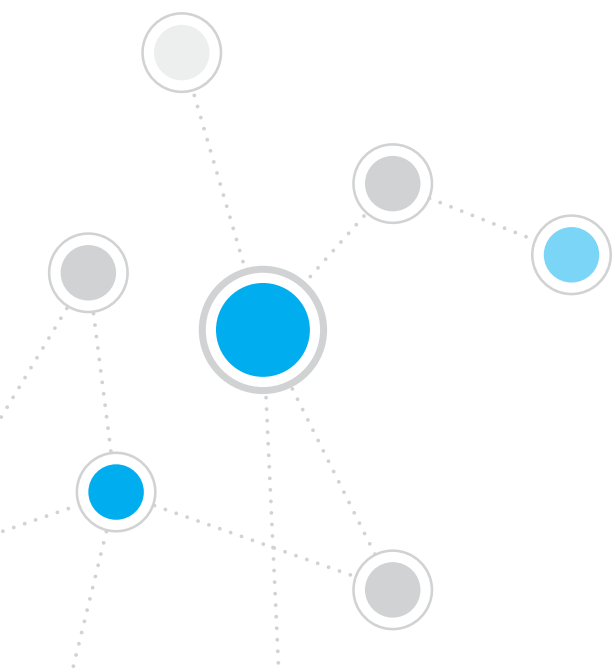




# ForeScout CounterACT<sup>®</sup> 7

Pojedyncze urządzenie CounterACT

## **Instrukcja szybkiej instalacji**



# Spis treści

<b>Witamy w ForeScout CounterACT® w wersji 7</b>	<b>3</b>
Zawartość pakietu CounterACT	3
<b>Informacje ogólne</b>	<b>4</b>
<b>1. Utworzenie planu wdrożenia</b>	<b>5</b>
Decyzja dotycząca miejsca wdrożenia urządzenia	5
Połączenia interfejsu urządzenia	5
<b>2. Konfiguracja przełącznika</b>	<b>8</b>
A. Opcje połączenia przełącznika	8
B. Uwagi dotyczące ustawiania przełącznika	9
<b>3. Podłączenie kabli sieciowych i włączenie zasilania</b>	<b>10</b>
A. Rozpakowanie urządzenia i podłączenie kabli	10
B. Rejestracja przypisań interfejsu	11
C. Włączenie urządzenia	11
<b>4. Konfiguracja urządzenia</b>	<b>12</b>
Licencja	14
Wymagania dotyczące połączenia sieciowego	14
<b>5. Zdalne zarządzanie</b>	<b>15</b>
Konfiguracja modułu iDRAC	15
Podłączenie modułu do sieci	18
Logowanie do modułu iDRAC	18
<b>6. Sprawdzenie łączności</b>	<b>19</b>
Sprawdzenie połączenia interfejsu zarządzania	19
Sprawdzenie łączności przełącznika/urządzenia	19
Wykonanie testu ping	20
<b>7. Konfiguracja aplikacji CounterACT Console</b>	<b>21</b>
Instalacja aplikacji CounterACT Console	21
Logowanie	22
Wykonanie konfiguracji początkowej	22
<b>Informacje kontaktowe</b>	<b>24</b>

# Witamy w ForeScout CounterACT® w wersji 7

ForeScout CounterACT to urządzenie zabezpieczające zapewniające bezpieczeństwo fizyczne lub wirtualne, które dynamicznie identyfikuje i ocenia urządzenia oraz aplikacje sieciowe w momencie, gdy łączą się one z siecią użytkownika. Ponieważ rozwiązanie CounterACT nie wymaga zastosowania agentów, umożliwia obsługę rozmaitych urządzeń — zarządzanych i niezarządzanych, znanych i nieznanych, stacjonarnych i mobilnych, osadzonych i wirtualnych. Urządzenie CounterACT szybko określa użytkownika, właściciela, system operacyjny, konfigurację urządzenia, oprogramowanie, usługi, stan poprawek i obecność agentów zabezpieczeń. Następnie zapewnia korygowanie, kontrolę i stały monitoring tych urządzeń, w miarę ich podłączania i opuszczania przez sieć. Spełnia wszystkie te funkcje, jednocześnie zapewniając płynną integrację z istniejącą infrastrukturą IT.



## ***W niniejszym przewodniku opisano instalację pojedynczego autonomicznego urządzenia CounterACT.***

Aby uzyskać bardziej szczegółowe informacje lub wiadomości na temat wdrożenia wielu urządzeń w celu zapewnienia zabezpieczenia sieci w skali firmy należy zapoznać się z *Przewodnikiem instalacji urządzenia CounterACT* oraz *Instrukcją obsługi aplikacji Console*. Te dokumenty są umieszczone na dysku CD dołączonym do urządzenia urządzenia CounterACT w katalogu /docs.

Ponadto można skorzystać z witryny internetowej pomocy pod adresem: <http://www.forescout.com/support>, aby uzyskać najnowszą dokumentację, artykuły bazy wiedzy oraz aktualizacje dla urządzenia.

## **Zawartość pakietu CounterACT**

- Urządzenie CounterACT
- Instrukcja szybkiej instalacji
- Dysk CD CounterACT zawierający oprogramowanie Console, Instrukcję obsługi aplikacji CounterACT Console oraz Instrukcję instalacji
- Dokument gwarancyjny
- Wsporniki montażowe
- Kabel zasilający
- Kabel połączeniowy konsoli DB9 (tylko dla połączeń szeregowych)

# Informacje ogólne

Aby skonfigurować urządzenie CounterACT, należy wykonać następujące czynności:

1. Utworzenie planu wdrożenia
2. Skonfigurowanie przełącznika
3. Podłączenie kabli sieciowych i zasilania
4. Skonfigurowanie urządzenia
5. Zdalne zarządzanie
6. Sprawdzenie łączności
7. Skonfigurowanie aplikacji CounterACT Console

# 1. Utworzenie planu wdrożenia

Przed przeprowadzeniem instalacji należy zdecydować, gdzie urządzenie zostanie wdrożone i zapoznać się z połączeniami interfejsu urządzenia.

## Decyzja dotycząca miejsca wdrożenia urządzenia

Określenie prawidłowej lokalizacji dla urządzenia ma kluczowe znaczenie dla prawidłowego wdrożenia i optymalnych parametrów systemu CounterACT. Prawidłowa lokalizacja jest uzależniona od zakładanych celów wdrożenia i reguł dostępu do sieci. Urządzenie powinno mieć możliwość monitorowania ruchu właściwego z uwagi na żądane reguły. Przykładowo jeśli reguły zależą od monitorowania zdarzeń autoryzacji z punktów końcowych do firmowych serwerów uwierzytelnień, urządzenie należy zainstalować tak, aby widziało ruch z punktów końcowych płynący do serwerów uwierzytelnień.

Aby uzyskać więcej informacji na temat instalacji i wdrożenia, należy zapoznać się z Instrukcją instalacji urządzenia CounterACT znajdującą się na dysku CD dołączonym do urządzenia CounterACT.

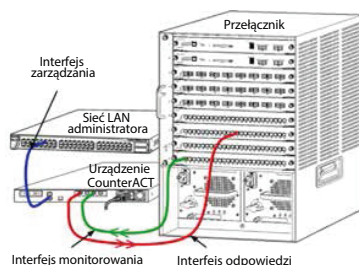
## Połączenia interfejsu urządzenia

Konfiguracja urządzenia obejmuje ogólnie trzy połączenia z przełącznikiem sieciowym.

### Interfejs zarządzania

Ten interfejs umożliwia zarządzanie urządzeniem CounterACT i wykonywanie zapytań oraz głębokiej kontroli punktów końcowych. Interfejs musi być połączony z portem przełącznika posiadającym dostęp do wszystkich punktów końcowych sieci.

Każde urządzenie wymaga pojedynczego połączenia zarządzania z siecią. Dla tego połączenia wymagany jest adres IP w lokalnej sieci LAN i dostęp do portu 13000/TCP z komputerów, na których będzie uruchomiony program zarządzający aplikacji CounterACT Console. Interfejs zarządzania musi mieć dostęp do następujących elementów sieci:



Port	Usługa	Do lub z urządzenia CounterACT	Funkcja
22/TCP	SSH	Do	Umożliwia dostęp do interfejsu wiersza polecenia urządzenia CounterACT.
2222/TCP			(Wysoka dostępność) Umożliwia dostęp do fizycznego urządzenia CounterACT, stanowiącego część klastra wysokiej dostępności. Portu 22/TCP należy używać w celu uzyskania dostępu do udostępnionego (wirtualnego) adresu IP klastra.

Port	Usługa	Do lub z urządzenia CounterACT	Funkcja
25/TCP	SMTP	Z	Wykorzystywany do wysyłania poczty z urządzenia CounterACT
53/UDP	DNS	Z	Umożliwia urządzeniu CounterACT rozpoznawanie wewnętrznych adresów IP.
80/TCP	HTTP	Do	Umożliwia przekierowywanie HTTP
123/UDP	NTP	Z	Umożliwia urządzeniu CounterACT dostęp do serwera czasu NTP. Urządzenie CounterACT używa domyślnie serwera ntp.foreScout.net.
135	WMI	Z	Umożliwia urządzeniu CounterACT wykonywanie głębokiego badania i kontroli punktów końcowych systemu Windows z wykorzystaniem WMI.
139/TCP	SMB, MS-RPP	Z	Umożliwia zdalną kontrolę punktów końcowych Windows (dla punktów końcowych z systemem Windows 7 i wcześniejszymi systemami).
445/TCP			Umożliwia zdalną kontrolę punktów końcowych Windows.
161/UDP	SNMP	Z	<p>Umożliwia urządzeniu CounterACT komunikację ze sprzętem tworzącym infrastrukturę sieciową, takim jak przełączniki i routery.</p> <p>Aby uzyskać informacje dotyczące konfigurowania protokołu SNMP, należy zapoznać się z <i>Instrukcją obsługi aplikacji CounterACT Console</i>.</p>
162/UDP	SNMP	Do	<p>Umożliwia urządzeniu CounterACT odbieranie ze sprzętu tworzącego infrastrukturę sieciową, takiego jak przełączniki i routery, pułapek SNMP.</p> <p>Aby uzyskać informacje dotyczące konfigurowania protokołu SNMP, należy zapoznać się z <i>Instrukcją obsługi aplikacji CounterACT Console</i>.</p>
443/TCP	HTTPS	Do	Umożliwia przekierowywanie HTTP z wykorzystaniem protokołu TLS
2200/TCP	Secure Connector	Do	<p>Umożliwia utworzenie przez narzędzie SecureConnector bezpiecznego (z szyfrowaniem SSH) połączenia z urządzeniem z komputerów z systemem Macintosh/Linux.</p> <p><i>SecureConnector</i> to agent oparty na skryptach, który umożliwia zarządzanie punktami końcowymi z systemem Macintosh i Linux, gdy są one połączone z siecią.</p>

10003/TCP	Secure Connector for Windows	Do	Umożliwia utworzenie przez narzędzie SecureConnector bezpiecznego (z szyfrowaniem TLS) połączenia z urządzeniem z komputerów z systemem Windows. <i>SecureConnector</i> to agent, który umożliwia zarządzanie punktami końcowymi z systemem Windows, gdy są one połączone z siecią. Zapoznaj się z <i>Instrukcją obsługi aplikacji CounterACT Console</i> , aby uzyskać więcej informacji o narzędziu SecureConnector.
			Gdy narzędzie SecureConnector łączy się z urządzeniem lub Menedżerem korporacyjnym, jest ono przekierowywane do urządzenia, do którego przydzielony jest jego host. Należy upewnić się, że ten port jest otwarty dla wszystkich urządzeń i Menedżera korporacyjnego, aby umożliwić zachowanie przejrzystej mobilności w ramach organizacji.
13000/TCP	CounterACT	Do	Umożliwia połączenie z urządzeniem z aplikacji Console.  W przypadku systemów z wieloma urządzeniami CounterACT umożliwia połączenie z Menedżerem korporacyjnym z aplikacji Console i z każdym z urządzeń z Menedżera korporacyjnego.

## Interfejs monitorowania

To połączenie umożliwia urządzeniu monitorowanie i śledzenie ruchu w sieci.

Ruch jest kopiowany do portu na przełączniku i monitorowany przez urządzenie.

W zależności od liczby kopiowanych sieci VLAN ruch może mieć znacznik VLAN 802.1Q lub go nie mieć.

- **Pojedyncza sieć VLAN (bez znacznika):** Jeśli monitorowany ruch jest generowany z pojedynczej sieci VLAN, kopiowany ruch nie musi mieć znacznika VLAN.
- **Wiele sieci VLAN (ze znacznikami):** Jeśli monitorowany ruch pochodzi z więcej niż jednej sieci VLAN, kopiowany ruch *musi* mieć znacznik VLAN 802.1Q.

Jeśli dwa przełączniki są połączone jako nadmiarowa para, urządzenie musi monitorować ruch z obu.

Dla interfejsu monitorowania nie jest wymagany adres IP.

## Interfejs odpowiedzi

Za pomocą tego interfejsu urządzenie odpowiada na ruch. Ruch odpowiedzi służy do ochrony przed złośliwą aktywnością i wykonywania działań związanych z regułami kontroli dostępu do sieci. Te działania mogą obejmować przykładowo przekierowywanie przeglądarek sieciowych lub wykonywanie blokad zapory.

Powiązana konfiguracja portu przełącznika zależy od monitorowanego ruchu.

- **Pojedyncza sieć VLAN (bez znacznika):** Jeśli monitorowany ruch jest generowany z pojedynczej sieci VLAN, interfejs odpowiedzi musi być skonfigurowany jako część tej samej sieci VLAN. W takim przypadku dla urządzenia wymagany jest jeden adres IP w tej sieci VLAN.
- **Wiele sieci VLAN (ze znacznikami):** Jeśli monitorowany ruch pochodzi z więcej niż jednej sieci VLAN, również interfejs odpowiedzi musi być skonfigurowany ze znacznikami 802.1Q dla tych samych sieci VLAN. Urządzenie musi mieć adres IP dla każdej zabezpieczonej sieci VLAN.

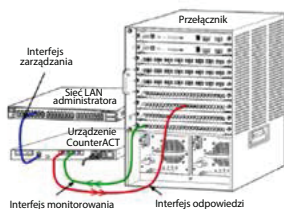
## 2. Konfiguracja przełącznika

### A. Opcje połączenia przełącznika

Urządzenie zostało zaprojektowane z myślą o płynnej integracji z szerokim zakresem środowisk sieciowych. W celu powodzenia integracji urządzenia z siecią należy sprawdzić, czy przełącznik jest skonfigurowany w celu monitorowania wymaganego ruchu. Dostępne są różne opcje połączenia urządzenia z przełącznikiem.

#### 1. Wdrożenie standardowe (oddzielne zarządzanie, interfejsy monitorowania i odpowiedzi)

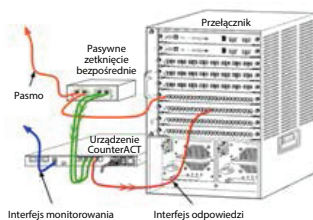
W zalecanej wdrożeniu wykorzystywane są trzy oddzielne porty. Porty te są opisane w części *Połączenia interfejsu urządzenia*.



#### 2. Pasywne zetknięcie bezpośrednie

Zamiast połączenia z portem monitorowania przełącznika urządzenie może użyć pasywnego zetknięcia bezpośredniego.

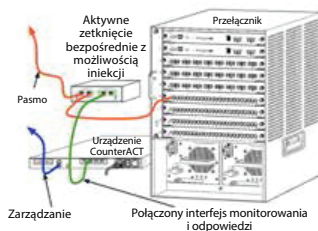
Do pasywnego zetknięcia bezpośredniego wymagane są dwa porty monitorowania, z wyjątkiem przypadku zetknięć rekombinacyjnych, w których dwa podwójne strumienie są łączone w jednym porcie. Ruch w porcie zetknięcia i interfejsie odpowiedzi musi być skonfigurowany w ten sam sposób. Jeśli na przykład ruch w porcie zetknięcia ma znacznik VLAN (802.1Q), interfejs odpowiedzi musi mieć również port ze znacznikiem VLAN.



#### 3. Aktywne (z możliwością iniekcji) zetknięcie bezpośrednie

Jeśli urządzenie korzysta z zetknięcia bezpośredniego z *możliwością iniekcji*, można połączyć interfejsy monitorowania i odpowiedzi. Nie ma konieczności konfigurowania oddzielnego portu odpowiedzi na przełączniku.

Tę opcję można zastosować dla dowolnej konfiguracji wcześniejszych lub dalszych przełączników.





#### 4. Odpowiedź warstwy IP (dla instalacji przełączników warstwy 3)

Urządzenie może w odpowiedzi na ruch korzystać z własnego interfejsu zarządzania. Chociaż z tej opcji można korzystać dla każdego monitorowanego ruchu, jest ona zalecana, gdy urządzenie monitoruje porty niebędące częścią żadnej sieci VLAN, przez co nie może odpowiadać na monitorowany ruch z wykorzystaniem żadnego innego portu przełącznika. Typową taką sytuacją jest monitorowanie łącza między dwoma routerami.

Dla tej opcji nie jest możliwa odpowiedź na żądania protokołu rozpoznawania adresów (ARP), ograniczające możliwość wykrywania przez urządzenie skanowań nakierowanych na adresy IP wewnątrz monitorowanej podsieci. To ograniczenie nie dotyczy sytuacji monitorowania ruchu między dwoma routerami.

## B. Uwagi dotyczące ustawiania przełącznika

### Znaczniki VLAN (802.1Q)

- **Monitorowanie pojedynczej sieci VLAN (ruch bez znaczników)** Jeśli monitorowany ruch pochodzi z pojedynczej sieci VLAN, nie wymaga znaczników 802.1Q.
- **Monitorowanie wielu sieci VLAN (ruch ze znacznikami)** Jeśli monitorowany ruch pochodzi z dwu lub więcej sieci VLAN, zarówno interfejs monitorowania, jak i odpowiedzi musi mieć włączone znaczniki 802.1Q. Monitorowanie wielu sieci VLAN jest zalecaną opcją, ponieważ zapewnia najlepsze ogólne pokrycie z minimalizacją liczby kopiowanych portów.
- Jeśli przełącznik nie może używać znaczników VLAN 802.1Q w kopiowanych portach, należy wykonać jedną z następujących czynności:
  - Skopiować tylko jedną sieć VLAN
  - Skopiować jeden nieoznaczony port pasma
  - Użyć opcji odpowiedzi warstwy IP
- Jeśli przełącznik może kopiować tylko jeden port, należy skopiować jeden port pasma. Może być on oznaczony. Ogólnie rzecz biorąc, jeśli przełącznik odbiera znaczniki VLAN 802.1Q, konieczne będzie użycie opcji odpowiedzi warstwy IP.

### Dodatkowe

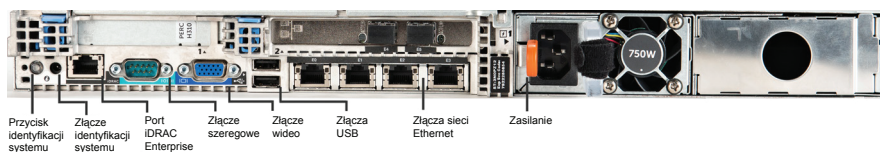
- Jeśli przełącznik nie może kopiować zarówno ruchu wysyłania, jak i odbioru, należy monitorować cały przełącznik, całe sieci VLAN (daje to wysyłanie/odbiór) lub tylko jeden interfejs (umożliwiający wysyłanie/ odbiór). Należy sprawdzić, czy port kopiowana nie jest przeciążony.
- W przypadku niektórych przełączników (takich jak Cisco 6509) może być wymagane całkowite skasowanie poprzednich konfiguracji portów przed wprowadzeniem nowych konfiguracji. Najczęstszym skutkiem nieskasowania starych informacji o portach jest odbieranie przez przełącznik znaczników 802.1Q.

### 3. Podłączenie kabli sieciowych i włączenie zasilania

#### A. Rozpakowanie urządzenia i podłączenie kabli

1. Wyjąć urządzenie i kable zasilające z pojemnika wysyłkowego.
2. Wyjąć zestaw szyn otrzymany z urządzeniem.
3. Zamontować zestaw szyn na urządzeniu i przytwierdzić je do stojaka.
4. Podłączyć kable sieciowe między interfejsami sieciowymi na tylnym panelu urządzenia a portami przełącznika.

#### **Przykładowy panel tylny — Urządzenie CounterACT**



## B. Rejestracja przypisań interfejsu

Po zakończeniu instalacji urządzenia w centrum danych i zainstalowaniu aplikacji CounterACT Console pojawi się monit o rejestrację przypisań interfejsu. Te przypisania, określane jako *definicje kanałów*, są wprowadzane w Kreatorze konfiguracji początkowej, otwieranym po pierwszym zalogowaniu się do aplikacji Console.

Należy zanotować przypisania interfejsu fizycznego podane poniżej i użyć ich podczas finalizacji konfiguracji kanałów w aplikacji Console.

Interfejs sieci Ethernet	Przypisanie interfejsu (np. zarządzanie, monitorowanie, odpowiedź)
Eth0	
Eth1	
Eth2	
Eth3	
Eth4	
Eth5	
Eth6	
Eth7	
Eth8	

## C. Włączenie urządzenia

1. Podłączyć kabel zasilania do złącza zasilania na tylnym panelu urządzenia.
2. Podłączyć drugi koniec kabla zasilania do uziemionego gniazda prądu przemiennego.
3. Podłączyć do urządzenia klawiaturę i monitor lub skonfigurować je dla połączenia szeregowego. Patrz *Instrukcja instalacji urządzenia CounterACT*, znajdujący się na dysku CD dołączonym do urządzenia CounterACT.
4. Włączyć urządzenie z panelu przedniego.

**Ważne: Przed wyjęciem wtyczki należy wyłączyć urządzenie.**

## 4. Konfiguracja urządzenia

Przed przystąpieniem do konfigurowania urządzenia należy przygotować następujące informacje.

<input type="checkbox"/> Nazwa hosta urządzenia	
<input type="checkbox"/> Hasło administratora urządzenia CounterACT	<b>Hasło należy przechowywać w bezpiecznym miejscu</b>
<input type="checkbox"/> Interfejs zarządzania	
<input type="checkbox"/> Adres IP urządzenia	
<input type="checkbox"/> Maska sieci	
<input type="checkbox"/> Adres IP bramy domyślnej	
<input type="checkbox"/> Nazwa domeny DNS	
<input type="checkbox"/> Adres serwera DNS	

Po włączeniu zostanie wyświetlony monit o rozpoczęcie konfiguracji z następującym komunikatem:

```
CounterACT Appliance boot is complete.
(Uruchamianie urządzenia CounterACT zakończone).
Press <Enter> to continue. (Naciśnij klawisz
<Enter>, aby kontynuować).
```

1. Należy nacisnąć klawisz **Enter**, aby wyświetlić następujące menu:

```
1) Configure CounterACT (Konfigurowanie urządzenia
CounterACT)
2) Restore saved CounterACT configuration
(Przywracanie zapisanej konfiguracji urządzenia
CounterACT)
3) Identify and renumber network interfaces
(Identyfikacja i zmiana numeracji
interfejsów sieciowych)
4) Configure keyboard layout (Konfigurowanie układu
klawiatury)
5) Turn machine off (Wyłączanie urządzenia)
6) Reboot the machine (Ponowne uruchamianie
urządzenia)
Choice (1-6) :1 (Wybór (1-6) :1)
```

2. Należy wybrać opcję **1** – Configure CounterACT (Konfigurowanie urządzenia CounterACT). Po wyświetleniu monitu:

```
Continue: (Kontynuuj:) (yes/no)? (Czy
kontynuować: tak/nie)?
```

Nacisnąć przycisk **Enter**, aby rozpocząć konfigurację.


3. Zostanie otwarte menu **High Availability Mode (Tryb wysokiej dostępności)**. Nacisnąć przycisk **Enter**, aby wybrać instalację standardową.
4. Zostanie wyświetlony monit **CounterACT Initial Setup (Początkowa konfiguracja urządzenia CounterACT)**. Nacisnąć klawisz **Enter**, aby kontynuować...
5. Zostanie otwarte menu **Select CounterACT Installation Type (Wybierz typ instalacji urządzenia CounterACT)**. Wpisać **1** i nacisnąć klawisz **Enter**, aby zainstalować standardowe urządzenie CounterACT. Rozpocznie się konfigurowanie. Może to potrwać chwilę.
6. Po wyświetleniu monitu **Enter Machine Description (Wprowadź opis urządzenia)** należy wprowadzić krótki tekst identyfikujący urządzenie i nacisnąć klawisz **Enter**. Zostanie wyświetlony następujący tekst:

```
>>>>> Set Administrator Password (Ustaw hasło
      administratora) <<<<<<

This password is used to log in as 'root' to the
machine Operating System and as 'admin' to the
CounterACT Console. (To hasło jest używane w celu
zalogowania jako użytkownik główny w systemie
operacyjnym urządzenia i jako administrator
w aplikacji CounterACT Console).
The password should be between 6 and 15 characters
long and should contain at least one non-alphabetic
character. (Hasło powinno mieć długość od 6 do
15 znaków i zawierać przynajmniej jeden znak
niebędący literą).
```

Administrator password (Hasło administratora):

7. Po wyświetleniu monitu **Set Administrator Password (Ustaw hasło administratora)** należy wpisać ciąg, który będzie stanowił hasło (nie jest on uwidoczniony na ekranie) i nacisnąć klawisz **Enter**. Wyświetlony zostaje monit o potwierdzenie hasła. Hasło musi mieć długość od sześciu do 15 znaków i zawierać przynajmniej jeden znak niebędący literą.character.

 *Logowanie do urządzenia jako użytkownik główny i logowanie do aplikacji Console jako administrator.*

8. Po wyświetleniu monitu **Set Host Name (Ustaw nazwę hosta)** należy wpisać nazwę hosta i nacisnąć klawisz **Enter**. Nazwa hosta może być używana podczas logowania do aplikacji Console i jest wyświetlana w aplikacji Console w celu ułatwienia identyfikacji wyświetlanego urządzenia CounterACT.
9. Na ekranie **Configure Network Settings (Konfiguracja ustawień sieciowych)** wyświetlane są monity o podanie szeregu parametrów konfiguracji. Należy wpisywać wartości dla poszczególnych monitów i naciskać klawisz **Enter**, aby przejść dalej.
  - Elementy urządzenia CounterACT komunikują się przez interfejsy zarządzania. Liczba wyświetlonych interfejsów zarządzania zależy od modelu urządzenia.

- **Adres IP zarządzania** to adres interfejsu, przez który komunikują się elementy urządzenia CounterACT. Identyfikator sieci VLAN dla tego interfejsu należy dodać jedynie wtedy, gdy interfejs używany do komunikacji między elementami urządzenia CounterACT jest podłączony do oznaczonego portu.
- Jeśli występuje więcej niż jeden **DNS server address (Adres serwera DNS)**, poszczególne adresy należy oddzielić spacjami. Większość wewnętrznych serwerów DNS rozpoznaje adresy zewnętrzne i wewnętrzne, ale może być konieczne uwzględnienie zewnętrznego rozpoznającego serwera DNS. Ponieważ niemal wszystkie zapytania DNS wykonywane przez urządzenie będą dotyczyły adresów wewnętrznych, zewnętrzny serwer DNS należy wymienić jako ostatni.

10. Zostanie wyświetlony ekran **Setup Summary (Podsumowanie konfiguracji)**. Wyświetlane są monity o wykonanie ogólnych testów łączności, zmianę konfiguracji ustawień bądź zakończenie konfiguracji. Aby zakończyć konfigurację, należy wpisać **D**.

## Licencja

Po zakończeniu instalacji należy zainstalować początkową licencję wersji demonstracyjnej, dostarczoną przez przedstawiciela producenta urządzenia CounterACT. Licencja jest instalowana podczas początkowej konfiguracji aplikacji Console. Początkowa licencja wersji demonstracyjnej jest ważna przez określoną liczbę dni. Po upływie tego okresu należy zainstalować licencję stałą. Użytkownik otrzyma wiadomość e-mail dotyczącą daty wygaśnięcia. Oprócz tego informacje na temat daty wygaśnięcia i statusu licencji są wyświetlone w aplikacji CounterACT Console, w oknie Appliances/Devices (Urządzenia).

Po otrzymaniu licencji stałej jest ona potwierdzana codziennie przez serwer licencji ForeScout. Alarmy dotyczące licencji i informacje o naruszeniach są wyświetlane w oknie Device Details (Szczegóły urządzenia).

Licencje, których nie można potwierdzić przez okres jednego miesiąca, zostaną cofnięte. Dodatkowe szczegóły na temat licencji zawiera Instrukcja instalacji urządzenia CounterACT.

## Wymagania dotyczące połączenia sieciowego

Przynajmniej jedno urządzenie CounterACT (urządzenie lub Menedżer korporacyjny) musi mieć możliwość uzyskania dostępu do Internetu. To połączenie służy do zatwierdzania licencji urządzenia CounterACT przez serwer licencji ForeScout.

Licencje, których nie można uwierzytelnić przez okres jednego miesiąca, zostaną cofnięte. Urządzenie CounterACT będzie wysyłało codziennie ostrzegawczą wiadomość e-mail, informującą o błędzie komunikacji z serwerem.

## 5. Zdalne zarządzanie

### Konfiguracja modułu iDRAC

Zintegrowany sterownik zdalnego dostępu Dell – Integrated Dell Remote Access Controller (iDRAC) jest zintegrowanym rozwiązaniem systemu serwerowego, umożliwiającym niezależny od lokalizacji i systemu operacyjnego zdalny dostęp przez sieć LAN lub Internet do urządzeń/Menedżerów korporacyjnych CounterACT. Tego modułu należy używać w celu uzyskiwania dostępu KVM, włączania/wyłączania/resetowania i wykonywania zadań związanych z rozwiązywaniem problemów oraz konserwacją.

Aby korzystać z modułu iDRAC, należy wykonać następujące czynności:

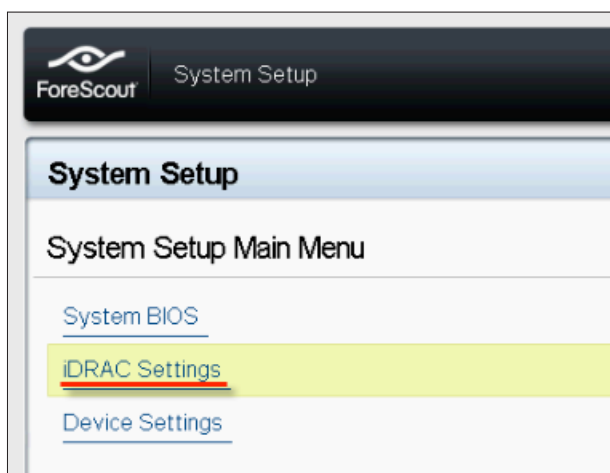
- *Włączenie i konfiguracja modułu iDRAC*
- *Podłączenie modułu do sieci*
- *Zalogowanie do modułu iDRAC*

#### Aby skonfigurować moduł iDRAC:

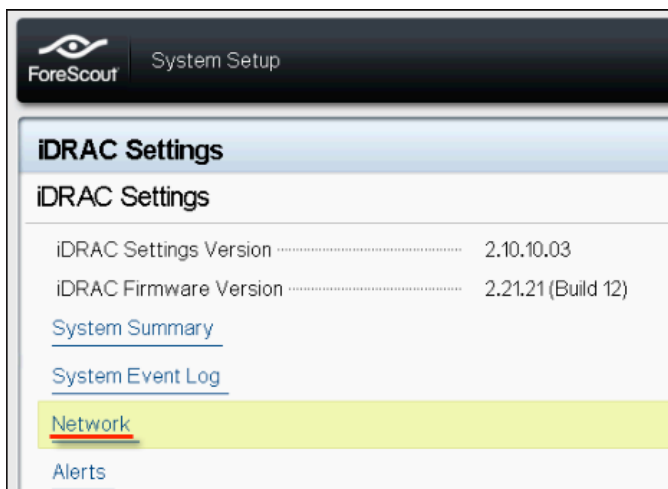
Należy zmienić ustawienia modułu iDRAC, aby umożliwić zdalny dostęp w urządzeniu CounterACT. W tej części opisano podstawowe ustawienia integracji, wymagane do pracy z urządzeniem CounterACT.

#### Aby skonfigurować moduł iDRAC:

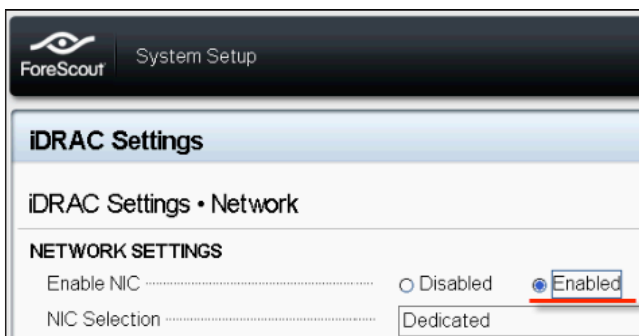
1. Należy włączyć zarządzany system.
2. Podczas procedury testowej POST wybrać klawisz F2.
3. Na stronie System Setup Main Menu (Menu główne konfiguracji systemu) wybrać opcję **iDRAC Settings (Ustawienia modułu iDRAC)**.



4. Na stronie iDRAC Settings (Ustawienia modułu iDRAC) wybrać opcję **Network (Sieć)**.



5. Należy skonfigurować następujące ustawienia sieciowe:
- **Network Settings (Ustawienia sieciowe)**. Sprawdzić, czy dla pola **Enable NIC (Włącz kartę interfejsu sieciowego)** wybrano ustawienie **Enabled (Włączona)**.



- **Common Settings (Ustawienia ogólne)**. W polu DNS DRAC Name (Nazwa DRAC DNS) można zaktualizować dynamiczny protokół DNS (Opcja).



- **IPv4 Settings (Ustawienia IPv4).** Sprawdzić, czy dla pola **Enable IPv4 (Włącz protokół IPv4)** wybrano ustawienie **Enabled (Włączone)**. Wybrać dla pola **Enable DHCP (Włącz protokół)** ustawienie **Enabled (Włączony)**, aby używać dynamicznego adresowania IP, lub **Disabled (Wyłączony)**, aby używać statycznego adresowania IP. W przypadku włączenia protokół DHCP będzie automatycznie przypisywał do modułu iDRAC adres IP, bramę i maskę podsieci. Jeśli jest on wyłączony, należy wprowadzić wartości w polach **Static IP Address (Statyczny adres IP)**, **Static Gateway (Statyczna brama)** i **Static Subnet Mask (Statyczna maska podsieci)**.

**ForeScout System Setup**

**iDRAC Settings**

**iDRAC Settings • Network**

**IPv4 SETTINGS**

Enable IPv4	<input type="radio"/> Disabled	<input checked="" type="radio"/> <b>Enabled</b>
Enable DHCP	<input checked="" type="radio"/> <b>Disabled</b>	<input type="radio"/> Enabled
Static IP Address	192.168.1.103	
Static Gateway	192.168.1.1	
Static Subnet Mask	255.255.255.0	
Use DHCP to obtain DNS server addresses	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled
Static Preferred DNS Server	192.168.1.2	
Static Alternate DNS Server	0.0.0.0	

- Wybrać opcję **Back (Wstecz)**.
- Wybrać opcję **User Configuration (Konfiguracja użytkownika)**.
- Skonfigurować następujące pola konfiguracji użytkownika:
  - **Enable User (Włącz użytkownika)**. Należy sprawdzić, czy dla tego pola wybrano ustawienie Enabled (Włączony).
  - **User Name (Nazwa użytkownika)**. Wprowadzić nazwę użytkownika.

**ForeScout System Setup** Help | About | E

**iDRAC Settings**

**iDRAC Settings • User Configuration**

User ID	2	
Enable User	<input type="radio"/> Disabled	<input checked="" type="radio"/> <b>Enabled</b>
User Name	root	
LAN User Privilege	Administrator	
Serial Port User Privilege	Administrator	
Change Password		

- **LAN and Serial Port User Privileges (Uprawnienia użytkownika sieci LAN i portów szeregowych).** Jako poziomy uprawnień należy wybrać opcję Administrator.
  - **Change Password (Zmień hasło).** Ustawić hasło logowania użytkownika.
9. Wybrać opcję **Back (Wstecz)**, a następnie opcję **Finish (Zakończ)**. Należy potwierdzić zmienione ustawienia. Ustawienia sieciowe zostaną zapisane, a system ponownie uruchomiony.

## Podłączenie modułu do sieci

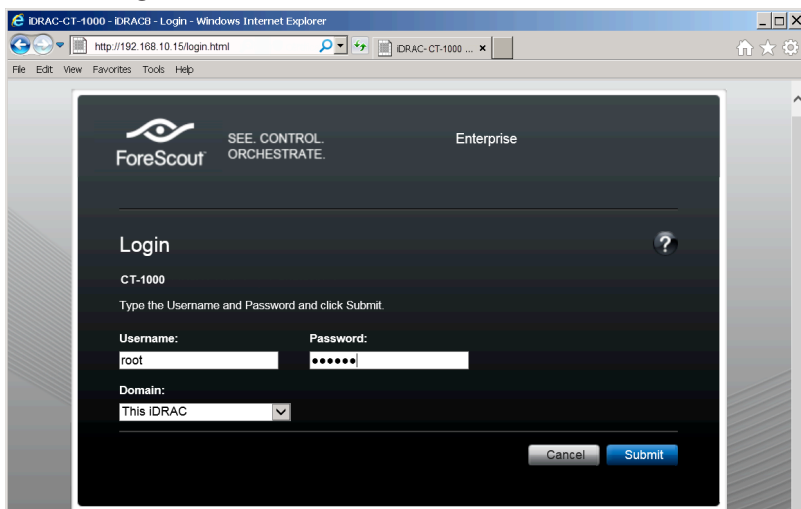
Moduł iDRAC łączy się z siecią Ethernet. Zwyczajowo podłącza się go do sieci zarządzania. Na poniższej ilustracji przedstawiono lokalizację portu iDRAC na panelu tylnym urządzenia CT-1000:



## Logowanie do modułu iDRAC

Aby zalogować się do modułu iDRAC:

1. Należy przejść do adresu IP lub nazwy domeny skonfigurowanej w obszarze **iDRAC Settings (Ustawienia modułu iDRAC) > Network (Sieć)**.



2. Wprowadzić nazwę użytkownika i hasło skonfigurowane na stronie User Configuration (Konfiguracja użytkownika) konfiguracji systemu iDRAC.
3. Wybrać opcję **Submit (Prześlij)**.

Aby uzyskać dalsze informacje na temat modułu iDRAC, patrz [Instrukcja użytkownika modułu iDRAC](#).

Bardzo ważna jest aktualizacja poświadczeń domyślnych.

## 6. Sprawdzenie łączności

### Sprawdzenie połączenia interfejsu zarządzania

Aby przetestować połączenie interfejsu zarządzania, należy zalogować się do urządzenia i uruchomić następujące polecenie:

```
fstool linktest
```

Zostanie wyświetlona następująca informacja:

```
Management Interface status (Status interfejsu  
zarządzania)  
Pinging default gateway information (Informacje  
o bramie domyślnej pingowania)  
Ping statistics (Statystyki pingowania)  
Performing Name Resolution Test (Wykonanie testu  
rozpoznawania nazwy)  
Test summary (Podsumowanie testu)
```

### Sprawdzenie łączności przełącznika/urządzenia

Przed opuszczeniem centrum danych należy sprawdzić, czy przełącznik został prawidłowo połączony z urządzeniem. W tym celu należy uruchomić na urządzeniu polecenie `fstool ifcount` dla każdego wykrytego interfejsu.

```
fstool ifcount eth0 eth1 eth2
```

*(Rozdzielić poszczególne interfejsy spacjami).*

To narzędzie w sposób ciągły wyświetla ruch sieciowy na określonych interfejsach. Pracuje w dwóch trybach: według interfejsu lub według sieci VLAN. Tryb można zmienić z wyświetlacza. Wyświetlana jest łączna liczba bitów na sekundę i wartość procentowa dla następujących kategorii ruchu:

- Dla interfejsu monitorowania powinien być widoczny przede wszystkim kopiowany ruch w zakresie powyżej 90%.
- Dla interfejsu odpowiedzi powinien być widoczny przede wszystkim ruch emisji.
- Zarówno dla interfejsu monitorowania, jak i odpowiedzi powinny być widoczne oczekiwane sieci VLAN.

#### Opcje poleceń:

**v** - wyświetlanie w trybie VLAN

**I** - wyświetlanie w trybie interfejsu

**P** - pokaż poprzedni

**N** - pokaż następny

**q** - zakończ wyświetlanie

## Tryb VLAN:

update=[4] [eth3: 14 vlans]					
Interface/Vlan	Total	Broadcast	Mirrored	*To my MAC	*From my MAC
eth3.untagged	4Mbps	0.2%	99.8%	0.0%	0.0%
eth3.1	9Mbps	0.0%	100.0%	0.0%	0.0%
eth3.2	3Mbps	0.1%	99.9%	0.0%	0.0%
eth3.4	542bps	100.0%	0.0%	0.0%	0.0%
eth3.20	1Kbps	100.0%	0.0%	0.0%	0.0%
Show [v]lans [i]nterfaces <-[p]rev [n]ext-> [q]uit					

## Tryb interfejsu:

update=[31] [eth0: 32 vlans] [eth1: 1 vlans]					
Interface	Total	Broadcast	Mirrored	*To my MAC	*From my MAC
eth0	3Kbps	42.3%	0.0%	14.1%	43.7%
eth1	475bps	0.0%	100.0%	0.0%	0.0%

\*To my MAC (Do mojego adresu MAC) — docelowym adresem MAC jest adres MAC urządzenia.

\*From my MAC (Z mojego adresu MAC) — ruch wysyłany przez urządzenie (źródłowym adresem MAC jest adres MAC urządzenia. Miejsce docelowe może być rozgłoszeniowe lub emisji pojedynczej).

Jeśli nie jest widoczny żaden ruch, należy sprawdzić, czy interfejs działa. Należy użyć następującego polecenia na urządzeniu:

```
ifconfig [interface name] up
```

## Wykonanie testu ping

Należy uruchomić na urządzeniu test ping komputera sieciowego, aby sprawdzić łączność.

### Aby uruchomić test:

1. Zalogować się do urządzenia.
2. Uruchomić następujące polecenie: **Ping [adres IP komputera sieciowego]**. Samo urządzenie domyślnie nie odpowiada na sygnał ping.

## 7. Konfiguracja aplikacji CounterACT Console

### Instalacja aplikacji CounterACT Console

CounterACT Console to aplikacja do centralnego zarządzania, używana do wyświetlania, śledzenia i analizowania aktywności wykrytych przez urządzenie. Z poziomu konsoli można zdefiniować kontrolę dostępu do sieci, ochronę przed zagrożeniami, zaporę lub inne reguły. Aby uzyskać więcej informacji, należy zapoznać się z *Instrukcją obsługi aplikacji CounterACT Console*.

Należy zapewnić komputer, który będzie hostem aplikacji CounterACT Console. Minimalne wymagania sprzętowe są następujące:

- Niededykowany komputer z systemem:
  - Windows XP, Windows Vista lub Windows 7
  - Windows Server 2003 lub Server 2008
  - Linux
- Pentium 3,1 GHz
- Ilość pamięci — 2 GB
- Ilość miejsca na dysku — 1 GB

Dostępne są dwie metody instalacji aplikacji Console:

#### **Z wykorzystaniem oprogramowania instalacyjnego wbudowanego w urządzenie.**

1. Otworzyć okno przeglądarki na komputerze z aplikacją Console.
2. W wierszu adresu przeglądarki wpisać  
**<http://<Appliance ip>/install>**  
Gdzie <Appliance ip> to adres IP urządzenia. W przeglądarce zostanie wyświetlone okno instalacji aplikacji Console.
3. Wykonać instrukcje wyświetlone na ekranie.

#### **Instalacja z dysku CD-ROM urządzenia CounterACT**

1. Włożyć dysk CD-ROM dołączony do urządzenia CounterACT do napędu DVD.
2. Otworzyć w przeglądarce plik **ManagementSetup.htm** z dysku CD ROM.
3. Wykonać instrukcje wyświetlone na ekranie.

## Logowanie

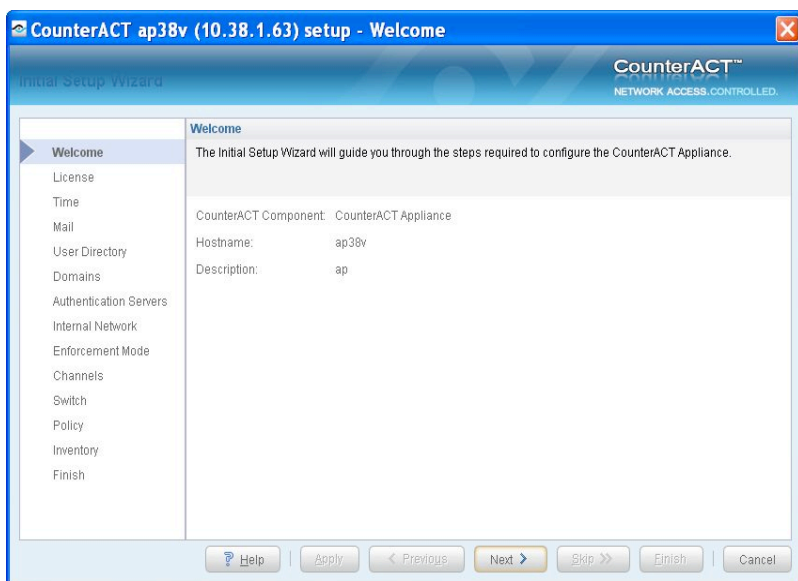
Po zakończeniu instalacji można zalogować się do aplikacji CounterACT Console.

1. Wybrać ikonę CounterACT w utworzonej lokalizacji skrótu.
2. W polu **IP/Name (Adres IP/nazwa)** wpisać adres IP lub adres hosta urządzenia.
3. W polu **User Name (Nazwa użytkownika)** wpisać **admin**.
4. W polu **Password (Hasło)** wpisać hasło utworzone podczas instalacji urządzenia.
5. Wybrać opcję **Login (Zaloguj)**, aby uruchomić aplikację Console.



## Wykonanie konfiguracji początkowej

Po pierwszym zalogowaniu zostanie wyświetlony Kreator konfiguracji początkowej. Kreator prowadzi przez konieczne kroki konfiguracji, aby zapewnić prawidłowe działanie oraz szybką i efektywną pracę urządzenia CounterACT.



## Przed rozpoczęciem początkowej konfiguracji

Przed przystąpieniem do pracy z Kreatorem należy przygotować następujące informacje.

Informacja	Wartości
<input type="checkbox"/> Adres serwera NTP używanego przez organizację (opcjonalny).	
<input type="checkbox"/> Adres IP urządzenia przekazującego pocztę wewnętrzną. Umożliwia on dostarczanie poczty e-mail z urządzenia CounterACT jeśli nie jest dozwolony ruch SMTP z urządzenia (opcja).	
<input type="checkbox"/> Adres e-mail administratora urządzenia CounterACT.	
<input type="checkbox"/> Przypisania interfejsów monitorowania i odpowiedzi zdefiniowane z centrum danych.	
<input type="checkbox"/> Dla segmentów lub sieci VLAN bez protokołu DHCP, segmenty sieci lub sieci VLAN, z którymi połączony jest bezpośrednio interfejs monitorowania oraz stały adres IP, który będzie używany przez urządzenie CounterACT dla każdej takiej sieci VLAN. Ta informacja nie jest wymagana do konfiguracji Menedżera korporacyjnego.	
<input type="checkbox"/> Zakres adresów IP, które będą chronione przez urządzenie (wszystkie adresy wewnętrzne, w tym nieużywane).	
<input type="checkbox"/> Informacje o koncie katalogu użytkowników i adres IP serwera katalogu użytkowników.	
<input type="checkbox"/> Poświadczenia domeny, w tym nazwa i hasło konta administratora.	
<input type="checkbox"/> Serwery uwierzytelnień umożliwiające urządzeniu CounterACT analizę powodzenia uwierzytelnień hostów sieciowych.	
<input type="checkbox"/> Adres IP przełącznika głównego, dostawca i parametry protokołu SNMP.	

Aby uzyskać informacje na temat pracy z Kreatorem, należy zapoznać się z *Instrukcją obsługi aplikacji CounterACT Console* lub pomocą online.

# Informacje kontaktowe

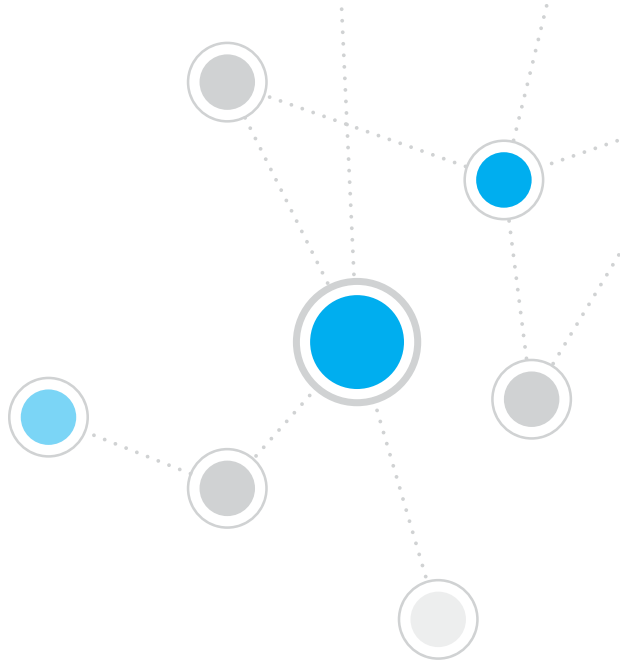
Aby uzyskać wsparcie techniczne od firmy ForeScout, należy wysłać wiadomości e-mail na adres [support@forescout.com](mailto:support@forescout.com) lub zadzwonić:

- Numer bezpłatny (Stany Zjednoczone): +1-866-377-8771
- Telefon (międzynarodowy): +1-408-213-3191
- Wsparcie: +1-708-237-6591
- Faks: +1-408-371-2284

©2016 ForeScout Technologies, Inc. Produkty chronione patentami amerykańskimi nr #6,363,489, #8,254,286, #8,590,004 and #8,639,800. Wszystkie prawa zastrzeżone. ForeScout Technologies i logo ForeScout są znakami towarowymi należącymi do firmy ForeScout Technologies, Inc. Wszystkie inne znaki towarowe są własnością ich odnośnych właścicieli.

Korzystanie ze wszystkich produktów firmy ForeScout podlega warunkom Umowy licencyjnej użytkownika końcowego ForeScout znajdującej się pod adresem [www.forescout.com/eula](http://www.forescout.com/eula).





# ForeScout®

ForeScout Technologies, Inc.  
900 E. Hamilton Avenue #300  
Campbell, CA 95008 USA

**Numer bezpłatny (Stany Zjednoczone):** +1-866-377-8771

**Telefon (międzynarodowy):** +1-408-213-3191

**Wsparcie:** +1-708-237-6591

**Faks:** +1-408-371-2284

400-00020-01