

Bitdefender® ENTERPRISE

# SMALL OFFICE SECURITY

Szybki Start Poradnik dla  
Partnerów >>

# Small Office Security

## Szybki Start Poradnik dla Partnerów

Data publikacji 2015.01.08

Copyright© 2015 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 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 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 znaków handlowych. Wszystkie zarejestrowane i niezarejestrowane znaki handlowe w tym dokumencie są własnością ich poszczególnych właścicieli, i tak powinny być traktowane.

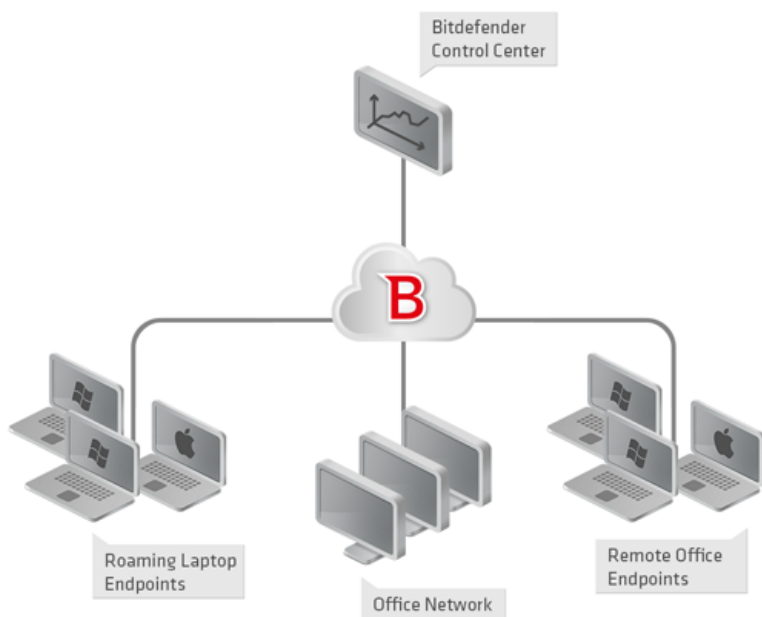


# Spis treści

<b>1. O Small Office Security</b>	<b>1</b>
<b>2. Pierwsze Kroki</b>	<b>3</b>
2.1. Łączenie z Control Center	3
2.2. Control Center w skrócie	4
2.2.1. Control Center Przegląda	4
2.2.2. Tabela Danych	5
2.2.3. Paski narzędzi działań	6
2.2.4. Menu Kontekstowe	7
2.3. Zarządzanie kontem	7
2.4. Zarządzanie swoją firmą	8
2.5. Zmiana hasła logowania	10
<b>3. Zarządzanie kontami</b>	<b>11</b>
3.1. Zarządzanie kontami firmowymi	11
3.1.1. Tworzenie Firm Partnerskich	12
3.1.2. Tworzenie Firm Kliencckich.	14
3.2. Zarządzanie kontami użytkownika	15
3.2.1. Role konta użytkownika	16
3.2.2. Prawa użytkownika	17
3.2.3. Tworzenie Kont Użytkowników	18
<b>4. Zarządzanie usługami dla twoich twoich klientów</b>	<b>20</b>
4.1. Instalacja i Ustawienia	20
4.1.1. Przygotowywanie do Instalacji	20
4.1.2. Instalowanie usługi na komputerach	21
4.1.3. Organizowanie Komputerów (Opcjonalnie)	30
4.1.4. Tworzenie i przypisywanie polityki bezpieczeństwa	31
4.2. Monitorowanie stanu bezpieczeństwa	34
4.3. Skanowanie zarządzanych komputerów	35
<b>5. Otrzymywanie pomocy</b>	<b>37</b>
<b>A. Wymagania</b>	<b>38</b>
A.1. Wymagania Security for Endpoints	38
A.1.1. Wspierane systemy operacyjne	38
A.1.2. Wymagania Sprzętowe	39
A.1.3. Obsługiwane przeglądarki	39
A.1.4. Porty Komunikacji Small Office Security	40
A.2. Jak działa wyszukiwanie sieci	40
A.2.1. Więcej o usłudze przeglądania komputerów Microsoft	41
A.2.2. Wymagania wyszukiwania sieci	42

# 1. 0 Small Office Security

Small Office Security to usługa ochrony przeciw malware bazująca na chmurze opracowana przez Bitdefender dla komputerów działających w systemach operacyjnych Microsoft Windows i Macintosh. Używa scentralizowanego Oprogramowania jako Usługi wielokrotnego modelu wdrażania nadającego się dla klientów biznesowych, przy jednoczesnym wykorzystaniu sprawdzonej pod każdym kątem technologii ochrony przed złośliwym oprogramowaniem opracowanym przez Bitdefender dla rynku konsumenckiego.



Architektura Small Office Security

Usługa bezpieczeństwa jest hostowana przez publiczną chmurę Bitdefender. Subskrybenci mają dostęp do interfejsu zarządzania sieciowego zwanego **Control Center**. W interfejsie, administratorzy mogą zdalnie zainstalować i zarządzać ochroną przed złośliwym oprogramowaniem na wszystkich komputerach z systemami Windows i Macintosh takich jak: serwery i stacje robocze w sieci wewnętrznej, korzystające z roamingu laptopy lu zdalne biurowe punkty końcowe.

Lokalna aplikacja **Endpoint Security** jest zainstalowana na każdym chronionym komputerze. Lokalni użytkownicy mają ograniczoną widoczność i dostęp tylko do odczytu w ustawieniach

bezpieczeństwa, które są zarządzane przez administratora z Control Center; natomiast skanowanie, aktualizacja i zmiany konfiguracji są zazwyczaj wykonywane w tle.

## 2. Pierwsze Kroki

Security for Endpoints może być skonfigurowany i zarządzany używając Control Center, a bazujący na sieci interfejs jest hostowany przez Bitdefender.

Control Center również zapewnia konsole zarządzania dla partnerów Bitdefender sprzedających usługi. To włącza je do stworzenia i zarządzania kontami dla ich klientów i opcjonalnie do zarządzania usługami klientów końcowych.

### 2.1. Łączenie z Control Center

Dostęp do Control Center odbywa się za pośrednictwem kont użytkowników. Po utworzeniu konta otrzymasz informacje dotyczące logowania na e-mail.

Warunki wstępne:

- Internet Explorer 9+, Mozilla Firefox 14+, Google Chrome 15+, Safari 5+
- Zalecana rozdzielczość ekranu: 1024x768 lub wyższa

Żeby połączyć się z Control Center:

1. Otwórz przeglądarkę.
2. Zobacz pod adresem: <https://gravityzone.bitdefender.com>
3. Podaj adres e-mail i hasło twojego konta.
4. Kliknij „Zaloguj”.

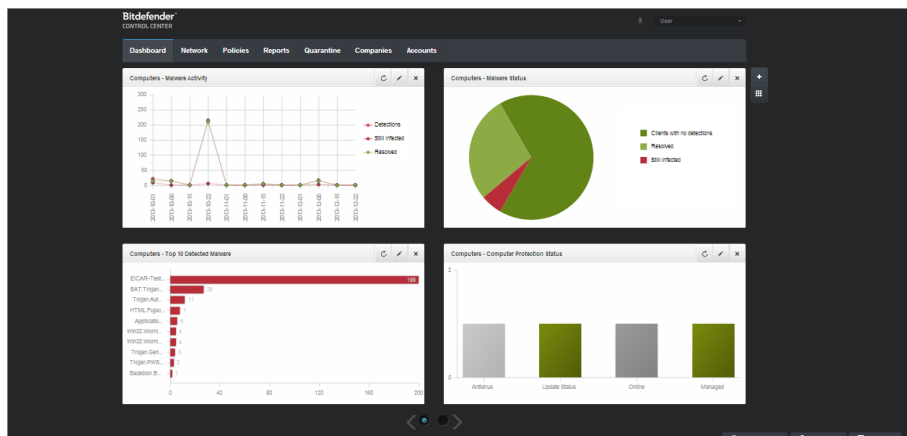


#### Notatka

Jeżeli zapomniałeś hasło, użyj linku przypomnienia hasła, aby otrzymać nowe hasło. Musisz podać adres e-mail twojego konta.

## 2.2. Control Center w skrócie

Control Center jest uporządkowana w taki sposób, aby umożliwić łatwy dostęp do wszystkich funkcji. Użyj paska menu w górnej części, aby poruszać się po konsoli. Dostępne funkcje zależą od typu użytkownika, który chce uzyskać dostęp do konsoli.



Panel

### 2.2.1. Control Center Przegląda

Partnerzy mają dostęp do poniższych sekcji w menu.

#### Panel nawigacyjny

Zobacz łatwe do czytania wykresy dostarczające kluczowe informacje na temat bezpieczeństwa sieci.

#### Sieć

Wyświetl swoje firmy i sieci, zainstaluj ochronę, zastosuj polityki do zarządzania ustawieniami bezpieczeństwa, uruchom zadania zdalnie i utwórz szybkie raporty.

#### Polityki

Utwórz i zarządzaj politykami bezpieczeństwa.

#### Raporty

Pobierz raporty bezpieczeństwa dotyczące zarządzania komputerami i firmami.

#### Kwarantanna

Zdalne zarządzanie plikami kwarantanny.

#### Firmy

Utwórz i zarządzaj kontem firmy (partnerzy i klienci firm)



## Konta


Stwórz i zarządzaj kontami użytkowników dla firm partnerów i klientów, którym świadczysz usługi.

W tym menu można również znaleźć stronę **Aktywność Użytkownika**, co pozwala na uzyskiwanie dostępu do dziennika aktywności użytkownika.



### Notatka

Dla partnerów bez praw zarządzania siecią, tylko monitoring i pozycje menu administracyjnego są dostępne.

Dodatkowo w górnym rogu konsoli ikona  **Powiadomienia** umożliwia łatwy dostęp do powiadomień i strony **powiadomienia**.

Wskazując nazwę użytkownika w prawym górnym rogu konsoli, dostępne są następujące opcje:

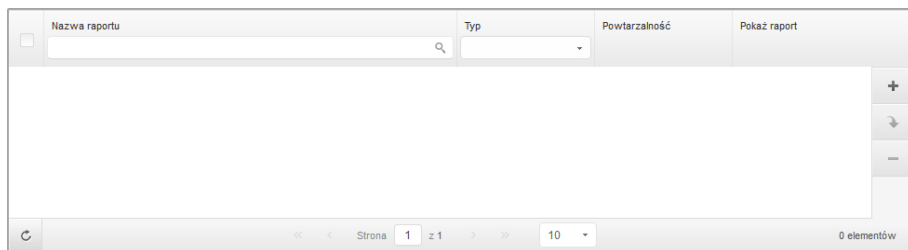
- **Moje konto.** Kliknij tę opcję, aby zarządzać danymi konta użytkownika i preferencjami.
- **Moja Firma.** Kliknij tę opcję, aby zarządzać danymi konta firmy i preferencjami.
- **Integracje.** Kliknij tę opcję, aby zarządzać integracją Small Office Security z innymi platformami zarządzania.
- **Menedżer uprawnień.** Naciśnij tę opcję aby dodać i zarządzać poświadczeniami uwierzytelniania potrzebnymi do zdalnej instalacji zadań.
- **Wyloguj.** Kliknij tę opcję, aby wylogować się z konta.

W prawym dolnym rogu konsoli dostępne są linki:

- **Pomoc.** Naciśnij ten przycisk aby znaleźć informacje o wsparciu.
- **Tryb Pomoc.** Naciśnij ten przycisk aby włączyć funkcję pomocy dostarczającą podpowiedzi w Control Center. Łatwo znajdziesz przydatne informacje dotyczące funkcji Control Center.
- **Opinie.** Naciśnij ten przycisk żeby wyświetlić pole umożliwiające edycję i wysyłanie wiadomości zwrotnych dotyczących twoich doświadczeń z Small Office Security.

## 2.2.2. Tabela Danych

Tabele są często używane przez konsolę do uporządkowania danych w przystępnym formacie.



Nazwa raportu	Typ	Powtarzalność	Pokaż raport
---------------	-----	---------------	--------------

0 elementów

Strona raportów - Tabele raportów

## Poruszanie się po stronach

Tabele z ponad 10 zgłoszeniami rozciągają się na kilka stron. Domyślnie tylko 10 wpisów jest wyświetlanych na stronie. Do poruszania się po kolejnych stronach służą przyciski nawigacji znajdujące się na dole tabeli. Możesz zmienić liczbę wpisów wyświetlanych na stronie, wybierając inną opcję z menu obok przycisków nawigacyjnych.

## Szukanie określonych wpisów


Żeby łatwo znaleźć określone wpisy, użyj pól wyszukiwania dostępnych poniżej kolumny nagłówków.

W odpowiednie pole wpisz szukany termin. Pasujące elementy są wyświetlane w tabeli w trakcie pisania. Aby przywrócić zawartość tabeli, wyczyść pola wyszukiwania.

## Sortowanie danych

Aby posortować dane według określonych kolumn, naciśnij na nagłówek kolumny. Kliknij nagłówek ponownie, aby przywrócić kolejność porządkowania.

## Odświeżanie Danych Tabeli

Abby upewnić się, że konsola wyświetla najnowsze informacje, naciśnij przycisk  **Odśwież** w dolnym lewym rogu tabeli.

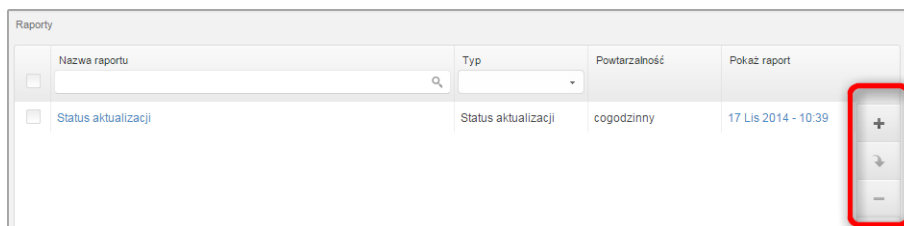
## 2.2.3. Paski narzędzi działań

W Control Center, paski narzędzi działań pozwalają na wykonanie określonych czynności należących do sekcji w której się znajdujesz. Każdy pasek narzędzi składa się z zestawu ikon, które zwykle umieszczone są z prawej strony tabeli. Na przykład, pasek narzędzi działań w sekcji **Raporty** pozwala wykonać poniższe akcje:

- Stwórz nowy raport.
- Pobierz raporty wygenerowane przez zaplanowany raport.

- Usuń zaplanowany raport.

Raporty				
<input type="checkbox"/>	Nazwa raportu	Typ	Powtarzalność	Pokaż raport
<input type="checkbox"/>	Status aktualizacji	Status aktualizacji	cogodzinny	17 Lis 2014 - 10:39

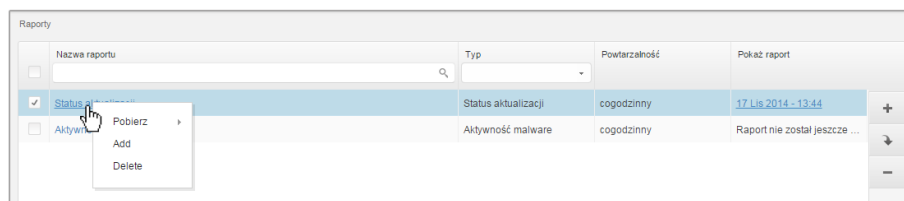


Strona raportów - Paski Narzędzi działań

## 2.2.4. Menu Kontekstowe

Komendy pasków narzędzi działań są również dostępne z menu kontekstowego. Naciśnij prawy przycisk w sekcji Centrum Kontroli, której aktualnie używaj i wybierz polecenie, które potrzebujesz z dostępnej listy.

Raporty				
<input type="checkbox"/>	Nazwa raportu	Typ	Powtarzalność	Pokaż raport
<input checked="" type="checkbox"/>	Status aktualizacji	Status aktualizacji	cogodzinny	17 Lis 2014 - 13:44
<input type="checkbox"/>	Aktywność malware	Aktywność malware	cogodzinny	Raport nie został jeszcze ...

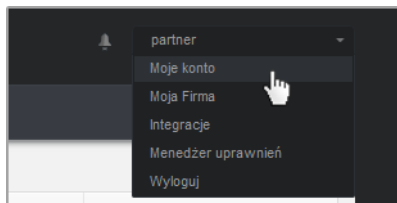


Strona Raportów - menu kontekstowe

## 2.3. Zarządzanie kontem

Żeby sprawdzić albo zmienić szczegółowe dane konta lub ustawić:

1. Wskaż nazwę użytkownika w prawym górnym rogu konsoli i wybierz **Moje konto**.



Menu konta użytkownika

2. W **Szczegóły konta**, popraw lub aktualizuje szczegóły twojego konta.

- **Pełna nazwa.** Wprowadź swoje imię i nazwisko.
  - **E-mail.** To jest twój login i kontaktowy adres e-mail. Raporty i ważne powiadomienia bezpieczeństwa będą wysyłane na ten adres. Powiadomienia e-mail są wysyłane automatycznie, gdy zostaną wykryte istotne ryzykowne warunki w sieci.
  - **Hasło.** Link **Zmień hasło** pozwala Ci na zmianę hasła logowania.
3. W **Ustawienia**, konfiguruj ustawienia konta zgodnie z własnymi preferencjami.
- **Strefa czasowa.** Wybierz z menu strefę czasową konta. Konsola wyświetli informację o czasie, w zależności od wybranej strefy czasowej.
  - **Język.** Wybierz z menu język wyświetlania w konsoli.
  - **Sesja wygasła.** Wybierz czas nieaktywności sesji zanim wygaśnie.
4. Naciśnij **Zapisz** aby zastosować zmiany.



### Notatka

Nie możesz usunąć swojego własnego konta.

## 2.4. Zarządzanie swoją firmą

Aby sprawdzić lub zmienić szczegóły twojej firmy i ustawienia licencji:

1. Wskaż nazwę użytkownika w prawym górnym rogu konsoli i wybierz **Moja Firma**.

Szczegółowe informacje o firmie

Nazwa firmy:

Adresy:

ID:

Telefon:

Logo:  Logo musi mieć wielkość 200x30 px, oraz być w formacie png lub jpg.

Pozwól innym firmą zarządzać bezpieczeństwem tej firmy

Licencja

Klucz licencyjny:

Data wygaśnięcia: 06 Paź 2018  
Używany: 19  
Dostępne do instalacji: 313  
Zarezerwowane: 20  
Całkowity: 333

Bitdefender Partner [Zmień](#)

Nazwa firmy:

ID:

Adresy:

Telefon:

[Połącz tą firmę z MyBitdefender \(opcjonalnie\)](#)

Strona Mojej Firmy

2. W **Szczegóły Firmy**, uzupełnij w informacjach twoich firmy, takie jak nazwa firmy, adres i telefon.
3. Możesz zmienić logo wyświetlane w Control Center jak również w raporcie twojej firmy i powiadomieniach e-mail, według poniższych:
  - Naciśnij **Zmiana** aby przeglądać obrazy logo na twoim komputerze. Obraz musi być w formacie .png lub .jpg i wielkość obrazu musi wynosić 200x30 pikseli.
  - Naciśnij **Domyślne** aby usunąć obraz i zresetować obraz do domyślnie dostarczonego przez Bitdefender.
4. Domyślnie, Twoja firma może być zarządzana przez konta partnerskie innych firm, które mogą mieć Twoją firmę wymienioną w swojej Bitdefender Control Center. Możesz blokować dostęp tych firm do swojej sieci przez wyłączenie opcji **Zezwól innym firmom na zarządzanie bezpieczeństwem firmy**. W rezultacie, Twoja sieć nie będzie już widoczna w innych Control Center przedsiębiorstw i nie będą one już w stanie zarządzać Twoją subskrypcją.
5. W sekcji **Licencja** możesz zobaczyć i zmodyfikować szczegóły Twojej licencji.
  - Aby dodać nowy klucz licencyjny:
    - a. Z **Menu typ**, wybierz typ subskrypcji **Licencja**.
    - b. Podaj klucz licencyjny w polu **Klucz Licencyjny**.
    - c. Naciśnij przycisk **Sprawdź** i poczekaj zanim Control Center prześle informacje o wpisanym kluczu licencyjnym.
  - Aby sprawdzić szczegóły twojego klucza licencyjnego, zobacz wyświetlone informacje poniżej klucza licencyjnego:
    - **Data wygaśnięcia** data do kiedy klucz licencyjny może być używany.
    - **Używane**: liczba używanych miejsc z ogólnej ilości miejsc w kluczu licencyjnym. Miejsce licencji używane w kliencie Bitdefender zainstalowane w punktach końcowych w zarządzanej sieci.
    - **Dostępne do zainstalowania**: liczba wolnych miejsc z ogólnej liczby miejsc z miesięcznej puli licencji (z wyjątkiem używanych i zarezerwowanych miejsc).
    - **Zarezerwowane**: całkowita liczba miejsc jakie są zarezerwowane dla innych firm z twojej puli licencji miesięcznych.
    - **Całkowite** całkowita liczba dostępnych miejsc dla twojego klucza licencyjnego.
6. W **Partner Bitdefender** możesz znaleźć informacje na temat Twojego usługodawcy.

Aby zmienić dostawcę usług zarządzalnych:

  - a. Kliknij przycisk **Zmień**.
  - b. Wprowadź kod ID firmy partnerskiej w polu **ID Partnera**.



### Notatka

Każda firma może znaleźć swoje ID na stronie **Moja Firma**. Po dokonaniu umowy z firmą partnerską, jej przedstawiciel musi dostarczyć Ci swój Control Center ID.

c. Kliknij **Zapisz**.

W rezultacie, Twoja firma jest automatycznie przeniesiona z poprzedniej partnerskiej do nowej partnerskiej Control Center.

7. Opcjonalnie, możesz połączyć swoją firmę z kontem MyBitdefender używając odpowiednich pól.
8. Naciśnij **Zapisz** aby zastosować zmiany.

## 2.5. Zmiana hasła logowania

Po utworzeniu Twojego konta, otrzymasz e-mail z poświadczeniami logowania.

Zaleca się, aby wykonać następujące czynności:

- Zmień domyślne hasło logowania, gdy po raz pierwszy odwiedzasz Control Center.
- Zmieniaj hasło logowania okresowo.

Aby zmienić hasło logowania:

1. Wskaż nazwę użytkownika w prawym górnym rogu konsoli i wybierz **Moje konto**.
2. W **Szczegóły Konta**, kliknij **Zmień hasło**.
3. Wprowadź bieżące hasło i nowe hasło w odpowiednich polach.
4. Naciśnij **Zapisz** aby zastosować zmiany.

## 3. Zarządzanie kontami

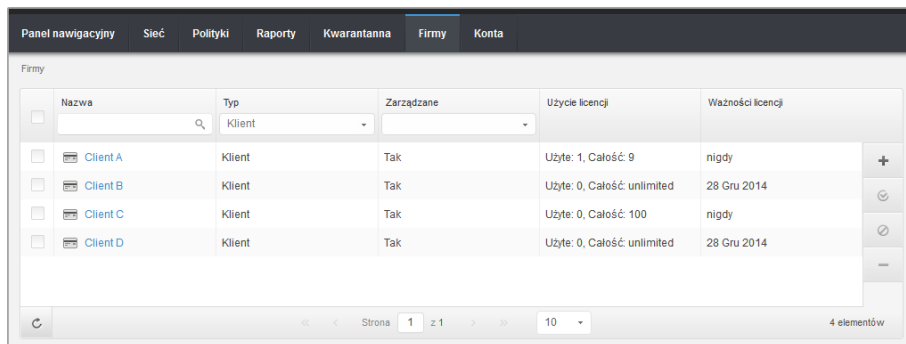
Partner Bitdefender, będzie odpowiedzialny za tworzenia i zarządzanie kontami Control Center dla twoich partnerów i klientów, którym świadczysz usługi. dodatkowo, możesz zarządzać subskrypcjami usług twoich klientów końcowych firmy.

Najpierw trzeba utworzyć konta firmowe dla swoich partnerów lub klientów firmy. Dla każdego przedsiębiorstwa w ramach swojej zarządzania można utworzyć jedno konto w jednej firmie. Następnie należy utworzyć konta użytkowników połączonych z odpowiednimi firmami. Dla każdej z firm można utworzyć wiele kont użytkowników, jeżeli jest to wymagane.

- [Zarządzanie kontami firmy](#)
- [Zarządzanie kontami użytkownika](#)

### 3.1. Zarządzanie kontami firmowymi

Możesz stworzyć lub zarządzać kontami firmy na stronie **Firmy**.



	Nazwa	Typ	Zarządzane	Uzycie licencji	Ważności licencji	
<input type="checkbox"/>	Client A	Klient	Tak	Użyte: 1, Całość: 9	nigdy	+
<input type="checkbox"/>	Client B	Klient	Tak	Użyte: 0, Całość: unlimited	28 Gru 2014	↻
<input type="checkbox"/>	Client C	Klient	Tak	Użyte: 0, Całość: 100	nigdy	↻
<input type="checkbox"/>	Client D	Klient	Tak	Użyte: 0, Całość: unlimited	28 Gru 2014	-

Strona Firm

Możesz utworzyć dwa rodzaje kont firmowych:

1. **Firmy partnerskie**, przeznaczone są dla firm, które sprzedają Small Office Security dla innych firm (użytkowników końcowych, dystrybutorów lub sprzedawców służby).

Small Office Security pozwala firmom partnerskim, dostarczać usługi przez zezwolenie im bezpośrednio zarządzać sieciami komputerowymi klientów.

Firmy partnerskie mogą również używać Small Office Security do ochrony ich sieci pod warunkiem, że mają włączone prawa **Zarządzanie Siecią** i ważny klucz licencyjny przypisany do ich konta firmowego.

Firma partnerska musi zostać połączona z przynajmniej jednym kontem partnerskim.

2. **Firmy klienckie**, są przeznaczone dla firm, które korzystają z usługi Security for Endpoints do ochrony swoich sieci komputerowych. Każda firma może zainstalować, skonfigurować, zarządzać i monitorować ich ochroną.

Firma kliencka musi zostać połączona z przynajmniej jednym kontem administratora firmy.

### 3.1.1. Tworzenie Firm Partnerskich

Aby utworzyć firmę partnerską:

1. Przejdź do strony **Firmy**.
2. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlono okno **Nowa firma**.
3. W sekcji **Nowa firma**, uzupełnij szczegółowe dane firmy.
  - **Nazwa**. Podaj nazwę partnera firmy. Nazwa firmy musi być unikalna.
  - **Adresy**. Możesz dodać adres partnera twojej firmy.
  - **Telefon**. Możesz dodać numer telefonu partnera firmy.
  - **Logo**. Możesz dodać obraz logo partnera firmy. Wszystkie raporty i powiadomienia e-mail wydane dla firmy będą zawierać logo.
    - Naciśnij **Zmiana** aby przeglądać obrazy logo na twoim komputerze.
    - Naciśnij **Domyślne** aby usunąć obraz i zresetować obraz do domyślnie dostarczonego przez Bitdefender.
  - Wybierz **Partner** dla rodzaju firmy.
  - Użyj opcji **Zarządzaj sieciami** aby skonfigurować prawa partnera firmy do zarządzania bezpieczeństwem klienckich sieci.
    - Kiedy ta opcja jest włączona, partner firmy będzie widoczny i będzie kontrolować sieci podrzędnych firm.
    - Kiedy ta opcja jest wyłączona, partner firmy może utworzyć inne firmy i zarządzać ich usługami subskrypcyjnymi, bez dostępu do ich sieci. Ta konfiguracja jest odpowiednia dla firm partnerskich działających wyłącznie jako sprzedawcy usług.
  - Domyślnie, każda utworzona firma może być zarządzana przez wszystkie macierzyste firmy. Możesz blokować dostęp macierzystej firmy do sieci nowej firmy przez wyłączenie opcji **Zezwól innym firmom na zarządzanie bezpieczeństwem firmy**. Firma będzie niewidoczna dla innych partnerów w twojej sieci, a ty nie będziesz już mieć dostępu do edycji i zarządzania subskrypcjami dla tej firmy.



#### WAŻNE

Raz zablokowana, ta opcja nie może zostać przywrócona.



4. W **Licencja**, możesz skonfigurować ustawienia subskrypcji dla partnerów firmy, używając również Small Office Security do zarządzania ich własną siecią.

- Dostępne są trzy opcje licencjonowania firmy dla twojego konta:
  - **Próbne.** Ta opcja przypisuje nową firmę z automatycznie wygenerowanym kluczem licencji próbnej.
  - **Licencja**, dla płatnych subskrypcji. W tym przypadku, wprowadź Klucz licencyjny odpowiedni dla typu subskrypcji klienta.

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



#### Notatka

Gdy licencjonujesz firmę partnerską, opcja **Zarządzanie Sieciami** musi być włączona.



#### Ostrzeżenie

Odnaczenie opcji **Zarządzanie Sieciami** podczas edytowania już stworzonych firm również usunie ich klucze licencyjne i całą ochronę komputera z bazy danych.

- **Miesięczna subskrypcja**, aby dzielić miesięczny klucz licencyjny między kilkoma podrzędnymi firmami dla twojego konta. Ta opcja jest dostępna tylko kiedy jedna z macierzystych firm ma miesięczny klucz licencyjny.

W tym przypadku podrzędne firmy do twojej firmy partnerskiej licencjonowanej przez miesięczny klucz licencyjny będzie dzielić taką samą liczbę licencji.

Możesz również ustawić limit liczby miejsc dla firmy, które może użyć do dzielenia miesięcznego klucza licencyjnego, przez wybranie opcji **Rezerwacja miejsc**. W tym przypadku wpisz liczbę miejsc jaką chcesz ustawić w odpowiednim polu. Firma będzie mogła licencjonować tylko określoną liczbę stanowisk.

5. Możesz podać poświadczenia konta partnerskiego **My Bitdefender**, jeśli są dostępne.
6. Opcjonalnie można przejść do tworzenia partnerskiego konta użytkownika, przewijając okno konfiguracji. Wprowadź szczegóły konta w sekcji **Dodaj nowe Konto**. Możesz przeglądać i zarządzać partnerskim kontem użytkownika później na stronie **Konta**.



#### Notatka

Możesz również utworzyć odpowiednie konta użytkowników w późniejszym czasie. Jednakże, jeśli opcja **Pozwól innym firmom zarządzać bezpieczeństwem tej firmy** jest wyłączona, ten krok jest obowiązkowy.

7. Kliknij **Zapisz**, aby utworzyć konto firmowe. Nowe konto pojawi się na liście kont firmowych.

Jeśli masz skonfigurowane konto użytkownika połączone a nową firmą, e-mail z danymi logowania jest natychmiast wysłany na podany adres e-mail.

Po utworzeniu konta, Twój partner może rozpocząć budowę i zarządzanie swoją siecią kliencką Small Office Security.

### 3.1.2. Tworzenie Firm Klienckich.

Aby utworzyć firmę kliencką:

1. Przejdź do strony **Firmy**.
2. Kliknij przycisk **+Dodaj** po prawej stronie tabeli. Wyświetlono okno **Nowa firma**.
3. W sekcji **Nowa firma**, uzupełnij szczegółowe dane firmy.
  - **Nazwa**. Wpisz nazwę firmy klienta. Nazwa firmy musi być unikalna.
  - **Adresy**. Możesz dodać adres klienta firmy.
  - **Telefon**. Możesz dodać numer telefonu klienta firmy.
  - **Logo**. możesz dodać obrazek logo klienta firmy. Wszystkie raporty i powiadomienia e-mail wydane dla firmy będą zawierać logo.
    - Naciśnij **Zmiana** aby przeglądać obrazy logo na twoim komputerze.
    - Naciśnij **Domyślnie** aby usunąć obraz (przywróć domyślne).
  - Wybierz **Klient** dla rodzaju firmy.
  - Domyślnie, każda utworzona firma może być zarządzana przez wszystkie macierzyste firmy. Możesz blokować dostęp macierzystej firmy do sieci nowej firmy przez wyłączenie opcji **Zezwól innym firmom na zarządzanie bezpieczeństwem firmy**. Firma będzie niewidoczna dla innych partnerów w twojej sieci, a ty nie będziesz już mieć dostępu do edycji i zarządzania subskrypcjami dla tej firmy.



#### WAŻNE

Raz zablokowana, ta opcja nie może zostać przywrócona.

4. W **Licencja** możesz skonfigurować ustawienia subskrypcji klientów.
  - Dostępne są trzy opcje licencjonowania firmy dla twojego konta:
    - **Próbne**. Ta opcja przypisuje nową firmę z automatycznie wygenerowanym kluczem licencji próbnej.
    - **Licencja**, dla płatnych subskrypcji. W tym przypadku, wprowadź **Klucz licencyjny** odpowiedni dla typu subskrypcji klienta.  
Naciśnij przycisk **Sprawdź** i poczekaj zanim Control Center prześle informacje o wpisanym kluczu licencyjnym.

- **Miesięczna subskrypcja**, aby dzielić miesięczny klucz licencyjny między kilkoma podrzędnymi firmami dla twojego konta. Ta opcja jest dostępna tylko kiedy jedna z macierzystych firm ma miesięczny klucz licencyjny.

W tym przypadku podrzędne firmy do twojej firmy partnerskiej licencjonowanej przez miesięczny klucz licencyjny będzie dzielić taką samą liczbę licencji.

Możesz również ustawić limit liczby miejsc dla firmy, które może użyć do dzielenia miesięcznego klucza licencyjnego, przez wybranie opcji **Rezerwacja miejsc**. W tym przypadku wpisz liczbę miejsc jaką chcesz ustawić w odpowiednim polu. Firma będzie mogła licencjonować tylko określoną liczbę stanowisk.

5. Możesz podać poświadczenia konta klienckiego **My Bitdefender**, jeśli są dostępne.
6. Opcjonalnie można przejść do tworzenia konta użytkownika administratora firmy, przewijając okno konfiguracji. Wprowadź szczegóły konta w sekcji **Dodaj nowe Konto**. Możesz przeglądać i zarządzać klienckim kontem użytkownika później na stronie **Konta**.



#### Notatka

Możesz również utworzyć odpowiednie konta użytkowników w późniejszym czasie. Jednakże, jeśli opcja **Pozwól innym firmom zarządzać bezpieczeństwem tej firmy** jest wyłączona, ten krok jest obowiązkowy.

7. Kliknij **Zapisz**, aby utworzyć konto firmowe. Nowe konto pojawi się na liście kont firmowych.

Jeśli masz skonfigurowane konto użytkownika połączone a nową firmą, e-mail z danymi logowania jest natychmiast wysłany na podany adres e-mail.

Po utworzeniu konta, klient może zacząć używać usługi. Zależnie od relacji biznesowej, usługi mogą być zarządzane przez klienta lub przez twoją firmę.

## 3.2. Zarządzanie kontami użytkownika

Small Office Security używa zintegrowanych dystrybucji i wdrożonego ekosystemu w którym różne rodzaje kont użytkowników są połączone w hierarchiczną strukturę dla każdej firmy. Każde konto ma wgląd w konta podrzędne. Ze względów odpowiedzialności, działania użytkowników są udokumentowane w dziennikach aktywności zarówno dla bieżących jak i podległych kont.

Aby zezwolić pracownikom firm na dostęp poprzez twoje konto Small Office Security, masz stworzyć konta użytkowników połączone z ich firmami. Każde konto firmy musi być połączone z ostatnim kontem użytkownika z przypisanymi prawami użytkownika. Dla każdej roli konta użytkownika, możesz dostosować dostęp do funkcji Small Office Security lub do określonych części sieci, do których należy.

Możesz stworzyć lub zarządzać kontami użytkownika na stronie **Konta**.

Pełna nazwa	E-mail	Rola	Firma
Comp Admin A	compadmina@bd.com	Administrator firmy	Client A
Net Admin A	netadmina@bd.com	Administrator sieci	Client A
Reporter A	reportera@bd.com	Sprawozdawca	Client A

Strona Kont

### 3.2.1. Rola konta użytkownika

Podczas tworzenia konta użytkownika, możesz wybrać jedną z predefiniowanych ról lub możesz stworzyć rolę niestandardową. Jako partner, możesz stworzyć poniższe role kont użytkownika:

- Partner** - Przystosowany dla dystrybutorów i resellerów Small Office Security. Użytkownicy z kontami partnerskimi mogą tworzyć i zarządzać innymi firmami. Gdy rozwija się ich sieć dystrybucji, tworzą konta partnerów podległych firmie. Przy sprzedaży bezpośrednio do użytkowników końcowych, tworzą konta firmowe klientów. Użytkownicy partnera mogą zarządzać licencjami podległych im firm i zarządzać kontami użytkowników powiązanych z tymi firmami. Ponieważ partnerzy mogą działać jako dostawcy usług bezpieczeństwa, mają uprawnienia administracyjne w ustawieniach zabezpieczeń dla kont podrzędnych klientów. Partnerskie konta użytkowników mogą również zarządzać bezpieczeństwem ich firmy.
- Administrator Firmy** - Nadaje się dla menedżerów firm klientów, którzy zakupili Small Office Security licencję od partnera. Administrator firmy zarządza licencjami, profilami firmowymi i całym wdrożeniem Small Office Security, zezwalając na najwyższy poziom kontroli nad wszystkimi ustawieniami bezpieczeństwa (chyba, że zostaje zastąpiony przez dominujące konto partnera w scenariuszu dostawcy usług bezpieczeństwa). Administrator firmy może podzielić się lub przekazać swoje obowiązki operacyjne podległym kontom administracyjnym i reporterowi kont użytkowników.
- Administrator Sieci** - Konta administratora sieci są wewnętrznymi kontami z przywilejami administracyjnymi we wdrożeniu Small Office Security całej firmy lub są określone dla grup komputerów. Administratorzy Sieci są odpowiedzialni za aktywne zarządzanie ustawieniami bezpieczeństwa Small Office Security.
- Reporter** - Konto reportera jest kontem wewnętrznym tylko do odczytu. Pozwalają jedynie na dostęp do raportów i dzienników aktywności użytkowników. Takie konta mogą być przydzielone dla pracowników z kontrolowaniem obowiązków lub dla innych pracowników którzy muszą utrzymywać wysoki stan bezpieczeństwa.

5. **Niestandardowe** - Wstępnie zdefiniowane konta użytkowników obejmują pewna kombinacje praw użytkowników. Jeżeli wcześniej zdefiniowana rola użytkownika nie spełnia twoich oczekiwań, możesz stworzyć niestandardowe konto poprzez wybranie tylko tych praw, które cie interesują.

Poniższa tabela podsumowuje relacje między różnymi rolami kont i ich prawami. Po szczególne informacje na temat uprawnień użytkownika, zobacz „Prawa użytkownika” (p. 17).

Rola konta	Dopuszcza konta dzieci	Prawa użytkownika
Partner	Partner, Administratorzy firm, administratorzy sieci, Reporterzy	Zarządzaj Firmami Zarządzaj Użytkownikami Zarządzaj Firmą Zarządzaj sieciami Zarządzaj Raportami
Administrator firmy	Administratorzy firm, administratorzy sieci, Reporterzy	Zarządzaj Firmą Zarządzaj Użytkownikami Zarządzaj sieciami Zarządzaj Raportami
Administrator sieci	Administratorzy sieci, Reporterzy	Zarządzaj Użytkownikami Zarządzaj sieciami Zarządzaj Raportami
Sprawozdawca	-	Zarządzaj Raportami

### 3.2.2. Prawa użytkownika

- **Zarządzaj Firmami.** Gdy rozwija się ich sieć dystrybucji, partnerzy użytkowników tworzą konta partnerów podległych firmie. Przy sprzedaży bezpośrednio do użytkowników końcowych, tworzą konta firmowe klientów. Użytkownicy partnerscy mogą również edytować, zawiesić lub usunąć firmy w ramach swojego konta. Przywilej ten jest specyficzny dla kont partnerskich.
- **Zarządzaj Użytkownikami.** Twórz, edytuj lub usuwaj konta użytkowników.
- **Zarządzaj Firmą.** Użytkownicy mogą zarządzać ich własnymi kluczami licencyjnymi Small Office Security i edytować ich ustawienia profilu firmy. Przywileje są określone dla kont administracyjnych firmy.
- **Zarządzaj sieciami.** Zapewnia uprawnienia administracyjne dla ustawień zabezpieczenia sieci (zasoby sieci, pakiety instalacyjne, kwarantanna). Przywilej ten jest specyficzny dla kont administratorów sieci.

Administratorzy z firm partnerskich mogą zarządzać uprawnieniami bezpieczeństwa dla sieci klientów firmy.

- **Zarządzaj Raportami.** Twórz, edytuj, usuń raporty i zarządzaj panelem.

### 3.2.3. Tworzenie Kont Użytkowników

Przed stworzeniem konta użytkownika, upewnij się, że masz odpowiedni adres email pod ręką. Ten adres jest obowiązkowy aby utworzyć konto użytkownika Small Office Security. Użytkownicy dostaną szczegółowe dane logowania z Small Office Security na podany adres e-mail. Użytkownicy będą używać adresu e-mail również do logowania do Small Office Security

Aby utworzyć konto użytkownika:

1. Zaloguj do Control Center.
2. Przejdź do strony **Konta**.
3. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlono okno konfiguracji.
4. W sekcji **Szczegóły**, uzupełnij szczegółowe dane użytkownika.
  - **E-mail.** Podaj adres e-mail użytkownika. Informacje logowania zostaną wysłane na ten adres niezwłocznie po utworzeniu konta.



#### Notatka

Adres e-mail musi być unikalny. Nie możesz stworzyć następnego konta użytkownika z tym samym adresem e-mail.

- **Pełna nazwa.** Podaj pełną nazwę dla właściciela konta.
  - **Firma.** Wybierz firmę, do której należy konto nowego użytkownika.
5. W sekcji **Ustawienia i Przywileje**, skonfiguruj poniższe ustawienia:
    - **Strefa czasowa.** wybierz z menu strefę czasową konta. Konsola wyświetli informację o czasie, w zależności od wybranej strefy czasowej.
    - **Język.** Wybierz z menu język wyświetlania w konsoli.
    - **Rola.** Wybierz rolę użytkownika. Aby uzyskać informacje o rolach użytkownika, odwołaj się do „[Role konta użytkownika](#)” (p. 16)
    - **Prawa.** Każda predefiniowana rola użytkownika ma pewną konfigurację [praw](#). Jednak, powinieneś wybrać jedynie prawa, które potrzebujesz. W tym przypadku, rola użytkownika zmienia się na **Niestandardowe**.

Na przykład, użytkownik z rolą partnera działa w charakterze dystrybutora usług tylko nie potrzebuje zarządzania sieciami. Kiedy tworzysz ten rodzaj konta użytkownika, możesz wyłączyć prawa zarządzania sieciami i rolę użytkownika staje się partnerem **Niestandardowym**.

6. **Wybierz Cele.** Przewiń w dół okno konfiguracji aby wyświetlić potrzebną sekcję. wybierz grupę sieciową do której użytkownik będzie miał dostęp. Możesz zastrzec dostęp do określonych obszarów sieci.
7. Naciśnij **Zapisz** aby dodać użytkownika. Nowe konto pokaże się na liście kont użytkowników.



### Notatka

Hasło dla każdego konta użytkownika jest automatycznie generowane podczas tworzenia konta i wysyłane do użytkownika wiadomością e-mail z innymi szczegółami dotyczącymi konta.

Możesz zmienić hasło po utworzeniu konta. Naciśnij nazwę konta na stronie **Konta** aby edytować hasło. Gdy hasło zostanie zmodyfikowane, użytkownik natychmiast zostanie powiadomiony przez e-mail.

Użytkownicy mogą zmieniać swoje hasło logowania z Control Center, uzyskując dostęp przez stronę **Moje konto**.

## 4. Zarządzanie usługami dla twoich twoich klientów

Oprócz kont klienta i zarządzania subskrypcją, konta partnerskie pozwalają również na zakładanie i zarządzania usługą dla klientów końcowych. W ten sposób, partnerzy Bitdefender mogą zapewnić klientom z pełnym zarządzaniem dodane usługi.

W dalszej części, nauczysz się podstaw tworzenia i zarządzania usługą dla klientów końcowych z konta partnerskiego.

### 4.1. Instalacja i Ustawienia

Instalacja i ustawienia są dość łatwe. To są główne kroki:

1. [Krok 1 - Przygotowanie dla instalacji.](#)
2. [Krok 2 - Instalacja usługi na komputerach.](#)
3. [Krok 3 - Organizacja komputerów w grupach \(opcjonalnie\).](#)
4. [Krok 4 - Tworzenie i konfiguracja polityk bezpieczeństwa.](#)

W dwóch pierwszych krokach, będziesz potrzebował wsparcia klienta, jako dostęp na żądanie i możliwe że informacje logowanie komputera będą wymagane do ich przeprowadzania. Inne dwa kroki są wykonywane z Control Center. Upewnij się czy zgadzasz się z klientem w tym jakie ustawienia bezpieczeństwa powinny być zastosowane na komputerach.

#### 4.1.1. Przygotowywanie do Instalacji

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

1. Upewnij się, że komputery spełniają [minimalne wymagania sprzętowe](#). Dla niektórych komputerów, możesz potrzebować zainstalować ostatni dostępny service pack dla systemu operacyjnego lub wolne miejsce na dysku. Sprządź listę komputerów, które nie spełniają niezbędnych wymogów, aby można było je wykluczyć z zarządzania.
2. Odinstaluj (nie tylko wyłącz) każde oprogramowanie antymalware, firewall lub ochronę Internetu z komputerów. Uruchomienie Endpoint Security jednocześnie z innym oprogramowaniem ochronnym na komputerze, może wpływać na ich działanie i spowodować problemy z systemem.



Wiele programów ochronnych jest niekompatybilne z Endpoint Security są automatycznie wykrywane i usuwane podczas instalacji. Aby nauczyć się więcej i sprawdzić listę wykrytych programów ochronnych, odwołaj się do [tego artykułu KB](#).



### WAŻNE

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

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

## 4.1.2. Instalowanie usługi na komputerach

Security for Endpoints jest przeznaczony dla stacji roboczych, laptopów i serwerów działających pod kontrolą systemów Microsoft® Windows. Aby chronić komputery z Security for Endpoints, musisz zainstalować Endpoint Security (oprogramowanie klienta) na któryś z nich. Endpoint Security zarządza ochroną na lokalnym komputerze. Komunikuje się również z Control Center aby otrzymać komendy administratora i wysłać wyniki przeprowadzonych działań.

Możesz zainstalować Endpoint Security z jedną z poniższych ról (dostępne w kreatorze instalacji):

1. **Punkt końcowy**, gdy odpowiadający komputer jest punktem końcowym.
2. **Endpoint Security Relay** gdy odpowiadający komputer jest używany przez inne punkty końcowe w sieci do komunikacji z Control Center. Rola Endpoint Security Relay instaluje Endpoint Security razem z aktualizacjami serwera, które mogą być użyte do aktualizacji wszystkich innych klientów w sieci. Punkty Końcowe w tej samej sieci mogą być konfigurowane przez polityki do komunikacji z Control Center poprzez jeden albo kilka komputerów z rolą Endpoint Security Relay. Gdy Endpoint Security Relay jest niedostępny, następnym jest brany pod uwagę w celu zapewnienia komunikacji komputera z Control Center.



### Ostrzeżenie

- Pierwszy komputer, na którym zainstalujesz zabezpieczenie musi mieć rolę Endpoint Security Relay, w przeciwnym razie nie będziesz w stanie wdrożyć Endpoint Security na innych komputerach w sieci.
- Komputer z rolą Endpoint Security Relay musi być włączony i widoczny online aby klienci mieli połączenie z Control Center.

Są dwie metody instalacji:

- **Instalacja lokalna**. Pobierz pakiety instalacyjne z Control Center na komputery, następnie uruchom lokalnie instalację Endpoint Security. Inna opcja jest pobranie pakietu, zapisanie

go udostępniając w sieci i wysłanie do użytkowników końcowych z firmowego adresu e-mail zaproszenia z odnośnikiem do pakietu, prosząc do pobrania i instalacji ochrony dla ich komputerów. Lokalna instalacja jest kierowana przez kreator.

- **Instalacja Zdalna.** Możesz lokalnie zainstalować pierwszego klienta dzięki roli Endpoint Security Relay, może to zająć kilka minut zanim inne komputery sieciowe zobaczą go w Control Center. Ochrona Security for Endpoints może być zdalnie zainstalowana z konsoli na innych komputerach w sieci. Zdalna instalacja jest wykonywana w tle, bez wiedzy użytkownika.

Endpoint Security ma minimalny interfejs użytkownika. Dopuszcza tylko użytkowników aby sprawdzić status ochrony i uruchomić podstawowe zadania bezpieczeństwa (aktualizacje i skanowanie), bez zapewnienia dostępu do ustawień.

Domyślnie, wyświetli język interfejsu użytkownika na chronionych komputerach jest ustawiony w czasie instalacji na język twojego konta. Aby zainstalować interfejs użytkownika w innym języku na wybranych komputerach, możesz stworzyć pakiet instalacyjny i ustawić preferowany język w opcjach konfiguracyjnych pakietu. Aby uzyskać więcej informacji o tworzeniu paczek instalacyjnych, odwołaj się do „[Tworzenie Endpoint Security pakietów instalacyjnych](#)” (p. 22).

## Instalacja lokalna

Lokalna instalacja wymaga pobrania z Control Center i uruchomienia pakietów instalacyjnych na każdym docelowym komputerze. Możesz stworzyć inne pakiety instalacyjne zależne od określonych wymagań każdego komputera (np. ścieżka instalacyjna lub język interfejsu użytkownika).

### Tworzenie Endpoint Security pakietów instalacyjnych

Można tworzyć pakiety instalacyjne dla własnej firmy lub dla każdej firmy w ramach Twojego konta. Pakiet instalacyjny jest ważny tylko dla firmy, dla której został on stworzony. Pakiet instalacji związany z pewną firmą nie może być stosowany na komputerach należących do innej firmy w Control Center.

Każdy pakiet instalacyjny będzie widoczny w Control Center tylko dla partnera, który utworzył pakiet i dla użytkownika kont w firmie związanej z pakietem instalacyjnym.

Stwórz paczkę instalacyjną Endpoint Security

1. Połącz się i zaloguj do Control Center używając twojego konta.
2. Przejdź do strony **Sieć > Pakiety**.

	Nazwa	Język	Opis	Status	Firma	
<input type="checkbox"/>	<input type="text"/>					
<input type="checkbox"/>	epsr	Polski		Gotowe do pobrania	Partner 2	+
<input type="checkbox"/>	Relay	English		Gotowe do pobrania	Client A	→
<input type="checkbox"/>	Endpoint	English		Gotowe do pobrania	Client A	✉
						-

Strona 1 z 1 10 3 elementów

Strona Pakietów

- Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Wyświetlone zostanie okno konfiguracji.

Endpoint Security

Opcje

Zaawansowane

**Szczegóły**

Nazwa:

Opis:

**Ogólne**

Rola:

Firma:

**Moduły, które będą zainstalowane:**

Antimalware ⓘ

Zapora sieciowa ⓘ

Kontrola zawartości

**Ustawienia**

Język:

Skanowanie przed instalacją

Użyj niestandardowej ścieżki instalacyjnej

Automatyczny restart systemu (jeżeli potrzebny)

Ustaw hasło deinstalacji

Hasło:

Potwierdź hasło:

Utwórz Paczki Endpoint Security - Opcje

- Wpisz sugestywną nazwę i opis dla pakietów instalacyjnych, które chcesz stworzyć.

5. Wybierz docelową rolę komputera:
  - **Punkt końcowy.** Wybierz opcje do stworzenia pakietu dla stałego punktu końcowego.
  - **Endpoint Security Relay.** Wybierz tę opcję aby stworzyć pakiet dla punktu końcowego z rolą Endpoint Security Relay. Endpoint Security Relay jest specjalną rolą która instaluje uaktualnienia serwera na maszynach docelowych z Endpoint Security, który może być użyty do aktualizacji wszystkich innych klientów w sieci, obniżając zużycie pasma między maszynami klientów a Control Center.
6. Wybierz firmę w której pakiety instalacyjne będą używane.
7. Wybierz moduły ochrony, które chcesz zainstalować.
8. Z pola **Języki**, wybierz żądany język dla interfejsu klienta.
9. Wybierz **Skanuj przed instalacją** jeżeli jesteś pewny, że komputery są czyste przed instalacją Endpoint Security. Szybkie skanowanie w chmurze zostanie przeprowadzone na odpowiednich komputerach przed rozpoczęciem instalacji.
10. Endpoint Security jest zainstalowany w domyślnym katalogu instalacyjnym na wybranych komputerach. Wybierz **Użyj niestandardowej ścieżki instalacyjnej** Jeżeli chcesz zainstalować Endpoint Security 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. Kliknij **Dalej**.
13. W zależności od roli pakietu instalacyjnego (Endpoint lub Endpoint Security Relay), wybierz wpis do tych komputerów docelowych, które będą okresowo łączyć się z klientach w celu aktualizacji:
  - **Bitdefender Cloud**, jeśli chcesz aktualizować klientów bezpośrednio z Internetu.:
  - **Endpoint Security Relay**, jeżeli chcesz połączyć punkt końcowy z Endpoint Security Relay zainstalowanych w twojej sieci. Wszystkie komputery z rolą Endpoint Security Relay wykryte w twojej sieci pokażą się w tabeli poniżej. Wybierz Endpoint Security Relay który chcesz. Połączone punkty końcowe będą komunikować się z Control Center tylko przez określonego Endpoint Security Relay.


**WAŻNE**

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

14. Kliknij **Zapisz**.

Nowe pakiety instalacyjne pojawią się na liście pakietów docelowej firmy.

## Pobieranie i Instalacja Endpoint Security

1. Połącz z <https://gravityzone.bitdefender.com/> używając twojego konta z komputera na którym chcesz zainstalować ochronę.
2. Przejdź do strony **Sieć > Pakiety**.
3. Wybierz pakiety instalacyjne Endpoint Security, które chcesz pobrać.
4. Naciśnij przycisk  **Pobierz** po prawej stronie 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.** Pełny zestaw jest używany do instalacji ochrony na komputerach z wolnym połączeniem z internetem. Pobierz ten plik na połączony z internetem komputer, następnie rozprowdź go na innych komputerach używając zewnętrznych nośników pamięci lub udostępniając w sieci. Należy pamiętać, że są dostępne dwie wersje dla Windows: jedna dla systemu 32-bit i druga dla systemu 64-bit. Upewnij się, że instalujesz poprawną wersję oprogramowania.
5. Zapisz plik na komputerze.
6. Uruchom pakiet instalacyjny.



### Notatka

Aby instalacja działała, pakiety instalacyjne muszą działać używając uprawnień administratora lub na koncie administracyjnym.

7. Postępuj według instrukcji na ekranie.

Gdy Endpoint Security zostanie zainstalowany, komputer pokaże się w zarządzaniu w Control Center (Strona **Sieć**) w ciągu kilku minut.

## Instalacja Zdalna

Możesz lokalnie zainstalować pierwszego klienta dzięki roli Endpoint Security Relay, może to zająć kilka minut zanim inne komputery sieciowe zobaczą go w Control Center. Od tego momentu, możesz zdalnie zainstalować Endpoint Security na komputerach zarządzanych przez Ciebie przy użyciu zadania instalacji z Control Center.

Aby uczynić wdrożenie łatwiejszym, Security for Endpoints zawiera mechanizm automatycznego wykrywania sieci, która umożliwia wykrywanie komputerów, w tej samej sieci. Wykryte komputery są wyświetlane jako **niezarządzane komputery** na stronie **Sieci**.

Aby włączyć wyszukiwanie sieci i zdalną instalację, musisz mieć zainstalowany Endpoint Security przynajmniej na jednym komputerze w sieci. Ten komputer będzie używany do

skanowania sieci i instalacji Endpoint Security na niechronionych komputerach. Może zająć kilka minut zanim reszta komputerów s sieci pojawi się w Control Center.

### Wymagania zdalnej instalacji

Aby działało wykrywanie sieci, musi być spełniona liczba wymagań. Aby dowiedzieć się więcej, zobacz „[Jak działa wyszukiwanie sieci](#)” (p. 40).

Aby zdalna instalacja działała:

- Każdy komputer docelowy musi mieć włączone udostępnianie administracyjne. Skonfiguruj każdą docelową stację roboczą do używania zaawansowanej wymiany plików.
- Tymczasowo wyłącz Kontrolę Konta użytkownika na wszystkich komputerach z systemami operacyjnymi Windows, które zawierają tę funkcję zabezpieczeń (Windows Vista, Windows 7, Windows Server 2008, itp.). Jeśli komputery wchodzą w skład domeny, za pomocą polityki możesz wyłączyć kontrolę użytkownika zdalnie.
- Wyłącz lub zamknij zapora sieciową na komputerach. Jeśli komputery wchodzą w skład domeny, za pomocą polityki możesz wyłączyć zaporę sieciową Windows zdalnie.

### Działanie zadań zdalnej instalacji Endpoint Security


Aby uruchomić zdalną instalację:

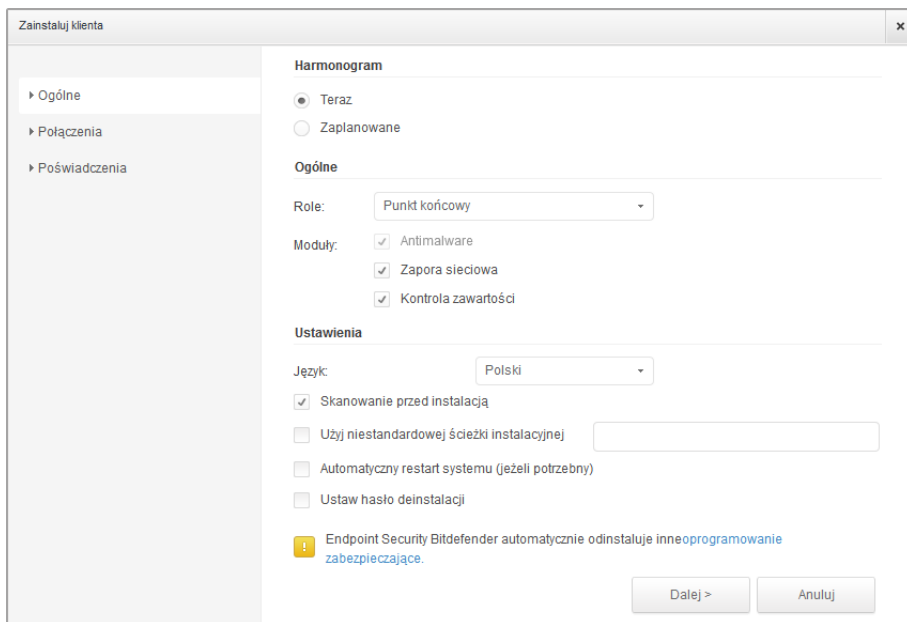
1. Połącz się i zaloguj do Control Center.
2. Przejdź do strony **Sieć**.
3. Wybierz żadaną grupę sieciową z lewego panelu bocznego. Jednostki należące do wybranej grupy są wyświetlone w prawym panelu bocznym tabeli.



#### Notatka

Opcjonalnie, możesz zastosować filtry, aby wyświetlić tylko komputery nie zarządzane. Naciśnij przycisk **Filtry** i wybierz poniższe opcje: **Niezarządzane** z kategorii **Bezpieczeństwo** i **Wszystkie elementy rekurencyjnie** z kategorii **Głębokość**.

4. Wybierz wpisy (komputery lub grupy komputerów), na których chcesz zainstalować ochronę.
5. Kliknij przycisk  **Zadania** po prawej stronie tabeli i wybierz **Instaluj klienta**. Kreator **Klienta Instalacji** został wyświetlony.



Instalowanie Endpoint Security z menu zadań

## 6. Skonfiguruj opcje instalacji:

- Harmonogram 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.

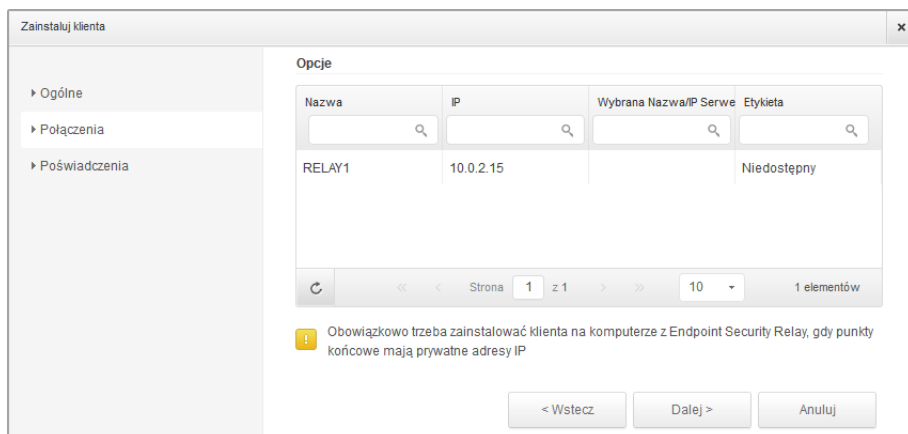


### Notatka

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.

- Wybierz moduły ochrony, które chcesz zainstalować. Należy pamiętać, że tylko ochrona antymalware jest dostępna dla systemów operacyjnych serwera.
- Z pola **Języki**, wybierz żądany język dla interfejsu klienta.

- Wybierz **Skanuj przed instalacją** jeżeli jesteś pewny, że komputery są czyste przed instalacją Endpoint Security. Szybkie skanowanie w chmurze zostanie przeprowadzone na odpowiednich komputerach przed rozpoczęciem instalacji.
- Endpoint Security jest zainstalowany w domyślnym katalogu instalacyjnym na wybranych komputerach. Wybierz **Użyj niestandardowej ścieżki instalacyjnej** Jeżeli chcesz zainstalować Endpoint Security 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.
- Podczas cichej instalacji, komputer jest skanowany w poszukiwaniu malware. Czasami, system może potrzebować restartu aby ukończyć usuwanie malware.  
Wybierz **Automatyczny restart (jeżeli potrzebny)** aby upewnić się, że wykryte malware zostało w pełni usunięte przed instalacją. W przeciwnym razie instalacja może się nie powieść.
- Jeżeli chcesz, możesz ustawić hasło aby zapobiec przed usunięciem ochrony przez użytkowników. Wybierz **Ustaw hasło do odinstalowania** i podaj hasło w odpowiednim polu.
- Kliknij **Dalej**.
- Na karcie **Połączenie** znajduje się lista punktów końcowych z rolą Endpoint Security Relay zainstalowanych w sieci. Każdy nowy klient musi być połączony z przynajmniej jednym Endpoint Security Relay z tej samej sieci, który będzie służyć do komunikacji i aktualizacji serwera. Wybierz Endpoint Security Relay jeżeli chcesz połączyć się z nowym klientem.



## 7. Kliknij **Dalej**.



8. W sekcji **Menadżer poświadczeń**, wybierz poświadczenia administracyjne potrzebne do zdalnego uwierzytelnienia na wybranych punktach końcowych. Możesz dodać potrzebne 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](#).



### Notatka

Ostrzeżenie jest wyświetlane tak długo jak nie wybierzesz żadnych poświadczeń. Ten krok jest obowiązkowy dla instalacji zdalnych Endpoint Security na komputerach.

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

Użytkownik powinien użyć formy DOMENAWAZWA UŻYTKOWNIKA, gdzie DOMENA jest nazwą NetBios domeny.

Aby dodać wymagane poświadczenia OS:

- a. Podaj nazwę użytkownika i hasło dla konta administracyjnego dla docelowego systemu operacyjnego w odpowiednich polach. Opcjonalnie, możesz dodać opis, który pomoże Ci zidentyfikować prościej dane konto. Jeżeli komputery są w domenie, wystarczy wprowadzić poświadczenia administratora domeny.

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



### Notatka

Określone poświadczenia, zostaną zapisane automatycznie w menadżerze poświadczeń, więc nie będziesz musiał wprowadzać ich ponownie następnym razem.

- b. Kliknij przycisk **+** **Dodaj** . Konto jest dodane do listy poświadczeń.
  - c. Zaznacz pola odpowiadające kontom które chcesz używać.
9. Kliknij **Zapisz**. Pojawi się nowa wiadomość potwierdzająca.

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

### 4.1.3. Organizowanie Komputerów (Opcjonalnie)

Sieci firmowe są wyświetlone w lewym panelu strony **Sieć**. To jest domyślna grupa administracyjna dla każdej firmy. Wszystkie z tych chronionych lub wykrytych komputerów są automatycznie umieszczone w tej grupie.

Jeżeli zarządzasz dużą liczbą komputerów (dziesiątkami lub więcej), prawdopodobnie będziesz potrzebował uporządkować je w grupach. Organizowanie komputerów w grupach pomaga zarządzać bardziej efektywnie. Główną zaletą jest to, że możesz korzystać z polityk grupy w celu spełnienia różnych wymogów bezpieczeństwa.

Możesz uporządkować komputery przez tworzenie grup w domyślnej grupie firmy i przeniesienie komputerów do odpowiedniej grupy.

Przed rozpoczęciem tworzenia grup, pomyśl dlaczego ich potrzebujesz i wymyśl schemat grup. Na przykład, możesz grupować komputery opierając się na jednej lub na kombinacji następujących kryteriów:

- Struktura organizacyjna (Sprzedaż, Marketing, Zapewnienie Jakości, Zarządzanie itp.).
- Potrzeby bezpieczeństwa (Komputery stacjonarne, Laptopy, Serwery, itd.).
- Lokalizacja (Siedziba Główna, Biura Lokalne, Pracownicy zdalni, Biura Domowe itp.).



#### Notatka

- Stworzone grupy mogą zawierać zarówno komputery i inne grupy.
- Kiedy wybierasz grupę w lewym panelu, możesz zobaczyć wszystkie komputery z wyjątkiem tych w podgrupach. Aby zobaczyć komputery zawarte w grupie i wszystkich jej podgrupach, naciśnij na menu Filtry znajdujące się poniżej tabeli i wybierz **Rodzaje > Komputery** i **Głębokość > Wszystkie elementy rekurencyjne**.

Aby uporządkować sieci klientów w grupach:

1. Przejdź do strony **Sieć**.
2. W panelu po lewej stronie, w **Firmy**, wybierz klient firmy jakim chcesz zarządzać.



#### Notatka

Dla partnerów firmowych w twoim koncie masz prawa zarządzania siecią, wybierz grupę **Sieci**.

3. Naciśnij przycisk **+** **Dodaj grupę** u góry lewego panelu bocznego.

4. Podaj sugestywną nazwę dla grupy i naciśnij **OK**. Nowa grupa jest wyświetlona w odpowiedniej firmie.
5. Wykonaj wcześniejsze kroki aby stworzyć dodatkowe grupy.
6. Przenieś komputery z grupy administracyjnej do odpowiedniej grupy:
  - a. Zaznacz pola odpowiadające komponentom które mają być przeniesione.
  - b. Przeciągnij i upuść wybrane elementy do pożądanej grupy w lewym panelu bocznym.

## 4.1.4. Tworzenie i przypisywanie polityki bezpieczeństwa

### 4.1.4. Tworzenie i przypisywanie polityki bezpieczeństwa

Po zainstalowaniu ochrony Security for Endpoints może być skonfigurowana i zarządzana z Control Center używając polityk bezpieczeństwa. Polityka określa ustawień bezpieczeństwa, które należy zastosować na docelowych komputerach.

Natychmiast po instalacji, komputerom zostanie przypisana domyślna polityka, która jest wstępnie skonfigurowana z zalecanymi ustawieniami ochrony. Aby sprawdzić ustawienia domyślnej ochrony, przejdź do strony **Polityki** i naciśnij domyślną nazwę polityki. Możesz zmienić ustawienia ochrony jakie potrzebujesz, również skonfigurować dodatkowe funkcje ochrony, tworząc i przypisując dostosowane polityki.



#### Notatka

Nie możesz modyfikować ani usuwać domyślnej polityki. Możesz użyć go tylko jako szablonu dla tworzenia nowej polityki.

Możesz stworzyć tak wiele polityk bazujących na wymaganiach bezpieczeństwa ile będziesz potrzebować. Na przykład, możesz skonfigurować inne polityki dla biurowych stacji roboczych, laptopów i serwerów. Innym podejściem jest stworzenie odrębnych zasad dla każdej z sieci klienta.

To jest to co potrzebujesz, żeby wiedzieć o politykach:

- Polityki są tworzone na stronie **Polityki** i przypisane do punktów końcowych ze strony **Sieć**.
- Punkty końcowe mogą tylko mieć aktywną jedną politykę w tym samym czasie.
- Polityki są przekazywane do docelowych komputerów natychmiast po stworzeniu lub modyfikacji. Ustawienia powinny być zastosowane na punktach końcowych w mniej niż minutę (jeżeli są online). Jeżeli komputery są offline, ustawienia nie będą stosowane tak długo jak nie pojawią się online.
- Polityka ma zastosowanie tylko do zainstalowanych modułów ochrony. Należy pamiętać, że tylko ochrona antymalware jest dostępna dla systemów operacyjnych serwera.

- Nie możesz edytować polityk stworzonych przez innych użytkowników (chyba że właściciel polityki dopuszcza to w ustawieniach polityki), ale nie możesz zmienić ich przypisując obiektom docelowym innej polityki.
- Komputery na koncie firmy mogą być zarządzane przez polityki przez administratora firmy i przez partnera, który stworzył konto. Polityki stworzone z konta partnera nie mogą być edytowane z konta firmy.

Aby utworzyć nową politykę:

1. Przejdź do strony **Polityki**.
2. Kliknij przycisk **+ Dodaj** po prawej stronie tabeli. Ta Komenda tworzy nową politykę używając domyślnego szablonu polityki.
3. Podaj sugestywną nazwę dla polityki. Wybierając nazwę, weź pod uwagę przeznaczenie i cel polityki.
4. Następnie, skonfiguruj ustawienia polityki. Domyślne ustawienia bezpieczeństwa są zalecane w większości sytuacji.
5. Kliknij **Zapisz**. Nowa polityka znajduje się na liście w tabeli **Polityki**.

Jak zdefiniowałeś niezbędne polityki w sekcji **Polityki**, możesz przypisać je do obiektów sieci w sekcji **Sieć**.

Wszystkie obiekty sieciowe są początkowo przypisane do domyślnej polityki.



#### Notatka

Możesz przypisać tylko polityki które stworzyłeś. Aby przypisać politykę stworzoną przez innego użytkownika, możesz ją najpierw sklonować na stronie **Polityki**.

Aby przypisać politykę:

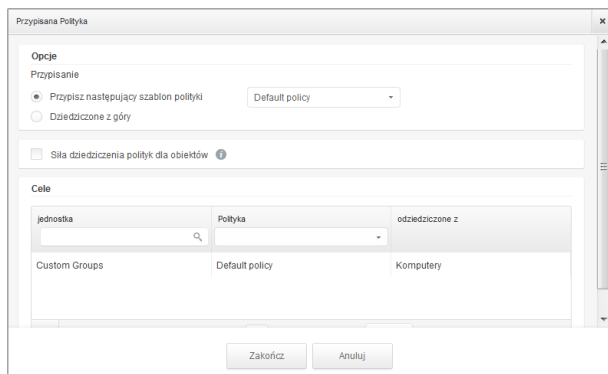
1. Przejdź do strony **Sieć**.
2. Zaznacz pole żądanego obiektu sieciowego. Możesz wybrać jeden z kilku obiektów tylko tego samego poziomu.
3. Kliknij przycisk **Przypisz Polityki** po prawej stronie tabeli.



#### Notatka

Możesz również nacisnąć prawym klawiszem mysz na grupę w drzewie sieci i wybrać **Przypisz politykę** z menu podręcznego.

Wyświetlono okno **Przypisania polityki**:



Ustawienia Przypisania Polityki

#### 4. Skonfiguruj przypisanie ustawień polityki dla wybranych obiektów:

- Zobacz przypisanie obecnej polityki dla wybranych obiektów w tabeli poniżej sekcji **Cele**.
- **Przypisz następujący szablon polityki**. wybierz tę opcje aby przypisać obiekty docelowe z jedną polityką z wyświetlonego menu po prawej stronie. Tylko polityki stworzone z twojego konta będą dostępne w menu.
- **Dziedziczone z góry**. Wybierz opcje **Dziedziczenie z góry** aby przypisać wybrane obiekty sieciowe z grupy macierzystej polityki.
- **Siła dziedziczenia polityk dla obiektów**. Domyślnie, każdy obiekt sieciowy dziedziczy polityką grupy macierzystej. Jeżeli zmieniasz grupę polityki, będzie miało to wpływ na wszystkie dzieci tej grupy, z wyjątków członków grupy ze specjalnie przypisaną inną polityką.

Wybierz opcje **Dziedziczenie polityki przez obiekty** aby zastosować wybraną politykę dla grupy, w tym grup podrzędnych przypisanych do innej polityki. W tym przypadku, tabela poniżej wyświetla wybrane grupy podzędne, które nie dziedziczą polityki grupy.

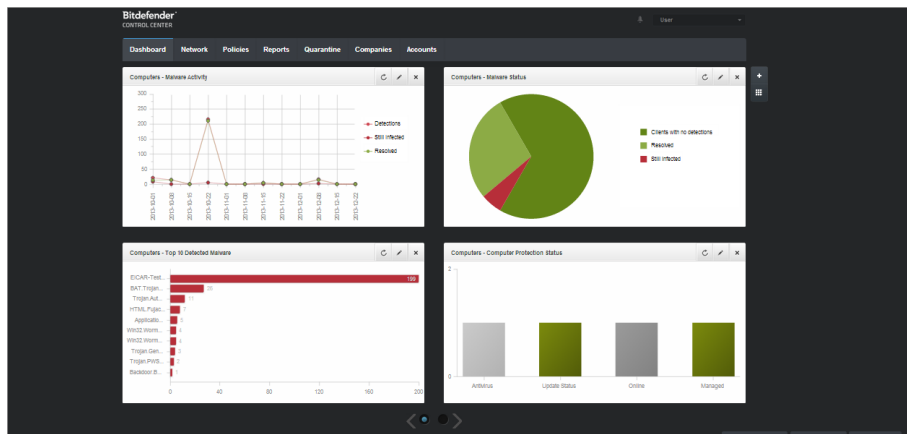
#### 5. Naciśnij **Zakończ** aby zapisać i potwierdzić zmiany.

Polityki są wysyłane do docelowych obiektów sieci zaraz po zmianie polityki przypisanej lub później modyfikując ustawienia polityki. Ustawienia powinny być zastosowane na obiektach sieci w mniej niż minutę (jeżeli są one online). Jeżeli obiekty sieciowe nie są online, ustawienia będą zastosowane jak tylko pojawią się online.

Aby sprawdzić czy polityka została poprawnie przypisana, przejdź do strony **Siec** i naciśnij nazwę obiektu jaki cię interesuje w wyświetlonym oknie **Szczegóły**. Sprawdź sekcję **Polityka** aby zobaczyć stan obecnej polityki. Jeżeli w oczekiwaniu na stan, polityka nie została zastosowana do obiektu docelowego.

## 4.2. Monitorowanie stanu bezpieczeństwa

Głównym nadzieniem monitorowania Security for Endpoints w Control Center jest konfigurowalny wyświetlacz zapewniający szybki przegląd bezpieczeństwa sieci.



Panel



Sprawdzaj stronę **Pulpit Nawigacyjny** regularnie aby zobaczyć w czasie rzeczywistym informację o stanie bezpieczeństwa twojej sieci.

Portlety panelu wyświetlają różne informacje dotyczące bezpieczeństwa, używając łatwych do przeczytania wykresów, pozwalając w ten sposób szybko zidentyfikować wszystkie problemy, które mogą wymagać uwagi.

To jest to czego potrzebujesz wiedzieć o zarządzaniu pulpitem nawigacyjnym:

- Control Center ma kilka wstępnie zdefiniowanych portletów w panelu. Możesz również dodać więcej portletów używając przycisk **+** **Dodaj Portlet** po prawej stronie panelu nawigacyjnego.
- Każdy portlet w panelu zawiera szczegółowy raport w tle, dostępny za pomocą jednego kliknięcia na wykresie.
- Informacje wyświetlone przez portlety zależą tylko od obiektów sieci w twoim koncie. Możesz dostosować informacje wyświetlane przez portlet (rodzaj, interwał raportów, cele) przez naciśnięcie ikony **Edytuj Portlet** w pasku tytułowym.

Na przykład, możesz skonfigurować portlety aby wyświetlały informacje w pewnej firmie w twojej sieci.


- Możesz w łatwy sposób usunąć każdy portlet naciskając ikonę  **Usuń** na pasku tytułu. Jeżeli usuniesz portlet, nie będziesz mógł go już więcej odzyskać. Jednak, możesz utworzyć inny portlet z takimi samymi ustawieniami.
- Kliknij pozycje legendy wykresu, gdy jest dostępna, aby ukryć lub wyświetlić odpowiednią zmienną na wykresie.
- Możesz zamienić miejscem portlety pulpitu nawigacyjnego aby lepiej dopasować go do swoich potrzeb, przez naciśnięcie przycisku  **Reorganizuj Portlety** po prawej stronie pulpitu nawigacyjnego. Możesz przeciągnąć i upuścić portlety na odpowiednią pozycję.
- Portlety są wyświetlane w czterech grupach. Użyj suwaka na dole strony aby przemieszczać się pomiędzy grupami portletów.

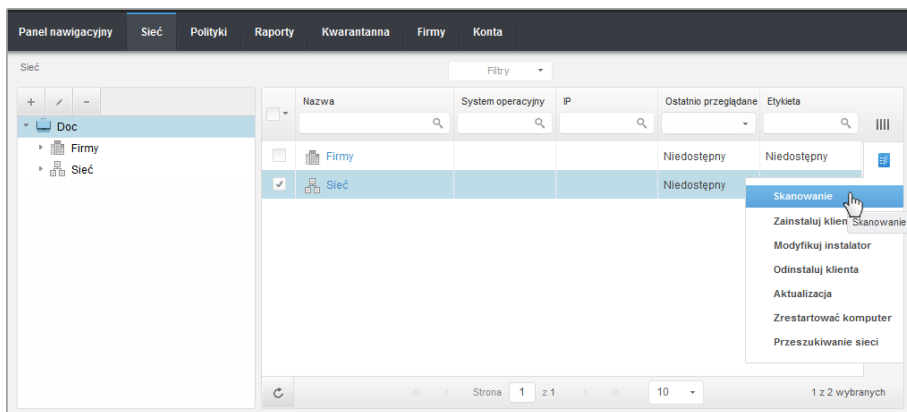
## 4.3. Skanowanie zarządzanych komputerów

Są trzy drogi do skanowania komputerów chronionych przez Endpoint Security:

- Użytkownik logując się na komputerze może rozpocząć skanowanie z interfejsu użytkownika Endpoint Security.
- Możesz stworzyć harmonogram zadań skanowania używając polityki.
- Natychmiast uruchom zadanie skanowania z konsoli.

Aby uruchomić zadanie skanowania na kilku komputerach:

1. Przejdź do strony **Sieć**.
2. Wybierz żądaną grupę sieciową z lewego panelu bocznego. Wszystkie komputery z wybranej grupy są wyświetlone w prawym panelu bocznym.
3. Wybierz elementy, które chcesz przeskanować. Możesz wybrać niektóre zarządzane komputery lub całe grupy.
4. Naciśnij przycisk  **Zadanie** po prawej stronie tabeli i wybierz **Skanowanie**. Wyświetlone zostanie okno konfiguracji.



Zadanie skanowania komputerów

5. W zakładce **Ogólne**, wybierz rodzaj skanowania z menu **Rodzaj**:

- **Szybkie Skanowanie** sprawdza czy nie działa złośliwe oprogramowanie w systemie, nie wykonuje żadnych działań. Jeżeli malware zostało znalezione podczas Szybkiego Skanowania, musisz uruchomić Pełne Skanowanie Systemu aby usunąć wykryte malware.
- **Pełne Skanowanie** sprawdza cały komputer w poszukiwaniu wszystkich rodzajów złośliwego oprogramowania zagrażającego bezpieczeństwu, takiego jak wirusy, oprogramowanie typu spyware/adware, rootkity i inne.
- **Niestandardowe skanowanie** dopuszcza wybranie lokacji, które mają zostać przeskanowane i skonfigurować opcje skanowania.

6. Kliknij **Zapisz**, aby utworzyć zadanie skanowania. Pojawi się nowa wiadomość potwierdzająca.



### Notatka

Po utworzeniu, zadanie skanowania od razu uruchomi się na komputerach będących online w sieci.

Jeżeli komputer jest offline, zostanie przeskanowany jak tylko znajdzie się z powrotem w sieci.

7. Możesz zobaczyć i zarządzać zadaniami na stronie **Sieć > Zadania**.



## 5. Otrzymywanie pomocy

Aby znaleźć dodatkowe środki pomocy lub uzyskać pomoc od Bitdefender:

- Naciśnij link **Pomoc i Wsparcie** w prawym dolnym rogu Control Center.
- Przejdź do [Centrum wsparcia online](#).

Aby otworzyć wiadomość e-mail wsparcia, użyj [tej strony](#).

# A. Wymagania

## A.1. Wymagania Security for Endpoints

### A.1.1. Wspierane systemy operacyjne

Security for Endpoints aktualnie chroni następujące systemy operacyjne:

#### **Systemy operacyjne stacji roboczych:**

- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista z dodatkiem Service Pack 1
- Windows XP z dodatkiem Service Pack 2 64-bit
- Windows XP z Service Pack 3
- Mac OS X Lion (10.7.x)
- Mac OS X Mountain Lion (10.8.x)
- Mac OS X Mavericks (10.9.x)

#### **Tablet i wbudowane systemy operacyjne:**

- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Standard 7
- Windows Embedded Compact 7
- Windows Embedded POSReady 7
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 2009
- Windows Embedded Standard 2009
- Windows XP z wbudowanym Service Pack 2
- Windows XP Tablet PC Edition\*

\*Konkretne moduły systemu operacyjnego muszą być zainstalowane na Security for Endpoints, aby pracował.

#### **Systemy operacyjne serwera:**

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

- Windows Small Business Server (SBS) 2003
- Windows Server 2003 R2
- Windows Server 2003 z Service Pack 1
- Windows Home Server

## A.1.2. Wymagania Sprzętowe

- Procesor kompatybilny z Intel® Pentium:

### Systemy operacyjne stacji roboczych

- 1 GHz lub szybszy dla Microsoft Windows XP SP3, Windows XP SP2 64 bit i Windows 7 Enterprise (32 i 64 bit)
- 2 GHz lub szybszy dla Microsoft Windows Vista SP1 lub wyższy (32 i 64 bit), Microsoft Windows 7 (32 i 64 bit), Microsoft Windows 7 SP1 (32 i 64bit), Windows 8
- 800 MHz lub szybszy dla Microsoft Windows Embedded Standard 7 SP1, Microsoft Windows POSReady 7, Microsoft Windows POSReady 2009, Microsoft Windows Embedded Standard 2009, Microsoft Windows XP Embedded z Service Pack 2, Microsoft Windows XP Tablet PC Edition

### Systemy operacyjne serwera

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

- **Wolna pamięć RAM:**

- Dla Windows: minimum 512 MB, rekomendowane 1 GB
- Dla MAC: minimum 1 GB

- **miejsce HDD:**

- 1.5 GB wolnego miejsca na dysku twardym



### Notatka

Wymagane jest co najmniej 6 GB wolnego miejsca na dysku dla podmiotów z rolą Endpoint Security Relay, gdzie będą przechowywać wszystkie aktualizacje i pakiety instalacyjne.

## A.1.3. Obsługiwane przeglądarki

Przeglądarka bezpieczeństwa Endpoint jest weryfikowana do pracy z następującymi przeglądarkami:

- Internet Explorer 8+
- Mozilla Firefox 8+
- Google Chrome 15+
- Safari 4+

## A.1.4. Porty Komunikacji Small Office Security

Poniższa tabela zawiera informacje na temat portów używanych przez składniki Small Office Security:

Port	Użycie
<b>80 (HTTP) / 443 (HTTPS)</b>	Port używany do uzyskania dostępu do konsoli webowej Control Center.
<b>80</b>	Port serwera aktualizacji.
<b>8443 (HTTPS)</b>	port używany przez klienta/agenta oprogramowania do połączenia z Serwerem komunikacji.
<b>7074 (HTTP)</b>	Komunikacja z Endpoint Security Relay (jeżeli dostępne)

Aby otrzymać więcej informacji na temat portów Small Office Security, patrz [ten artykuł KB](#).

## A.2. Jak działa wyszukiwanie sieci

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

Security for Endpoints opiera się na **Usłudze Microsoft Computer Browser** do wyszukiwania sieci. Usługa przeglądania komputera jest 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
\\SCIREFL
\\SCIREFMB
\\SCIREFMN
\\SCIREFMP
\\SCIREFYS
```

Polecenie zobacz sieć

Aby włączyć wyszukiwanie sieci, musisz mieć zainstalowany Endpoint Security 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 zaangażowana w działanie operacji usługi Przeglądania Komputerów Endpoint Security wysyła zapytanie tylko do usługi Przeglądarki Komputera dla listy stacji roboczych i serwisów obecnie widocznych w sieci i wysyła je do Control Center. Control Center przetwarza listy przeglądania, dołączając nowo wykryte komputery do listy **Niezarządzane Komputery**. Wcześniej wykryte komputery nie są usunięte po ponownym zapytaniu wykrywania sieci, musisz wyłączyć & ręcznie; usuń komputery, które nie są już w sieci.

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

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

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 Endpoint Security w każdym obszarze, aby wykonać zadanie. Widocznym obszarem jest grupa komputerów, które wykrywają siebie nawzajem. Zazwyczaj, widoczny obszar jest definiowany przez grupę robocza lub domenę, ale to zależy od topologii sieci i konfiguracji. W niektórych przypadkach, widoczność obszaru może zależeć od wielu domen i grup roboczych.

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

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

### A.2.1. 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.

## A.2.2. Wymagania wyszukiwania sieci

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

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

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

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

Komputery z których Endpoint Security wysyła zapytania do usługi Przeglądarki Komputerów 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.