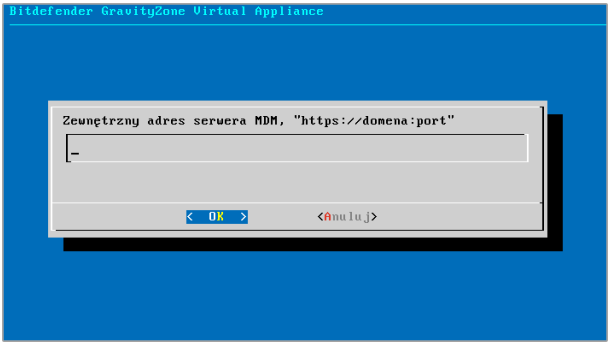
3. wybierz **Konfiguruj zewnętrzny adres serwera MDM**



Konfiguruj okno Serwera komunikacji

4. Podaj adres zewnętrzny.

   Użyj następującej składni: `https://<IP/Domain>:<Port>`.



Okno do wprowadzenia Zewnętrznego adresu serwera MDM

- Jeśli używasz przekierowania portów, musisz wpisać publiczny adres IP lub nazwę domeny oraz port otwarty na bramce.
- Jeśli korzystasz z publicznego adresu dla serwera komunikacyjnego, należy wprowadzić publiczny adres IP lub nazwę domeny oraz port komunikacyjny serwera. Domyślny port `8443`.

5. Wybierz **OK** aby zapisać zmiany.

3.6.2. Utwórz i uporządkuj niestandardowych użytkowników

W sytuacji gdy nie ma przynależności do Active Directory, musisz najpierw stworzyć niestandardowego użytkownika w celu oznaczenia właścicieli do identyfikacji urządzeń przenośnych. Określeni użytkownicy urządzeń mobilnych nie są związane w żaden sposób z Active Directory lub z innymi użytkownikami zdefiniowanymi w Control Center

Tworzenie niestandardowych użytkowników.

Aby utworzyć niestandardowego użytkownika:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektora wyświetleń.
3. W panelu po lewej stronie **Niestandardowe Grupy**.
4. Naciśnij ikonę **Dodaj użytkownika** na pasku narzędzi działań. Wyświetlone zostanie okno konfiguracji.
5. Określ szczegóły wymaganego użytkownika:
   - sugestywna nazwa użytkownika (np. pełna nazwa użytkownika)
   - Adres e-mail użytkownika

   WAŻNE
   - Upewnij się, że podano poprawny adres e-mail. Użytkownik dostanie instrukcje instalacyjne na maila, po dodaniu urządzenia.
   - Każdy adres e-mail może być połączony tylko z jednym użytkownikiem.

6. Kliknij **OK**.

Porządkowanie niestandardowych użytkowników

Aby uporządkować niestandardowych użytkowników:

1. Dodaj niestandardowe grupy.
   a. Wybierz **Niestandardową Grupę** w panelu po lewej stronie i kliknij ikonę **Dodaj** na pasku narzędzi działań (nad panelem).
   b. Podaj sugestywna nazwę dla grupy i naciśnij **OK**. Nowa grupa wyświetli się w **Grupy Niestandardowe**.
2. Przesuń niestandardowych użytkowników do niestandardowych grup.

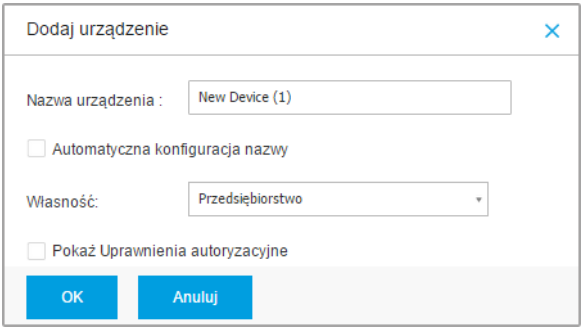
a. Wybierz użytkowników w prawym panelu.

b. Przeciągnij i upuść wybrane elementy w pożądanej grupie w lewym panelu bocznym.

3.6.3. Dodaj urządzenia do użytkowników

Aby dodać urządzenie do użytkownika:

1. Przejdź do strony **Sieć**.
2. Wybierz **Urządzenia Mobilne** z selektora wyświetleń.
3. Wyszukaj użytkownika w folderze Active Directory lub w innej grupie niestandardowej.
4. Kliknij ikonę ⊕ **Dodaj Urządzenie** w górnej części tabeli sieci. Wyświetlone zostanie okno konfiguracji.



Dodaj urządzenie mobilne do użytkownika.

5. Podaj sugestywną nazwę dla urządzenia.
6. Użyj opcji **Automatyczna konfiguracja nazwy** jeśli chcesz aby nazwa była automatycznie generowana. kiedy dodajesz urządzenia ma wygenerowaną nazwę. Kiedy urządzenie jest włączone, automatycznie zmienia nazwę z odpowiednimi informacjami producenta i modelu.
7. Wybierz rodzaj własności urządzenia (Enterprise lub Personal).
8. Zaznacz opcje **Pokaż poświadczenia aktywacyjne** po naciśnięciu przycisku **OK** jeżeli instalujesz GravityZone Mobile Client na urządzeniu użytkownika.

9. Kliknij **OK**. Użytkownik niezwłocznie dostanie wiadomość e-mail z instrukcjami dotyczącymi instalacji i szczegółami aktywacji do konfiguracji urządzenia przenośnego. Szczegóły aktywacyjne zawierają token aktywacyjny i adres serwera komunikacyjnego (i odpowiedni QR kod).

Notatka

- Możesz zobaczyć szczegóły aktywacji urządzenia w każdym momencie poprzez naciśnięcie nazwy w Control Center.
- Możesz również dodać urządzenie przenośne dla wybranych użytkowników i grup. W tym przypadku, okno konfiguracyjne pozwoli zdefiniować tylko właściciela urządzenia. Urządzenia przenośne stworzone przez wielokrotną selekcje dostaną domyślna nazwę rodzajową. Jak tylko urządzenie zostanie zapisane, jego nazwa automatycznie się zmieni, w tym odpowiednie etykiety producenta i modelu.

3.6.4. Zainstaluj GravityZone Mobile Client na urządzeniu

Aplikacja GravityZone Mobile Client jest rozprowadzana wyłącznie za pośrednictwem Apple App Store i Google Play.

Zainstaluj GravityZone Mobile Client na urządzeniu

1. Poszukaj aplikacji w oficjalnym sklepie.
   - Google Play link
   - Apple App Store link
2. Pobierz i zainstaluj aplikację na urządzeniu.
3. Uruchom aplikację i dokonaj wymaganą konfigurację:
   a. Na urządzeniu Android, zakładka **Aktywne** służy do włączenia GravityZone Mobile Client na urządzeniu administratora. Przeczytaj uważnie dostarczone informacje.
   b. Podaj token aktywacyjny i adres serwera komunikacyjnego, alternatywnie możesz zeskanować kod QR otrzymany mailem.
   c. Dotknij **Aktywuj**.
   d. Na urządzeniu iOS, pojawi się monit o zainstalowanie profilu MDM. Jeśli urządzenie jest chronione hasłem, użytkownik zostanie poproszony o podanie go. Uzupełnij profil instalacyjny zgodnie z instrukcjami pojawiającymi się na ekranie.

3.7. Instalowanie Kreatora Raportów

Kreator Raportów pozwala Ci na tworzenie i zarządzanie zapytaniami i szczegółowymi raportami w GravityZone

Konstruktor Raportów jest wyposażony w dwie role: Baza danych i Procesory. Musisz utworzyć dwie instancje Kreatora Raportów z Wirtualnego Narzędzia, jedno na każdą rolę. Te działają obok Urządzenia Wirtualnego GravityZone, będąc połączonym do drugiej bazy danych.

Dla sprawnej instalacji, najpierw upewnij się, że środowisko wirtualne spełnia wymagania sprzętowe i programowe. Następnie, musisz mieć pod ręką:

- Obraz urządzenia wirtualnego Konstruktora Raportu, który użyjesz do zainstalowania obu ról Bazodanowej i Procesorów.. Można pobrać obraz Report Builder VA stąd.
- Nazwa DNS lub adres IP GravityZone Virtual Appliance
- Nazwa użytkownika i hasło administratora domeny
- Hasło lub baza danych GravityZone. Jeśli zapomniałeś, możesz utworzyć jeszcze jeden w interfejsie konsoli urządzenia GravityZone.

Instalacja Konstruktora Raportów zakłada dwa etapy:

- Instalowanie Bazy danych Kreatora Raportu
- Instalowanie Procesorów Kreatora Raportu

W najlepsza praktyka, należy najpierw zainstalować GravityZone i ustawić Control Center (w razie potrzeby), a następnie zaktualizować GravityZone, wdrożyć ochronę na punktach końcowych, a w końcu zainstalować role Konstruktor Raportu.

3.7.1. Instalowanie Bazy danych Kreatora Raportu

Aby zainstalować rolę Kreatora Raportu Bazodanowego:

1. Importuj urządzenie wirtualne Konstruktor Raportu w swoim zwirtualizowanym środowisku.
2. Zasilanie urządzenia.
3. Z Twojego narzędzia do zarządzania wirtualizacjami, wejdź do interfejsu konsoli Kreatora Raportów.
4. Ustaw hasło dla wbudowanego `bdadmin` administratora systemu.

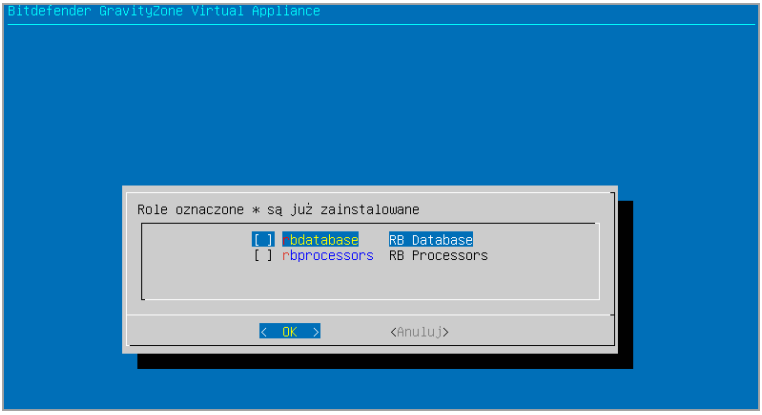
5. Zaloguj się korzystając z hasła, które ustawiłeś, aby uzyskać dostęp do interfejsu urządzenia konfiguracji. Użyj klawiszy strzałek i przycisku `Tab` do nawigacji w menu i opcjach. Naciśnij `Enter`, aby wybrać konkretną opcję.

   Początkowo, interfejs urządzenia jest po angielsku.

   Aby zmienić język interfejsu:
   a. Wybierz **Konfiguracja Języka** z menu głównego.
   b. Wybierz język z dostępnych opcji. Pojawi się nowa wiadomość potwierdzająca.

   Notatka
   Być może trzeba przewinąć w dół, aby zobaczyć swój język.

   c. Wybierz **OK** aby zapisać zmiany.
6. Idź do **Ustawienia Zaawansowane** i wybierz **Połącz do Istniejącej Bazy Danych**.
7. Wprowadź adres IPC i hasło bazy danych GravityZone.
8. Z menu **Zaawansowane Ustawienia**, zaznacz **Zainstaluj/Odinstaluj Role**.
9. Idź do **Dodaj lub usuń role** i wybierz **Baza danych RB**. Naciśnij `Spację`, aby zaznaczyć, aby zainstalować tę rolę, a następnie `Enter`, aby kontynuować. Naciśnij ponownie `Enter` aby zatwierdzić i czekać na koniec instalacji.



Kreator raportów w interfejsie konsoli: instaluje Bazę Danych

Notatka
Report Builder Database instaluje i działa tylko w samodzielnej instancji. Replica Set kopie zapasowe nie są obsługiwane.

3.7.2. Instalowanie Procesorów Kreatora Raportu

Aby zainstalować rolę Kreatora Raportu Procesorów:

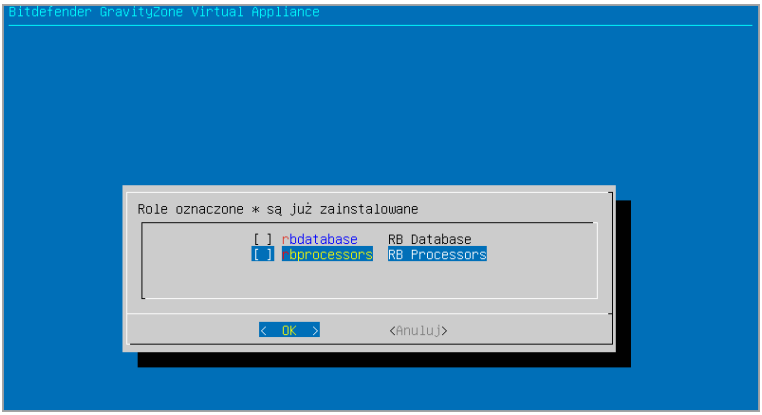
1. Importuj urządzenie wirtualne Konstruktor Raportu w swoim zwirtualizowanym środowisku.
2. Zasilanie urządzenia.
3. Z Twojego narzędzia do zarządzania wirtualizacjami, wejdź do interfejsu Kreatora Raportów.
4. Ustaw hasło dla wbudowanego `bdadmin` administratora systemu.
5. Zaloguj używając ustawionego hasła. Będziesz miał dostęp do interfejsu konfiguracyjnego urządzenia. Użyj klawiszy strzałek i przycisku `Tab` do nawigacji w menu i opcjach. Naciśnij `Enter`, aby wybrać konkretną opcję.

   Początkowo, interfejs urządzenia jest po angielsku.

   Aby zmienić język interfejsu:
   a. Wybierz **Konfiguracja Języka** z menu głównego.
   b. Wybierz język z dostępnych opcji. Pojawi się nowa wiadomość potwierdzająca.

      Notatka
      Być może trzeba przewinąć w dół, aby zobaczyć swój język.

   c. Wybierz **OK** aby zapisać zmiany.
6. Idź do **Ustawienia Zaawansowane** i wybierz **Połącz do Istniejącej Bazy Danych**.
7. Wprowadź adres IPC i hasło bazy danych GravityZone.
8. Z menu **Zaawansowane Ustawienia**, zaznacz **Zainstaluj/Odinstaluj Role**.
9. Idź do **Dodaj lub usuń role** i wybierz **Procesory RB**. Naciśnij `Spację`, aby zaznaczyć, aby zainstalować tę rolę, a następnie `Enter`, aby kontynuować. Naciśnij ponownie `Enter` aby zatwierdzić i czekać na koniec instalacji.



Kreator raportów w interfejsie konsoli: instaluje procesory

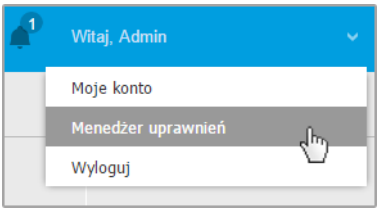
Po zainstalowaniu Kreatora raportów, nowa opcja **Zapytania** wyświetli się pod sekcją **Raporty** w Control Center

Role Baza Danych i Procesory Konstruktora Raportu są wyświetlane w sekcji **Infrastruktura** na stronie **Konfiguracja > Aktualizacja**, wraz z innymi rolami GravityZone.

3.8. Menedżer uprawnień

Menadżer Poświadczeń pomaga definiować poświadczenia wymagane podczas dostępu do zasobów Serwera vCenter i do zdalnego uwierzytelniania na rożnych systemach operacyjnych w twojej sieci.

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



Menu menadżera poświadczeń

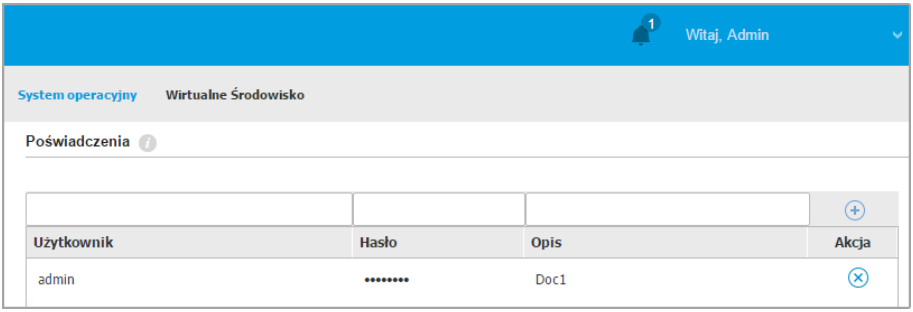
Okno **Menadżer poświadczeń** zawiera dwie zakładki:

- System operacyjny
- Wirtualne Środowisko

3.8.1. System operacyjny

Z zakładki **System Operacyjny** możesz zarządzać poświadczeniami administratora wymaganymi do zdalnego uwierzytelniania podczas zadań instalacji 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.

3.8.2. Wirtualne Środowisko

W zakładce Środowisko Wirtualne, możesz zarządzać uwierzytelnianiem poświadczeń dla dostępnych systemów serwera zwirtualizowanego.

Aby mieć dostęp do zwirtualizowanej struktury zintegrowanej z Control Center musisz podać swoje poświadczenia użytkownika dla każdego dostępnego systemu serwera wirtualizacji. Control Center używa twoich poświadczeń, aby połączyć z wirtualną infrastrukturą, pokazywanie tylko zasobów do których masz dostęp (jak określono w serwerze zwirtualizowanym).

Aby określić poświadczenia wymagane do połączenia się z serwerem zwirtualizowanym:

1. Wybierz serwer z odpowiedniego menu.

Notatka
Jeżeli menu jest niedostępne, albo nie została jeszcze skonfigurowana integracja lub wszystkie niezbędne poświadczenia zostały już skonfigurowane.

2. Podaj swoją nazwę użytkownika, hasło i sugestywny opis.
3. Kliknij przycisk ⊕ **Dodaj** . Nowe ustawienia poświadczeń zostały dodane do tabeli.

Notatka
Jeżeli nie skonfigurowałeś poświadczeń uwierzytelnienia w Menadżerze poświadczeń, będziesz musiał podać je podczas próby przeglądania spisu dowolnego systemu serwera zwirtualizowanego. Po wprowadzeniu swoich poświadczeń, zostaną one zapisane w Menadżerze Poświadczeń tak, by nie było potrzeby wprowadzania ich ponownie.

WAŻNE
Za każdym razem, gdy zmienisz hasło użytkownika serwera zwirtualizowanego, pamiętaj aby uaktualnić je w Menadżerze Poświadczeń.

3.8.3. 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. AKTUALIZOWANIE GRAVITYZONE

Bitdefender publikuje wszystkie aktualizacje produktu i sygnatur serwery Bitdefender w Internecie. Wszystkie aktualizacje są zaszyfrowane i podpisane cyfrowo, żeby nie można nimi było manipulować.

GravityZone zawiera role Aktualizacji Serwera, został zaprojektowany aby służyć jako centralny punkt dystrybucji aktualizacji dla twojego wdrożenia GravityZone Serwer Aktualizacji sprawdza za dostępnymi aktualizacjami GravityZone do pobrania z serwera aktualizacji Bitdefender w Internecie, tworząc je dostępnymi w sieci lokalnej. komponenty GravityZone mogą być konfigurowane do automatycznej aktualizacji z lokalnego serwera aktualizacji zamiast z Internetu.

Kiedy nowa aktualizacja jest dostępna, appliance GravityZone, agent ochrony Security Server sprawdza cyfrowe sygnatury aktualizacji pod kątem autentyczności i integralność zawartości pakietu. Następnie, każdy plik aktualizacji jest parsowany a jego wersja sprawdzona w porównaniu z zainstalowanym. Nowsze pliki są pobierane lokalnie i sprawdzane pod kątem ich MD5 hash, aby się upewnić, że nie są zmienione.

Jeśli w jakimś momencie sprawdzanie będzie błędne, proces aktualizacji zatrzyma się i wyrzuci błąd. W innym przypadku, aktualizacja jest pozytywna i gotowa do zainstalowania.

Aby zaktualizować urządzenia GravityZone zainstalowane w twoim środowisku i pakiety instalacyjne komponentów GravityZone, zaloguj się do firmy poprzez konto administracyjne i idź do strony **Konfiguracja > Aktualizacja**.

4.1. Aktualizacja urządzeń GravityZone

Aby zobaczyć informacje na temat wdrożonej wersji GravityZone i dostępnych aktualizacjach, przejdź do strony **Konfiguracja > Aktualizacja**. Możesz przejrzeć zainstalowane urządzenia GravityZone i uruchomione role w sekcji **Infrastruktura**. Możesz:

- Aktualizuj manualnie Urządzenia GravityZone
- Włącz automatyczną aktualizację

Ręczne Aktualizacje

W zakładce **Role GravityZone**, kliknij **Aktualizuj**, aby zrobić upgrade GravityZone do najnowszej wersji. Przed jakąkolwiek aktualizacją, zaleca się by sprawdzić

dziennik zmian nowej wersji. Informacje o Wydaniu dla każdej nowej wersji produktu, są również publikowane w Bitdefender Centrum Wsparcia.

Notatka
Klawisz **Aktualizuj** jest dostępny tylko kiedy **Status** aktualizacji wykazuje **Błąd** lub **Nieaktualny** aktualizacja może zająć chwile. po aktualizacji, upewnij się, wyczyściłeś pamięć podręczna przeglądarki.

Automatyczna aktualizacja

Automatyczna aktualizacja jest domyślnie wyłączona. Aby zmienić te ustawienie, idź do **Konfiguracja >Aktualizacja** i zaznacz checkbox**Włącz automatyczna aktualizacje**

Aby zaplanować automatyczne aktualizacje:

1. Ustaw **Powtarzalność** na **Codziennie**, **Tygodniowy** (zaznacz jeden lub więcej dni tygodnia) or **Miesięczna**.
2. Zdefiniuj **Interwał**. Można zaplanować czas procesu aktualizacji, aby rozpocząć, gdy nowa aktualizacja jest dostępna.

Zaznacz checkbox **alarm 30 minut do aktualizacji** zanim wyświetlisz wszystkim użytkownikom ostrzeżenie o 30 minutach do automatycznej aktualizacji.

W trakcie aktualizacji, wszyscy użytkownicy zostaną wylogowani, wyświetli się też ekran informujący użytkowników, że aktualizacja jest w toku.

Po zakończeniu automatycznego upgrade'u, wszyscy użytkownicy zostaną przekierowani do strony logowania. Wyskakujące okienko wyświetli nowe funkcje.

Jeżeli masz więcej urządzeń GravityZone w swoim środowisku sieciowym, wraz z automatyczną aktualizacją, wszystkie zostaną podniesione do najnowszej wersji.

4.2. Konfigurowanie Serwera Aktualizacji

Domyślne, Serwer Aktualizacji będzie pobierał aktualizacje z Internetu co godzinę. Zaleca się, aby nie zmieniać ustawienia domyślnych serwera aktualizacji.

Aby sprawdzić i skonfigurować ustawienia aktualizacji serwera:

1. Przejdź do strony **Aktualizacja** w Control Center i kliknij zakładkę **Komponenty**.
2. Kliknij przycisk **Ustawienia** w górnej części panelu po lewej stronie, aby wyświetlić okno **Aktualizuj Ustawienia Serwera**.

3. W **Konfiguracja Serwera Aktualizacji**, możesz sprawdzić konfiguracje głównych ustawień.
   - **Adres Pakietów.** Adres, z którego pobierane są paczki.
   - **Adres Aktualizacji.** Serwer Aktualizacji jest skonfigurowany żeby sprawdzać czy są aktualizacje do pobrania z `upgrade.bitdefender.com:80`. Jest to standardowy adres przekierowujący do najbliższego serwera Bitdefender, na którym znajdują się aktualizacje.
   - **Port.** Kiedy konfigurujesz różne komponenty GravityZone, żeby uaktualnić z Serwera Aktualizacji, musisz podać ten port. Domyślny port `7074`.
   - **IP.** Adres IP Serwera Aktualizacji.
   - **Okres aktualizacji (godziny).** Jeśli chcesz zmienić okres aktualizacji, wpisz w to pole nową wartość. Wartość domyślna to 1.
4. Możesz skonfigurować Serwer Aktualizacji, aby automatycznie pobierał Security Server i zestawy punktów końcowych.
5. Serwer Aktualizacji może działać jako brama dla danych wysyłanych przez klienta produktów Bitdefender zainstalowanych w sieci dla serwerów Bitdefender. Dane te mogą obejmować anonimowe raporty dotyczące aktywności wirusów, zgłoszenia awarii produktu i dane wykorzystane do rejestracji on-line. Uruchomienie roli bramy jest przydatne do kontrolowania ruchu i w sieciach bez dostępu do Internetu.

   Notatka
   W dowolnym momencie możesz zablokować moduły wysyłające do laboratorium Bitdefender dane statystyczne lub dane o awariach. Możesz użyć polityk, aby zdalnie kontrolować te opcje na komputerach i wirtualnych maszynach zarządzanych przez Control Center.

6. Kliknij **Zapisz**.

4.3. Pobieranie Aktualizacji Produktu

Możesz zobaczyć informacje na temat istniejących paczek komponentów GravityZone w zakładce **Komponenty**. Dostępne informacje o obecnej wersji, wersji aktualizacji (jeśli jest jakaś) i status operacji aktualizacji jakie rozpocząłeś.

Aby zaktualizować komponenty GravityZone:

1. Przejdź do strony **Aktualizacja** w Control Center i kliknij zakładkę **Komponenty**.
2. Kliknij komponent, który chcesz aktualizować na liście **Produktów**. Wszystkie dostępne wersje będą wyświetlone w tabeli **Pakiety**. Zaznacz pole wyboru odpowiednie dla wersji, którą chcesz pobrać.

   Notatka
   Nowe pakiety będą miały status **Niepobrane**. Gdy nowsza wersja jest wydana przez Bitdefender, najstarsza niepobrana wersja zostanie usunięta z tabeli.

3. Kliknij **Akcje** w górnej części tabeli i wybierz **Opublikuj** . Wybrana wersja zostanie pobrana i status zmieni się odpowiednio. Odśwież zawartość tabeli klikając przycisk **Odśwież** i sprawdź odpowiedni status.

WAŻNE
Urządzenie GravityZone nie obejmuje pakietów Security Server domyślnie. Musisz ręcznie ściągnąć potrzebne pakiety Security Server dla swojego środowiska.

4.4. Staging Updates

Staging pozwala Ci na testowanie nowszych zestawów lub aktualizacji produktów w wyizolowanym i kontrolowanym środowisku przed ich publikacją w sieci. Środowisko staging powinno odzwierciedlać produkcję, tak bardzo jak to tylko możliwe, do celów testowania. Poprzez takie działania, możesz zmaksymalizować szansę na odnalezienie jakichkolwiek problemów, które mogą pojawić się w Twoim środowisku, przed wypuszczeniem wersji do produkcji.

Funkcja staging pozwala Ci również tworzyć politykę dla krytycznych punktów końcowych z produkcji. Możesz aktualizować te punkty końcowe, tylko po tym jak aktualizacje zostały przetestowane w środowisku staging'u i na niekrytycznych maszynach z produkcji. Aby uzyskać więcej informacji, odwołaj się do „Publikowanie z Alertami Aktualizacji" (p. 142).

Notatka

- Staging jest domyślnie wyłączony.
- Security Server (VMware z ESX) nie obsługuje staging.

4.4.1. Warunki wstępne

Tryb Staging wymaga od infrastruktury GravityZone spełnienia następujących warunków:

- Serwer aktualizacji należy zainstalować sam na urządzeniu wirtualnym.

  Jeśli masz serwer aktualizacji wraz z innymi rolami na urządzeniu, należy wykonać następujące kroki:

  1. Usuń starą rolę Serwera Aktualizacji.
  2. Zainstaluj nowe urządzenie tylko z Serwerem Aktualizacji.
  3. Podłącz Serwer Aktualizacji do istniejącej bazy danych GravityZone.

  Aby uzyskać więcej informacji na temat instalowania ról GravityZone, przejdź do „Zarządzanie Urządzeniem GravityZone” (p. 70).
- Urządzenie Serwer Aktualizacji musi mieć co najmniej 120 GB.
- Urządzenie Konsola Webowa musi mieć co najmniej 120 GB.

4.4.2. Korzystając ze Staging'u

Aby skonfigurować środowisko staging i przetestować najnowsze aktualizacje należy:

1. Włącz staging i zdefiniuj ustawienia serwera aktualizacji.
2. Zdefiniuj politykę staging'u dla testowanych punktów końcowych.
3. Instaluj pakiety na testowym punkcie końcowym.
4. Przypisz politykę staging'u do testowanych punktów końcowych.
5. Aktualizacja testowych punktów końcowych do najnowszej wersji i test aktualizacji w środowisku staging.
6. Uruchom drugi test przed aktualizacją wszystkich punktów końcowych z produkcji. Możesz najpierw przetestować aktualizację na niekrytycznych punktach końcowych.

Włączanie Staging'u

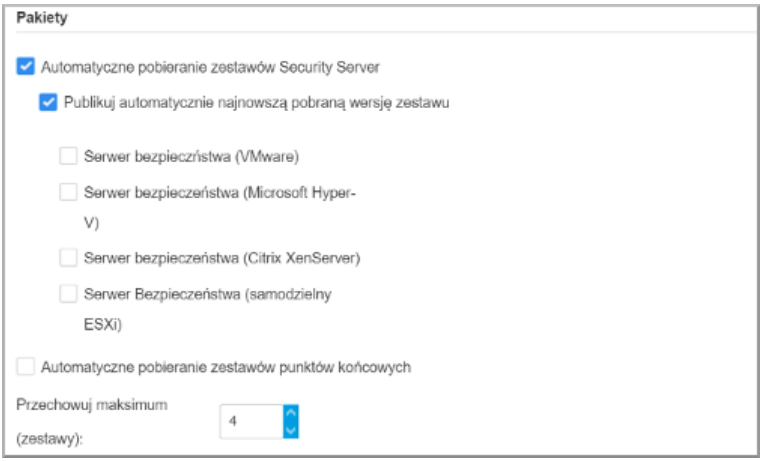
Aby włączyć tryb staging dla aktualizacji GravityZone:

1. Przejdź do strony **Konfiguracja** > **Aktualizacja** i kliknij zakładkę **Komponenty**.

2. Kliknij przycisk **Ustawienia** w górnej części panelu po lewej stronie, aby wyświetlić okno **Aktualizuj Ustawienia Serwera**.
3. Zaznacz pole wyboru **Włącz Staging**.
4. W **Konfiguracja Serwera Produkcyjnego**, konfiguruj główne ustawienia:
   - **Adres Pakietów.** Adres, z którego pobierane są pakiety:`download.bitdefender.com/SMB/Hydra/release`
   - **Adres Aktualizacji.** Adres, z którego pobierane są aktualizacje produktu:`upgrade.bitdefender.com:80`.
   - **Port.** Domyślny port `7074`. Nie możesz edytować tego pola.
   - **IP.** Adres IP Serwera Aktualizacji. Nie możesz edytować tego pola.
   - **Okres aktualizacji (godziny).** Jeśli chcesz zmienić okres aktualizacji, wpisz w to pole nową wartość. Wartość domyślna to 1.
5. Produkcja i serwer aktualizacji mogą działać jako bramy dla danych wysyłanych przez klienta produktów Bitdefender zainstalowanych w sieci dla serwerów Bitdefender. Dane te mogą obejmować anonimowe raporty dotyczące aktywności wirusów, zgłoszenia awarii produktu i dane wykorzystane do rejestracji on-line. Uruchomienie roli bramy jest przydatne do kontrolowania ruchu i w sieciach bez dostępu do Internetu.

   Notatka
   W dowolnym momencie możesz zablokować moduły wysyłające do laboratorium Bitdefender dane statystyczne lub dane o awariach. Możesz użyć polityk, aby zdalnie kontrolować te opcje na komputerach i wirtualnych maszynach zarządzanych przez Control Center.

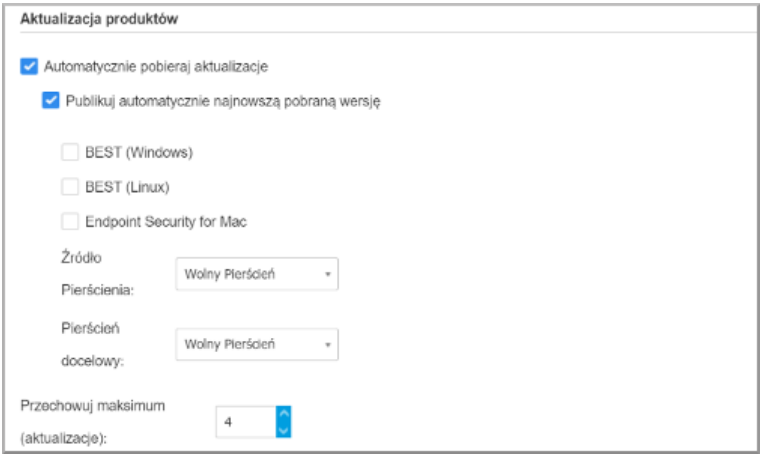
6. W **Serwer Konfiguracji Staging'u**, konfiguruj następujące opcje:
   - **Port.** Domyślny port `7077`.
   - **IP.** Adres IP Serwera Aktualizacji. Nie możesz edytować tego pola.
7. W **Pakietach**, możesz skonfigurować Serwer Aktualizacji, aby automatycznie pobierał i publikował Security Server i zestawy punktów końcowych.



Pakiety - Autopublikowanie

Można również skonfigurować maksymalną liczbę zestawów, które można przechowywać na urządzeniu GravityZone. Wpisz liczbę między 4 a 10 w menu **Zachowaj maksimum (zestawy)**.

8. W **Aktualizacja Produktów**, możesz skonfigurować Serwer Aktualizacji, aby pobrać aktualizacje dla agentów bezpieczeństwa.



Pakiety - Autopublikowanie

Możesz wybrać, aby także automatycznie publikować najnowsze pobrane wersje:

a. Wybierz co najmniej jednego agenta bezpieczeństwa z dostępnej listy.

b. Zdefiniuj alerty źródłowe i docelowe:

- **Alert źródłowy**. Alert wykorzystywany do wysłania aktualizacji w środowisku staging. Gdy wersja jest potwierdzona przez jego wczesne adaptery zostanie to opublikowane na powolnym alercie. To jest wartość domyślna. Najnowsze dostępne aktualizacje będą publikowane na szybkim alercie.
- **Alert docelowy**. Alert wykorzystywany do publikowania aktualizacji w produkcji. Możesz wybrać pomiędzy szybkim i wolnym.

Można również skonfigurować maksymalną liczbę aktualizacji, które można przechowywać na urządzeniu GravityZone. Wpisz liczbę między 4 a 10 w menu **Zachowaj maksimum (aktualizacje)**.

9. Kliknij **Zapisz**.

Po włączeniu staging'u, zbuduj swoje stanowisko staging'u, aby rozpocząć testowanie dostępnych zestawów oraz aktualizacji produktu.

WAŻNE
Wyłączenie staging'u spowoduje usunięcie wszystkich niepublikowanych pakietów oraz aktualizacji produktu.

Definiowanie Polityki Staging'u

Musisz zdefiniować politykę staging'u:

1. Przejdź do strony **Polityki**.
2. Wybierz lub utwórz politykę, aby ją używać w środowisku testowym.
3. W sekcji **Ogólne** > **Aktualizuj**, wprowadź adres Serwera Staging w tabeli **Aktualizuj Lokalizacje**.
4. Skonfiguruj inne ustawienia polityki według uznania. Po więcej szczegółów, zajrzyj do rozdziału **Polityki Bezpieczeństwa** w Przewodniku Administratora GravityZone.
5. Kliknij **Zapisz**.

Staging Pakietów

Aby zainstalować najnowszą paczkę na testowych punktach końcowych:

1. Przejdź do strony **Konfiguracja > Aktualizacja** i wybierz zakładkę **Komponenty**.
2. Kliknij **Sprawdź aktualizacje**, aby upewnić się, że wyświetlasz najnowszą wypuszczoną wersję produktu.
3. Kliknij komponent, który chcesz aktualizować na liście **Produktów**.
4. Wybierz dostępne pakiety z tabeli **Pakiety**, które chcesz testować. Możesz pobrać kilka zestawów dla każdego produktu, do wysokości limitu określonego w oknie **Ustawienia Serwera Aktualizacji**. Gdy ten limit jest osiągnięty, najstarsza wersja jest usuwana z tabeli.
5. Kliknij **Akcje** i wybierz **Pobierz**, aby uzyskać paczkę do swojego urządzenia GravityZone.
6. Mając wybrany pakiet, kliknij **Zapisz na dysku**. Okno konfiguracji pakietu jest wyświetlone.
7. Konfiguruj paczkę. Aby uzyskać więcej informacji, odwołaj się do „Tworzenie pakietów instalacyjnych” (p. 96).
8. Instaluj zestaw na testowych punktach końcowych.
9. Monitoruj zachowanie punktów końcowych.
10. Jeśli paczka została zainstalowana pomyślnie i punkty końcowe zachowują się normalnie, możesz opublikować paczkę w sieci produkcyjnej.

    Aby opublikować paczkę, wybierz to w tabeli **Paczki**, kliknij **Akcje** w górnej części tabeli i wybierz **Publikuj**.

    WAŻNE
    Nie możesz publikować paczek starszych niż te, które już są opublikowane.

11. Jeśli spotkałeś problem z paczką, możesz napisać zgłoszenie do wsparcia. Aby uzyskać więcej informacji, odwołaj się do „Otrzymywanie pomocy” (p. 158).

    Aby usunąć pakiet z urządzenia GravityZone, kliknij przycisk **Akcje** i wybierz **Usuń z dysku**.

Przypisywanie Polityki Staging

Aby przypisać politykę staging'u do testowanych punktów końcowych:

1. Przejdź do strony **Sieć**.
2. Wybierz **Komputery i Wirtualne Maszyny** z selektora widoku.
3. Wybierz pożądaną grupę z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
4. Zaznacz pole wyboru docelowych komputerów lub grup. Możesz wybrać jeden z kilku obiektów tego samego rodzaju tylko tego samego poziomu.
5. Kliknij przycisk **Przypisz Polityki** w górnej części tabeli.
6. Dokonaj niezbędnych ustawień w oknie Przypisanie polityki. Po więcej informacji, odnieś się do rozdziału **Polityka Ochrony >Zarządzanie Politykami > Przypisywanie polityk do punktów końcowych** Przewodnika Administratora GravityZone.

Aktualizacje Produktu Staging

Aby zainstalować najświeższe aktualizacje:

1. Przejdź do strony **Konfiguracja > Aktualizacja** i wybierz zakładkę **Komponenty**.
2. Kliknij **Sprawdź aktualizacje**, aby upewnić się, że wyświetlasz najnowszą wypuszczoną aktualizację produktu.
3. Zaznacz produkt Bitdefender, który wybierasz z listy **Produkt**.

   Notatka
   Możesz używać staging tylko z aktualizacjami dla agentów bezpieczeństwa i nie dla Security Server.

4. Wybierz dostępną aktualizację z tabeli **Aktualizacje**, które chcesz testować.
5. Kliknij **Akcje** i wybierz **Pobierz**, aby uzyskać aktualizację dla swojego urządzenia GravityZone.

   Możesz pobrać kilka aktualizacji dla każdego produktu, do wysokości limitu określonego w oknie **Ustawienia Serwera Aktualizacji**. Gdy ten limit jest osiągnięty, najstarsza wersja jest usuwana z tabeli.
6. Mając wybraną aktualizację, kliknij **Akcje** i wybierz **Dodaj do staging'u**. Aktualizację można zainstalować na testowych punktach końcowych, zgodnie z ustawieniami polityki. Aby uzyskać więcej informacji odwołaj się do „Definiowanie Polityki Staging'u" (p. 139).

7. Jeśli aktualizacja została zainstalowana pomyślnie i punkty końcowe zachowują się normalnie, rozpocznij wysyłanie aktualizacji do maszyn w produkcji. Najpierw, aktualizuj maszyny niekrytyczne, aby uruchomić kolejny test przed aktualizacją krytycznych punktów końcowych. Aby uzyskać więcej informacji, odwołaj się do „Publikowanie z Alertami Aktualizacji" (p. 142).
8. Jeśli spotkałeś problem z aktualizacją, możesz napisać zgłoszenie do wsparcia. Aby uzyskać więcej informacji, odwołaj się do „Otrzymywanie pomocy" (p. 158).

   Aby usunąć niepublikowaną aktualizację z urządzenia GravityZone, kliknij przycisk **Akcje** i wybierz **Usuń**. Możesz usunąć tylko nieopublikowane aktualizacje.

Publikowanie z Alertami Aktualizacji

Aby przetestować aktualizację na niekrytycznych punktach końcowych związanych z produkcją, należy najpierw zmodyfikować istniejące polityki i przypisać im politykę szybkiego pierścienia.

Notatka
Polityka wolnego alertu jest automatycznie przypisana dla wszystkich polityk, które tworzysz.

1. Przejdź do strony **Polityki**.
2. Edytuj ustawienie polityki dla niekrytycznych punktów końcowych w produkcji. W sekcji **Aktualizuj Alert** wybierz **Szybki alert**.

   Notatka
   Aktualizacja publikowana na szybkim alercie nie może być starsza niż publikowana na wolnym alercie.

3. Publikuj aktualizację na szybkim alercie:
   a. Przejdź do strony **Konfiguracja** > **Aktualizacja** i wybierz zakładkę **Komponenty**.
   b. Wybierz aktualizację w tabeli Aktualizacje kliknij przycisk **Akcje** w górnej części tabeli i wybierz **Publikuj**.
   c. Zaznacz opcję szybkiego alertu.

Notatka
Kiedy po raz pierwszy publikujesz aktualizację, będzie ona dostępna na szybkich i wolnych alertach.

W tym punkcie, wszystkie punkty końcowe z polityką szybkiego alertu są aktualizowane w wersji opublikowanej.

4. Monitoruj zachowanie punktów końcowych szybkiego alertu.
5. Jeśli aktualizacja została zainstalowana pomyślnie i punkty końcowe zachowują się normalnie, możesz opublikować aktualizację na wolnym alercie:
   a. Przejdź do strony **Konfiguracja** > **Aktualizacja** i wybierz zakładkę **Komponenty**.
   b. Wybierz aktualizację w tabeli Aktualizacje kliknij przycisk **Akcje** w górnej części tabeli i wybierz **Publikuj**.
   c. Zaznacz opcję wolnego alertu.

      Każdy punkt końcowy z produkcji jest teraz aktualizowany do nowej wersji, którą opublikujesz.
6. Jeśli spotkałeś problem z paczką, możesz napisać zgłoszenie do wsparcia. Aby uzyskać więcej informacji, odwołaj się do „Otrzymywanie pomocy” (p. 158).

4.5. Aktualizacje Produktu Offline

GravityZone wykorzystuje domyślnie system aktualizacji podłączony do Internetu. Dla izolowanych sieci, Bitdefender oferuje alternatywę, dzięki czemu składniki i sygnatury aktualizacji dostępne są także w trybie offline.

4.5.1. Warunki wstępne

Aby użyć aktualizacji offline, potrzebujesz:

- Jedno lub więcej urządzeń GravityZone wdrożono w sieci bez dostępu do Internetu, znane także jako "instancje offline".
- Dodatkowa instancja GravityZone jest wdrażana normalnej sieci, znana tez jako "instancja online", z następującymi wymaganiami:
  – Tylko role Serwera Bazodanowego i Aktualizacji muszą być zainstalowane.
  – Dostęp do Internetu, jako, że instancja będzie źródłem archiwów z aktualizacjami dla wdrożenia GravityZone offline.

– Port komunikacji 80/443 musi być otwarty.

4.5.2. Ustawianie Instancji Online GravityZone

1. Połącz się z urządzeniem za pośrednictwem SSH, używając **PuTTY**, na przykład.
2. Uruchom komendę `sudo su` aby uzyskać uprawnienia **roota**
3. Zainstaluj paczkę która przekonwertuje Serwer aktualizacji aby generował archiwa do aktualizacji offline.

```
# ap-get update # ap-get install gzou-mirror
```

Po instalacji `obrazu gzou` ustawi serwis webowy, przez który możesz konfigurować generowanie archiwów aktualizacji offline.

Możesz uzyskać dostęp do serwisu webowego przez dany URL: `https://Update-Server-IP-or-Hostname`, z nazwą użytkownika `bdadmin` oraz hasłem które ustawiłeś.

Masz kilka opcji, aby pobrać zaktualizowane archiwa:

- Poprzez zasób Samby - tylko do odczytu zasób Samba będzie skonfigurowany i wykorzystany do otrzymania archiwum z aktualizacją offline. Możesz uzyskać dostęp do udziału jako:

  `\\updateServerIPorHostname\gzou-snapshots`

- Poprzez SCP/SCTP- wygenerowane archiwa z aktualizacjami offline będą składowane w miejscu, z którego mogą być odbierane poprzez wybrany klient SCP/SFTP. Ścieżka jest:

  `/opt/bitdefender/share/gzou/snapshots`

- Poprzez usługę webową - adres URL to:

  `https://updateServerIPorHostname/snapshots`

Zadanie CRON jest zainstalowane i sprawdzi, co minutę, jeśli musi zostać utworzone nowe archiwum (w zależności od przedziału (w godzinach) **utworzenia archiwum** ustawienie z poziomu konsoli webowej). Domyśle ustawienie to 2 godziny.

4.5.3. Ustawianie Instancji Offline GravityZone

Chyba, że jest ustalone inaczej, wszystkie komendy muszą być uruchamiane jako **root**

1. Zainstaluj role Bazy Danych oraz Serwera Aktualizacji. Jeśli w trakcie instalacji, konsola jest podłączona do Internetu, zainstaluj również pozostałe role(konsole webową oraz serwer komunikacji) W przeciwnym razie, połącz się przez SSH i skopiuj do `/home/bdadmin` archiwum aktualizacji `gzou-bootstrap.sh` z instancji offline, korzystając z **WinSCP**
2. SSH w konsoli. Musisz:
   a. Przekształcenie `gzou- bootstrap` do pliku wykonywalnego:

```
#
chmod +x gzou-bootstrap.sh
```

   b. Uruchom: `./gzou-bootstrap.sh`
3. Jeśli korzystasz z SAMBA, wprowadź ścieżkę współdzielonego folderu zawierającego archiwa aktualizacji wzięte z `\\HostnameorIP\ShareName`, nazwa użytkownika i hasło.
4. Zainstaluj role Konsola Webowa i Serwer Komunikacji (dostarczone ci jeśli nie masz połączenia z internetem aby je zainstalować)
5. Wejdź do konsoli offline przez twoją przeglądarkę i wprowadź klucz licencyjny(w trybie offline).

4.5.4. Korzystając z Aktualizacji Offline

Kiedy instalacja jest zainicjowana na środowiskach online i offline, możesz użyć tych procedur do aktualizacji instalacji offline:

1. Odbierz najnowsze archiwum aktualizacji offline z serwera komunikacji pochodzące ze środowiska online. Aby uzyskać więcej informacji, odwołaj się do „Używając Konsoli Webowej” (p. 146).

2. Przenieś archiwum do środowiska offline(poprzez np.: USB, przenośny dysk) i skopiuj do lokacji gdzie skonfigurował role Serwera Aktualizacji aby odebrać archiwum do aktualizacji offline z danej lokacji:

   `/opt/bitdefender/share/gzou/snapshots/`

3. W tym momencie, jeśli korzystasz z SAMBA (konsole się komunikują) archiwa powinny zostać automatycznie pobrane i zainstalowane offline. W innym przypadku, od czasu do czasu musisz manualnie przenieść archiwa(lekkie) sygnatur offline lub archiwa aktualizacji offline(pełne), generowane w konsoli online przeznaczone do lokalizacji w konsoli offline:

   `/opt/bitdefender/share/gzou/snapshots/`

4.5.5. Używając Konsoli Webowej

Wejdź do konsoli webowej przez wpisanie IP/Nazwy hosta urządzenia wirtualnego w przeglądarce webowej. Możesz edytować dostępne opcje:

- Panel sterowania
- Ustawienia ogólne

Panel sterowania

Status urządzenia wyświetla szczegóły ostatniej wykonanej pracy(typ archiwum, data i czas) i następna zaplanowana praca.

Masz opcję aby:

- **Utwórz Archiwum Sygnatury**
- **Utwórz Pełne Archiwum**

W sekcji **Utworzone Archiwa**, możesz pobrać sygnaturę i pełne archiwa.

Zaznacz archiwa z dostępnej listy i kliknij przycisk **Pobierz**.

Możesz także zobaczyć dostępne miejsce na dysku appliance.

Ustawienia ogólne

Możesz zdefiniować harmonogram pobierania dla zestawów GravityZone.

1. Kliknij przycisk **Edytuj Ustawienia**.
2. Wybierz jeden lub więcej zestawów z listy **Dostępne Zestawy**.

3. W sekcji **Harmonogram** możesz zdefiniować przedział dla tworzenia archiwów, jak również liczbę sygnatur i pełnych archiwów, które zachowasz na dysku.
4. Kliknij przycisk **Zastosuj**, aby zapisać zmiany.

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 HVI
- Odinstalowywanie Ochrony Exchange
- Odinstalowywanie Ochrony Urządzeń Mobilnych
- Odinstalowanie Kreatora Raportów
- Odinstalowywanie Ról GravityZone Virtual Appliance

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

   Dla środowisk zintegrowanych VMware vShield, musisz wybrać wymagane poświadczenia dla każdej maszyny, w innym wypadku odinstalowanie nie powiedzie się. Wybierz **Użyj poświadczeń dla integracji vShield**, po czym sprawdź wszystkie wymagane dane w tabeli Menadżera Poświadczeń wyświetlonej poniżej.
7. 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. 85).

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. 85).

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**.
6. Wprowadź poświadczenia vShield (jeśli dotyczy) i kliknij **Tak**, aby utworzyć zadanie.

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 HVI

Aby usunąć HVI z hosta, wystarczy odinstalować Pakiet Uzupełniający HVI. Możesz dalej używać Security Server jako serwera skanowania, pod warunkiem posiadania ważnego klucza licencyjnego dla Security for Virtualized Environments.

Jeśli chcesz całkowicie usunąć Bitdefender, musisz odinstalować zarówno Pakiet Uzupełniający HVI jak i Security Server.

Odinstalowywanie Pakietu Uzupełniającego HVI.

Masz dwie opcje, aby usunąć Pakiet Uzupełniający:

- Zdalnie z Control Center przez uruchomienie zadanie deinstalacji.
- Zdalnie z XenCenter, przez uruchomienia kilku komend na docelowym hoście.

Aby usunąć pakiet HVI użyj Control Center:

1. Zaloguj do Control Center.
2. Przejdź do strony **Sieć** i wybierz **Maszyny Wirtualne** z selektora widoków.
3. Wybierz **Serwer** z menu **Widoki** w lewym panelu.
4. Wybierz jeden lub więcej hostów Xen z inwentaryzacji sieci. Możesz łatwo zobaczyć dostępne hosty zaznaczając opcję **Wpisz > Hosty** z menu **Filtry**.
5. Kliknij przycisk **Zadania** po prawej stronie panelu i wybierz **Zainstaluj Pakiet Uzupełniający HVI**. Otwiera się okno konfiguracji.
6. Zaplanuj czas usunięcia pakietu. Możesz wybrać czy uruchomić zadanie natychmiast po zapisaniu zadania, czy w określonym czasie. W przypadku, gdy deinstalacja nie może zostać wykonana w określonym czasie, zadanie automatycznie powtarza się zgodnie z ustawieniami powtarzania. Na przykład, jeśli zaznaczyłeś więcej hostów i jeden host nie jest dostępny, gdy pakiet jest zaplanowany do deinstalacji, zadanie zostanie uruchomione ponownie w określonym czasie.
7. Host musi się zresetować aby ukończyć usuwanie. Jeśli chcesz restartować hosta bez nadzoru, zaznacz **Automatyczny restart(jeśli potrzebny)**.
8. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

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

Aby usunąć pakiet HVI użyj XenCenter:

1. Zaloguj się do XenCenter.
2. Otwórz konsolę hosta Xen.
3. Wprowadź hasło hosta XenServer.
4. Uruchom następujące komendy:

```
# rpm -ebitdefender-xen-dom0 # rm -rf /etc//xensource/installed-r
  /bitdefender\:bitdefender-hvi/ # rm -rf/opt/bitdef* # usługaxap
```

Odinstalowywanie Security Server

Aby odinstalować Security Server z jednego lub kilku hostów:

1. Zaloguj do Control Center.

2. Przejdź do strony **Sieć**.
3. Wybierz **Maszynę Wirtualną** z selektora widoku.
4. Przejrzyj inwentaryzację Citrix i zaznacz pola wyboru odpowiadające żądanym hostom. Dla szybkiego wyboru, możesz filtrować inwentaryzację sieci, aby wyświetlić tylko Security Server.
5. Kliknij przycisk **Zadania** w górnej części tabeli i wybierz **Odinstaluj Security Server** z menu. Pojawi się nowa wiadomość potwierdzająca. Kliknij **Tak**, aby kontynuować.

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

5.3. 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 **Komputery i Wirtualne Maszyny** z selektora widoku.
3. Wybierz pożądany kontener z lewego panelu bocznego. Wpisy będą wyświetlane po prawej stronie panelu tabeli.
4. Wybierz punkt końcowy, z którego chcesz odinstalować Ochronę Exchange.
5. Kliknij **Rekonfiguruj Klienta** w menu **Zadania**, w górnym panelu tabeli. Wyświetlono okno konfiguracji.
6. 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.

7. Naciśnij **Zapisz** aby utworzyć zadanie.

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

Jeśli chcesz przeinstalować Ochronę Exchange, przejdź do „Instalowanie Ochrony Exchange” (p. 114).

5.4. Odinstalowywanie Ochrony Urządzeń Mobilnych

Gdy usuwasz ochronę Bitdefender z urządzenia mobilnego, musisz to zrobić zarówno z Control Center jak i urządzenia.

Kiedy usuwasz urządzenie z Control Center:

- GravityZone Mobile Client jest odłączony, ale nie usunięty z urządzenia.
- Wszystkie logi połączone z usuniętym urządzeniem pozostaną nadal dostępne.
- Nie wpłynie to na twoje osobiste informacje i zainstalowane aplikacje.
- Dla urządzeń iOS, Profil MDM jest usunięty. Jeśli urządzenie nie jest podłączone do Internetu, Profil MDM pozostaje zainstalowany do czasu dostępności nowego połączenia.

Ostrzeżenie

- Nie można przywrócić usuniętych urządzeń przenośnych.
- Upewnij się, że urządzenie docelowe nie jest zablokowane przed usunięciem. Jeśli jest to potrzebne, wykonaj **Odblokuj** w menu **Zadania**. Jeżeli przypadkowo usunąłeś zablokowane urządzenie, musisz zrestartować urządzenie do ustawień fabrycznych, to je odblokuje.

1. Przejdź do strony **Sieć**.
2. Zaznacz **Urządzenia Mobilne** w selektorze wyświetleń.
3. Kliknij **Filtry** w górnej części panelu sieciowego i zaznacz **Urządzenia** w kategorii **Widok**. Kliknij **Zapisz**.
4. Wybierz pożądany kontener z lewego panelu bocznego. Wszystkie urządzenia są wyświetlane po prawej stronie panelu tabeli.
5. Zaznacz pole wyboru urządzenia, z którego chcesz usunąć ochronę.
6. Kliknij ⊖ **Usuń** w górnej części tabeli.

Następnie, musisz odinstalować oprogramowanie z urządzenia.

Aby odinstalować ochronę Bitdefender z urządzenia Android:

1. Idź do **Bezpieczeństwo > Administratorzy Urządzenia**.
2. Odznacz pole wyboru GravityZone. Pojawia się okno potwierdzające.

3. Dotknij **Deaktywuj**. Wyświetlany jest komunikat ostrzegawczy, informujący, że funkcje anti-theft nie będą już działać i stracisz dostęp do sieci korporacyjnych i danych.
4. Odinstaluj GravityZone Mobile Client jak każdą inną aplikację.

Aby odinstalować ochronę Bitdefender z urządzenia iOS:

1. Przejdź do ikony Bitdefender GravityZone Mobile Client i przytrzymaj ją przez kilka sekund.
2. Dotknij dołączony ⊗ krąg, kiedy się pojawi. Aplikacja została usunięta.

Jeśli chcesz przeinstalować ochronę mobile, przejdź do„Instalowanie Ochrony Urządzeń Mobilnych" (p. 119)

5.5. Odinstalowanie Kreatora Raportów

Aby prawidłowo usunąć Kreatora Raportów z twojego rozwiązania GravityZone, musisz odinstalować dwie role: Bazę Danych i Processors

Aby odinstalować Bazę Danych Kreatora Raportu:

1. Zaloguj się do Kreatora Raportów z Baz Danych przez interfejs konsoli Twojego narzędzia do zarządzania wirtualizacją(np. vSphere Client) Użyj klawiszy strzałek i przycisku `Tab` do nawigacji w menu i opcjach. Naciśnij `Enter`, aby wybrać konkretną opcję.
2. Z głównego menu, wybierz **Zaawansowane Ustawienia**.
3. Idź do **Zainstaluj/Osinstaluj Role**, potem **Dodaj lub Usuń role**
4. Używając `Spacji` odznacz rolę **Bazę Danych RB** i naciśnij `Enter` Pojawi się nowe okno potwierdzające.
5. Wybierz **Tak** i naciśnij `Enter` aby kontynuować i czekać na koniec deinstalacji.

Aby odinstalować Procesory Kreatora Raportu:

1. Zaloguj się do Kreatora Raportów z Procesorów przez interfejs konsoli Twojego narzędzia do zarządzania wirtualizacją(np. vSphere Client) Użyj klawiszy strzałek i przycisku `Tab` do nawigacji w menu i opcjach. **Naciśnij Enter**, aby wybrać konkretną opcję.
2. Z głównego menu, wybierz **Zaawansowane Ustawienia**.
3. Idź do **Zainstaluj/Osinstaluj Role**, potem **Dodaj lub Usuń role**

4. Używając `Spacji` odznacz rolę **Procesory RB** i naciśnij `Enter` Pojawi się nowe okno potwierdzające.
5. Wybierz **Tak** i naciśnij `Enter` aby kontynuować i czekać na koniec deinstalacji.

Ostrzeżenie
JEśli wyłączysz urządzenia Konstruktora Raportów w środowisku zwirtualizowanym bez odinstalowywania ról Bazodanowych i Procesorów, nie będziesz z stanie połączyć się do GravityZone Control Center.

5.6. Odinstalowywanie Ról GravityZone Virtual Appliance

Możesz odinstalować role urządzenia wirtualnego GravityZone poprzez interfejs wiersza poleceń (CLI). Nawet jeśli je usuniesz, Twoja sieć jest dalej chroniona. Niemniej jednak, potrzebujesz co najmniej jednej instancji dla każdej roli w GravityZone, aby działało prawidłowo.

W scenariuszu z pojedynczym urządzeniem GravityZone z wszystkimi rolami zainstalowanymi, kiedy usuniesz jedną z nich, końcówki dalej będą chronione, lecz niektóre z opcji urządzenia nie będą dostępne, zależnie od roli.

W scenariusz w wieloma urządzeniami GravityZone możesz bezpiecznie odinstalować rolę, tak długo jak inna instancja tej samej roli jest dostępna. Według projektu, wiele instancji z rolami Serwera Komunikacyjnego i Konsoli Webowej może być zainstalowane na różnych urządzeniach i połączonych do innych ról poprzez stabilizator ról. Stąd, jeśli odinstalujesz jedną instancję określonej roli, jej funkcję przejmuje inna.

Jeśli potrzeba, możesz odinstalować Serwer Komunikacji z jednego urządzenia w międzyczasie przypisując jego funkcje to innej instancji z tą rolą. Dla sprawnej migracji, wykonaj następujące kroki:

1. W Control Center, przejdź do strony **Polityki**.
2. Zaznacz istniejącą lub kliknij ⊕**Dodaj**, aby utworzyć nową.
3. W sekcji **Ogólne**, przejdź do **Komunikacja**.
4. W tabeli **Przypisanie Komunikacji Punktu końcowego** naciśnij pole **Nazwa**. Wyświetlono listę wykrytych serwerów komunikacji.
5. Wybierz serwer komunikacji, do którego chcesz, aby powiązane były punkty końcowe.

6. Kliknij przycisk ⊕**Dodaj** po prawej stronie tabeli. Jeśli masz na liście więcej niż jeden serwer komunikacyjny, możesz skonfigurować ich priorytet za pomocą strzałek w górę i w dół po prawej stronie każdego wpisu.
7. Kliknij **Zapisz**, aby utworzyć politykę. Punkty końcowe będą się komunikować z Control Center poprzez określony serwer komunikacji.
8. W interfejsie wiersza poleceń GravityZone, odinstaluj starą rolę Serwera Komunikacji.

Ostrzeżenie
Jeśli odinstalujesz stary Serwer Komunikacji bez ustawiania pierwszej polityki, komunikacja będzie całkowicie stracona i będziesz musiał reinstalować agenty ochrony.

Aby zainstalować role wirtualnego urządzenia GravityZone:

1. Zaloguj się do interfejsu konsoli ze swojego narzędzia do zarządzania wirtualizacją (np. vSphere Client). Użyj klawiszy strzałek i przycisku `Tab` do nawigacji w menu i opcjach. Naciśnij `Enter`, aby wybrać konkretną opcję.
2. Wybierz **Zaawansowane Ustawienia**.
3. Wybierz **Zainstaluj/Odinstaluj Role**.
4. Przejdź do **Dodaj lub usuń role**.
5. Korzystając ze `Spacji`, odznacz każdą rolę, którą chcesz odinstalować, następnie naciśnij `Enter`. Pojawia się okno potwierdzające, informujące Ciebie, że rola zostanie usunięta.
6. Naciśnij `Enter`, aby kontynuować i poczekaj na zakończenie deinstalacji.

Jeśli chcesz przeinstalować rolę, przejdź do „Role Instalowania/Odinstalowywania” (p. 74).

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