Bitdefender

GravityZone

INSTRUKCJA INSTALACJI

Bitdefender GravityZone
Instrukcja Instalacji

Data publikacji 2021.04.20

Notka prawna

Notka prawna

Wszelkie prawa zastrzeżone. Żadna część tej publikacji nie może być kopiowana w żadnej formie lub postaci elektronicznej, mechanicznej, w formie fotokopii lub w postaci nagrań głosowych, ani przechowywana w jakimkolwiek systemie udostępniania i wyszukiwania informacji, bez pisemnej zgody upoważnionego przedstawiciela firmy

Spis treści

Wstęp

Przewodnik jest skierowany do administratorów IT odpowiedzialnych za wdrożenie ochrony GravityZone wewnątrz organizacji. Menedżerowie IT szukający informacji o GravityZone mogą je uzyskać w przewodniku GravityZone wymagania i dostępne moduły ochrony.

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. Dowiedz się o ich aspektach i znaczeniu z poniższej tabeli.

Wygląd	Opis
`wzorzec`	Nazwy i składnie poleceń liniowych, ścieżki i nazwy plików, dane wyjściowe plików konfiguracyjnych, tekst wejściowy są zapisane z użyciem czcionki `o stałej szerokości znaków`.
http://www.bitdefender.com	Link URL wskazuje na zewnętrzną lokalizację, na serwerach http lub ftp.
gravityzone-docs@bitdefender.com	W tekście umieszczono adresy e-mail w celu podania informacji kontaktowych.
„Wstęp” (p. vii)	To link wewnętrzny, do miejsca wewnątrz dokumentu.
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 to notatki tekstowe oznaczone graficznie wskazujące na dodatkowe informacje związane z bieżącym akapitem.

Notatka

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

WAŻNE

Wymaga to Państwa uwagi i nie jest wskazane pomijanie tego. Zazwyczaj nie są to wiadomości krytyczne, ale znaczące.

Ostrzeżenie

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

1. O GRAVITYZONE

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

GravityZone jest jednym produktem z ujednoliconą konsolą zarządzania dostępną w chmurze, której gospodarzem jest Bitdefender lub jednym wirtualnym urządzeniem instalowanym w siedzibie firmy i stanowi jeden punkt wdrażania, egzekwowania i zarządzania zasadami zabezpieczeń dla dowolnej liczby urządzeń końcowych i dowolnego typu w dowolnym miejscu.

GravityZone zapewnia wielowarstwową ochronę dla punktów końcowych: antymalware wraz z monitorowaniem behawioralnym, ochronę przed zagrożeniami typu zero-day, czarną listę aplikacji i sandboxa, firewall'a, kontrolę urządzeń i zawartości.

2. GRAVITYZONE WARSTWY OCHRONNE

GravityZone udostępnia następujące warstwy ochrony:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- Zaawansowany Anty-Exploit
- Zapora Sieciowa
- Kontrola Zawartości
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne szyfrowanie dysku
- Network Traffic Security Analytics (NTSA)

2.1. Antymalware

Warstwa ochrony antymalware bazuje na skanowaniu sygnatur i analizie heurystycznej (B-HAVE, ATC) przeciwko: wirusom, robakom, Trojanom, spyware, adware, keyloggerom, rootkitom i innym rodzajom 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.

Silniki Skanowania

Bitdefender GravityZone jest w stanie automatycznie ustawić silniki skanowania podczas tworzenia pakietów agentów bezpieczeństwa, zgodnie z konfiguracją punktu końcowego.

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 jest odpowiedni dla potężnych maszyn, posiadających zawartość bezpieczeństwa przechowywaną lokalnie.
2. **Skanowanie hybrydowe za pomocą lekkich silników (chmura publiczna)** , o średnim zasięgu, z wykorzystaniem skanowania w chmurze i częściowo lokalnej zawartości zabezpieczeń. Ten tryb skanowania przynosi korzyści z lepszego wykorzystania zasobów oraz angażuje poza przesłankowe skanowanie.
3. **Centralne skanowanie w chmurze publicznej lub prywatnej** , z niewielkim rozmiarem wymagającym Security Server do skanowania. W takim przypadku żaden zestaw zawartości zabezpieczeń nie jest przechowywany lokalnie, a skanowanie jest odciążane na Security Server.

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

4. **Centralne skanowanie (skanowanie w chmurze publicznej lub prywatnej za pomocą Security Server) z powrotem * na skanowanie lokalne (pełne silniki)**
5. **Centralne skanowanie (skanowanie w chmurze publicznej lub prywatnej za pomocą Security Server) z powrotem * na Hybrid Scan (Publiczna Chmura z Lekkimi Silnikami**

2.2. 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.

2.3. Zaawansowany Anty-Exploit

Zaawansowana technologia Anty-Exploit, oparta na uczeniu maszynowym, jest proaktywną technologią, która powstrzymuje ataki zerowe przeprowadzane przez nieuchwytne exploity. Zaawansowany Anti-Exploit przechwytuje najnowsze exploity w czasie rzeczywistym i łagodzi luki w zabezpieczeniach pamięci, które mogą ominąć inne rozwiązania bezpieczeństwa. Chroni najczęściej używane aplikacje, takie jak przeglądarki, Microsoft Office lub Adobe Reader, a także inne. Nadzoruje procesy systemowe i chroni przed naruszeniami bezpieczeństwa i przejmowaniem istniejących procesów.

2.4. 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.

2.5. Kontrola Zawartości

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.

2.6. Network Attack Defense

Moduł Network Attack Defense polega na Bitdefender technologii skoncentrowanej na wykrywaniu ataków sieciowych zaprojektowanych w celu uzyskania dostępu do punktów końcowych za pomocą określonych technik, takich jak: ataki brute-force, sieciowe exploity, złodzieje haseł, wektory infekcji drive-by-download, boty i Trojany.

2.7. Zarządzanie Aktualizacjami

W pełni zintegrowany z GravityZone, moduł Zarządzania Aktualizacjami aktualizuje systemy operacyjne i oprogramowanie i zapewnia kompleksowy widok statusu aktualizacji zarządzanych punktów końcowych Windows.

Moduł Zarządzania Aktualizacjami GravityZone zawiera kilka funkcji, takich jak skanowanie na żądanie / zaplanowane skanowanie aktualizacji, automatyczne / ręczne aktualizowanie lub raportowanie brakujących aktualizacji .

Możesz dowiedzieć się więcej na temat dostawców i produktów Zarządzania Aktualizacjami GravityZone w tym artykule KB.

Notatka
Moduł Zarządzania Aktualnościami jest dodatkiem dostępnym z oddzielnym kluczem licencyjnym dla wszystkich dostępnych pakietów GravityZone.

2.8. Kontrola Urządzenia

Moduł Kontroli Urządzenia pozwala na zapobieganie wyciekaniu danych wrażliwych i infekcji malware przez urządzenia zewnętrzne podłączone do punktów końcowych przez zastosowanie zasad blokowania i wykluczeń przez politykę w szerokim zasięgu rodzajów urządzeń (tj. Pamięci flash USB, urządzenia Bluetooth, odtwarzacze CD/DVD, urządzenia pamięci masowej itp.).

2.9. Pełne szyfrowanie dysku

Ta warstwa ochrony umożliwia zapewnienie pełnego szyfrowania dysku na punktach końcowych, zarządzając funkcją BitLocker w systemie Windows oraz FileVault i diskutil w systemie MacOS. Możesz zaszyfrować i odszyfrować woluminy rozruchowe i nierozruchowe za pomocą kilku kliknięć, podczas gdy GravityZone obsługuje cały proces, przy minimalnej interwencji użytkowników. Dodatkowo GravityZone przechowuje klucze odzyskiwania wymagane do odblokowania woluminów w przypadku, gdy użytkownicy zapomną hasła.

Notatka
Pełne Szyfrowanie Dysku jest dodatkiem dostępnym z oddzielnym kluczem licencyjnym dla wszystkich dostępnych pakietów GravityZone.

2.10. Sandbox Analyzer

Bitdefender Sandbox Analyzer zapewnia potężną warstwę ochrony przeciwko zaawansowanym zagrożeniom działającą automatycznie, dzięki dogłębnej analizie podejrzanych plików, które nie są jeszcze podpisane przez silniki skanowania Bitdefender. W sandboxie zastosowano obszerny zestaw technologii Bitdefender, aby wykonywać ładunki w zamkniętym środowisku wirtualnym wdrożonym lokalnie, analizować ich zachowanie i zgłaszać wszelkie subtelne zmiany systemowe, które wskazują na złośliwe zamiary.

Sandbox Analyzer wykorzystuje serię czujników do detonacji zawartości ze strumieni ruchu sieciowego, scentralizowanej kwarantanny i serwerów ICAP.

Dodatkowo, Sandbox Analyzer umożliwia ręczne przesłanie próbki i poprzez API.

Notatka
Funkcjonalność tego modułu zapewnia Sandbox Analyzer On-Premises, który jest dostępny z oddzielnym kluczem licencyjnym.

2.11. Network Traffic Security Analytics (NTSA)

Bitdefender [NTSA_ LONG] ([NTSA_ SHORT]) to rozwiązanie bezpieczeństwa sieciowego, które analizuje strumienie ruchu IPFIX pod kątem obecności złośliwego zachowania i złośliwego oprogramowania.

Bitdefender [NTSA_ SHORT] ma działać równolegle z istniejącymi środkami bezpieczeństwa jako zabezpieczenie uzupełniające, które jest w stanie pokryć martwe pola, których tradycyjne narzędzia nie monitorują.

Tradycyjne narzędzia bezpieczeństwa sieci zazwyczaj próbują zapobiegać infekcjom złośliwego oprogramowania, sprawdzając ruch przychodzący (za pośrednictwem sandbox, zapór sieciowych, antywirusa itp.). Bitdefender [NTSA_ SHORT] koncentruje się wyłącznie na monitorowaniu wychodzącego ruchu sieciowego pod kątem złośliwego zachowania.

2.12. GravityZone Dostępność Warstw Ochrony

Dostępność warstw ochrony GravityZone różni się w zależności od systemu operacyjnego punktu końcowego. Aby dowiedzieć się więcej, zapoznaj się z artykułem Dostępność warstw ochrony w GravityZone.

3. 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, Nutanix Prism, Microsoft Azure.

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

Rozwiązanie GravityZone zawiera następujące składniki:

- Urządzenie Wirtualne GravityZone
- Agenci Bezpieczeństwa

3.1. GravityZone VA

Rozwiązanie lokalne GravityZone dostarczane jest jako samoczynnie konfigurowane, hartowane urządzenie wirtualne (VA) Linux, osadzone w obrazie maszyny wirtualnej, łatwe do zainstalowania i skonfigurowania za pomocą interfejsu CLI (Wiersz Poleceń Interfejs). Wirtualne urządzenia są dostępne w kilku formatach kompatybilnych z platformami wirtualizacji (OVA, XVA, VHD, OVF, RAW).

3.1.1. Baza danych GravityZone

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

3.1.2. 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.

3.1.3. 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.

3.1.4. Konsola Web (GravityZone 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 oraz serwery. Zasilana przez Architekturę Gravity, Control Center jest w stanie odpowiedź na potrzeby nawet największych organizacji.

Control Center integruje się z zarządzaniem istniejącym systemem i systemem monitorowania, aby uczynić łatwym automatyczne zastosowanie ochrony niezarządzanym stacjom roboczym lub serwerom które pojawiły się w Microsoft Active Directory lub są po prostu wykryte w sieci.

3.2. 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

3.2.1. Bitdefender Endpoint Security Tools

GravityZone zapewnia ochronę maszynom fizycznym i wirtualnym systemów Windows i Linux za pomocą Bitdefender Endpoint Security Tools, inteligentnego agenta ochrony środowiska, który dostosowuje się do typu punktu końcowego. Bitdefender Endpoint Security Tools może być wdrożony na dowolnym komputerze, albo wirtualnym lub fizycznym, zapewniając elastyczny system skanowania, będący

idealnym wyborem dla środowisk mieszanych (fizycznych, wirtualnych i cloudowych).

Bitdefender Endpoint Security Tools wykorzystuje pojedynczy szablon zasad dla maszyn fizycznych i wirtualnych i jedno źródło zestawu instalacyjnego dla wszelkich środowisk (fizycznych czy wirtualnych) uruchomionych na bieżących edycjach Windows.

Warstwy bezpieczeństwa

Następujące moduły powłok zabezpieczających dostępne są z Bitdefender Endpoint Security Tools:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- Zapora Sieciowa
- Kontrola Zawartości
- Network Attack Defense
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne szyfrowanie dysku

Role Punktów Końcowych

- Power User
- Relay
- Serwerów Buforowania Łatek

Power User

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
Moduł ten jest dostępny wyłącznie dla komputerów stacjonarnych i serwerów obsługiwanych systemów operacyjnych Windows. Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne” (p. 21).

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 rozproszonymi sieciami, agenci relay pomagają obniżyć wykorzystanie pasma, zapobiegając bezpośredniemu połączeniu chronionych punktów końcowych z urządzeniem 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.

Serwerów Buforowania Łatek

Punkty końcowe z rolą Relay mogą również działać jako Serwer Buforowania Aktualizacji. Po włączeniu tej roli, Relay służą do przechowywania aktualizacji oprogramowania pobranych ze stron internetowych dostawców i dystrybuowania ich do docelowych punktów końcowych w sieci. Kiedy podłączony punkt końcowy ma oprogramowanie z brakującymi aktualizacjami, pobiera je z serwera, a nie ze strony internetowej producenta, optymalizując w ten sposób generowany ruch i obciążenie sieci.

WAŻNE
Ta dodatkowa rola jest dostępna z zarejestrowanym dodatkiem Patch Management.

3.2.2. Endpoint Security for Mac

Endpoint Security for Mac to agent bezpieczeństwa zaprojektowany w celu ochrony stacji roboczych i laptopów opartych na procesorze Intel. Dostępna technologia skanowania to **Skanowanie lokalne** , z zawartością zabezpieczeń przechowywaną lokalnie.

Warstwy bezpieczeństwa

Następujące moduły powłok zabezpieczających dostępne są z Endpoint Security for Mac:

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- Kontrola Zawartości
- Kontrola Urządzenia
- Pełne szyfrowanie dysku

3.3. Architektura Sandbox Analyzer

Bitdefender Sandbox Analyzer zapewnia potężną warstwę ochrony przed zaawansowanymi zagrożeniami, wykonując automatyczną, szczegółową analizę podejrzanych plików, które jeszcze nie zostały podpisane przez silniki antimalware Bitdefender.

Aby używać ten moduł z GravityZone, potrzebujesz zainstalować Sandbox Analyzer On-Premises.

Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises jest dostarczany jako urządzenie wirtualne z Linux Ubuntu, osadzony w obrazie maszyny wirtualnej, łatwy do instalacji i konfiguracji poprzez interfejs linii komend (CLI). Sandbox Analyzer On-Premises jest dostępny w formacie OVA, możliwy do wrdożenia w VMWare ESXi.

Instancja Sandbox Analyzer On-Premises zawiera następujące komponenty:

- **Menedżer Sandboxa**. Ten komponent jest orkiestratorem sandboxa. Menedżer Sandbox łączy się z hiperwisorem ESXi poprzez API i wykorzystuje swoje zasoby sprzętowe do budowy i obsługi środowiska analizy złośliwego oprogramowania.
- **Detonacja maszyn wirtualnych**. Ten komponent składa się z maszyn wirtualnych wykorzystywanych przez Sandbox Analyzer do wykonywania plików i analizy

ich zachowania. Maszyny wirtualne do detonacji mogą działać w 64-bitowych systemach operacyjnych Windows 7 i Windows 10.

GravityZone Control Center działa jako konsola zarządzania i raportowania, w której konfigurujesz polityki bezpieczeństwa, oraz przeglądasz raporty i powiadomienia z analizy.

Sandbox Analyzer On-Premises obsługuje następujące czujniki zasilające:

- **Czujnik sieci**. Wirtualne Urządzenie Zabezpieczeń Sieciowych (NSVA) jest urządzeniem wirtualnym, które jest możliwe do wdrożenia w tym samym środowisku zwirtualizowanym ESXi jako instancja Sandbox Analyzer. Czujnik sieciowy pobiera zawartość ze strumieni sieciowych i przesyła ją do Sandbox Analyzer.
- **Czujnik ICAP**. Wdrożony na urządzeniach sieciowej pamięci masowej (NAS), za pomocą protokołu ICAP, Bitdefender Security Server wspiera obsługę przesyłania treści do Sandbox Analyzer.

Oprócz tych czujników, Sandbox Analyzer On-Premises obsługuje ręczne przesyłanie i przez API. Szczegółowe informacje znajdują się w rozdziale **Korzystanie z Sandbox Analyzer** w Przewodniku Administratora GravityZone.

4. WYMAGANIA

Wszystkie rozwiązania GravityZone są instalowane i zarządzane przez Control Center.

4.1. Urządzenie Wirtualne GravityZone

4.1.1. Wspierane formaty i platformy wirtualizacji.

GravityZone jest dostarczane jako maszyna wirtualna (VA). Jest ono dostępne w następujących formatach, które obsługują najbardziej popularne platformy wirtualizacji:

- OVA (kompatybilny z VMware vSphere, View, VMware Player)
- XVA (kompatybilny z Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (kompatybilny z Microsoft Hyper-V)
- VMDK (kompatybilny z Nutanix Prism)
- 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.

4.1.2. Sprzęt komputerowy

Wymagania sprzętowe wirtualnego urządzenia GravityZone różnią się w zależności od rozmiaru sieci i wybranej architektury wdrażania. W przypadku sieci do 3000 punktów końcowych można zainstalować wszystkie role GravityZone w jednym urządzeniu, natomiast w przypadku większych sieci należy rozważyć podział ról między kilka urządzeń. Zasoby wymagane przez urządzenie zależą od ról, które zainstalujesz na nim i od tego, czy używasz zestawu replik.

Notatka
Zestaw replik jest cechą MongoDB, która zapewnia replikację bazy danych i zapewnia nadmiarowość oraz wysoką dostępność składowanych danych. Aby uzyskać więcej informacji, zapoznaj się z dokumentacją MongoDB i „Zarządzanie Urządzeniem GravityZone" (p. 77).

WAŻNE
Pomiary są wynikiem wewnętrznych testów Bitdefender na podstawowej konfiguracji GravityZone i regularnego użytkowania. Wyniki mogą się różnić w zależności od konfiguracji sieci, zainstalowanego oprogramowania, liczby wygenerowanych zdarzeń itp. Aby uzyskać niestandardowe dane dotyczące skalowalności, skontaktuj się z Bitdefender.

vCPU

Poniższa tabela informuje o liczbie vCPU wymaganej dla każdej roli, jaką przyjąć może urządzenie wirtualne.

Każdy vCPU musi mieć co najmniej 2GHz.

Składnik	Ilość punktów końcowych (maksymalna)							
	250	500	1000	3000	5000	10000	25000	50000
Podstawowe cechy GravityZone								
Serwer aktualizacji*	8	12	14	16	4	4	6	8
Konsola sieciowa**					6	10	12	12
Serwer komunikacji					6	10	12	18
Baza danych***					6	6	9	12
Łącznie	**8**	**12**	**14**	**16**	**22**	**30**	**39**	**50**
GravityZone z Bitdefender HVI								
Serwer aktualizacji*	8	4	4	4	4	4	6	8
Konsola sieciowa**		6	8	8	10	10	12	12
Serwer komunikacji		6	8	8	10	10	16	20
Baza danych***		6	6	6	6	6	9	12
Łącznie	**8**	**22**	**26**	**26**	**30**	**30**	**43**	**52**

* Doradzany kiedy nie są wykorzystywane żadne Relaye.

** Dla każdej aktywnej integracji dodaj jeden vCPU na urządzeniu wirtualnym z rolą konsoli sieciowej.
*** W przypadku rozproszonej instalacji ról, wraz z zestawem replik: dla każdej dodatkowej instancji bazy danych dodaj podaną liczbę do całkowitej wartości.

RAM (GB)

Składnik	Ilość punktów końcowych (maksymalna)							
	250	500	1000	3000	5000	10000	25000	50000
Podstawowe cechy GravityZone								
Serwer aktual.	16	16	18	20	2	2	3	3
Konsola internetowa*					8	8	12	16
Serwer komunikacji					6	12	12	16
Baza danych**					8	10	12	12
Łącznie	**16**	**16**	**18**	**20**	**24**	**32**	**39**	**47**
GravityZone z Bitdefender HVI								
Serwer aktual.	16	2	2	2	2	2	3	3
Konsola internetowa*		8	10	10	10	10	12	16
Serwer komunikacji		8	10	10	12	12	16	20
Baza danych**		8	8	8	8	12	12	12
Łącznie	**16**	**26**	**30**	**30**	**32**	**36**	**43**	**51**

* Dla każdej aktywnej integracji, dodaj jeden gigabajt RAM na wirtualnej maszynie z rolą konsoli sieciowej.
** W przypadku rozproszonej instalacji ról, wraz z zestawem replik: dla każdej dodatkowej instancji bazy danych dodaj podaną liczbę do wartości całkowitej.

Wolna przestrzeń dyskowa (w GB)

Składnik	Ilość punktów końcowych (maksymalna)								
	250	250*	500	1000	3000	5000	10000	25000	50000
Podstawowe cechy GravityZone									
Serwer aktual.	120	**160**	160	200	200	80	80	80	80
Konsola internetowa						80	80	80	80
Serwer komunikacji						80	80	80	80
Baza danych**						80	120	200	500
Łącznie	**120**	**160**	**160**	**200**	**200**	**320**	**360**	**440**	**740**
GravityZone z Bitdefender HVI									
Serwer aktual.	120	160	80	80	80	80	80	80	80
Konsola internetowa			80	80	80	80	80	80	80
Serwer komunikacji			80	80	80	80	80	80	80
Baza danych**			80	80	100	100	160	300	700
Łącznie	**120**	**160**	**320**	**320**	**340**	**340**	**400**	**540**	**940**

WAŻNE
Zalecane jest użycie dysków Solid-state (SSD).

* Dodatkowa przestrzeń na dysku SSD jest potrzebna kiedy wybierasz instalację automatyczną, ponieważ wtedy jest także instalowany Security Server Kiedy instalacja zostanie zakończona, możesz usunąć Security Server aby zwolnić przestrzeń dyskową.
** W przypadku rozproszonej instalacji ról, wraz z zestawem replik: dla każdej dodatkowej instancji bazy danych dodaj podaną liczbę do wartości całkowitej.

4.1.3. Połączenie z Internetem

Urządzenie GravityZone wymaga dostępu do Internetu.

4.2. Control Center

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 16+
- Zalecana rozdzielczość ekranu: 1280 x 800 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.

4.3. Ochrona Punktu Końcowego

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

Wymagania dla agenta bezpieczeństwa są różne, w zależności od tego, czy ma dodatkowe role serwera, takie jak Relay, Ochrona Exchange lub Serwer pomocniczy zarządzania aktualizacjami. W celu uzyskania większej ilości informacji na temat ról agenta, zobacz „Agenci Bezpieczeństwa” (p. 8).

4.3.1. Sprzęt komputerowy

Agent bezpieczeństwa bez ról

Użycie procesora

Docelowe systemy	Typ procesora	Wspierane systemy operacyjne (OS)
Stacje robocze	Procesory kompatybilne z Intel® Pentium, 2 GHz bądź szybsze	Systemy Operacyjne Microsoft Windows
	Intel® Core 2 Duo, 2 GHz lub szybszy	macOS
Inteligentne Urządzenia	Procesory kompatybilne z Intel® Pentium, 800 MHZ lub szybsze	Systemy osadzone Microsoft Windows
Serwery	Minimum: procesory kompatybilne z Intel® Pentium, 2.4 GHz	Systemy operacyjne Microsoft Windows Server i Linux
	Rekomendowane: procesory wielordzeniowe Intel® Xeon, 1.86 GHz lub szybsze	

Ostrzeżenie
Procesory ARM obecnie nie są wspierane.

Wolna pamięć RAM

Podczas instalacji (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
macOS	1024	1024	n/d	n/d	n/d	n/d

Do codziennego użycia (MB)*

OS	Antywirus (Poj. Silnik)			Moduły Ochrony				
	Lokalny	Hybrydowy	Scentraliz.	Skanowanie Behaw.	Zapora Sieciowa	Kontrola Zaw.	Power User	Serw Aktu
Windows	75	55	30	+13	+17	+41	+29	+8
Linux	200	180	90	-	-	-	-	-
macOS	650	-	-	+100	-	+50	-	-

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

Wolna przestrzeń dyskowa

Podczas 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	1600	1600	1100	1100	600	600	1600	1600	1100	1100
macOS	1024	1024	n/d	n/d	n/d	n/d	n/d	n/d	n/d	n/d

Do codziennego użycia (MB)*

OS	Antywirus (Poj. Silnik)			Moduły Ochrony				
	Lokalny	Hybrydowy	Scentraliz.	Skanowanie Behaw.	Zapora Sieciowa	Kontrola Zaw.	Power User	Serw Aktu
Windows	410	190	140	+12	+5	+60	+80	+1
Linux	500	200	110	-	-	-	-	-
macOS	1700	-	-	+20	-	+0	-	-

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

Agent bezpieczeństwa z rolą relay

Rola relay wymaga dodatkowych zasobów sprzętowych w porównaniu z podstawową konfiguracją agenta bezpieczeństwa. Wymagania te dotyczą obsługi serwera aktualizacji i pakietów instalacyjnych obsługiwanych przez punkt końcowy:

Ilość podłączonych punktów końcowych	CPU wspierający serwer aktualizacji	RAM	Wolna przestrzeń dyskowa dla serwera aktualizacji
1-300	minimum to procesor Intel® Core™ i3 bądź równoważny, 2 vCPU na rdzeń	1.0 GB	10 GB
300-1000	minimum to procesor Intel® Core™ i5 bądź równoważny, 4 vCPU na rdzeń	1.0 GB	10 GB

Ostrzeżenie

- Procesory ARM obecnie nie są wspierane.
- Agenci Relay wymagają dysków SSD, aby obsługiwać dużą liczbę operacji odczytu / zapisu.

WAŻNE

- Jeśli chcesz zapisać pakiety instalacyjne i aktualizacje na innej partycji niż ta, w której zainstalowany jest agent, upewnij się, że obie partycje mają wystarczającą ilość wolnego miejsca na dysku (10 GB), w przeciwnym razie agent przerwie instalację. Jest to konieczne tylko podczas instalacji.
- W punktach końcowych Windows muszą być włączone linki symboliczne lokalne do lokalnych

Agent bezpieczeństwa z funkcją serwera pomocniczego aktualizacji łatek.

Agent z rolą serwera pomocniczego łatek musi spełniać następujące wymagania zbiorcze:

- Wszystkie wymagania sprzętowe pojedynczego agenta bezpieczeństwa (bez ról).
- Wszystkie wymagania sprzętowe dla roli Relay.
- Dodatkowo 100 GB wolnej przestrzeni dyskowej dla składowania ściągniętych łatek

WAŻNE
Jeśli chcesz zapisać poprawki na innej partycji niż ta, na której zainstalowany jest agent, upewnij się, że obie partycje mają wystarczającą ilość wolnego miejsca na dysku (100 GB), w przeciwnym razie agent przerwie instalację. Jest to konieczne tylko podczas instalacji.

4.3.2. Wspierane systemy operacyjne

system Windows w wersji na komputery stacjonarne

- Windows 10 October 2020 Update (20H2)
- Windows 10 May 2020 Update (20H1)
- Windows 10 November 2019 Update (19H2)
- Windows 10 May 2019 Update (19H1)
- Aktualizacja Windows 10 z 10 październik 2018 (Redstone 5)
- Windows 10 April 2018 Update (Redstone 4)
- Windows 10 Fall Creators Update (Redstone 3)
- Windows 10 Creators Update (Redstone 2)
- Windows 10 Anniversary Update (Redstone 1)
- Windows 10 November Update (Threshold 2)
- Windows 10
- Windows 8.1

- Windows 8
- Windows 7

Ostrzeżenie
Bitdefender nie obsługuje Windows Insider Program builds.

Windows Tablet and Embedded

- Windows 10 IoT Enterprise
- 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 Serwer

- Windows Server 2019
- Windows Server 2019 Core
- Windows Server 2016
- Windows Server 2016 Core
- Windows Server 2012 R2
- Windows Server 2012
- Windows Small Business Server (SBS) 2011
- Windows Server 2008 R2

Linux

WAŻNE
Punkty końcowe Linux używają miejsc licencji z puli licencji dla systemów operacyjnych serwera.

- Ubuntu 14.04 LTS lub wyższy

- Red Hat Enterprise Linux / CentOS 6.0 lub wyżej[2]
- SUSE Linux Enterprise Server 11 SP4 lub wyższy
- OpenSUSE Leap 42.x
- Fedora 25 lub wyższy[1]
- Debian 8.0 lub wyższy
- Oracle Linux 6.3 lub nowszy
- Amazon Linux AMI 2016.09 lub nowszy
- Amazon Linux 2

Ostrzeżenie

(1) W Fedora 28 i wyżej, Bitdefender Endpoint Security Tools wymaga ręcznej instalacji pakietu `libnsl`, uruchamiając następujące polecenie:

```
sudo dnf install libnsl -y
```

(2) Dla minimalnych instalacji CentOS Bitdefender Endpoint Security Tools wymaga ręcznej instalacji pakietu `libnsl` poprzez następujące polecenie:

```
sudo yum install libnsl
```

Wymagania Active Directory

Gdy integrujesz punkty końcowe z Linux z domeną Active Directory przez System Security Services Daemon (SSSD) upewnij się, że narzędzia **ldbsearch, krb5-user,** and **krb5-config** są zainstalowane i kerberos jest poprawnie skonfigurowany.

```
/etc/krb5.conf

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
        default_realm = DOMAIN.NAME
        dns_lookup_realm = true
        dns_lookup_kdc = true
        kdc_timesync = 1
```

```
        ccache_type = 4
        forwardable = true
        proxiable = true
        fcc-mit-ticketflags = true
        default_keytab_name = FILE:/etc/krb5.keytab

[realms]
        DOMAIN.NAME = {
                        kdc = dc1.domain.name
                        kdc = dc2.domain.name
                        admin_server = dc.domain.com
                        default_domain = domain.com
        }

[domain_realm]
 domain.name = DOMAIN.NAME
 .domain.name = DOMAIN.NAME

[appdefaults]
 pam = {
        debug = false
        ticket_lifetime = 36000
        renew_lifetime = 36000
        forwardable = true
        krb4_convert = false
        }
```

Notatka
We wszystkich wpisach rozróżniane są wielkie i małe litery.

Wsparcie skanowania Dostępowego

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

Wersje Jądra	Dystrybucje Linux	Wymagania Dostępowe
2.6.38 lub wyższe*	Red Hat Enterprise Linux / CentOS 6.0 lub wyżej	Opcja jądra **fanotify** musi być włączona.

Wersje Jądra	Dystrybucje Linux	Wymagania Dostępowe
	Ubuntu 14.04 lub wyższy SUSE Linux Enterprise Server 11 SP4 lub wyższy OpenSUSE Leap 42.x Fedora 25 lub wyższy Debian 9.0 lub wyższy Oracle Linux 6.3 lub nowszy Amazon Linux AMI 2016.09 lub nowszy	
2.6.38 lub wyższe	Debian 8	**Fanotify** musi być włączone i ustawione na tryb egzekwowania, a następnie pakiet jądra musi zostać przebudowany. Więcej szczegółów znajdziesz w tym artykule KB.
2.6.32 - 2.6.37	CentOS 6.x Red Hat Enterprise Linux 6.x	Bitdefender zapewnia wsparcie poprzez **DazukoFS** z prekombilowanymi modułami jądra.
Wszystkie inne jądra	Wszystkie inne obsługiwane systemy plików	Moduł **DazukoFS** musi zostać skompilowany ręcznie. Szczegółowe informacje znajdują się w „Ręcznie skompiluj moduł DazukoFS.” (p. 112).

* Z pewnymi ograniczeniami opisanymi poniżej.

Ograniczenia Skanowania Dostępowego

Wersje Jądra	Dystrybucje Linux	Szczegóły
2.6.38 lub wyższe	Wszystkie wspierane systemy	Monitory skanowania dostępowego montowały udziały sieciowe tylko w tych warunkach: • **Fanotify** jest włączone zarówno w systemach zdalnych, jak i lokalnych. • Udział jest oparty na systemach plików CIFS i NFS. **Notatka** Skanowanie dostępowe nie skanuje udziałów sieciowych podłączonych za pomocą SSH lub FTP.
Wszystkie jądra	Wszystkie wspierane systemy	Skanowanie dostępowe nie jest obsługiwane w systemach z **DazukoFS** dla udziałów sieciowych zamontowanych na ścieżkach już chronionych przez moduł dostępowy.

macOS

- macOS Big Sur (11.0)*
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)

Kontrola Zawartości nie jest wspierana w macOS Big Sur (11.0).

4.3.3. 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.

4.3.4. 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+

4.3.5. Wspierane platformy wirtualizacyjne

Security for Virtualized Environments zapewnia wsparcie dla następujących platform wirtualizacji:

- VMware vSphere & vCenter Server 7.0, 6.7 update 3, update 2a, 6.7 update 1, 6.7, 6.5, 6.0, 5.5, 5.1, 5.0

  Notatka
  Funkcja Zarządzania Obciążeniem w vSphere 7.0 nie jest obsługiwana.

- VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x
- Stacje robocze VMware 11.x, 10.x, 9.x, 8.0.6
- VMware Player 7.x, 6.x, 5.x
- Citrix XenServer 8.x, 7.x, 6.5, 6.2, 6.0, 5.6 or 5.5 (włączając Xen Hypervisor)
- Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906
- Citrix XenApp i XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR
- 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
- Oracle VM VirtualBox 5.2, 5.1
- Nutanix Prism with AOS (LTS) 5.5, 5.10, 5.15
- Nutanix Prism with AOS (STS) 5.6, 5.11, 5.18
- Nutanix Prism with AHV (Community Edition) 20170830.115, 20170830.301, 20170830.395, 20190916.294

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

Wspierane platformy w chmurze

Wraz z lokalnymi środowiskami wirtualizacji GravityZone może również zintegrować się z następującymi platformami chmurowymi:

- **Amazon EC2**

  Jako klient Amazon EC2 możesz zintegrować zasoby instancji EC2 pogrupowanych według regionów i stref dostępności za pomocą zasobów sieciowych GravityZone.

- **Microsoft Azure**

  Jako klient Amazon Azure możesz zintegrować zasoby maszyn wirtualnych Azure pogrupowanych według regionów i stref dostępności za pomocą zasobów sieciowych GravityZone.

Zgodność z Technologiami Wirtualizacji Komputerów Stacjonarnych i Aplikacji

GravityZone jest kompatybilny z następującymi technologiami wirtualizacji, począwszy od wersji Bitdefender Endpoint Security Tools 6.6.16.226:

- **VMware:**

  VMware V-App (ta sama wersja z vCenter Server)

  VMware ThinApp 5.2.6

  VMware AppVolumes 2.180

WAŻNE
Nie zaleca się instalowania w Stosie Aplikacji ani woluminach do zapisu.

- **Microsoft:**

  Microsoft App-V 5.0, 5.1

  Microsoft FSLogix 2.9.7237

- **Citrix:**

  Citrix App Layering 19.10

  Citrix Appdisks 7.12

WAŻNE
Przypisz polityki na podstawie reguł użytkownika, aby Kontrola Urządzenia nie uniemożliwiała działania systemu operacyjnego i tworzeniu warstw platformy. Może być konieczne skonfigurowanie reguł Zapory Sieciowej GravityZone, aby zezwalała na ruch sieciowy dla każdej z tych aplikacji. Po więcej informacji zajrzyj do Dokumentacja produktu Citrix App Layering.

Wspierane Narzędzia Zarządzania Wirtualizacjami

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

- Serwer VMware vCenter
- Citrix XenServer
- Nutanix Prism Element

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

4.3.6. 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
- On macOS: ~25 MB

- **Pobrany ruch aktualizacji zawartości zabezpieczeń między klientem punktu końcowego a serwerem aktualizacji (MB/dzień)**

Typ Serwera Aktualizacji	Typ Silnika Skanowania		
	Lokalny	Hybrydowy	Scentraliz.
Relay	65	58	55
Bitdefender publiczny serwer aktualizacji	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

Przeskanowane Obiekty	Typ Ruchu	Pobrano (MB)	Przesłano (MB)
	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 między klientami Bitdefender Endpoint Security Tools Relay a serwerem aktualizacji do pobierania zawartości zabezpieczeń**

  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.

4.4. Sandbox Analyzer On-Premises

Sandbox Analyzer On-Premises ma następujące szczegółowe wymagania:

- ESXi Hypervisor (platforma wirtualizacyjna, na której będzie działać środowisko).
- Sandbox Analyzer Urządzenie Wirtualne (urządzenie zarządzające, które będzie kontrolować detonujące maszyny wirtualne).
- Urządzenie Wirtualne Ochrony Sieci (maszyna wirtualna, która hermetyzuje czujnik sieciowy zdolny do wyodrębniania ładunku z ruchu sieciowego).
- Łączność z istniejącą GravityZone Control Center służy do zarządzania wysokiego poziomu środowiskiem sandbox.
- Połączenie internetowe do pobrania Wirtualnego Urządzenia Sandbox Analyzer z minimalną przepustowością 5 MBps.

WAŻNE
Upewnij się, że nie działają żadne inne aplikacje lub procesy, które mogą blokować połączenie z internetem podczas pobierania i instalacji Sandbox Analyzer.

4.4.1. ESXi Hypervisor

Wirtualne Urządzenie Sandbox Analyzer jest dostępne w formacie OVA, do wdrożenia na pojedynczym fizycznym hoście z Hiperwizorem Vmware ESXo (wersja 6.5 lub 6.7)

Wymagania Sprzętowe dla Fizycznego Hosta

- CPU: całkowita liczba rdzeni procesora (uwzględniając hyperthreading) może być ekstrapolowana używając obliczeń przedstawionych w sekcji „Wymagania Fizycznego Hosta i Skalowania Hardware” (p. 35).
- RAM: całkowita ilość wymaganej pamięci RAM dla fizycznego hosta może być ekstrapolowana używając obliczeń przedstawionych w sekcji „Wymagania Fizycznego Hosta i Skalowania Hardware” (p. 35).
- Przestrzeń Dyskowa: co najmniej 1TB dysk SSD (adekwatne dla 8-WM środowiska detonacyjnego, skalowalne z co najmniej 50GB dla każdej dodatkowej WM detonacyjnej).
- Sieć: jedna dedykowana fizyczna karta sieciowa (NIC)

  Ta NIC może być podzielona na dwie wirtualne karty sieciowe z następującymi mapowaniami:

  – Jeden NIC dla interfejsu zarządzania.
  – Jeden NIC dla sieci detonacyjnej.

  Notatka
  Zalecane jest używanie dedykowanych fizycznych NIC'ów z takim samym mapowaniem jak powyżej wspomniane vNIC jeżeli konfiguracja sprzętowa na to zezwala.

Wymagania Systemowe

Wspierane wersje serwera ESXi: 6.5 lub wyżej, VMFS wersja 5.

Dodatkowo konfiguracja hosta ESXi:

- SSH włączone podczas startu.
- Usługa NIP skonfigurowana i aktywna.
- Opcja **uruchamiaj/zatrzymuj wraz z hostem** włączona.

Notatka
Sandbox Analyzer jest kompatybilny z wersją próbną VMWare ESXi. Jednak w przypadku wdrożeń produkcyjnych zaleca się uruchamianie na licencjonowanej wersji ESXi.

4.4.2. Sandbox Analyzer Urządzenie Wirtualne

Sandbox Analyzer Urzadzenie Wirtualne dostarcza nielimitowaną wirtualną skalowalność, tak długo jak podstawowe zasoby sprzętowe są dostępne.

Z całkowitej ilości dostępnych zasobów ESXi, Sandbox Analyzer współdzieli procesor i pamięć RAM między Menedżerem Sandbox, a wirtualnymi maszynami do detonacji.

Minimalne Wymagania Systemowe Menedżera Sandbox

- 6 vCPU
- 20 GB pamięci RAM
- 600 GB miejsca na dysku

Menedżer Sandbox ma trzy wewnętrzne wirtualne karty sieciowe (NIC) przydzielone w następujący sposób:

- Jedna karta sieciowa (NIC) do komunikacji z konsolą zarządzania (GravityZone Control Center)
- Jedna karta sieciowa (NIC) do połączenia z Internetem.
- Jedna karta sieciowa (NIC) do komunikacji z detonacyjnymi maszynami wirtualnymi

Notatka
Aby umożliwić komunikację, zarówno karta zarządzająca ESXi, jak i karta zarządzająca Menedżera Sandbox muszą znajdować się w tej samej sieci.

Detonacja maszyn wirtualnych

Wymagania systemowe

- 4 vCPU (nadwyżka w stosunku 4:1, odnieś się do „Wymagania Fizycznego Hosta i Skalowania Hardware” (p. 35))
- 3GB RAM
- 50 GB miejsca na dysku

Sandbox Analyzer On-Premises posiada wsparcie dla niestandardowych obrazów maszyn wirtualnych. Pozwala to na detonację próbek w środowisku wykonawczym, które naśladuje realistyczne środowisko produkcyjne.

Utworzenie obrazu maszyny wirtualnej wymaga:

- Obraz maszyny wirtualnej musi być w formacie VMDK, wersja 5.0.
- Obsługiwane systemy operacyjne do budowy wirtualnych maszyn detonacyjnych:
  - Windows 7 64-bit (dowolny poziom aktualizacji)
  - Windows 10 64-bit (dowolny poziom aktualizacji)

WAŻNE

- System operacyjny musi być zainstalowany na drugiej partycji w tablicy partycji i zamontowany na dysku C: (domyślna konfiguracja instalacji systemu Windows).
- Lokalne konto „Administrator” musi być włączone i mieć pusty ciąg hasła (wyłączenie hasła).
- Przed wyeksportowaniem obrazu maszyny wirtualnej należy poprawnie licencjonować system operacyjny i całe zainstalowane oprogramowanie na obrazie maszyny wirtualnej.

Oprogramowanie do Obrazu Maszyny Wirtualnej

Sandbox Analyzer obsługuje detonację w szerokiej gamie formatów i typów plików. Szczegółowe informacje znajdują się w „Obiekty Sandbox Analyzer ” (p. 156).

W przypadku rozstrzygających raportów upewnij się, że na niestandardowym obrazie zainstalowano oprogramowanie, które może otworzyć określony typ pliku, który chcesz zdetonować. Szczegółowe informacje znajdują się w „Zalecane Aplikacje dla Detonacyjnych VM” (p. 157).

4.4.3. Wirtualny Serwer Bezpieczeństwa Sieci

Urządzenie Wirtualnej Ochrony Sieci obsługuje czujnik sieciowy, który pobiera zawartość ze strumieni sieciowych i przesyła ją do Sandbox Analyzer. Minimalne wymagania sprzętowe to:

- 4 vCPU
- 4 GB pamięci RAM
- 1 TB miejsca na dysku
- 2 vNIC

4.4.4. Wymagania Fizycznego Hosta i Skalowania Hardware

Algorytm skalowania Sandbox Analyzer rozważa następującą formułę, gdzie "K" równa się liczbie slotów detonacji (lub WM do detonacji):

- Sandbox Analyzer VA vCPU = 6 vCPUs + K x 1vCPU
- Sandbox Analyzer VA RAM = 20 GB RAM + K x 2GB

Podobnie, algorytm skalowania dla hosta jest następujący:

- ESXi Host vCPU = 6 vCPUs + K x 2 vCPU
- ESXi Host RAM = 20 GB RAM + K x 5 GB

Główną różnicą pomiędzy zasobami Sandbox Analyzer VA i ESXi wynika z zasobów przypisanych do każdej WM do detonacji.

W związku z tym, typowe środowisko detonacyjne (8 WM) miałoby następujące wymagania:

- Sandbox Analyzer VA vCPU = 6 vCPUs + 8 x 1vCPU = 14 vCPUs
- Sandbox Analyzer VA RAM = 20 GB RAM + 8 x 2GB = 36GB RAM
- ESXi Host vCPU = 6 vCPUs + 8 x 2 vCPUs = 22 vCPUs

  Notatka
  Każda WM do detonacji wymaga przypisanego 1 vCPU do Sandbox Analyzer VA i 1 vCPU dla WM do detonacji. WM do detonacji będzie zaopatrzona w 4 vCPU, ale ze względu na nadwyżkę 4:1, tylko 1 vCPU będzie wymagany dla hosta ESXi.

- ESXi Host RAM = 20 GB RAM + 8 x 5 GB = 60 GB RAM

Notatka
RAM jest wykorzystywany w stosunku 1:1 pomiędzy Sandbox Analyzer VA, WM do detonacji i hostem ESXi. Tak więc, każda WM do detonacji będzie wymagać 5 GB Ramu z hosta ESXi, z czego 2 GB zostaną przydzielone do Sandbox Analyzer VA i 3 GB bezpośrednio do WM.

Wynikowy fizyczny host wymaga, we wspomnianym wyżej scenariuszu wymaga, co najmniej 22 rdzeni procesora (razem z hyperthreadingiem), co najmniej 60 GB ramu, z dodatkowym 10-20% RAM zarezerwowanym dla hypervisora.

Wykonanie detonacji próbka i wygenerowanie raportu zazwyczaj zajmuje 9 minut i wykorzystuje wszystkie przypisane zasoby. Zalecanym jest, aby zaprojektować swoje środowisko sandbox zaczynając od pojemności detonacji (pliki/godzina) i następnie przeliczyć to na wymagane zasoby dla poziomie hosta i WM.

4.4.5. Sandbox Analyzer Wymagania Komunikacji

Komponenty Sandbox Analyzer On-Premises używają pewnych portów komunikacyjnych przypisanych do określonych interfejsów sieciowych, w celu komunikacji między sobą i z publicznymi serwerami Bitdefender.

Środowisko sandbox wymaga trzech interfejsów sieciowych:

- **eth0 - Zarządzający interfejs sieciowy**. Łączy się z GravityZone i hostem ESXi.

  Zalecane jest eth0 do tej samej sieci co interfejs zarządzania ESXi. Zalecane również jest zmapowanie go do dedykowanego fizycznego adaptera.

  Następująca tabela opisuje wymagania komunikacyjne dla eth0:

Kierunek	Porty komunikacyjne (na TCP)	Źródło/miejsce docelowe
Wysyłane	8443	Serwer Komunikacji GravityZone
	443	Urządzenie Wirtualne GravityZone
	80	Urządzenie Wirtualne GravityZone
	22	Host ESXi
	443	API hosta ESXi
Odbierane	8443	Dowolny

- **eth1 - Sieć detonacji**. Nie wymaga żadnej konfiguracji. Proces instalacyjny tworzy potrzebne wirtualne zasoby.

- **eth2 - Sieć dostępu do internetu**. Zalecane jest nieograniczone i niefiltrowane połączenie z internetem.

  Zalecane jest aby sieć zarządzająca i sieć dostępu do internetu były przypisane do innych podsieci.

Wirtualne Urządzenie GravityZone wymaga dostępu do Wirutalnego Urządzenia Sandbox Analyzer na porcie 443 (na TCP) w celu przeglądania i pobierania raportów Sandbox Analyzer.

Wirtualne Urządzenie GravityZone wymaga połączenia do Wirutalnego Urządzenia Sandbox Analyzer na porcie 443 (na TCP) do zapytań o stan zdetonowanych próbek.

4.5. Pełne szyfrowanie dysku

GravityZone Full Disk Encryption pozwala na obsługę BitLocker w punktach końcowych Windows i FileVault oraz w narzędziu wiersza poleceń diskutil w punktach końcowych macOS poprzez Control Center.

W celu ochrony danych, moduł zapewnia pełne szyfrowanie dysku dla woluminów rozruchowych i woluminów non-boot na dyskach stałych. Zapisuje również klucze odzyskiwania na wypadek, gdyby użytkownicy zapomnieli hasła.

Moduł szyfrowania wykorzystuje istniejące zasoby sprzętu w Twoim środowisku GravityZone.

Z perspektywy oprogramowania wymagania są prawie takie same jak w przypadku BitLocker, FileVault i narzędzia wiersza polecenia diskutil, a większość ograniczeń dotyczy tych narzędzi.

Dla Windows

GravityZone Szyfrowanie obsługuje funkcję BitLocker, począwszy od wersji 1. 2, na komputerach z i bez chipu Moduł Platformy Zaufanej (TPM)

GravityZone obsługuje funkcję BitLocker na punktach końcowych z następującymi systemami operacyjnymi:

- Windows 10 Education
- Windows 10 Enterprise
- Windows 10 Pro
- Windows 8.1 Enterprise
- Windows 8.1 Pro

- Windows 8 Enterprise
- Windows 8 Pro
- Windows 7 Ultimate (z TPM)
- Windows 7 Enterprise (z TPM)
- Windows Server 2019*
- Windows Server 2016*
- Windows Server 2012 R2*
- Windows Server 2012*
- Windows Server 2008 R2* (z TPM)

* BitLocker nie dotyczy tych systemów operacyjnych i musi być zainstalowany osobno. Aby uzyskać więcej informacji na temat wdrażania BitLocker w systemie Windows Server, zapoznaj się z artykułami KB, udostępnionymi przez firmę Microsoft:

- https://technet.microsoft.com/en-us/itpro/bitlocker-how-to-deploy-on-windows-server
- https://technet.microsoft.com/en-us/library/cc732725(v=ws.10).aspx

WAŻNE
GravityZone nie obsługuje szyfrowania w systemie Windows 7 i Windows 2008 R2 bez modułu TPM.

Szczegółowe wymagania dotyczące BitLocker znajdziesz w artykule KB firmy Microsoft: https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx

Dla Mac

GravityZone obsługuje FileVault i diskutil na punktach końcowych MacOS z następującymi systemami operacyjnymi:

- macOS Big Sur (11.0)
- macOS Catalina (10.15)
- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)

- OS X El Capitan (10.11)

4.6. Porty Komunikacji GravityZone

GravityZone jest rozwiązaniem rozproszonym, oznacza to, że jego komponenty komunikują się ze sobą poprzez sieć lokalną lub Internet. Każdy komponent wykorzystuje serię portów do komunikacji z pozostałymi. Musisz się upewnić, że te porty są otwarte dla GravityZone.

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

5. INSTALOWANIE OCHRONY

GravityZone to rozwiązanie typu klient-serwer. Aby chronić swoją sieć za pomocą Bitdefender, musisz wdrożyć role serwera GravityZone, zarejestrować swoją licencję, skonfigurować pakiety instalacyjne i wdrożyć je za pośrednictwem agentów bezpieczeństwa na punktach końcowych.

5.1. Instalacja i konfiguracja GravityZone

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

1. Przygotowanie do instalacji
2. Wdrożenie i instalacja GravityZone
3. Połącz się z Control Center i ustaw pierwsze konto użytkownika
4. Konfiguruj ustawienia Control Center

5.1.1. Przygotowanie do Instalacji

Do instalacji, potrzebujesz obrazu urządzenia wirtualnego GravityZone. Po wdrożeniu i skonfigurowaniu urządzenia GravityZone można zdalnie zainstalować klienta lub pobrać niezbędne pakiety instalacyjne z webowego interfejsu Control Center.

Obraz urządzenia GravityZone jest dostępny w kilku różnych formatach, kompatybilnych z głównymi platformami wirtualizacyjnymi. Linki do pobierania można uzyskać, rejestrując się po wersję trial na stronie internetowej Bitdefender .

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, szczegóły XenServer (nazwa hosta lub adres IP, port komunikacyjny, nazwa użytkownika i hasła dla administratora)
- Klucz licencyjny (sprawdź rejestracje wersji trial lub zakup e-mail)
- Ustawienia serwera poczty wychodzącej
- Jeżeli potrzebne, ustawienia serwera proxy

- Certyfikaty bezpieczeństwa

5.1.2. Wdrożenie GravityZone

Wdrożenie GravityZone składa się z jednego lub kilku urządzeń z rolami serwera. Liczba urządzeń zależy od różnych kryteriów, takich jak: rozmiar i projekt infrastruktury sieciowej lub funkcje GravityZone, których będziesz używać. Role serwera mają trzy typy: podstawowe, pomocnicze i opcjonalne.

WAŻNE
Role pomocnicze i opcjonalne są dostępne tylko dla niektórych rozwiązań GravityZone.

Rola GravityZone	Typ Reguły	Zainstaluj
Serwer bazodanowy Update Server Konsola internetowa Serwer komunikacji	Podstawowe (wymagane)	Przynajmniej jedna instancja każdej roli. Urządzenie GravityZone może uruchomić jedną, kilka lub wszystkie z tych ról.
Niedostępny	Opcjonalne	Niedostępny

W zależności od tego, jak rozdzielasz role GravityZone, wdrożysz jeden lub więcej urządzeń GravityZone. Serwer 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.

Możesz wdrożyć więcej instancji Serwera Bazy Danych, Konsoli Internetowej i Ról Serwera Komunikacyjnego. W takim przypadku użyjesz zestawu replik dla serwera bazy danych i równoważników obciążenia dla konsoli internetowej i serwera komunikacyjnego na urządzeniach GravityZone.

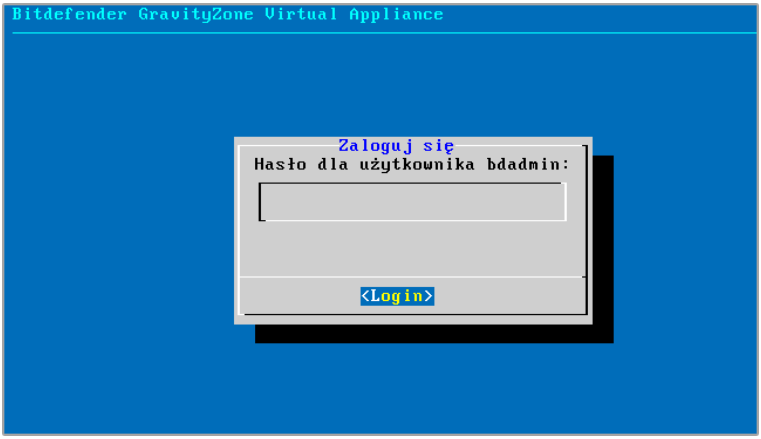
Aby wdrożyć i zainstalować GravityZone:

1. Pobierz obraz urządzenia wirtualnego GravityZone ze strony internetowej Bitdefender (link podany podczas rejestracji lub w e-mailu potwierdzającym zakup).
2. Importuj obraz urządzenia wirtualnego GravityZone w środowisku wirtualnym.
3. Zasilanie urządzenia.

4. Z narzędzia do zarządzania wirtualizacją, dostęp do interfejsu konsoli urządzenia GravityZone.
5. Ustaw hasło dla wbudowanego `bdadmin` administratora systemu.

Interfejs konsoli urządzenia: podaj nowe hasło.

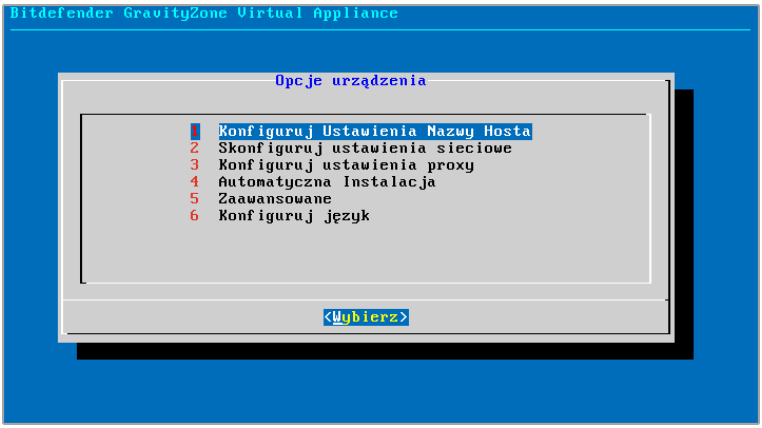
6. Zaloguj się używając ustawionego hasła



Interfejs konsoli urządzenia: login

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

7. Jeśli chcesz zmienić język interfejsu, wybierz opcję **Konfiguruj Język** . Szczegóły konfiguracji znajdują się w „Konfiguruj język” (p. 49).
8. Skonfiguruj nazwę hosta urządzenia.
9. Konfiguruj ustawienia sieciowe.
10. Skonfiguruj ustawienia serwera proxy. (w razie potrzeby)
11. Zainstaluj Role Serwera GravityZone. Masz dwie opcje:
    - Automatyczna Instalacja. Wybierz tę opcję, jeśli chcesz wdrożyć tylko jedno urządzenie GravityZone w swojej sieci.
    - Ustawienia Zaawansowane . Wybierz tę opcję, jeśli chcesz wdrożyć GravityZone ręcznie lub w architekturze rozproszonej.

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. 77).

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.

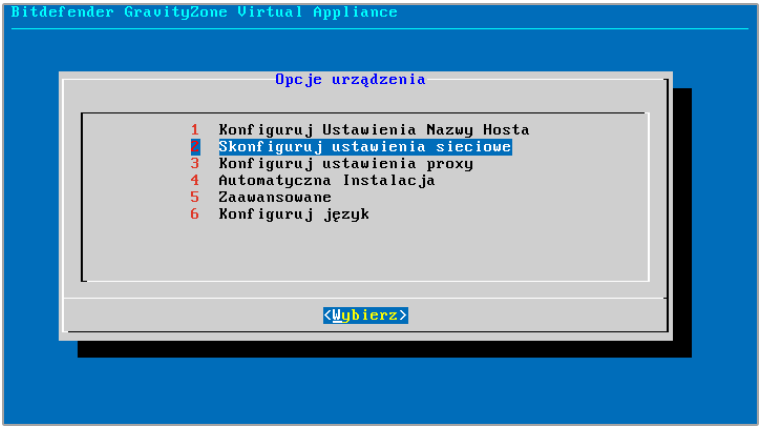
Aby skonfigurować ustawienia nazwy hosta:

1. Z menu głównego wybierz **Konfiguruj ustawienia nazwy hosta**.
2. Wprowadź nazwę hosta urządzenia i nazwę domeny usługi Active Directory (w razie potrzeby).
3. Wybierz **OK** aby zapisać zmiany.

Skonfiguruj ustawienia sieciowe

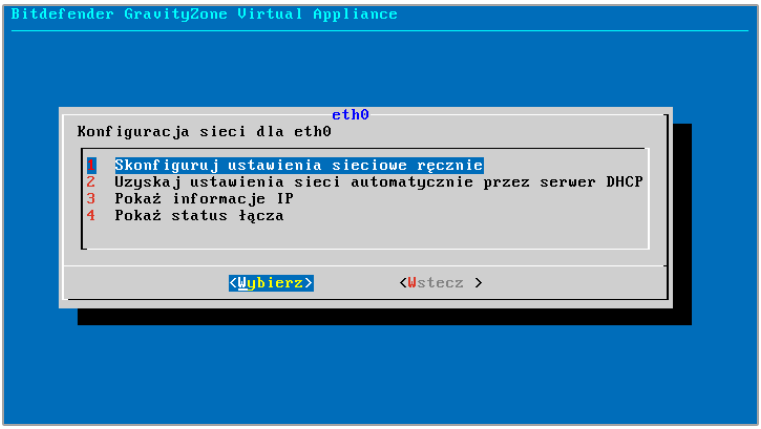
Można skonfigurować urządzenie, aby automatycznie uzyskać ustawienia sieciowe z serwera DHCP lub ręcznie skonfigurować ustawienia sieciowe. Jeśli zdecydujesz się skorzystać z DHCP, należy skonfigurować serwer DHCP, aby zarezerwować konkretny adres IP dla urządzenia.

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



Interfejs konsoli urządzenia: opcja ustawień sieciowych

2. Wybierz interfejs sieciowy.
3. 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.** Uzyj tej opcji tylko jeżeli masz skonfigurować serwer DHCP do zarezerwowania konkretnego adres IP dla urządzenia.



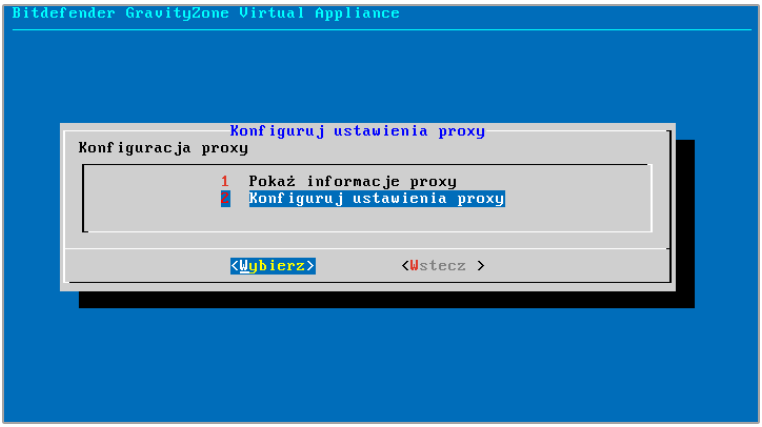
Interfejs konsoli urządzenia: ustawienia sieciowe

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

Konfiguruj ustawienia proxy

Jeśli chcesz, aby urządzenie łączyło się z Internetem za pośrednictwem serwera proxy, musisz skonfigurować ustawienia proxy.

1. Z menu głównego wybierz **Konfiguruj ustawienia Proxy**.
2. Wybierz **Pokaż informacje proxy** , aby sprawdzić, czy serwer proxy jest włączony.
3. Wybierz **OK** , aby powrócić do poprzedniego ekranu.
4. Wybierz ponownie **Skonfiguruj ustawienia proxy** .



Interfejs konsoli urządzenia: skonfiguruj ustawienia proxy

5. 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>`
6. Wybierz **OK** aby zapisać zmiany.

Automatyczna Instalacja

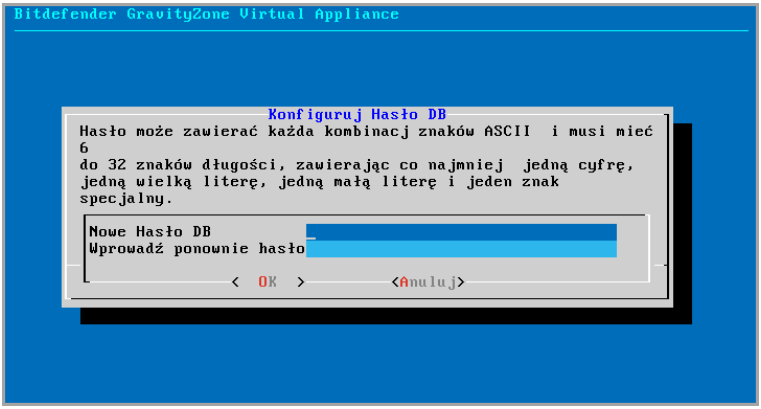
Podczas automatycznej instalacji wszystkie podstawowe role są instalowane na tym samym urządzeniu. W przypadku dystrybucji rozproszonej GravityZone zapoznaj się z „Zaawansowane” (p. 47).

WAŻNE
Wdrożenie automatyczne spowoduje również zainstalowanie Security Server wbudowanego w urządzenie GravityZone. Możesz usunąć tę rolę później, ponieważ twój typ licencji ogranicza jej użycie.
Opcja automatycznego instalowania ról jest dostępna tylko w początkowej konfiguracji GravityZone.

Aby zainstalować role automatycznie:

1. Z głównego menu, wybierz **Automatyczna Instalacja**.
2. Przeczytaj i zaakceptuj umowę licencyjną użytkownika końcowego (EULA), aby kontynuować.
3. Potwierdź role do zainstalowania.
4. Ustaw hasło dla Serwera 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

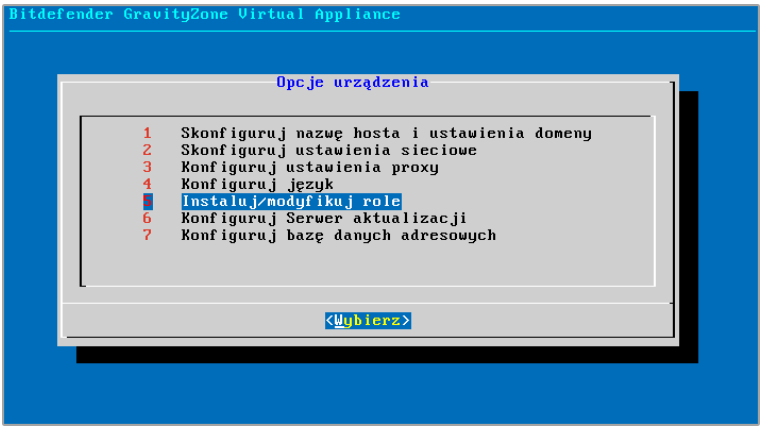
5. Poczekaj na zakończenie procesu instalacji.

Zaawansowane

Użyj tej opcji, aby zainstalować tylko część lub wszystkie role GravityZone, pojedynczo lub w celu rozszerzenia infrastruktury GravityZone. Możesz zainstalować role na jednym lub kilku urządzeniach. Ta metoda instalacji jest wymagana w przypadku rozmieszczania aktualizacji lub w rozproszonych architekturach GravityZone w celu skalowania GravityZone w dużych sieciach i zapewnienia wysokiej dostępności usług GravityZone.

Aby zainstalować role indywidualnie:

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



Interfejs konsoli urządzenia: instalowanie ról

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

   Notatka
   Inne opcje dotyczą rozszerzenia wdrożenia GravityZone do dystrybuowanej architektury. Po więcej informacji zajrzyj do „Połącz z Istniejącą Bazą Danych” (p. 88) lub do „Połącz z istniejącą bazą danych (bezpieczny klaster VPN)” (p. 89).

3. Wybierz **Dodaj lub usuń role**. Pojawi się nowa wiadomość potwierdzająca.
4. Naciśnij `Enter`, aby kontynuować.
5. Naciśnij `Spację`, a następnie `Enter`, aby zainstalować rolę bazy danych serwera. Musisz potwierdzić swój wybór naciskając ponownie `Enter`.
6. Ustaw 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.
7. Naciśnij `Enter` i poczekaj na zakończenie instalacji.
8. Zainstaluj inne role, wybierając **Dodaj lub usuń role** z menu **Instaluj/Odinstaluj Role** , a następnie role, które chcesz zainstalować.

a. Wybierz **Dodaj lub usuń role** z menu **Zainstaluj/ Odinstaluj role** .

b. Przeczytaj Umowę licencyjną użytkownika końcowego. Naciśnij `Enter` , aby zaakceptować i kontynuować.

> **Notatka**
> Jest to wymagane tylko raz po zainstalowaniu serwera bazy danych.

c. Wybierz role do zainstalowania. Naciśnij `Spację`, aby wybrać rolę, a następnie `Enter`, aby kontynuować.

d. Naciśnij `Enter` , aby potwierdzić, a następnie poczekaj 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.

Konfiguruj język

Początkowo, interfejs konfiguracji urządzenia jest po angielsku.

Aby zmienić język interfejsu:

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.

5.1.3. 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. Podaj klucz licencyjny wymagany do zatwierdzenia zakupionego rozwiązania GravityZone. Możesz również podać dowolny klucz add-on 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.

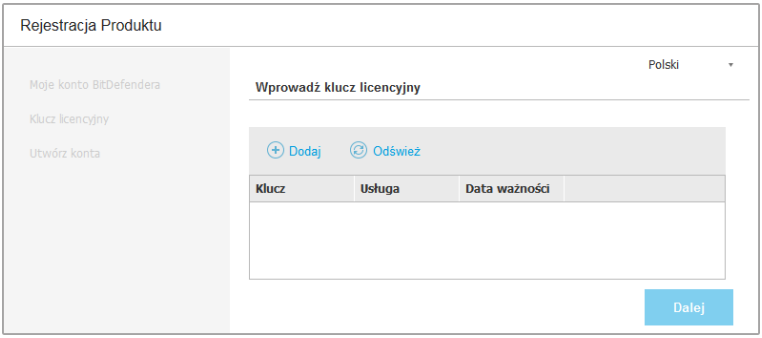
   b. Wybierz typ rejestracji licencji (online lub offline).

   c. Wprowadź 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 i jego termin ważności pojawią się w tabeli licencyjnej.

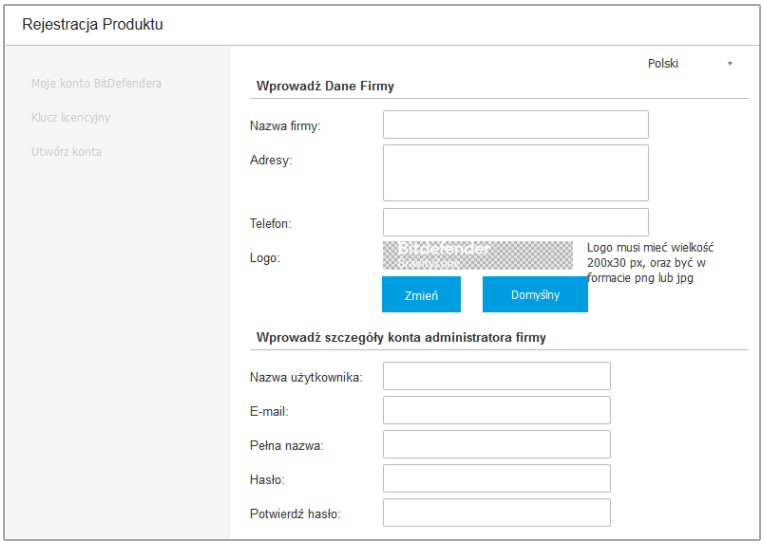
> **Notatka**
>
> - Podczas wstępnej konfiguracji musisz podać prawidłowy podstawowy klucz licencyjny, aby rozpocząć korzystanie z GravityZone. Możesz później dodać więcej kluczy licencyjnych dla dodatków lub modyfikować istniejące.
> - Możesz używać tych dodatków, o ile dostarczona jest ważna licencja podstawowa. W przeciwnym razie zobaczysz funkcje, ale nie będziesz mógł ich użyć.



Ustawienia początkowe - Zapewnia klucz licencyjny

3. Kliknij **Dalej** aby kontynuować.

4. Uzupełnij informacje Twojej firmy, takie jak nazwa firmy, adres i telefon.
5. 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.
6. 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

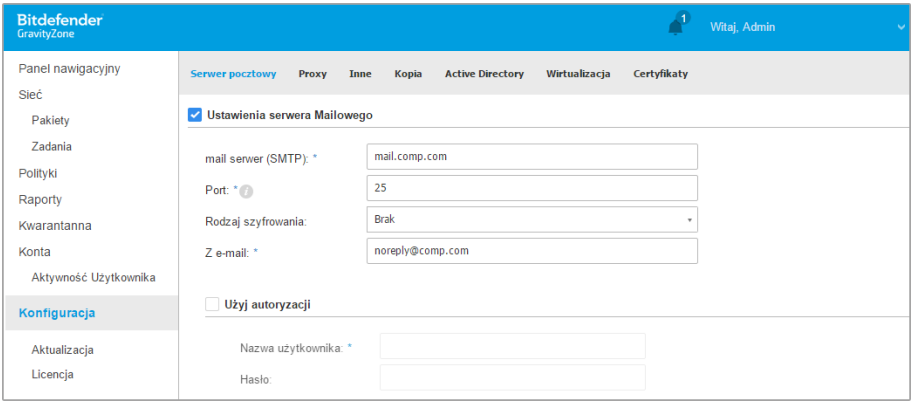
7. Kliknij **Utwórz konto**.

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

5.1.4. 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:
   - **Serwer pocztowy (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 uwierzytelnienia .** 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 zestaw.** 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.
- **Wymuś uwierzytelnianie dwuskładnikowe dla wszystkich kont.** Uwierzytelnienie dwuskładnikowe (2FA) dodaje dodatkową warstwę zabezpieczenia do kont GravityZone, wymagając oprócz danych uwierzytelniających Control Center, kodu uwierzytelniającego. Ta funkcja wymaga pobrania i zainstalowana albo Google Authenticator, Microsoft Authenticator lub inną aplikację uwierzytelniania dwuskładnikowego TOTP (Time-Based One-Time Password Algorithm) - kompatybilną ze standardem RFC6328 - na urządzeniu mobilnym użytkownika, następnie połączenie aplikacji z kontem GravityZone i używanie jej podczas każdego logowania do Control Center. Aplikacja Uwierzytelniająca generuje sześciocyfrowy kod co 30 sekund. Aby dokończyć logowanie do Control Center, po wprowadzeniu hasła użytkownik musi podać sześciocyfrowy kod uwierzytelniający.

  Uwierzytelnianie dwuskładnikowe jest domyślnie włączone podczas tworzenia firmy. Następnie podczas logowania okno konfiguracji poprosi użytkowników o włączenie tej funkcji. Użytkownicy będą mogli pominąć włączanie opcji 2FA tylko trzy razy. Przy czwartej próbie logowania pominięcie konfiguracji 2FA nie będzie możliwe, a użytkownik nie będzie mógł się zalogować.

Jeśli chcesz dezaktywować wymuszanie 2FA dla wszystkich kont GravityZone w swojej firmie, po prostu odznacz opcję. Przed wprowadzeniem zmian zostaniesz poproszony o potwierdzenie. Od tego momentu użytkownicy będą nadal mieli aktywowane 2FA, ale będą mogli dezaktywować go z poziomu ustawień konta.

Notatka

- Możesz wyświetlić status 2FA dla konta użytkownika na stronie **Konta**.
- Jeśli użytkownik z włączoną usługą 2FA nie może zalogować się do GravityZone (z powodu nowego urządzenia lub zgubionego tajnego klucza), można zresetować aktywację uwierzytelniania dwuskładnikowego ze strony konta użytkownika, pod **Uwierzytelnianie dwuskładnikowe**. Aby uzyskać więcej informacji, zapoznaj się z rozdziałem **Konta użytkowników > Zarządzanie uwierzytelnianiem dwuskładnikowym** w podręczniku administratora.

- **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 wysyłanych do serwera Syslog, zapoznaj się z rozdziałem **Powiadomienia** z Podręcznika 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. Wybierz format, w jakim dane mają być wysyłane do serwera Syslog:
     - **Format JSON**. JSON to lekki format wymiany danych, który jest całkowicie niezależny od jakiegokolwiek języka programowania. JSON reprezentuje dane w czytelnym formacie tekstowym W formacie JSON, szczegóły

każdego zdarzenia są podzielone na obiekty, a każdy obiekt składa się z pary nazwa / wartość.

Na przykład:

```
{
    "name":"Login from new device",
    "created":"YYYY-MM-DDThh:mm:ss+hh:ss",
    "company_name":"companyname",
    "user_name":"username",
    "os":"osname",
    "browser_version":"browserversion",
    "browser_name":"browsername",
    "request_time":"DD MMM YYYY, hh:mm:ss +hh:ss",
    "device_ip":"computerip"
}
```

Więcej informacji można znaleźć w www.json.org .

Jest to domyślny format w GravityZone.

– **Common Event Format(CEF)**. CEF to otwarty standard opracowany przez ArcSight, który upraszcza zarządzanie logami.

Na przykład:

```
CEF:0|Bitdefender|GZ|<GZ version>|NNNNN|Login from new
device|3|start=MMM DD YYYY hh:mm:ss+hh:mm
BitdefenderGZCompanyName=companyname suser=username
BitdefenderGZLoginOS=osname
BitdefenderGZAuthenticationBrowserName=browsername
BitdefenderGZAuthenticationBrowserVersion=browserversion
dvchost=computerip
```

Więcej iformacji znajdziesz ArcSight Common Event Format (CEF) Implementation Standard.

W rozdziale **Powiadomienia** w Podręczniku Administratora możesz wyświetlić dostępne typy powiadomień dla każdego formatu.

4. Naciśnij przycisk ⊕ **dodaj**a kolumny **Działanie**.

Naciśnij **Zapisz** aby zastosować zmiany.

Kopia zapasowa

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 najbardziej 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.
- Kopia zapasowa została zrobiona nie później niż 30.04.2017, a wersja GravityZone jest nowsza niż 6.2.1-30. W przeciwnym razie, skontaktuj się z zespołem Wsparcia Technicznego.
- 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. 64).

- 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. Przejdź do lokalizacji zawierającej archiwum bazy danych:

   ```
   # cd /directory-z kopią zapasową
   ```

   , gdzie `lokalizacja kopii zapasowej` jest ścieżką do lokalizacji z plikami kopii zapasowej.

   Na przykład:

   ```
   # cd /tmp/backup
   ```

2. Przywróć bazę danych.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_hasło
--authenticationDatabase admin --gzip --drop --archive < \
gz-backup-$RRRRMMDDdatownik
```

WAŻNE

Pamiętaj, aby zastąpić `[GZ_ db_ haslo]` rzeczywistym hasłem do serwera bazy danych GravityZone i zmiennymi datownika w nazwie archiwum za pomocą rzeczywista data.
Na przykład rzeczywista data powinna wyglądać tak:

```
gz-backup-2019-05-17(1495004926).tar.gz
```

3. Uruchom ponownie urządzenia.

   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 zainstalowaną TYLKO 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.
- Kopia zapasowa została zrobiona nie później niż 30.04.2017.
- 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. 64).

Przywracanie bazy danych

1. Połącz się z urządzeniem GravityZone za pomocą SSH i przełącz na **rdzeń** .
2. Przerwij VASync:

```
# stop vasync
```

3. Przerwij CLI:

```
# # killall -9 perl
```

4. Przejdź do lokalizacji kopii zapasowej:

```
# cd /directory-z kopią zapasową
```

, gdzie `lokalizacja kopii zapasowej` jest ścieżką do lokalizacji z plikami kopii zapasowej.
Na przykład:

```
# cd /tmp/backup
```

5. Przywróć bazę danych.

```
# /opt/bitdefender/bin/mongoshellrestore -u bd -p 'GZ_db_hasło
--authenticationDatabase=admin --gzip --drop \
--archive='/home/bdadmin/gz-backup-$RRRRMMDDdatownik
```

WAŻNE
Pamiętaj, aby zastąpić `[GZ_ db_ haslo]` rzeczywistym hasłem do serwera bazy danych GravityZone i zmiennymi datownika w nazwie archiwum za pomocą rzeczywista data.
Na przykład rzeczywista data powinna wyglądać tak:

```
gz-backup-2019-05-17(1495004926).tar.gz
```

6. Przywrócenia ID starego urządzenia:

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

WAŻNE
Pamiętaj, aby zastąpić `[GZ_ db_ hasło]` rzeczywistym hasłem do serwera bazy danych GravityZone.

7. Usuń odniesienie do ról pierwotnych.

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

WAŻNE
Pamiętaj, aby zastąpić `[GZ_ db_ hasło]` rzeczywistym hasłem do serwera bazy danych GravityZone.

8. Rozpocznij VASync.

```
# start vasync
```

9. Rozpocznij CLI:

```
# /opt/bitdefender/eltiw/installer
```

10. Zainstaluj inne role.

```
# dpkg -l gz*
```

Schemat bazy danych został pomyślnie uaktualniony do najnowszej wersji:

```
> db.settings.findOne().database
{
"previousVersion" : "000-002-009",
"ranCleanUpVersions" : {
"b0469c84f5bf0bec0b989ae37161b986" : "000-002-008"
},
"updateInProgress" : false,
"updateTimestamp" : 1456825625581,
"version" : "000-002-011"
}
```

11. Uruchom ponownie urządzenia.

    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.

Active Directory

Dzięki integracji Active Directory można importować do Control Center istniejące zasoby z Active Directory on-premise oraz z Active Directory hostowanego w Microsoft Azure, co upraszcza wdrażanie zabezpieczeń, zarządzanie nimi, monitorowanie i raportowanie. Dodatkowo, użytkownikom usługi Active Directory mogą być przypisane różne role w Control Center.

Żeby zintegrować i zsynchronizować GravityZone z domeny Active Directory:

1. Przejdź do strony **Konfiguracja > Active Directory > Domains** i kliknij ⊕ **Dodaj** .
2. Konfiguruj wymagane ustawienia:
   - Przedział synchronizacji (w godzinach)
   - Nazwa domeny Active Directory (łącznie z rozszerzeniem domeny)
   - Nazwa użytkownika i hasło administratora domeny
   - Lokalizacja w Network Inventory, gdzie wyświetlać punkty końcowe AD:

  - Zostaw strukturę AD i zignoruj puste OU
  - Zignoruj strukturę AD, importuj do Niestandardowych Grup
  - Zostaw strukturę AD tylko dla wybranych OU
- Kontrolery Domeny, którymi synchronizuje się Control Center. Rozwiń sekcję **Zażądaj Kontrolera Domeny** i wybierz kontrolery z tabeli.

3. Kliknij **Zapisz**.

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

Uprawnienia Dostępu

Z uprawnieniami dostępu możesz udzielić GravityZone Control Center dostępu do użytkowników usługi Active Directory (AD) na podstawie reguł dostępu. Aby zintegrować i zsynchronizować domeny AD, zapoznaj się z Active Directory. Więcej informacji na temat zarządzania kontami użytkowników za pomocą reguł dostępu można znaleźć w rozdziale **Konta użytkowników** w Przewodniku Instalacji GravityZone.

Dostawcy Wirtualizacji

GravityZone może obecnie zintegrować się z VMware vCenter Server, Citrix XenServer, Nutriix Prism Element, Amazon EC2 i Microsoft Azure.

- „Integracja z Serwerem vCenter” (p. 66)
- „Integracja z Serwerem XenServer” (p. 67)
- „Integracja z Nutanix Prism Element” (p. 67)
- „Integracja z Amazon EC2” (p. 69)
- „Integracja z Microsoft Azure” (p. 70)
- „Zarządzanie Integracjami Platformy” (p. 71)

WAŻNE
Kiedy ustawiasz nowa integracje z innym serwerem vCenter, XenServer, Nutanix Prism Element lub Microsoft Azure, pamiętaj aby przejrzeć i uaktualnić przywileje dostępu dla istniejących użytkowników.

Integracja z Serwerem vCenter

Możesz zintegrować GravityZone 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. Wejdź na stronę **Konfiguracja** w Control Center i przejdź do **Dostawcy Wirtualizacji > Platform Zarządzania** .
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. Użytkownik, którego poświadczenia dostarczasz musi mieć uprawnienia administratora lub roota na serwerze vCenter.
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**. 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.
7. Zaznacz pola wyboru, aby zaakceptować używane certyfikaty.
8. Kliknij **Zapisz**. Będziesz mógł zobaczyć vCenter Server na liście aktywnych integracji.

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

Integracja z Serwerem XenServer

Możesz zintegrować GravityZone z jednym albo wieloma Systemami serwera XenServer.

aby ustawić integracje z Serwerem XenServer:

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Dostawcy wirtualizacji**.
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.

Integracja z Nutanix Prism Element

Możesz zintegrować GravityZone z jednym lub wieloma klasterami Elementów Prism Nutanix, niezależnie od tego, czy są one zarejestrowane w Nutanix Prism Central, czy też nie.

Aby ustawić integrację z Nutanix Prism Element:

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Dostawcy wirtualizacji**.

2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli i wybierz **Nutanix Prism Element** z menu. Wyświetlone zostanie okno konfiguracji.
3. Określ szczegóły Nutanix Prism Element:
   - Nazwa Nutanix Prism Element w Control Center.
   - Adres IP Wirtualnej Maszyny Kontrolera (CVM) z klastra Nutanix Prism Element lub adres IP Wirtualnego adresu IP Klastra.
   - Nutanix Prism Element port (default `9440`).
4. Określ dane logowania, które maja zostać użyte do uwierzytelnienia z Nutanix Prism Element.

   WAŻNE
   Użytkownik, którego dane uwierzytelniające podasz, musi mieć uprawnienia Administratora Klastra lub Administratora Użytkownika w Nutriix Prism Element.

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 **Sieć**. Gdy ta opcja jest zaznaczona, administratorzy mogą zmienić politykę maszyn wirtualnych tylko z widoku Maszyn Wirtualnych w zasobach sieci.
6. Kliknij **Zapisz**. Zostaniesz poproszony o zaakceptowanie certyfikatów bezpieczeństwa dla Nutanix Prism. Certyfikaty te zapewniają bezpieczną komunikację pomiędzy GravityZone i Nutanix Prism Element, rozwiązując ryzyko ataków man-in-the-middle.

   Możesz sprawdzić, czy zostały zainstalowane poprawne certyfikaty poprzez sprawdzenie informacji w witrynie przeglądarki dla każdego klastra Nutanix Prism Element lub CVM na podstawie informacji certyfikatu wyświetlonego w polu Control Center.
7. Zaznacz pola wyboru, aby zaakceptować używane certyfikaty.
8. Kliknij **Zapisz**.

   Jeśli wprowadziłeś adres IP CVM, aby skonfigurować integrację, zostaniesz zapytany, czy chcesz użyć wirtualnego adresu IP klastra, zamiast adresu CVM:

   a. Kliknij **Tak**, aby użyć Wirtualnego adresu IP Klastra do integracji. Wirtualny adres IP Klastra zastąpi adres IP CVM w szczegółach Nutanix Prism Element.

   b. Kliknij **Nie**, aby dalej korzystać z CVM IP.

Notatka
Najlepszą praktyką jest używanie Wirtualnego adresu IP Klastra zamiast adresu CVM. W ten sposób integracja pozostaje aktywna nawet wtedy, gdy dany host staje się niedostępny.

c. W oknie **Dodaj Nutanix Prism Element** kliknij **Zapisz**.

Będziesz mógł zobaczyć Nutanix Prism Element na liście aktywnych integracji. Odczekaj kilka minut, aż do zakończenia synchronizacji.

Integracja z Amazon EC2

Możesz zintegrować GravityZone z zasobami Amazon EC2 i chronić swoje instancje EC2 hostowane w chmurze Amazon.

Warunki wstępne:

- Klucz dostępu i klucze tajne ważnego konta AWS
- Konto AWS musi mieć następujące uprawnienia:
  - `IAMReadOnlyAccess`
  - `AmazonEC2ReadOnly` dla wszystkich regionów AWS

Możesz utworzyć kilka integracji Amazon EC2. Dla każdej integracji musisz zapewnić prawidłowe konto użytkownika AWS.

Notatka
Nie można dodawać wielu integracji za pomocą poświadczeń ról IAM utworzonych dla tego samego konta AWS.

Aby skonfigurować integrację z Amazon EC2:

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Dostawcy wirtualizacji**.
2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli i wybierz **Integracja z Amazon EC2** z menu. Wyświetlone zostanie okno konfiguracji.
3. Podaj szczegóły integracji z Amazon EC2:
   - Nazwa integracji. Podczas dodawania kilku integracji z Amazon EC2 można je identyfikować według nazwy.
   - Klucze dostępu i tajne klucze do konta użytkownika AWS.

4. **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**.
5. Kliknij **Zapisz**. Jeśli podane poświadczenia są poprawne, integracja zostanie utworzona i dodana do siatki.

Poczekaj chwilę, a GravityZone zsynchronizuje się z zasobami Amazon EC2.

Integracja z Microsoft Azure

Możesz zintegrować GravityZone z Microsoft Azure i chronić swoje maszyny wirtualne hostowane w chmurze Microsoft.

Warunki wstępne:

- Aplikacja Azure z uprawnieniami do odczytu
- Active Directory ID
- ID aplikacji
- Sekret aplikacji

Szczegółowe informacje na temat uzyskiwania wymaganych poświadczeń i konfigurowania aplikacji Azure znajdują się w tym artykule KB.

Możesz utworzyć kilka integracji Microsoft Azure. Dla każdej integracji musisz mieć poprawny identyfikator Active Directory.

Aby skonfigurować integrację z Microsoft Azure:

1. Przejdź do strony **Konfiguracja** w Control Center i kliknij zakładkę **Dostawcy wirtualizacji**.
2. Kliknij przycisk ⊕ **Dodaj** w górnej części tabeli i wybierz **Azure Integration** z menu. Wyświetlone zostanie okno konfiguracji.
3. Podaj szczegóły integracji z Azure:
   - **Nazwa integracji**. Podczas dodawania kilku integracji z Azure można je identyfikować według nazwy.
   - **Active Directory ID**. Każde instancja Azure Active Directory ma unikalny identyfikator dostępny w szczegółach konta Microsoft Azure.
   - **ID Aplikacji**. Każda aplikacja Azure ma unikalny identyfikator dostępny w szczegółach aplikacji.

- **Sekret Aplikacji**. Tajny klucz aplikacji to wartość wyświetlana podczas zapisywania klucza w ustawieniach aplikacji Azure.

4. Wybierz opcję **Ogranicz przydział zasad z widoku sieciowego**, aby zmienić zasady tylko z widoku **Maszyny Wirtualne**. Jeśli opcja nie jest zaznaczona, możesz zmienić zasady z widoku **Komputery i Maszyny Wirtualne**.
5. Kliknij **Zapisz**. Jeśli podane poświadczenia są poprawne, integracja zostanie utworzona i dodana do siatki.

Poczekaj chwilę, a GravityZone zsynchronizuje się z zasobami Microsoft Azure.

Zarządzanie Integracjami Platformy

Aby edytować lub zaktualizować integrację platformy:

1. W Control Center przejdź do zakładki **Konfiguracja > Dostawcy Wirtualizacji**.
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. 66)
   - „Integracja z Serwerem XenServer” (p. 67)
   - „Integracja z Nutanix Prism Element” (p. 67)
   - „Integracja z Amazon EC2” (p. 69)
   - „Integracja z Microsoft Azure” (p. 70)
4. Kliknij **Zapisz**. Poczekaj kilka minut, aż do ponownej synchronizacji serwera.

Integracje Nutriix Prism Element, Amazon EC2 i Microsoft Azure są automatycznie synchronizowane co 15 minut. Możesz ręcznie zsynchronizować integrację w dowolnym momencie w następujący sposób:

1. W Control Center przejdź do zakładki **Konfiguracja > Dostawcy Wirtualizacji**.
2. Naciśnij przycisk **Resynchronizuj Zasoby** w kolumnie **Działanie**.
3. Kliknij **Tak**, aby potwierdzić akcję.

Przycisk **Resynchronizuj Zasoby** jest przydatny zwłaszcza, gdy zmienia się status integracji i wymaga on synchronizacji, tak jak w następujących sytuacjach:

- Do integracji z Nutriix Prism Element:
  - Użytkownik nie ma więcej uprawnień administracyjnych w inwentarzu.
  - Użytkownik staje się nieprawidłowy (zmienione lub usunięte hasło).

- Certyfikat ochrony jest staje się nieważny.
- Nie ma błędu połączenia.
- Host został dodany lub usunięty z klastra Nutanix Prism Element.

- Do integracji z Microsoft Azure:
  - Subskrypcja została dodana lub usunięta w Microsoft Azure.
  - Maszyny wirtualne są dodawane lub usuwane w zasobach Microsoft Azure.

Możesz także zsynchronizować integrację, klikając przycisk **Edytuj** , a następnie klikając **Zapisz**.

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

Dostawcy Bezpieczeństwa

GravityZone Security for Virtualized Environments integruje się z Centrum Danych VMware NSX-T poprzez Managera NSX-T.

Integracja z Managerem NSX-T

Manager NSX-T to płaszczyzna zarządzania Serwerami vCenter zintegrowana z Centrum Danych NSX-T. Aby integracja działała, należy skonfigurować integrację z Serwerami vCenter powiązanymi z Managerem NSX-T. Aby uzyskać więcej informacji, patrz Integracja z Serwerem vCenter.

Aby skonfigurować integrację z Managerem NSX-T:

1. W Control Center przejdź do **Konfiguracja > Dostawcy wirtualizacji > Dostawcy Zabezpieczeń** .
2. Kliknij przycisk **Dodaj** w górnej części tabeli. Wyświetlone zostanie okno konfiguracji.
3. Określ szczegóły integracji NSX-T:
   - Nazwa integracji NSX-T
   - Nazwa hosta lub adres IP powiązanego systemu Serwera vCenter.
   - Port NSX-T (domyślnie 433).
4. Określ poświadczenia 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. Kliknij **Zapisz**.

   Control Center jest teraz zintegrowana z NSX-T. Aby zastosować ochronę punktów końcowych do swoich maszyn wirtualnych za pomocą polityki Introspekcji Gości GravityZone, zapoznaj się z Konfiguruj i zastosuj ochronę punktu końcowego dla VMware NSX - T guest VMs przez GravityZone Guest Introspection policy Artykuł KB.

Notatka
GravityZone może być używany tylko do ochrony powiązanego Serwera vCenter.

NTSA

W tej sekcji możesz skonfigurować integrację z Bitdefender [NTSA_ LONG], rozwiązanie bezpieczeństwa dla przedsiębiorstw, które dokładnie wykrywają naruszenia i zapewniają wgląd w zaawansowane ataki, analizując ruch sieciowy. Aby dowiedzieć się więcej na temat tego rozwiązania, zapoznaj się z dokumentacją Bitdefender [NTSA_ SHORT] .

WAŻNE
Sekcja integracji [NTSA_ SHORT] jest dostępna tylko po podaniu ważnego klucza licencyjnego [NTSA_ SHORT] na stronie **Konfiguracja > Licencja** .

Aby skonfigurować integrację [NTSA_ SHORT], musisz zainstalować w swoim środowisku rozwiązanie i poświadczenia [NTSA_ SHORT] , aby uzyskać dostęp do konsoli internetowej [NTSA_ SHORT].

Podczas integracji wymagane będzie podanie adresu konsoli internetowej [NTSA_ SHORT] (IP lub Nazwy Hosta) oraz tokena (klucza parowania) wygenerowanego w konsoli internetowej [NTSA_ SHORT], jak wyjaśniono poniżej.

Skonfiguruj integrację NTSA

1. Zaloguj się do GravityZone Control Center.
2. Przejdź na stronę **Konfiguracja** i kliknij zakładkę [NTSA_ SHORT].
3. Włącz **Integruj z [NTSA_ LONG] ([NTSA_ SHORT])** .
4. Wprowadź następujące dane:
   - Adres konsoli internetowej [NTSA_ SHORT] (IP/Nazwa Hosta).

- Port używany przez GravityZone do komunikacji z [NTSA_ SHORT] (domyślnie 443).
- Klucz parowania (token) generowany przez konsolę [NTSA_ SHORT] w następujący sposób:
  a. Uzyskaj dostęp do konsoli internetowej [NTSA_ SHORT] i przejdź na stronę **Licencjonowanie** .
  b. Wybierz opcję **Integracja z GravityZone** .
  c. Kliknij **Generuj Klucz Parujący**. Klucz pojawi się automatycznie.
  d. Użyj przycisku **Kopiuj do schowka** , aby uzyskać klucz parowania.
  e. Kliknij **OK**, aby potwierdzić.

5. Sprawdź, czy wyświetlany odcisk palca hosta jest zgodny z hashem certyfikatu SSL z urządzenia [NTSA_ SHORT], a następnie włącz opcję **Akceptuję certyfikat** .
6. Kliknij **Zapisz**.

Po pomyślnym zakończeniu konfiguracji integracja zostanie wyświetlona jako **Zsynchronizowane** . Integracja [NTSA_ SHORT] może mieć następujące statusy:

- **N/A** : integracja nie została jeszcze skonfigurowana.
- **Zsynchronizowane** : integracja jest skonfigurowana i włączona.
- **Nieprawidłowy token** : klucz parowania z konsoli internetowej [NTSA_ SHORT] jest nieprawidłowy.
- **Błąd połączenia** : nie można połączyć się z określonym adresem konsoli internetowej [NTSA_ SHORT] (nieprawidłowy adres IP /Nazwa Hosta).
- **Błąd certyfikatu** : bieżący odcisk palca certyfikatu SSL z urządzenia [NTSA_ SHORT] nie pasuje do początkowo zaakceptowanego odcisku palca.
- **Nieznany błąd** : wystąpił nieznany błąd komunikacji.

Pole **Ostatnia zmiana statusu** wyświetla datę i godzinę ostatniej pomyślnej zmiany ustawień integracji lub gdy zmienił się status integracji.

Po skonfigurowaniu integracji z [NTSA_ SHORT] możesz wyłączyć/ włączyć integrację za pomocą pola wyboru dostępnego w górnej części strony **[NTSA_ SHORT]** .

Łączenie kont GravityZone i [NTSA_ SHORT]

Po skonfigurowaniu integracji Twoje konta GravityZone i [NTSA_ SHORT] zostaną połączone i możesz łatwo przejść do konsoli internetowej [NTSA_ SHORT] w następujący sposób:

1. W GravityZone Control Center kliknij przycisk **[NTSA_ SHORT]** umieszczony w lewym dolnym rogu okna.
2. Zostaniesz przekierowany na stronę logowania konsoli internetowej [NTSA_ SHORT]. Po wprowadzeniu danych logowania [NTSA_ SHORT] możesz rozpocząć nawigację w konsoli internetowej [NTSA_ SHORT].

   Wystarczy podać swoje dane uwierzytelniające [NTSA_ SHORT] za pierwszym razem. Następnie automatycznie uzyskasz dostęp do konsoli internetowej [NTSA_ SHORT], klikając przycisk **[NTSA_ SHORT]** , bez potrzeby logowana się .

Usuwanie integracji NTSA

Usunięcie klucza licencyjnego [NTSA_ SHORT] ze strony **Konfiguracja > Licencja** spowoduje również usunięcie integracji [NTSA_ SHORT].

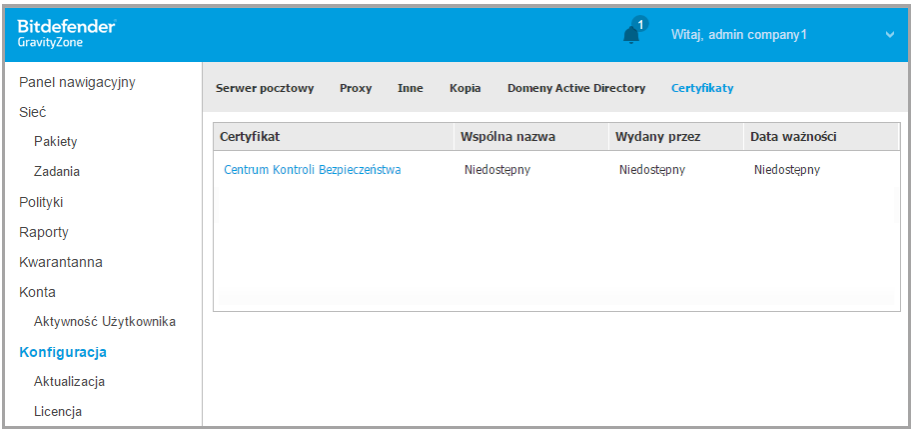
Notatka

Twoje konto [NTSA_ SHORT] i GravityZone będą odłączone w następujących sytuacjach:

- Klucz licencyjny [NTSA_ SHORT] został usunięty.
- Twoje hasło NTSA zostało zmienione.
- Twoje hasło GravityZone zostało zmienione.
- Integracja ustawień NTSA została zmodyfikowana.

Certyfikaty

Aby umożliwić GravityZone wdrożenie do prawidłowego działania i w bezpieczny sposób, musisz utworzyć i dodać certyfikat 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)

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**.

Repozytorium

Ta zakładka wyświetla informacje na temat aktualizacji agenta bezpieczeństwa razem z wersjami produktu przechowywanymi na Serwerze Aktualizacji i wersjami dostępnymi o oficjalnym repozytorium Bitdefender, pierścienie aktualizacji, data i czas ostatniej aktualizacji oraz data ostatniego sprawdzenia dostępności nowej wersji.

Notatka
Wersje produktu nie są dostępne dla Serwera Bezpieczeństwa.

5.1.5. Zarządzanie Urządzeniem GravityZone

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

Oto dostępne główne opcje po pierwszym wdrożeniu urządzenia GravityZone:

- Konfiguruj Ustawienia Nazwy Hosta
- Skonfiguruj ustawienia sieciowe
- Konfiguruj ustawienia proxy
- Serwer Komunikacji MDM
- Zaawansowane
- Konfiguruj język

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.** Uzyj 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
Konfiguracja jest wymagana tylko dla zarządzania urządzeniami mobilnymi jeśli twój klucz licencyjny pokrywa usługę Security for Mobile. Opcja pojawia się w menu po instalacji Roli Serwera Komunkiacji.

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.

Zaawansowane

Zaawansowane ustawienia obejmują kilka opcji ręcznego wdrażania, rozszerzenia środowiska i ulepszeń bezpieczeństwa:

- Role Instalowania/Odinstalowywania

- Zainstaluj Security Server
- Ustawiono Nowe Hasło do Bazy Danych
- Serwer aktual.
- Konfiguruj role balancerów
- Replica Set
- Włącz bezpieczny klaster VPN
- Połącz z Istniejącą Bazą Danych
- Połącz z istniejącą bazą danych (bezpieczny klaster VPN)
- Zaznacz Bezpieczny Klaster VPN

Dostępność opcji różni się w zależności od zainstalowanych ról i włączonych usług. Na przykład, jeśli rola Serwera Bazodanowego nie jest zainstalowana na urządzeniu, możesz zainstalować tylko role lub połączyć się z bazą danych GravityZone wdrożoną w sieci. Po zainstalowaniu roli Serwera Bazodanowego na urządzeniu opcje połączenia z inną bazą danych stają się niedostępne.

Role Instalowania/Odinstalowywania

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

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

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. 85).

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.

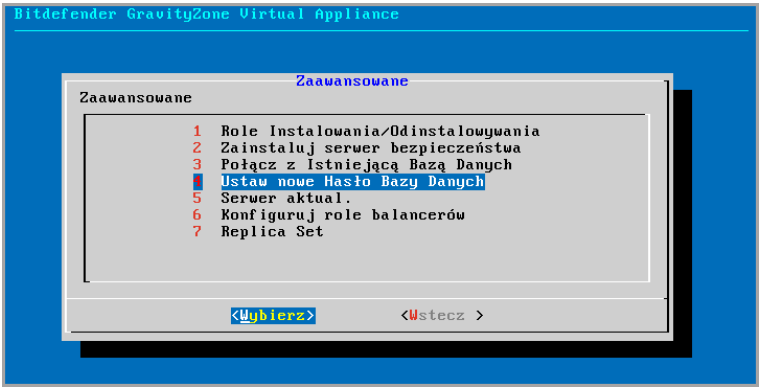
Aby zainstalować Security Server z interfejsu urządzenia:

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.

Ustawiono Nowe Hasło do Bazy Danych

Podczas instalowania roli Serwera Bazodanowego konieczne jest skonfigurowanie hasła w celu ochrony bazy danych. Jeśli chcesz to zmienić, ustaw nowy, uzyskując dostęp do **Ustawienia Zaawansowane > Ustaw nowe hasło do bazy danych** z głównego menu.



Interfejs konsoli urządzenia: Ustaw opcję Nowego Hasła Bazy Danych

Postępuj zgodnie z wytycznymi, aby ustawić silne hasło.

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 Incydentów, 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.

     WAŻNE
     To install multiple instances of the Incidents Server role you may only use the built-in balancer.
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 do uruchomienia co najmiej trzech członków.
- 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. 81).
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. 88).
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.

Włącz bezpieczny klaster VPN

Role GravityZone mają kilka wewnętrznych usług, które komunikują się wyłącznie między sobą. Dla bezpieczniejszego środowiska, możesz odizolować te usługi, tworząc dla nich klaster VPN. Zarówno usługi będące na tym samym urządzeniu lub na większej ich liczbie, będą komunikować się za pomocą bezpiecznego kanału.

WAŻNE

- Ta funkcja wymaga standardowego wdrożenia GravityZone bez zainstalowanych narzędzi niestandardowych.
- Po włączeniu klastra nie można go wyłączyć.

Aby zabezpieczyć usługi wewnętrzne w urządzeniach:

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

3. Wybierz Włącz **Bezpieczny Klaster VPN**.

   Wiadomość informuje o zmianach, które zostaną wprowadzone.

4. Wybierz **Tak**, aby potwierdzić i kontynuować instalację VPN.

   Po zakończeniu zostanie wyświetlony komunikat potwierdzający.

Odtąd wszystkie role na urządzeniu są instalowane w trybie bezpiecznym, a usługi będą komunikować się przez interfejs VPN. Każde nowe urządzenie dodane do środowiska musi dołączyć do klastra VPN. Aby uzyskać więcej informacji, odwołaj się do „Połącz z istniejącą bazą danych (bezpieczny klaster VPN)" (p. 89).

Połącz z Istniejącą Bazą Danych

W architekturze rozproszonej GravityZone musisz zainstalować rolę Serwera Bazodanowego na pierwszym urządzeniu, a następnie skonfigurować wszystkie inne urządzenia, aby łączyły się z istniejącą instancją bazy danych. W ten sposób wszystkie urządzenia będą korzystać z tej samej bazy danych.

WAŻNE
Zalecane jest włączenie bezpiecznego klastra VPN i połączenie się z bazą danych w takim klastrze. Aby uzyskać więcej informacji, odwołaj się do:

- „Włącz bezpieczny klaster VPN" (p. 87)
- „Połącz z istniejącą bazą danych (bezpieczny klaster VPN)" (p. 89)

Aby podłączyć urządzenie do bazy danych GravityZone poza Bezpiecznym Klastrem VPN:

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**.

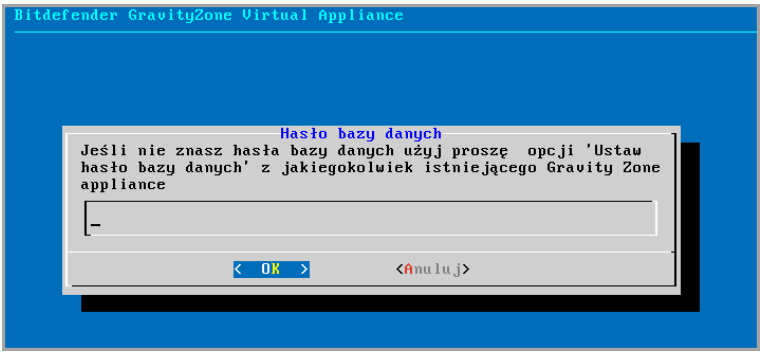
   Notatka
   Upewnij się, że ustawiłeś hasło bazy danych zanim uzyskasz dostęp do tych opcji. Jeśli nie znasz hasła bazy danych, skonfiguruj nowe, wybierając **Ustawienia Zaawansowane > Ustaw nowe hasło bazy danych** z menu głównego.

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.

Połącz z istniejącą bazą danych (bezpieczny klaster VPN)

Użyj tej opcji, jeśli chcesz rozszerzyć wdrożenie GravityZone o więcej urządzeń, a Bezpieczny Klaster VPN jest włączony. W ten sposób nowe urządzenie będzie dzielić tę samą bazę danych z istniejącym wdrożeniem w bezpiecznym trybie.

Po więcej informacji na temat Bezpiecznego Klastra VPN zajrzyj do „Włącz bezpieczny klaster VPN” (p. 87).

Warunki wstępne

Przed kontynuowaniem upewnij się, że masz pod ręką:

- Adres IP Serwera Bazodanowego
- Hasło dla użytkownika **bdadmin** na urządzeniu z rolą Serwera Bazodanowego.

Połącz z Bazą Danych

Aby podłączyć urządzenie do bazy danych GravityZone przez Bezpieczny Klaster VPN:

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 (Bezpieczny Klaster VPN)**.

   Zostaniesz poinformowany o wymaganiach i alternatywach, jeśli nie zostaną one spełnione.
4. Wybierz **OK**, aby potwierdzić i kontynuować.
5. Wprowadź adres IP Serwera Bazodanowego w ramach Bezpiecznego Klastra VPN.
6. Wprowadź hasło dla użytkownika **bdadmin** na urządzeniu z Serwerem Bazodanowym.
7. Wybierz **OK**, aby zapisać zmiany i kontynuować.

Po zakończeniu procesu otrzymasz komunikat potwierdzający. Nowe urządzenie staje się członkiem klastra i będzie komunikować się z innymi urządzeniami w bezpieczny sposób. Wszystkie urządzenia będą korzystać z tej samej bazy danych.

Sprawdź Status Bezpiecznego Klastra VPN

Ta opcja jest dostępna tylko po uprzednim włączeniu bezpiecznego klastra VPN. Wybierz tę opcję, aby sprawdzić, które urządzenia w Twoim wdrożeniu GravityZone nie mają jeszcze zabezpieczonych usług. Konieczne może być dalsze zbadanie i sprawdzenie, czy urządzenia są dostępne online.

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.

5.2. Zarządzanie Licencjami

Licencja GravityZone posiada jeden klucz licencyjny dla wszystkich usług bezpieczeństwa.

Poza podstawowymi usługami bezpieczeństwa, GravityZone zapewnia także ważne funkcje ochrony w postaci dodatków. Każdy dodatek jest licencjonowany oddzielnym kluczem i można go używać tylko razem z podstawową ważną licencją. Jeśli główna licencja jest nieważna, zobaczysz ustawienia funkcji, ale nie będziesz mógł ich użyć.

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

Aby kontynuować używanie GravityZone po wygaśnięciu wersji próbnej, musisz kupić klucz licencyjny do rejestracji produktu.

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

Klucz licencyjny GravityZone mogą być zarządzane na stronie **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 **Licencja**.

5.2.1. 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.

5.2.2. Wprowadzanie Twoich kluczy licencyjnych

Rejestracja licencji GravityZone może być przeprowadzona online lub offline (gdy połączenie internetowe nie jest możliwe). W obu przypadkach, potrzebujesz podać ważny klucz licencyjny.

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

Aby zmienić bieżący klucz licencyjny lub zarejestrować dodatek:

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.

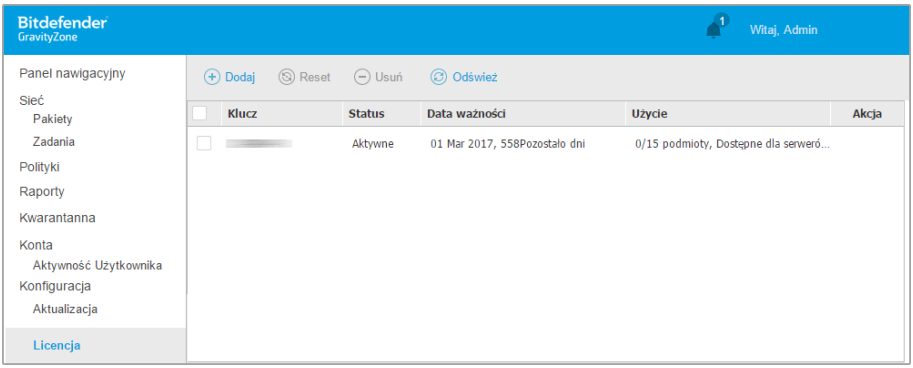
   Jeżeli klucz licencyjny nie jest ważny, zostanie wyświetlony błąd weryfikacji jako podpowiedź w polu **Klucz Licencyjny**.
5. Kliknij **Dodaj**. Klucz licencyjny zostanie dodany do strony **Licencja**, gdzie możesz wybrać jego szczegóły.
6. Naciśnij **Zapisz** aby zastosować zmiany. Control Center uruchamia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

Notatka
Możesz używać tych dodatków, o ile odpowiednia licencja podstawowa jest ważna. W przeciwnym razie zobaczysz funkcje, ale nie będziesz mógł ich użyć.

5.2.3. 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. W tabeli, możesz zobaczyć szczegóły klucza licencyjnego.
   - Klucz licencyjny
   - Status klucza licencji
   - 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

5.2.4. Resetowanie licznika zużycia licencji

Możesz znaleźć informacje o liczbie wykorzystania klucza licencyjnego na stronie **Licencja** w kolumnie **Wykorzystanie**.

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

5.3. 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. 8).

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 Windows jest ustawiony w czasie instalacji na język Twojego konta GravityZone.

W systemie Mac język wyświetlania interfejsu użytkownika jest ustawiony na czas instalacji w oparciu o język systemu końcowego punktu końcowego. W systemie Linux agent bezpieczeństwa nie ma zlokalizowanego interfejsu użytkownika.

Aby zainstalować interfejs użytkownika w innym języku na wybranych punktach końcowych Windows, możesz stworzyć pakiet instalacyjny i ustawić preferowany język w opcjach konfiguracyjnych. Ta opcja nie jest dostępna dla punktów końcowych Mac i Linux. Aby uzyskać więcej informacji o tworzeniu paczek instalacyjnych, odwołaj się do „Tworzenie pakietów instalacyjnych" (p. 97).

5.3.1. 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, 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 dowiedzieć się więcej i sprawdzić listę oprogramowania zabezpieczającego wykrytego przez Bitdefender Endpoint Security Tools dla bieżących systemów operacyjnych Windows, zobacz ten artykuł KB.

   WAŻNE
   Jeśli chcesz zainstalować agenta bezpieczeństwa na komputerze z programem Bitdefender Antivirus for Mac 5.X, musisz go najpierw usunąć ręcznie. Szczegółowe instrukcje można znaleźć w tym artykule KB.

3. Instalacja wymaga praw administracyjnych i dostępu do internetu. Jeśli docelowe punkty końcowe znajdują się w domenie Active Directory, należy użyć poświadczeń administratora domeny do zdalnej instalacji. W przeciwnym razie 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.
6. Podczas wdrażania agenta za pośrednictwem Relaya Linux muszą być spełnione następujące dodatkowe warunki:

   - Punkt końcowy Relay musi mieć zainstalowany pakiet Samba (`smbclient`) w wersji 4.1.0 lub nowszy i binarny/ wiersz poleceń `net` do wdrażania agentów Windows.

Notatka
Polecenie binarne/ `net` jest zwykle dostarczane razem z pakietami samba-client i/lub samba-common. W niektórych dystrybucjach Linuxa (takich jak CentOS 7.4) polecenie `net` jest instalowane tylko podczas instalowania pełnego pakietu Samba (Common + Client + Server) Upewnij się, że Twój punkt końcowy Relay ma dostępne polecenie `net`.

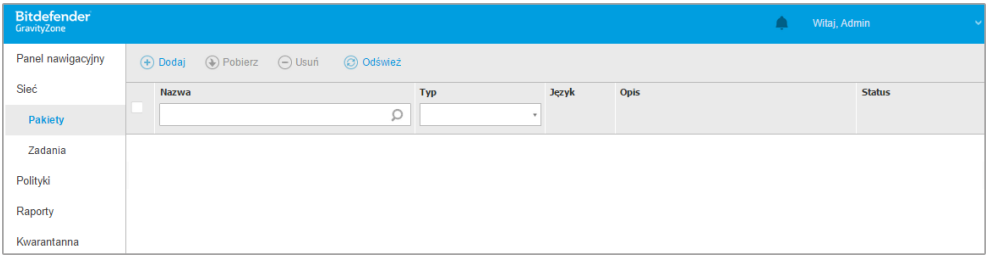
- Docelowe punkty końcowe Windows muszą mieć włączone Zasoby Administracyjne i udostępnianie Sieciowe.
- Docelowe punkty końcowe dla systemu Linux i Mac muszą mieć włączoną obsługę SSH.

7. Począwszy od macOS High Sierra (10.13), po zainstalowaniu Endpoint Security for Mac ręcznie lub zdalnie, użytkownicy są proszeni o zatwierdzenie rozszerzeń jądra Bitdefender na swoich komputerach. Dopóki użytkownicy nie zaakceptują rozszerzeń jądra Bitdefender, niektóre funkcje Endpoint Security for Mac nie będą działać. Aby wyeliminować interwencję użytkownika, możesz wstępnie zatwierdzić rozszerzenia jądra Bitdefender, dodając je do białej listy za pomocą narzędzia do zarządzania urządzeniami przenośnymi.

5.3.2. 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. 114).

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

1. Utwórz pakiet instalacyjny według swoich potrzeb.

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

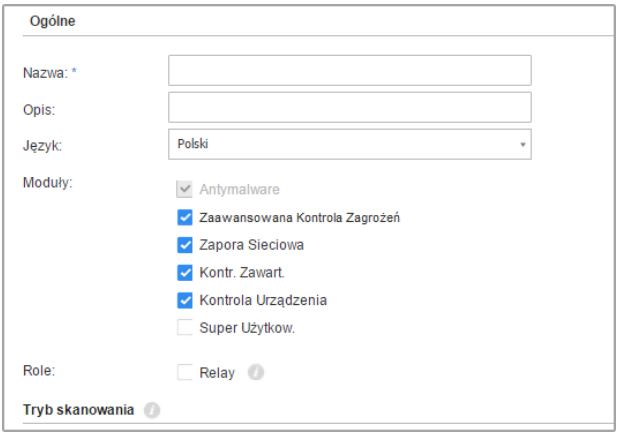
2. Pobierz pakiet instalacyjny na docelowy punkt końcowy.

   Alternatywnie możesz wysłać linki do pobrania pakietów instalacyjnych w wiadomości e-mail do kilku użytkowników sieci.
3. Uruchom pakiet instalacyjny na docelowym punkcie końcowym.

Tworzenie pakietów instalacyjnych

Aby utworzyć pakiet instalacyjny:

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



Tworzenie Paczek - Opcje

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

> **Notatka**
> Ta opcja jest dostępna tylko dla niektórych systemów operacyjnych Windows.

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 „Agenci Bezpieczeństwa” (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 „Relay” (p. 10)
   - **Serwer Buforujący Zarządzania Aktualizacjami**, aby serwer Relay był serwerem wewnętrznym dla aktualizacji oprogramowania. Ta rola jest wyświetlana, gdy wybrana jest rola Relay. Aby uzyskać więcej informacji, odwołaj się do „Serwerów Buforowania Łatek ” (p. 10)

8. **Usuń Konkurentów**. Zaleca się pozostawienie zaznaczenia tego pola wyboru, aby automatycznie usunąć niekompatybilne oprogramowanie zabezpieczające podczas gdy agent Bitdefender instaluje się na punkcie końcowym. Odznaczając tą opcję, agent Bitdefender agent zainstaluje się obok istniejącego rozwiązania bezpieczeństwa. Możesz ręcznie usunąć poprzednio zainstalowane rozwiązanie bezpieczeństwa później, na własne ryzyko.

   WAŻNE
   Uruchomienie agenta Bitdefender jednocześnie z innym oprogramowaniem zabezpieczającym na punkcie końcowym może wpływać na ich działanie i powodować poważne problemy z systemem.

9. **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:
     - Lokalne Skanowanie (z Pełnymi Silnikami) na fizycznych komputerach z wysokimi wymaganiami sprzętowymi.
     - Skanowanie lokalne dla instancji EC2 i maszyn wirtualnych Microsoft Azure.

     Notatka
     Komputery ze słabą wydajnością posiadające częstotliwość procesora niższą niż 1.5 Ghz, lub pamięć RAM niższą niż 1GB.

   - **Użytkownika**. W tym przypadku, można skonfigurować tryb skanowania, wybierając spośród kilku technologii skanowania dla maszyn fizycznych i wirtualnych:
     - Hybrydowe Skanowanie (z Lekkimi Silnikami)
     - Lokalne Skanowanie (z Pełnymi Silnikami)

     Domyślnym trybem skanowania dla instancji EC2 jest Skanowanie Lokalne (zawartość bezpieczeństwa jest przechowywana na zainstalowanym agencie zabezpieczeń, a skanowanie jest uruchamiane lokalnie na komputerze). Jeśli chcesz skanować instancje EC2 za pomocą Security Server, musisz

odpowiednio skonfigurować pakiet instalacyjny agenta bezpieczeństwa i zastosowane zasady.

Domyślnym trybem skanowania dla maszyn wirtualnych Microsoft Azure jest skanowanie lokalne (zawartość bezpieczeństwa jest przechowywana w zainstalowanym agencie bezpieczeństwa, a skanowanie jest uruchamiane lokalnie na komputerze). Jeśli chcesz skanować maszyny wirtualne Microsoft Azure za pomocą Security Server, musisz odpowiednio skonfigurować pakiet instalacyjny agenta bezpieczeństwa i zastosowane polityki.

Aby uzyskać więcej informacji na temat dostępnych technologii skanowania, zapoznaj się z „Silniki Skanowania" (p. 3)

10. **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.
11. 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.
12. Bitdefender Endpoint Security Tools jest zainstalowany w domyślnym katalogu instalacyjnym. Zaznacz **Użyj niestandardowej ścieżki instalacji** jeśli chcesz zainstalować agenta Bitdefender w innej lokacji. Jeżeli folder docelowy nie istnieje, zostanie stworzony podczas instalacji.

- Na Windows, domyślna ścieżka to `C:\Program Files\`. By zainstalować Bitdefender Endpoint Security Tools w niestandardowej lokacji użyj schematu Windows podczas wprowadzania ścieżki. Na przykład, `D:\folder`.
- Na systemach Linux, Bitdefender Endpoint Security Tools jest zainstalowany domyślnie w folderze `/opt`. By zainstalować agenta Bitdefender w niestandardowej lokacji użyj schematu Linux podczas wprowadzania ścieżki. Na przykład, `/folder`.

  Bitdefender Endpoint Security Tools nie wspiera instalacji w następujących niestandardowych ścieżkach:
  - Każda ścieżka, która nie rozpoczyna się slashem (/). Jedynym wyjątkiem jest lokacja Windows `%PROGRAMFILES%`, którą agent interpretuje jako domyślny folder Linux `/opt`.
  - Każda ścieżka, która jest w `/tmp` lub `/proc`.
  - Każda ścieżka, która zawiera następujące symbole specjalne: `$, !, *, ?, ", ', `, \, (,), [,], {, }`.
  - Specyfikator `systemd` (%)

  Na systemach Linux instalacja do niestandardowej ścieżki wymaga glibc 2.21 lub wyżej.

WAŻNE
Gdy używasz niestandardowej ścieżki, upewnij się, że masz odpowiedni pakiet instalacyjny dla każdego systemu operacyjnego.

13. Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.
14. 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.
15. 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. 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.

16. 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
  - **macOS:** tylko 64-bitowe systemy

  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.

6. Dodatkowo, jeśli wybrałeś Downloader, możesz stworzyć pakiet MSI dla punktów końcowych Windows. Więcej informacji, szukaj w artykule KB

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

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

1. Przejdź do strony **Sieć > Pakiety**.

2. Wybierz pakiety instalacyjne, które potrzebujesz.
3. Kliknij przycisk **Wyślij linki pobierania** z górnej strony tabeli. Wyświetlone zostanie okno konfiguracji.
4. Wpisz adres e-mail dla każdego użytkownika, który chce otrzymać link do pobrania pakietu instalacyjnego. Naciśnij `Enter` po każdym adresu e-mail.

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

Uruchamianie Pakietów Instalacyjnych

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

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

- Na systemach operacyjnych Windows i macOS:
  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.

  Notatka
  W systemie MacOS po zainstalowaniu Endpoint Security for Mac użytkownicy są proszeni o zatwierdzenie rozszerzeń jądra Bitdefender na swoich komputerach. Dopóki użytkownicy nie zaakceptują rozszerzeń jądra Bitdefender, niektóre funkcje agenta zabezpieczeń nie będą działać. Więcej szczegółów znajdziesz w tym artykule KB.

- 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.

WAŻNE
Jeśli korzystasz z VMware Horizon View Persona Management, zaleca się skonfigurowanie zasad grupy Active Directory w celu wykluczenia następujących procesów Bitdefender (bez pełnej ścieżki):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Wykluczenia te muszą obowiązywać, dopóki agent bezpieczeństwa działa na punkcie końcowym. Aby uzyskać szczegółowe informacje, zapoznaj się z tą stroną dokumentacji VMware Horizon.

5.3.3. 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 i Nutanix Prism Element, 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. 114).

Wymagania zdalnej instalacji

Aby zdalna instalacja działała:

- Dla Windows:
  - Udziały administracyjne `admin$` muszą być włączone. Skonfiguruj każdą docelową stacje roboczą do nie używania zaawansowanej wymiany plików.
  - Skonfiguruj Kontrolę Konta Użytkownika (UAC) w zależności od systemu operacyjnego uruchomionego na docelowych punktach końcowych. Jeśli punkty końcowe znajdują się w domenie Active Directory, można użyć zasad grupy do skonfigurowania Kontroli Konta Użytkownika. Więcej szczegółów znajdziesz w tym artykule KB.
  - Wyłącz Windows Firewall lub skonfiguruj ją tak, aby zezwalała na ruch przez protokół udostępniania plików i drukarek.

Notatka
Zdalne wdrażanie działa tylko w nowoczesnych systemach operacyjnych, zaczynając od Windows 7 / Windows Server 2008 R2, dla których Bitdefender zapewnia pełne wsparcie. Aby uzyskać więcej informacji, odwołaj się do „Wspierane systemy operacyjne" (p. 21).

- Na Linux: SSH musi być włączone.
- Na MacOS: zdalne logowanie i udostępnianie plików musi być włączone.

Uruchamianie Zadania Zdalnej Instalacji

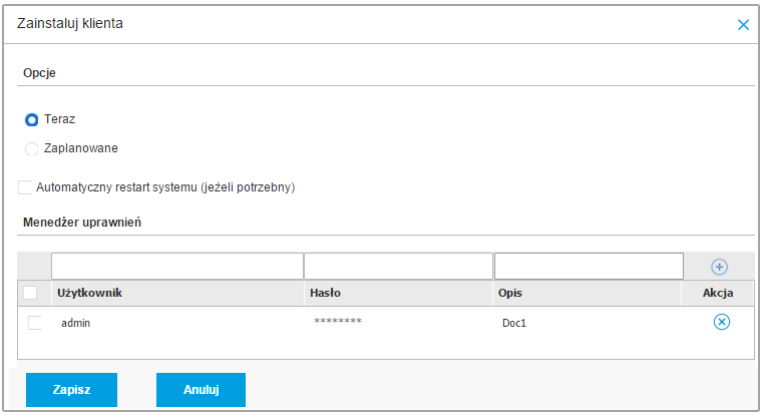
Aby uruchomić zdalną instalacje:

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.

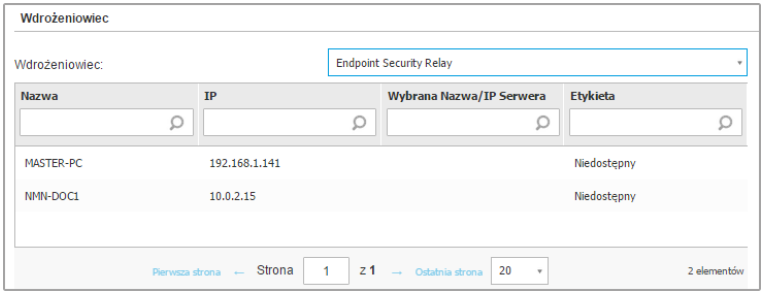
11. W sekcji **Wdrożeniowiec**, wybierz podmiot, do którego będzie podłączony docelowy punkt końcowy do instalacji i aktualizacji klienta:
    - **Urządzenie GravityZone**, gdy punkty końcowe łączą się bezpośrednio do Urządzenia GravityZone.

      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. 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. 97).

    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**.

WAŻNE

Jeśli korzystasz z VMware Horizon View Persona Management, zaleca się skonfigurowanie zasad grupy Active Directory w celu wykluczenia następujących procesów Bitdefender (bez pełnej ścieżki):

- `bdredline.exe`
- `epag.exe`
- `epconsole.exe`
- `epintegrationservice.exe`
- `epprotectedservice.exe`
- `epsecurityservice.exe`
- `epupdateservice.exe`
- `epupdateserver.exe`

Wykluczenia te muszą obowiązywać, dopóki agent bezpieczeństwa działa na punkcie końcowym. Aby uzyskać szczegółowe informacje, zapoznaj się z tą stroną dokumentacji VMware Horizon.

5.3.4. Przygotowywanie Systemów Linux do Skanowania Dostępowego

Wersja Bitdefender Endpoint Security Tools dla Linux zawiera możliwości skanowania dostępowego, które pracują z określoną dystrybucją Linux i wersjami jądra. Więcej informacji można znaleźć w wymaganiach systemu.

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/modules/dazukofs/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.

5.3.5. Jak działa wyszukiwanie sieci

Oprócz integracji z usługa Active Directory, GravityZone zawiera również mechanizm automatycznego wykrywania sieci, przeznaczony do wykrywania komputerów grupy roboczej.

GravityZone opiera się na usłudze **Microsoft Computer Browser** oraz narzędziu **NBTscan** aby wykryć urządzenie w 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

Narzędzie NBTscan skanuje sieci komputerowe korzystając z NetBIOS'a. Służy do sprawdzania każdego punktu końcowego w sieci i pobierania informacji, takich jak adres IP, nazwa komputera NetBIOS i adres MAC.

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

WAŻNE

Control Center nie wykorzystuje informacji sieciowych z Active Directory lub funkcji mapy sieci. 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 Relay jest zainstalowany na komputerze grupy roboczej, tylko komputery z grupy roboczej będą widoczne w Control Center.
- Jeżeli Relay 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 Relay.

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 Relay 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 Relay wyświetli błąd podczas wykonywania zapytania, Control Center poczeka do następnego zaplanowanego zapytania, aby spróbować ponownie, bez wybierania innego Relaya.

Dla pełnej widoczności sieci Relay 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.
- Jeśli korzystając z Relaya na Linuxie do wykrycia pozostałych punktów końcowych z systemem Mac lub Linux, musisz zainstalować Sambę na punktach końcowych lub dołączyć je poprzez Active Directory korzystając z DHCP. W ten sposób NetBIOS zostanie na nie automatycznie skonfigurowany.
- 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.
- Odnajdywanie Sieci musi być uruchomione (**Panel Sterownia > Centrum Sieci i Udostępniania > Zmień Zaawansowane Ustawienia udostępniania**).

  By uruchomić tę funkcję muszą być uruchomiony następujące 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.

5.4. Instalowanie Sandbox Analyzer On-Premises

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

1. Przygotowanie do Instalacji
2. Wdrożyć Urządzenie Wirtualne Sandbox Analyzer
3. Wdróż Urządzenie Wirtualne Ochrony Sieci

5.4.1. Przygotowanie do Instalacji

Przed instalacją Sandbox Analyzer On-Premises upewnij się że:

- Hiperwizor WMVare ESXi jest zainstalowany i skonfigurowany. Po szczegóły zajrzyj do dokumentacji vSphere Installation and Setup, sekcja 2: "Installing and Setting Up ESXi".
- Urządzenie wirtualne Bitdefender GravityZone jest wdrożone i skonfigurowane.

Notatka
Jeśli chodzi o hiperwizora VMWare ESXi, upewnij się że:

- ESXi w wersji 6.5 lub nowszej.
- Wersja magazynu danych VMFS to 5.
- SSH jest włączone w **Polityka uruchamiania** z konfiguracją **Uruchom i zatrzymaj wraz z hostem**
- Usługa NTP jest aktywna i skonfigurowana.

Klucz licencyjny Sandbox Analyzer On-Premises kontroluje liczbę maksymalnych równoczesnych detonacji. Ponieważ każda detonacja wymaga działającej instancji maszyny wirtualnej, liczba jednoczesnych detonacji odzwierciedla liczbę utworzonych maszyn wirtualnych. Po szczegółowe informacje na temat dodawania kluczy licencyjnych w GravityZone Control Center zajrzyj do „Wprowadzanie Twoich kluczy licencyjnych” (p. 92).

5.4.2. Wdrożyć Urządzenie Wirtualne Sandbox Analyzer

Aby wdrożyć Urządzenie Wirtualne Sandbox Analyzer:

1. Zaloguj się do Control Center GravityZone.
2. Przejdź do strony **Sieć > Pakiety**.
3. Zaznacz pole wyboru **Sandbox Analyzer** z tabeli.
4. Kliknij przycisk **Pobierz** w lewej górnej części strony. Wybierz opcję **Urządzenie zabezpieczające (samodzielny ESXi)**.
5. Użyj narzędzia do zarządzania wirtualizacją (na przykład vSphere Client), aby zaimportować pobrany plik OVA do środowiska wirtualnego.

   Notatka
   Podczas wdrażania pliku OVA skonfiguruj sieci w następujący sposób:

- **Sieć Bitdefender** - jest to sieć w której znajdują się komponenty innej Bitdefender (interfejs `eth0`). Sandbox Analyzer i urządzenie GravityZone muszą być w tej samej sieci i muszą komunikować się prze `eth0`
- **Prywatna Sieć Detonacji** - Sandbox Analyzer używa tej sieci do wewnętrznej komunikacji (interfejs `eth1`). Ta sieć musi być odizolowana od innych segmentów sieci.
- **Dostęp do Sieci Internet** - Sandbox Analyzer używa tej sieci do uzyskania najnowszych aktualizacji (interfejs `eth2`). Interfejs `eth2` nie powinien mieć takiego samego IP lub sieci jak `eth0`.

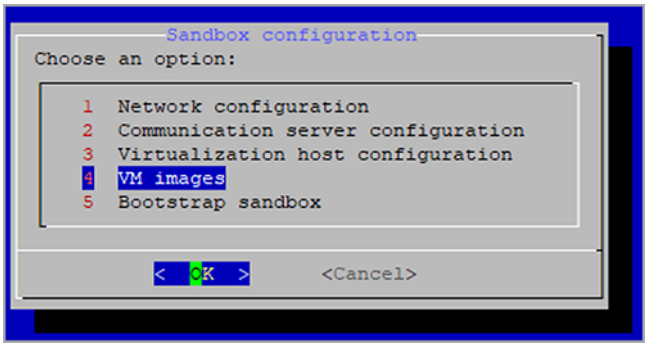
6. Zasilanie urządzenia.
7. Z narzędzia do zarządzania wirtualizacją uzyskaj dostęp do interfejsu konsoli Urządzenia Wirtualnego Sandbox Analyzer.
8. Po wyświetleniu monitu o podanie poświadczeń użyj `root` jako nazwę użytkownika i `sve` jako hasło.
9. Uzyskaj dostęp do menu konfiguracji, uruchamiając następujące polecenie:

```
/opt/bitdefender/bin/sandbox-setup
```

10. W menu **Konfiguracja Sandbox** wprowadź następujące ustawienia:
    a. **Konfiguracja sieci**. Wybierz tę opcję, aby skonfigurować zarządzanie NIC. Sandbox Analyzer będzie używał tego interfejsu sieci do komunikacji z GravityZone.

       Adres IP możne być określony ręcznie lub automatycznie przez DHCP.

       Notatka
       Jeżeli urządzenie GravityZone jest w innej sieci niż `eth0`, musisz dodać statyczną ścieżkę w **Konfiguracja Sieci >Bitdefender Network > Scieżki** aby Sandbox Analyzer mógł poprawnie funkcjonować.



Konsola urządzenia Analizator Sandbox

b. **Konfiguracja internet proxy**. Aby instalacja się powiodła, Sandbox Analyzer wymaga połączenia z internetem. W tym wypadku możesz skonfigurować Sandbox Analyzer, aby użyć serwera proxy, określając następujące szczegóły:
   - **Host** - Adres IP lub FQDN serwera proxy. Użyj następującej składni: `http://<IP/Hostname>:<Port>`.
   - **Użytkownik i hasło** - musisz wpisać hasło dwa razy.
   - **Domena** - w tym przypadku domena Active Directory.

c. **Konfiguracja serwera komunikacji**. Podaj adres IP lub nazwę hosta urządzenia, na którym działa rola Serwera Komunikacji.

   Użyj następującej składni: `http://<IP/Hostname>:<Port>`. Domyślny port `8443`.

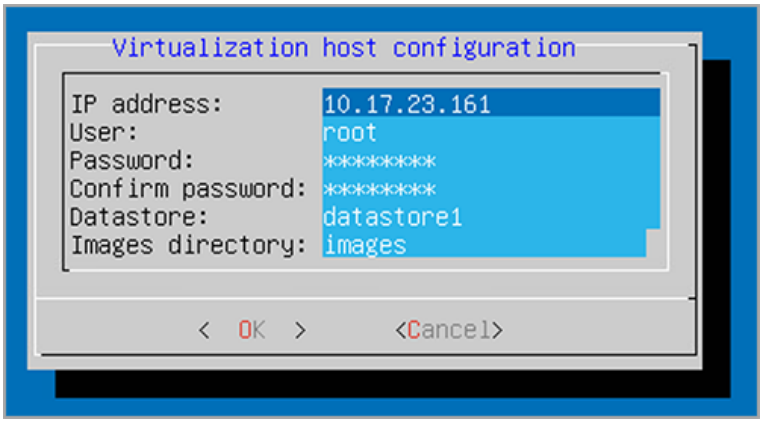
   Notatka
   Gdy tylko zostanie podany adres IP lub nazwa hosta, a konfiguracja zostanie zapisana, instancja Sandbox Analyzer będzie widoczna w Control Center GravityZone, na stronie **Sandbox Analyzer > Infrastruktura**.

d. **Konfiguracja zwirtualizowanego hosta**. Sandbox Analyzer używa serwera ESXi by udostępnić infrastrukturę analizy złośliwego oprogramowania. Używając **Konfiguracja zwirtualizowanego hosta**, łączysz urządzenie Sandbox Analyzer z hostem ESXi, podając następujące informacje:
   - Adres IP serwera ESXi.

- Poświadczenia root do uzyskania dostępu do hosta ESXi.
- Magazyn danych dedykowany dla Sandbox Analyzer.

  Wpisz nazwę magazynu danych wyświetlaną przez ESXi.
- Nazwa folderu używanego w magazynie danych do przechowywania obrazów maszyn wirtualnych.

  Jeśli ten folder nie istnieje, musisz go utworzyć w magazynie danych przed zapisaniem konfiguracji Sandbox Analyzer.



Konsola urządzenia Sandbox Analyzer

e. **Obrazy VM**. Aby zbudować wirtualne maszyny detonacyjne dla Sandbox Analyzer, musisz skopiować pliki VMDK zawierające żądane obrazy do folderu **Obrazy** określonego w **Konfiguracja zwirtualizowanego hosta**. Dla każdego obrazu możesz wykonać w menu **Obrazy VM** następujące ustawienia:

   i. W menu **Konfiguracja obrazu** określ nazwę obrazu (jaka będzie wyświetlana w Control Center GravityZone) i w systemie operacyjnym.

   > **Notatka**
   > Folder zawierający obrazy maszyn wirtualnych jest okresowo skanowany, a nowe wpisy są zgłaszane do GravityZone. Te wpisy są widoczne w Control Center, na stronie **Analizator Sandbox > Infrastruktura > Zarządzanie obrazem**.

W niektórych sytuacjach podczas korzystania z Sandbox Analyzer, możesz napotkać problemy z wirtualnymi maszynami detonacyjnymi. Aby rozwiązać te problemy, musisz wyłączyć opcję ochrony przed odciskami palców. Szczegółowe informacje znajdują się w „Techniki ochrony przed odciskami palców” (p. 122).

ii. W menu **Hosty DMZ** możesz dodać do białej listy nazwy hostów wymagane przez usługi i komponenty innych firm wbudowane w maszyny wirtualne do komunikacji z Sandbox Menedżerem. Po szczegóły zajrzyj do „Hosty DMZ” (p. 123)

iii. W menu **Czyszczenie** możesz usunąć niepotrzebne już obrazy VM.

f. **Bootstrap sandbox**. Po dodaniu szczegółów konfiguracyjnych Sandbox Analyzer kontynuuj instalację, wybierając tę opcję. Status instalacji będzie odzwierciedlony w Control Center GravityZone na stronie **Analizator Sandbox > Infrastruktura**.

Techniki ochrony przed odciskami palców

Domyślnie podczas procesu tworzenia obrazu, Analizator Sandbox włączy różne techniki zabezpieczające przed odciskami palców. Niektóre rodzaje malware są w stanie ustalić, czy działają same w środowisku sandbox, a jeśli tak, nie aktywują złośliwych procedur.

Techniki zapobiegające pobieraniu odcisków palców mają na celu symulację różnych warunków w celu naśladowania środowiska rzeczywistego. Z powodu wirtualnie wyeliminowanej kombinacji wdrożonego oprogramowania i konfiguracji środowiska, kombinacji, której nie można przewidzieć ani kontrolować, możliwe jest, że niektóre techniki nie będą kompatybilne z oprogramowaniem zainstalowanym na złotym obrazie. Takie rzadkie sytuacje można rozpoznać po następujących objawach:

- Błędy podczas procesu tworzenia obrazu.
- Błędy podczas próby uruchomienia oprogramowania wewnątrz obrazu.
- Komunikaty o niepowodzeniu zwracane podczas detonacji próbek.
- Licencjonowane oprogramowanie nie działa dłużej z powodu nieprawidłowych kluczy licencyjnych.

Szybki sposób na takie rzadkie zdarzenia polega na odbudowaniu obrazu przy wyłączonych technikach ochrony przed odciskami palców. Aby to zrobić, wykonaj następujące czynności:

1. Zaloguj się do Control Center GravityZone i usuń obraz.
2. Zaloguj się do urządzenia Sandbox Analyzer i uruchom konsolę urządzenia Sandbox Analyzer, uruchamiając następujące polecenie:

```
/opt/bitdefender/bin/sandbox-setup
```

3. Przejdź do **Obrazy VM > Konfiguracja Obrazu**.
4. Wybierz obraz, który powoduje problemy.
5. Przejdź do opcji **Anti-fingerprinting**.
6. Usuń zaznaczenie odpowiedniego pola wyboru, aby wyłączyć techniki anti-fingerprinting.

Hosty DMZ

Podczas procesu tworzenia obrazu zostanie utworzona wirtualna infrastruktura, aby ułatwić komunikację między Menedżerem Sandbox, a maszynami wirtualnymi. Z perspektywy sieci przekłada się to na izolowane środowisko sieciowe, które będzie zawierało całą potencjalną komunikację, jaką mogłaby stworzyć zdetonowana próbka.

Menu serwerów DMZ pozwala na umieszczenie na białej liście nazw hostów, z którymi muszą się komunikować usługi i komponenty innych firm osadzone w maszynach wirtualnych, aby działać poprawnie.

Przykładem takiej sytuacji mogą być serwery licencyjne KMS używane przez licencjonowanie systemu Windows, jeśli na dostarczonych maszynach wirtualnych zostanie zastosowana licencja zbiorowa.

5.5. Instalacja Pełnego Szyfrowania Dysku

Pełne Szyfrowanie Dysku GravityZone jest usługą, która wymaga aktywacji na podstawie klucza licencyjnego. Aby to zrobić, przejdź do **Konfiguracja > Licencja** i wprowadź klucz licencyjny.

Aby uzyskać więcej informacji o kluczu licencyjnym, przejdź do „Zarządzanie Licencjami” (p. 91).

Agenci bezpieczeństwa Bitdefender obsługują Pełne Szyfrowanie Dysku, zaczynając od wersji Windows 6.2.22.916 i Mac 4.0.0173876. Masz dwie opcje, aby upewnić się, że agenci są kompatybilni z tym modułem:

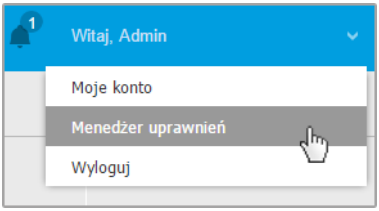
- Zainstaluj agentów bezpieczeństwa za pomocą dołączonego modułu Szyfrowania.
- Uruchom zadanie **Rekonfiguruj**.

Aby uzyskać szczegółowe informacje na temat korzystania z Pełnego Szyfrowania Dysku, zapoznaj się z rozdziałem **Polityki Bezpieczeństwa > Szyfrowanie** w Przewodniku Administratora GravityZone.

5.6. Manager 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

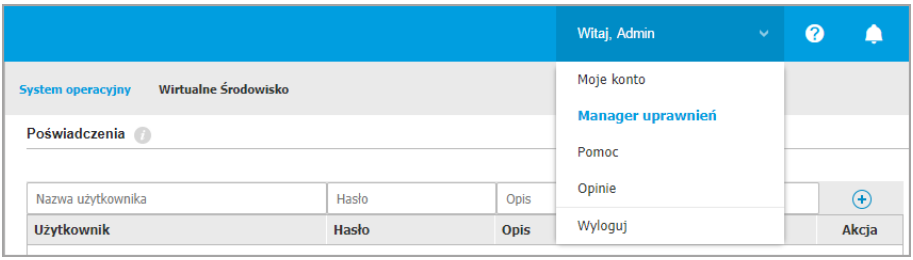
Okno **Menadżer poświadczeń** zawiera dwie zakładki:

- System Operacyjny
- Wirtualne środowisko

5.6.1. 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:



Manager 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.

5.6.2. Wirtualne środowisko

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

Aby mieć dostęp do zwirtualizowanej infrastruktury 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.

5.6.3. 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.

6. AKTUALIZOWANIE GRAVITYZONE

Bitdefender publikuje wszystkie aktualizacje produktów i treści zabezpieczeń za pośrednictwem serwerów 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,serwer lub agent ochrony GravityZonea sprawdza cyfrowe sygnatury aktualizacji pod kątem autentyczności i integralności 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**.

6.1. Aktualizacja urządzeń GravityZone

Dzięki aktualizacjom urządzeń GravityZone, Bitdefender wydaje nowe funkcje i ulepszenia już istniejących. Są one widoczne w Control Center.

Przed uruchomieniem aktualizacji zaleca się sprawdzenie następujących elementów:

- Status aktualizacji
- Wszelkie informacje lub komunikaty ostrzegawcze, które mogą się pojawić.
- Dziennik Zmian

Aby sprawdzić stan aktualizacji:

1. Przejdź na stronę **Konfiguracja > Aktualizuj > Role GravityZone**.

2. W sekcji **Bieżący Stan** przejrzyj wiadomość wskazującą ogólny stan wdrożenia. Jeśli GravityZone wymaga aktualizacji, przycisk **Aktualizuj** stanie się dostępny.
3. W sekcji **Infrastruktura** sprawdź szczegóły każdej roli GravityZone wdrożonej w Twojej sieci. Ponieważ role aktualizują się niezależnie, dla każdej roli można wyświetlić: nazwę urządzenia, które go obsługuje, jego adres IP, aktualną wersję, najnowszą dostępną wersję i stan aktualizacji.

Aby sprawdzić dziennik zmian:

1. Przejdź na stronę **Konfiguracja > Aktualizuj > Role GravityZone**.
2. Kliknij link **Wyświetl dziennik zmian** . Wyskakujące okienko wyświetla listę wszystkich dostępnych wersji i zmian.

   Informacje o Wydaniu dla każdej nowej wersji produktu, również publikowanej na Bitdefender Centrum Wsparcia.

Możesz zaktualizować GravityZone na dwa sposoby:

- Ręcznie
- Automatycznie

6.1.1. Ręczne Aktualizacje

Wybierz tę metodę, jeśli chcesz mieć pełną kontrolę nad tym, kiedy aktualizacja powinna zostać uruchomiona.

Aby ręcznie zaktualizować GravityZone:

1. Przejdź na stronę **Konfiguracja > Aktualizuj > Role GravityZone**.
2. Kliknij przycisk **Aktualizuj** (jeśli jest dostępny).

   Aktualizacja może zająć chwile. Poczekaj, aż się zakończy.
3. Wyczyść pamięć podręczną przeglądarki.

Podczas aktualizacji, Control Center wylogowuje wszystkich użytkowników i informuje ich o aktualizacji w toku. Będziesz mógł zobaczyć szczegółowy postęp procesu aktualizacji.

Po zakończeniu aktualizacji, Control Center wyświetla stronę logowania.

6.1.2. Automatyczna aktualizacja

Instalując aktualizacje automatycznie, masz pewność, że GravityZone jest zawsze aktualizowany o najnowsze funkcje i poprawki zabezpieczeń.

GravityZone ma dwa typy automatycznych aktualizacji:

- Aktualizacje produktów
- Aktualizacje oprogramowania firm trzecich

Aktualizacje produktów

Te aktualizacje wprowadzają nowe funkcje w GravityZone i rozwiązują problemy wynikające z tych funkcji.

Ponieważ aktualizacje są uciążliwe dla użytkowników GravityZone, są one zaprojektowane do uruchamiania zgodnie z harmonogramem. Możesz przełożyć aktualizację na dogodną dla Ciebie godzinę. Automatyczna aktualizacja produktu jest wyłączona domyślnie.

Aby włączyć i przełożyć aktualizacje produktu:

1. Przejdź do strony **Konfiguracja > Aktualizuj > Role GravityZone**.
2. Zaznacz pole wyboru **Włącz automatyczne aktualizacje produktu GravityZone** .
3. Ustaw **Powtarzalność** na **Codziennie**, **Tygodniowy** (zaznacz jeden lub więcej dni tygodnia) or **Miesięczna**.
4. Zdefiniuj **Interwał**. Można zaplanować czas procesu aktualizacji, aby rozpocząć, gdy nowa aktualizacja jest dostępna.

GravityZone wyświetla domyślnie komunikat ostrzegawczy dla wszystkich użytkowników Control Center 30 minut przed rozpoczęciem automatycznej aktualizacji. Aby wyłączyć ostrzeżenie, usuń zaznaczenie pola wyboru **Włącz 30 minutowy alert o przestoju przed aktualizacją** .

Aktualizacje Oprogramowania Firm Trzecich

GravityZone urządzenie wirtualne osadza serię oprogramowania dostarczanego przez innych dostawców. Tego typu aktualizacje mają na celu jak najszybsze załatanie takiego oprogramowania, co zmniejsza ryzyko związane z bezpieczeństwem.

Aktualizacje są uruchamiane bezgłośnie i nie przerywają pracy z Control Center.

Domyślnie ta opcja jest włączona. Aby wyłączyć tę opcję:

1. Przejdź do strony **Konfiguracja > Aktualizuj > Role GravityZone**.

2. Usuń zaznaczenie pola wyboru **Włącz automatyczne aktualizacje zabezpieczeń dla komponentów GravityZone firm trzecich** .

   Poprawki oprogramowania firm trzecich zostaną wydane z aktualizacją produktu GravityZone.

6.2. 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.
   - **Częstotliwość 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 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**.

6.3. 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.

6.4. Aktualizacje Produktu Offline

GravityZone wykorzystuje domyślnie system aktualizacji podłączony do Internetu. W przypadku sieci izolowanych Bitdefender oferuje alternatywę, udostępniając komponenty i aktualizacje zawartości zabezpieczeń również w trybie offline.

6.4.1. Warunki wstępne

Aby użyć aktualizacji offline, potrzebujesz:

- Instancja GravityZone zainstalowana w sieci z dostępem do Internetu ("instancja online"). Instancja online musi mieć:

  - Bezpośredni dostęp do internetu
  - Dostęp na portach 80 i 443. Aby uzyskać więcej informacji na temat portów używanych przez GravityZone, zapoznaj się z tym artykułem KB.
  - Tylko zainstalowane role Bazy Danych i Serwera Aktualizacji
- Jedna lub kilka instancji GravityZone zainstalowanych w sieci bez dostępu do Internetu ("instancje offline")
- Obie instancje GravityZone muszą mieć tę samą wersję urządzenia

6.4.2. Ustawianie Instancji Online GravityZone

Podczas tej fazy użytkownik wdroży instancję GravityZone w sieci z dostępem do Internetu, a następnie skonfiguruje ją do działania jako serwer aktualizacji offline.

1. Wdróż GravityZone na maszynie z połączeniem internetowym.
2. Zainstaluj tylko role Bazy Danych oraz Serwera Aktualizacji.
3. Uzyskaj dostęp do terminalu TTY urządzenia w swoim środowisku wirtualnym (lub połącz się z nim przez SSH).
4. Zaloguj się za pomocą użytkownika `bdadmin` i ustawionego hasła.
5. Uruchom komendę `sudo su` aby uzyskać uprawnienia **roota**
6. Uruchom następujące polecenia, aby zainstalować pakiet offline `gzou-mirror`:

```
# apt update # gzcli update # apt install gzou-mirror
```

`gzou-mirror` ma następujące role:

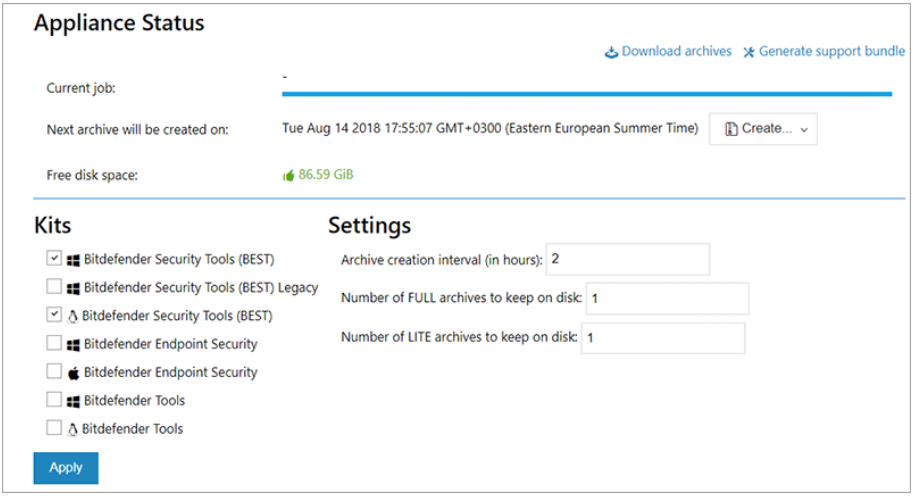
- Skonfiguruj serwer aktualizacji, aby automatycznie generował archiwa aktualizacji offline.
- Skonfiguruj usługę internetową do instancji online, zapewniając opcje konfiguracji i pobierania dla archiwów aktualizacji offline.

6.4.3. Konfigurowanie i pobieranie wstępnych plików aktualizacji

Podczas tej fazy skonfigurujesz ustawienia archiwizacji aktualizacji za pośrednictwem usługi internetowej zainstalowanej w instancji online, a następnie utworzysz pliki archiwum wymagane dla konfigurowania instancji offline. Następnie

musisz pobrać pliki aktualizacji i umieścić je na przenośnym urządzeniu multimedialnym (pamięci USB).

1. Uzyskaj dostęp do usługi internetowej za pomocą adresu URL w tym formularzu: `https://Online-Instance-Update-Server-IP-or-Hostname`, z nazwą użytkownika `bdadmin` i ustawionym hasłem.



Instancja online - Serwis Web

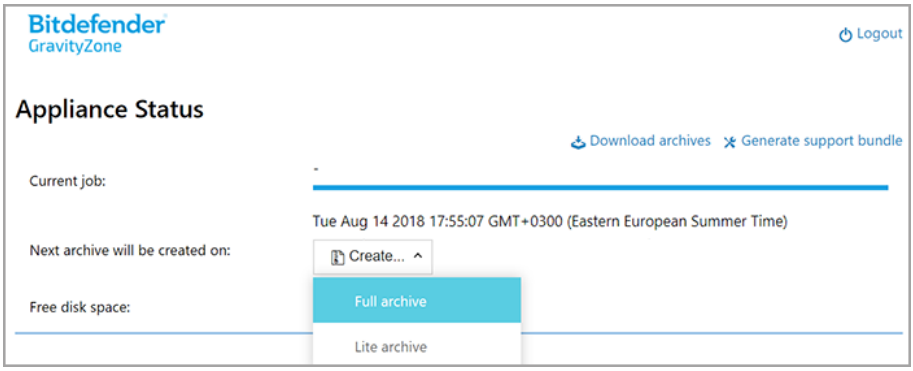
2. Skonfiguruj archiwum aktualizacji offline w następujący sposób:
   - W **Zestawach**: wybierz zestawy agentów końcowych, które chcesz uwzględnić w archiwum aktualizacji offline.
   - W obszarze **Ustawienia** edytuj preferencje archiwum aktualizacji.

     Zadanie CRON zainstalowane w instancji online sprawdza co minutę, czy dostępne są nowe pliki aktualizacji i czy wolne miejsce na dysku jest większe niż 10 GB. W każdym okresie ustawionym przez opcję **Utwórz przedział tworzenia archiwów (w godzinach)**, zadanie CRON utworzy następujące pliki:
     - **Pełne archiwum (produkt + zawartość zabezpieczenia)** , gdy dostępne są nowe pliki aktualizacji
     - **Archiwum Lite** (tylko zawartość zabezpieczenia), gdy nie ma nowych plików aktualizacji

Archiwa zostaną utworzone w następującej lokalizacji:

`https://Online-Instance-Update-Server-IP-or-Hostname/snapshots`

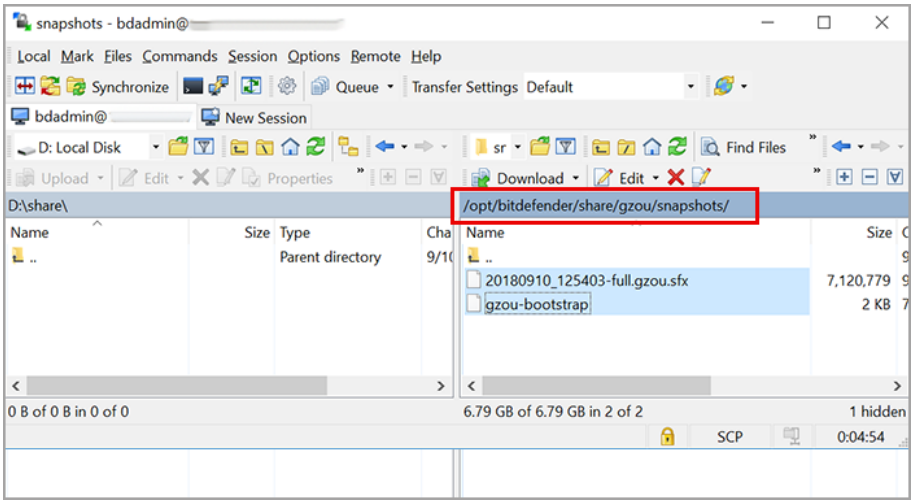
3. Kliknij **Utwórz > Pełne** archiwum, aby utworzyć pierwsze pełne archiwum. Zaczekaj, aż archiwum zostanie utworzone.



Instancja online - Usługa internetowa: Tworzenie archiwum

4. Pobierz pełne archiwum aktualizacji i plik `gzou-bootstrap` z instancji online. Masz do dyspozycji kilka opcji:
   - Za pomocą usługi internetowej: kliknij **Pobierz archiwa**, aby uzyskać dostęp do strony zawierającej linki do plików aktualizacji. Kliknij pełne archiwum aktualizacji i linki do plików `gzou-bootstrap`, aby pobrać je na swój punkt końcowy.
   - Użyj preferowanego klienta SCP/SCTP (na przykład WinSCP), aby ustanowić sesję SCP z instancją online i przenieść wyżej wymienione pliki do dowolnego miejsca w sieci online. Domyślna ścieżka do instancji online to:

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



Przesyłanie plików aktualizacji za pomocą SCP

- Za pośrednictwem udziału SAMBA. Użyj udziału SAMBA tylko do odczytu, aby pobrać archiwa aktualizacji offline z następującej lokalizacji:

  `\\Online-Instance-Update-Server-IP-or-Hostname\gzou-snapshots`

  Notatka
  Poświadczenia dostępu do udziału SAMBA, jeśli są wymagane, są identyczne z poświadczeniami instancji online (użytkownik i hasło `bdadmin`).

6.4.4. Ustawianie Instancji Offline GravityZone

Podczas tego kroku wdrożysz i skonfigurujesz instancję trybu offline, aby otrzymywać aktualizacje za pośrednictwem archiwum wygenerowanego przez instancję online. Chyba, że jest ustalone inaczej, wszystkie komendy muszą być uruchamiane jako **root**

1. Wdróż GravityZone na maszynie z odizolowanego środowiska.
2. Zainstaluj tylko role Bazy Danych oraz Serwera Aktualizacji.

3. Przenieś archiwum aktualizacji i plik `gzou-bootstrap` pobrany z instancji online do katalogu `/home/bdadmin` z instancji offline przy użyciu przenośnego urządzenia medialnego (pamięci USB).

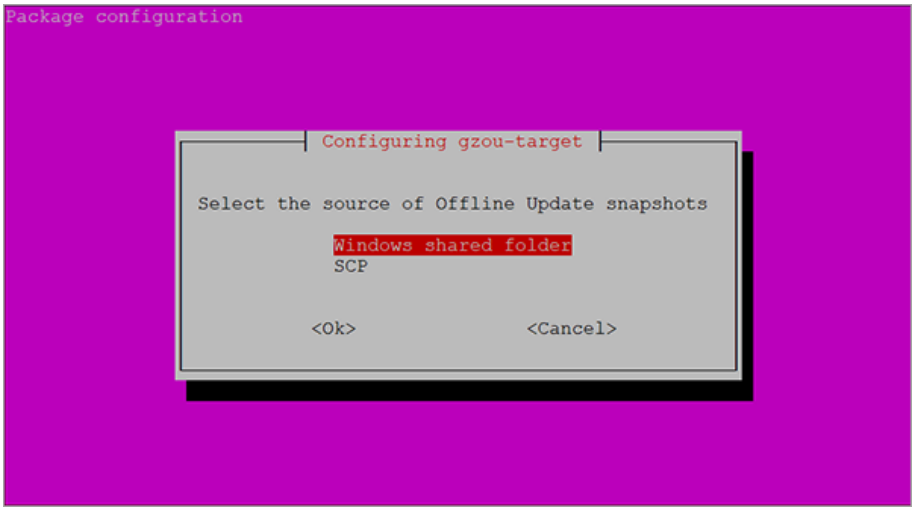
   WAŻNE
   Aby aktualizacja offline działała, upewnij się, że:
   - Archiwum aktualizacji i `gzou-bootstrap` znajdują się w tym samym folderze.
   - Archiwum aktualizacji jest **pełnym** archiwum.

4. Wykonaj plik `gzou-bootstrap` w następujący sposób:
   a. Uzyskaj dostęp do terminalu TTY urządzenia w swoim środowisku wirtualnym (lub połącz się z nim przez SSH).
   b. Przekształcenie `gzou- bootstrap` do pliku wykonywalnego:

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

   c. Uruchom: `./gzou-bootstrap`

5. Wybierz metodę przesyłania archiwów aktualizacji do instancji offline:
   - Wybierz **Folder współdzielony Windows** (udział Samby). W takim przypadku będziesz musiał określić ścieżkę do udziału Windows z izolowanej sieci, gdzie instancja offline automatycznie połączy się, aby pobrać archiwa aktualizacji. Wprowadź poświadczenia wymagane do uzyskania dostępu do określonej lokalizacji.
   - Wybierz SCP, jeśli ręcznie przeniesiesz pliki do folderu `/opt/bitdefender/share/gzou/snapshot/` instancji offline przez SCP.



Instancja Offline GravityZone - Konfigurowanie trybu przesyłania plików aktualizacji

Notatka
Jeśli chcesz zmienić metodę przesyłania w późniejszym czasie:

a. Uzyskaj dostęp do terminalu TTY instancji offline w swoim środowisku wirtualnym (lub połącz się z nim przez SSH).
b. Zaloguj się za pomocą użytkownika `bdadmin` i ustawionego hasła.
c. Uruchom komendę `sudo su` aby uzyskać uprawnienia roota
d. Uruchom:

```
# rm -f /opt/bitdefender/etc/gzou-target.json # dpkg-recon
```

Pojawi się okno dialogowe konfiguracji, w którym możesz wprowadzić żądane zmiany.

6. Przejdź do wiersza poleceń konsoli trybu offline GravityZone i zainstaluj pozostałe role.
7. Wejdź do konsoli offline przez twoją przeglądarkę i wprowadź klucz licencyjny(w trybie offline).

6.4.5. Korzystając z Aktualizacji Offline

Po skonfigurowaniu instancji GravityZone wykonaj następujące kroki, aby zaktualizować instalację offline:

1. Pobierz najnowsze archiwum aktualizacji offline z instancji online do preferowanego udziału sieciowego. Aby uzyskać więcej informacji, odwołaj się do „Konfigurowanie i pobieranie wstępnych plików aktualizacji" (p. 132).
2. Użyj pamięci USB, aby przenieść archiwum aktualizacji do skonfigurowanego udziału Samby z odizolowanej sieci. Aby uzyskać więcej informacji, odwołaj się do „Ustawianie Instancji Offline GravityZone" (p. 135).

   Pliki zostaną automatycznie przeniesione do następującego katalogu instancji offline:

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

6.4.6. 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 zawartości bezpieczeństwa**
- **Utwórz Pełne Archiwum**

W sekcji **Utworzone Archiwa** można pobrać zawartość zabezpieczeń 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 interwał tworzenia archiwów, a także liczbę archiwów do przechowywania na dysku.
4. Kliknij przycisk **Zastosuj**, aby zapisać zmiany.

7. 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 Ról Serwera GravityZone

7.1. Odinstalowywanie Ochrony Endpoint

Masz dwie opcje na odinstalowanie agentów bezpieczeństwa:

- Zdalnie w Control Center
- Manualnie na maszynie docelowej

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 Agentów Bezpieczeństwa" (p. 93).

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 Agentów Bezpieczeństwa" (p. 93).

7.2. Odinstalowywanie Sandbox Analyzer On-Premises

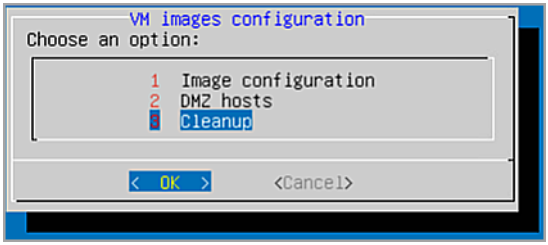
Aby odinstalować Sandbox Analyzer On-Premises:

1. Usuń obrazy maszyny wirtualnej (VM) z konsoli urządzenia Sandbox Analyzer.
   a. Zaloguj się do interfejsu urządzenia Sandbox Analyzer.

      Użyj klawiszy strzałek i przycisku `Tab` do nawigacji w menu i opcjach.

      Naciśnij `Enter`, aby wybrać konkretną opcję.

   b. W menu **Konfiguracja Sandbox**, przejdź do opcji **Obrazy VM**.
   c. W menu **Konfiguracja obrazów VM**, przejdź do opcji **Czyszczenie**.



Konsola urządzenia Sandbox Analyzer - Konfiguracja Sandbox - Czyszczenie

   d. Potwierdź, że chcesz usunąć zainstalowane obrazy maszyny wirtualnej.

      Poczekaj na zakończenie tej akcji. Podczas tej akcji dane powiązane z obrazami maszyny wirtualnej również zostaną usunięte.

2. Usuń Urządzenie Wirtualne Sandbox Analyzer:
   a. Wyłącz Urządzenie Wirtualne Sandbox Analyzer.
   b. Usuń urządzenie z inwentarza ESXi.

7.3. Odinstalowywanie Ról GravityZone Virtual Appliance

Możesz odinstalować role urządzenia wirtualnego GravityZone za pomocą interfejsu opartego na menu. 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. 81).

8. UZYSKIWANIE 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.

8.1. 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 znalezienia 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.

Najłatwiejszy sposób aby dostać się do dokumentacji jest poprzez stronę w Control Center **Pomoc & Wsparcie**. Kliknij swoją nazwę użytkownika w prawym górnym rogu konsoli, wybierz **Pomoc & Wsparcie**, a następnie link przewodnika, którym jesteś zainteresowany. Podręcznik zostanie otwarty w nowej karcie przeglądarki.

Dokumentację można też sprawdzić i pobrać w Centrum Pomocy w sekcji **Dokumentacja** dostępnej na każdej stronie pomocy technicznej.

8.2. Prośba o pomoc

Możesz poprosić o pomoc za pośrednictwem naszego Centrum Wsparcia Online. Wypełnij formularz kontaktowy i wyślij go do nas.

8.3. 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.

8.3.1. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Windows

Uruchamianie aplikacji Support Tool

Aby wygenerować dziennik na zagrożonym komputerze, użyj jednej z następujących metod:

- Wiersz poleceń

  Dla problemów z BEST, zainstalowanego na komputerze.

- Problem z instalacją

  Dla sytuacji gdzie BEST nie jest zainstalowany na komputerze i instalacja kończy się niepowodzeniem.

Metoda wiersza poleceń

Używając wiersza poleceń możesz zbierać logi bezpośrednio z zainfekowanego komputera. Metoda ta przydaje się w sytuacjach gdy nie masz dostępu do Centrum Kontroli GravityZone lub komputer nie komunikuje się z konsolą.

1. Otwórz wiersz polecenia z uprawnieniami administratora.
2. Przejdź do folderu instalacji produktu. Domyślna ścieżka to:

   ```
   C:\Program Files\Bitdefender\Endpoint Security
   ```

3. Zbieraj i zapisuj logi, uruchamiając to polecenie:

   ```
   Product.Support.Tool.exe collect
   ```

   Dzienniki są domyślnie zapisywane w `C:\Windows\Temp`.

   Opcjonalnie, jeśli chcesz zapisać dziennik Support Tool w niestandardowej lokalizacji, użyj ścieżki opcji:

```
Product.Support.Tool.exe collect [path="<path-to-file>"]
```

Przykład:

```
Product.Support.Tool.exe collect path="D:\Test"
```

Podczas wykonywania polecenia można zauważyć na ekranie pasek postępu. Po zakończeniu procesu dane wyjściowe wyświetlają nazwę archiwum zawierającego dzienniki i ich lokalizację.

By wysłać logi do Biznesowej Pomocy Bitdefender przejdź do `C:\Windows\Temp` lub do niestandardowej lokacji i znajdź archiwum o nazwie `ST_[computername]_[currentdate]`. Załącz archiwum do zgłoszenia do pomocy technicznej w celu dalszego rozwiązywania problemów.

Problem z instalacją

1. By pobrać BEST Support Tool kliknij tutaj.
2. Uruchom plik wykonywalny jako administrator. Zostanie wyświetlone okno.
3. Wybierz lokację by zapisać archiwum logów.

   Podczas zbierania logów zauważysz pasek postępu na ekranie. Po zakończeniu procesu dane wyjściowe wyświetlają nazwę archiwum i ich lokalizację.

By wysłać logi do Biznesowej Pomocy Bitdefender przejdź do wybranej lokacji i znajdź archiwum o nazwie `ST_[computername]_[currentdate]`. Załącz archiwum do zgłoszenia do pomocy technicznej w celu dalszego rozwiązywania problemów.

8.3.2. 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 utworzyć:
  - Archiwum zawierające logi produktu i modułu komunikacyjnego dostarczone do folderu `/tmp` w następującym formacie: `bitdefender_machineName_timeStamp.tar.gz`.

    Po utworzeniu archiwum:

    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).

Możesz także uruchomić polecenie `/bdconfigure` bezpośrednio z pakietu BEST (pełny lub downloader) bez zainstalowanego produktu.

Aby zaraportować zdarzenie GravityZone dotyczące twojego systemu Linux, przejdź do kolejnego kroku, wykorzystując wcześniej 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 `/tmpvar/log/BitDefender/bdinstall.log` zawierający informacje dotyczące instalacji
- Plik `network.txt`, zawierający ustawienia sieci / informacje połączenia maszyny
- Plik `product.txt`, zawierający zawartość wszystkich plików `update.txt` z `/opt/BitDefender/var/lib/scan` i rekursywna pełna lista wszystkich plików z `/opt/BitDefender`
- 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

8.3.3. 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. Weź plik **BDProfiler.tool** z archiwum.
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**) na pulpicie.

8.4. Informacje o produkcie

Skuteczna komunikacja jest kluczem do udanej współpracy. Przez ostatnie 18 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.

8.4.1. Adresy Internetowe

Dział sprzedaży: enterprisesales@bitdefender.com
Centrum pomocy:http://bitdefender.pl/dla-biznesu/uzyteczne-linki/wsparcie-techniczne
Dokumentacja: gravityzone-docs@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

Strona: http://www.bitdefender.com

8.4.2. 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.

8.4.3. 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

Bitdefender
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: b2b@bitdefender.fr
Strona internetowa: http://www.bitdefender.fr
Centrum pomocy: http://www.bitdefender.fr/support/business.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 internetowa: http://www.bitdefender.es
Centrum pomocy: http://www.bitdefender.es/support/business.html

Niemcy

Bitdefender GmbH
Technologiezentrum Schwerte
Lohbachstrasse 12
D-58239 Schwerte
Deutschland
Telefon (biuro i sprzedaż): +49 (0) 2304 94 51 60
Telefon (pomoc techniczna): +49 (0) 2304 99 93 004
Sprzedaż: firmenkunden@bitdefender.de
Strona internetowa: 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 internetowa: http://www.bitdefender.co.uk

Centrum pomocy: http://www.bitdefender.co.uk/support/business.html

Rumunia

BITDEFENDER SRL
Orhideea Towers
15A Orhideelor Street
060071 Bucharest, Sector 6
Faks: +40 21 2641799
Telefon (sprzedaż&pomoc techniczna): +40 21 2063470
Sprzedaż: sales@bitdefender.ro
Strona internetowa: 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
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

A.2. Obiekty Sandbox Analyzer

A.2.1. Obsługiwane Typy Plików i Rozszerzenia do Wysyłania Ręcznego

Obsługiwane są następujące rozszerzenia plików i można je ręcznie zdetonować w Sandbox Analyzer:

Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files (executable), PDF, PEF (executable), PIF (executable), RTF, SCR, URL (binary), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Sandbox Analyzer jest w stanie wykryć wyżej wymienione typy plików, także jeśli są one zawarte w archiwach następujących typów: 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, skompresowane archiwum LZMA, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ .

A.2.2. Typy Plików Obsługiwane przez Filtrowanie Zawartości podczas Automatycznego Wysyłania

Wstępne filtrowanie zawartości określi konkretny typ pliku za pomocą kombinacji, która implikuje treść i rozszerzenie obiektu. Oznacza to, że plik wykonywalny z rozszerzeniem .tmp zostanie rozpoznany jako aplikacja i jeśli okaże się podejrzany, zostanie wysłany do Sandbox Analyzer.

- Aplikacje - pliki o formacie PE32, w tym między innymi następujące rozszerzenia: exe, dll, com .
- Dokumenty - pliki o formacie dokumentu, w tym między innymi następujące rozszerzenia: xlsx, xls, ppt, doc, docx, dot, chm, xlm, docm

, Dotm, potm, potx, ppam, ppax, pps, ppsm, pptx, sldm, sldx, xlam, xlm, xltm, rtf, pdf .

- Skrypty: ps, wsf, ws, php, py, js, vb, vbs, pyc, pyo, wsc, wsh, psc1, jse, vbe.
- Archiwa: zip, jar, 7z, bz, bz2, tgz , msi, rar, rev, z, arj, iso, lha, lhz, uu, uue, xxe, lzma, ace, r00.
- E-maile (zapisane w systemie plików): eml, tnef .

A.2.3. Domyślne Wykluczenia przy Automatycznym Wysyłaniu

asc, avi, bmp, gif, jpeg, jpg, mkv, mp4, pgp, png, txt.

A.2.4. Zalecane Aplikacje dla Detonacyjnych VM

Sandbox Analyzer On-Premises wymaga pewnych aplikacji, aby były zainstalowane na detonacyjnych maszynach wirtualnych, aby mogły otwierać przesłane próbki.

Aplikacje	Typy plików
Pakiet Microsoft Office	xls, xltm, xltx, ppt, doc, dotx, docm, potm, potx, ppam, ppax, pps, ppsm, ppsx
Adobe Flash Player	swf
Adobe Acrobat Reader	pdf
Domyślny system Windows	bat, cmd, ws, wsf, reg, exe, dll, lnk, com, chm, application, gadget, hta, cpl, msc, vbe, jse, wsc, wsh, psc1, scf, vb, vbs, pif
7zip WinZip WinRAR	7z, zip, z, arj, bz, bz2, tgz, jar, r00, ace, lzma, xxe, uue
Google Chrome Internet Explorer	html, url
Python	py, pyc, pyp
Mozilla Thunderbird Microsoft Outlook	eml