

Bitdefender®

GravityZone

INSTRUKCJA INSTALACJI

Bitdefender GravityZone Instrukcja Instalacji

Data publikacji 2019.08.22

Copyright© 2019 Bitdefender

Uwagi prawne

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 Bitdefender. Umieszczenie krótkich cytatów w recenzjach może być dopuszczalne tylko z powołaniem się na cytowane źródło. Zawartość nie może być w żaden sposób modyfikowana.

Ostrzeżenie i zrzeczenie się odpowiedzialności. Ten produkt i jego dokumentacja są chronione prawami autorskimi. Informacja w tym dokumencie została dostarczona w stanie „w jakim jest” i bez żadnych dodatkowych gwarancji. Dołożyliśmy wszelkich starań w przygotowanie tego dokumentu, jednak autorzy nie ponoszą żadnej odpowiedzialności w stosunku do żadnych osób lub jednostek, w przypadku szkód lub strat spowodowanych lub stwierdzenia, że wynikły one bezpośrednio lub pośrednio z powodu informacji zawartych w tej pracy.

Dokument zawiera odnośniki do stron internetowych, które nie są pod kontrolą firmy Bitdefender. Firma Bitdefender nie odpowiada za zawartość serwisów zewnętrznych. Jeśli odwiedzasz zewnętrzną stronę internetową, wymienioną w tej instrukcji - robisz to na własne ryzyko. Firma Bitdefender umieszcza te odnośniki tylko dla wygody użytkownika, a umieszczenie takiego odnośnika nie pociąga za sobą żadnej odpowiedzialności firmy Bitdefender za zawartość zewnętrznych stron internetowych.

Znaki handlowe. W tym dokumencie mogą występować nazwy i znaki handlowe. Wszystkie zarejestrowane i niezarejestrowane znaki handlowe w tym dokumencie są własnością ich poszczególnych właścicieli, i tak powinny być traktowane.

Spis treści

Wstęp	v
1. Znaki umowne stosowane w przewodniku	v
1. O GravityZone	1
2. GravityZone Warstwy Ochronne	2
2.1. Antymalware	2
2.2. Zaawansowana Kontrola Zagrożeń	3
2.3. Zaawansowany Anti-Exploit	4
2.4. Zapora Sieciowa	4
2.5. Kontr. Zawart.	4
2.6. Zarządzanie Aktualizacjami	4
2.7. Kontrola Urządzenia	5
2.8. Pełne Szyfrowanie Dysku	5
2.9. Zarządzanie Ryzykiem Punktu Końcowego (ERA)	5
2.10. GravityZone Dostępność Warstw Ochrony	6
3. Architektura GravityZone	7
3.1. Konsola Web (GravityZone Control Center)	7
3.2. Agenci Bezpieczeństwa	7
3.2.1. Bitdefender Endpoint Security Tools	7
3.2.2. Bitdefender Endpoint Security Tools for Windows Legacy	10
3.2.3. Endpoint Security for Mac	10
4. Wymagania	12
4.1. Control Center	12
4.2. Ochrona Punktu Końcowego	12
4.2.1. Sprzęt komputerowy	13
4.2.2. Wspierane systemy operacyjne	16
4.2.3. Obsługiwane systemy plików	22
4.2.4. Obsługiwane przeglądarki	22
4.2.5. Wykorzystanie Ruchu	22
4.3. Pełne Szyfrowanie Dysku	24
4.4. Porty Komunikacji GravityZone	26
5. Instalowanie Ochrony	27
5.1. Zarządzanie Licencjami	27
5.1.1. Szukanie sprzedawcy	27
5.1.2. Aktywowanie Licencji	28
5.1.3. Sprawdzanie szczegółów aktualnej licencji	28
5.2. Instalowanie Agentów Bezpieczeństwa	29
5.2.1. Przygotowywanie do Instalacji	30
5.2.2. Instalacja lokalna	32
5.2.3. Instalacja Zdalna	40
5.2.4. Przygotowywanie Systemów Linux do Skanowania Dostępnego	45
5.2.5. Jak działa wyszukiwanie sieci	48
5.3. Instalacja Pełnego Szyfrowania Dysku	51

5.4. Manager uprawnień	52
5.4.1. Dodaj Poświadczenia to Menadżera Poświadczeń	52
5.4.2. Usuwanie Poświadczeń z Menadżera Poświadczeń	53
6. Integracje	54
6.1. Integracja z Amazon EC2	54
7. Odinstalowywanie Ochrony Endpoint	55
8. Otrzymywanie pomocy	57
8.1. Bitdefender Wsparcie Techniczne	57
8.2. Prośba o pomoc	58
8.3. Używanie Narzędzi Pomocy	59
8.3.1. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Windows	59
8.3.2. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Linux	61
8.3.3. Korzystając z Narzędzia Wsparcia na Systemach Operacyjnych Mac	62
8.4. Informacje o produkcie	63
8.4.1. Adresy Internetowe	63
8.4.2. Lokalni Dystrybutorzy	64
8.4.3. Biura Bitdefender	64
A. Aneksy	67
A.1. Wspierane Typy Plików	67

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.

Te dokumenty służą pomocą przy wdrożeniu agentów ochrony Bitdefender na wszystkich rodzajach punktów końcowych w zarządzanej firmie, oraz jak skonfigurować rozwiązanie GravityZone.

1. Znaki umowne stosowane w przewodniku

Konwencje Typograficzne

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

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

Uwagi

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



Notatka

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



WAŻNE

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



Ostrzeżenie

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

1. O GRAVITYZONE

GravityZone jest biznesowym rozwiązaniem bezpieczeństwa zaprojektowanym od podstaw z myślą o wirtualizacji i chmurze by dostarczać usługę ochrony dla fizycznych punktów końcowych i maszyn wirtualnych opartych na prywatnej 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 Anti-Exploit
- Zapora Sieciowa
- Kontr. Zawart.
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne Szyfrowanie Dysku
- Zarządzanie Ryzykiem Punktu Końcowego (ERA)

2.1. Antymalware

Warstwa ochrony antymalware opiera się na skanowaniu sygnatur i analizie heurystycznej (B-HAVE, ATC) przeciwko: wirusom, robakom, trojanom, programom szpiegującym, reklamowym, keyloggerom, rootkitom i innym typom 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 spośród 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 Lekкими 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 podejrzone 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 podejrzone

zachowanie podnosi rating procesu. Gdy próg zostanie osiągnięty, wyzwalany jest alarm.

2.3. Zaawansowany Anti-Exploit

Zaawansowana technologia Anti-Exploit, oparta na uczeniu maszynowym, jest proaktywną technologią, która powstrzymuje ataki zerowe przeprowadzane przez nieuchwytny exploit. 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. Kontr. Zawart.

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

2.6. 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.

2.7. Kontrola Urządzenia

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

2.8. 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.

2.9. Zarządzanie Ryzykiem Punktu Końcowego (ERA)

Zarządzanie Ryzykiem Punktów Końcowych (ERA) identyfikuje, ocenia i naprawia słabości punktów końcowych systemu Windows poprzez skanowanie ryzyka bezpieczeństwa (na żądanie lub zaplanowane za pomocą polityki), biorąc pod uwagę ogromną liczbę lub wskaźniki ryzyka. Po zeskanowaniu sieci przy użyciu pewnych wskaźników ryzyka, uzyskasz przegląd stanu ryzyka sieciowego za pomocą pulpitu nawigacyjnego **Zarządzanie ryzykiem**, dostępnego w menu głównym. Będziesz mógł automatycznie rozwiązać pewne zagrożenia bezpieczeństwa z GravityZone Control Center i zobaczyć zalecenia dotyczące łagodzenia narażeń punktu końcowego

2.10. 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 [GravityZone Dostępność Warstw Ochrony](#).

3. ARCHITEKTURA GRAVITYZONE

Rozwiązanie GravityZone zawiera następujące składniki:

- [Konsola Webowa \(Control Center\)](#)
- [Agenci Bezpieczeństwa](#)

3.1. 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 odpowiedzieć na potrzeby nawet największych organizacji.

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

3.2. Agenci Bezpieczeństwa

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

- [Bitdefender Endpoint Security Tools](#)
- [Bitdefender Endpoint Security Tools for Windows Legacy](#)
- [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. Oddzielny zestaw instaluje się w starszych wersjach systemu Windows. Aby uzyskać szczegółowe informacje, przejdź do [\[BEST_SHORT_LEGACY\]](#).

Warstwy bezpieczeństwa

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

- Antymalware
- Zaawansowana Kontrola Zagrożeń
- Zapora Sieciowa
- Kontr. Zawart.
- Zarządzanie Aktualizacjami
- Kontrola Urządzenia
- Pełne Szyfrowanie Dysku
- Zarządzanie Ryzykiem Punktu Końcowego (ERA)

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. 16).

Relay

Agenci Endpoint z rolą Bitdefender Endpoint Security Tools Relay służą 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 dużymi rozproszonymi sieciami, agenci relay pomagają obniżyć wykorzystanie pasma, zapobiegając bezpośredniemu połączeniu chronionych punktów końcowych z GravityZone.

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

Agenci Bitdefender Endpoint Security Tools Relay służą do następujących czynności:

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

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. Bitdefender Endpoint Security Tools for Windows Legacy

Wraz z rozwojem technologii bezpieczeństwa, niektóre funkcje w Bitdefender Endpoint Security Tools nie są już obsługiwane w starszych wersjach systemu Windows. [BEST LEGACY] to osobny zestaw przeznaczony do ochrony tych wersji systemu Windows, bez dokonywania szkody dla bezpieczeństwa obecnych.

Bitdefender Endpoint Security Tools for Windows Legacy nie może zostać zdalnie wdrożony z konsoli GravityZone. Administratorzy muszą zainstalować pakiet BEST for Windows Legacy ręcznie lub przy użyciu narzędzia innej firmy, takiego jak Microsoft SCCM.

Warstwy bezpieczeństwa

Następujące moduły powłok zabezpieczających dostępne są z [BEST LEGACY]:

- [Antymalware](#)
- [Zaawansowana Kontrola Zagrożeń](#)



WAŻNE

Zaawansowana Kontrola Zagrożeń nie jest dostępna w systemie Windows Server 2003.

Role Punktów Końcowych

- [Ochrona Exchange](#)

Power User i role Relay nie są dostępne w [BEST_ SHORT_ LEGACY].

3.2.3. 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](#)
- [Kontr. Zawart.](#)
- [Kontrola Urządzenia](#)

- [Pełne Szyfrowanie Dysku](#)

4. WYMAGANIA

Wszystkie rozwiązania GravityZone są instalowane i zarządzane przez Control Center.

4.1. 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



Ostrzeżenie

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

4.2. 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. 7).

4.2.1. Sprzęt komputerowy

Agent bezpieczeństwa bez ról

Użycie procesora

Docelowe systemy	Typ procesora	Wspierane systemy operacyjne (OS)
Stacje robocze	Procesory kompatybilne z Intel® Pentium, 1 Ghz bądź szybsze	Microsoft Windows XP SP3 32-bitowy i Windows XP SP2 64-bit
	Procesory kompatybilne z Intel® Pentium, 2 GHz bądź szybsze	Systemy operacyjne Microsoft Windows dla komputerów stacjonarnych, oprócz Windows XP
	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	

12

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

OS	POJEDYNCZY SILNIK					
	Skan. Lokalne		Skan. Hybrydowe		Scentraliz. Skan.	
	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje	Tylko AV	Pełne Opcje
macOS	1024	1024	n/d	n/d	n/d	n/d

Do codziennego użycia (MB)*

OS	Antywirus (Poj. Silnik)			Moduły Ochrony				
	Lokalny	Hybryda	Scentraliz.	Skanowanie Behaw.	Zapora Sieciowa	Kontrola Zaw.	Power User	Serwer Aktual.
Windows	75	55	30	+13	+17	+41	+29	+80
Linux	200	180	90	-	-	-	-	-
macOS	300	-	-	-	-	-	-	-

* 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	1300	1450	800	950	300	450	1300	1450	800	950
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	Hybryda	Scentraliz.	Skanowanie Behav.	Zapora Sieciowa	Kontrola Zaw.	Power User	Serwer Aktual.
Windows	410	190	140	+12	+5	+60	+80	+10
Linux	500	200	110	-	-	-	-	-
macOS	1024	-	-	-	-	-	-	-

* 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

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 roli).
- 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.

4.2.2. Wspierane systemy operacyjne

system Windows w wersji na komputery stacjonarne

Pełne Wsparcie

- 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

Ograniczone Wsparcie

W tych systemach operacyjnych agent bezpieczeństwa ma tylko narzędzie Antimalware i Advanced Threat Control. Power User i Relay nie są obsługiwane.

- Windows Vista z dodatkiem Service Pack 1
- Windows XP z dodatkiem Service Pack 2 (64 bit).
- Windows XP z dodatkiem Service Pack 3 (32 bity)



Ostrzeżenie

Bitdefender nie obsługuje Windows Insider Program builds.

Windows Tablet and Embedded

Pełne Wsparcie

- 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

Ograniczone Wsparcie

W tych systemach operacyjnych agent bezpieczeństwa obsługuje tylko narzędzie Antimalware i Advanced Threat Control. Power User i Relay nie są obsługiwane.

- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP z wbudowanym Service Pack 2⁽¹⁾
- Windows XP Tablet PC Edition⁽¹⁾



Ostrzeżenie

(1) Te specyficzne wbudowane komponenty systemów operacyjnych muszą być zainstalowane:

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

Windows Serwer

Pełne Wsparcie

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

Ograniczone Wsparcie

W tych systemach operacyjnych agent bezpieczeństwa obsługuje tylko narzędzie Antimalware i Advanced Threat Control. Power User i Relay nie są obsługiwane. Windows Serwer 2008 i Windows Small Business Serwer (SBS) 2008 także wspierają Ochronę Exchange

- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows Small Business Server (SBS) 2008

- Windows Small Business Server (SBS) 2003
- Windows Home Server

**WAŻNE**

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

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 wyższej
- 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

**Ostrzeżenie**

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

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

Wymagania Active Directory

Podczas integrowania punktów końcowych Linuxa z domeną Active Directory za pośrednictwem demona System Security Services (SSSD), upewnij się, że zainstalowane jest narzędzie **ldbsearch**.

Wsparcie skanowania Dostępowego

Skanowanie dostępne jest dostępne dla wszystkich gościnnych systemów operacyjnych. Na systemach Linux, skanowanie dostępne 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 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	Opcja jądra fanotify musi być włączona.
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 prekompilowanymi modułami jądra.
Wszystkie inne jądra	Wszystkie inne obsługiwane systemy plików	Moduł DazukoFS musi zostać skompilowany ręcznie. Aby uzyskać więcej informacji, odwołaj się do „ Ręcznie skompiluj moduł DazukoFS. ” (p. 46).

* Z pewnymi ograniczeniami opisanymi poniżej.

Ograniczenia Skanowania Dostępowego

Wersje Jądra	Dystrybucje Linux	Szczegóły
2.6.38 lub wyższe	Wszystkie wspierane systemy	<p>Monitory skanowania dostępowego montowały udziały sieciowe tylko w tych warunkach:</p> <ul style="list-style-type: none"> ● Fanotify jest włączone zarówno w systemach zdalnych, jak i lokalnych. ● Udział jest oparty na systemach plików CIFS i NFS. <p>Notatka Skanowanie dostępowe nie skanuje udziałów sieciowych podłączonych za pomocą SSH lub FTP.</p>
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.



Notatka

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

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

macOS

- macOS Mojave (10.14.x)
- macOS High Sierra (10.13.x)
- macOS Sierra (10.12.x)
- OS X El Capitan (10.11.x)
- OS X Yosemite (10.10.5)
- OS X Mavericks (10.9.5)

**Notatka**

System OS X Mountain Lion (10.8.5) nie jest już obsługiwany, ale istniejące instalacje będą nadal otrzymywać aktualizacje zawartości zabezpieczeń.

4.2.3. 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.

4.2.4. 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+

4.2.5. Wykorzystanie Ruchu

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

Każda okresowa 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

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

Typ Serwera Aktualizacji	Typ Silnika Skanowania		
	Lokalny	Hybryda	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**	P i e r w s z e skanowanie	Ruch sieciowy	621	Niedostępny
		Security Server	54	1050
	S k a n o w a n i e buforowane	Ruch sieciowy	654	Niedostępny
		Security Server	0.2	0.5

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

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

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

Przeskanowane Obiekty	Typ Ruchu	Pobrano (MB)	Przesłano (MB)
Pliki*	Pierwsze skanowanie	1.7	0.6
	Skanowanie buforowane	0.6	0.3
Ruch sieciowy**	Ruch sieciowy	650	Niedostępny

Przeskanowane Obiekty	Typ Ruchu	Pobrano (MB)	Przesłano (MB)
	Usługi w Chmurze Bitdefender	2.6	2.7

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

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



Notatka

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

- **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 webową Control Center**

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

4.3. 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 poleceń 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](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](https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx)

Dla Mac

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

- macOS Mojave (10.14)
- macOS High Sierra (10.13)
- macOS Sierra (10.12)
- OS X El Capitan (10.11)
- OS X Yosemite (10.10)
- OS X Mavericks (10.9)

**Notatka**

Możesz zainstalować agenta Bitdefender na Mac OS X Mountain Lion (10.8), ale moduł Szyfrowania pozostanie niedostępny.

4.4. 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

Aby chronić Twoją sieć z Bitdefender, musisz zainstalować agenty bezpieczeństwa GravityZone na punktach końcowych. W tym celu potrzebny jest użytkownik GravityZone Control Center z uprawnieniami administratora w punktach końcowych zarządzanych przez Ciebie.

5.1. Zarządzanie Licencjami

GravityZone jest licencjonowany z jednym kluczem dla wszystkich usług bezpieczeństwa, z wyjątkiem Pełnego Szyfrowania Dysku, do którego dołączony jest oddzielny klucz.

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

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

Twoja subskrypcja jest zarządzana przez Bitdefender lub przez partnera Bitdefender który sprzedaje ci usługę. Niektórzy partnerzy Bitdefender są dostawcami usług bezpieczeństwa. W zależności od ustaleń subskrypcyjnych, GravityZone operacje dzień w dzień mogą być obsługiwane zarówno wewnętrznie lub przez firmę zewnętrzną przez dostawcę usług bezpieczeństwa.

5.1.1. Szukanie sprzedawcy

Nasi sprzedawcy prześlą 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.

5.1.2. Aktywowanie Licencji

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



Ostrzeżenie

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

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

1. Zaloguj się do Control Center korzystając ze swojego konta.
2. Kliknij swoją nazwę użytkownika w górnym prawym rogu konsoli i wybierz **Moja Firma**.
3. Sprawdź szczegóły obecnej licencji w sekcji **Licencja**.
4. W sekcji **Licencja**, wybierz typ **Licencja**.
5. W polu **Klucz licencyjny** podaj klucz licencyjny.
6. Naciśnij przycisk **Sprawdź** i poczekaj zanim Control Center prześle informacje o wpisanym kluczu licencyjnym.
7. W polu **Dodatkowy klucz**, wpisz klucz konkretnego dodatku (np. Szyfrowanie).
8. Kliknij **Dodaj**. Szczegóły dodatku pojawią się w tabeli: typ, klucz licencyjny i opcja usunięcia klucza.
9. Kliknij **Zapisz**.
10. Aby używać dodatku, wyloguj się z Control Center, a następnie zaloguj się ponownie. To sprawi, że funkcje dodatku będą widoczne w GravityZone.

5.1.3. Sprawdzanie szczegółów aktualnej licencji

zobacz szczegóły twojej licencji:

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

5.2. Instalowanie Agentów Bezpieczeństwa

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

Aby dowiedzieć się więcej o dostępnych agentach bezpieczeństwa, przejdź do „[Agenci Bezpieczeństwa](#)” (p. 7).

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 także jako serwer komunikacyjny, proxy i serwer aktualizacji dla innych punktów końcowych w sieci.



Ostrzeżenie

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

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

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

W trybie normalnym, agenty bezpieczeństwa 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. 33).

5.2.1. Przygotowywanie do Instalacji

Przed instalacją, 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. Sprawdź 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](#).

Aby 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 z Control Center.
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.

5.2.2. 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**.

Bitdefender GravityZone						
Witaj, Admin						
Panel nawigacyjny	Dodaj Pobierz Wyślij linki do pobrania Usuń Odśwież					
Sieć						
Pakiety	Nazwa	Typ	Język	Opis	Status	Firma
Zadania	<input type="text"/>	<input type="text"/>				
Polityki	<input type="checkbox"/> ABS	BEST	English		Gotowe do pobrania	CompanyABS
Raporty	<input type="checkbox"/> Endpoint	BEST	English		Gotowe do pobrania	Documentation Bitdefender
Kwarantanna						

Strona Pakietów



Ostrzeżenie

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

Gdy pierwszy klient zostanie zainstalowany, zostanie on wykorzystany do wykrycia innych punktów końcowych w tej samej sieci, bazując na mechanizmie wykrywania sieci. Aby uzyskać więcej informacji o wykrywaniu sieci, odwołaj się do „[Jak działa wyszukiwanie sieci](#)” (p. 48).

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.

Ogólne

Nazwa: *

Opis:

Język: Polski ▼

Firma: Company1 ▼

Moduły:

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

Role: ☐ Relay ⓘ

Tryb skanowania ⓘ

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 „[Agencji Bezpieczeństwa](#)” (p. 7).

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. 9)

**Ostrzeżenie**

Rola relay nie jest obsługiwana w starszych systemach operacyjnych. Aby uzyskać więcej informacji, odwołaj się do „[Wspierane systemy operacyjne](#)” (p. 16).

- **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. 9)
8. **Tryb skanowania.** Wybierz technologię skanowania, która najlepiej pasuje do Twojego środowiska sieciowego i zasobów punktów końcowych. Możesz zdefiniować tryb skanowania, poprzez wybranie jednego z następujących typów:
- **Automatyczne.** W tym przypadku, agent bezpieczeństwa będzie automatycznie wykrywał konfigurację punktu końcowego i odpowiednio dostosuje technologię skanowania:
 - Lokalne Skanowanie (z Pełnymi Silnikami) na fizycznych komputerach z wysokimi wymaganiami sprzętowymi.

**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 Lekkiemi 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)



Ostrzeżenie

Endpoint Security (dziedziczony agent) wspiera tylko Lokalne Skanowanie.

9. 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.
10. Na punktach końcowych Windows, Bitdefender Endpoint Security Tools jest zainstalowany w domyślnym katalogu instalacyjnym. Wybierz **Użyj niestandardowej ścieżki instalacyjnej** jeżeli chcesz zainstalować Bitdefender Endpoint Security Tools w innej lokalizacji. W tym przypadku, podaj ścieżkę docelową w odpowiednim polu. Użyj konwencji Windows podczas wprowadzania ścieżki (np. D: \folder). Jeżeli folder docelowy nie istnieje, zostanie stworzony podczas instalacji.
11. Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.

12. 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.

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

- **Bitdefender Cloud**, jeśli chcesz aktualizować klientów bezpośrednio z Internetu.:

W tym przypadku, można również zdefiniować ustawienia serwera proxy, jeśli docelowe punkty końcowe są połączone z Internetem za pośrednictwem serwera proxy. Wybierz **Użyj proxy do komunikacji** i wprowadź wymagane ustawienia proxy w polach poniżej.

- **Endpoint Security Relay**, jeśli chcesz połączyć punkty końcowe z zainstalowanym w Twojej sieci klientem Relay. Wszystkie maszyny z rolą Relay wykryte w Twojej sieci pokażą się w tabeli poniżej. Wybierz maszynę Relay. 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.

14. 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 instalację. 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
- **Starsze systemy operacyjne Windows:** 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 downlodaera, 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 adresie 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, wyodrębni 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 kopij 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](#).

5.2.3. Instalacja Zdalna

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

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

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

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. 48).

Wymagania zdalnej instalacji

Aby zdalna instalacja działała:

- Bitdefender Endpoint Security Tools Relay musi być zainstalowany w Twojej sieci.
- Dla Windows:
 - Udziały administracyjne `admin$` muszą być włączone. Skonfiguruj każdą docelową stację 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. 16).

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


Uruchamianie Zadania Zdalnej Instalacji

Aby uruchomić zdalną instalację:

1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć**.
3. Wybierz żadaną 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**.

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

Zainstaluj klienta

Opcje

☒ Teraz
☐ Zaplanowane

☐ Automatyczny restart systemu (jeżeli potrzebny)

Menedżer uprawnień

<input type="checkbox"/>	Użytkownik	Hasło	Opis	Akcja
<input type="checkbox"/>	admin	*****	Doc1	<input checked="" type="checkbox"/>

Zapisz Anuluj

Instalowanie Bitdefender Endpoint Security Tools z menu zadań

6. W sekcji **Opcje** skonfiguruj czas instalacji:

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



Notatka

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

7. Jeśli chcesz, by docelowe punkty końcowe samoczynnie się uruchamiały, aby zakończyć instalację, wybierz **Automatyczny restart (w razie potrzeby)**.
8. W sekcji **Menadżer poświadczeń**, wybierz poświadczenia administracyjne potrzebne do zdalnego uwierzytelnienia na docelowych punktach końcowych. Możesz dodać poświadczenia 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 [Menedżer Poświadczeń](#) tak, by nie trzeba było wprowadzać ich następnym razem. Aby uzyskać dostęp do Menedżera Poświadczeń wskaż tylko swoją nazwę użytkownika w prawym górnym rogu konsoli.

**WAŻNE**

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

9. Zaznacz pola odpowiadające kontom, które chcesz używać.

**Notatka**

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

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

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

**WAŻNE**

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

Wdrożeniowiec

Wdrożeniowiec: Endpoint Security Relay

Nazwa	IP	Wybrana Nazwa/IP Serwera	Etykieta
MASTER-PC	192.168.1.141		Niedostępny
NMNI-DOC1	10.0.2.15		Niedostępny

Pierwsza strona Strona 1 z 1 Ostatnia strona 20 2 elementów

- Jeżeli docelowy punkt końcowy komunikuje się z agentem Relay poprzez proxy, musisz również zdefiniować ustawienia proxy. W tym przypadku, wybierz **Użyj proxy do komunikacji** i wprowadź wymagane ustawienia proxy w polach poniżej.
11. Musisz wybrać jeden pakiet instalacyjny dla aktualnego wdrożenia. Kliknij listę **Użyj pakietu** i wybierz pakiet instalacyjny, który chcesz. Można tu znaleźć wszystkie pakiety instalacyjne wcześniej utworzone dla Twojego konta, a także domyślny pakiet instalacyjny dostępny z Control Center.

12. Jeśli to potrzebne, można zmienić niektóre ustawienia wybranego pakietu instalacyjnego, klikając przycisk **Dostosuj** obok pola **Użycie pakietu**.

Ustawienia pakietu instalacyjnego pojawią się poniżej i możesz wprowadzić zmiany, które potrzebujesz. Aby dowiedzieć się więcej o edycji pakietów instalacyjnych, patrz „[Tworzenie pakietów instalacyjnych](#)” (p. 33).

Jeśli chcesz zapisać zmiany jako nowy pakiet, wybierz opcję **Zapisz jako pakiet** umieszczoną na dole listy ustawień pakietów, a następnie wpisz nazwę dla nowego pakietu instalacyjnego.

13. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

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



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](#).

5.2.4. 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 systemu 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 -xzf 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 instalacją 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 ładuje. 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 smb start
```

**WAŻNE**

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

5.2.5. Jak działa wyszukiwanie sieci

Oprócz integracji z usługą 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 technologią 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.

```
Z:\>net view
Server Name      Remark
-----
\\SCIREFDL
\\SCIREFJM
\\SCIREFLL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

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 używa informacji sieciowych z Active Directory ani z funkcji mapy sieci dostępnej w Windows Vista i późniejszych. Mapa sieci zależy od innych technologii 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; usunąć 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 roboczą 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.
- Dla Windows Vista lub wyższych wersji, wykrywanie sieci musi być włączone (**Panel Kontrolny > Centrum Wykrywania i Udostępniania > Zmień Zaawansowane Ustawienia udostępniania**).

Aby móc włączyć tę funkcję, musisz najpierw uruchomić poniższe usługi:

- Klient DNS
 - Funkcja wykrywania zasobów publikacji
 - Wykrywanie SSDP
 - Host UPnP Urządzenia
- W środowiskach z wieloma domenami, jest rekomendowane aby ustawić zaufaną relację pomiędzy domenami, dzięki czemu komputery będą miały dostęp do przeglądania listy z innych domen.

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



Notatka

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

5.3. Instalacja Pełnego Szyfrowania Dysku

Pełne Szyfrowanie Dysku wymaga aktywacji opartej na kluczu licencyjnym.

Aby uzyskać więcej informacji o kluczu licencyjnym, przejdź do „[Zarządzanie Licencjami](#)” (p. 27).

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 modulem:

- 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**.

5.4. Manager uprawnień

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

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

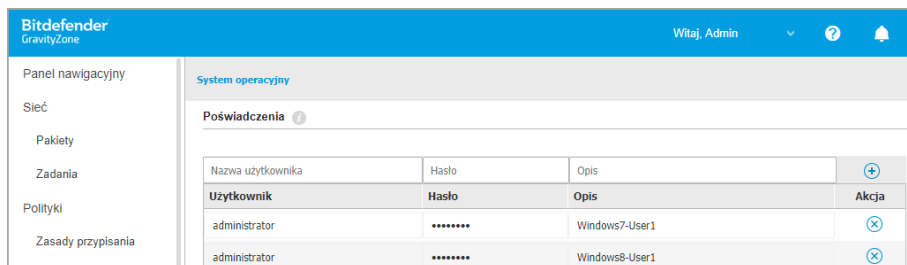


Menu menadżera poświadczeń

5.4.1. Dodaj Poświadczenia to Menadżera Poświadczeń

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

Aby dodać zestaw poświadczeń:



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 domenę, 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.

5.4.2. Usuwanie Poświadczeń z Menadżera Poświadczeń

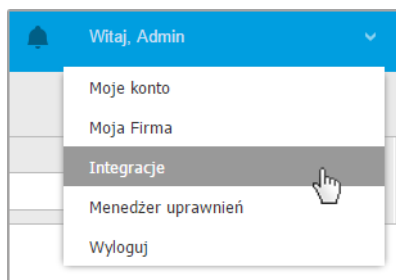
aby usunąć nieaktualne poświadczenia z Menadżera Poświadczeń:

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

6. INTEGRACJE

GravityZone zapewnia możliwość integracji Control Center z rozwiązaniami stron trzecich.

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



Na tej stronie możesz dodawać, edytować lub usuwać integracje zgodnie z własnymi potrzebami.

6.1. Integracja z Amazon EC2

Jeśli Twoja firma ma licencję na usługi Bitdefender Security for AWS lub korzystasz z subskrypcji próbnej Bitdefender Security for AWS, możesz skonfigurować integrację z tą usługą z GravityZone Control Center i centralnie wdrożyć, zarządzać i monitorować zabezpieczenia Bitdefender w inwentaryzacjach ich instancji. Posiadane serwery skanowania są hostowane przez Bitdefender wewnątrz chmury AWS Cloud w celu zapewnienia optymalnego odcisku na chronionych przypadkach by wyeliminować skanowanie napowietrznego występującego w tradycyjnym oprogramowaniu ochrony.

Aby uzyskać pełne informacje o architekturze Bitdefender Security for AWS, wymaganiach wstępnych, trybie subskrypcji, tworzeniu i zarządzaniu integracją z Amazon EC2, zapoznaj się z [przewodnikiem po integracji Amazon EC2](#).

7. ODINSTALOWYWANIE OCHRONY ENDPOINT

Masz dwie opcje na odinstalowanie agentów bezpieczeństwa:

- **Zdalnie** w Control Center
- **Manualnie** na maszynie docelowej



Ostrzeżenie

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

Zdalne Odinstalowywanie

Aby zdalnie odinstalować ochronę Bitdefender z jakiegokolwiek zarządzanego punktu końcowego:

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

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

Jeśli chcesz przeinstalować agenty bezpieczeństwa, przejdź do „[Instalowanie Agentów Bezpieczeństwa](#)” (p. 29).

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 postępowanie 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 agenta bezpieczeństwa, przejdź do „[Instalowanie Agentów Bezpieczeństwa](#)” (p. 29).

8. OTRZYMYWANIE POMOCY

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



Notatka

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

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 dostępna 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](#)
- [GUI wizard](#)

Jeśli opcja BEST nie została zainstalowana na komputerze, użyj pliku wykonywalnego BEST Support Tool.

Metoda wiersza poleceń

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.

Metoda GUI Wizard

1. Pobierz BEST Support Tool z odpowiednich linków poniżej:
 - W przypadku 32-bitowego systemu operacyjnego Windows kliknij [tutaj](#).
 - W przypadku 64-bitowego systemu operacyjnego Windows kliknij [tutaj](#).
2. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby uruchomić narzędzie pomocy technicznej.

Plik wyjściowy można znaleźć na pulpicie jako archiwum o następującej nazwie:
BDST_[computername]_[currentdate].

Prześlij plik dziennika

Aby przesłać dziennik Support Tool, w zależności od zastosowanej metody, wykonaj następujące kroki:

Jeśli użyłeś linii poleceń:

1. Przejdź do C:\Windows\Temp i znajdź plik archiwum o nazwie ST_[computername]_[currentdate].
2. Wewnątrz archiwum otwórz plik problem.txt.
3. Wypełnij plik niezbędnymi danymi.
4. Załącz archiwum do zgłoszenia do pomocy technicznej w celu dalszego rozwiązywania problemów.

Jeśli używasz kreatora GUI:

1. Przejdź do Pulpit i znajdź plik archiwum o nazwie BDST_[computername]_[currentdate].
2. 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 chcesz 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 zraportować 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 produkcji

Skuteczna komunikacja jest kluczem do udanej współpracy. Przez ostatnie 15 lat Bitdefender uzyskał niekwestionowaną reputację dzięki ciągłemu dążeniu do poprawy komunikacji z klientami, aby przewyższyć oczekiwania partnerów oraz klientów. Jeśli miałbyś jakiegokolwiek problemy czy pytania, bez wahania skontaktuj się z nami.

8.4.1. Adresy Internetowe

Dział sprzedaży: enterprisesales@bitdefender.com

C e n t r u m

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 Spamów: 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) 231 98 92 80 16

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

rsOrhideea Towe
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; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf;
xsn; xtp; xz; z; zip; zl?; zoo