Wheel Fudo PAM 3.0 - Dokumentacja Systemu

Wydanie niewspierane

Wheel Systems

09.09.2021

Spis treści

1 Informacje ogólne **1**
- 1.1 O dokumentacji . . . 1
- 1.2 Opis systemu . . . 2
  - 1.2.1 PSM (Privileged Sessions Management) . . . 2
  - 1.2.2 Skarbiec haseł (Secret Manager) . . . 3
  - 1.2.3 AAPM (Application to Application Password Manager) . . . 4
  - 1.2.4 Efficiency Analyzer . . . 4
  - 1.2.5 Portal użytkownika . . . 4
- 1.3 Model danych . . . 5
- 1.4 Scenariusze wdrożenia . . . 6
- 1.5 Metody i tryby uwierzytelniania użytkowników . . . 9
- 1.6 Mechanizmy bezpieczeństwa . . . 11
- 1.7 Wymagania . . . 14

2 Konfiguracja **15**
- 2.1 Urządzenie . . . 15
- 2.2 Pierwsze uruchomienie . . . 16
  - 2.2.1 Urządzenie fizyczne . . . 16
- 2.3 Szybki start . . . 21
  - 2.3.1 SSH . . . 21
  - 2.3.2 RDP . . . 27
  - 2.3.3 MySQL . . . 36
  - 2.3.4 HTTP . . . 42
  - 2.3.5 Telnet . . . 47
  - 2.3.6 Konfigurowanie modyfikatora haseł . . . 52
- 2.4 Dashboard . . . 55
- 2.5 Użytkownicy . . . 56
  - 2.5.1 Dodawanie użytkownika . . . 57
  - 2.5.2 Blokowanie i odblokowanie użytkownika . . . 60
  - 2.5.3 Usuwanie użytkownika . . . 60
  - 2.5.4 Role . . . 61
- 2.6 Serwery . . . 62
- 2.7 Konta . . . 65
- 2.8 Sejfy . . . 72
- 2.9 Gniazda nasłuchiwania . . . 75
- 2.10 Modyfikatory haseł . . . 79

2.10.1 Polityka haseł . . . 79
2.10.2 Uniwersalne modyfikatory haseł . . . 80
2.11 Polityki . . . 82

3 Sesje **87**
3.1 Filtrowanie sesji . . . 88
3.1.1 Definiowanie filtrów . . . 88
3.1.2 Przeszukiwanie pełnotekstowe . . . 90
3.1.3 Zarządzanie definicjami filtrowania . . . 91
3.2 Raporty . . . 92
3.3 Odtwarzanie sesji . . . 95
3.4 Podgląd trwających sesji . . . 98
3.5 Wstrzymywanie połączenia . . . 98
3.6 Przerywanie połączenia . . . 99
3.7 Dołączanie do sesji . . . 100
3.8 Udostępnianie sesji . . . 101
3.9 Komentowanie sesji . . . 104
3.10 Eksportowanie sesji . . . 106
3.11 Usuwanie sesji . . . 107
3.12 Przetwarzanie OCR sesji . . . 107

4 Analiza produktywności **111**
4.1 Zestawienie . . . 111
4.2 Analiza sesji . . . 112
4.3 Porównanie aktywności . . . 114

5 AAPM (Application to Application Password Manager) **115**
5.1 Informacje ogólne . . . 115
5.2 *fudopv* . . . 115
5.3 Interfejs API . . . 123

6 Administracja **125**
6.1 System . . . 125
6.1.1 Data i czas . . . 125
6.1.2 Certyfikat HTTPS . . . 127
6.1.3 Dostęp SSH . . . 128
6.1.4 Funkcjonalności wrażliwe . . . 129
6.1.5 Aktualizacja systemu . . . 130
6.1.5.1 Aktualizowanie systemu . . . 131
6.1.5.2 Weryfikacja wykonalności aktualizacji . . . 131
6.1.5.3 Usuwanie migawki aktualizacji . . . 132
6.1.6 Licencja . . . 132
6.1.7 Diagnostyka . . . 133
6.2 Konfiguracja sieci . . . 135
6.2.1 Konfiguracja ustawień sieciowych . . . 135
6.2.1.1 Zarządzanie interfejsami fizycznymi . . . 135
6.2.1.2 Ustawianie adresu IP z konsoli . . . 139
6.2.1.3 Konfigurowanie mostu sieciowego . . . 143
6.2.1.4 Konfigurowanie sieci wirtualnych (VLAN) . . . 144
6.2.2 Konfiguracja tras routingu . . . 144
6.2.3 Konfiguracja serwerów DNS . . . 146
6.3 Powiadomienia . . . 148

6.4 Znakowanie czasem . . . 150
6.5 Zewnętrzne serwery uwierzytelniania . . . 150
6.6 Zewnętrzne repozytoria haseł . . . 153
6.7 Zasoby . . . 155
6.8 Przywracanie poprzedniej wersji systemu . . . 156
6.9 Ponowne uruchomienie systemu . . . 158
6.10 Kopie zapasowe i retencja . . . 158
6.11 Eksportowanie/importowanie konfiguracji systemu . . . 160
6.11.1 Eksportowanie konfiguracji . . . 161
6.11.2 Importowanie konfiguracji . . . 161
6.12 Konfiguracja klastrowa . . . 162
6.12.1 Inicjowanie klastra . . . 162
6.12.2 Węzły klastra . . . 163
6.12.3 Grupy redundancji . . . 168
6.13 Synchronizacja użytkowników . . . 172
6.14 Dziennik zdarzeń . . . 175
6.15 Integracja z serwerem CERB . . . 179
6.16 Czynności serwisowe . . . 189
6.16.1 Monitorowanie stanu systemu . . . 189
6.16.2 Wymiana dysku macierzy . . . 191

7 Informacje uzupełniające 193
7.1 Broker połączeń RDP . . . 193
7.2 Kody błędów . . . 194
7.3 Mapowanie parametrów Wheel Fudo PAM 2.2 na Wheel Fudo PAM 3.0 . . . 198
7.3.1 Połączenie . . . 198
7.3.2 Serwer . . . 200
7.4 Migracja modelu danych wersji 2.2 do 3.0 . . . 200
7.4.1 Serwer . . . 200
7.4.2 Sejf (dawniej *połączenie*) . . . 201
7.4.3 Konto (dawniej *dane logowania*) . . . 201
7.4.4 Gniazdo nasłuchiwania (dawniej *bastion* lub część serwera) . . . 201
7.4.5 Sesje . . . 202
7.5 Obsługa wspieranych protokołów . . . 202
7.5.1 Citrix StoreFront (HTTP) . . . 202
7.5.2 HTTP . . . 202
7.5.3 ICA . . . 203
7.5.4 Modbus . . . 203
7.5.5 MS SQL (TDS) . . . 203
7.5.6 MySQL . . . 203
7.5.7 Oracle . . . 204
7.5.8 RDP . . . 204
7.5.9 SSH . . . 205
7.5.10 Telnet . . . 205
7.5.11 Telnet 3270 . . . 205
7.5.12 Telnet 5250 . . . 206
7.5.13 VNC . . . 206
7.5.14 X11 . . . 206

8 Rozwiązywanie problemów 207
8.1 Uruchamianie Wheel Fudo PAM . . . 207
8.2 Połączenia z serwerami . . . 208

8.3 Logowanie do panelu administracyjnego 212
8.4 Odtwarzanie sesji 213
8.5 Konfiguracja klastrowa 213

9 Często zadawane pytania **215**

10 Słownik pojęć **219**

Indeks **223**

ROZDZIAŁ 1

Informacje ogólne

1.1 O dokumentacji

Struktura dokumentacji

1. Informacje ogólne

Rozdział zawiera opis działania systemu, model danych, metody uwierzytelniania użytkowników.

2. Konfiguracja

Rozdział opisuje szczegółowo procedury konfiguracyjne Wheel Fudo PAM.

3. Sesje

Rozdział zawiera informacje dotyczące rejestrowanych sesji dostępowych.

4. Analiza produktywności

Rozdział opisuje moduł analizy produktywności użytkowników.

5. Administracja

Rozdział zawiera opisy procedur administracyjnych.

6. Informacje uzupełniające

Rozdział zawiera informacje uzupełniające bezpośrednio związane z procedurami zarządzania.

7. Rozwiązywanie problemów

Rozdział zawiera rozwiązania potencjalnych problemów jakie mogą pojawić się podczas korzystania z Wheel Fudo PAM.

8. Często zadawane pytania

Rozdział zawiera odpowiedzi na często zadawane pytania.

9. Słownik pojęć

Rozdział zawiera listę pojęć występujących w dokumentacji.

Konwencje i symbole

Poniższa sekcja opisuje konwencje nazewnicze użyte w dokumentacji.

kursywa

Element interfejsu graficznego użytkownika.

`przykład`

Przykładowa wartość parametru konfiguracyjnego.

Informacja: Informacja uzupełniająca ściśle związana z opisywanym zagadnieniem, np. sugestia dotycząca postępowania; dodatkowe warunki, które należy spełnić.

Ostrzeżenie: Ostrzeżenie. Informacja istotna z punktu widzenia działania systemu. Nie zastosowanie się do zalecenia może mieć nieodwracalne skutki.

Nota prawna

Wszystkie nazwy, grafiki i znaki firmowe lub towarowe, niebędące własnością firmy Wheel Systems, występujące w tym dokumencie, należą do ich właścicieli i zostały użyte wyłącznie w celach informacyjnych.

1.2 Opis systemu

Wheel Fudo PAM jest rozwiązaniem do zarządzania zdalnym dostępem uprzywilejowanym. System składa się z czterech modułów:

- PSM (Privileged Sessions Management)
- Secret Manager
- AAPM (Application to Application Password Manager)
- Efficiency Analyzer

1.2.1 PSM (Privileged Sessions Management)

Moduł PSM służy do stałego monitorowania zdalnych sesji dostępu do infrastruktury IT. Wheel Fudo PAM pośredniczy w zestawianiu połączenia ze zdalnym zasobem i rejestruje wszelkie akcje użytkownika, włącznie z ruchem kursora myszy, danymi wprowadzanymi za pomocą klawiatury i przesyłanymi plikami.

Rejestrowany jest kompletny ruch sieciowy, włącznie z meta danymi, co pozwala na precyzyjne odtworzenie przebiegu sesji dostępowej oraz pełnotekstowe przeszukiwanie treści.

Wheel Fudo PAM pozwala również na podgląd aktualnie trwających połączeń i ingerencję administratora w monitorowaną sesję w przypadku stwierdzenia nadużycia praw dostępu.

Wspierane protokoły i systemy

Wheel Fudo PAM obsługuje następujące protokoły komunikacyjne:

- *SSH*,
- *RDP*,
- *VNC - tylko połączenia w trybie 24-bit (true color)*,
- *HTTP/HTTPS*,
- *MySQL*,
- *MS SQL*,
- *Oracle* (aplikacje klienckie: SQLDeveloper 4.1.3.20.78, SQL*Plus: Release 11.2.0.4.0 Production),

---

Informacja: Wsparcie protokołu *Oracle* jest ograniczone z uwagi na jego zamknięty charakter. Firma Wheel Systems nie gwarantuje prawidłowej obsługi wszystkich funkcji tego protokołu.

- *Telnet/Telnet 3270*
- *modbus*.

Szczegółowe informacje na temat zakresu w jakim wspierane są poszczególne protokoły znajdziesz w rozdziale *Informacje uzupełniające > Obsługa wspieranych protokołów*.

Wheel Fudo PAM wspiera następujące konfiguracje systemowe:

- Linux,
- FreeBSD,
- Mac OS X
- Microsoft Windows Server,
- Microsoft Windows,
- TightVNC,
- Solaris.

1.2.2 Skarbiec haseł (Secret Manager)

Moduł *Secret Manager* umożliwia automatyczne zarządzanie danymi logowania na monitorowanych systemach i okresową zmianę haseł po upływie zdefiniowanego interwału czasowego.

Secret Manager potrafi zmieniać hasła na następujących systemach:

- Unix
- MySQL
- Cisco
- Cisco Enable Password

- MS Windows

Moduł *Secret Manager* umożliwia także zdefiniowanie własnych modyfikatorów haseł w postaci zestawu komend wykonywanych na zdalnej maszynie.

Wiecej informacji na temat modyfikatorów haseł znajdziesz w rozdziale *Konfiguracja > Modyfikatory haseł*.

1.2.3 AAPM (Application to Application Password Manager)

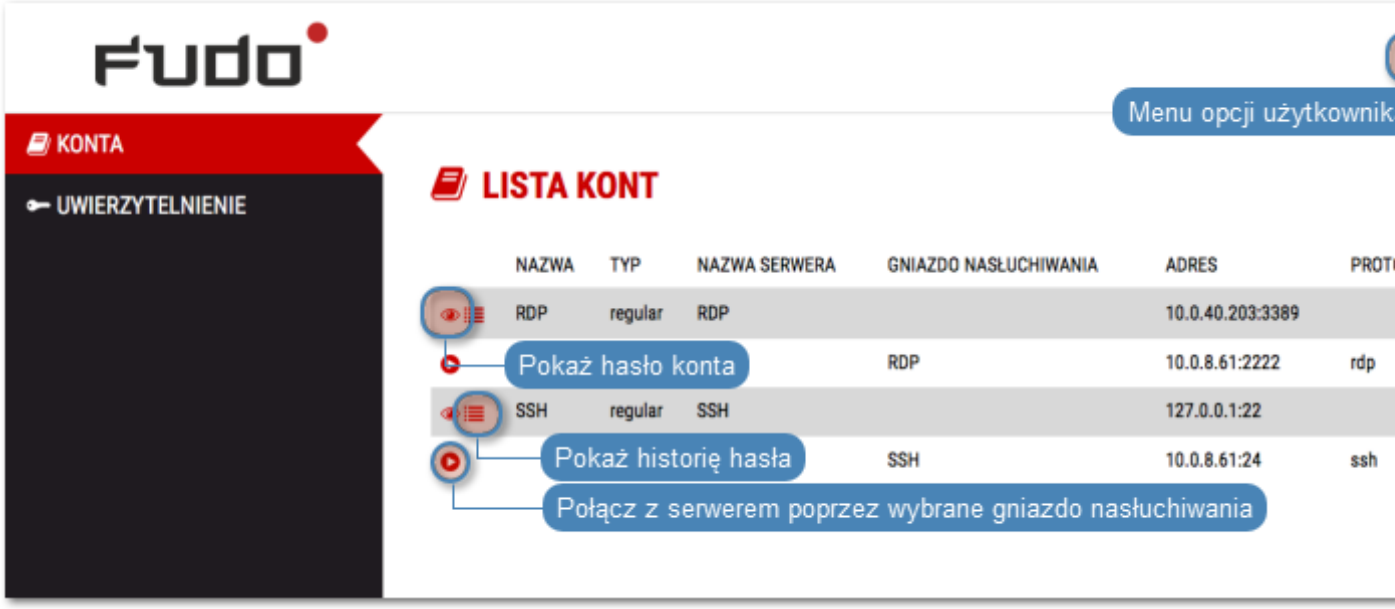
Moduł *AAPM* umożliwia bezpieczną wymianę haseł pomiędzy aplikacjami.

1.2.4 Efficiency Analyzer

Moduł analizy wydajności śledzi akcje użytkowników i pozwala dostarczyć szczegółowych informacji o czasie aktywności i bezczynności.

1.2.5 Portal użytkownika

Portal użytkownika umożliwia przeglądanie listy zasobów, do których użytkownik posiada stosowne uprawnienia i inicjowanie połączenia z monitorowanym zasobem za pośrednictwem wybranego gniazda nasłuchiwania.



Tematy pokrewne:

- *Wymagania*
- *Model danych*
- *Mechanizmy bezpieczeństwa*

1.3 Model danych

Wheel Fudo PAM operuje na pięciu podstawowych typach obiektów: użytkownik, serwer, konto, sejf oraz gniazdo nasłuchiwania.

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (indywidualny login, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzilnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

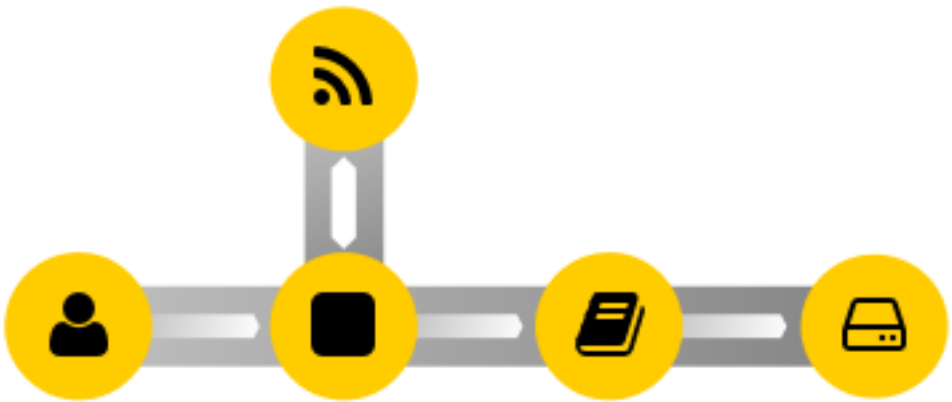
Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

Prawidłowe działanie systemu wymaga odpowiedniego skonfigurowania *serwerów*, *kont uprzywilejowanych*, *sejfów*, *użytkowników* oraz *gniazd nasłuchiwania*.

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z relpikacją danych, skontaktuj się z działem wsparcia technicznego.

Schemat relacji obiektów



Tematy pokrewne:

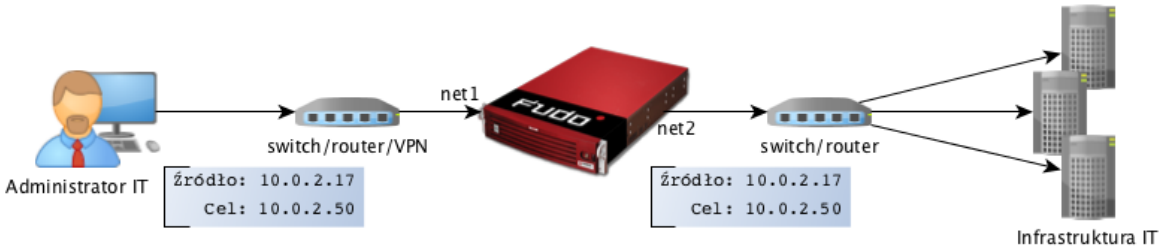
- *Opis systemu*
- *Metody i tryby uwierzytelniania użytkowników*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*

1.4 Scenariusze wdrożenia

Informacja: Zaleca się umiejscowienie Wheel Fudo PAM w infrastrukturze IT tak, aby pośredniczyło jedynie w połączeniach administracyjnych. Pozwoli to na ograniczenie obciążenia systemu, optymalizację ruchu w sieci a także zachowanie ciągłości dostępu do usług w okoliczności awarii sprzętowej.

Most

W trybie mostu Wheel Fudo PAM pośredniczy w komunikacji pomiędzy użytkownikami i monitorowanymi serwerami bez względu na to czy ruch podlega monitorowaniu (tj. komunikacja przebiega z użyciem wspieranych protokołów) czy nie.



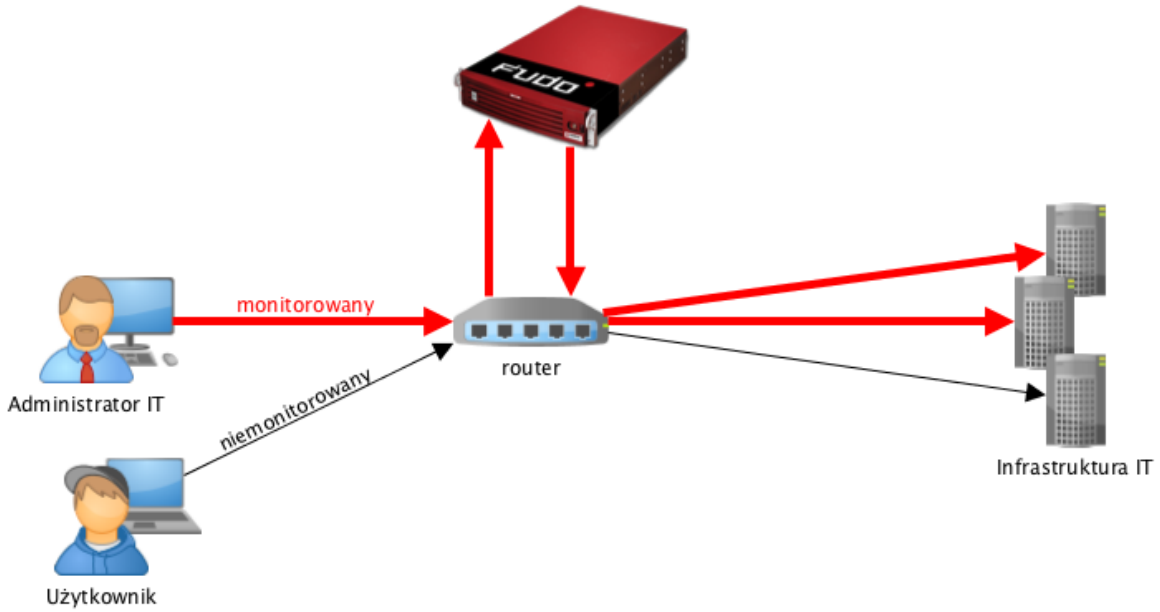
Wheel Fudo PAM pośrednicząc w przekazywaniu ruchu, zachowuje źródłowy adres IP klienta wysyłającego zapytania do serwerów.

Takie rozwiązanie pozwala na zachowanie dotychczasowych reguł na zaporach ogniowych regulujących dostęp do zasobów wewnętrznych.

Szczegóły na temat konfigurowania mostu znajdziesz w rozdziale *Konfiguracja sieci*.

Wymuszony routing

Tryb wymuszonego routingu wymaga użycia i odpowiedniego skonfigurowania routera. Taka topologia wdrożenia pozwala na sterowanie ruchem w sieci na poziomie trzeciej warstwy (sieci) modelu ISO/OSI, tak aby poprzez Wheel Fudo PAM kierowany był ruch administracyjny natomiast pozostałe zapytania były kierowane bezpośrednio do serwera docelowego.



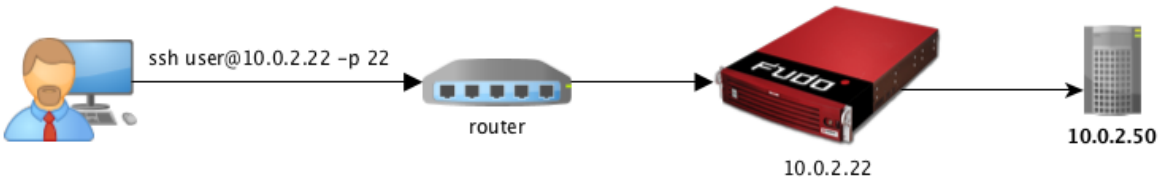
Tryb ten nie wymaga zmian w topologii sieci i pozwala na optymalizację ruchu i obciążenia sprzętu poprzez rozdzielenie zapytań administracyjnych i produkcyjnych.

Tryby połączenia

Niezależnie od zastosowanego scenariusza wdrożenia, Wheel Fudo PAM może pracować w trybie transparentnym, trybie bramy lub jako pośrednik (proxy).

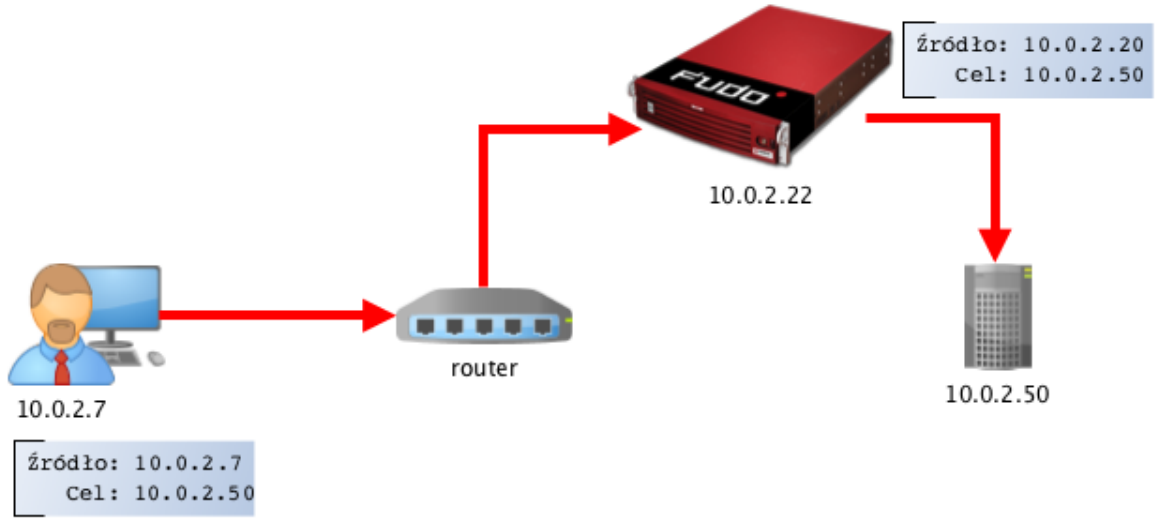
Tryb transparentny

W trybie transparentnym, klient łączy się z serwerem docelowym wskazując bezpośrednio jego adres IP. Wheel Fudo PAM zestawiając połączenie z monitorowanym zasobem używa adresu IP klienta.



Tryb bramy

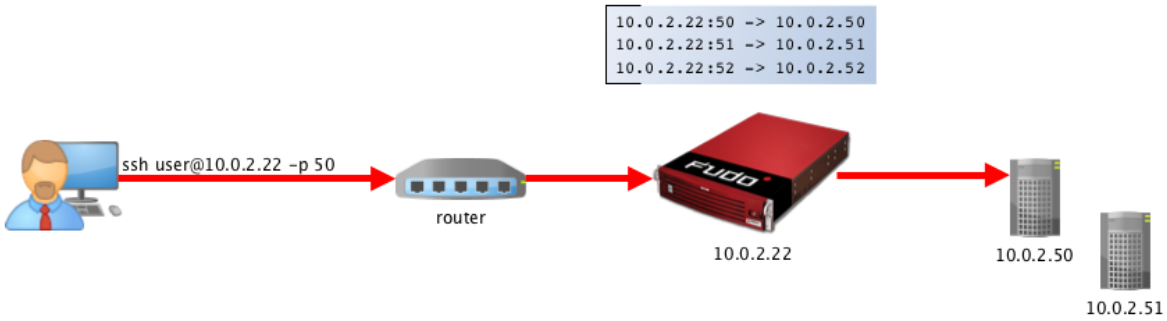
W trybie bramy, klient łączy się z serwerem docelowym wskazując bezpośrednio jego adres IP. Wheel Fudo PAM zestawiając połączenie z monitorowanym zasobem używa własnego adresu IP. Tryb pracy bramy pozwala na sterowanie ruchem sieciowym, by ten stale przechodził przez Wheel Fudo PAM, w przypadku gdy zastosowanie mają polityki kierowania ruchem.



Ustawienie adresu IP Wheel Fudo PAM jako adresu źródłowego pakietu sprawi, że odpowiedź z serwera trafi do Wheel Fudo PAM i dalej do klienta, a nie bezpośrednio do klienta.

Pośrednik

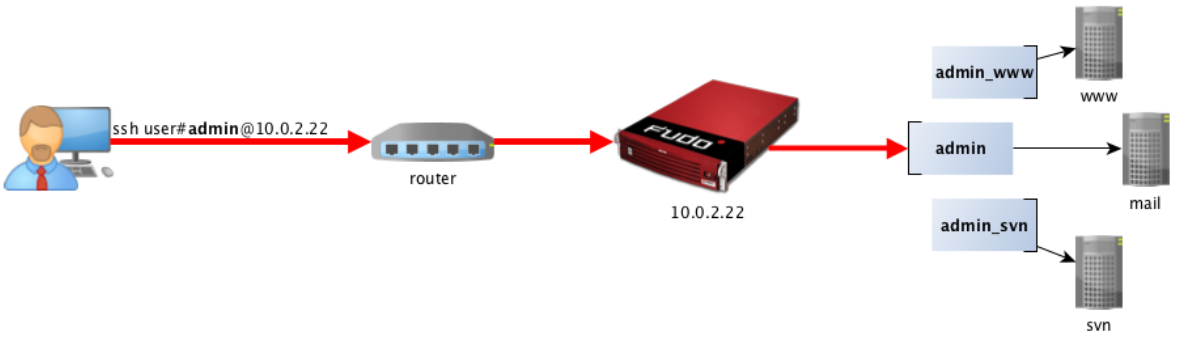
W trybie pośrednika, użytkownik nawiązuje połączenie z serwerem docelowym wskazując adres IP Wheel Fudo PAM i numer portu przypisany do danego serwera. Unikalność numeru portu pozwala na zestawienie połączenia z właściwym zasobem.



Takie rozwiązanie ukrywa faktyczną adresację serwerów, a odpowiednie ich skonfigurowanie pozwala na odrzucanie zapytań ze źródłowym adresem IP innym niż adres IP Wheel Fudo PAM.

Bastion

W trybie bastionu, konto na serwerze docelowym zdefiniowane jest w ciągu identyfikującym użytkownika, np. `ssh jan_kowalski#admin_mail_server@10.0.0.8`. Bastion pozwala na realizowanie dostępu do szeregu serwerów poprzez tę samą kombinację adresu IP i numeru portu, umożliwiając zachowanie domyślnych numerów portów dla poszczególnych protokołów.



Informacja:

- Tryb bastion wspierany jest w połączeniach realizowanych za pośrednictwem protokołów: SSH, RDP, VNC, Telnet, Telnet 3270.
- W przypadku gdy wskazane konto nie istnieje, Wheel Fudo PAM dokona próby dopasowania podanego ciągu znaków do nazwy serwera.

Tematy pokrewne:

- *Zarządzanie serwerami*
- *Metody i tryby uwierzytelniania użytkowników*
- *Opis systemu*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*
- *Pierwsze uruchomienie*

1.5 Metody i tryby uwierzytelniania użytkowników

Metody uwierzytelniania użytkowników

Wheel Fudo PAM pośrednicząc w nawiązywaniu połączeń z serwerami dokonuje uwierzytelnienia użytkowników.

Wspierane metody uwierzytelnienia:

- *Hasło statyczne*,
- *Klucz publiczny*,
- *CERB*,
- *RADIUS*,
- *LDAP*,
- *Active Directory*.

Informacja: Zewnętrzne serwery uwierzytelniania CERB, RADIUS, LDAP oraz Active Directory, wymagają wcześniejszego skonfigurowania. Szczegółowe informacje na ten temat znajdziesz w rozdziale *Zarządzanie zewnętrznymi serwerami uwierzytelnienia*.

Tryby uwierzytelnienia

Po uwierzytelnieniu użytkownika, Wheel Fudo PAM zestawia połączenie ze zdalnym serwerem używając oryginalnych danych logowania, bądź dokonując ich podmiany.

Uwierzytelnianie z przekazywaniem loginu i hasła

W trybie uwierzytelniania z przekazywaniem loginu i hasła, Wheel Fudo PAM przekazuje wprowadzone przez użytkownika dane i wykorzystuje je w stanie niezmienionym do zestawienia połączenia z serwerem.

Uwierzytelnienie z podmianą loginu i hasła

W tym trybie uwierzytelniania, wprowadzone przez użytkownika login i hasło, przy zestawianiu połączenia z serwerem, są podmieniane na wcześniej zdefiniowane.

Uwierzytelnianie z podmianą loginu i hasła pozwala na jednoznaczne wskazanie podmiotu, który nawiązywał połączenie z serwerem, w sytuacji gdy wielu użytkowników korzysta z tego samego konta użytkownika na monitorowanym serwerze.

Takie rozwiązanie pozwala na uproszczenie zarządzania użytkownikami na monitorowanych serwerach.

Informacja: Hasło dostępu do serwera docelowego może być zdefiniowane w obiekcie *Konto*, lub każdorazowo pobierane z wewnętrznego lub zewnętrznego repozytorium haseł. Więcej informacji znajdziesz w rozdziałach *Modyfikatory haseł* i *Zewnętrzne repozytoria haseł*.

Informacja: W przypadku monitorowania dostępu do baz danych Oracle, hasło użytkownika i hasło do konta uprzywilejowanego, muszą być oba krótsze niż 16 znaków lub zawierać się w

przedziale 16-32 znaków.

Podwójne uwierzytelnienie

W trybie podwójnego uwierzytelniania, użytkownik dwukrotnie podaje dane logowania. Pierwszy raz celem uwierzytelnienia przed Wheel Fudo PAM, drugi raz w celu zalogowania się do systemu docelowego.

Tematy pokrewne:

- *Opis systemu*
- *Mechanizmy bezpieczeństwa*

1.6 Mechanizmy bezpieczeństwa

Szyfrowanie danych

Dane przechowywane na Wheel Fudo PAM szyfrowane są za pomocą algorytmu AES-XTS, który wykorzystuje 256 bitowe klucze szyfrujące. Algorytm AES-XTS jest najefektywniejszym rozwiązaniem szyfrowania danych przechowywanych na napędach dyskowych.

Urządzenie fizyczne

Klucze szyfrujące przechowywane są na dwóch modułach pamięci USB (pendrive). Moduły te dostarczane są wraz z Wheel Fudo PAM w stanie niezainicjowanym. Ustalenie kluczy następuje przy pierwszym uruchomieniu urządzenia, podczas którego oba moduły pamięci USB muszą być podłączone (procedura pierwszego uruchomienia opisana jest w rozdziale *Pierwsze uruchomienie*).

Po zainicjowaniu kluczy i uruchomieniu Wheel Fudo PAM, oba moduły pamięci USB mogą zostać odłączone od urządzenia i umieszczone w bezpiecznym miejscu. W codziennej eksploatacji, klucz szyfrujący wymagany jest jedynie podczas uruchamiania systemu. Jeśli procedury bezpieczeństwa na to pozwalają, jeden z kluczy może być stale podłączony do Wheel Fudo PAM, dzięki czemu urządzenie będzie mogło uruchomić się samoczynnie w sytuacji np. zaniku zasilania, lub ponownego uruchomienia po aktualizacji systemu.

Środowisko wirtualne

W środowisku wirtualnym, system plików szyfrowany jest za pomocą frazy szyfrującej, definiowanej w procesie inicjalizacji obrazu systemu. Określony ciąg znaków musi być wprowadzony każdorazowo, podczas startu maszyny.

Kopie zapasowe

Wheel Fudo PAM posiada zaimplementowany mechanizm tworzenia kopii zapasowych danych na zewnętrznych serwerach, przy wykorzystaniu protokołu rsync.

Uprawnienia użytkowników

Każdy obiekt modelu danych posiada przypisanych użytkowników uprawnionych do zarządzania obiektem w zakresie określonym rolą użytkownika.

Rola	Prawa dostępu
user	• łączenie z serwerami w ramach zdefiniowanych sejfów, do których użytkownik został przypisany • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
operator	• logowanie do panelu administracyjnego • przeglądanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • odtwarzanie sesji, w której pośredniczyły obiekty, do których użytkownik posiada uprawnienia • blokowanie/odblokowywanie wybranych obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • generowanie i subskrybowanie raportów • włączanie/wyłączanie powiadomień email • konwersja sesji i pobieranie skonwertowanego materiału • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
admin	• logowanie do panelu administracyjnego • zarządzanie obiektami: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, do których użytkownik posiada uprawnienia • blokowanie/odblokowywanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • generowanie i subskrybowanie raportów • konwersja sesji i pobieranie skonwertowanego materiału • włączanie/wyłączanie powiadomień email • zarządzanie politykami • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • odtwarzanie sesji, w której pośredniczyły obiekty, do których użytkownik posiada uprawnienia • zarządzanie modyfikatorami haseł • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
superadmin	• zarządzanie obiektami bez ograniczeń • zarządzanie konfiguracją urządzenia bez ograniczeń • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).

Sandboxing

Wheel Fudo PAM wykorzystuje mechanizm sandboxowania CAPSICUM, który separuje poszczególne połączenia na poziomie systemu operacyjnego Wheel Fudo PAM. Ścisła kontrola przydzielonych zasobów systemowych i ograniczenie dostępu do informacji na temat systemu operacyjnego, zwiększają bezpieczeństwo oraz znacząco wpływają na stabilność systemu.

Niezawodność

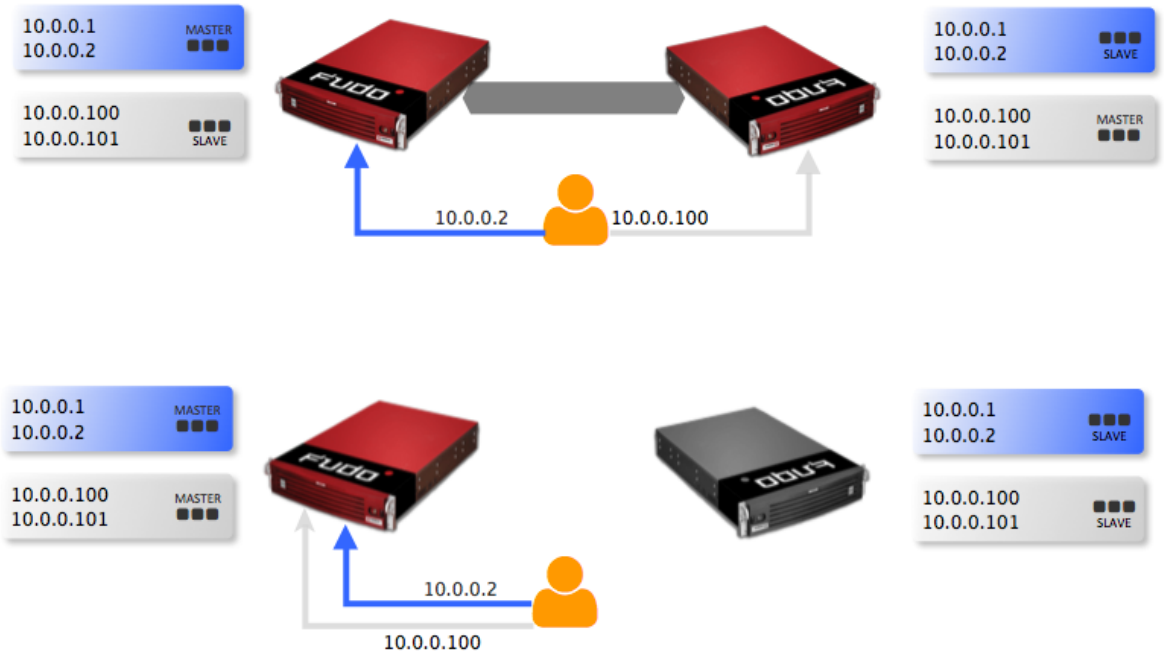
Wheel Fudo PAM dostarczane jest w konfiguracji sprzętowej zapewniającej optymalną wydajność i wysoką niezawodność systemu.

Konfiguracja klastrowa

Wheel Fudo PAM może pracować w konfiguracji klastrowej. Układ klastrowy pracuje w trybie multimaster, w którym konfiguracja systemu (połączenia, serwery, sesje, etc.) synchronizowana jest na każdym z węzłów klastra. W przypadku awarii węzła następuje automatyczne przełączenie na inny węzeł, co pozwala na zachowanie ciągłości świadczenia usług.

Ostrzeżenie: Konfiguracja klastrowa nie jest mechanizmem tworzenia kopii zapasowych danych. Dane sesji usunięte z jednego węzła, zostaną również usunięte z pozostałych węzłów klastra.

Adresy klastrowe agregowane są w grupy redundancji, które pozwalają na realizowanie statycznej dystrybucji żądań użytkowników na poszczególne węzły klastra, zachowując przy tym niezawodnościowy charakter klastra.



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Opis systemu*
- *Szybki start*
- *Pierwsze uruchomienie*

1.7 Wymagania

Panel zarządzający

Zarządzanie systemem odbywa się za pomocą panelu administracyjnego dostępnego z poziomu przeglądarki internetowej. Zalecanymi przeglądarkami są Google Chrome oraz Mozilla Firefox.

Wymagania sieciowe

Poprawne działanie Wheel Fudo PAM wymaga:

- możliwości wykonywania połączeń dla sesji administracyjnych na port 443 urządzenia,
- możliwości wykonywania połączeń do Wheel Fudo PAM przez klientów oraz z Wheel Fudo PAM do maszyn docelowych.

Wymagania sprzętowe (*nie dotyczy maszyny wirtualnej*)

Wheel Fudo PAM jest całościowym rozwiązaniem sprzętowo-programowym. Zainstalowanie urządzenia wymaga fizycznej przestrzeni 2U w szafie serwerowej oraz podłączenie do infrastruktury sieciowej.

Wymagania dla klienta VNC

Połączenia VNC muszą być realizowane w trybie odwzorowania kolorów 24-bit (true color).

ROZDZIAŁ 2

Konfiguracja

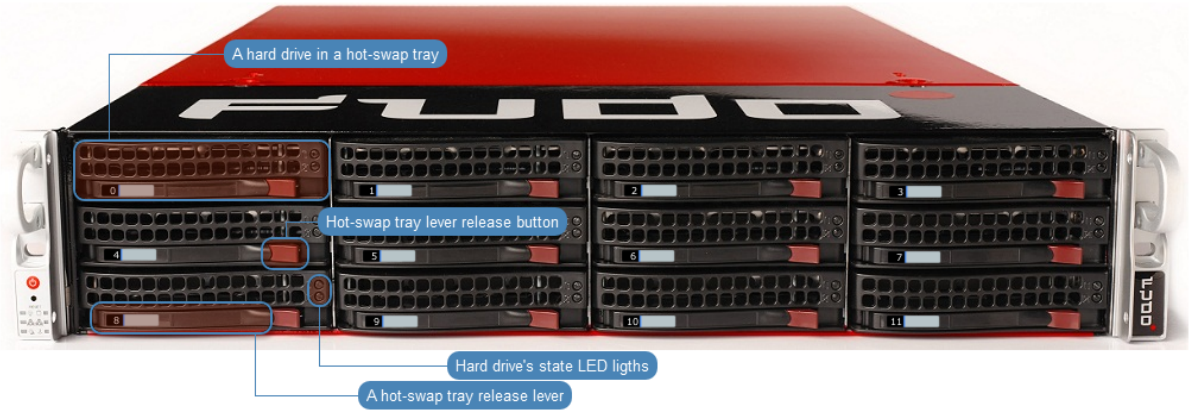
2.1 Urządzenie

Wheel Fudo PAM dostarczane jest w obudowie do montażu w standardowej szafie serwerowej 19".

Panel przedni

Zatoki dysków twardych

Pod przednim panelem obudowy, znajdują się zatoki dysków twardych, w kieszeniach umożliwiających wymianę dysku bez konieczności wyłączania urządzenia («hot-swap»).



Tematy pokrewne:

- *Pierwsze uruchomienie*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*

2.2 Pierwsze uruchomienie

2.2.1 Urządzenie fizyczne

Wheel Fudo PAM dostarczane jest z dwoma nośnikami pamięci USB, w stanie niezainicjowanym. Podczas pierwszego uruchomienia generowane są klucze szyfrujące, które zostają zapisane na dołączonych modułach pamięci USB. Więcej na temat kluczy szyfrujących znajdziesz w rozdziale *Mechanizmy bezpieczeństwa*.

Procedura pierwszego uruchomienia

1. Umieść urządzenie w szafie serwerowej 19".
2. Podłącz obydwa zasilacze do instalacji elektrycznej 230V.

Informacja: Podłączenie obydwu zasilaczy jest konieczne do uruchomienia systemu.

---

3. Podłącz kabel sieciowy do jednego z portów RJ-45.
4. Podłącz dostarczone wraz z urządzeniem nośniki pamięci flash do portów USB.

Informacja: Pierwsze uruchomienie wymaga podłączenia obu nośników pamięci. Więcej na temat inicjacji kluczy szyfrujących znajdziesz w rozdziale *Mechanizmy bezpieczeństwa*.

---

5. Wciśnij przycisk zasilania znajdujący się na przednim panelu obudowy.

6. Po zainicjowaniu kluczy szyfrujących, odłącz nośniki pamięci.

Ostrzeżenie:

- Bezwzględnie odłącz jeden z nośników i umieść w bezpiecznym miejscu, do którego dostęp mają tylko osoby upoważnione.
- Jeśli nośniki pamięci z zapisanymi kluczami zostaną utracone, urządzenie nie będzie mogło zostać uruchomione, a przechowywane tam dane nie będą dostępne. Producent nie przechowuje żadnych kluczy.

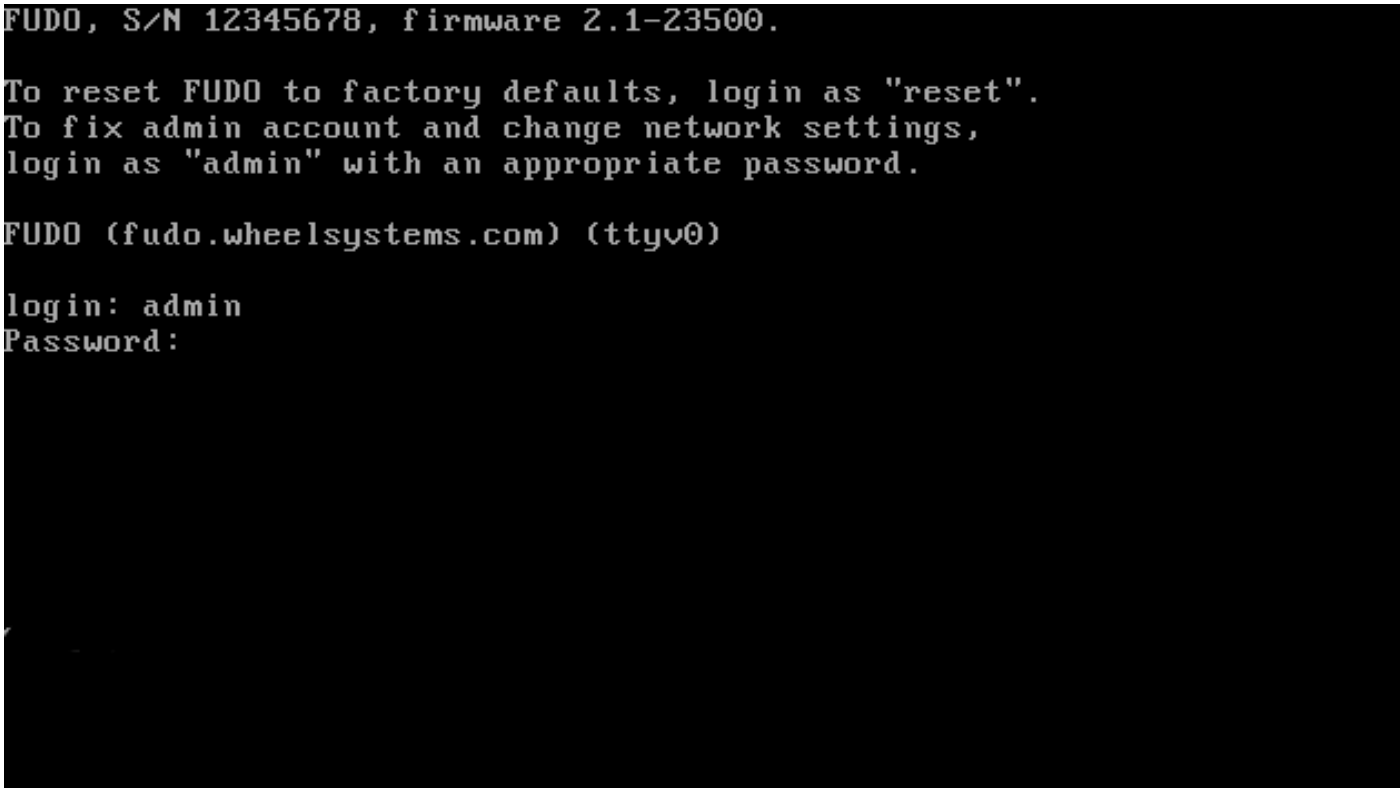
Informacja:

- W codziennej eksploatacji, jeden klucz szyfrujący potrzebny jest tylko do uruchomienia urządzenia, po czym może zostać odłączony.
- Zaleca się utworzenie dodatkowej kopii bezpieczeństwa klucza szyfrującego.

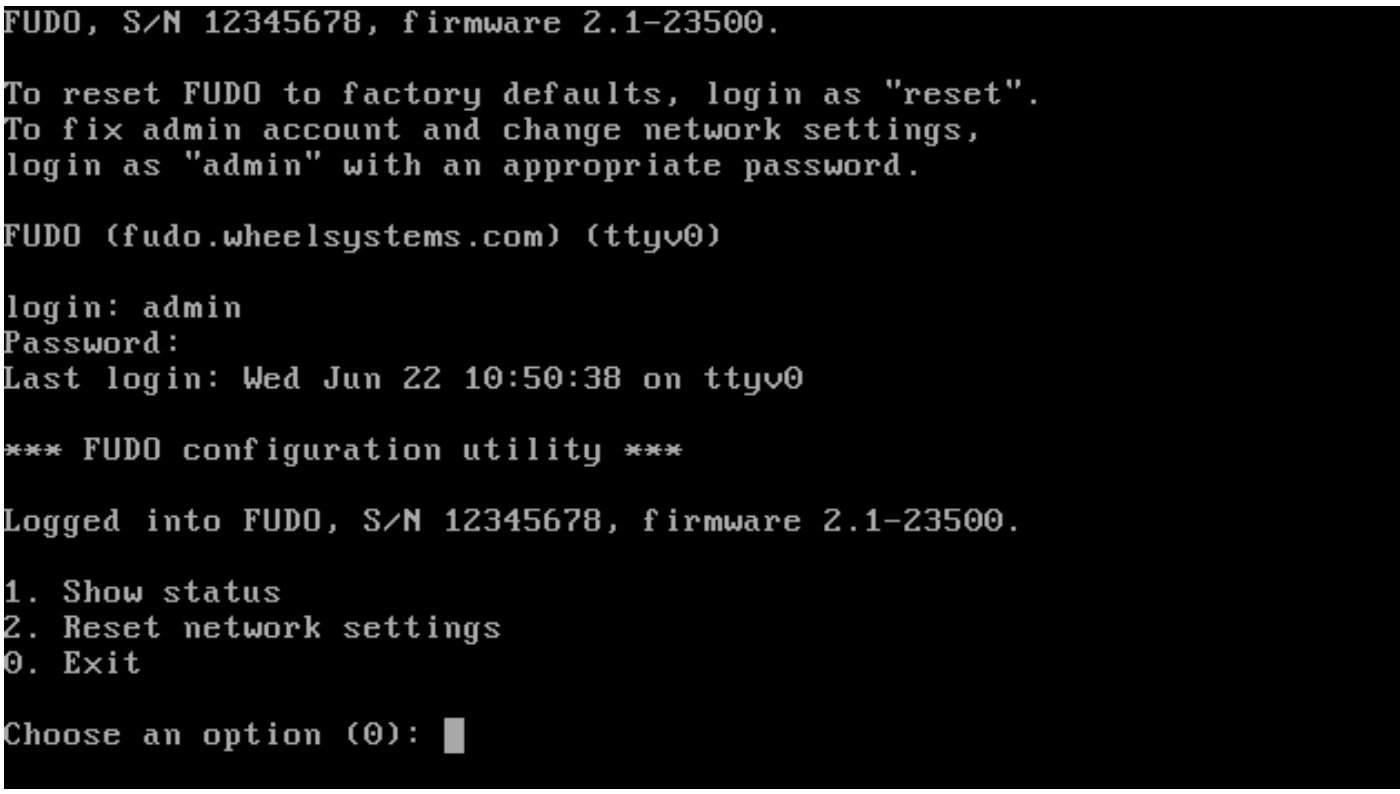
Ustawienie adresu IP z konsoli

1. Wprowadź login konta administratora.

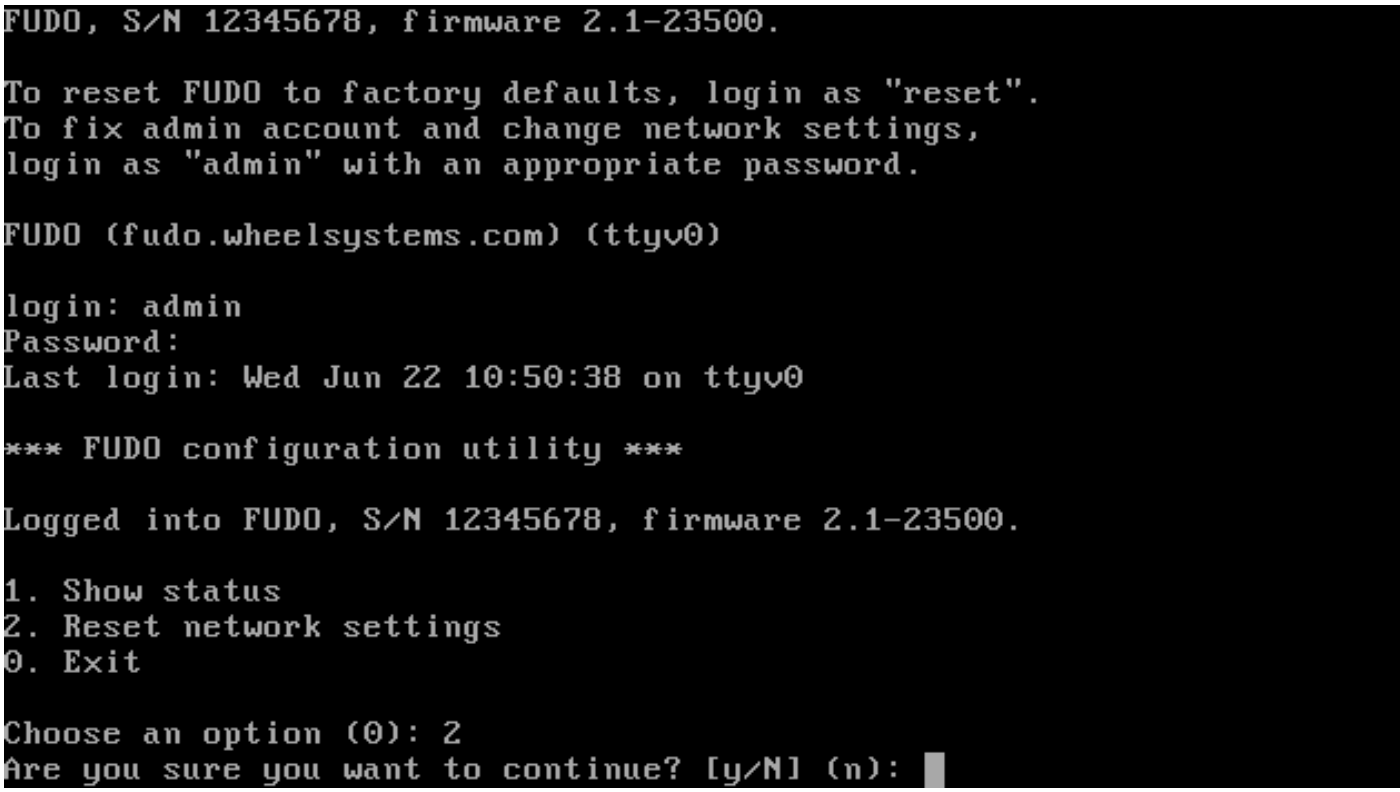
2. Wprowadź hasło do konta administratora.



3. Wpisz 2 i naciśnij klawisz *Enter*.



4. Wpisz y i naciśnij klawisz *Enter*, aby potwierdź chęć zmiany ustawień sieciowych.



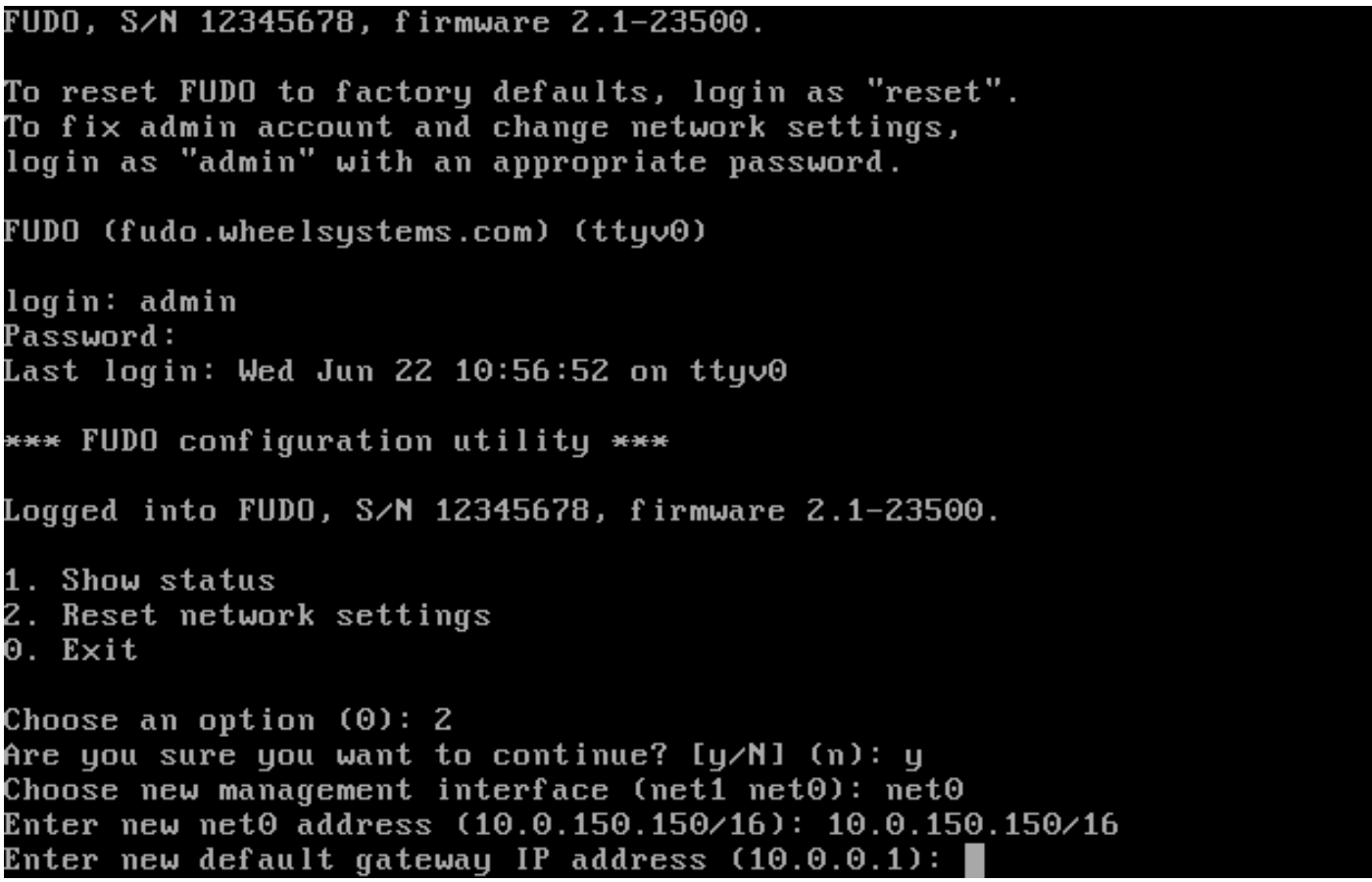
5. Wprowadź nazwę interfejsu zarządzającego (poprzez interfejs zarządzający udostępniany jest panel administracyjny Wheel Fudo PAM) i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0):
```

6. Wprowadź adres IP urządzenia wraz z maską podsieci oddzieloną znakiem `/` (np. `10.0.0.8/24`) i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
```

7. Wprowadź bramę sieci i naciśnij klawisz *Enter*.



Tematy pokrewne:

- *Wymagania*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*
- *Opis systemu*
- *Mechanizmy bezpieczeństwa*

2.3 Szybki start

2.3.1 SSH

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń SSH ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *SSH* uwierzytelnia się na Wheel Fudo PAM używając własnego loginu i hasła (`john_smith`/`john`). Wheel Fudo PAM zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `root`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

Konfiguracja

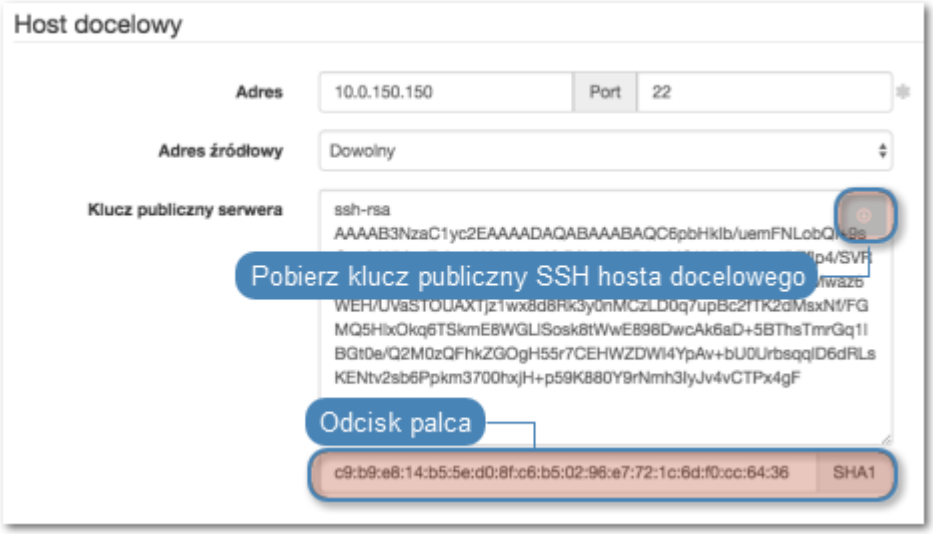
Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	ssh_server
Zablokowane	✗
Protokół	`SSH`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.150.150`
Port	`22`
Adres źródłowy	`Dowolny`

4. Pobierz lub wprowadź klucz publiczny SSH hosta docelowego.



5. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (indywidualny login, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzilnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Sejfy	ustawienia domyślne
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

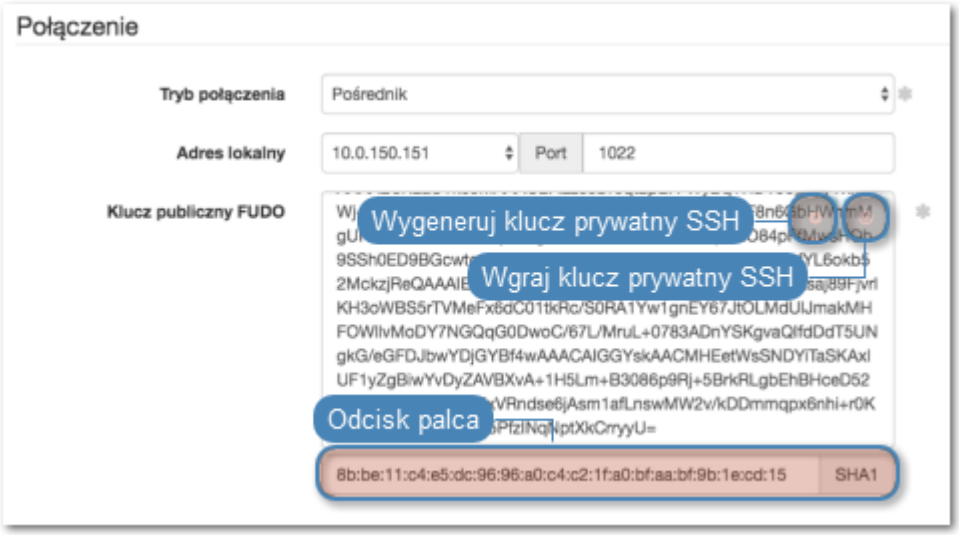
Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`ssh_listener`
Zablokowane	✗
Protokół	`SSH`
Uprawnienia	
Uprawnieni użytkownicy	✗
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`1022`

4. Kliknij ikonę wygenerowania klucza SSH lub wgraj klucz prywatny serwera.



Informacja: Ze względów bezpieczeństwa, formularz wyświetla klucz publiczny odpowiadający wgranemu lub wygenerowanemu kluczowi prywatnemu.

5. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_ssh_server`
Zablokowane	
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	
Serwer	
Serwer	`ssh_server`
Dane uwierzytelniające	
Domena	
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	
Modyfkator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	
Hasło użytkownika uprzywilejowanego	

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

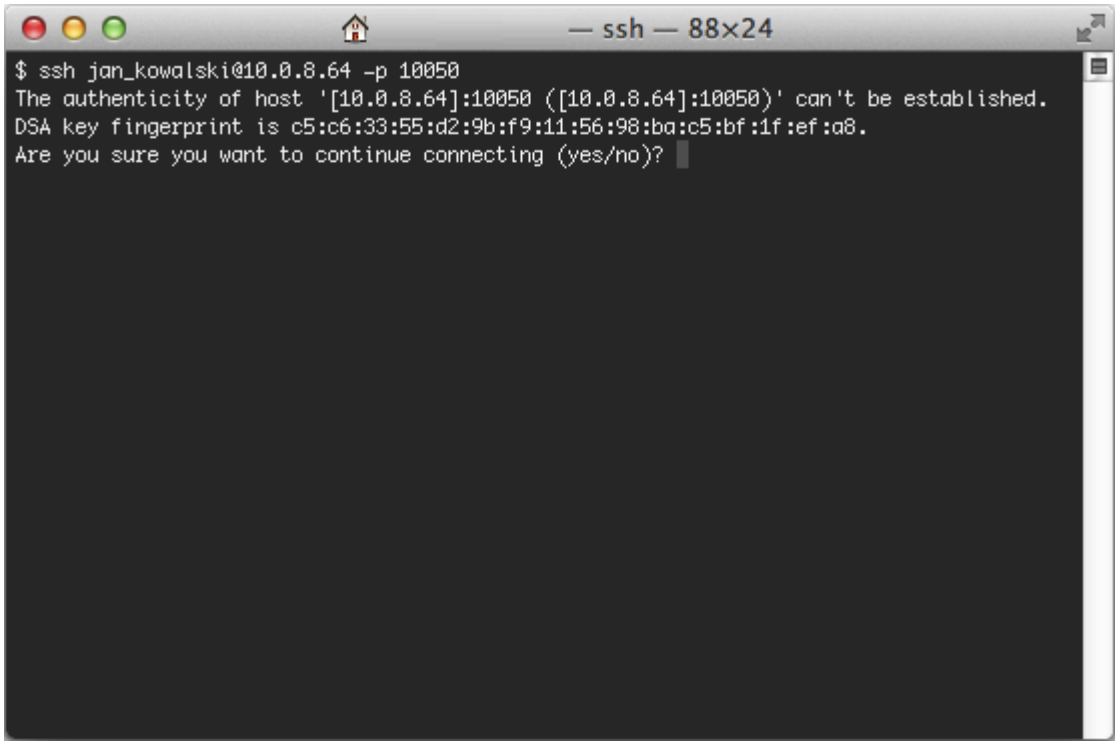
Parametr	Wartość
Nazwa	`ssh_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Funkcjonalność protokołów	
RDP	✗
SSH	✓
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Powiązania obiektu	
Użytkownicy	`john_smith`
Konta	`admin_ssh_server`
Gniazda nasłuchiwania	`ssh_listener`

4. Kliknij *Zapisz*.

Nawiązanie połączenia

W tym momencie użytkownik `jan_kowalski` może już podjąć próbę logowania.

Przykład:



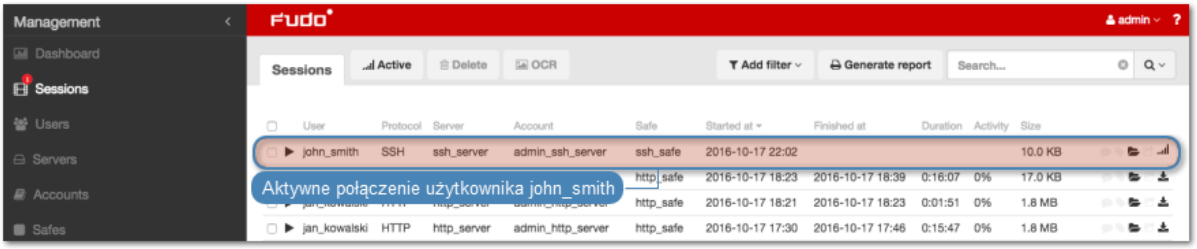
Informacja: Zwróć uwagę na *Odcisk Palca* (fingerprint), który wyświetla się przy pierwszym

połączeniu. Jest to ten sam odcisk, który został wygenerowany w czasie dodawania serwera.

Po potwierdzeniu połączenia, użytkownik zostanie zapytany o hasło. Po uwierzytelnieniu sesja będzie podlegała monitorowaniu i rejestracji.

Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres `10.0.150.151`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Wymagania*
- *Model danych*
- *Konfiguracja*

2.3.2 RDP

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń RDP ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta *RDP* używając indywidualnego loginu i hasła. Wheel Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników i zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `admin`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone a system został skonfigurowany do pracy w trybie mostu lub odpowiednio został skonfigurowany routing połączeń administracyjnych. Informacje na temat scenariuszy wdrożenia znajdziesz w rozdziale *Scenariusze wdrożenia*.

Konfiguracja

Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	rdp_server
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Opis	`Serwer RDP`
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.35.10`
Port	`3389`
Adres źródłowy	`Dowolny`

4. Pobierz lub wprowadź certyfikat hosta docelowego.
5. Kliknij *Zapisz*.

Dodanie użytkownika

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Sejfy	ustawienia domyślne
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

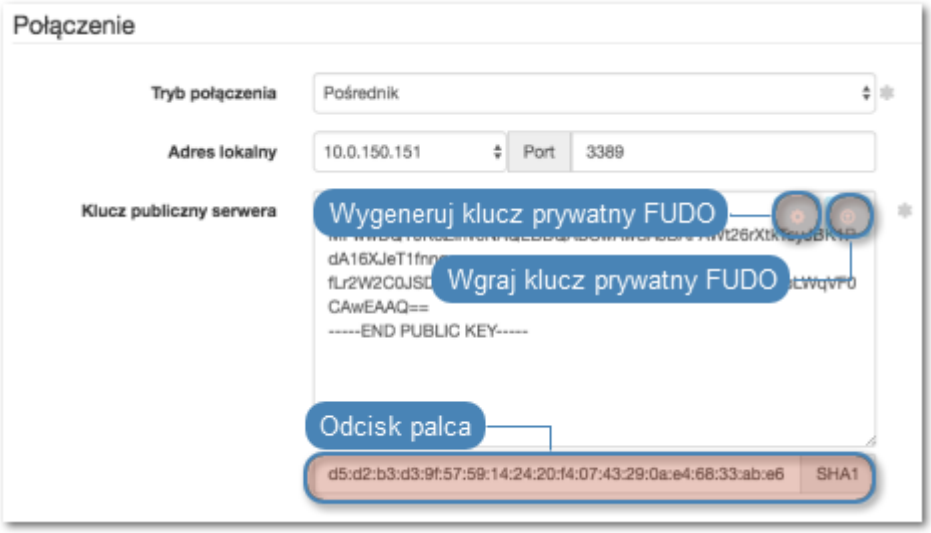
Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`rdp_listener`
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Komunikat	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`3389`

4. Kliknij ikonę wygenerowania certyfikatu TLS lub wgraj klucz prywatny i publiczny w formacie PEM.



5. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_rdp_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✓
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`rdp_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗
Modyfkator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

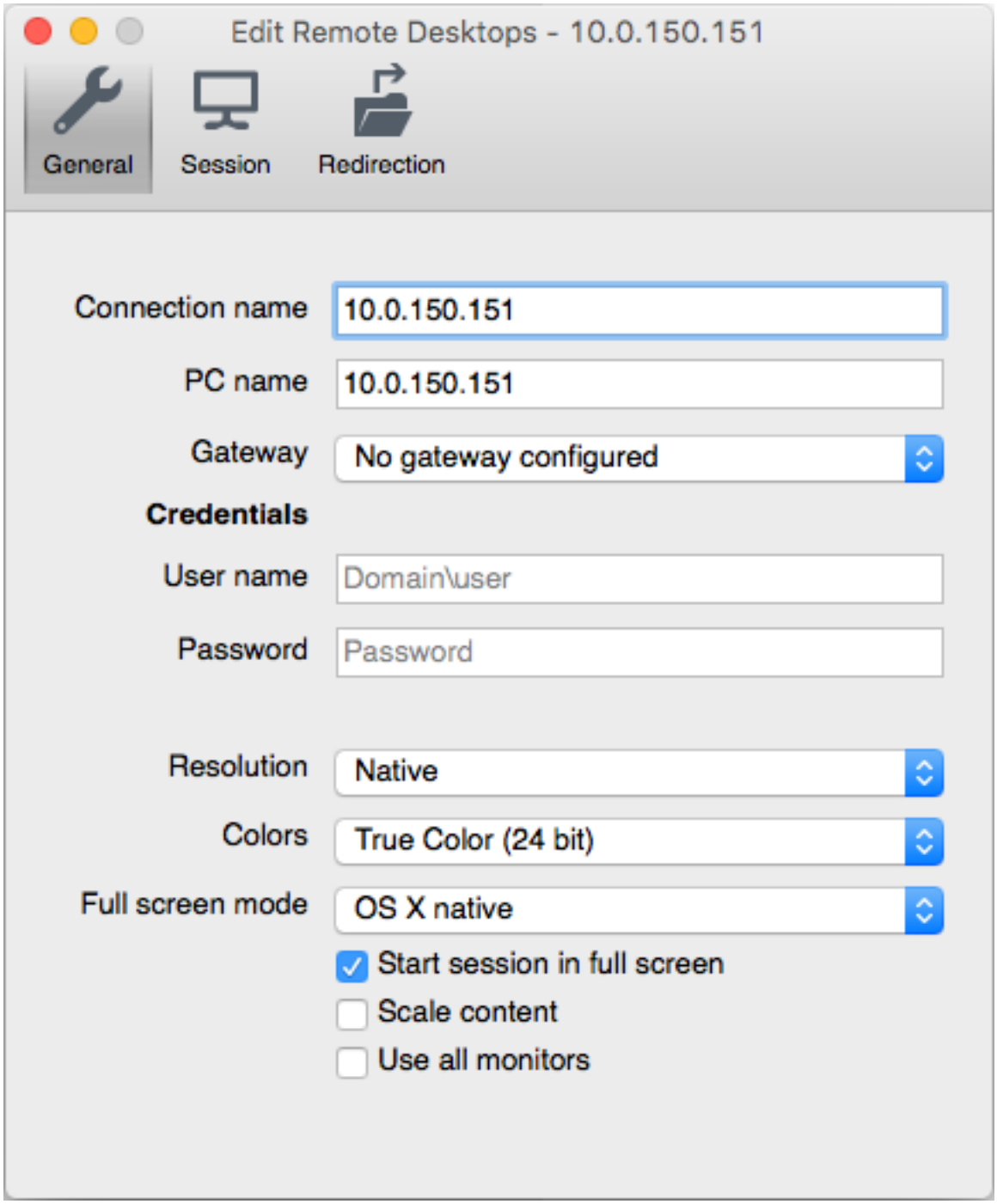
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`rdp_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Funkcjonalność protokołów	
RDP	✓
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Powiązania obiektu	
Użytkownicy	`john_smith`
Konta	`admin_rdp_server`
Gniazda nasłuchiwania	`rdp_listener`

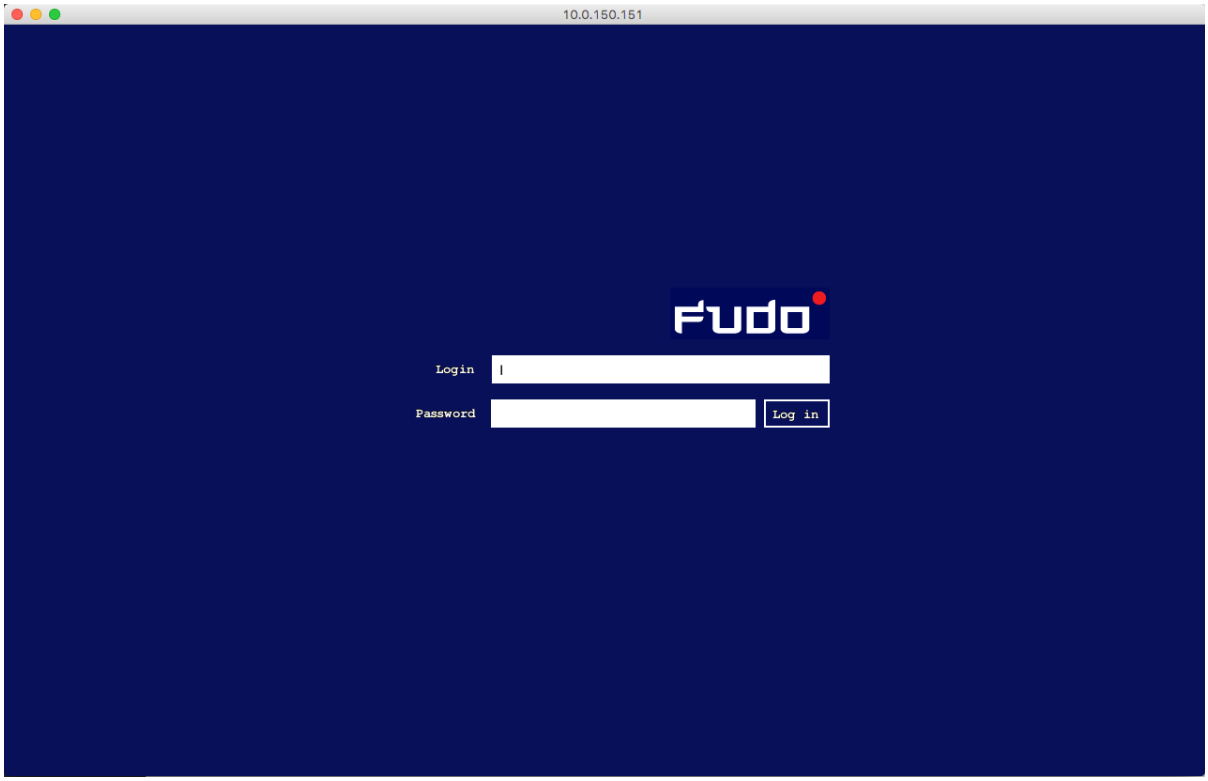
4. Kliknij *Zapisz*.

Nawiązanie połączenia

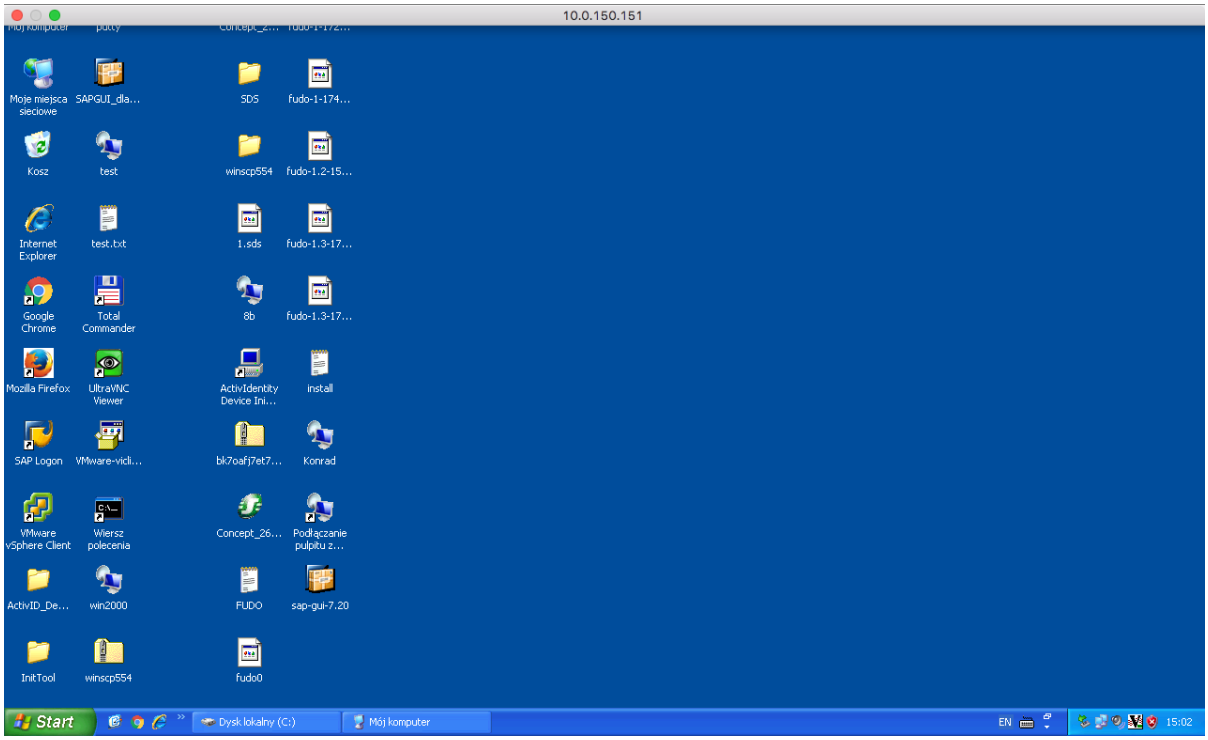
1. Uruchom klienta połączeń RDP.
2. Skonfiguruj połączenie zdalnego pulpitu.



3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter].



Informacja: Wheel Fudo PAM pozwala na zastosowanie własnych ekranów logowania, braku dostępu i zakończenia sesji dla połączeń RDP i VNC. Więcej informacji na temat konfigurowania własnych ekranów dla połączeń graficznych, znajdziesz w sekcji *Zasoby*.



Podgląd sesji połączeniowej

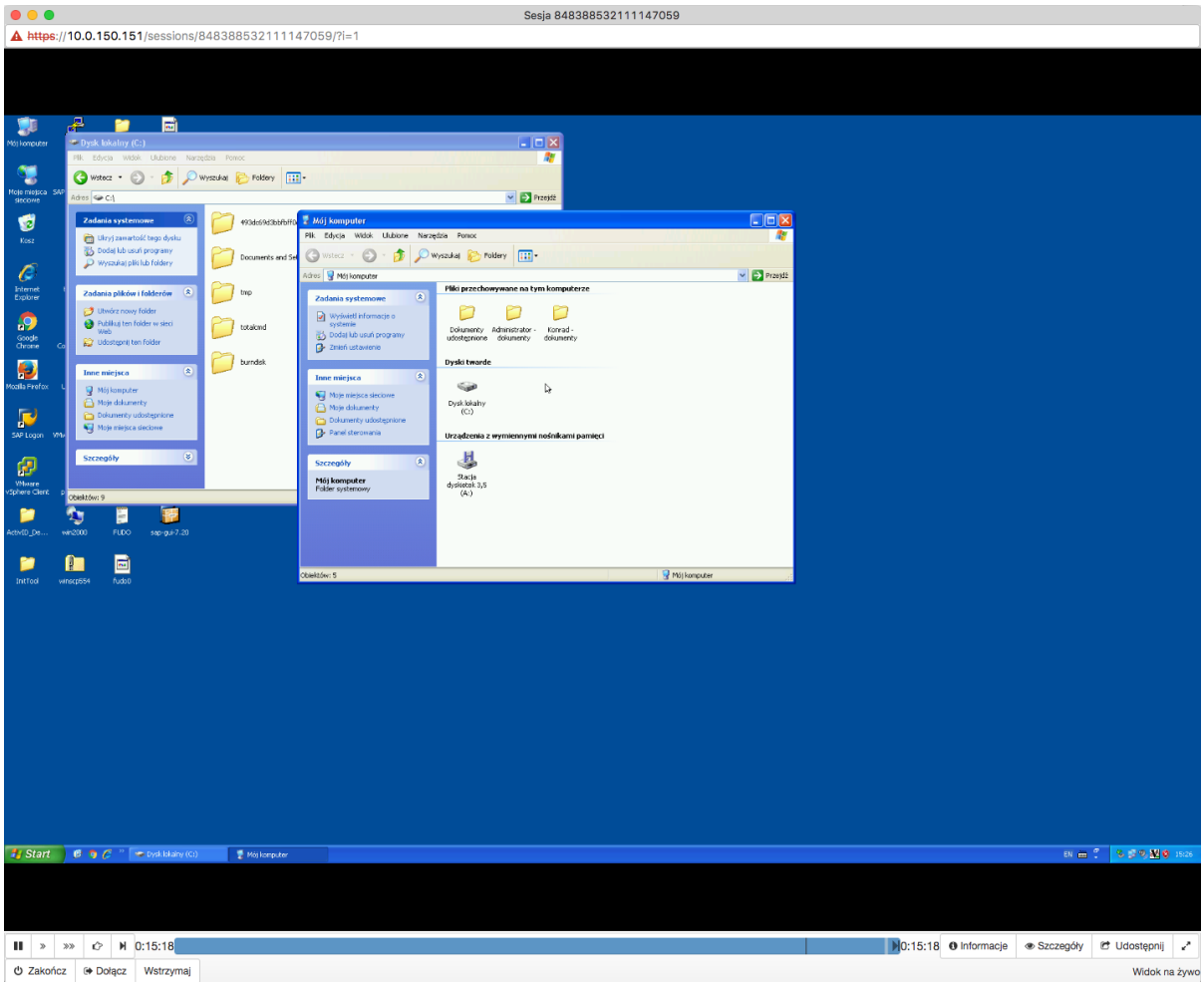
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający

Wheel Fudo PAM.

Informacja: Upewnij się, że wskazany adres IP ma włączoną opcję udostępniania panelu zarządzającego.

---

2. Wprowadź nazwę użytkownika oraz hasło aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia SSH*

- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Telnet*
- *Zasoby*
- *Model danych*
- *Konfiguracja*

2.3.3 MySQL

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń ze zdalnym serwerem baz danych MySQL. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta MySQL używając indywidualnego loginu i hasła. Wheel Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników i zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `admin`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

Konfiguracja

Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	mysql_server
Zablokowane	✗
Protokół	`MySQL`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.1.35`
Port	`3306`
Adres źródłowy	`Dowolny`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (indywidualny login, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzilnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`mysql_listener`
Zablokowane	
Protokół	`MySQL`
Uprawnienia	
Uprawnieni użytkownicy	
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.40.50`
Port	`3306`

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_mysql_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`mysql_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗
Modyfkator hasła	
Modyfikator hasła	`brak`
Użytkownik uprzywilejowany	✗
Hasło użytkownika uprzywilejowanego	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

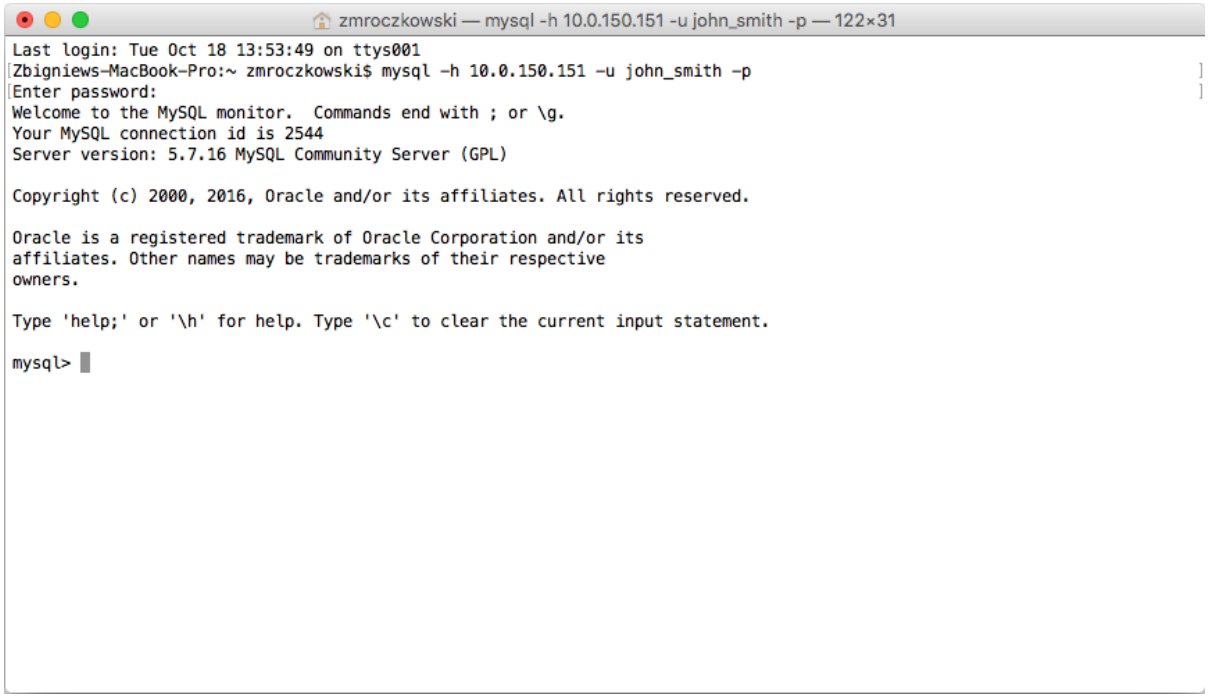
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`msyql_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Powiązania obiektu	
Użytkownicy	`john_smith`
Konta	`admin_mysql_server`
Gniazda nasłuchiwania	`mysql_listener`

4. Kliknij *Zapisz*.

Nawiązanie połączenia

1. Uruchom terminal tekstowy.
2. Wprowadź komendę `mysql -h 10.0.150.151 -u john_smith -p`, aby nawiązać połączenie z serwerem baz danych.
3. Wprowadź hasło użytkownika.



4. Kontynuuj przeglądanie zawartości serwera poprzez zapytania sql.

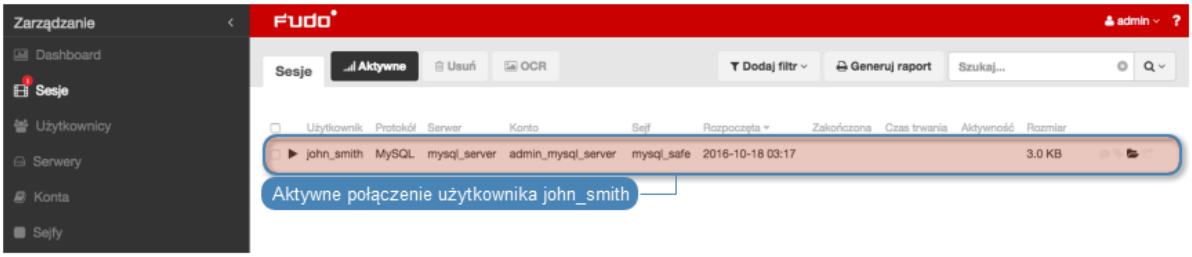
Podgląd sesji połączeniowej

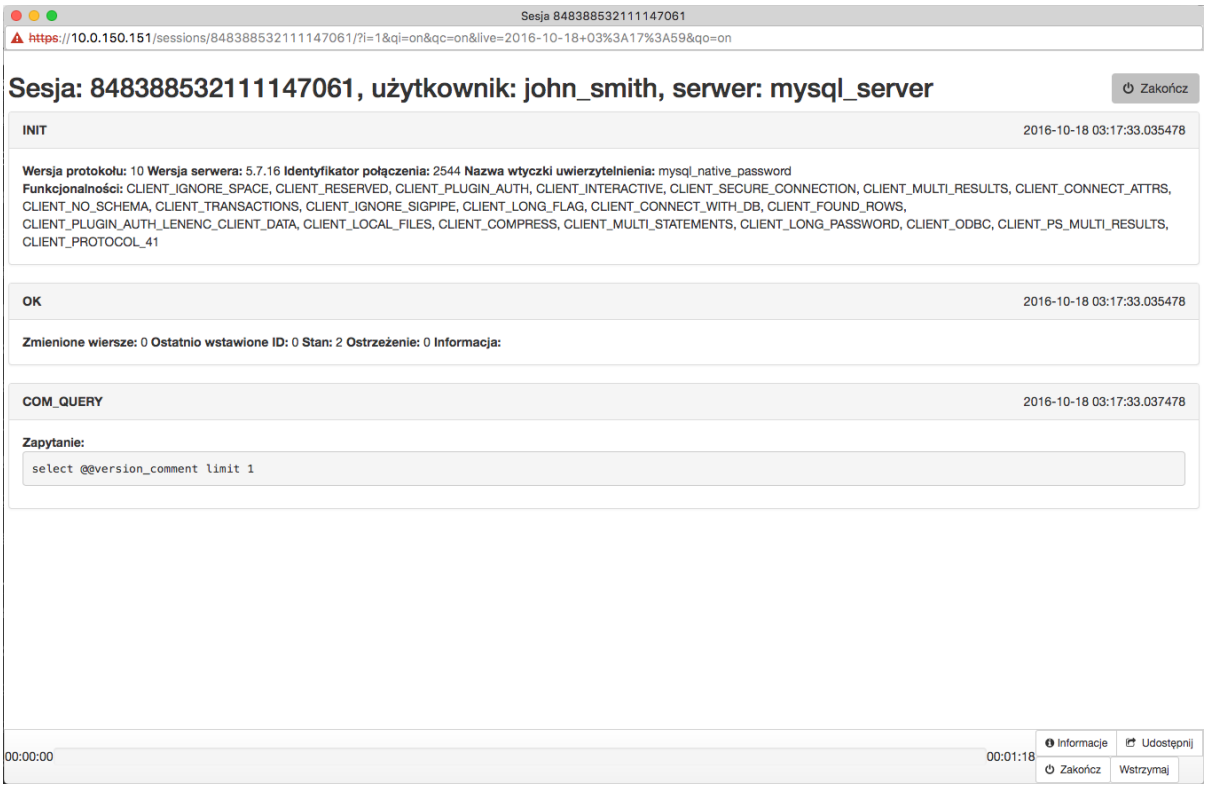
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.

Informacja: Upewnij się, że wskazany adres IP ma włączoną opcję udostępniania panelu zarządzającego.

---

2. Wprowadź nazwę użytkownika oraz hasło aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.





Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia RDP*

- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Telnet*
- *Wymagania*
- *Model danych*
- *Konfiguracja*

2.3.4 HTTP

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń HTTP ze zdalnym serwerem. Scenariusz zakłada, że użytkownik przegląda zasoby monitorowanego serwera korzystając z przeglądarki internetowej. Użytkownik uwierzytelniany jest przez Wheel Fudo PAM na podstawie danych zapisanych w lokalnej bazie użytkowników. Sesja połączeniowa będzie wymagała ponownego uwierzytelnienia po 15 minutach (900 sekund) braku aktywności.

Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

Konfiguracja

Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery.*
2. Kliknij + *Dodaj.*
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	http_server
Zablokowane	✗
Protokół	`HTTP`
Czas oczekiwania HTTP	`900`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`www.wheelsystems.com`
Port	`80`
Host HTTP	✗
Użyj TLS	✗

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (indywidualny login, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzilnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	✗
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗
Domena AD	✗
Baza LDAP	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij Zapisz.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`http_listener`
Zablokowane	
Protokół	`HTTP`
Uprawnienia	
Uprawnieni użytkownicy	
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`8080`
Użyj bezpiecznych połączeń (TLS)	

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_http_server`
Zablokowane	✗
Typ	`forward`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`http_server`
Dane uwierzytelniające	
Zastąp sekret	`hasłem`
Hasło	✗
Powtórz hasło	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

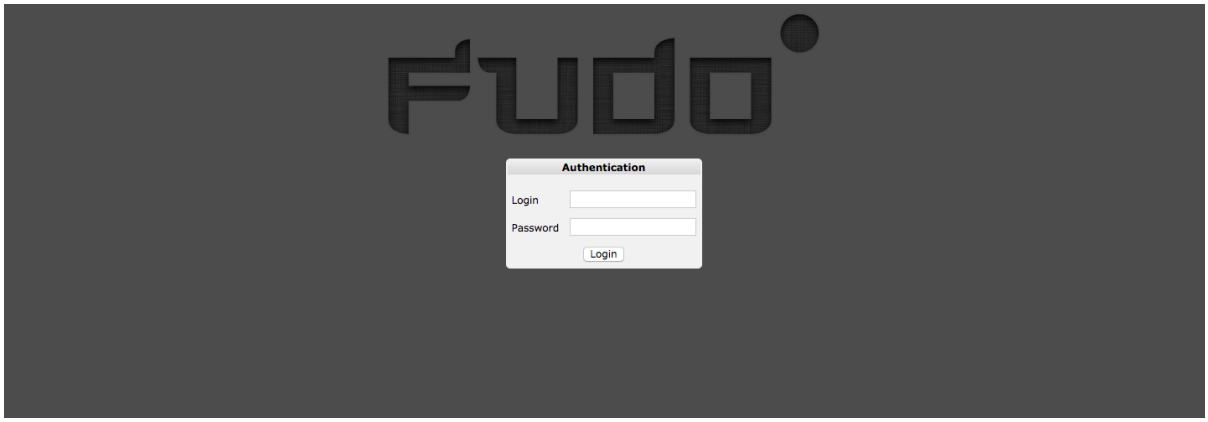
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`http_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Powiązania obiektu	
Użytkownicy	`john_smith`
Konta	`admin_http_server`
Gniazda nasłuchiwania	`http_listener`

4. Kliknij *Zapisz*.

Nawiązanie połączenia

1. Uruchom przeglądarkę internetową.
2. W pasku adresu wprowadź 10.0.150.151:8080.
3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter] lub klikając przycisk *Login*.

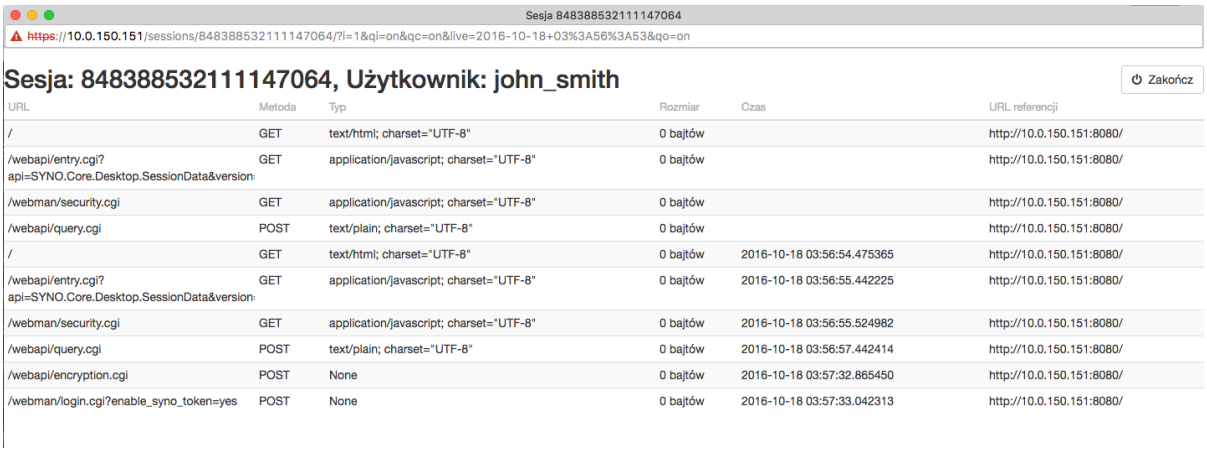


4. Kontynuuj przeglądanie serwisu.

Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.

4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Wymagania*
- *Model danych*
- *Konfiguracja*

2.3.5 Telnet

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Wheel Fudo PAM, której celem jest monitorowanie połączeń Telnet ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta protokołu Telnet używając indywidualnego loginu i hasła. Wheel Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników, zestawia połączenie ze zdalnym zasobem i rozpoczyna rejestrowanie akcji użytkownika.

Informacja: Połączenia telnet realizowane za pośrednictwem Wheel Fudo PAM nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu przez Wheel Fudo PAM musi uwierzytelnić się na serwerze docelowym po zestawieniu połączenia.

Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia opisana jest w rozdziale *Pierwsze uruchomienie*.

Konfiguracja

Dodanie serwera

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	telnet_server
Zablokowane	✗
Protokół	`Telnet`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres	`10.0.35.137`
Port	`23`
Adres źródłowy	`Dowolny`
Użyj bezpiecznych połączeń TLS	✗

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (indywidualny login, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzilnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij + *Dodaj*.

3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Login	`john_smith`
Zablokowane	
Ważność konta	`Bezterminowe`
Rola	`user`
Preferowany język	`polski`
Pełna nazwa	`John Smith`
Email	
Organizacja	
Telefon	
Domena AD	
Baza LDAP	
Uprawnienia	
Uprawnieni użytkownicy	
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`telnet_listener`
Zablokowane	
Protokół	`Telnet`
Włącz obsługę SSLv2	
Włącz obsługę SSLv3	
Uprawnienia	
Uprawnieni użytkownicy	
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`23`
Użyj bezpiecznych połączeń TLS	

4. Kliknij *Zapisz*.

Dodanie konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`admin_telnet_server`
Zablokowane	✗
Typ	`forward`
Nagrywanie sesji	`wszystko`
OCR sesji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`telnet_server`
Dane uwierzytelniające	
Zastąp sekret	`hasłem`
Hasło	✗
Powtórz hasło	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Ogólne	
Nazwa	`telnet_safe`
Zablokowane	✗
Powód logowania	✗
Powiadomienia	✗
Polityki	✗
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Powiązania obiektu	
Użytkownicy	`john_smith`
Konta	`admin_telnet_server`
Gniazda nasłuchiwania	`telnet_listener`

4. Kliknij *Zapisz*.

Nawiązanie połączenia

1. Uruchom klienta połączeń Telnet.
2. Nawiąż połączenie z serwerem:

```
telnet> open 10.0.150.151
Trying 10.0.150.151...
Connected to 10.0.150.151.
Escape character is '^]'.
```

3. Wprowadź dane uwierzytelniające użytkownika na Wheel Fudo PAM:

```
FUDO Authentication.
FUDO Login: john_smith
FUDO Password: john
```

4. Wprowadź dane uwierzytelniające użytkownika na serwerze:

```
FreeBSD/amd64 (fbsd83-cerb.whl) (pts/0)
login:
password:
```

Informacja: Połączenia telnet nie wspierają mechanizmów podmiany danych logowania.

Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Wheel Fudo PAM.

Informacja: Upewnij się, że wskazany adres IP ma włączoną opcję udostępniania panelu zarządzającego.

2. Wprowadź nazwę użytkownika oraz hasło aby zalogować się do interfejsu administracyjnego Wheel Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Kliknij *Aktywne*.
5. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.

Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia RDP*
- *Zasoby*
- *Model danych*
- *Konfiguracja*

2.3.6 Konfigurowanie modyfikatora haseł

W tym rozdziale przedstawiony jest przykład konfigurowania automatycznej zmiany haseł na serwerze Unix.

Konfiguracja

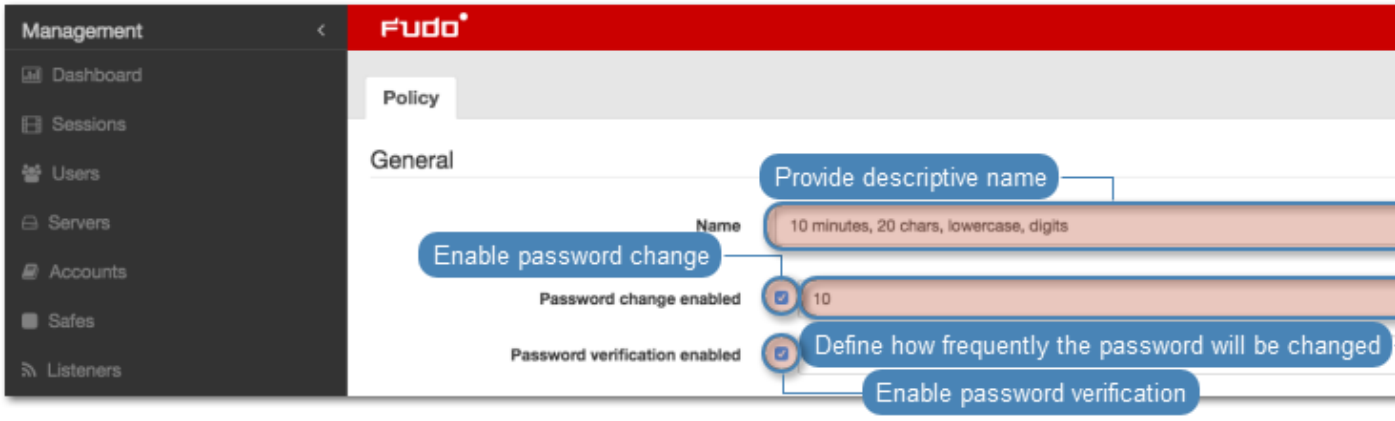
Dodanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Kliknij *+ Dodaj*.
3. Wprowadź nazwę polityki zmany haseł.

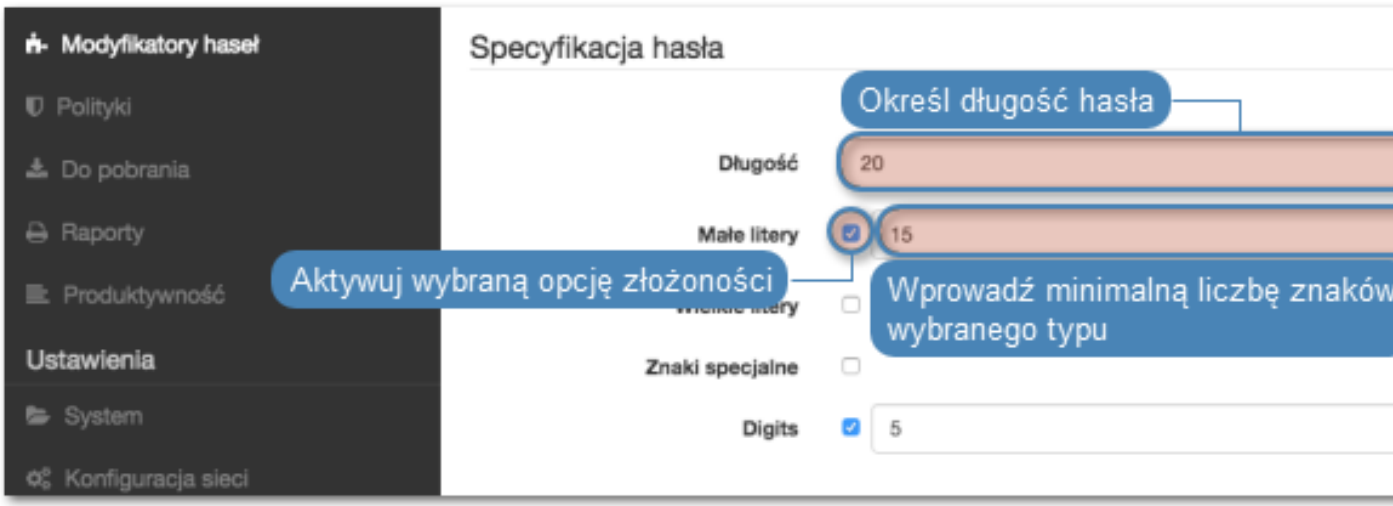
Informacja: Opisowa nazwa pozwoli osobom administrującym Wheel Fudo PAM, szybko zorientować się w charakterystyce polityki zmiany haseł, np. `10 minut, 20 znaków, znaki specjalne, wielkie litery`.

4. Zaznacz opcję *Zmiana haseł włączona* i zdefiniuj częstotliwość zmiany haseł.

5. Zaznacz opcję *Weryfikacja haseł włączona* i zdefiniuj jak często mechanizm będzie weryfikował, czy hasło nie zostało zmienione w sposób nieuprawniony.



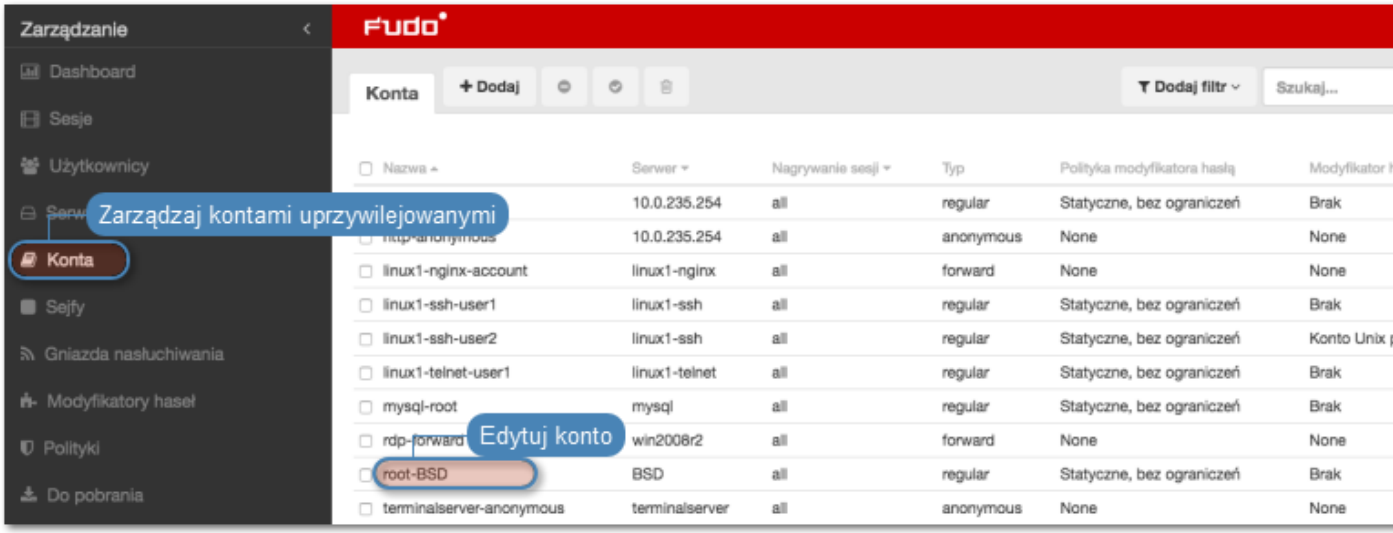
6. Wprowadź liczbę znaków hasła.
7. Zaznacz wybrane opcje złożoności hasła i wprowadź minimalną liczbę znaków dla każdej z nich.



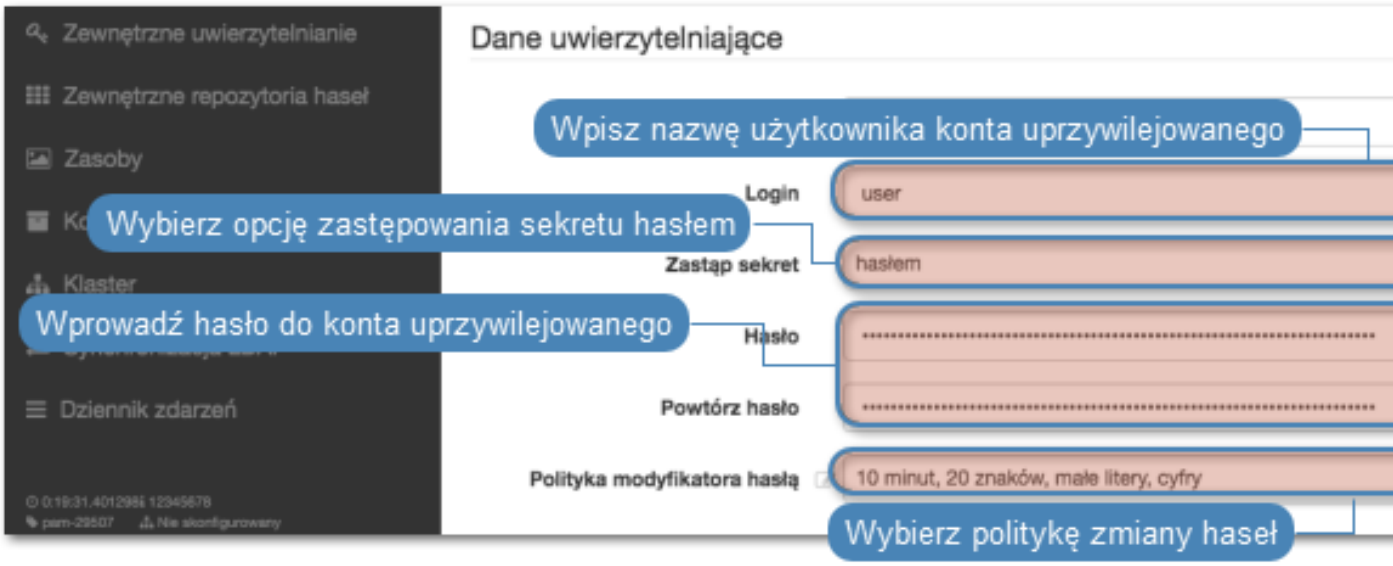
8. Kliknij *Zapisz*, aby zapisać politykę zmiany haseł.

Przypisanie modyfikatora haseł do konta uprzywilejowanego

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Znajdź i kliknij wybrany obiekt.



3. W sekcji *Dane uwierzytelniające*, wprowadź login konta uprzywilejowanego.
4. Z listy rozwijalnej *Zastąp sekret*, wybierz `hasłem`.
5. Wprowadź hasło konta uprzywilejowanego.
6. Z lity rozwijalnej *Polityka modyfikatora hasła*, wybierz wcześniej zdefiniowaną politykę.



7. W sekcji *Modyfikator hasła*, wybierz `Unix Account over SSH`.
8. Uzupełnij dane logowania superużytkownika.

Informacja: Superuser account enables resetting the password in case the *Secret manager* detects that it has been changed by someone else.

9. Kliknij *Zapisz*.

Tematy pokrewne:

- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Wymagania*
- *Model danych*
- *Konfiguracja*

2.4 Dashboard

Widok startowy Wheel Fudo PAM umożliwia szybki dostęp do informacji o stanie urządzenia, a także pozwala na wykonanie procedury wyłączenia lub ponownego uruchomienia systemu.

Tematy pokrewne:

- *Pierwsze uruchomienie*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*

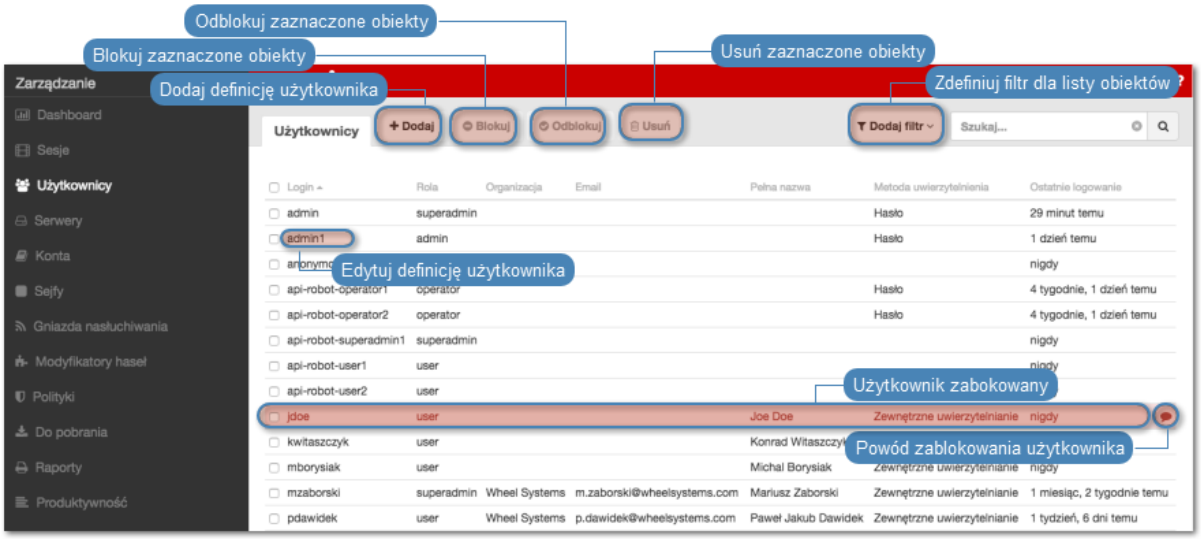
2.5 Użytkownicy

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (indywidualny login, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzilnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

Widok zarządzania użytkownikami

Widok *zarządzania użytkownikami* pozwala na dodanie nowych oraz edycję istniejących użytkowników, którym można nadać dostęp do zasobów infrastruktury.

Aby przejść do widoku *zarządzania użytkownikami* wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.



2.5.1 Dodawanie użytkownika

Aby dodać definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z relpikacją danych, skontaktuj się z działem wsparcia technicznego.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Kliknij *+ Dodaj*.

Informacja: Wheel Fudo PAM umożliwia tworzenie użytkowników na podstawie istniejących definicji. Otwórz formularz edycji istniejącego użytkownika i kliknij *Kopiuj użytkownika*, aby stworzyć nowy obiekt na podstawie wybranej definicji.

3. Uzupełnij parametry obiektu.

Parametr	Opis
Ogólne	
Login	Unikatowy login użytkownika. **Informacja:** Pole *login* nie rozróżnia wielkości liter.
Zablokowane	Zaznacz jeśli obiekt ma być niedostępny po utworzeniu.
Ważność konta	Ustal ważność konta.
Rola	Rola determinująca prawa dostępu użytkownika.
Preferowany język	Preferowany język panelu administracyjnego Wheel Fudo PAM.

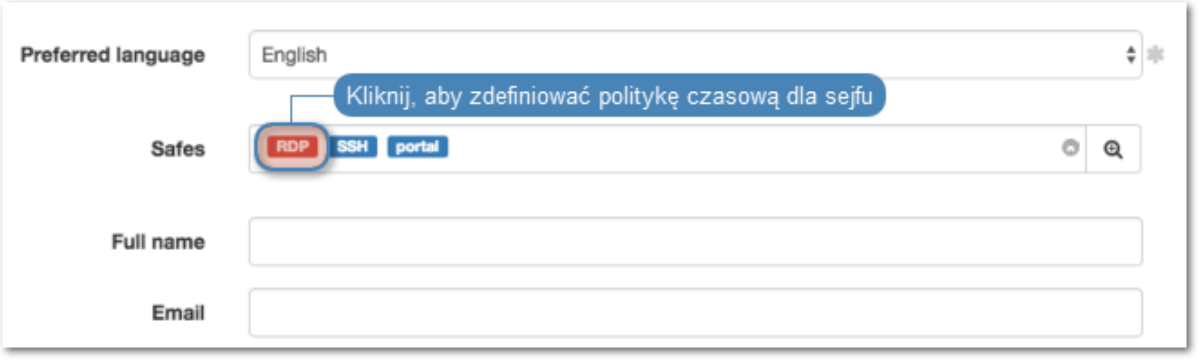
Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

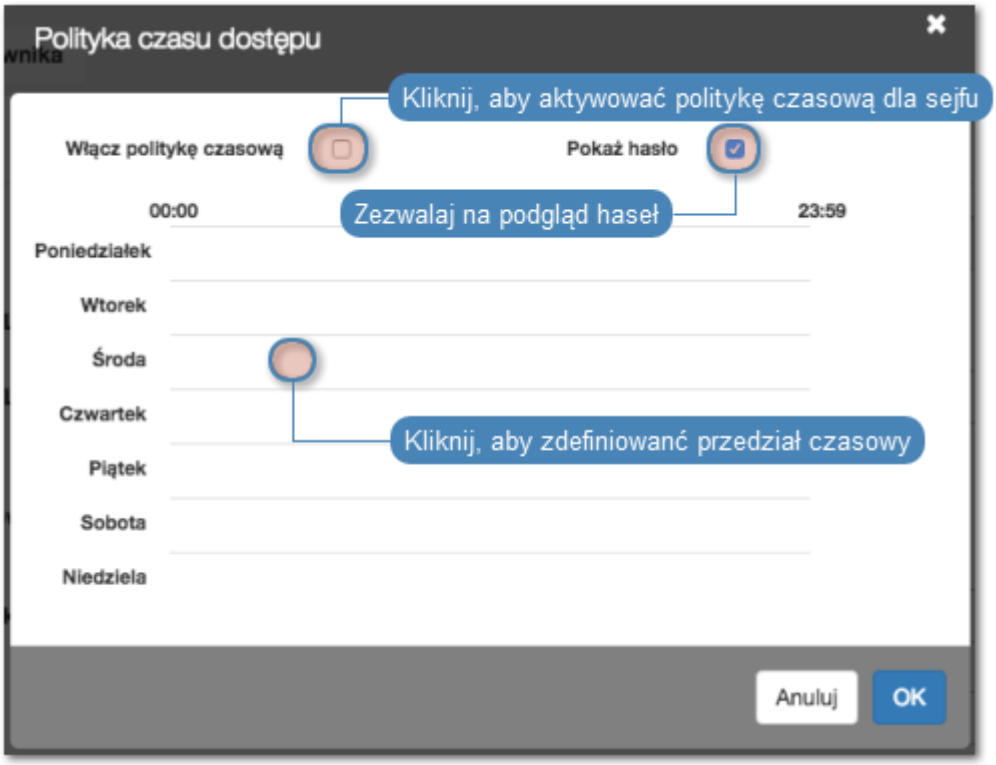
Parametr	Opis
Sejfy	Sejfy, do których dostęp będzie miał użytownik. **Informacja:** • SSH_sejf wskazuje, że opcja Pokaż hasło jest wyłączona. • RDP_sejf wskazuje, że opcja Pokaż hasło jest włączona.
Pełna nazwa	Nazwa użytkownika umożliwiająca jego jednoznaczną identyfikację.
Email	Adres email użytkownika.
Organizacja	Organizacja, do której przynależy użytkownik.
Telefon	Numer telefonu użytkownika.
Domena AD	Domena, do której należy konto użytkownika.
Baza LDAP	Parametr bazowy usługi katalogowej LDAP.
Uprawniania	
Uprawnieni użytkownicy	Użytkownicy uprawnieni do zarządzania obiektem.
Uwierzytelnienie	
Typ	Sposób uwierzytelnienia użytkownika.
	`Zewnętrzne źródło uwierzytelnienia`
Zewnętrzne źródło uwierzytelnienia	Zewnętrzne źródło uwierzytelnienia.
	`Hasło`
Hasło	Hasło statyczne użytkownika.
Powtórz hasło	Hasło statyczne użytkownika.
	`Klucz SSH`
Klucz publiczny	
	`Hasło jednorazowe`
Hasło jednorazowe	Hasło, które posłuży do jednokrotnego zalogowania.
API	
Adres IP	Adres IP, z którego będą wysyłane zapytania API.

4. Kliknij *+ Dodaj metodę uwierzytelnienia*, aby zdefiniować kolejną metodę uwierzytelniania.
5. Zdefiniuj politykę czasową dostępu do sejfu.

- Kliknij wybrany sejf.



- Zaznacz opcję *Włącz politykę czasową*, aby zastosować politykę czasową do sejfu.
- Zaznacz opcję *Pokaż hasło*, aby zezwolić użytkownikowi na podgląd haseł w portalu użytkownika.
- Kliknij kalendarz, aby zdefiniować przedziały czasowe, w których użytkownik będzie mógł się łączyć poprzez konta przypisane do wybranego sejfu.



- Kliknij *OK*.

6. Kliknij *Zapisz*.

Informacja: Wheel Fudo PAM pozwala synchronizować definicje użytkowników z serwerem usług katalogowych, tj. Active Directory, LDAP. Szczegółowa instrukcja konfiguracji synchronizacji bazy danych użytkowników znajduje się w rozdziale *Synchronizacja użytkowników*.

Modyfikowanie użytkownika

Aby zmodyfikować definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

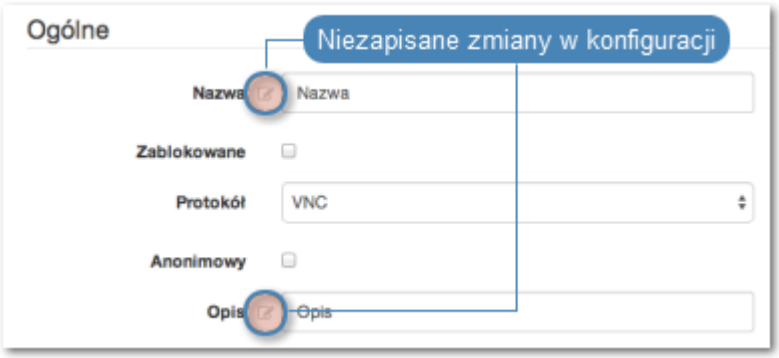
1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście definicję użytkownika, którą chcesz edytować.
3. Kliknij login użytkownika, aby przejść do formularza edycji danych wybranego użytkownika.

Informacja: Edycja danych użytkowników synchronizowanych z serwerem usług katalogowych wymaga wyłączenia opcji `Synchronizacja z LDAP` dla żądanych użytkowników.

---

4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną.



5. Kliknij *Zapisz*.

2.5.2 Blokowanie i odblokowanie użytkownika

Aby zablokować/odblokować użytkownikowi możliwość nawiązywania połączeń ze zdefiniowanymi zasobami, postępuj zgodnie z poniższą instrukcją.

Ostrzeżenie: Zablokowanie użytkownika spowoduje przerwanie aktualnie nawiązanych przez niego połączeń.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i zaznacz użytkownika, którego chcesz zablokować/odblokować.
3. Kliknij *Blokuj*, aby zablokować użytkownikowi możliwość nawiązywania połączeń z zasobami serwerowymi lub *Odblokuj*, aby przywrócić możliwość nawiązywania połączeń.

2.5.3 Usuwanie użytkownika

Aby usunąć definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

Ostrzeżenie: Usunięcie użytkownika spowoduje przerwanie aktualnie nawiązanych przez niego połączeń.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i zaznacz użytkownika, którego chcesz usunąć.
3. Kliknij *Usuń*.
4. Potwierdź operację usunięcia zaznaczonych użytkowników.

Informacja: Usunięcie definicji użytkownika nie skutkuje usunięciem skojarzonych, zarejestrowanych sesji. Sesje usuniętych użytkowników charakteryzują się przekreślonym loginem użytkownika.

2.5.4 Role

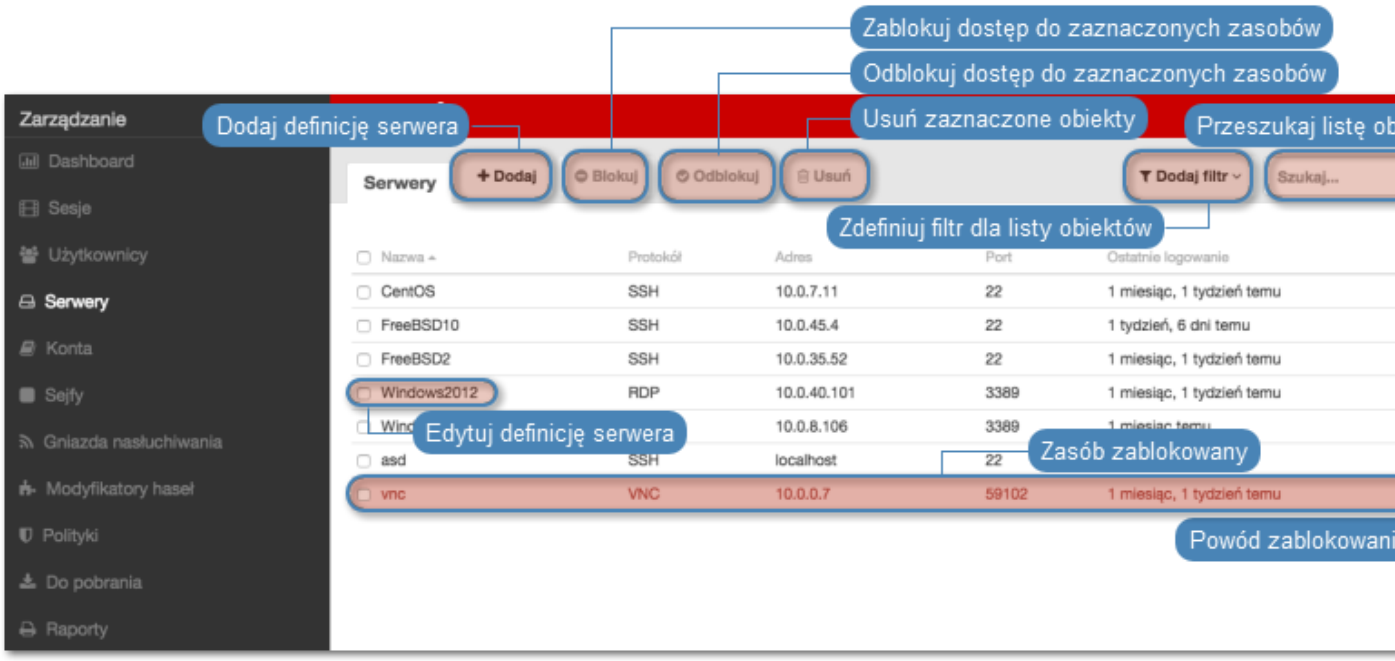
Rola	Prawa dostępu
user	• łączenie z serwerami w ramach zdefiniowanych sejfów, do których użytkownik został przypisany • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
operator	• logowanie do panelu administracyjnego • przeglądanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • odtwarzanie sesji, w której pośredniczyły obiekty, do których użytkownik posiada uprawnienia • blokowanie/odblokowywanie wybranych obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • generowanie i subskrybowanie raportów • włączanie/wyłączanie powiadomień email • konwersja sesji i pobieranie skonwertowanego materiału • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
admin	• logowanie do panelu administracyjnego • zarządzanie obiektami: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, do których użytkownik posiada uprawnienia • blokowanie/odblokowywanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania • generowanie i subskrybowanie raportów • konwersja sesji i pobieranie skonwertowanego materiału • włączanie/wyłączanie powiadomień email • zarządzanie politykami • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • odtwarzanie sesji, w której pośredniczyły obiekty, do których użytkownik posiada uprawnienia • zarządzanie modyfikatorami haseł • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).
superadmin	• zarządzanie obiektami bez ograniczeń • zarządzanie konfiguracją urządzenia bez ograniczeń • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`) • pobieranie haseł do serwerów (wymaga stosownego uprawnienia).

Tematy pokrewne:

- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Konta*

2.6 Serwery

Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.



Dodawanie definicji serwera

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z relpikacją danych, skontaktuj się z działem wsparcia technicznego.

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.

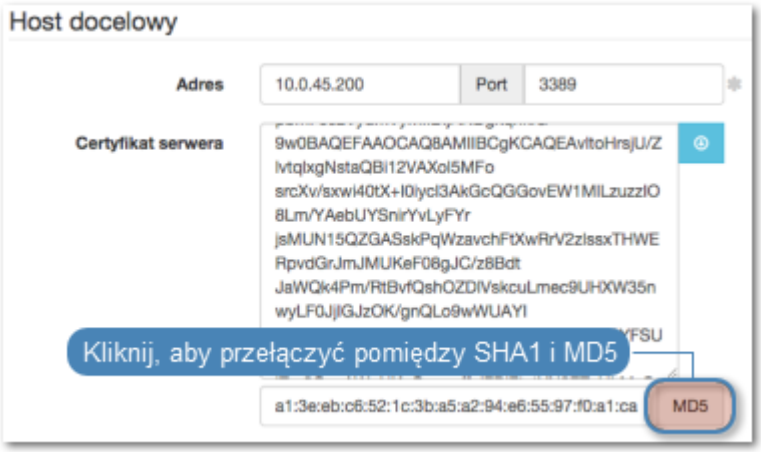
2. Kliknij *+ Dodaj*.
3. Zdefiniuj parametry serwera.

Parametr	Opis
Ogólne	
Nazwa	Nazwa obiektu.
Zablokowane	Zaznacz jeśli obiekt ma być niedostępny po utworzeniu.
Protokół	Protokół komunikacji z serwerem.
Czas oczekiwania HTTP (*dotyczy protokołu HTTP*)	Czas bezczynności, po którym połączenie będzie wymagało ponownego uwierzytelnienia.
Bezpieczeństwo (*dotyczy protokołu RDP*)	Tryb bezpieczeństwa połączeń RDP. `Enhanced RDP Security (TLS) + NLA` pozwala na ukrycie ekranu logowania Wheel Fudo PAM przy zestawianiu połączenia z serwerem.
Opis	Opis ułatwiający identyfikację zasobu.

Uprawnienia	
Uprawnieni użytkownicy	Użytkownicy uprawnieni do zarządzania definicją obiektu. Lista zawiera użytkowników o zdefiniowanej roli `admin` lub `operator`. Więcej informacji na temat uprawnień użytkowników, znajdziesz w rozdziale *Bezpieczeństwo*.

Host docelowy	
Adres	Adres serwera docelowego wraz z numerem portu, na którym skonfigurowana jest usługa łączenia za pośrednictwem wybranego protokołu.
Certyfikat serwera (*dotyczy protokołów RDP i HTTPS*)	Umożliwia pobranie certyfikatu SSL serwera celem zweryfikowania jego poprawności.
Klucz publiczny serwera (*dotyczy protokołu SSH*)	Pole umożliwia pobranie certyfikatu SSL serwera celem zweryfikowania jego poprawności.
Host HTTP (*dotyczy protokołu HTTP*)	Umożliwia wskazanie zasobu na serwerze, który ma podlegać monitorowaniu.

Informacja: Kliknij specyfikator funkcji skrótu, aby przełączyć pomiędzy wyświetlaniem skrótu klucza wygenerowanego przez algorytm SHA1 lub MD5.



4. Kliknij *Zapisz*.

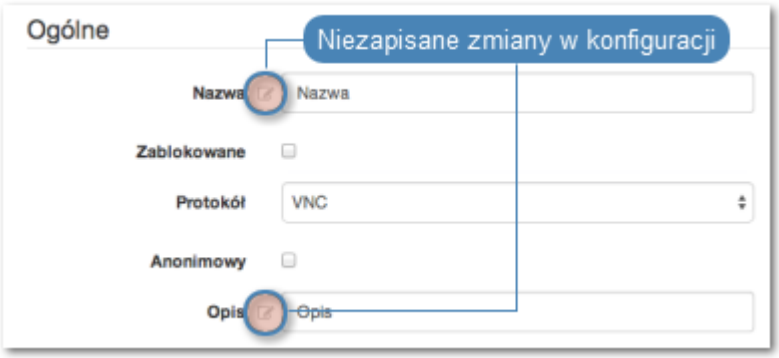
Modyfikowanie serwera

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście definicję serwera, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij nazwę serwera.
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną.



5. Kliknij *Zapisz*.

Blokowanie i odblokowanie serwera

Wheel Fudo PAM pozwala na zablokowanie wszystkim użytkownikom możliwości nawiązywania połączeń z wybranym serwerem.

Ostrzeżenie: Zablokowanie serwera spowoduje zerwanie aktualnie trwających sesji połączeniowych z danym zasobem.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i zaznacz serwer, który chcesz zablokować/odblokować.
3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z danym zasobem lub *Odblokuj*, aby przywrócić możliwość nawiązywania połączeń.
4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.

Usuwanie serwera

Ostrzeżenie: Usunięcie serwera spowoduje przerwanie aktualnie trwających sesji połączeniowych z danym zasobem.

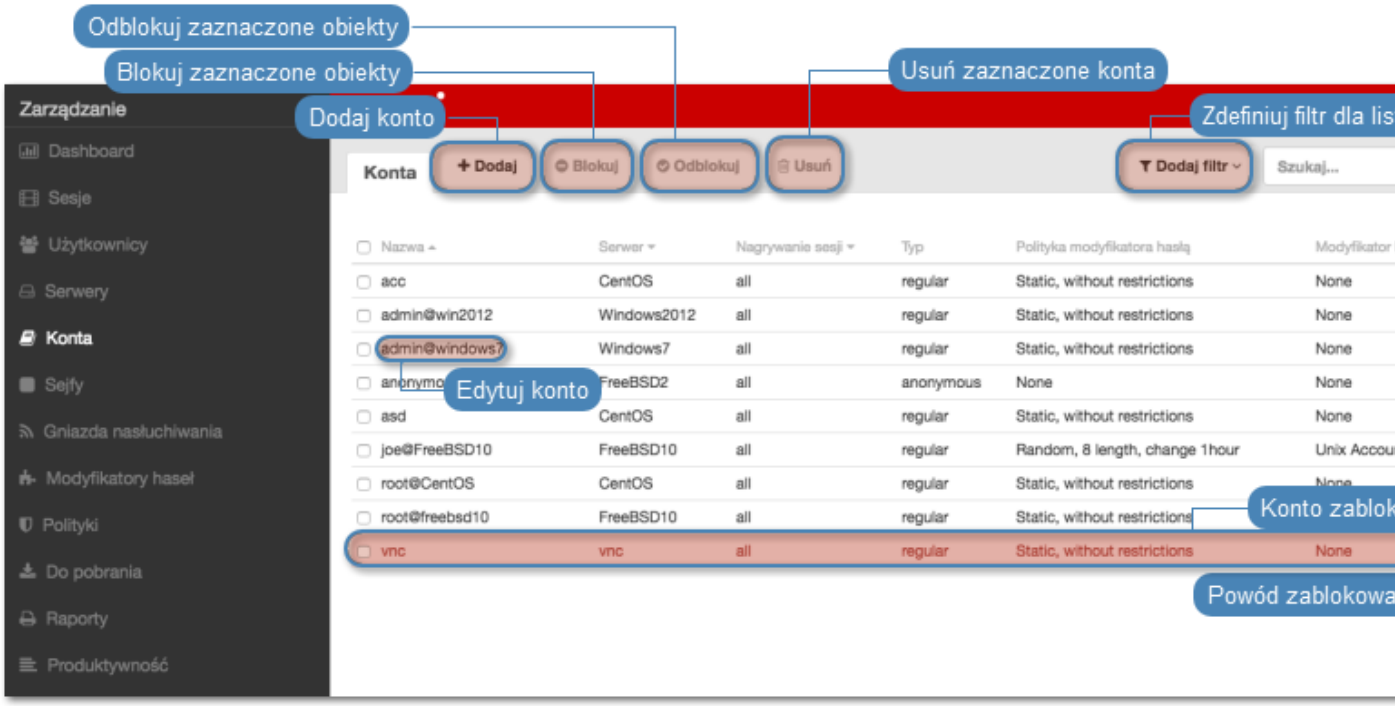
1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i zaznacz serwery, które chcesz usunąć.
3. Kliknij *Usuń*.
4. Potwierdź operację usunięcia zaznaczonych obiektów.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*

2.7 Konta

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.



Dodawanie konta

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z relpikacją danych, skontaktuj się z działem wsparcia technicznego.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Kliknij *+ Dodaj*.
3. Zdefiniuj parametry konta.

Parametr	Opis
Ogólne	
Nazwa	Nazwa obiektu.
Zablokowane	Zaznacz jeśli obiekt ma być niedostępny po utworzeniu.

Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

Parametr	Opis
Typ	Typ konta. • `anonymous` - zestawiając połączenie z serwerem anonimowym, Wheel Fudo PAM nie sprawdza istnienia definicji użytkownika w lokalnej bazie danych, tylko przekazuje dane logowania do serwera docelowego i po uwierzytelnieniu użytkownika, rejestruje przebieg sesji. **Informacja:** Dodanie konta anonimowego do sejfu czyni go anonimowym i wszystkie konta przypisane do tego sejfu muszą być typu `anonymous`. • `forward` - dane logowanie przekazywane są do serwera docelowego. • `regular` - login i hasło użytkownika zamieniane są na zdefiniowane dane logowania konta uprzywilejowanego.
Nagrywanie sesji	Wybierz tryb rejestrowania sesji. • `wszystko`, Wheel Fudo PAM rejestruje ruch sieciowy, umożliwiając późniejsze odtworzenie materiału w odtwarzaczu sesji oraz konwersję do wybranego formatu wideo. • `raw`, Wheel Fudo PAM rejestruje ruch sieciowy, umożliwiając późniejsze pobranie surowych danych, bez możliwości odtworzenia materiału w odtwarzaczu sesji. • `brak`, Wheel Fudo PAM jedynie odnotowuje fakt, że połączenie miało miejsce, jednak nie rejestruje wymiany danych pomiędzy użytkownikiem i serwerem.
OCR sesji	Opcja pełnego indeksowania materiału sesji RDP i VNC.
Język OCR	Języki przetwarzanych treści.
Usuń dane po upływie	Liczba dni, po której materiał sesji zostanie automatycznie usunięty przez mechanizm retencji danych.
Uprawnienia	
Uprawnieni użytkownicy	Użytkownicy uprawnieni do zarządzania obiektem.
Serwer	
Serwer	Serwer korzystający z definicji konta.
Dane uwierzytelniające	

Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

Parametr	Opis
Domena	Domena przypisana do definiowanego konta. **Informacja:** W przypadku połączeń z serwerami MS SQL, uzupełnienie pola *domena* spowoduje, że Wheel Fudo PAM będzie korzystało z mechanizmu NTLM negocjując połączenie z serwerem docelowym. W innym przypadku, Wheel Fudo PAM skorzysta z mechanizmu *SQL Server Authentication*. Mechanizm *SQL Server Authentication* jest używany do uwierzytelnienia użytkowników przed Wheel Fudo PAM, niezależnie od tego, czy pole *domena* jest wypełnione czy nie.
Login	Login konta uprzywilejowanego.
Zastąp sekret	Zastąp sekret podany przez użytkownika.
	`hasłem`
Hasło	
Powtórz hasło	
	`kluczem`
Klucz publiczny	
	`hasłem z zewnętrznego repozytorium`
Zewnętrzne repozytorium haseł	Zewnętrzne repozytorium haseł zarządzające danymi logowania do wybranego konta.
Polityka modyfikatora haseł	Polityka zmiany haseł, determinująca częstotliwość zmian oraz złożoność automatycznie generowanch sekretów.
Modyfikator hasła	
Modyfikator hasła	Wybierz modyfikator odpowiedzialny za zmianę haseł na definiowanym koncie.
`Konto Unix poprzez SSH`	
Użytkownik uprzywilejnowany	Login użytkownika uprawnionego do zmiany hasła do konta zdefiniowanego w obiekcie.
Hasło użytkownika uprzywilejowanego	Hasło dostępu konta uprzywilejowanego.
`Konto Windows poprzez WMI`	
Użytkownik uprzywilejnowany	Login użytkownika uprawnionego do zmiany hasła do konta zdefiniowanego w obiekcie.
Hasło użytkownika uprzywilejowanego	Hasło dostępu konta uprzywilejowanego.
`Konto Uzytkownika MySQL na serwerze Unix poprzez SSH`	
Użytkownik SSH	Login użytkownika uprawnionego do nawiązywania połączeń SSH z maszyną docelową.
Hasło SSH	Hasło użytkownika.

Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

Parametr	Opis
Adres serwera SSH	Adres IP serwera SSH.
Port serwera SSH	Numer portu serwera SSH.
Użytkownik uprzywilejnowany	Login użytkownika uprawnionego do zmiany hasła do konta zdefiniowanego w obiekcie.
Hasło użytkownika uprzywilejowanego	Hasło dostępu konta uprzywilejowanego.
`Konto Cisco poprzez Telnet`	
Hasło trybu uprzywilejowanego	Hasło aktywujące tryb uprzywilejowany.
Użytkownik uprzywilejnowany	Login użytkownika uprawnionego do zmiany hasła do konta zdefiniowanego w obiekcie.
Hasło użytkownika uprzywilejowanego	
`Cisco Enable Password poprzez Telnet`	
Hasło trybu uprzywilejowanego	Hasło aktywujące tryb uprzywilejowany.
Użytkownik uprzywilejnowany	Login użytkownika uprawnionego do zmiany hasła do konta zdefiniowanego w obiekcie.
Hasło użytkownika uprzywilejowanego	Hasło dostępu konta uprzywilejowanego.
`Konto Cisco poprzez SSH`	
Hasło trybu uprzywilejowanego	Hasło aktywujące tryb uprzywilejowany.
Użytkownik uprzywilejnowany	Login użytkownika uprawnionego do zmiany hasła do konta zdefiniowanego w obiekcie.
Hasło użytkownika uprzywilejowanego	Hasło dostępu konta uprzywilejowanego.
`Cisco Enable Password poprzez SSH`	
Hasło trybu uprzywilejowanego	Hasło aktywujące tryb uprzywilejowany.
Użytkownik uprzywilejnowany	Login użytkownika uprawnionego do zmiany hasła do konta zdefiniowanego w obiekcie.
Hasło użytkownika uprzywilejowanego	Hasło dostępu konta uprzywilejowanego.
`LDAP`	

Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

Parametr	Opis
Użytkownik uprzywilejnowany	Login użytkownika uprawnionego do zmiany hasła do zdefiniowanego konta. **Informacja:** • Użytkownik musi mieć wskazaną domeną, np. `nazwa_domeny\administrator`. • Dopuszcza się użycie pełnej nazwy FQDN jako domeny np. `nazwa_domeny.corp`. • Dopuszcza się podanie nazwy użytkownika uprzywilejowanego w formie `administrator@nazwa_domeny`.
Hasło użytkownika uprzywilejowanego	Hasło dostępu konta uprzywilejowanego.
Baza LDAP	Ścieżka, w której należy szukać użytkownika dla którego zmieniane jest hasło.
Certyfikat CA serwera LDAP	Klucz publiczny CA, którym podpisany jest certyfikat serwera LDAP. **Informacja:** • Nazwa serwera (adres IP), z którym skojarzone jest konto, musi być podana dokładnie w takiej postaci w jakiej pojawia się w certyfikacie TLS, którym posługuje się serwer. Jeżeli nazwa serwera w certyfikacie to: `ad.example.com`, to adres serwera skonfigorowany na Fudo musi być podany jako `ad.example.com`. • Serwer Active Directory musi posiadać aktywną usługę LDAPS.

Informacja: *Podwójne uwierzytelnienie*

Funkcjonalność podwójnego uwierzytelnienia polega na dwukrotnym żądaniu wprowadzenia danych logowania podczas nawiązywania połączenia. Pierwsze zapytanie dotyczy uwierzytelnienia użytkownika przed Wheel Fudo PAM, drugie służy uwierzytelnieniu przed systemem docelowym.

Aby aktywować funkcję podwójnego uwierzytelnienia, postępuj zgodnie z poniższą instrukcją.

- Z listy rozwijalnej *Typ*, wybierz `forward`.
- W sekcji *Dane uwierzytelniające* zaznacz opcję *Podwójne uwierzytelnienie*.

4. Kliknij *Zapisz*.

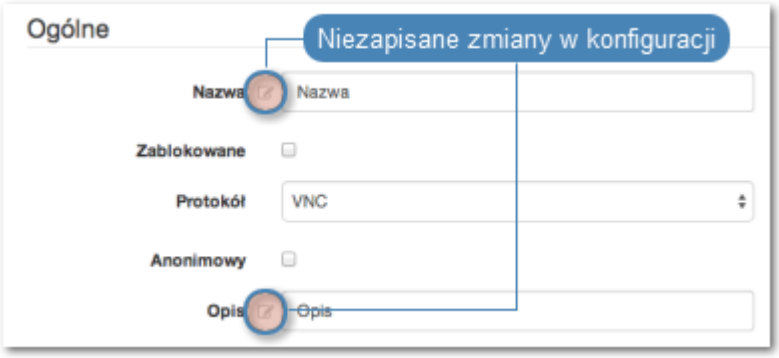
Modyfikowanie konta

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście definicję konta, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij nazwę konta.
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną.



5. Kliknij *Zapisz*.

Blokowanie i odblokowanie konta

Ostrzeżenie: Zablokowanie konta spowoduje zerwanie aktualnie trwających sesji połączeniowych z powiązanym serwerem.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować/odblokować.
3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z serwerem za pośrednictwem z wybranego konta.
4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.

Usuwanie konta

Ostrzeżenie: Usunięcie konta spowoduje zerwanie aktualnie trwających sesji połączeniowych z powiązanym serwerem.

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz konta, które chcesz usunąć.
3. Kliknij *Usuń*.
4. Potwierdź operację usunięcia zaznaczonych obiektów.

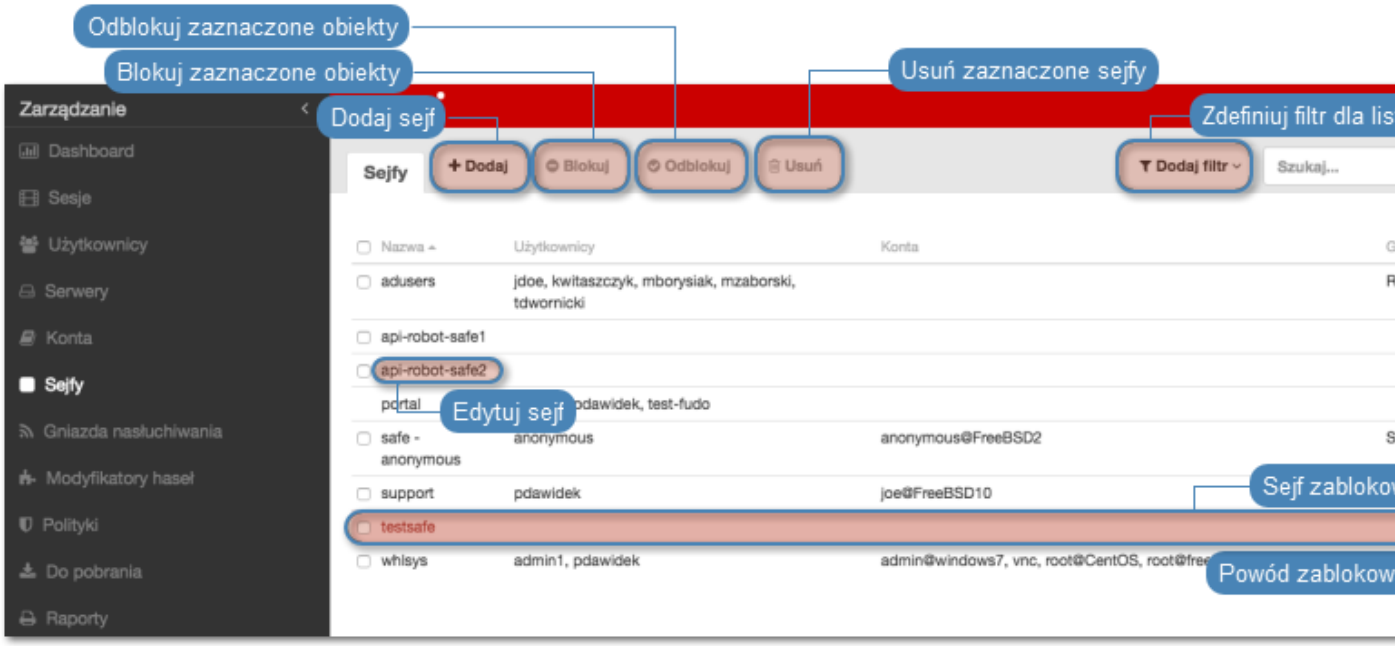
Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*

- *Serwery*
- *Gniazda nasłuchiwania*
- *Sejfy*

2.8 Sejfy

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.



Dodawanie sejfu

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z relpikacją danych, skontaktuj się z działem wsparcia technicznego.

Informacja:

- Sejf `system` może posiadać tylko konto `system`.
- Sejf `portal` może posiadać tylko konto `portal`.
- Użytkownik o roli `operator`, `admin` lub `superadmin` zawsze posiada dostęp do sejfu `system`.
- Użytkownik o roli `user` nie może posiadać dostępu do sejfu `system`.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.

3. Zdefiniuj parametry sejfu.

Parametr	Opis
Ogólne	
Nazwa	Nazwa obiektu.
Zablokowane	Zaznacz jeśli obiekt ma być niedostępny po utworzeniu.
Powód logowania	Wymusza na użytkownikach podanie powodu logowania przy nawiązywaniu połączenia z monitorowanym zasobem.
Powiadomienia	Zaznacz zdarzenia, o których będzie powiadamiany administrator Wheel Fudo PAM.
Polityki	Przypisz polityki proaktywnego monitoringu.
Funkcjonalność protokołów	
	Funkcjonalność RDP
Przekierowanie schowka	Funkcjonalność przenoszenia tekstu pomiędzy komputerem lokalnym a zdalnym systemem za pomocą schowka.
Przekierowanie dźwięku	Pozwala na odtwarzanie dźwięków zdalnego systemu na maszynie lokalnej, z której łączy się użytkownik.
Przekierowanie urządzeń	Pozwala na użycie urządzeń podłączonych do lokalnej maszyny (tj. drukarka, napęd CD, urządzenia Plug and Play, itp.) a także dostęp do mapowanych dysków sieciowych w zdalnej sesji RDP.
Dynamiczne wirtualne kanały	Rozszerzenia pozwalające na implementację dodatkowych funkcjonalności w połączeniach RDP.
Przekierowanie wejścia audio	Przekierowanie wejścia audio lokalnej maszyny na zdalny system.
Przekierowanie multimediów	Pozwala na przetwarzanie strumienia multimediów po stronie maszyny lokalnej, ograniczając obciążenie zdalnego serwera oraz ilość przesyłanych danych sesji.
Maksymalna rozdzielczość sesji RDP	Umożliwia ograniczenie rozdzielczości połączeń RDP.
	Funkcjonalność SSH
Sesje	Nawiązywanie połączeń SSH.
Przekierowanie portu	Lokalne i zdalne tunelowanie połączeń SSH.
Terminal	Nawiązywanie połączeń SSH za pośrednictwem terminala.
Środowisko	Dostęp do środowiska zdalnego systemu.
X11	Uruchamianie programów graficznych na zdalnym systemie.
SSH Agent forwarding	Przekazywanie klucza przez agenta SSH w łańcuchu kolejnych połączeń SSH.
Powłoka	Możliwość wykonywania komend powłoki.
SCP	Bezpieczne kopiowanie zasobów dyskowych z wykorzystaniem protokołu SSH.
	Funkcjonalność VNC
Schowek klienta	Obsługa schowka po stronie klienta.
Schowek serwera	Obsługa schowka po stronie serwera.
Uprawnienia	
Uprawnieni użytkownicy	Użytkownicy uprawnieni do zarządzania obiektem.
Powiązania obiektu	
Użytkownicy	Użytkownicy uprawnieni do nawiązywania połączeń za pośrednictwem kont uprzywilejowanych przypisanych do sejfu.

Kontynuacja na następnej stronie

Tabela 3 – kontynuacja poprzedniej strony

Parametr	Opis
Konta	Konta uprzywilejowane na monitorowanych serwerach.
Gniazda nasłuchiwania	Gniazda nasłuchiwania determinujące sposób nawiązywania połączenia z maszynami docelowymi.

4. Kliknij *Zapisz*.

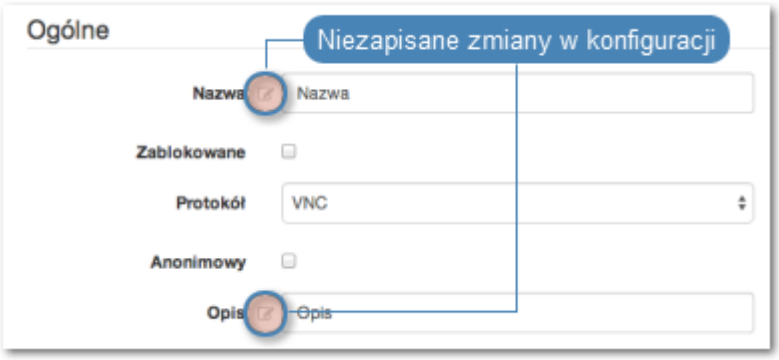
Modyfikowanie sejfu

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście definicję sejfu, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij nazwę sejfu.
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną.



5. Kliknij *Zapisz*.

Blokowanie i odblokowanie sejfu

Wheel Fudo PAM pozwala na zablokowanie wszystkim użytkownikom możliwości nawiązywania połączeń z serwerami przypisanymi do sejfu.

Ostrzeżenie: Zablokowanie sejfu spowoduje zerwanie aktualnie trwających sesji połączeniowych z serwerami przypisanymi do danego sejfu.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować/odblokować.
3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z serwerami z wykorzystaniem kont uprzywilejowanych przypisanych do wybranego sejfu.
4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.

Usuwanie sejfu

Ostrzeżenie: Usunięcie sejfu spowoduje przerwanie aktualnie trwających sesji z serwerami, do połączenia z którymi zostały wykorzystane konta przypisane do sejfu.

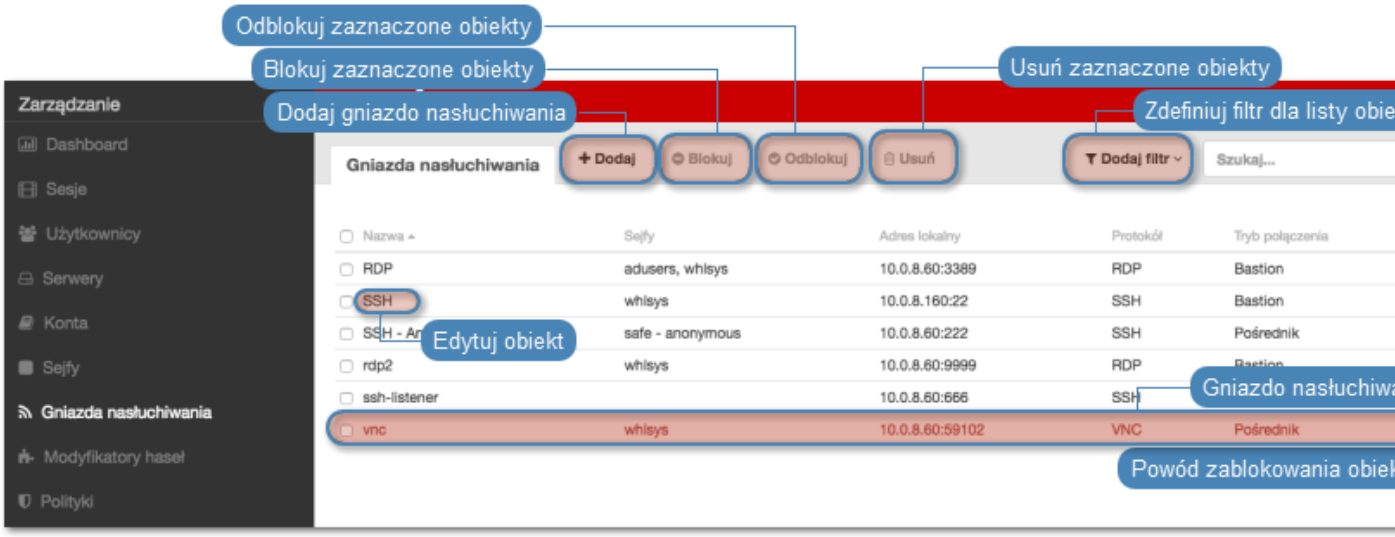
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście i zaznacz sejfy, które chcesz usunąć.
3. Kliknij *Usuń*.
4. Potwierdź operację usunięcia zaznaczonych obiektów.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*

2.9 Gniazda nasłuchiwania

Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.



Dodawanie definicji gniazda nasłuchiwania

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z relpikacją danych, skontaktuj się z działem wsparcia technicznego.

Informacja:

- Gniazdo nasłuchiwania typu *pośrednik* może zawierać co najwyżej jedno konto do serwera o tym samym protokole, co protokół gniazda nasłuchiwania za pośrednictwem sejfów.

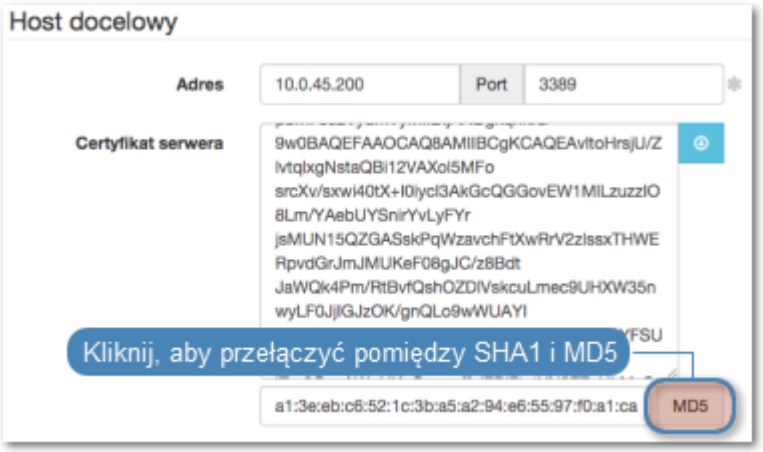
- Gniazdo nasłuchiwania typu *bastion* nie może zawierać konta anonimowego do serwera o tym samym protokole, co protokół gniazda nasłuchiwania.
- Gniazdo nasłuchiwania nie może zawierać konta anonimowego i *regular* lub *forward* do tego samego serwera o tym samym protokole, co protokół gniazda nasłuchiwania.
- Gniazdo nasłuchiwania nie może posiadać dwóch kont *regular* lub *forward* do tego samego serwera o tym samym protokole, co protokół gniazda nasłuchiwania, do których jeden użytkownik ma dostęp.
- Dla danego gniazda nasłuchiwania RDP i serwera RDP, do którego gniazdo nasłuchiwania ma dostęp, gniazdo nasłuchiwania i serwer korzystają ze Standard RDP Security lub gniazdo nasłuchiwania i serwer korzystają z TLS lub NLA.

---

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Kliknij *+ Dodaj*.
3. Zdefiniuj parametry gniazda nasłuchiwania.

Parametr	Opis
Ogólne	
Nazwa	Nazwa obiektu.
Zablokowane	Zaznacz jeśli obiekt ma być niedostępny po utworzeniu.
Protokół	Protokół komunikacji z serwerem.
Bezpieczeństwo (*dotyczy protokołu RDP*)	Tryb bezpieczeństwa połączeń RDP. `Enhanced RDP Security (TLS) + NLA` pozwala na ukrycie ekranu logowania Wheel Fudo PAM przy zestawianiu połączenia z serwerem.
Komunikat (*dotyczy protokołu RDP/VNC*)	Lokalny komunikat serwera wyświetlany na ekranie logowania.
Uprawnienia	
Uprawnieni użytkownicy	Użytkownicy uprawnieni do zarządzania obiektem.
Połączenie	
Tryb połączenia	Tryb determinujący sposób nawiązywania połczenia z serwerem. • `Przezroczysty` - użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Wheel Fudo PAM w *trybie mostu*. • `Pośrednik` - użytkownik nawiązuje połączenie z serwerem podając adres IP Wheel Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę. • `Brama` - użytkownik łączy się z serwerem docelowym podając jego adres IP. Wheel Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Wheel Fudo PAM w *trybie bramy*. • `Bastion` - użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
Adres lokalny (*dotyczy trybu* `pośrednik`)	Adres IP, na który użytkownicy będą łączyć się z Wheel Fudo PAM w celu uzyskania połączenia ze zdalnym serwerem. Więcej na temat przydzielania adresów IP można przeczytać w rozdziale *Ustawienia sieciowe*. Numer portu pozwala na jednoznaczną identyfikację serwera docelowego.
Interfejs (*dotyczy trybu transparentnego i bramy*)	Interfejs sieciowy wykorzystywany w komunikacji z serwerem.
Użyj HTTPS (*dotyczy protokołu HTTP*)	Zaznacz, aby połączenie z Wheel Fudo PAM było szyfrowane protokołem SSL.
Certyfikat HTTPS (*dotyczy protokołu HTTPS*)	Certyfikat Wheel Fudo PAM wymagany do zestawienia połączenia szyfrowanego HTTPS.
Klucz prywatny (*dotyczy protokołu HTTPS*)	Klucz prywatny Wheel Fudo PAM wymagany do zestawienia połączenia szyfrowanego HTTPS.
Certyfikat TLS (*dotyczy protokołu RDP z Enhanced RDP security*)	Certyfikat TLS dla połączeń wykorzystujących mechanizm `Enhanced RDP security`.
Klucz publiczny serwera (*dotyczy protokołu RDP*)	Klucz publiczny Wheel Fudo PAM dla bezpiecznych połączeń RDP.

Informacja: Kliknij specyfikator funkcji skrótu, aby przełączyć pomiędzy wyświetlaniem skrótu klucza wygenerowanego przez algorytm SHA1 lub MD5.



4. Kliknij *Zapisz*.

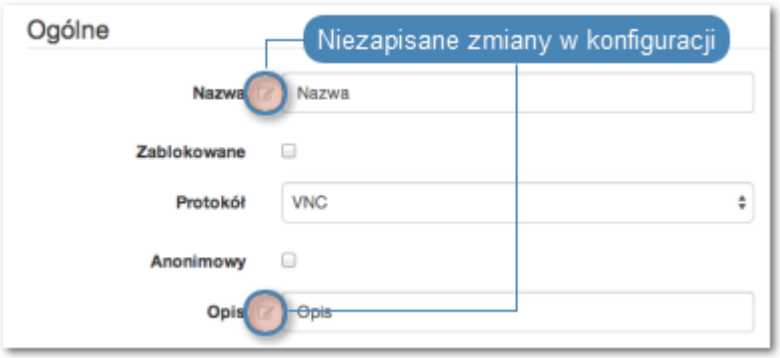
Modyfikowanie gniazda nasłuchiwania

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście definicję gniazda nasłuchiwania, którą chcesz edytować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij nazwę gniazda nasłuchiwania.
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja: Zmiany w konfiguracji, które nie zostały zapisane, oznaczone są ikoną.



5. Kliknij *Zapisz*.

Blokowanie i odblokowanie gniazda nasłuchiwania

Ostrzeżenie: Zablokowanie gniazda spowoduje zerwanie aktualnie trwających sesji z serwerami, w połączeniach z którymi pośredniczy wybrane gniazdo nasłuchiwania.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować/odblokować.
3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z serwerami, z którymi połączenia realizowane są za pośrednictwem danego gniazda nasłuchiwania.
4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.

Usuwanie gniazda nasłuchiwania

Ostrzeżenie: Zablokowanie gniazda spowoduje zerwanie aktualnie trwających sesji z serwerami, w połączeniach z którymi pośredniczy wybrane gniazdo nasłuchiwania.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście i zaznacz gniazdo nasłuchiwania, które chcesz usunąć.
3. Kliknij *Usuń*.
4. Potwierdź operację usunięcia zaznaczonych obiektów.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

2.10 Modyfikatory haseł

Wheel Fudo PAM umożliwia zarządzanie hasłami dostępu do kont uprzywilejowanych zdefiniowanych na monitorowanych systemach. Funkcjonalność modyfikatorów haseł wspiera następujące scenariusze:

- Unix poprzez SSH
- MySQL poprzez SSH
- Cisco poprzez SSH and Telnet
- Cisco Enable Password poprzez SSH i Telnet
- MS Windows poprzez WMI

2.10.1 Polityka haseł

Polityka zmiany haseł określa częstotliwość zmiany hasła oraz jego złożoność.

Dodawanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Kliknij *+ Dodaj*.

3. Zdefiniuj parametry konfiguracyjne.

Parametr	Opis
Ogólne	
Nazwa	Nazwa obiektu.
Zmiana hasła włączona	Włącz funkcję automatycznej zmiany hasła i określ interwał pomiędzy wykonaniem skryptów modyfikatorów.
Weryfikacja hasła włączona	Włącz funkcję sprawdzania hasła i określ interwał pomiędzy wykonaniem skryptów weryfikujących.

Specyfikacja hasła	
Długość	Liczba znaków hasła.
Małe litery	Określ, czy hasło ma zawierać małe litery i ich minimalną liczbę.
Duże litery	Określ, czy hasło ma zawierać wielkie litery i ich minimalną liczbę.
Znaki specjalne	Określ, czy hasło ma zawierać znaki specjalne i ich minimalną liczbę.
Cyfry	Określ, czy hasło ma zawierać cyfry i ich minimalną liczbę.

Informacja: Suma wszystkich znaków wszystkich wybranych opcji nie może być większa niż określona całkowita liczba znaków w haśle.

4. Kliknij *Zapisz*.

Edytowanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Odszukaj i kliknij wybraną politykę.
3. Zmodyfikuj parametry konfiguracyjne.
4. Kliknij *Zapisz*.

Usuwanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Zaznacz wybrane polityki zmiany haseł.
3. Kliknij *Usuń*.
4. Potwierdź usunięcie obiektów.

2.10.2 Uniwersalne modyfikatory haseł

Uniwersalne modyfikatory haseł umożliwiają zdefiniowanie sekwencji komend, które zostaną wykonane na zdalnej maszynie w celu zmiany hasła.

Dodawanie uniwersalnego modyfikatora haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.

3. Kliknij *+ Dodaj*.
4. Zdefiniuj nazwę modyfikatora haseł.
5. Kliknij *+*, aby dodać komendę.
6. Wprowadź komendę.

Informacja: W komendach można stosować zmienne wymienione w sekcji *Lista zmiennych*. Ciąg znaków definiujący zmienną, zawarty pomiędzy znakami `%%`, zostanie zamieniony w każdej komendzie (np. `%%host%%`).

---

7. Dodaj opcjonalny opis.
8. Powtarzaj kroki 5-7, aby dodać kolejne komendy.
9. Powtarzaj kroki 5-8, aby zdefiniować weryfikator hasła w sekcji *Lista komend weryfikatora haseł*.
10. Kliknij *Zapisz*.

Informacja: Przeciągnij i upuść komendy aby zmieniać kolejność ich wykonania.

Edytowanie uniwersalnego modyfikatora haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.
3. Znajdź i kliknij wybrany modyfikator.
4. Zmień wybrane komendy.
5. Kliknij *X*, aby usunąć komendę.
6. Kliknij *Zapisz*.

Usuwanie modyfikatora haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.
3. Zaznacz wybrane obiekty i kliknij *Usuń*.
4. Potwierdź usunięcie wybranych obiektów.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*

2.11 Polityki

Polityki to grupy definicji wzorców pozwalające na proaktywny monitoring przebiegu sesji. W przypadku wykrycia wzorca, Wheel Fudo PAM pozwala na automatyczne wstrzymanie sesji, zakończenie połączenia, zablokowanie użytkownika i wysłanie stosownego powiadomienia do administratora.

Definiowanie wzorców

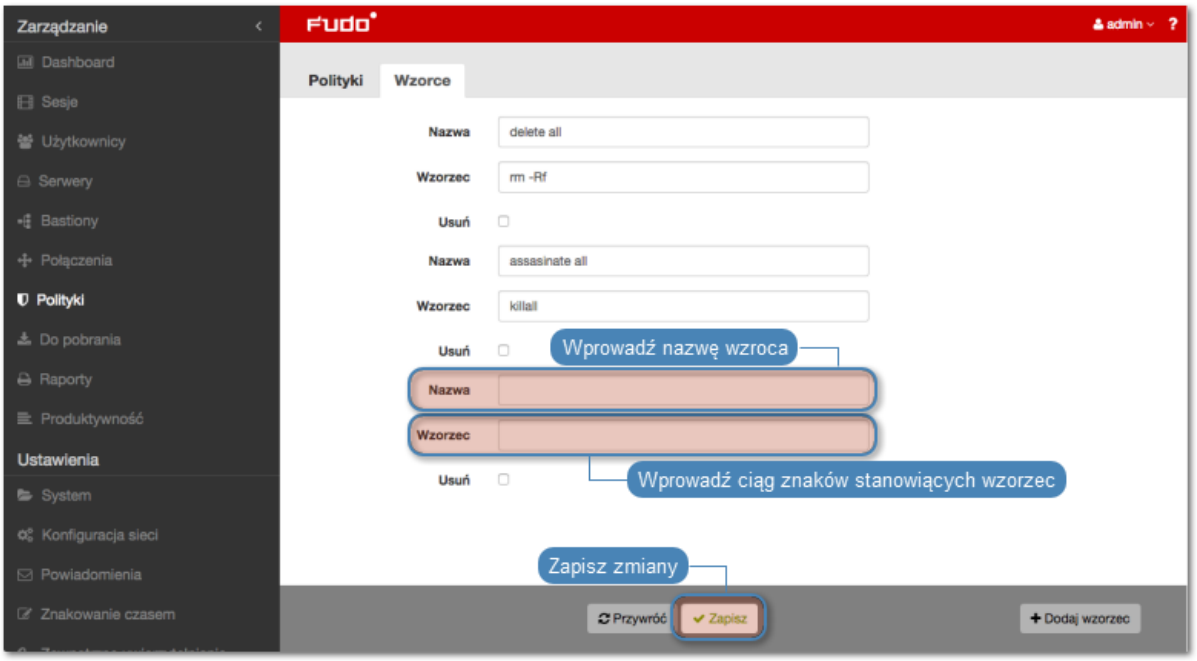
1. Wybierz z lewego menu *Zarządzanie* > *Polityki*.
2. Wybierz zakładkę *Wzorce*.
3. Kliknij + *Dodaj wzorzec*.

4. Zdefiniuj nazwę i ciąg znaków stanowiący wzorzec.

Informacja: Wheel Fudo PAM nie rozpoznaje wzorców zdefiniowanych z użyciem znaku \ (backslash); np. `\d`, `\D`, `\w`, `\W`.

---

5. Powtarzaj kroki 3-5, aby zdefiniować kolejne wzorce.
6. Kliknij *Zapisz*.



Informacja: Przykłady wyrażeń regularnych

Komenda `rm`

```
(^|[^a-zA-Z])rm[[:space:]]
```

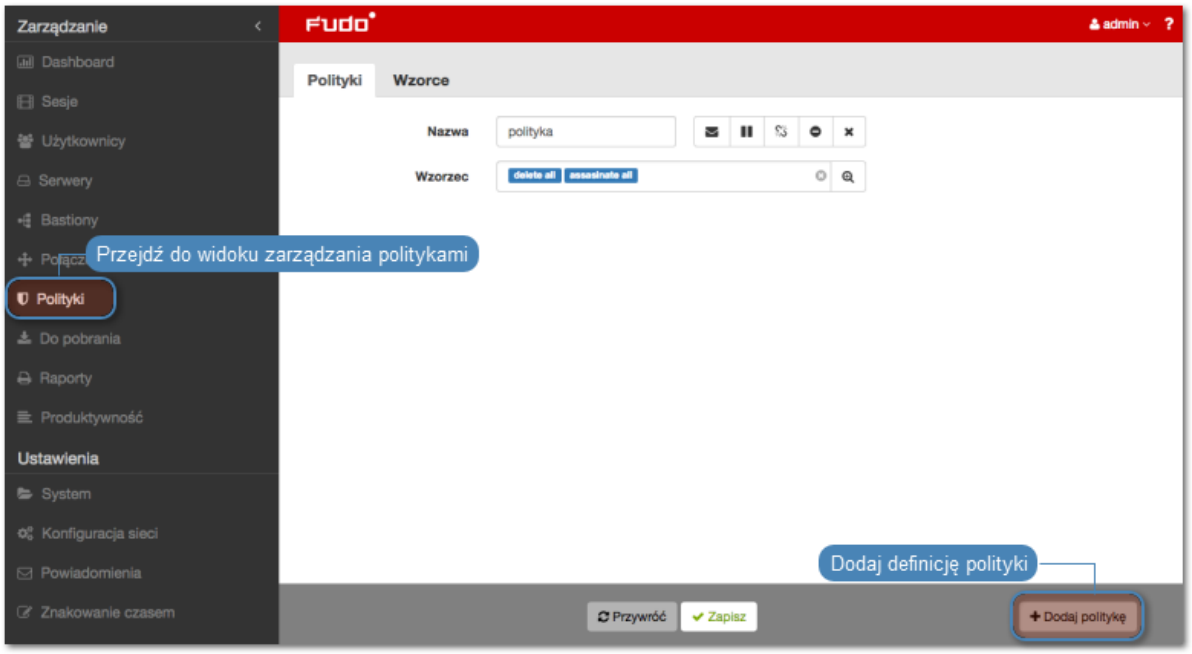
Komenda `rm -rf` (*także* `-fr`; `-Rf`; `-fR`)

```
(^|[^a-zA-Z])rm[[:space:]]+-([rR]f|f[rR])
```

Komenda `rm file` `(^|[^a-zA-Z])rm[[:space:]]+([^[:space:]]+[[:space:]]*)?/full/path/to/a/file([[:space:]]|\;|$) (^|[^a-zA-Z])rm[[:space:]]+.*justafilename`

Definiowanie polityk

1. Wybierz z lewego menu *Zarządzanie* > *Polityki*.
2. Kliknij + *Dodaj politykę*.

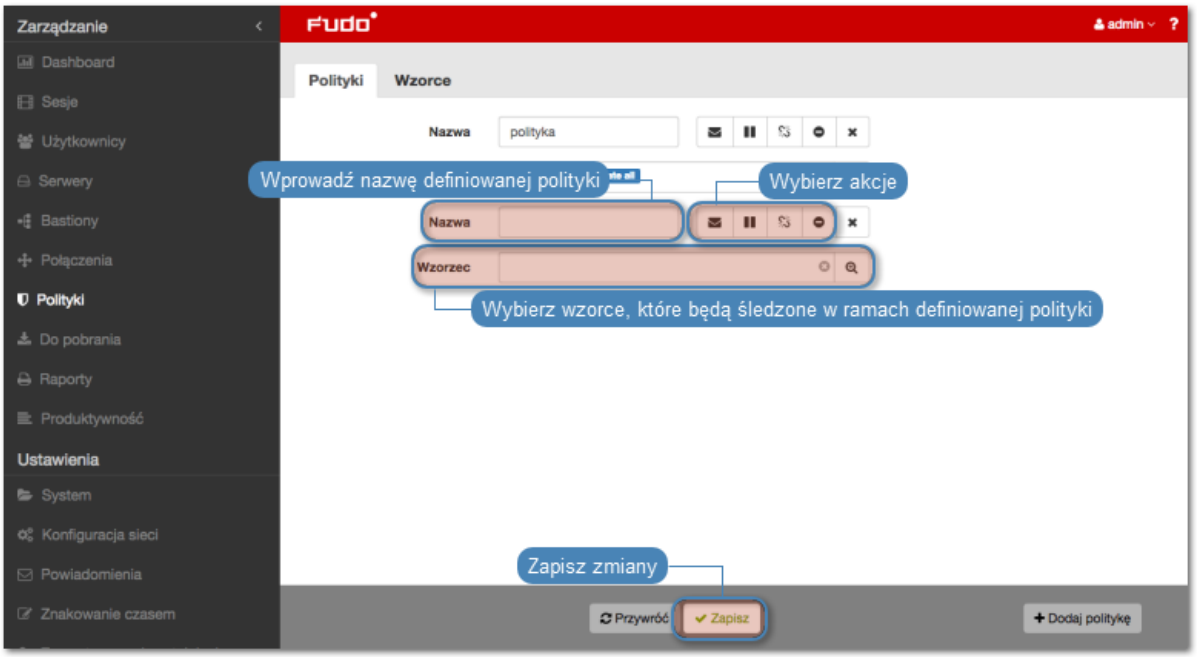


3. Wprowadź nazwę dla definiowanej polityki.
4. Określ akcje, które Wheel Fudo PAM podejmie z chwilą stwierdzenia wystąpienia któregoś ze wzorców.

	Wyślij powiadomienie email do administratora systemu.
	Wstrzymaj połączenie.
	Przerwij połączenie.
	Zablokuj konto użytkownika.

Informacja: Przerwanie połączenia skutkuje automatycznym zablokowaniem użytkownika. Podobnie, zablokowanie użytkownika powoduje automatyczne przerwanie połączenia.

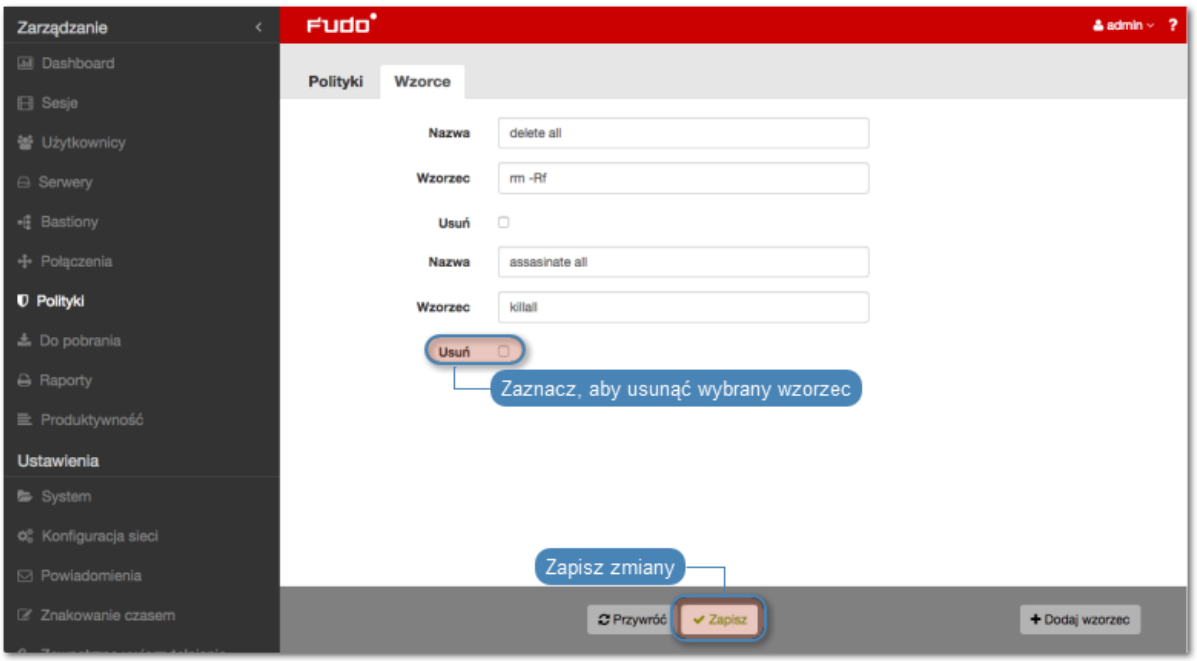
5. Wybierz wzorce śledzone w ramach danej polityki.
6. Kliknij *Zapisz*.



Informacja: Po utworzeniu polityki, można ją przypisać do serwera zdefiniowanego w połączeniu.

Usuwanie definicji wzorców

1. Wybierz z lewego menu *Zarządzanie* > *Polityki*.
2. Wybierz zakładkę *Wzorce*.
3. Zaznacz opcję *Usuń* przy wybranym wzorcu.
4. Kliknij *Zapisz*.



Usuwanie definicji polityk

Aby usunąć definicję polityki, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Polityki*.
2. Zaznacz opcję *Usuń* przy wybranej polityce.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Przerywanie połączenia*
- *Powiadomienia*
- *Sejfy*
- *Bezpieczeństwo*

ROZDZIAŁ 3

Sesje

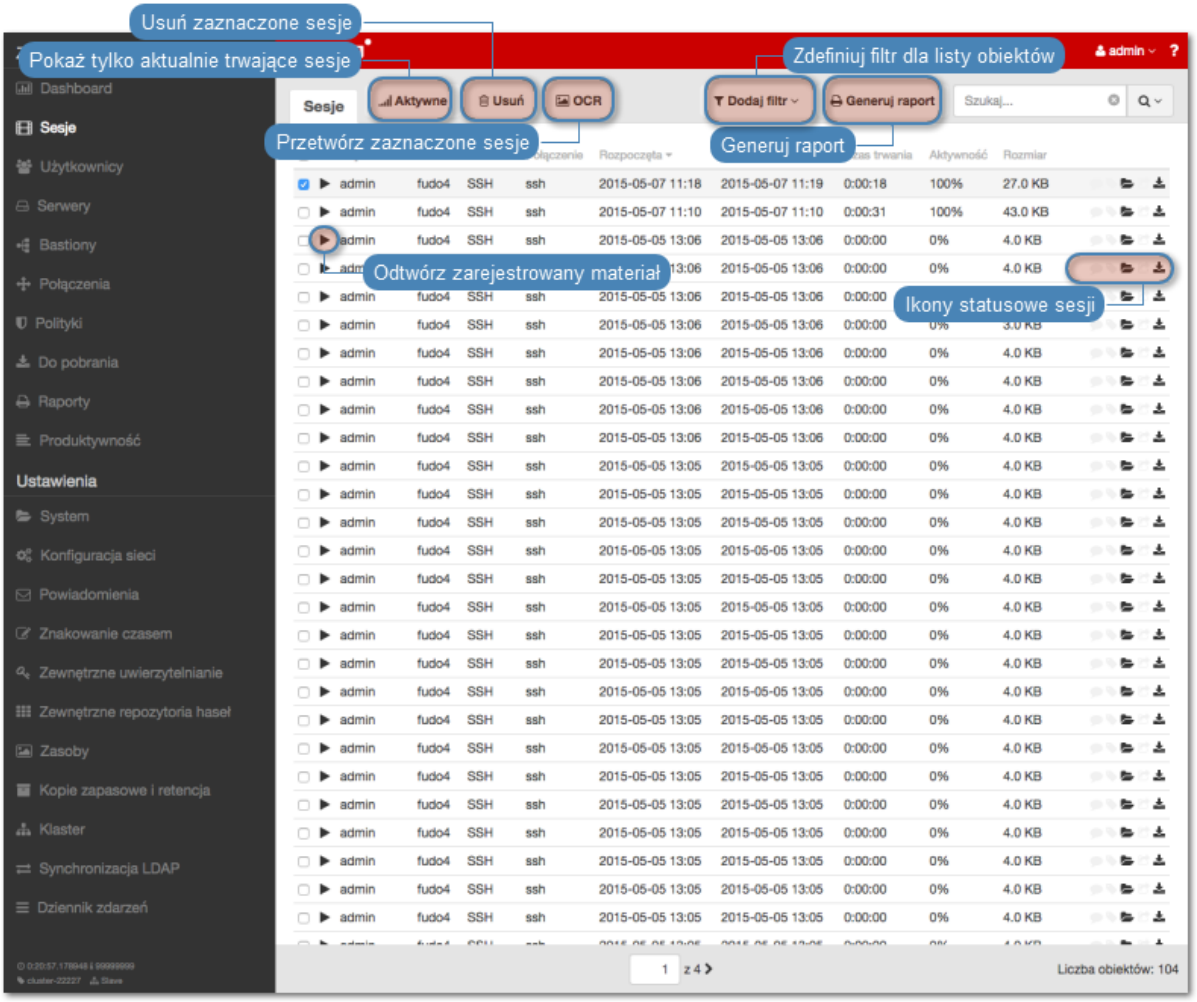
Wheel Fudo PAM przechowuje wszystkie nagrane sesje administracyjne, dając możliwość ich odtworzenia, przejrzenia, kasowania oraz eksportowania.

Widok zarządzania sesjami pozwala na filtrowanie zapisanych sesji, podgląd sesji aktualnie trwających oraz pobranie zapisanych sesji dostępu. Widok dostrcza także informacji statusowych na temat każdej z sesji oraz pozwala zarządzać wygenerowanymi wcześniej odnośnikami.

Ikona	Opis
	Odtwarzaj sesję (*dotyczy sesji nagranych z opcją rejestrowania pełnego ruchu*).
	Sesja opatrzona znacznikiem czasu.
	Powód nawiązania sesji.
	Sesja zawiera naniesione komentarze.
	Sesja została przetworzona na potrzeby przeszukiwania pełnotekstowego.
	Otwórz zarządzanie udostępnianiem sesji.
	Pobierz materiał sesji w wybranym formacie (*dotyczy sesji nagranych z opcją rejestrowania pełnego lub surowego ruchu*).
	Monitor aktywności użytkownika (*dotyczy sesji aktualnie trwających*).

Aby przejść do widoku zarządzania sesjami wybierz z lewego menu opcję *Zarządzanie* > *Sesje*.

Informacja: Wheel Fudo PAM przechowuje materiał sesji w formie skompresowanej, z czego wynikać mogą różnice pomiędzy podawanym a faktycznym rozmiarem sesji.

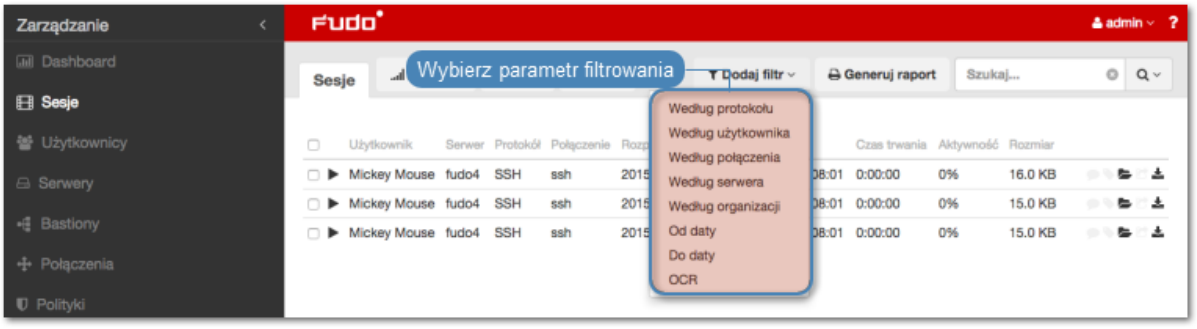


3.1 Filtrowanie sesji

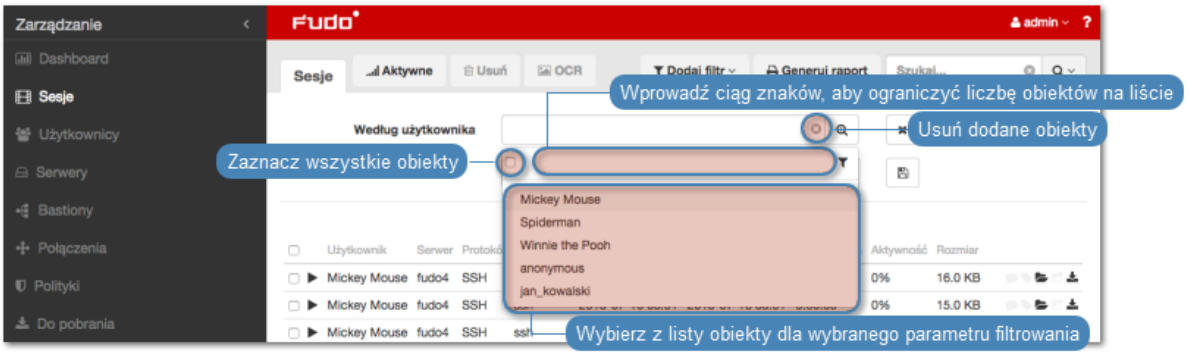
Filtrowanie pozwala na łatwiejsze odnalezienie żądanej sesji dzięki ograniczeniu ilości pozycji na liście zarejestrowanych sesji. Opcje filtrowania pozwalają na wybranie wielu obiektów jednego typu a zdefiniowany zestaw filtrów może zostać zapisany dla wygody operatora systemu.

3.1.1 Definiowanie filtrów

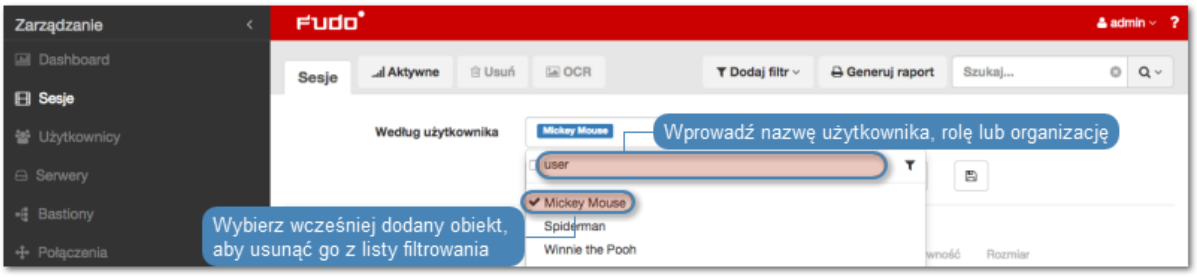
1. Kliknij *Dodaj filtr* i wybierz z listy rozwijalnej typ parametru filtrowania.



2. Wybierz wartości dla wcześniej dodanego parametru filtrowania.



Informacja: Wprowadź ciąg znaków, aby ograniczyć liczbę pozycji na liście. W przypadku użytkowników, zawartość listy można ograniczyć do użytkowników o przypisanej roli lub należących do określonej organizacji.



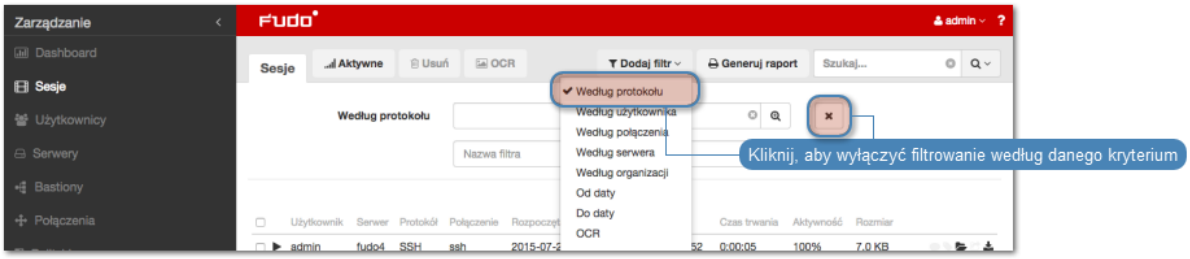
Ponownie wybierz wcześniej dodany obiekt, aby usunąć go z listy.

Dla parametrów filtrowania według protokołu, użytkownika, połączenia, serwera, organizacji możliwe jest wybranie wielu obiektów danego typu.

3. Powtarzaj kroki 1. i 2., aby zdefiniować kolejne kryteria filtrowania.

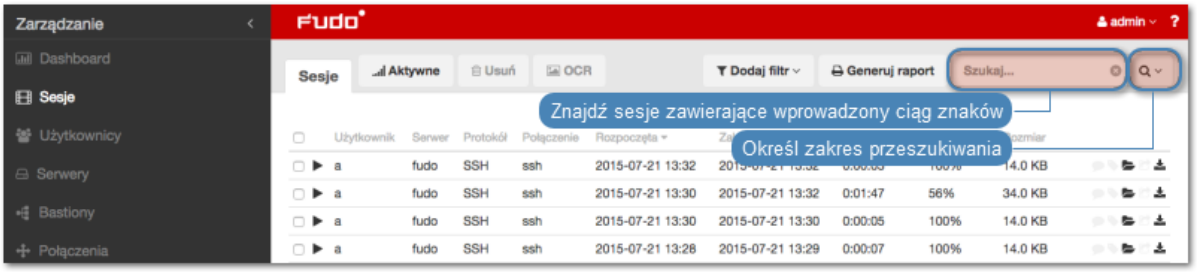
Informacja: Na liście sesji wyświetlone zostaną tylko pozycje, które spełniają wszystkie warunki filtrowania.

4. Kliknij *Dodaj filtr* i wybierz ponownie wcześniej zaznaczony parametr filtrowania, aby wyłączyć filtrowanie według zadanego parametru.



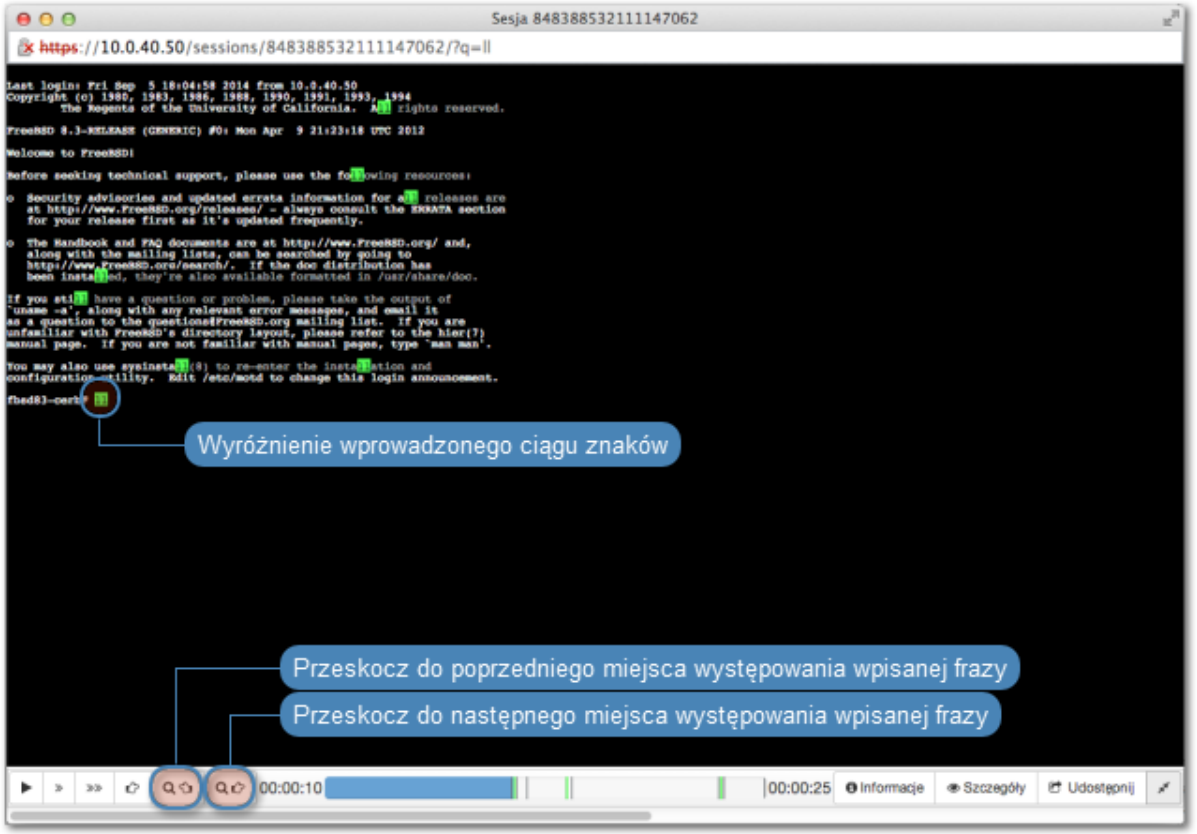
3.1.2 Przeszukiwanie pełnotekstowe

Wheel Fudo PAM pozwala na przeszukiwanie zapisanego materiału, ograniczając listę sesji do pozycji zawierających wskazany ciąg znaków.



Informacja: Odtwarzanie sesji znalezionych na podstawie wprowadzonej frazy rozpoczyna się w miejscu jej pierwszego wystąpienia.

Odtwarzacz pozwala na przeskakiwanie pomiędzy wystąpieniami wprowadzonego ciągu znaków.

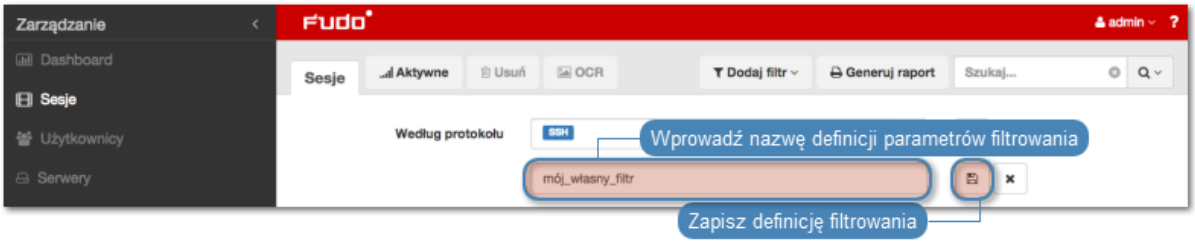


3.1.3 Zarządzanie definicjami filtrowania

Aktualne parametry filtrowania mogą zostać zapisane z wybraną nazwą dla wygody operatora systemu.

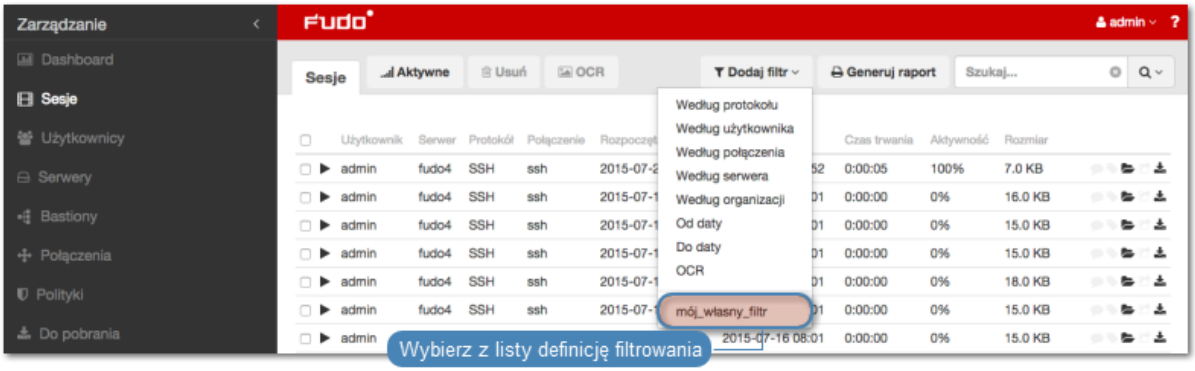
Zapisywanie definicji filtrowania

1. Zdefiniuj parametry filtrowania zgodnie z procedurą opisaną w sekcji *Filtrowanie sesji*.
2. Wprowadź nazwę definicji filtrowania.
3. Kliknij ikonę zapisu ustawień.



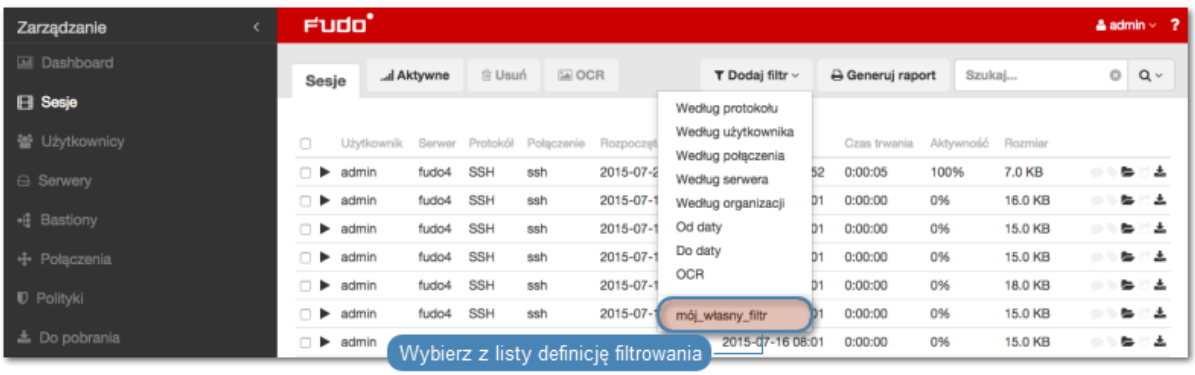
Edycja definicji filtrowania

1. Kliknij *Dodaj filtr* i wybierz żądaną definicję filtrowania.
2. Zmodyfikuj opcje filtrowania zgodnie z potrzebą.
3. Kliknij ikonę zapisu ustawień.

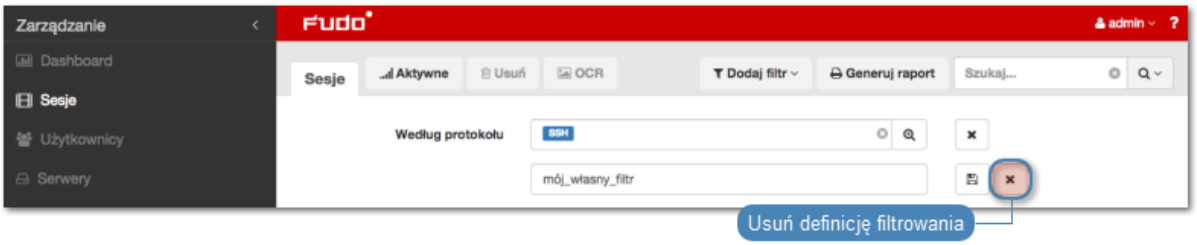


Usuwanie definicji filtrowania

1. Kliknij *Dodaj filtr* i wybierz żądaną definicję filtrowania.



2. Kliknij ikonę usunięcia definicji filtrowania.



3. Potwierdź usunięcie wybranej definicji filtrowania.

Tematy pokrewne:

- *Widok zarządzania sesjami*
- *Opis systemu*
- *Raporty*

3.2 Raporty

Usługa raportowania generuje szczegółową statystykę połączeń użytkowników w ramach określonych sesji dostępowych.

Pełne raporty generowane są cyklicznie przez system (dziennie, tygodniowo, miesięcznie, kwartalnie), i dostępne dla użytkowników o zdefiniowanej roli `superadmin`. Raporty generowane cyklicznie dla użytkowników o rolach `admin` lub `operator`, generowane są indywidualnie i zawierają jedynie dane sesji, do których określony użytkownik posiada uprawnienia.

Oprócz domyślnych raportów systemowych, raporty cykliczne mogą być także generowane na podstawie zapisanej *definicji filtrowania*. Raport może być również wygenerowany na żądanie, i zawierać dane dotyczące wskazanych sesji.

Subskrybowanie raportu cyklicznego

Aby włączyć usługę generowania raportów cyklicznych dla zalogowanego użytkownika, postępuj zgodnie z poniższą instrukcją.

Informacja: Raporty cykliczne, generowane na żądanie określonego użytkownika, zawierają dane sesji, do których użytkownik posiada uprawnienia.

---

1. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
2. Kliknij *Zarządzaj subskrypcją*, aby wyświetlić dostępne opcje raportów cyklicznych.
3. Wybierz z listy rozwijalnej typ raportu.

Informacja: Lista zawiera opcje domyślne oraz zapisane przez użytkownika *definicje filtrowania*.

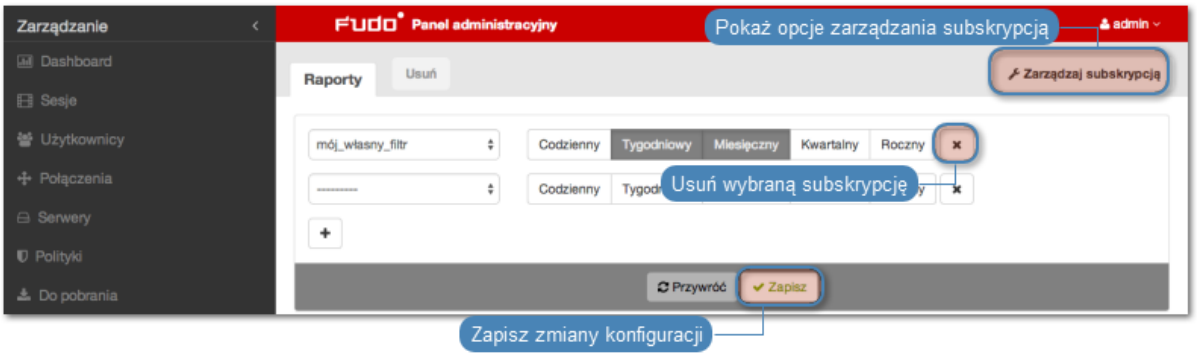
---

4. Zaznacz częstotliwość generowania wybranego raportu.
5. Kliknij *Zapisz*.

Rezygnacja z subskrypcji raportu cyklicznego

Aby zrezygnować z subskrypcji raportu cyklicznego, postępuj zgodnie z poniższą instrukcją.

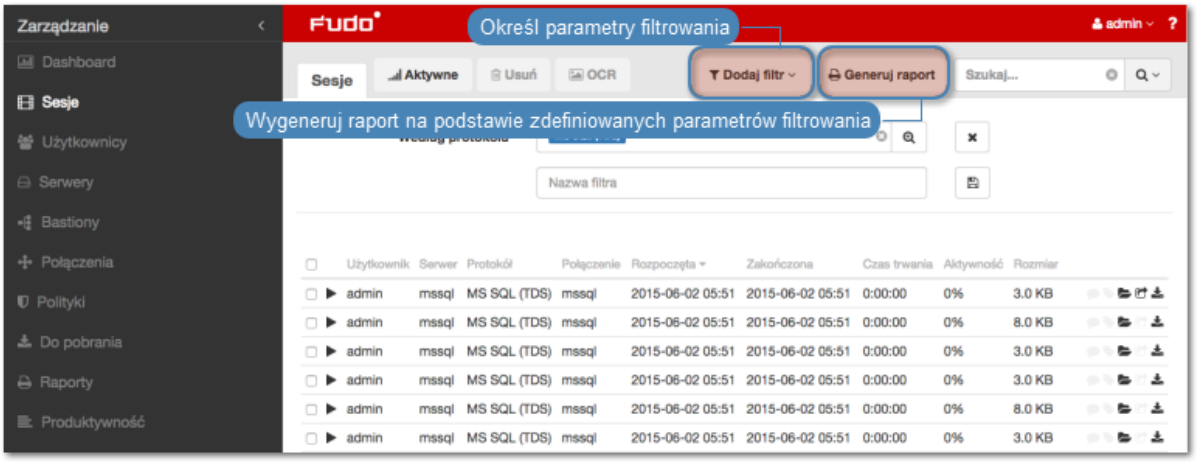
1. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
2. Kliknij *Zarządzaj subskrypcją*, aby wyświetlić dostępne opcje raportów cyklicznych.
3. Zaznacz opcję usunięcia przy wybranej definicji subskrypcji.
4. Kliknij *Zapisz*.



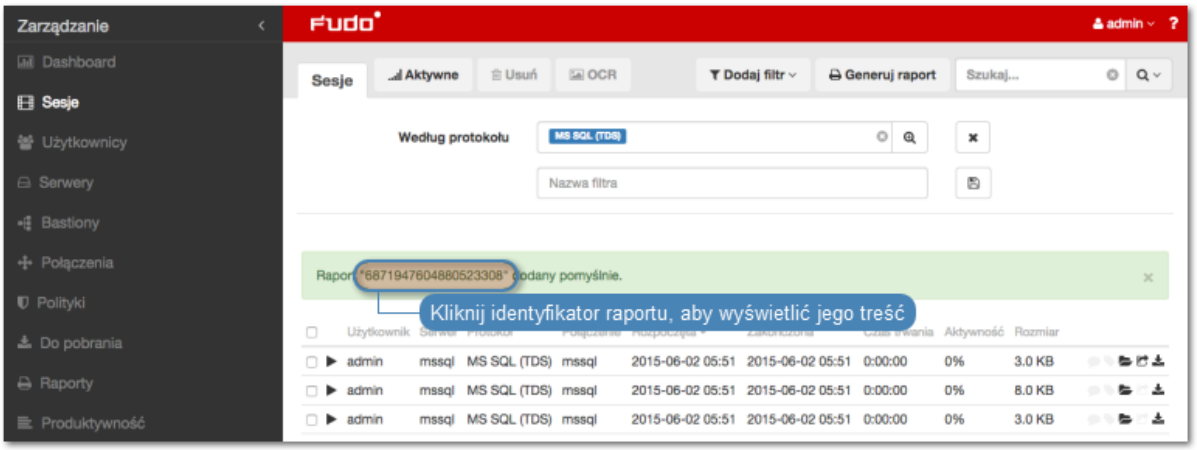
Generowanie raportu na żądanie

Raport może zostać wygenerowany dla określonego podzbioru sesji, zdefiniowanego parametrami filtrowania.

1. Wybierz z lewego menu‘Zarządzanie > Sesje‘.
2. Kliknij *Dodaj filtr* i zdefiniuj parametry filtrowania (więcej na temat filtrowania sesji, znajdziesz w rozdziale *Kontrola sesji zdalnego dostępu: Filtrowanie sesji*).
3. Kliknij *Generuj raport*.



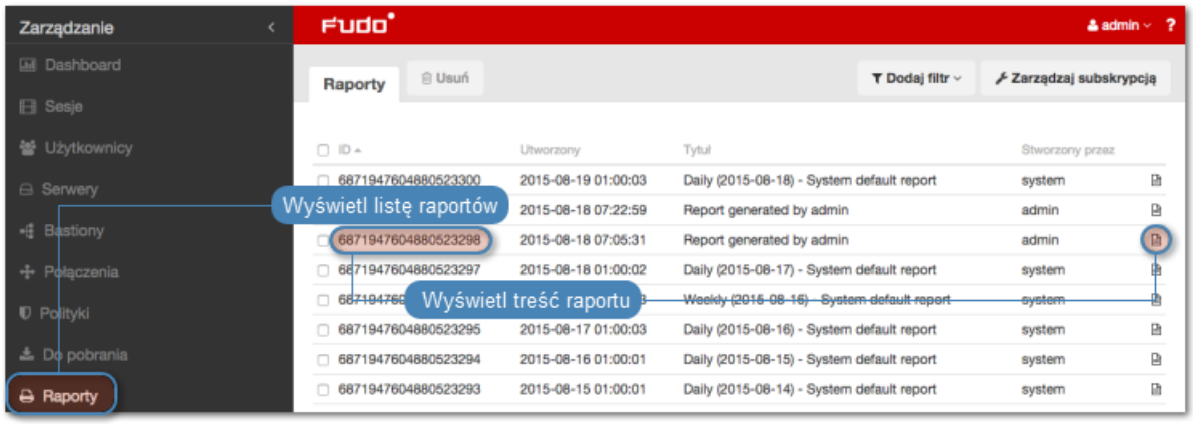
4. Kliknij identyfikator raportu, aby wyświetlić jego treść.



5. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
6. Kliknij ikonę podglądu raportu przy wybranym raporcie lub jego identyfikator, aby zobaczyć jego treść.
7. Kliknij *CSV*, *PDF*, *HTML*, aby zapisać raport w wybranym formacie.

Wyświetlanie i zapisywanie raportów

1. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
2. Odszukaj i kliknij identyfikator lub ikonę podglądu treści wybranego raportu.



3. Kliknij *CSV*, *PDF*, *HTML*, aby zapisać raport w wybranym formacie.

Usuwanie raportów

1. Wybierz z lewego menu‘Zarządzanie > Raporty‘.
2. Zaznacz żądane raporty i kliknij *Usuń*.
3. Potwierdź usunięcie zaznaczonych raportów.

Tematy pokrewne:

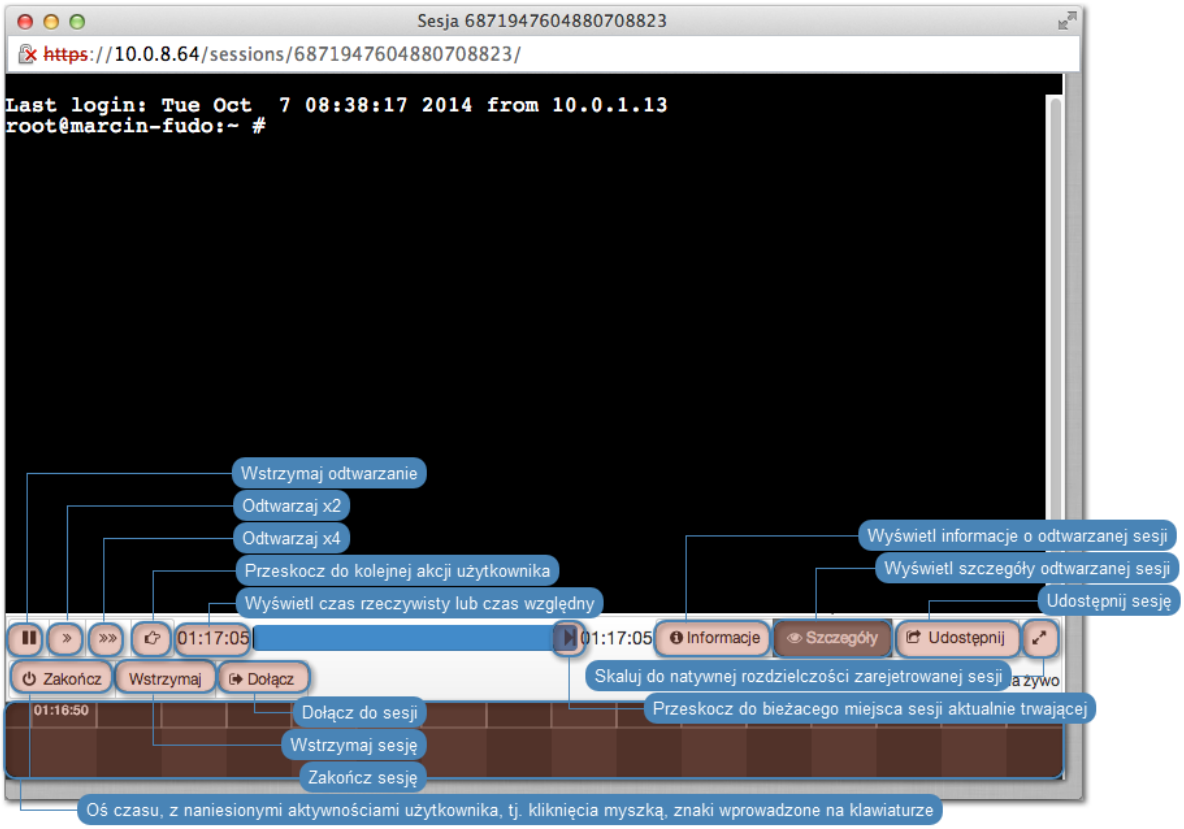
- *Powiadomienia*
- *Filtrowanie sesji*

3.3 Odtwarzanie sesji

Wheel Fudo PAM pozwala zarówno na odtwarzanie zarejestrowanych sesji połączeniowej jak i podgląd aktualnie trwających połączeń.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Wyszukaj na liście żądaną sesję i kliknij ikonę rozpoczęcia odtwarzania.

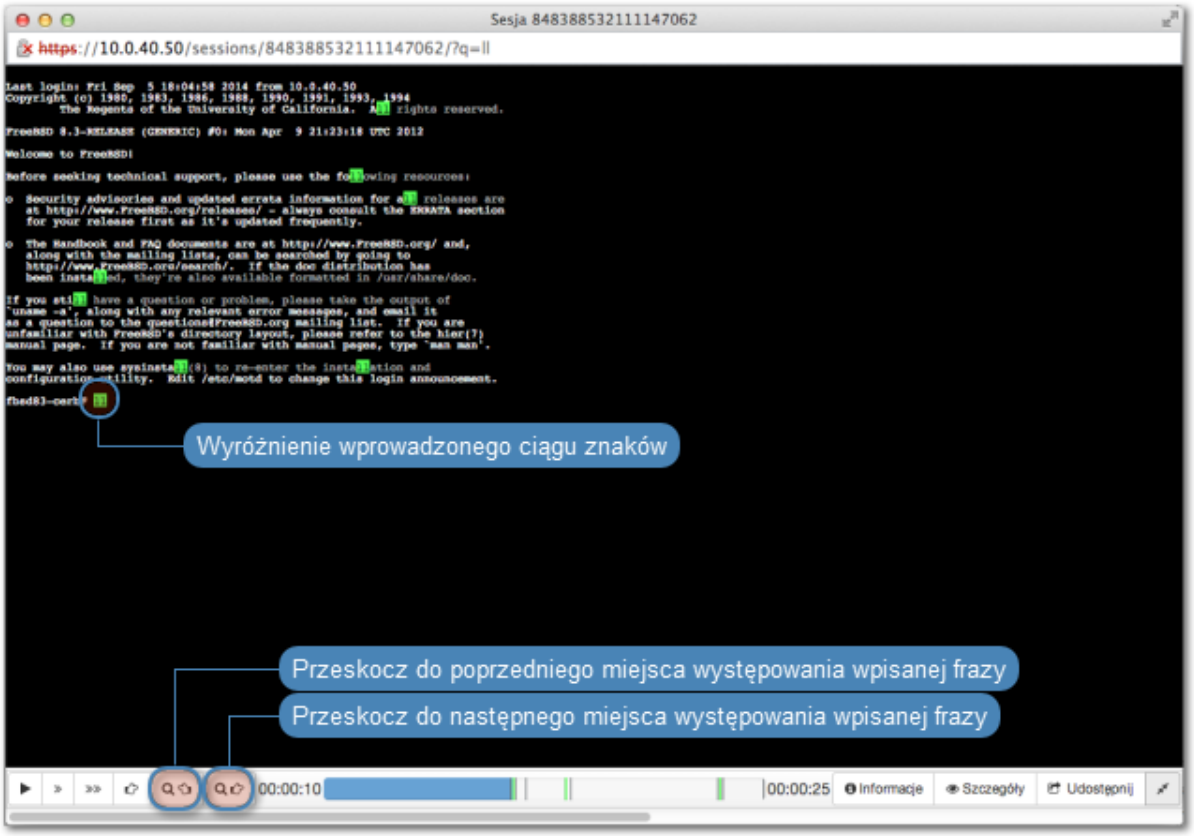
Opcje odtwarzacza



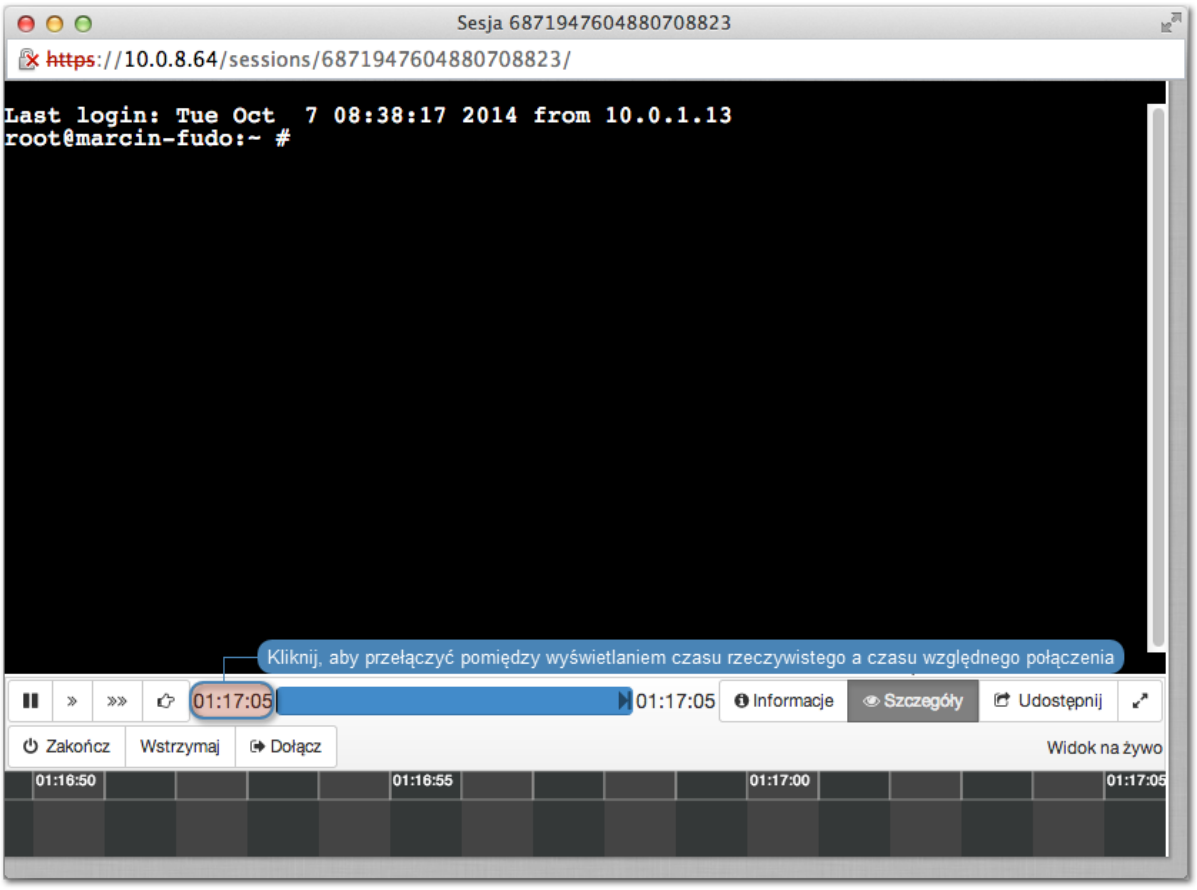
Informacja: Niektóre funkcje dostępne są tylko dla podglądu sesji aktualnie trwających.

Informacja: Odtwarzanie sesji znalezionych na podstawie wprowadzonej frazy rozpoczyna się w miejscu jej pierwszego wystąpienia.

Odtwarzacz pozwala na przeskakiwanie pomiędzy wystąpieniami wprowadzonego ciągu znaków.



Informacja: Kliknij w zegar odmierzający czas odtwarzanej sesji, aby przełączyć pomiędzy czasem bezwzględnym i względnym.



Tematy pokrewne:

- *Funkcjonalności wrażliwe*

3.4 Podgląd trwających sesji

Wheel Fudo PAM umożliwia podgląd sesji aktualnie trwających, co pozwala na bieżącą kontrolę aktywności użytkowników.

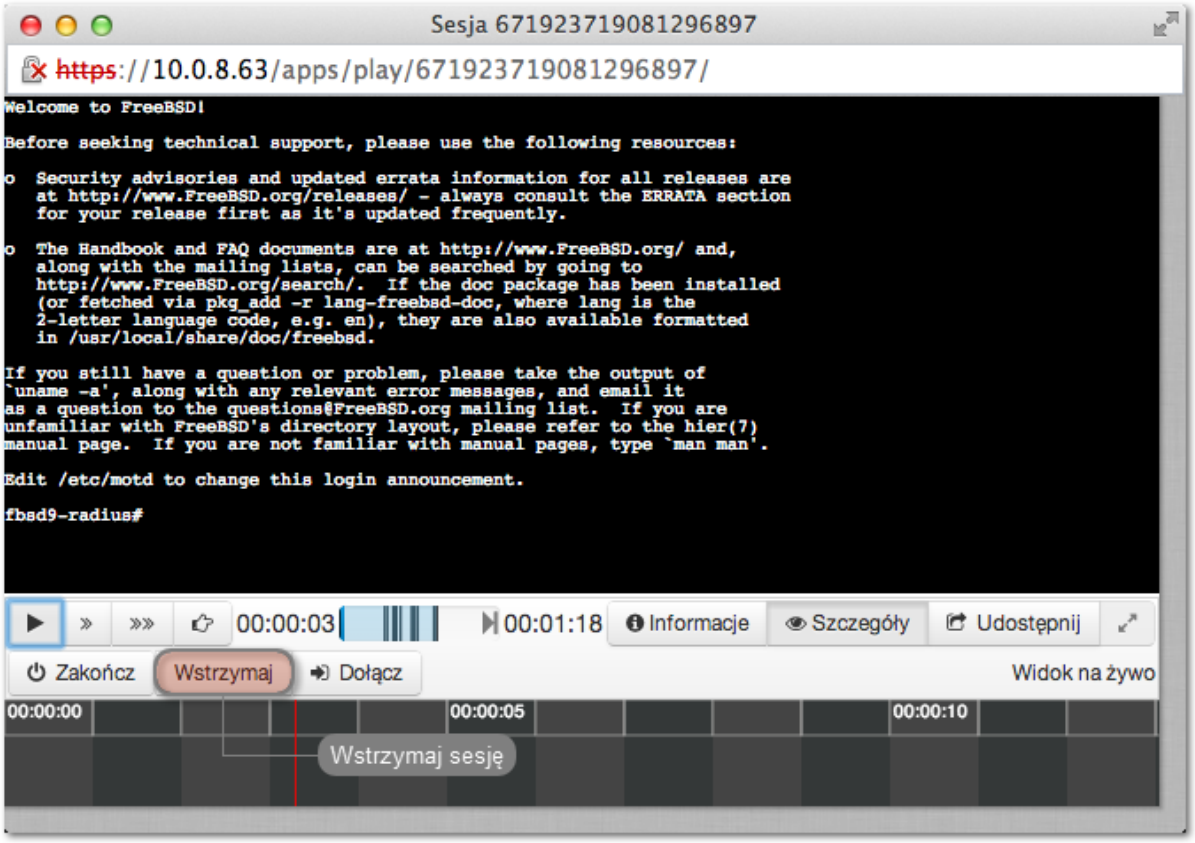
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij *Aktywne*, aby wyświetlić listę trwających połączeń.
3. Wyszukaj żądaną sesję i kliknij ikonę odtwarzania, aby otworzyć *okno odtwarzacza*.

3.5 Wstrzymywanie połączenia

W przypadku gdy aktualne akcje użytkownika wymagają analizy, połączenie może zostać wstrzymane.

Informacja: Wstrzymanie połączenia powoduje czasowe wstrzymanie transmisji pakietów. W przypadku wznowienia połączenia, akcje wykonane przez użytkownika w czasie wstrzymania sesji zostaną przesłane do serwera.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij *Aktywne*, aby wyświetlić listę aktualnie trwających połączeń.
3. Wyszukaj i kliknij żądaną sesję i kliknij ikonę rozpoczęcia odtwarzania.
4. Kliknij *Wstrzymaj*.



Tematy pokrewne:

- *Odtwarzanie sesji*
- *Dołączanie do sesji*
- *Filtrowanie sesji*

3.6 Przerywanie połączenia

W przypadku gdy administrator stwierdzi nadużycie praw dostępu, może przerwać sesję połączeniową użytkownika.

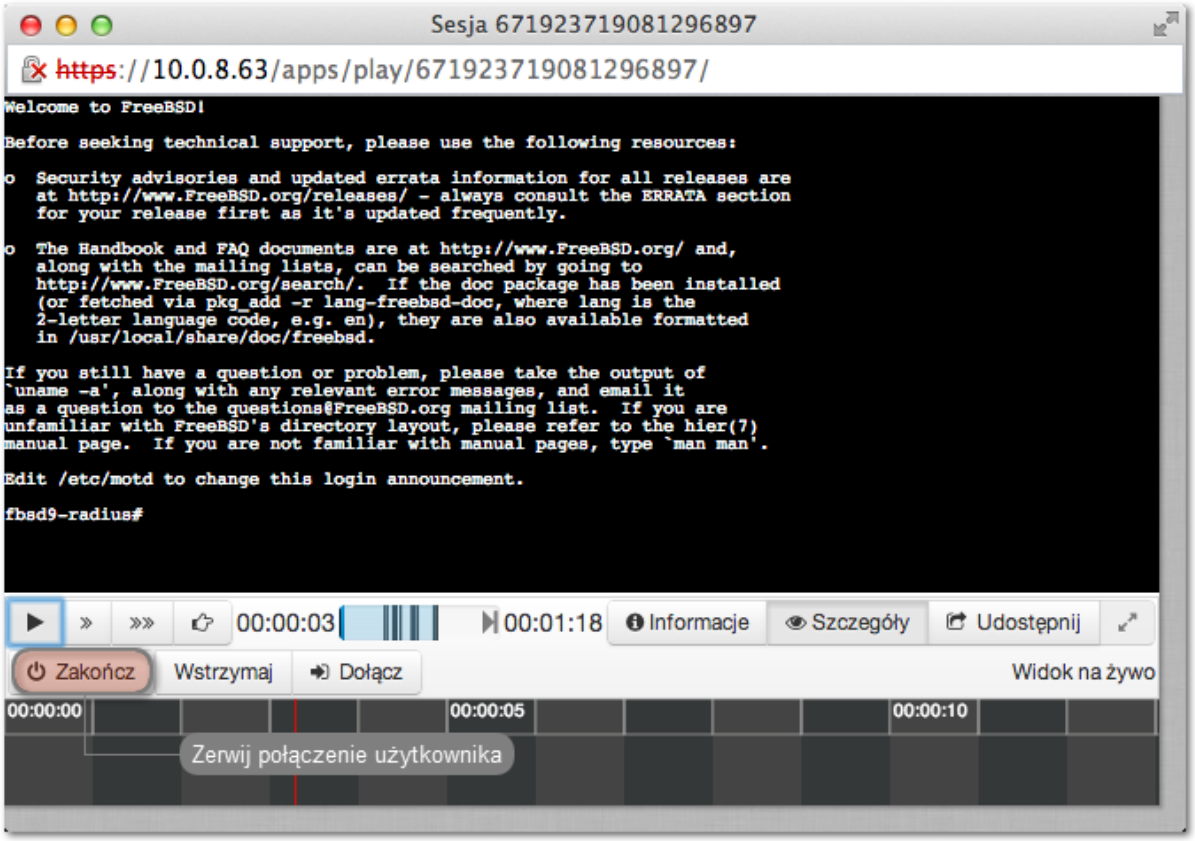
Informacja: Wheel Fudo PAM umożliwia automatyczne zablokowanie użytkownika, z chwilą wykrycia zdefiniowanego ciągu znaków. Więcej informacji na temat polityk i wzorców znajdziesz w rozdziale *Polityki*.

---

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij *Aktywne*, aby wyświetlić listę aktualnie trwających połączeń.

3. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
4. Kliknij *Zakończ*, aby przerwać połączenie.

Informacja: Zerwanie połączenia automatycznie blokuje konto użytkownika.



5. Zdecyduj czy użytkownik powinien pozostać zablokowany.

Tematy pokrewne:

- *Polityki*
- *Mechanizmy bezpieczeństwa*
- *Dołączanie do sesji*
- *Udostępnianie sesji*
- *Filtrowanie sesji*

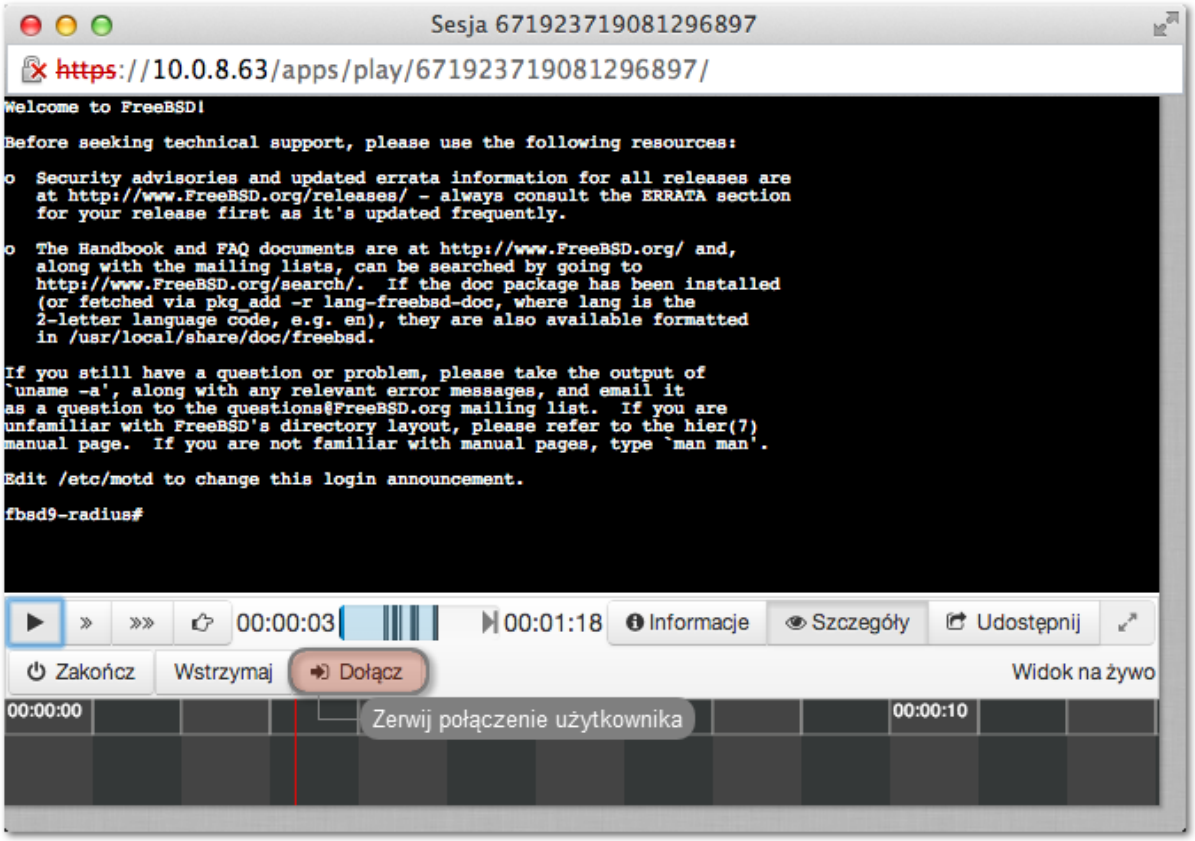
3.7 Dołączanie do sesji

Wheel Fudo PAM pozwala administratorowi na dołączenie do aktualnie trwającej sesji i jednoczesną pracę z użytkownikiem.

Aby dołączyć do aktualnie trwającej sesji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij przycisk *Aktywne*.

3. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
4. Kliknij przycisk *Dołącz*.



Tematy pokrewne:

- *Odtwarzanie sesji*
- *Udostępnianie sesji*
- *Filtrowanie sesji*

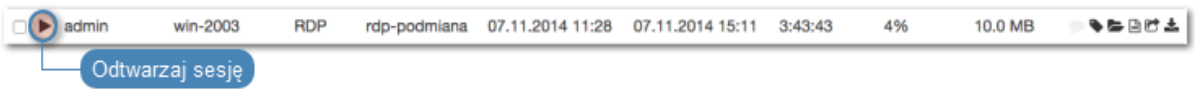
3.8 Udostępnianie sesji

Wheel Fudo PAM umożliwia udostępnienie innemu użytkownikowi sesji zapisanej oraz aktualnie trwającej.

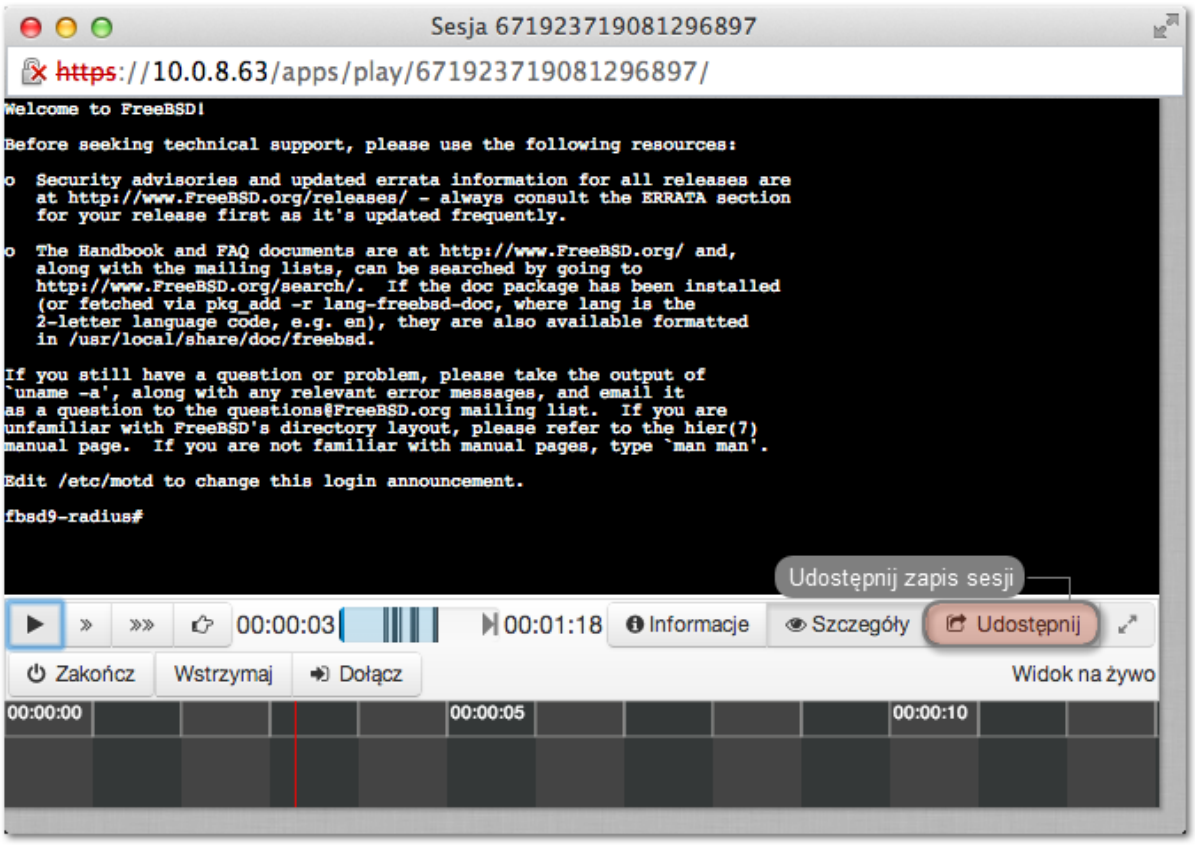
Udostępnianie sesji

Aby udostępnić sesję, postępuj zgodnie z poniższą instrukcją.

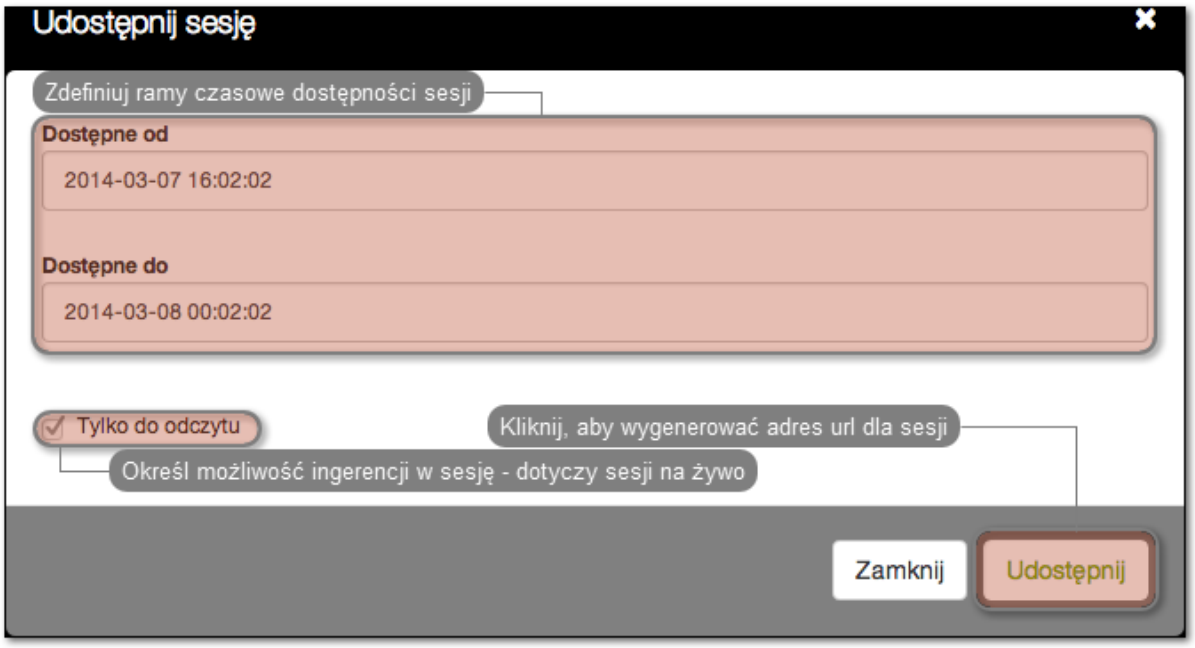
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.



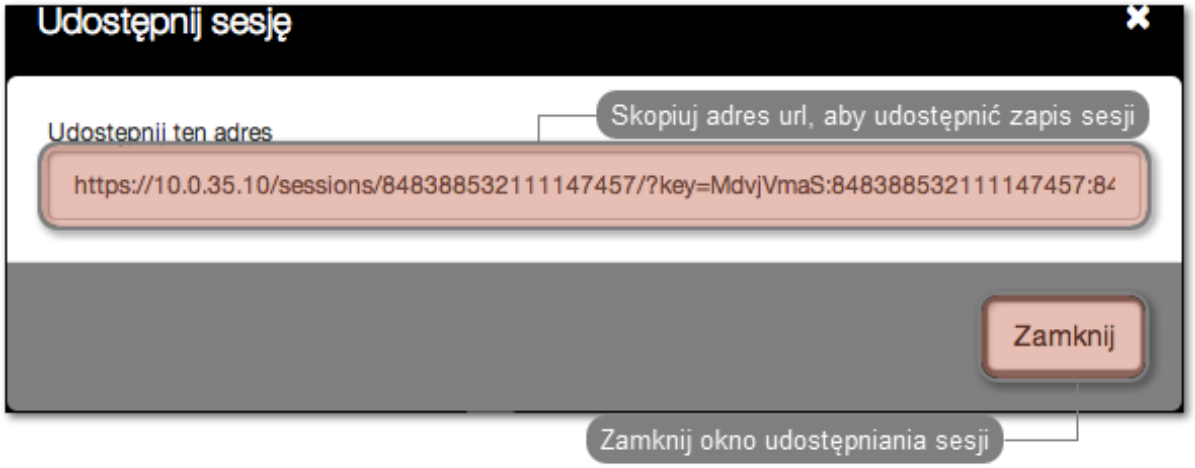
3. Kliknij *Udostępnij*.



4. Określ ramy czasowe dostępności sesji i kliknij *Zatwierdź*, aby wygenerować adres URL, pod którym udostępniony zostanie zapis sesji.

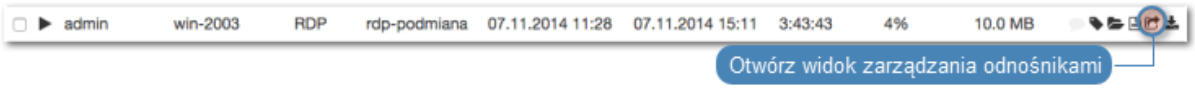


5. Skopiuj odnośnik i kliknij *Zamknij*.

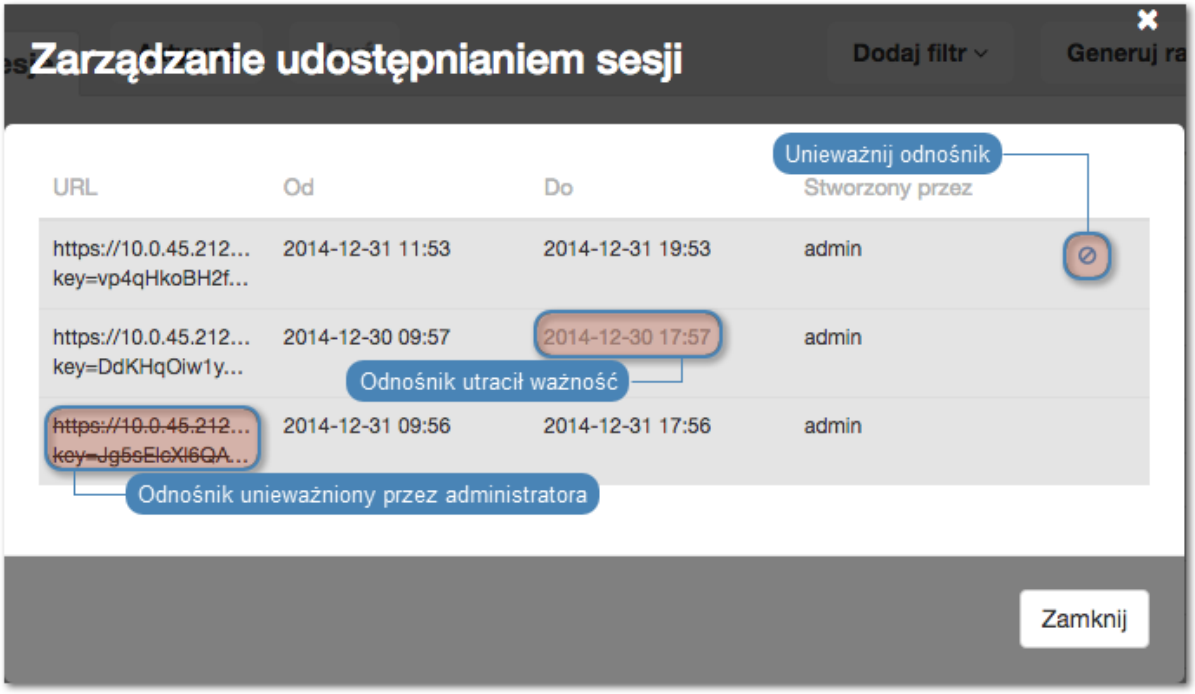


Unieważnienie odnośnika

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Znajdź żądaną sesję i kliknij ikonę udostępniania, aby otworzyć okno zarządzania odnośnikami.



3. Kliknij ikonę unieważnienia odnośnika.



Tematy pokrewne:

- *Odtwarzanie sesji*
- *Dołączanie do sesji*
- *Filtrowanie sesji*

3.9 Komentowanie sesji

Wheel Fudo PAM pozwala na dodawanie komentarzy i znaczników do zarejestrowanych sesji.

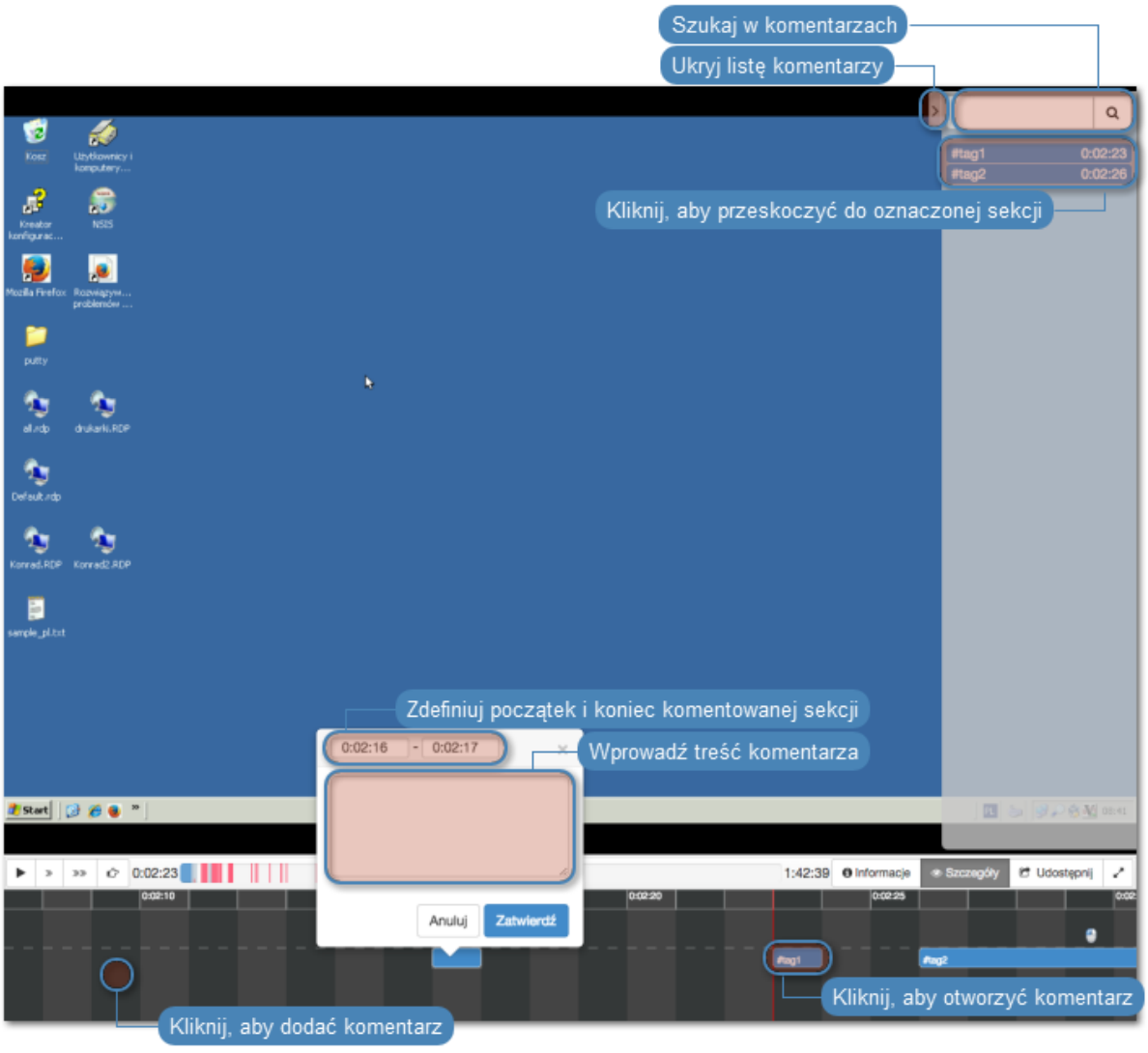
Dodawanie komentarza

1. Wybierz *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
3. Kliknij *Szczegóły*.
4. Kliknij w dolnym obszarze osi czasu, aby dodać komentarz.
5. Zdefiniuj przedział czasu, którego dotyczy dodawany komentarz.

Informacja: Kliknij i przeciągnij bok prostokąta, aby zmienić ramy czasowe komentarza.

---

6. Dodaj treść komentarza.
7. Kliknij *Zatwierdź*.



Edytowanie komentarza

1. Wybierz *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
3. Kliknij *Szczegóły*.
4. Znajdź i kliknij wybrany komentarz.
5. Kliknij ikonę edycji komentarza.
6. Wprowadź zmiany i kliknij *Zatwierdź*.

Usuwanie komentarza

1. Wybierz *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
3. Kliknij *Szczegóły*.
4. Znajdź i kliknij wybrany komentarz.
5. Kliknij ikonę kosza.
6. Kliknij *Usuń*.

Dodawanie odpowiedzi do komentarza

1. Wybierz *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
3. Kliknij *Szczegóły*.
4. Znajdź i kliknij wybrany komentarz.

5. Kliknij *Odpowiedz*.
6. Wprowadź treść odpowiedzi i kliknij *Zatwierdź*.

Tematy pokrewne:

- *Funkcjonalności wrażliwe*

3.10 Eksportowanie sesji

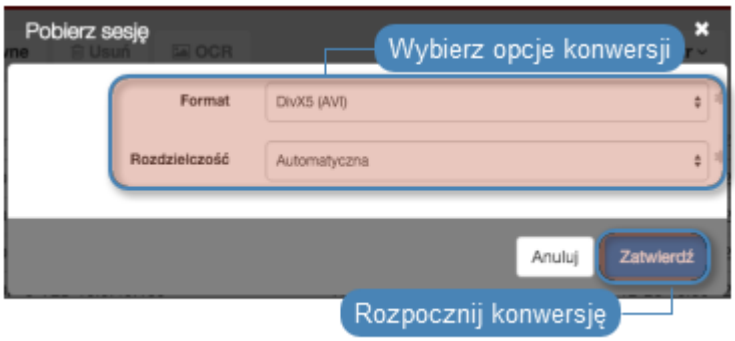
Wheel Fudo PAM pozwala na konwersję zapisanej sesji do jednego ze wspieranych formatów wyjściowych.

Aby wyeksportować sesję, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Znajdź żądaną sesję i kliknij ikonę eksportu zarejestrowanego materiału.

3. Wybierz format pliku wyjściowego.

Informacja: Format pliku wyjściowego oraz rozdzielczość obrazu wideo wpływają na czas trwania konwersji oraz rozmiar pliku wynikowego.



4. Wybierz rozdzielczość w jakiej zapisany ma być strumień wideo (*nie dotyczy konwersji materiału do formatu tekstowego*).

Informacja: Wybór opcji `Automatyczna` spowoduje wybór rozdzielczości odpowiadający rozdzielczości ekranu użytkownika z zapisanej sesji.

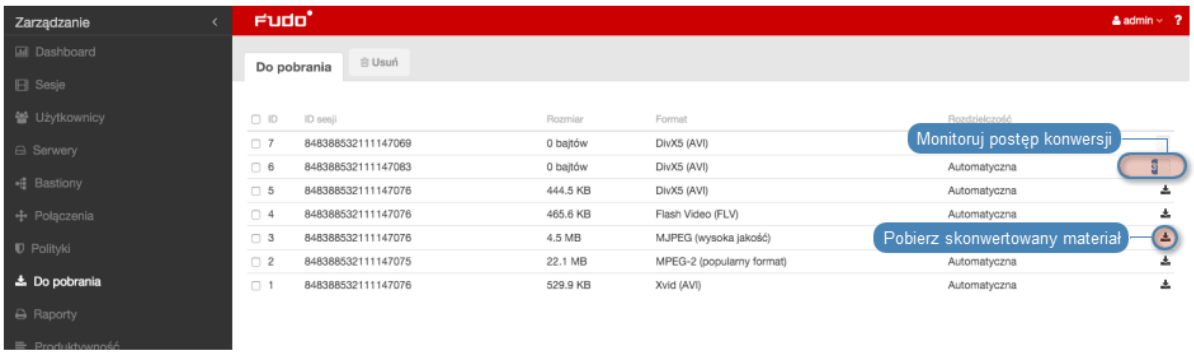
---

5. Kliknij *Zatwierdź*, aby rozpocząć konwersję i przejść do widoku *Do pobrania*.

Informacja: Widok *Do pobrania* umożliwia monitorowanie postępu konwersji.

---

6. Kliknij ikonę pobrania sesji.



Tematy pokrewne:

- *Filtrowanie sesji*
- *Udostępnianie sesji*
- *Odtwarzanie sesji*
- *Dołączanie do sesji*

3.11 Usuwanie sesji

Aby usunąć zarejestrowaną sesję, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Znajdź i zaznacz żądaną sesję.
3. Kliknij *Usuń*.
4. Potwierdź operację usunięcia sesji.

Informacja: Wheel Fudo PAM może automatycznie usuwać dane sesji po upływie czasu zadanego parametrem retencji. Więcej informacji znajdziesz w rozdziale *Kopie bezpieczeństwa i retencja danych*.

Tematy pokrewne:

- *Filtrowanie sesji*
- *Współdzielenie sesji*
- *Odtwarzanie sesji*
- *Eksportowanie sesji*

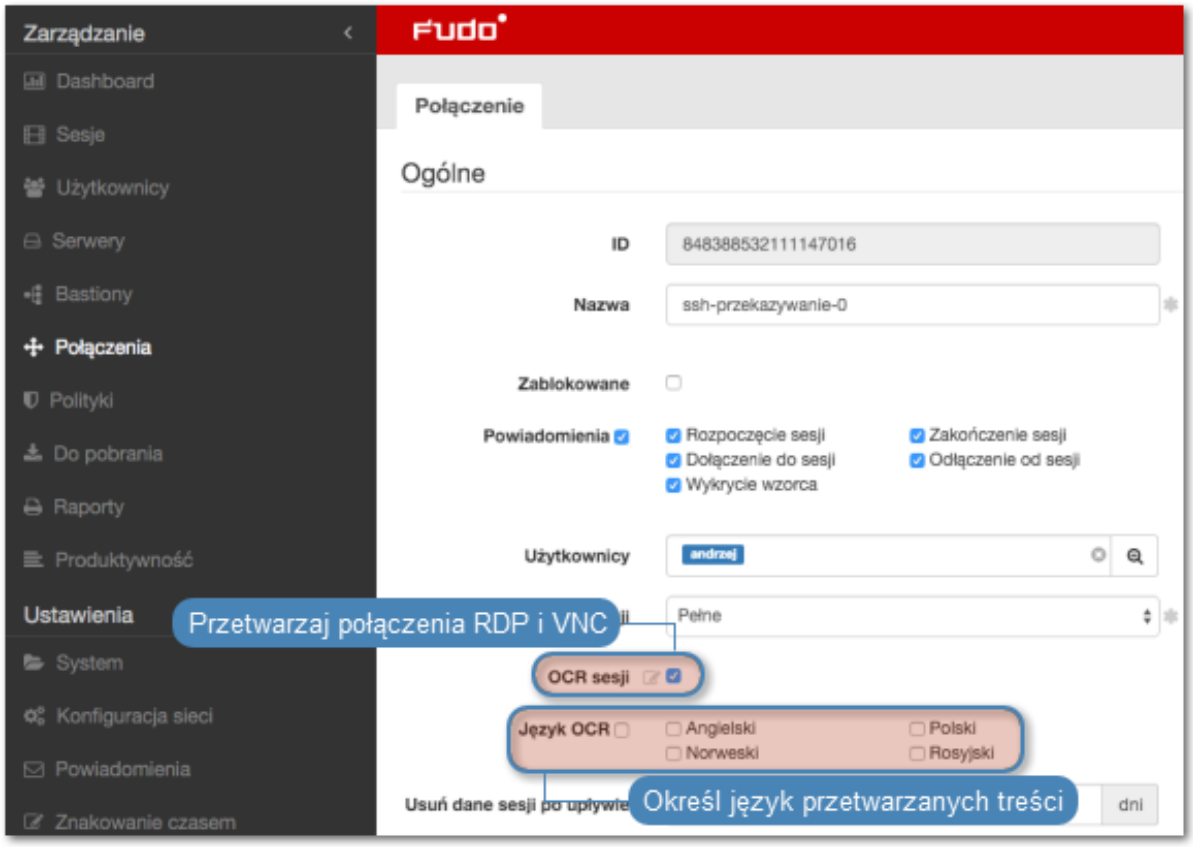
3.12 Przetwarzanie OCR sesji

Zarejestrowany materiał sesji RDP i VNC może być indeksowany na potrzeby przeszukiwania pełnotekstowego.

Automatyczne przetwarzanie OCR sesji w ramach wybranego połączenia

Aby włączyć przetwarzanie OCR sesji w ramach wybranego połączenia, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Połączenia*.
2. Znajdź i wybierz żądane połączenie.
3. Zaznacz opcję *OCR sesji*.
4. Wybierz język przetwarzanych treści.

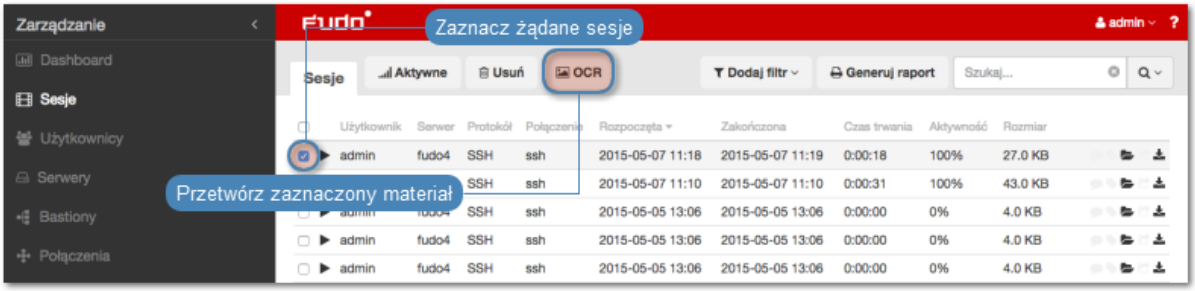


5. Kliknij *Zapisz*.

Przetwarzanie OCR wybranych sesji

Aby przetworzyć wybrane sesje, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Zaznacz żądane sesje i kliknij *OCR*.



Informacja: Opcje filtrowania sesji pozwalają na wybranie obiektów przetworzonych lub

nieprzetworzonych.

3. Zatwierdź przetwarzanie wybranych sesji.

Tematy pokrewne:

- *Filtrowanie sesji*
- *Konta*

ROZDZIAŁ 4

Analiza produktywności

Wheel Fudo PAM dostarcza narzędzie wspomagające analizę produktywności użytkowników monitorowanych systemów. Urządzenie śledzi aktywność użytkownika i pozwala wykazać aktywny czas połączenia.

4.1 Zestawienie

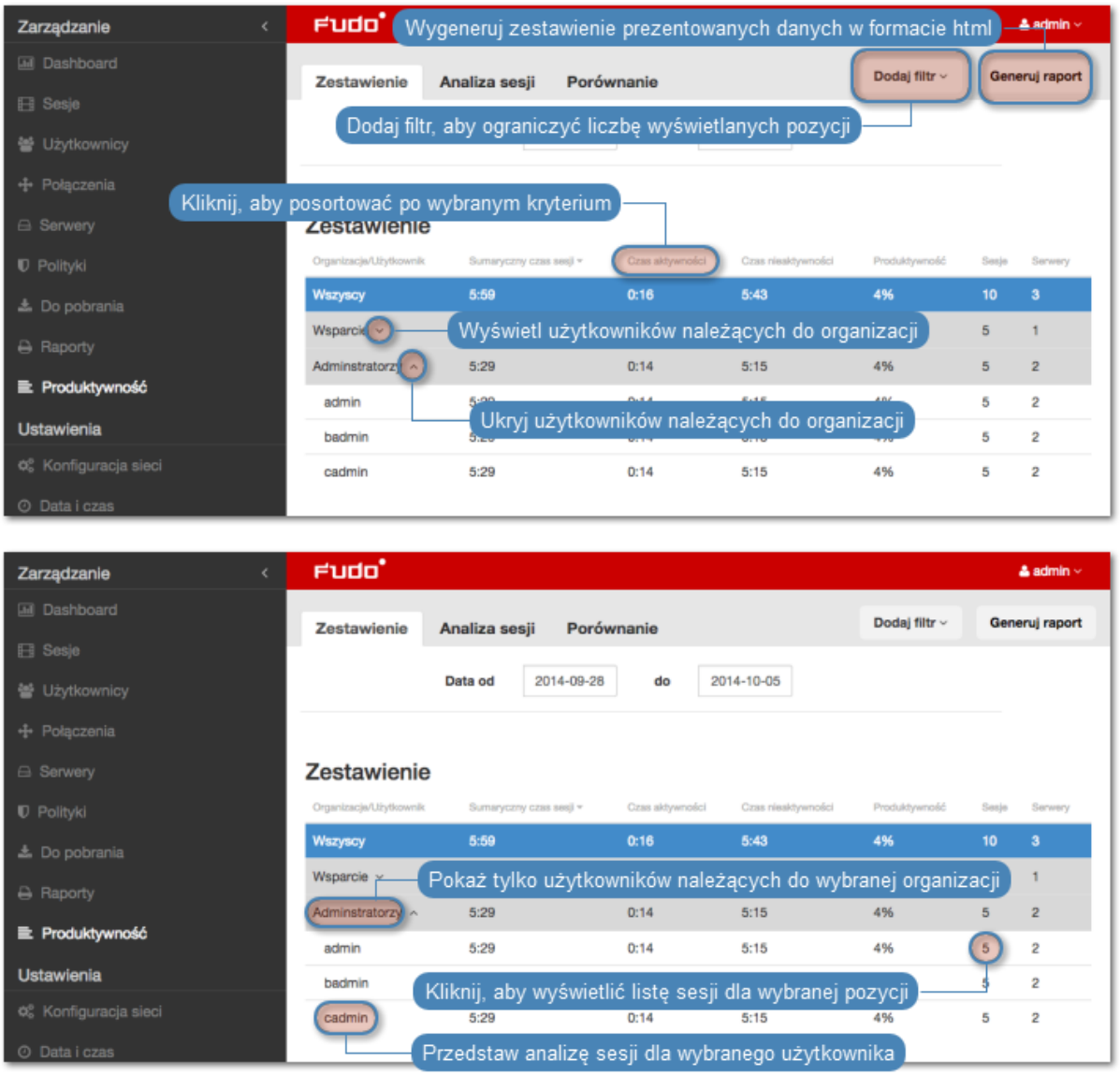
Zestawienie przedstawia dane o aktywności użytkowników i organizacji w wybranym przedziale czasu.

Informacja: Wskaźnik aktywności określany jest na podstawie interakcji użytkownika z systemem. Wheel Fudo PAM dzieli czas sesji na 60 sekundowe interwały. Brak akcji ze strony użytkownika przez czas trwania interwału powoduje zaliczenie danego przedziału do czasu bezczynności.

Aby wyświetlić zestawienie aktywności użytkowników, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Produktywność*.
2. Przejdź na zakładkę *Zestawienie*.
3. Zdefiniuj parametry filtrowania listy użytkowników.
4. Kliknij *Generuj raport*, aby wygenerować zestawienie prezentowanych danych w formacie HTML, CSV lub PDF.

Informacja: Zestawienie dostępne jest w sekcji *Raporty*.



Tematy pokrewne:

- *Analiza produktywności - Analiza sesji*
- *Analiza produktywności - Porównanie*
- *Sesje*

4.2 Analiza sesji

Analiza sesji przedstawia szczegółowo jak kształtowała się produktywność użytkowników/organizacji w zadanym przedziale czasu. Konfigurowalny parametr określający próg aktywności pozwala na szybkie identyfikowanie sesji, użytkowników oraz organizacji, które nie przekroczyły wymaganego poziomu aktywności oraz wspomaga ustalenie wartości progowej, przy której zadana liczba użytkowników lub sesji osiąga wymagany poziom aktywności.

Wykaz wskaźników aktywności użytkowników

Wskaźniki aktywności użytkowników umożliwia szybkie odnalezienie sesji, które nie przekraczają zdefiniowanego progu produktywności. Dalsze zapoznanie się z materiałem pozwala na ustalenie przyczyn niskiej aktywności w danej sesji i wyciągnięcie stosownych wniosków.

Informacja: Wykaz obejmuje przedział czasu nie dłuższy niż 31 dni. W przypadku zdefiniowania dłuższego interwału czasu, prezentowane zestawienie ograniczone jest do 31 dni.

Tematy pokrewne:

- *Analiza produktywności - Zestawienie*
- *Analiza produktywności - Porównanie*
- *Sesje*

4.3 Porównanie aktywności

Komponent analizy produktywności pozwala porównać aktywność organizacji lub użytkowników w zadanych przedziałach czasu.

Aby porównać organizacje/użytkowników, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Produktywność*.
2. Przejdź na zakładkę Porównanie.
3. Wybierz typ porównywanych obiektów.
4. Wybierz porównywany interwał czasu.
5. Dodaj obiekty do porównania, definiując czas początkowy indywidualnie dla każdego obiektu.
6. Kliknij *Zatwierdź*, aby wygenerować porównanie.

Tematy pokrewne:

- *Analiza produktywności - Zestawienie*
- *Analiza produktywności - Zestawienie*
- *Sesje*

ROZDZIAŁ 5

AAPM (Application to Application Password Manager)

5.1 Informacje ogólne

Moduł AAPM umożliwia bezpieczne przesyłanie haseł pomiędzy aplikacjami.

Kluczowym elementem modułu AAPM jest skrypt `fudopv`. Skrypt jest instalowany na serwerze aplikacyjnym i komunikuje się z modułem Secret Manager w celu pobrania haseł dostępu.

W komunikacji z Wheel Fudo PAM, skrypt `fudopv` jest uwierzytelniany na podstawie adresu IP oraz hasła jednorazowego/statycznego.

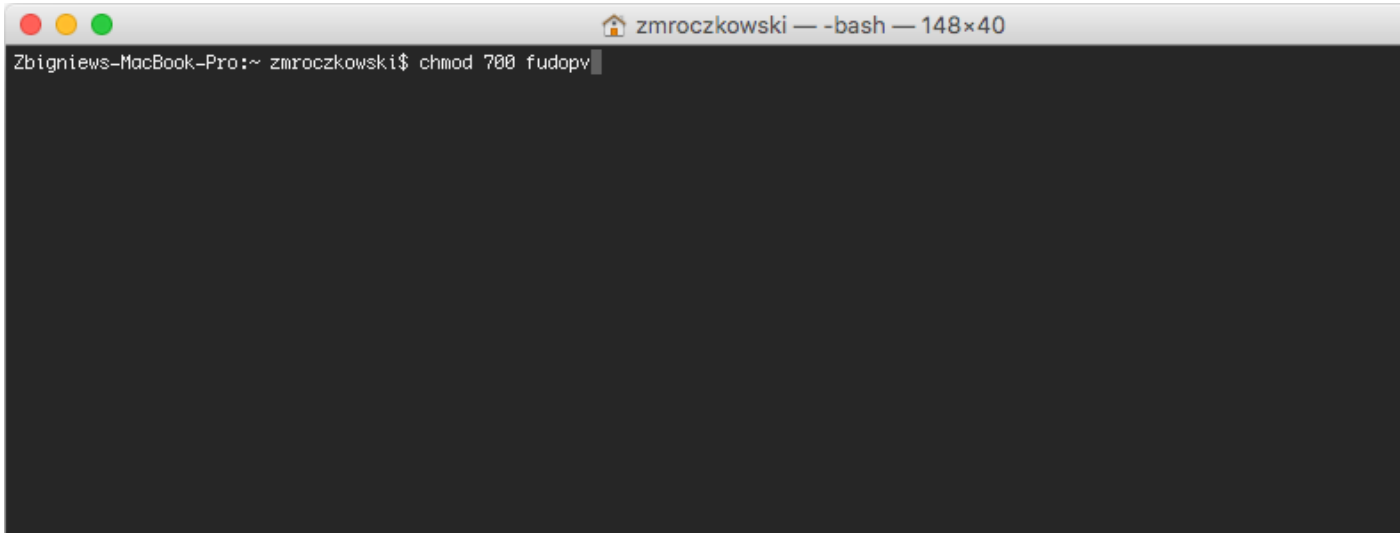
5.2 *fudopv*

Parametry wywołania

`fudopv [<opcje>] <komenda> [<parametry>]`

Komenda/opcja/parametr	Opis
Komendy	
`getcert`	Pobierz certyfikat SSL Wheel Fudo PAM.
`getpass` <typ> <konto>	Pobierz hasło do wybranego konta. typ: • `direct` - połączenie bezpośrednie, niemonitorowane; • `fudo` - połączenie monitorowane przez moduł PSM
Opcje	
`-c <ścieżka>`	Użyj pliku konfiguracyjnego znajdującego się we wskazanej lokalizacji.
`--cfg <ścieżka>`	
`-h, --help`	Wyświetl listę opcji i parametrów wywołania skryptu.

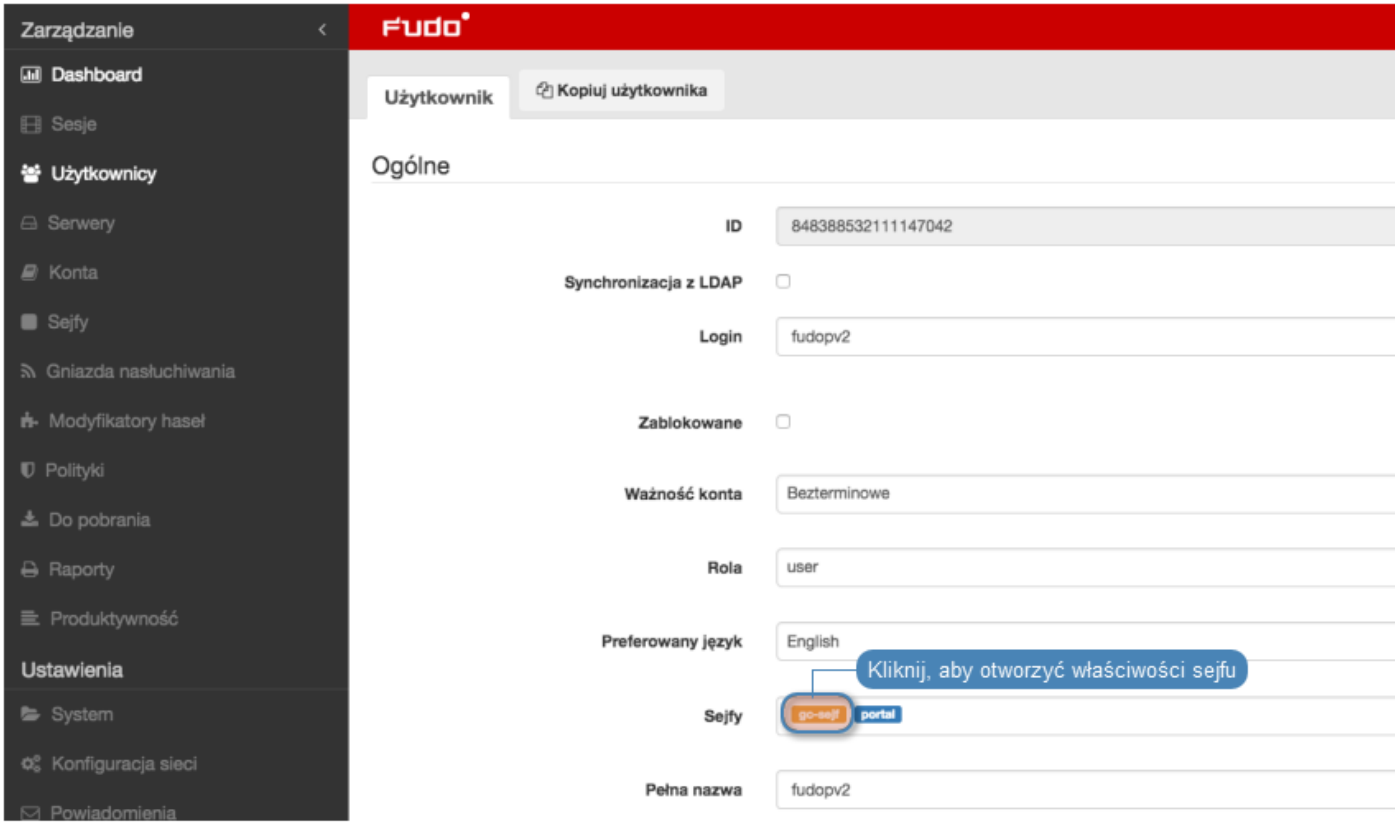
1. Umieść na serwerze skrypt `fudopv` i nadaj mu prawa wykonywalności.



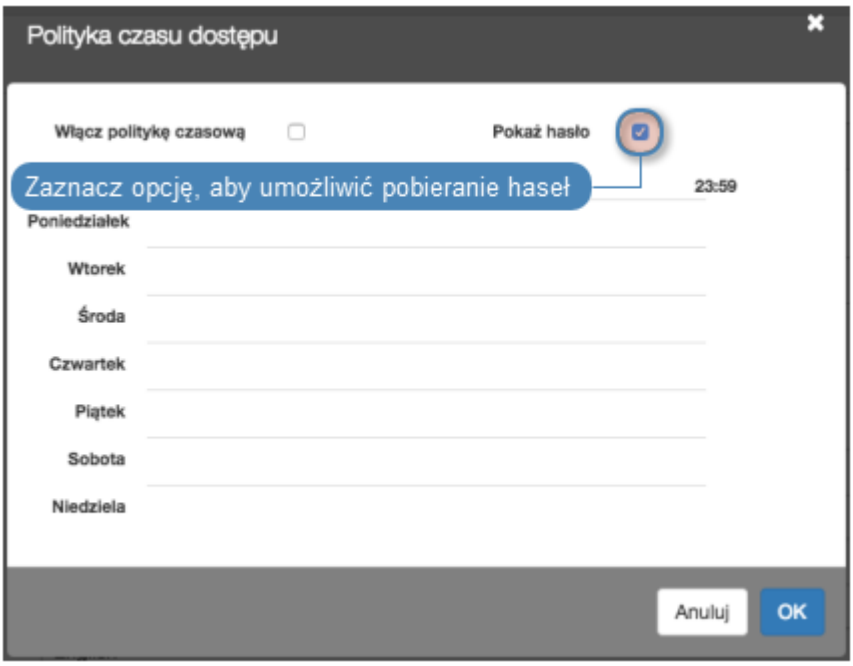
2. Zaloguj się do panelu administracyjnego Wheel Fudo PAM.
3. Stwórz konto użytkownika o roli `user`, uwierzytelnianego hasłem statycznym lub jednorazowym i dodanym adresem IP serwera w sekcji *API*.

Informacja:

- Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
- Kliknij *+Dodaj*.
- Wprowadź nazwę użytkownika.
- Określ termin ważności konta.
- Z listy rozwijalnej *Rola*, wybierz `user`.
- Przypisz użytkownikowi sejf i kliknij obiekt, aby wywołać jego właściwości.

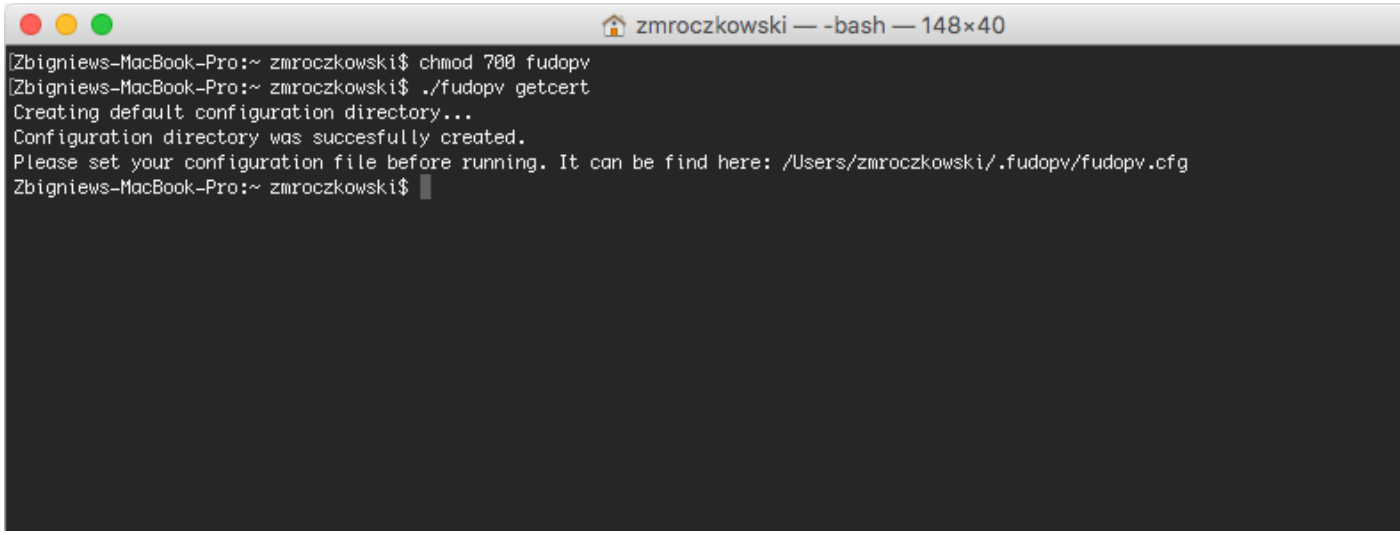


- Zaznacz opcję *Pokaż hasło*.



- W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Typ*, wybierz `Hasło` lub `Hasło jednorazowe`.
- Dla uwierzytelnienia hasłem, wprowadź hasło w polach *Hasło* i *Powtórz hasło*.
- W sekcji *API*, kliknij ikonę + i wpisz adres IP serwera, na którym uruchamiany będzie skrypt `fudopv`.
- Kliknij *Zapisz*.

4. Wykonaj komendę `fudopv getcert`, aby zainicjować konfigurację narzędzia.



5. Otwórz plik `fudopv.cfg`, aby skonfigurować skrypt pobierania haseł.

Sekcja	Opis
`[FUDO]`	
`address`	Adres IP Wheel Fudo PAM.
`cert_path`	Ścieżka pliku z certyfikatem SSL Wheel Fudo PAM.

`[CONN]`	
`bind_ip`	Adres IP serwera, na którym uruchamiany jest skrypt `fudopv`. Adres IP musi być taki sam jak podany w sekcji *API* w konfiguracji użytkownika.

`[AUTH]`	
`username`	Nazwa obiektu użytkownika zdefiniowanego w kroku 3.
`otp`	Ścieżka pliku z hasłem jednorazowym, w przypadku gdy użytkownik jest uwierzytelniany hasłem jednorazowym.
`secret`	Lokalizacja pliku z hasłem statycznym, w przypadku uwirzytelnienia hasłem.

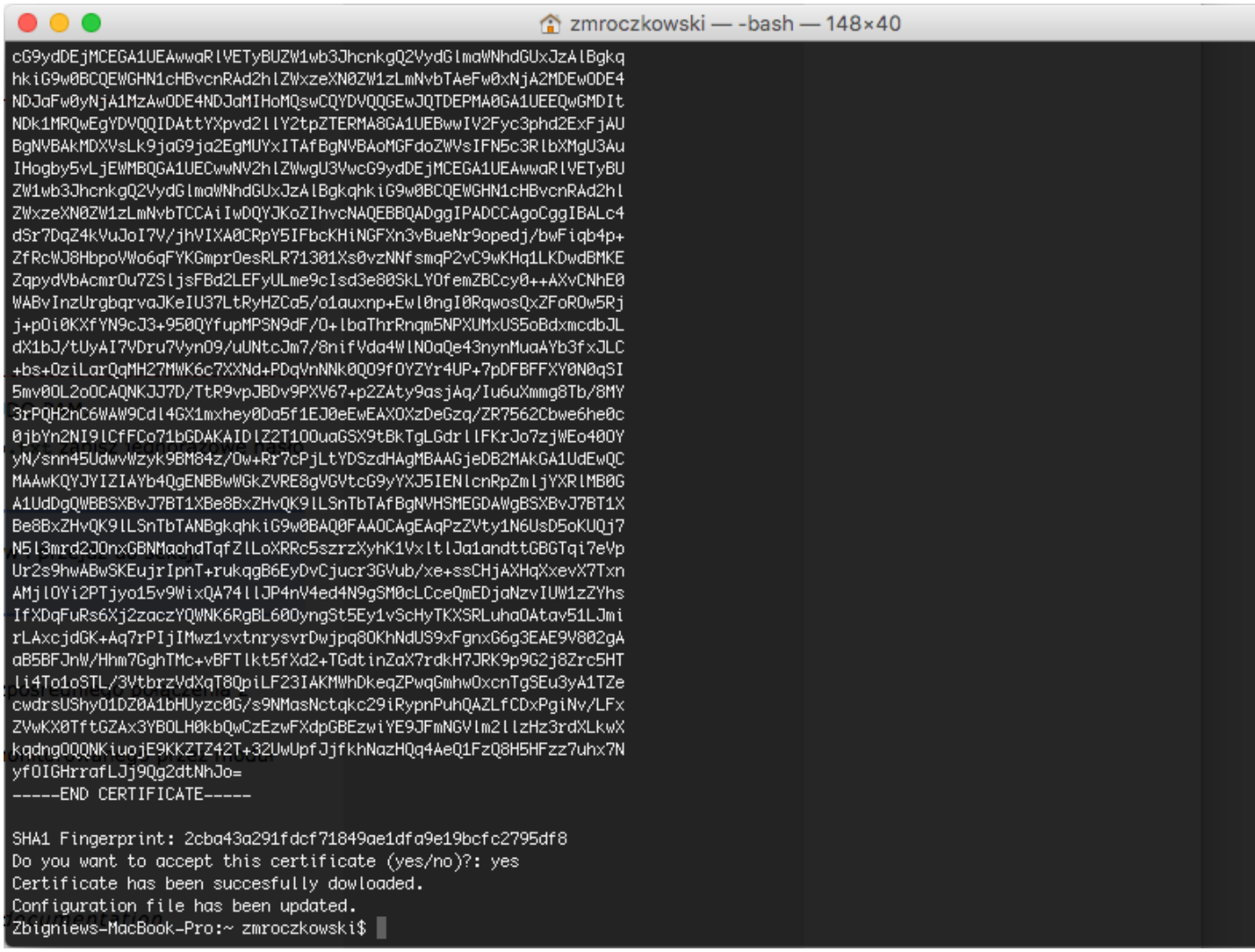
Informacja:

- W sekcji `[FUDO]`, w linii `address`, wprowadź adres IP Wheel Fudo PAM.
- Linię `cert_path` pozostaw bez zmian, zostanie ona uzupełniona automatycznie przy okazji poprawnego wykonania komendy `fudopv getcert`.
- W sekcji `[CONN]`, odkomentuj linię `bind_ip` i wprowadź adres IP serwera, na którym wykonywany jest skrypt `fudopv`.
- W sekcji `[AUTH]`, w linii `username`, uzupełnij nazwę konta obiektu użytkownik, stworzonego w kroku 3.
- W zależności od wybranego sposobu uwierzytelnienia, zakomentuj linię odpowiadającą wybranej metodzie.

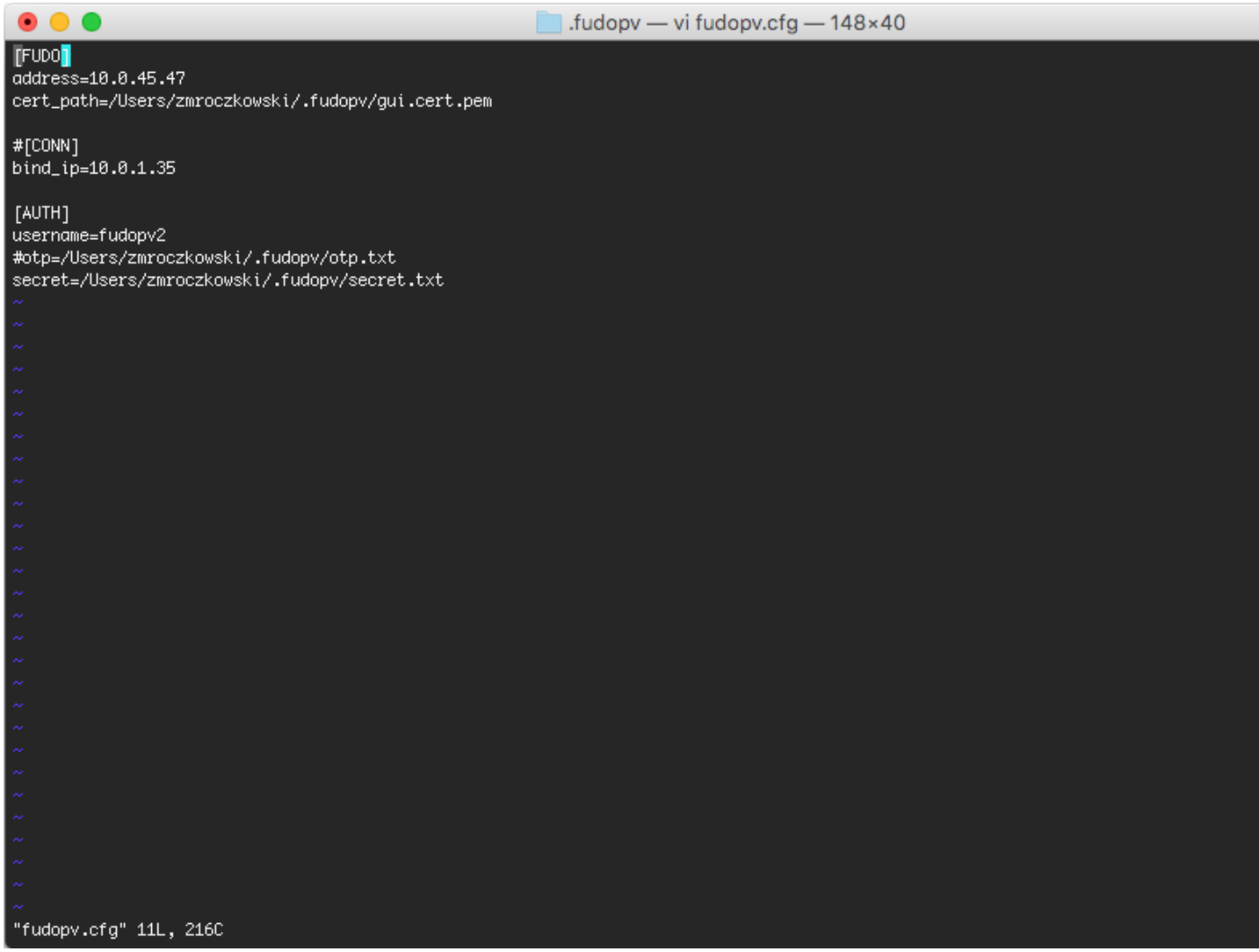
Na przykład:

```
[FUDO]
address=10.0.0.8.61
cert_path=<CERT_PATH>

#[CONN]
bind_ip=10.0.0.8.11

[AUTH]
username=fudopv
#otp=/Users/zmroczkowski/.fudopv/otp.txt
secret=/Users/zmroczkowski/.fudopv/secret.txt
```

6. Wykonaj komendę `fudopv getcert`, aby pobrać certyfikat Wheel Fudo PAM.

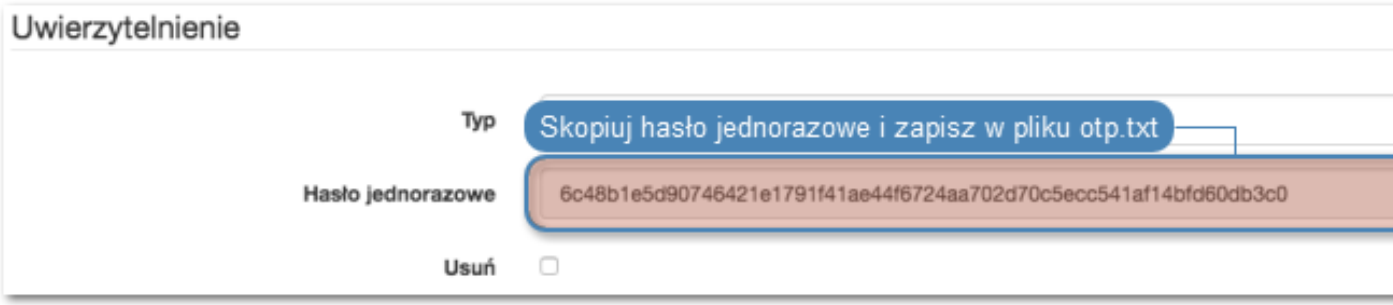


Informacja: Po prawidłowym wykonaniu komendy, ścieżka certyfikatu w pliku konfiguracyjnym zostanie automatycznie uzupełniona.



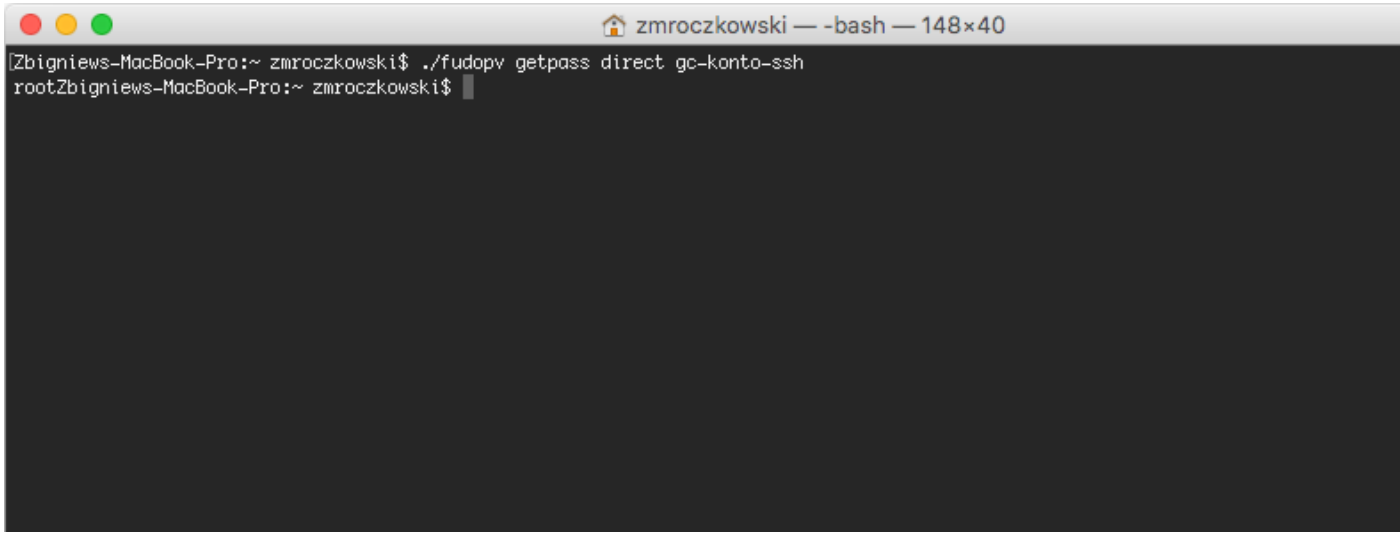
7. W pliku `secret.txt`, zapisz hasło konta użytkownika; lub w pliku `otp.txt` zapisz jednorazowe hasło dostępu.

Informacja: Aby uzyskać hasło jednorazowe, wybierz użytkownika z listy obiektów i przejdź do sekcji *Uwierzytelnienie*.

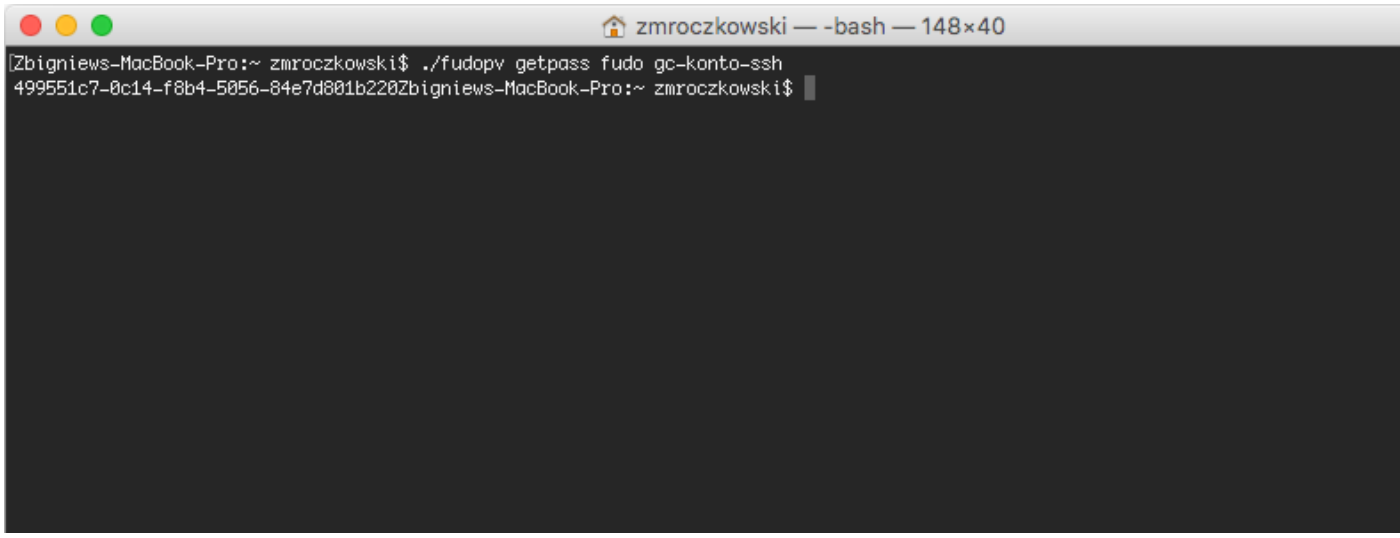


8. Wykonaj komendę:

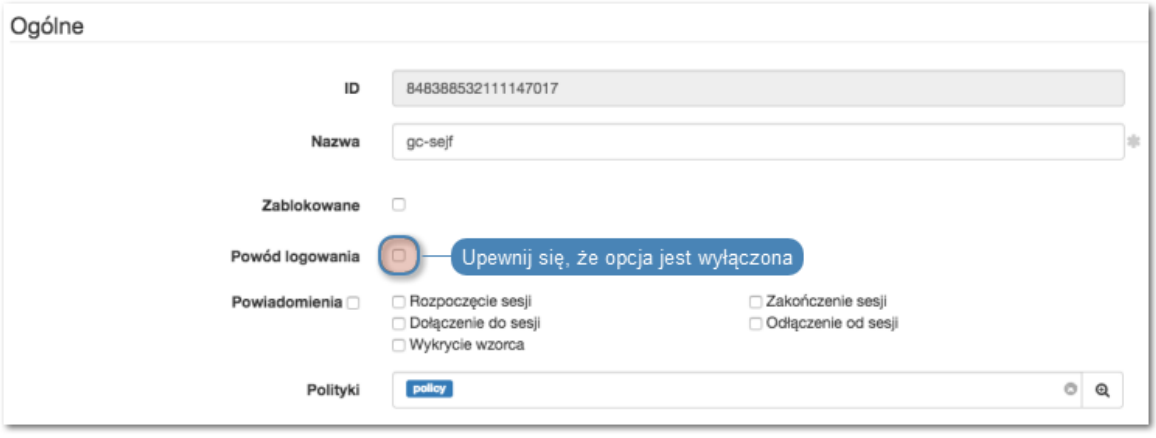
- `fudopv getpass direct <nazwa_konta>`, aby pobrać hasło do nawiązania bezpośredniego połączenia z serwerem.



- `fudopv getpass fudo <nazwa_konta>`, aby pobrać hasło do nawiązania połączenia monitorowanego przez moduł PSM.



Ostrzeżenie: Prawidłowe działanie skryptu `fudopv` wymaga wyłączenia we właściwościach sejfu, opcji wymuszania na użytkowniku podania powodu logowania przy nawiązywaniu połączenia z serwerem docelowym.



5.3 Interfejs API

Interfejs API modułu AAPM jest opisany w dokumencie *Wheel Fudo PAM 3.0 - API documentation.*

Related topics:

- *Model danych*
- *Opis systemu*
- *Konfigurowanie modyfikatora haseł*

ROZDZIAŁ 6

Administracja

Poniższy rozdział zawiera opisy czynności administracyjnych.

6.1 System

6.1.1 Data i czas

Wiele zdarzeń rejestrowanych przez Wheel Fudo PAM (sesje, wpisy dziennika zdarzeń) znakowanych jest czasem. Wheel Fudo PAM może pobierać czas z *serwera NTP* lub z zegara systemowego.

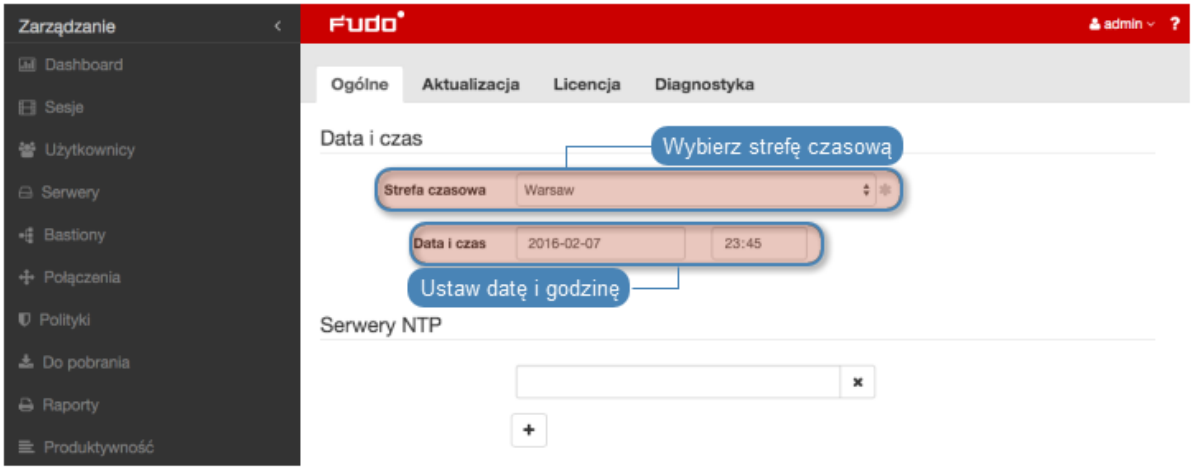
Ostrzeżenie: Zaleca się, aby data i czas pobierane były z serwera NTP, będącego pewnym źródłem danych referencyjnych. Ręczna zmiana ustawień daty i czasu może spowodować nieprawidłowości w funkcjonowaniu urządzenia.

Zmiana daty i czasu

Informacja: Opcja ręcznego ustawienia czasu nie jest dostępna, jeśli skonfigurowany jest serwer NTP.

Aby zmienić datę i czas serwera Wheel Fudo PAM, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Zmień ustawienia daty i czasu w sekcji *Data i czas*.



3. Kliknij *Zapisz*.

Informacja: Zmiana czasu i daty nie zostanie zastosowana jeśli zdefiniowany jest serwer NTP.

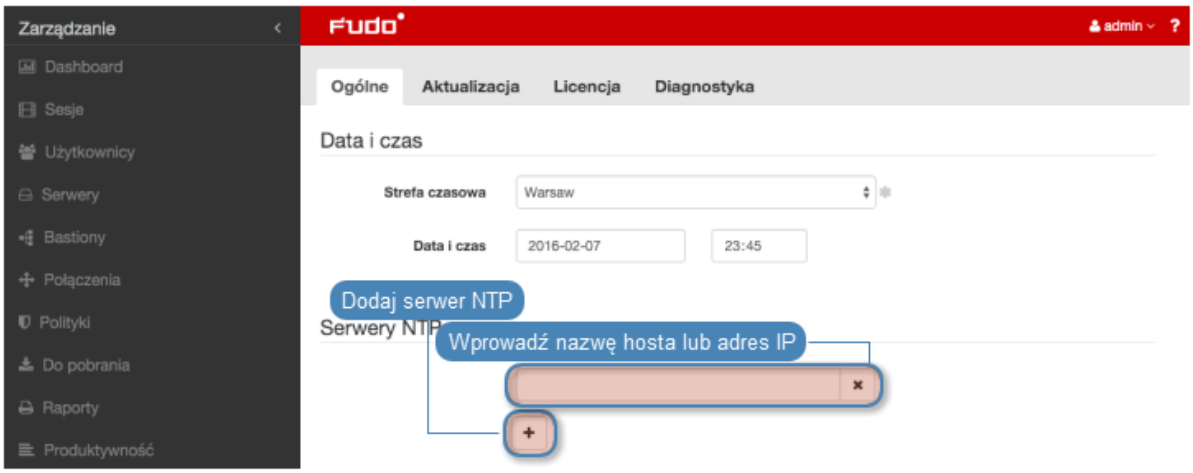
Konfiguracja serwerów czasu

Informacja: Serwer NTP pozwala na synchronizację czasu systemowego na urządzeniach będących częścią zakładowej infrastruktury IT. Zastosowanie serwera NTP zapewnia zgodność czasu rejestrowanej sesji, z czasem monitorowanego serwera.

Dodawanie serwera NTP

Aby dodać serwer NTP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Kliknij + w sekcji *Serwery NTP*, aby dodać definicję serwera czasu.
3. Wprowadź adres IP lub nazwę hosta serwera NTP.

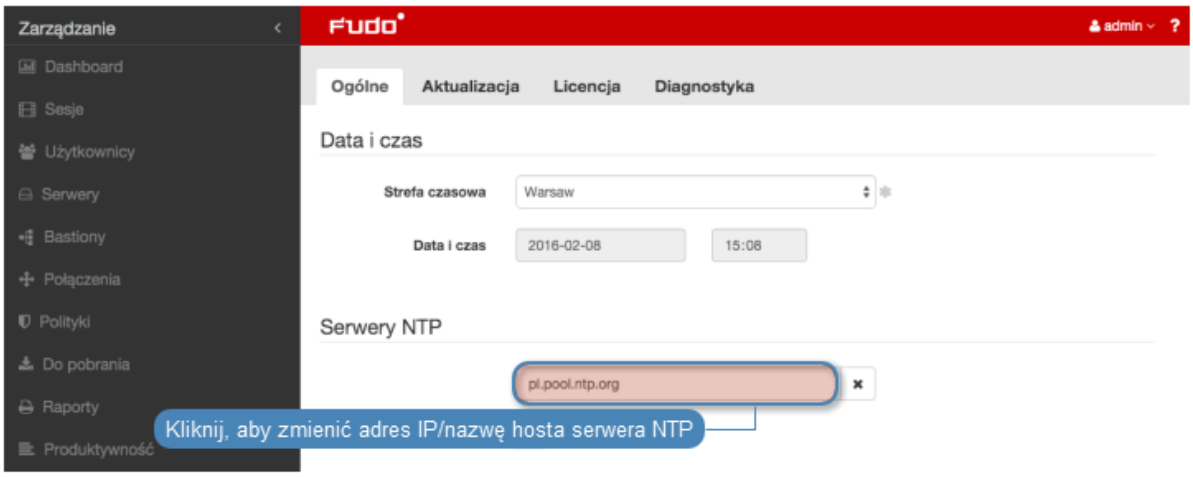


4. Kliknij *Zapisz*.

Modyfikowanie serwera NTP

Aby zmodyfikować serwer NTP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wyszukaj i zmodyfikuj żądany wpis w sekcji *Serwery NTP*.

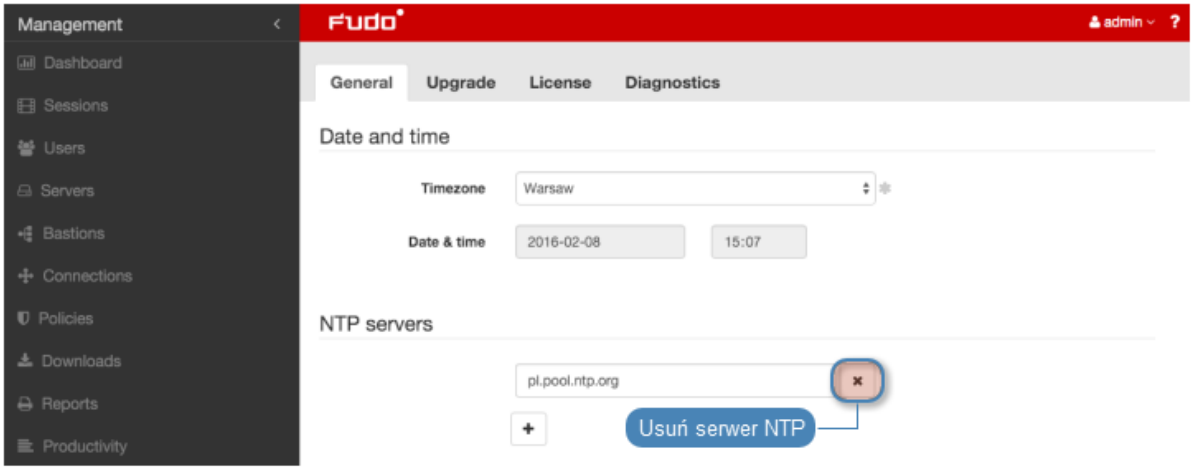


3. Kliknij *Zapisz*.

Usuwanie serwera NTP

Aby usunąć serwer NTP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. Zaznacz opcję *x* przy żądanej definicji serwera NTP i kliknij *Zapisz*.



Tematy pokrewne:

- *Znakowanie czasem*

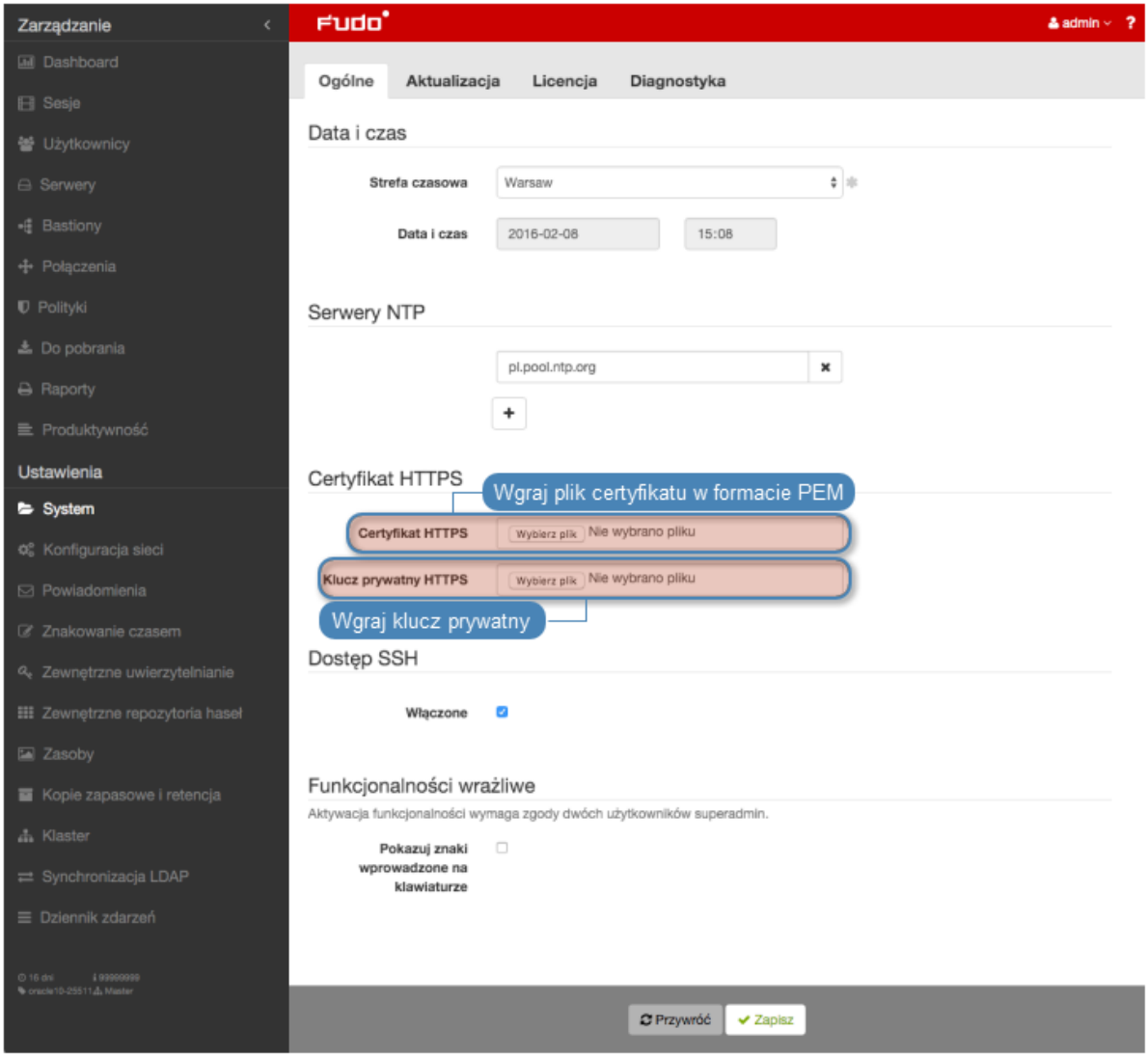
6.1.2 Certyfikat HTTPS

Certyfikat HTTPS pozwala administratorowi upewnić się, że nawiązał połączenie z panelem administracyjnym Wheel Fudo PAM a nie ze stroną próbującą podszyć pod panel administracyjny celem pozyskania danych logowania konta administratora.

Konfigurowanie certyfikatu SSL

Aby skonfigurować certyfikat SSL, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Kliknij przycisk *Wybierz plik* w polu *Certyfikat HTTPS* i wskaż w systemie plików definicję certyfikatu SSL w formacie PEM.
3. Kliknij przycisk *Przeglądaj* w polu *Klucz prywatny HTTPS* i wskaż w systemie plików definicję klucza prywatnego SSL.



4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Bezpieczeństwo*
- *Zarządzanie serwerami*

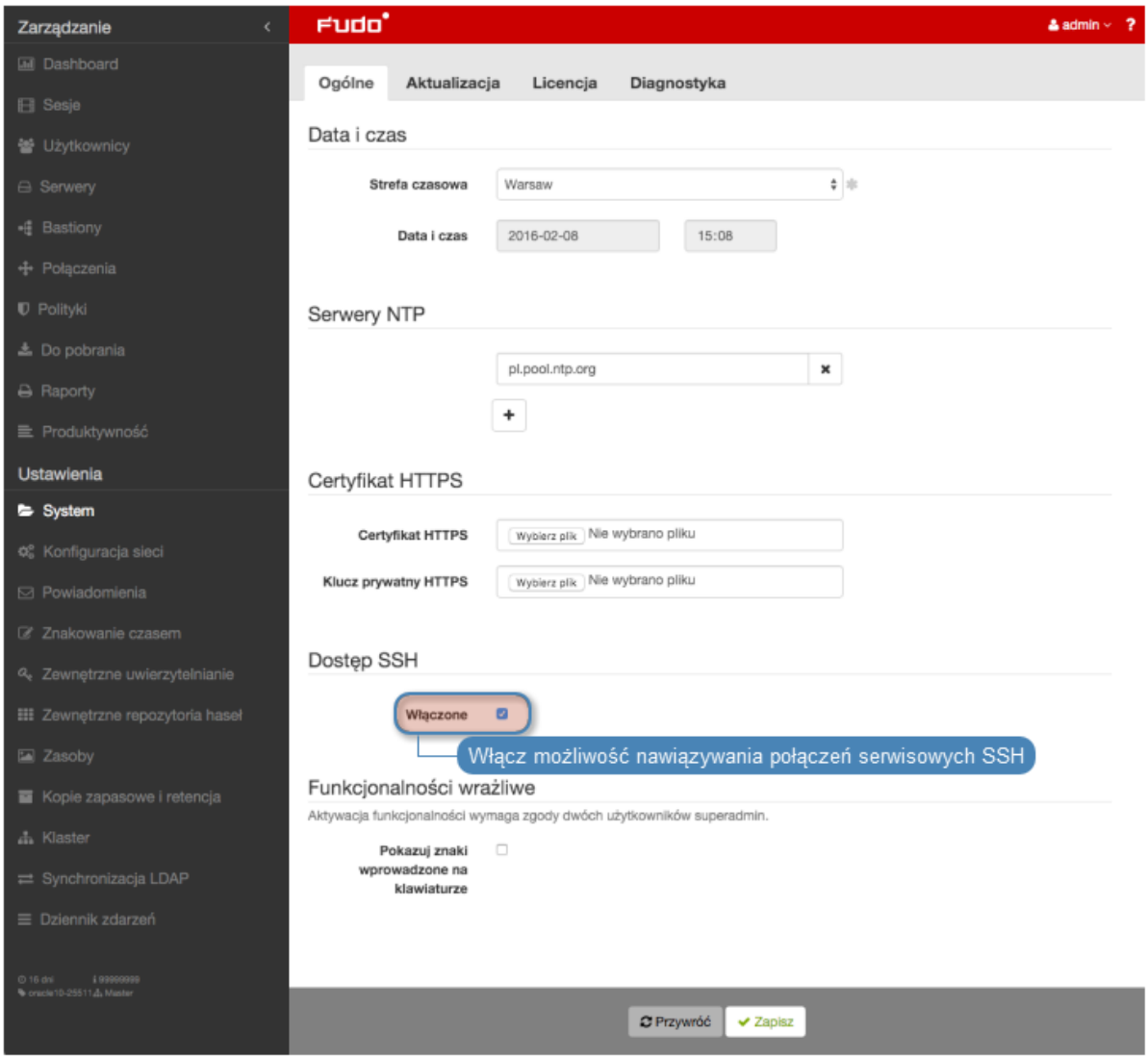
6.1.3 Dostęp SSH

Opcja umożliwia zdalny dostęp serwisowy do Wheel Fudo PAM za pośrednictwem protokołu SSH.

Włączanie dostępu SSH

Aby włączyć zdalny dostęp serwisowy, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. W sekcji *Dostęp SSH* zaznacz opcję *Zezwalaj na dostęp SSH*.



3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

6.1.4 Funkcjonalności wrażliwe

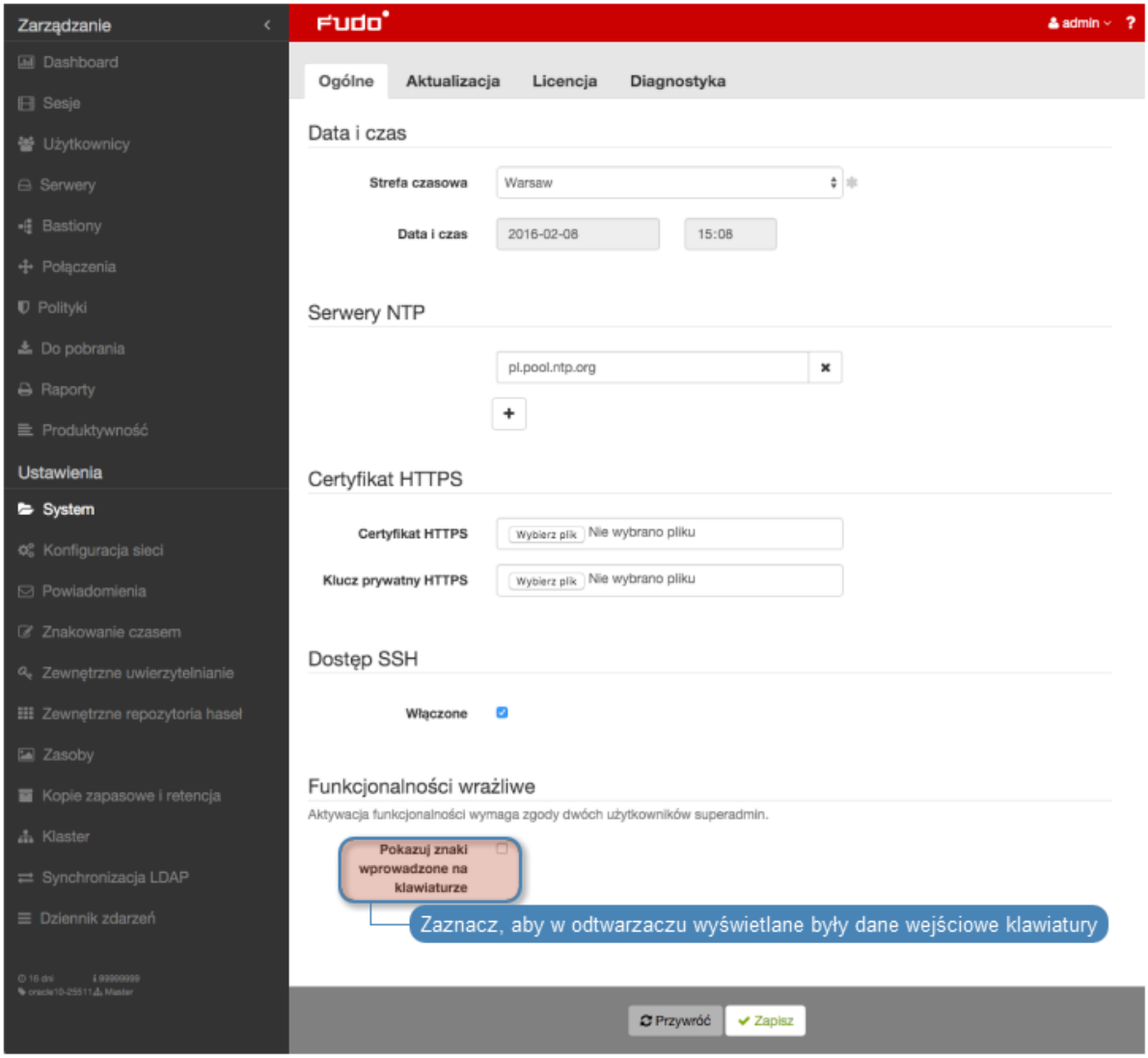
Funkcjonalności wrażliwe to zestaw opcji, których włączenie wymaga decyzji dwóch użytkowników o roli `superadmin`.

Włączanie pokazywania wejścia klawiatury

Informacja: Znaki wprowadzone na klawiaturze są domyślnie niepokazywane w odtwarzaczu. Włączenie podglądu znaków klawiatury wymaga zgody dwóch użytkowników `superadmin`.

Aby włączyć pokazywanie znaków wprowadzonych przez użytkownika na klawiaturze, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. Zaznacz opcję *Pokazuj znaki wprowadzone na klawiaturze* w sekcji *Funkcjonalności wrażliwe*, aby zainicjować włączenie funkcji.
3. Kliknij Zapisz.



4. Powiadom innego użytkownika `superadmin` o zainicjowaniu funkcjonalności, która wymaga potwierdzenia.

Tematy pokrewne:

- *Odtwarzanie sesji*

6.1.5 Aktualizacja systemu

Wheel Fudo PAM oprócz bieżącej wersji systemu, przechowuje jego poprzednią wersję, pozwalając na jej przywrócenie.

Informacja: Proces aktualizacji systemu nie dokonuje zmian w konfiguracji urządzenia ani nie narusza integralności zarejestrowanych sesji.

6.1.5.1 Aktualizowanie systemu

Ostrzeżenie:

- Przed wykonaniem skryptów aktualizacyjnych, zaleca się dokonanie sprawdzenia wykonalności aktualizacji.
- W procesie aktualizacji, trwające połączenia użytkowników zostaną zerwane.
- Skorzystaj z opcji *Blokowanie nowych połączeń*, w sekcji *Sesja* ustawień systemowych, aby zablokować możliwość nawiązywania nowych połączeń i ograniczyć liczbę aktywnych użytkowników przed ponownym uruchomieniem systemu.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Aktualizacja*.
3. Kliknij *Wgraj*.
4. Wskaż plik zawierający aktualizację systemu (`.upg`).
5. Kliknij *Aktualizacja* przy wybranym pliku obrazu.

Ostrzeżenie: Po aktualizacji systemu, Wheel Fudo PAM zostanie uruchomione ponownie.

Ponowne uruchomienie wymaga obecności klucza szyfrującego. Włóż nośnik z kluczem szyfrującym do portu USB.

Informacja: W przypadku gdy uruchomienie systemu w nowej wersji nie powiedzie się, Wheel Fudo PAM wykryje problem i uruchomi system w poprzedniej wersji.

6.1.5.2 Weryfikacja wykonalności aktualizacji

Przed przystąpieniem do aktualizacji systemu, zaleca się zweryfikowanie czy bieżący stan konfiguracji pozwala na prawidłowe wykonanie skryptów aktualizacyjnych. Proces weryfikacyjny umożliwia też określenie przybliżonego czasu trwania aktualizacji.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Aktualizacja*.
3. Kliknij *Wgraj*.
4. Wskaż plik zawierający aktualizację systemu (`.upg`).
5. Kliknij przycisk *Próbna aktualizacja*.

Informacja:

- Kliknij *Anuluj sprawdzanie*, aby przerwać działanie skryptów próbnej aktualizacji.
- Kliknij *Pobierz log*, aby pobrać plik z zapisem przebiegu aktualizacji próbnej i czasem wykonania skryptów aktualizacyjnych.

6.1.5.3 Usuwanie migawki aktualizacji

Usunięcie migawki aktualizacji ma na celu zwolnienie przestrzeni dyskowej zajętej przez poprzednią wersję systemu.

Ostrzeżenie: Usunięcie migawki aktualizacji uniemożliwi przywrócenie poprzedniej wersji systemu.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Aktualizacja*.
3. Kliknij *Usuń migawkę aktualizacji*.
4. Potwierdź usunięcie migawki.

Tematy pokrewne:

- *Przywracanie poprzedniej wersji systemu*
- *Ponowne uruchomienie systemu*

6.1.6 Licencja

Wgrywanie licencji

Aby wgrać nowy plik licencji, postępuj zgodnie z poniższą instrukcją.

Informacja: Nowa licencja zastąpi istniejącą.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Przejdź na zakładkę *Licencja*.
3. Kliknij *Wgraj*.

4. Wskaż plik licencji i kliknij *OK*, aby zainicjować system nową definicją.

Tematy pokrewne:

- *Opis systemu*
- *Wymagania*

6.1.7 Diagnostyka

Moduł diagnostyczny pozwala na wykonanie podstawowych komend systemowych, tj. ping, netcat czy traceroute.

Aby uruchomić program narzędziowy, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Przejdź na zakładkę Diagnostyka.
3. Znajdź żądaną komendę, wprowadź parametry wykonania i kliknij przycisk wykonania komendy.

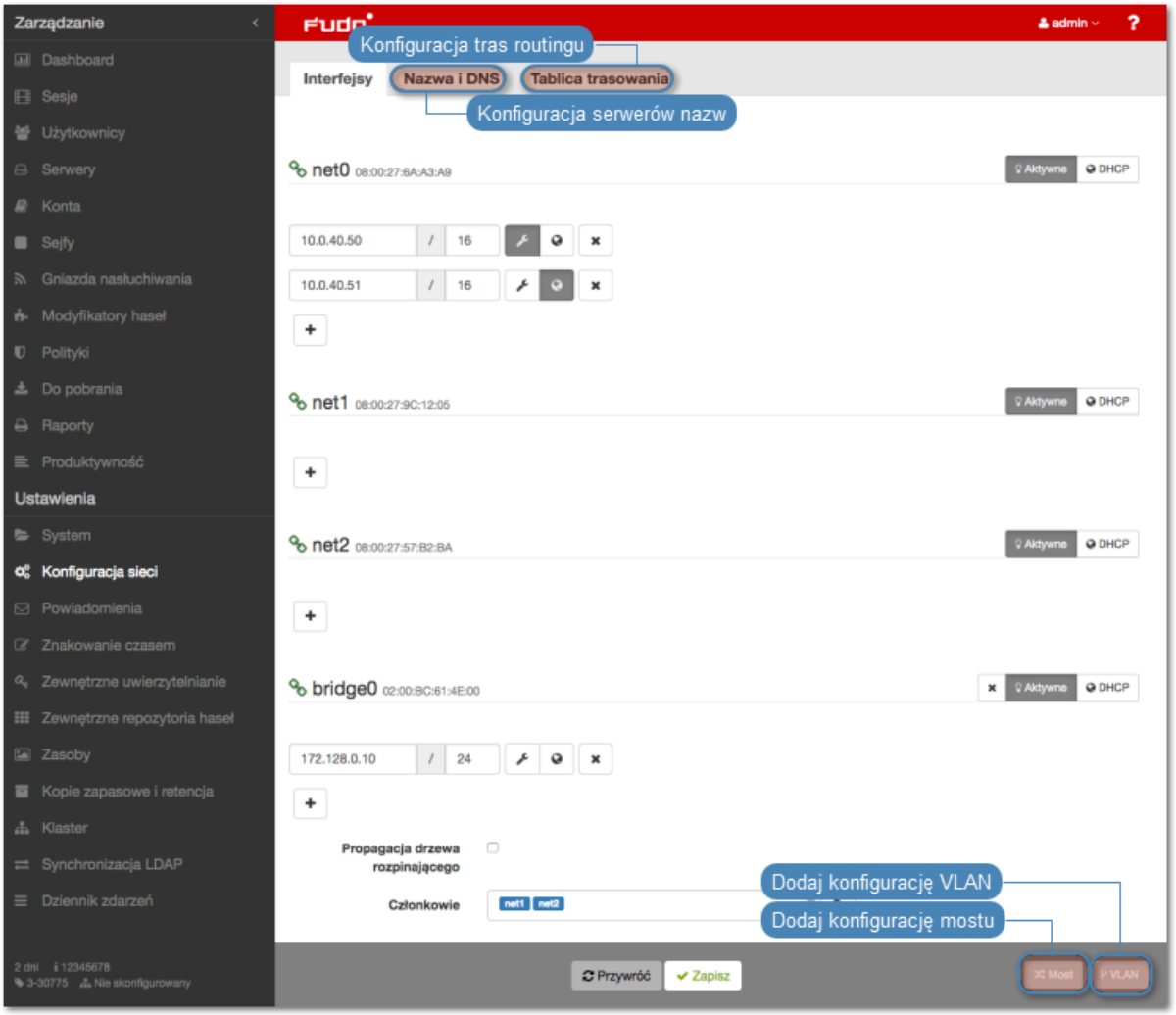
Komenda/ parametr	Opis
Ping	Ping wysyła sekwencję 10 pakietów icmp do wskazanego hosta.
Wyświetlaj adresy w formie numerycznej	Nie rozwiązuje adresu IP hosta do nazwy mnemonicznej.
Zapisz trasę	Umożliwia śledzenie trasy pakietów.
netcat	Netcat służy do nawiązywania połączeń ze zdalnym hostem na określonym numerze portu.
host	Polecenie host służy sprawdzeniu czy serwer DNS prawidłowo rozwiązuje nazwę maszyny docelowej.
traceroute	Komenda służy ustaleniu trasy, którą pokonują pakiety pomiędzy Wheel Fudo PAM i hostem docelowym.
Nie rozwiązuj nazw skoków	Adresy kolejnych punktów przeskoku nie będą rozwiązywane do nazw mnemonicznych.
Uzyj protokołu ICMP zamiast UDP	Wymusza użycie pakietów UDP zamiast ICMP.
Tryb omijania firewall-a	Wymusza użycia niezmiennych numerów portu dla pakietów UDP i TCP. Port docelowy nie jest inkrementowany z każdym wysłanym pakietem.
Ustaw flagę „Nie fragmentuj”	Nie pozwala na fragmentację pakietów, w przypadku gdy przesyłany pakiet przekracza zdefiniowaną dla sieci wartość MTU (Maximum Transmission Unit). W przypadku przekroczenia MTU, zwrócony zostanie błąd.

Tematy pokrewne:

- *Rozwiązywanie problemów*

6.2 Konfiguracja sieci

Aby przejść do widoku zarządzania ustawieniami sieci, wybierz z lewego menu opcję *Ustawienia > Konfiguracja sieci*.



6.2.1 Konfiguracja ustawień sieciowych

W specyfikacji domyślnej, Wheel Fudo PAM wyposażone jest w dwa fizyczne interfejsy LAN, a opcje ustawień sieciowych umożliwiają:

- dodawanie aliasów IP interfejsów fizycznych, wykorzystywanych do konfigurowania zdalnych serwerów,
- konfigurowanie parametrów sieciowych wymaganych do komunikacji klastrowej,
- konfigurowanie adresacji IP do pracy w sieciach wirtualnych (VLAN),
- mostkowanie interfejsów fizycznych oraz sieci VLAN.

6.2.1.1 Zarządzanie interfejsami fizycznymi

Definiowanie adresu IP interfejsu

Definiowane adresy IP to aliasy interfejsu fizycznego, które wykorzystywane są w procedurach *konfiguracji serwerów* (pole *Adres lokalny* w sekcji *Pośrednik*).

Informacja: Jeśli lista adresów IP przypisanych do interfejsu sieciowego jest pusta i nie ma możliwości dodania adresu, sprawdź czy dany interfejs nie jest częścią mostu.

Aby dodać adres IP do fizycznego interfejsu sieciowego, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij + przy wybranym interfejsie i wprowadź adres IP oraz maskę podsieci, zapisaną w notacji CIDR.

Informacja: + będzie nieaktywny, jeśli włączona jest opcja pobierania adresu IP z serwera DHCP.

---

3. Zaznacz opcje dodatkowe dla definiowanego adresu IP.

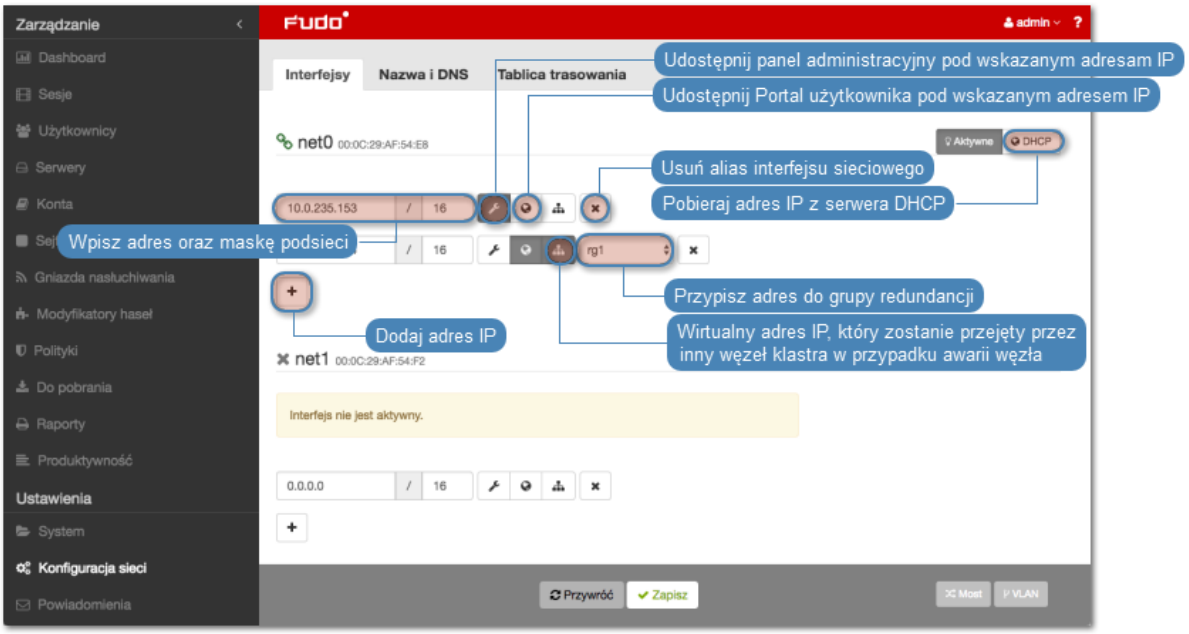
	Udostępnij panel administracyjny Wheel Fudo PAM pod wskazanym adresem IP. Adres zarządzający używany jest również do replikacji danych pomiędzy węzłami klastra.
	Wirtualny adres IP, który zostanie automatycznie przejęty przez drugi węzeł klastra w przypadku awarii węzła głównego.
	Udostępnij *Portal użytkownika* pod wskazanym adresem IP.

4. Określ grupę redundancji, do której zostanie przypisany adres IP (*dotyczy adresów klastrowych*).

Informacja: Grupy redundancji definiowane są w widoku *Klaster*, w zakładce *Grupy redundancji*.

---

5. Kliknij *Zapisz*.



Informacja: Każdy interfejs sieciowy opatrzony jest ikoną statusu.

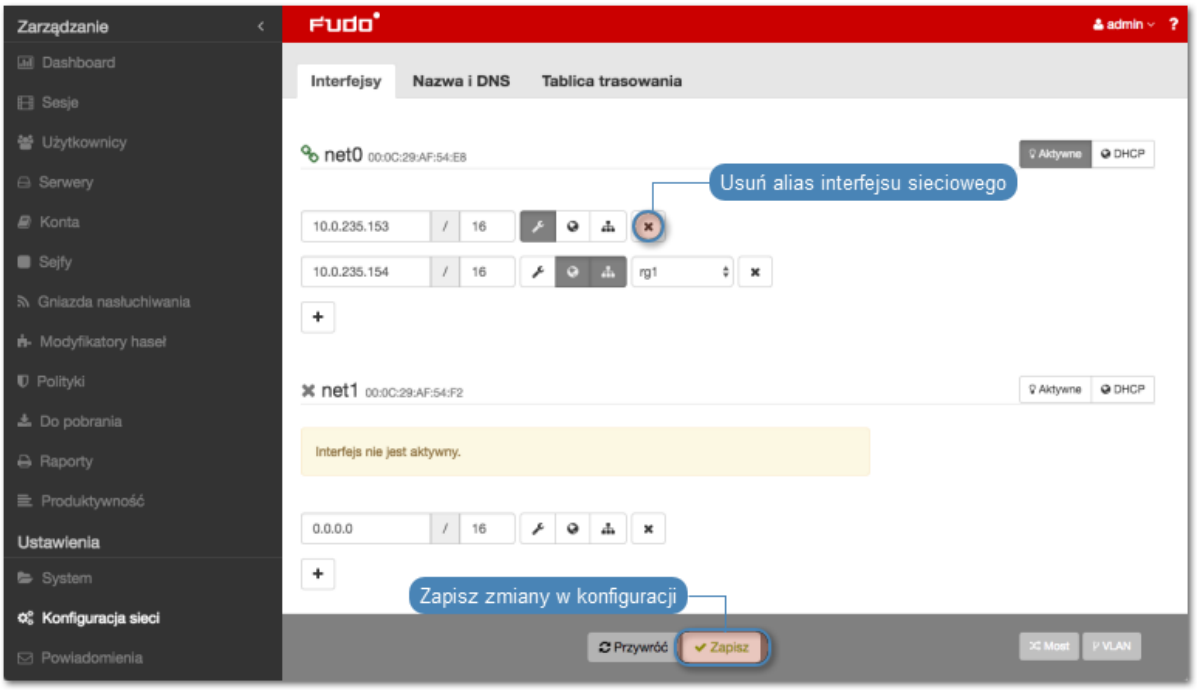
	Interfejs aktywny i podłączony.
	Interfejs aktywny ale odłączony.
	Interfejs wyłączony.

Usuwanie przypisanych adresów IP interfejsu

Ostrzeżenie: Usunięcie adresu IP uniemożliwi nawiązywanie połączeń z serwerami, które w polu *Adres lokalny* w sekcji *Pośrednik*, miały ustawiony usuwany adres IP.

Aby usunąć adres IP przypisany do fizycznego interfejsu sieciowego, postępuj zgodnie z poniższą instrukcją.

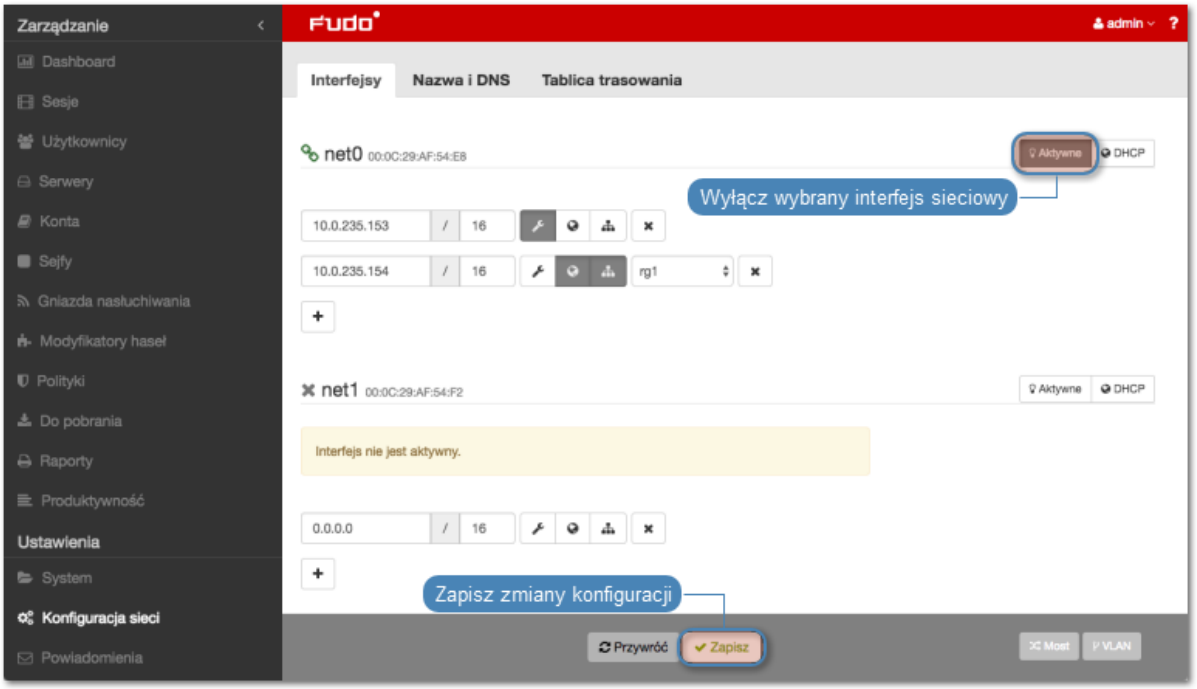
1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Zaznacz opcję usunięcia wybranego interfejsu.
3. Kliknij *Zapisz*.



Wyłączanie interfejsu sieciowego

Aby wyłączyć adres IP przypisany do fizycznego interfejsu sieciowego, postępuj zgodnie z poniższą instrukcją.

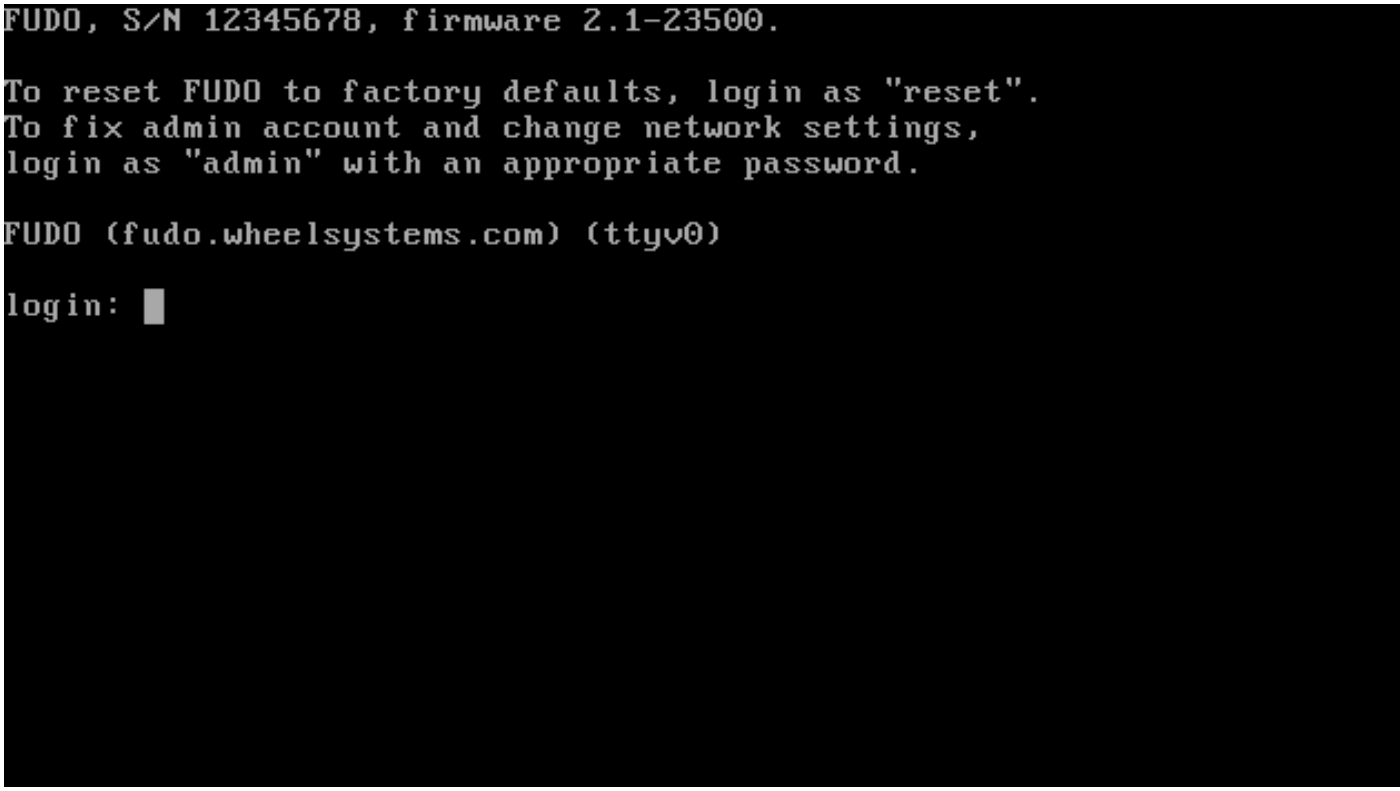
1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij *Aktywne*, aby wyłączyć wybrany interfejs.
3. Kliknij Zapisz.



6.2.1.2 Ustawianie adresu IP z konsoli

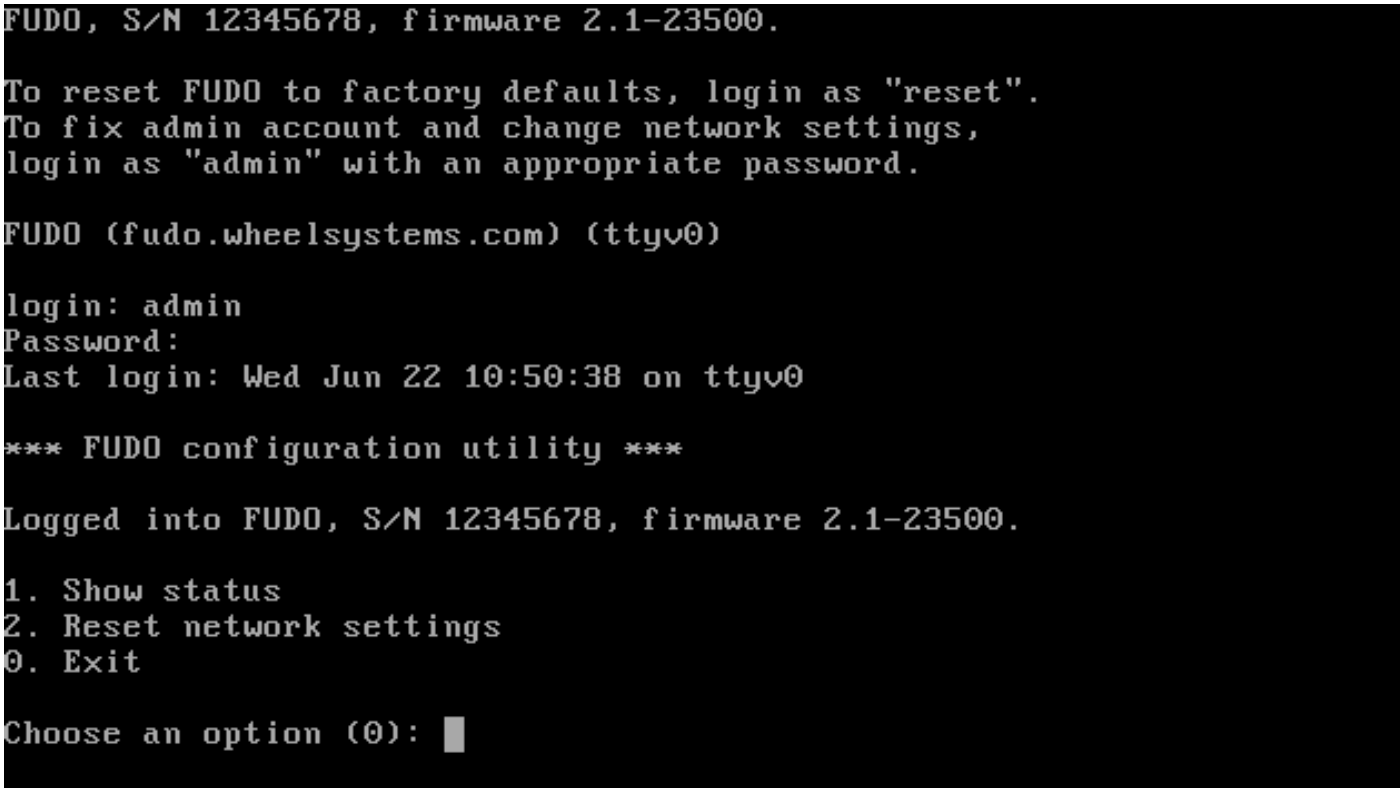
W sytuacji braku możliwości zalogowania się do zdalnego panelu administracyjnego, adres IP może zostać skonfigurowany z poziomu konsoli urządzenia.

1. Wprowadź login konta administratora.



2. Wprowadź hasło do konta administratora.

3. Wpisz 2 i naciśnij klawisz *Enter*.



4. Wpisz y i naciśnij klawisz *Enter*, aby potwierdź chęć zmiany ustawień sieciowych.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n):
```

5. Wprowadź nazwę interfejsu zarządzającego (poprzez interfejs zarządzający udostępniany jest panel administracyjny Wheel Fudo PAM) i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:50:38 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0):
```

6. Wprowadź adres IP urządzenia wraz z maską podsieci oddzieloną znakiem `/` (np. `10.0.0.8/24`) i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
```

7. Wprowadź bramę sieci i naciśnij klawisz *Enter*.

```
FUDO, S/N 12345678, firmware 2.1-23500.

To reset FUDO to factory defaults, login as "reset".
To fix admin account and change network settings,
login as "admin" with an appropriate password.

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Wed Jun 22 10:56:52 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 12345678, firmware 2.1-23500.

1. Show status
2. Reset network settings
0. Exit

Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
Enter new default gateway IP address (10.0.0.1):
```

6.2.1.3 Konfigurowanie mostu sieciowego

Scenariusz wdrożeniowy *trybu pracy mostu*, wymaga wskazania interfejsów sieciowych przez które przekazywany będzie ruch pomiędzy administratorem i serwerem.

Aby stworzyć most sieciowy, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij Most.
3. Skonfiguruj przypisanie interfejsów fizycznych lub sieci VLAN do konfigurowanego mostu.

Informacja: Konfiguracja mostu wymaga usunięcia wszystkich adresów IP przypisanych bezpośrednio do interfejsów sieciowych będących członkami mostu.

---

4. Wprowadź adres IP oraz maskę podsieci, zapisaną w notacji CIDR, dla wirtualnego interfejsu definiowanego mostu.
5. Zaznacz opcję Propagacja drzewa rozpinającego, aby włączyć mechanizm wykrywania i zapobiegania zapętleń w sieci (STP - Spanning Tree Protocol).
6. Zaznacz opcję *Zarządzanie*, jeśli panel zarządzania ma być dostępny pod wybranym adresem IP, i kliknij *Aktywne*.
7. Kliknij *Zapisz*.

6.2.1.4 Konfigurowanie sieci wirtualnych (VLAN)

Sieci VLAN pozwalają na segmentację sieci w celu odseparowania domen rozgłoszeniowych.

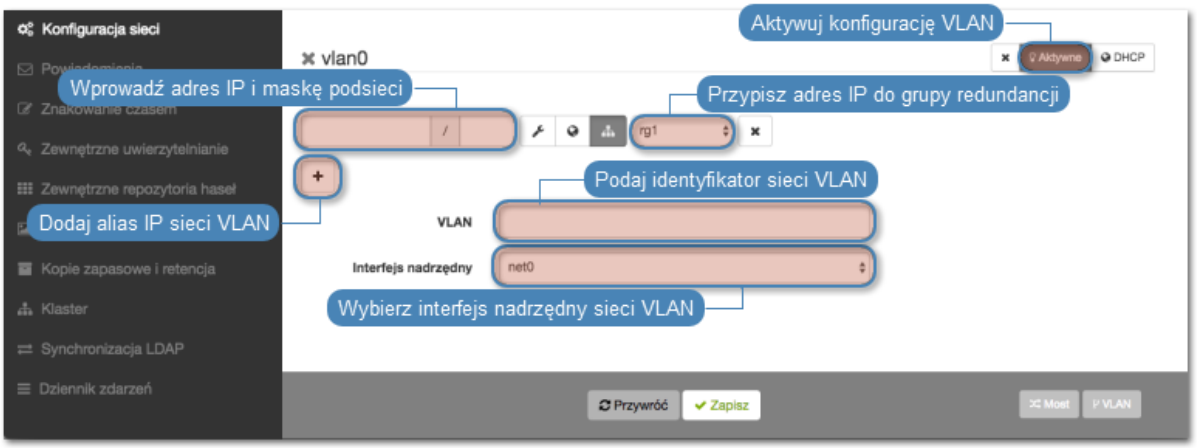
Aby skonfigurować Wheel Fudo PAM do pracy w sieci VLAN, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij *VLAN*, aby dodać definicję sieci wirtualnej.
3. Wybierz nadrzędny interfejs sieciowy oraz nadaj identyfikator konfigurowanej sieci wirtualnej.
4. Dodaj adresy IP przynależne do konfigurowanej sieci VLAN lub kliknij DHCP, aby pobrać adres IP z serwera DHCP.

Informacja: Wprowadzone adresy IP będą dostępne jako adresy lokalne pośrednika w *konfiguracji serwerów*.

---

5. Kliknij *Aktywne*, aby aktywować VLAN.
6. Kliknij *Zapisz*.



Tematy pokrewne:

- *Zarządzanie serwerami*
- *Gniazda nasłuchiwania*

6.2.2 Konfiguracja tras routingu

W konfiguracji domyślnej, Wheel Fudo PAM kieruje cały ruch przychodzący, do zdefiniowanej bramy. Routing statyczny pozwala na zdefiniowanie tras dla pakietów pochodzących ze wskazanych podsieci.

Informacja: Definiując domyślną trasę routowania pakietów, w polu *Sieć* wpisz `default`.

Dodawanie trasy routingu

Aby dodać trasę routingu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Kliknij *+ Dodaj trasę*, aby zdefiniować nową trasę routingu.
4. Wprowadź adres sieci, maskę w notacji CIDR (np. `192.168.0.1/29`) oraz adres IP bramy (np. `10.0.0.1`).
5. Kliknij *Zapisz*.

Modyfikowanie trasy routingu

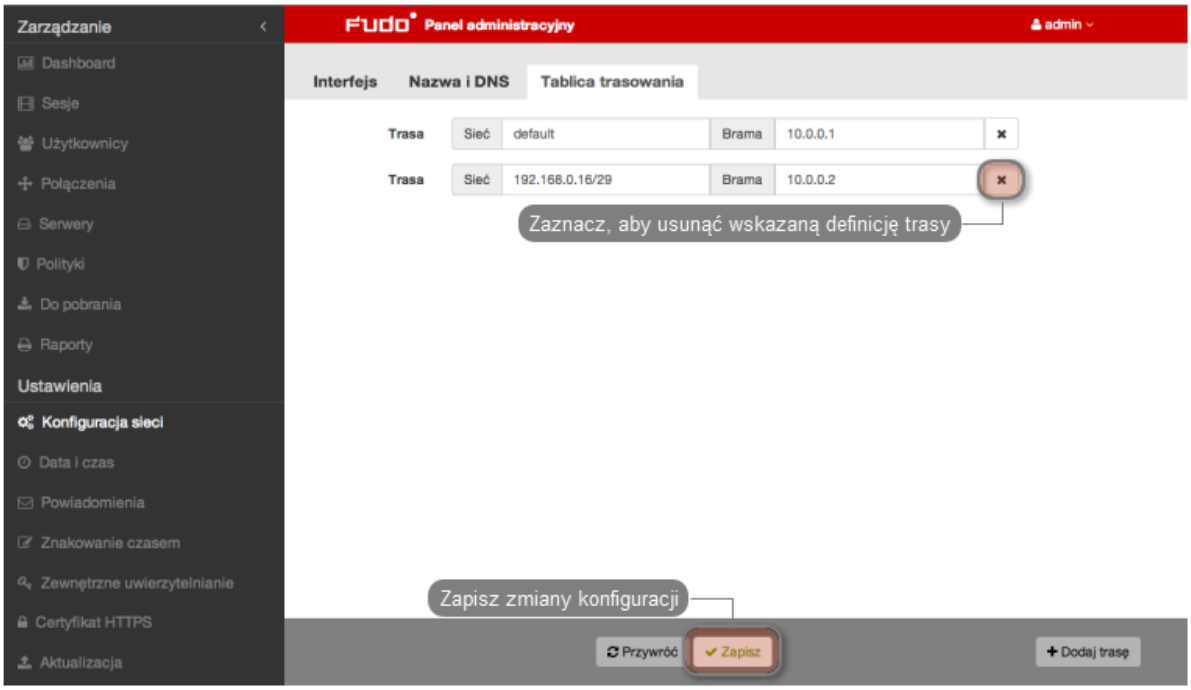
Aby zmodyfikować trasę routingu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Wyszukaj i zmień żądany wpis.
4. Kliknij *Zapisz*.

Usuwanie trasy routingu

Aby usunąć trasę routingu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Zaznacz opcję usunięcia wybranej trasy routingu i kliknij *Zapisz*.

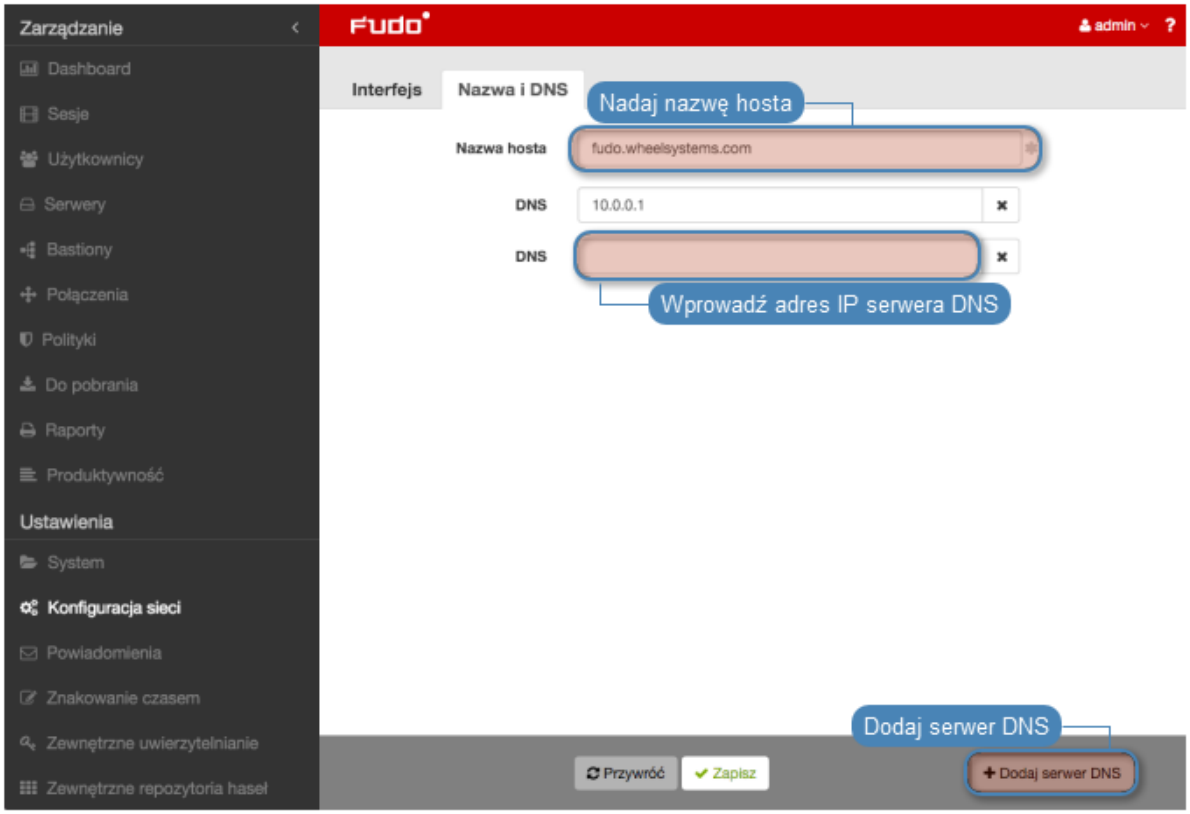


Tematy pokrewne:

- *Konfiguracja interfejsów sieciowych*
- *Konfiguracja serwerów czasu*

6.2.3 Konfiguracja serwerów DNS

Informacja: Serwer DNS pozwala na używanie mnemonicznych nazw hostów zamiast adresów IP w konfiguracji zasobów.



Dodawanie serwera DNS

Aby dodać serwer DNS, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Nazwa i DNS*.
3. Kliknij *+ Dodaj serwer DNS*, aby zdefiniować nowy serwer DNS.
4. Wprowadź adres IP serwera DNS.
5. Kliknij *Zapisz*.

Modyfikowanie serwera DNS

Aby zmodyfikować definicję serwera DNS, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki Nazwa i DNS.
3. Wyszukaj i zmień żądany wpis.
4. Kliknij Zapisz.

Usuwanie serwera DNS

Aby usunąć definicję serwera DNS, postępuj zgodnie z poniższą instrukcją.

Informacja: Usunięcie definicji serwera DNS może spowodować zakłócenia w pracy urządzenia, jeśli w konfiguracji wykorzystywane były nazwy hostów zamiast adresów IP.

---

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.

2. Przejdź do zakładki *Nazwa i DNS*.
3. Wyszukaj i kliknij opcję usunięcia wybranego wpisu.
4. Kliknij *Zapisz*.

Tematy pokrewne:

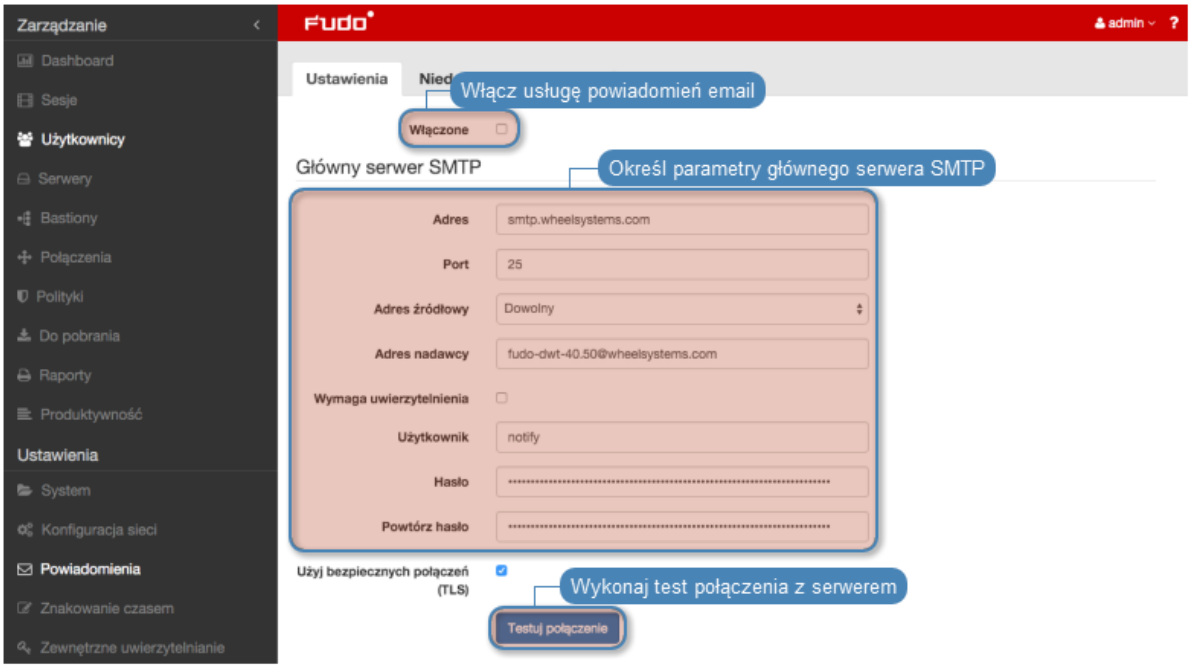
- *Konfiguracja interfejsów sieciowych*
- *Konfiguracja serwerów czasu*
- *Konfiguracja tras routingu*

6.3 Powiadomienia

Wheel Fudo PAM może wysyłać powiadomienia email o zdarzeniach dotyczących zdefiniowanych połączeń (rozpoczęcie sesji, zakończenie sesji, otwarcie pomocy zdalnej, zakończenie pomocy zdalnej, wykrycie wzorca). Usługa powiadomień dla poszczególnych obiektów połączenia, definiowana jest przy tworzeniu nowego obiektu lub podczas edycji istniejącego połączenia. Wysyłanie powiadomień wymaga skonfigurowania serwera poczty SMTP.

Aby skonfigurować serwer SMTP, postępuj zgodnie z poniższą instrukcją.

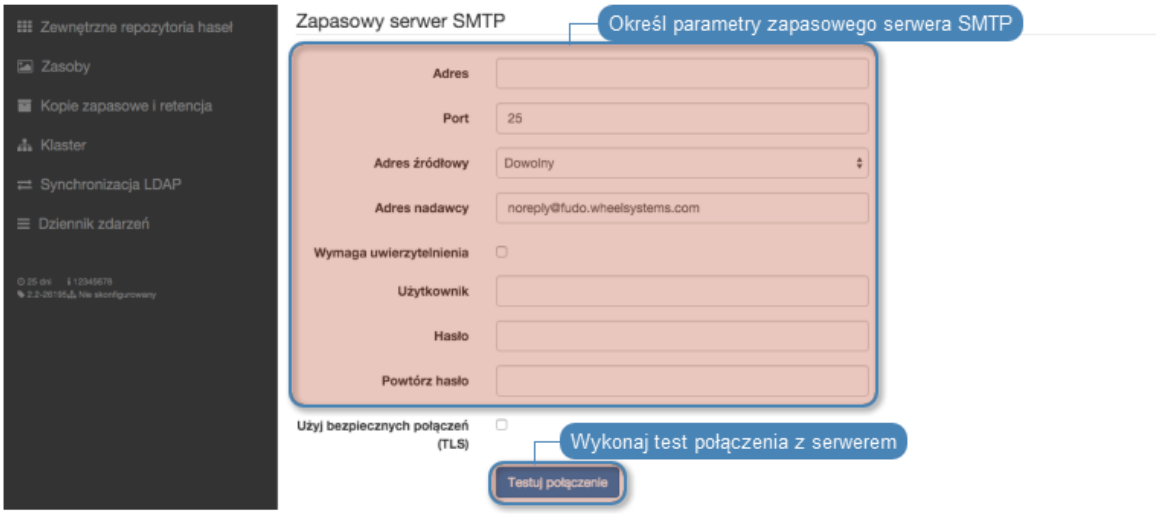
1. Wybierz z lewego menu *Ustawienia* > *Powiadomienia*.
2. Zaznacz opcję *Włączone*, aby system wysyłał powiadomienia.
3. Uzupełnij parametry konfiguracyjne głównego serwera SMTP.



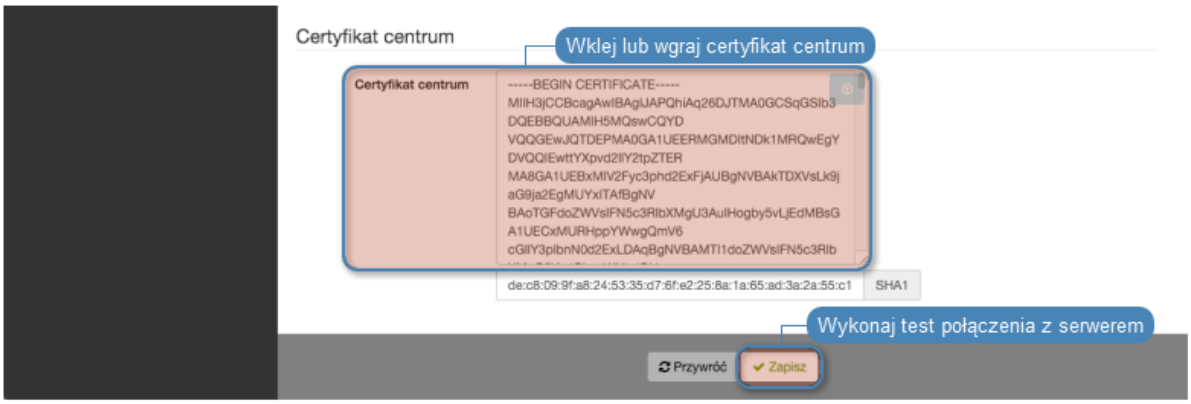
Parametr	Opis
Adres	Adres IP serwera SMTP.
Port	Numer portu, na którym działa usługa SMTP.
Adres nadawcy	Adres email, z którego wysyłane będą powiadomienia.
Wymaga uwierzytelnienia	Czy serwer SMTP wymaga uwierzytelniania.
Użytkownik	Nazwa użytkownika dla uwierzytelnienia usługi SMTP.
Hasło	Hasło użytkownika dla uwierzytelnienia usługi SMTP.
Użyj bezpiecznych połączeń (TLS)	Zaznacz, jeśli serwer pocztowy wykorzystuje protokół szyfrujący TLS.

Informacja: Kliknij *Testuj połączenie*, aby zweryfikować prawidłowość parametrów konfiguracyjnych.

4. Opcjonalnie, uzupełnij parametry konfiguracyjne dla zapasowego serwera SMTP.



5. Wprowadź treść certyfikatu urzędu certyfikacji, w formacie PEM.



6. Kliknij *Zapisz*.

Tematy pokrewne:

- *Sejfy*

6.4 Znakowanie czasem

Opatrzenie zarejestrowanej sesji znacznikiem czasu, czyni materiał bardziej wiarygodnym dowodem rzeczowym.

Informacja: Funkcjonalność znakowania sesji wymaga podpisania odrębnej umowy z instytucją świadczącą usługę znakowania czasem.

Konfigurowanie usługi znakowania czasem

Aby włączyć i skonfigurować usługę znakowania czasem, postępuj zgodnie z poniższą instrukcją.

Informacja: Znacznikiem czasu zostaną opatrzone również sesje, które zostały zarejestrowane przed włączeniem usługi.

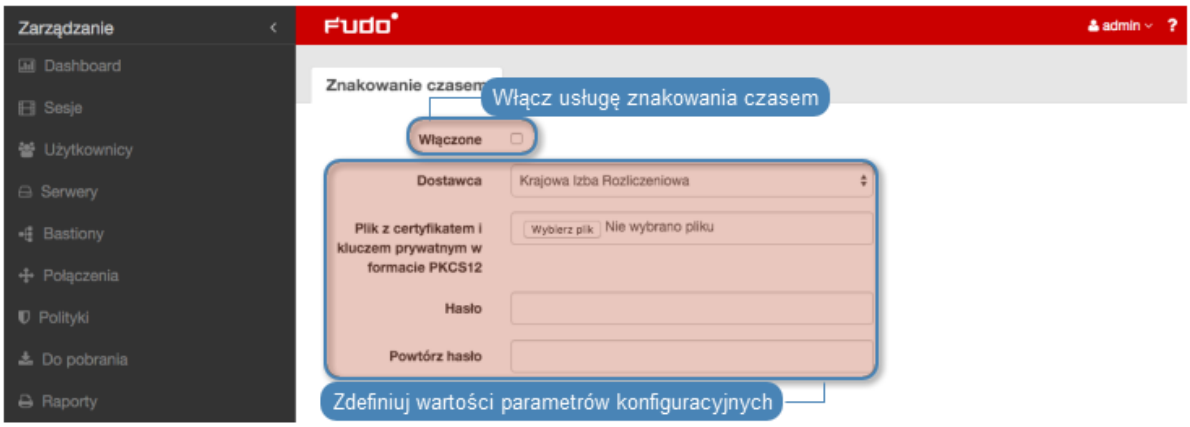
---

1. Wybierz z lewego menu *Ustawienia* > *Znakowanie czasem*.
2. Zaznacz opcję *Włącz*, aby znakować znacznikiem czasu zarejestrowane sesje.
3. Wybierz z listy rozwijalnej dostawcę usługi.
4. Wskaż plik z certyfikatem i kluczem.

Informacja: Certyfikat oraz klucz prywatny otrzymasz od dostawcy usługi znakowania czasem.

---

5. Kliknij *Zapisz*.



6.5 Zewnętrzne serwery uwierzytelniania

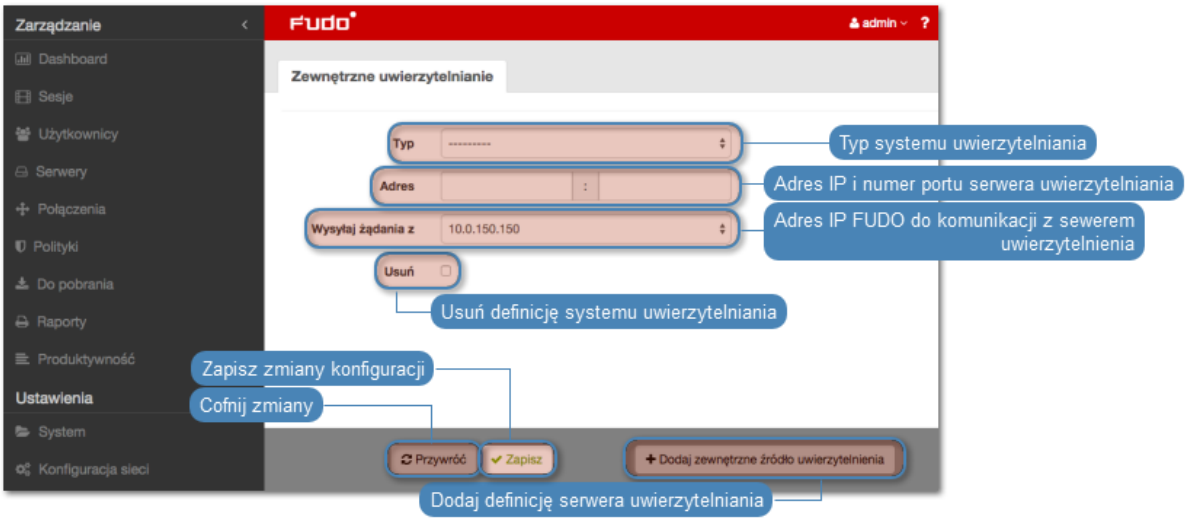
Uwierzytelnienie użytkowników za pomocą zewnętrznych serwerów uwierzytelniania (tj. *CERB*, *RADIUS*, *LDAP*, *Active Directory*) wymaga skonfigurowania połączeń z serwerami usług danego

typu.

Widok zarządzania serwerami uwierzytelniania

Widok zarządzania zewnętrznymi serwerami uwierzytelniania pozwala na dodanie nowych oraz edycję istniejących serwerów.

Aby przejść do widoku zarządzania serwerami uwierzytelniania, wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.



Dodawanie definicji serwera zewnętrznego uwierzytelniania

Aby dodać serwer uwierzytelniania, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Kliknij *+ Dodaj zewnętrzne źródło uwierzytelnienia*.
3. Z listy rozwijalnej *Typ*, wybierz rodzaj systemu uwierzytelnienia.
4. Uzupełnij parametry konfiguracyjne, zależne od typu wybranego systemu uwierzytelnienia.

Parametr	Opis
CERB	
Adres	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa CERB.
Wysyłaj żądania z	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelnienia.
Serwis	Serwis w systemie CERB w oparciu o który będzie uwierzytelniany użytkownik.
Sekret	Sekret wykorzystywany do połączeń z serwerem. Sekret odpowiada hasłu zdefiniowanemu podczas konfiguracji klienta RADIUS w systemie CERB.
Powtórz sekret	Sekret wykorzystywany do połączeń z serwerem.
RADIUS	
Adres	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa RADIUS.
Wysyłaj żądania z	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelniania.
NAS ID	Parametr, który zostanie przekazany w atrybucie NAS-Identifier do serwera RADIUS.
Sekret	Sekret serwera RADIUS służący szyfrowaniu haseł użytkowników.
Powtórz sekret	Sekret serwera RADIUS służący szyfrowaniu haseł użytkowników.
LDAP	
Host	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa LDAP.
Wysyłaj żądania z	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelniania.
Szablon DN użytkownika	Definicja użytkownika uprawnionego do przeszukiwania zawartości katalogu LDAP.
Active Directory	
Adres	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa AD.
Wysyłaj żądania z	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelnienia.
Domena Active Directory	Domena, w oparciu o którą będzie wykonywane uwierzytelnienie w serwerze Active Directory.

6. Kliknij *Zapisz*.

Modyfikowanie definicji serwera zewnętrznego uwierzytelniania

Aby zmodyfikować serwer uwierzytelniania, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Zmień parametry konfiguracyjne żądanej definicji serwera.
3. Kliknij *Zapisz*.

Usuwanie definicji serwera zewnętrznego uwierzytelniania

Aby usunąć definicję serwera uwierzytelniania, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia > Zewnętrzne uwierzytelnianie*.
2. Zaznacz opcję *Usuń* przy żądanej definicji serwera uwierzytelniania.
3. Kliknij Zapisz.

Tematy pokrewne:

- *Metody uwierzytelniania*
- *Opis systemu*
- *Integracja z serwerem CERB*

6.6 Zewnętrzne repozytoria haseł

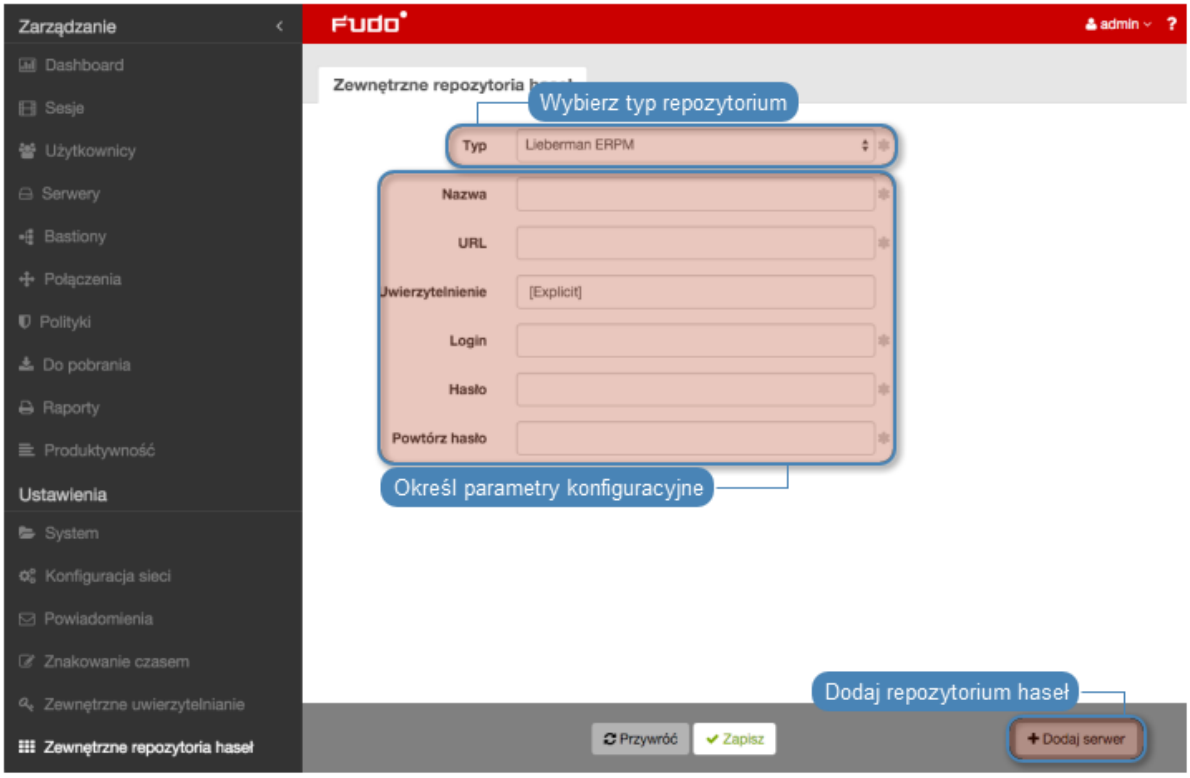
Wheel Fudo PAM wspiera zewnętrzne repozytoria haseł do zarządzania hasłami dostępowymi.

Dodawanie definicji repozytorium haseł

Aby dodać definicję repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia > Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Uzupełnij parametry konfiguracyjne serwera.

Pole	Opis
Typ	Typ definiowanego repozytorium haseł.
Nazwa	Nazwa definiowanego repozytorium haseł.
URL	Ścieżka do API repozytorium haseł.
Uwierzytelnienie (dotyczy serwerów Lieberman ERPM)	Moduł uwierzytelnienia przypisany do użytkownika uprawnionego do przeglądania zawartości repozytorium.
Login	Nazwa użytkownika uprawnionego do przeglądania zawartości repozytorium.
Hasło	Hasło uwierzytelniające użytkownika.
Powtórz hasło	Hasło uwierzytelniające użytkownika.
Format sekretu (dotyczy serwerów Thycotic Secret Server)	Ciąg znaków definiujący format identyfikatorów obiektów w systemie Thycotic Secret Server.



Informacja: Dla Hitachi ID PAM, konto użytkownika wskazane w konfiguracji, musi być typu OTP (One Time Password).

Informacja: Określ w ścieżce URL użycie protokółu HTTPS, aby komunikacja z serwerem podlegała szyfrowaniu.

Przykład: `https://10.0.0.2/PWCWeb/`

4. Kliknij *Zapisz*.

Modyfikowanie definicji repozytorium haseł

Aby zmodyfikować repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zmień parametry konfiguracyjne wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Usuwanie definicji repozytorium haseł

Aby usunąć definicję repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Zaznacz opcję *Usuń* przy wybranej definicji repozytorium haseł.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Zewnętrzne serwery uwierzytelniania*
- *Opis systemu*
- *Integracja z serwerem CERB*

6.7 Zasoby

Wheel Fudo PAM pozwala na dostosowanie do własnych potrzeb ekranów logowania dla połączeń graficznych RDP i VNC.

Zmiana logo

1. Wybierz z lewego menu *Ustawienia* > *Zasoby*.
2. Przejdź na zakładkę *RDP* lub *VNC*.
3. Kliknij *Wybierz Plik* i wskaż plik z nowym obrazem dla wybranego ekranu.

Informacja: Maksymalny rozmiar logo to 512 x 512 px.

4. Kliknij *Zapisz*.

Przywracanie domyślnego logo

1. Wybierz z lewego menu *Ustawienia* > *Zasoby*.
2. Przejdź na zakładkę *RDP* lub *VNC*.
3. Zaznacz opcję *Przywróć domyślne*.
4. Kliknij *Zapisz*.

Definiowanie komunikatu globalnego

Komunikat globalny wyświetlany jest na ekranie logowania serwerów RDP i VNC.

Informacja: Oprócz komunikatu globalnego, możliwe jest zdefiniowanie komunikatu dla pojedynczego serwera w formularzu edycji obiektu.

---

1. Wybierz z lewego menu *Ustawienia* > *Zasoby*.
2. Przejdź na zakładkę *RDP* lub *VNC*.
3. Uzpełnij treść w sekcji *Komunikat globalny*.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Szybki start - RDP*

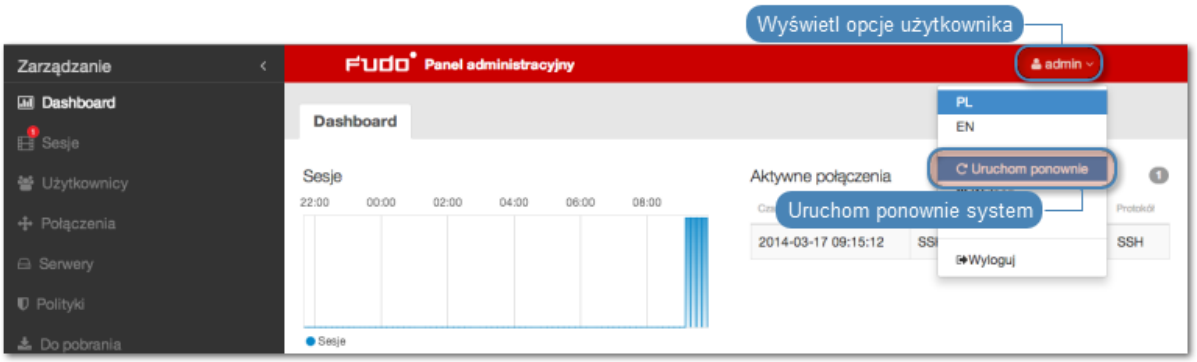
6.8 Przywracanie poprzedniej wersji systemu

W przypadku gdy wystąpił problem z bieżącą wersją oprogramowania, istnieje możliwość przywrócenia poprzedniej wersji oprogramowania.

Ostrzeżenie: Przywrócenie poprzedniej wersji spowoduje odtworzenie stanu systemu sprzed jego aktualizacji. Dane sesji oraz zmiany w konfiguracji dokonane na nowej wersji systemu zostaną utracone.

Aby przywrócić poprzednią wersję systemu, postępuj zgodnie z poniższą instrukcją.

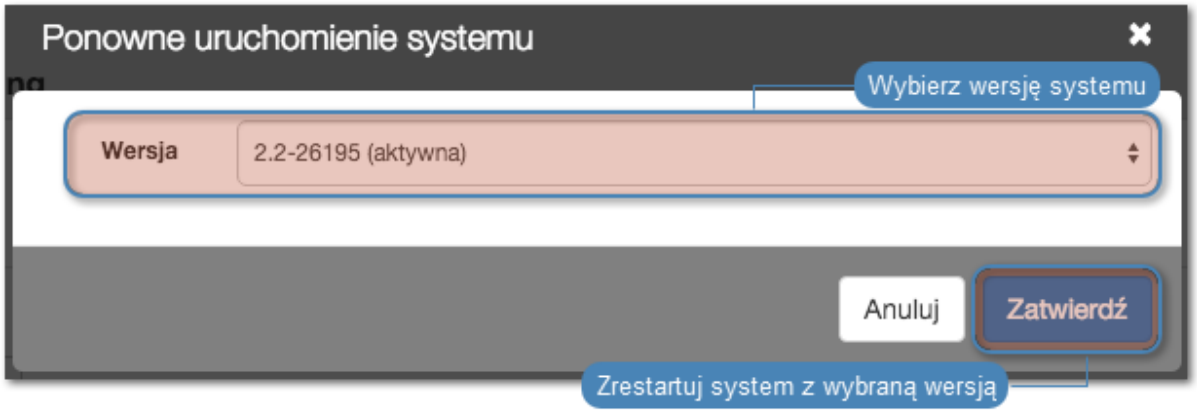
1. Podłącz nośnik z kluczem szyfrującym do portu USB.
2. Z menu opcji użytkownika, wybierz opcję *Uruchom ponownie*.



3. Wybierz wersję systemu, jaką chcesz załadować po zrestartowaniu urządzenia.

Informacja: Domyślnie zaznaczona jest wersja bieżąca.

4. Kliknij *Zatwierdź*, aby potwierdzić operację ponownego uruchomienia, z wybraną wersją systemu.



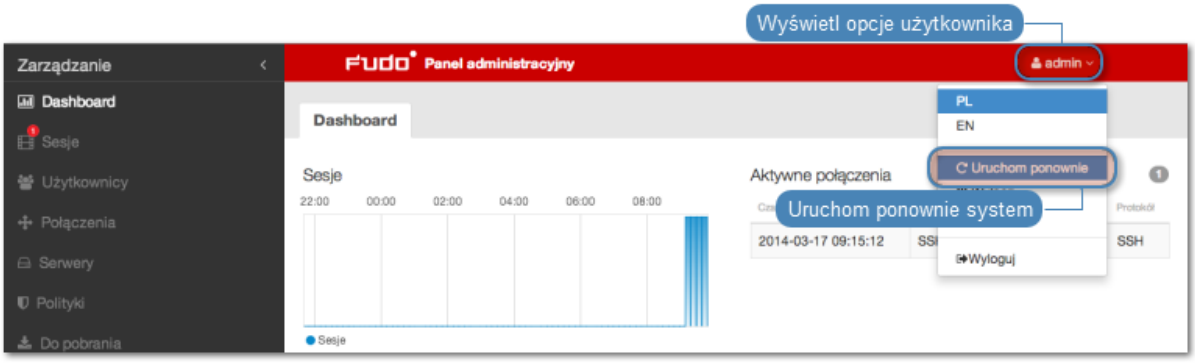
Ostrzeżenie: Ponowne uruchomienie systemu spowoduje rozłączenie bieżących połączeń użytkowników.

Tematy pokrewne:

- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

6.9 Ponowne uruchomienie systemu

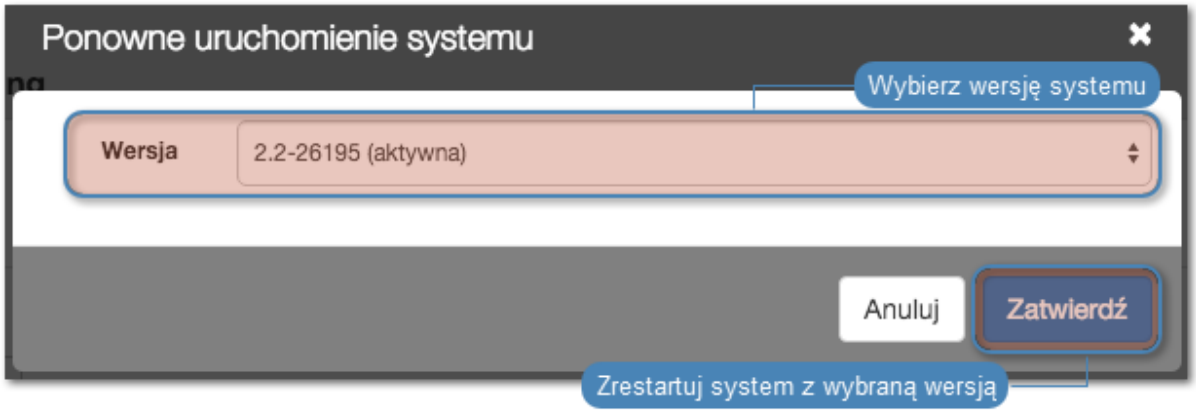
1. Podłącz nośnik z kluczem szyfrującym do portu USB.
2. Z menu opcji użytkownika, wybierz opcję *Uruchom ponownie*.



3. Wybierz wersję systemu, jaką chcesz załadować po zrestartowaniu urządzenia.

Informacja: Domyślnie zaznaczona jest wersja bieżąca.

4. Kliknij *Zatwierdź*, aby potwierdzić operację ponownego uruchomienia, z wybraną wersją systemu.



Ostrzeżenie: Ponowne uruchomienie systemu spowoduje rozłączenie bieżących połączeń użytkowników.

Tematy pokrewne:

- *Pierwsze uruchomienie*
- *Przywracanie poprzedniej wersji systemu*

6.10 Kopie zapasowe i retencja

Retencja danych

Mechanizm retencji danych umożliwia automatyczne usuwanie danych sesji starszych niż zdefiniowana liczba dni.

Aby włączyć retencję danych, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Kopie zapasowe i retencja*.
2. W sekcji *Retencja danych*, zaznacz opcję *Włączone*, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.
3. Wprowadź wartość w polu *Usuń dane sesji po upływie*, aby określić czas przechowywania danych sesji.

Informacja: Globalna wartość parametru retencji danych ma niższy priorytet niż wartość retencji zdefiniowana w obiekcie typu *konto*.

---

4. Kliknij *Zapisz*.

Kopia zapasowa systemu

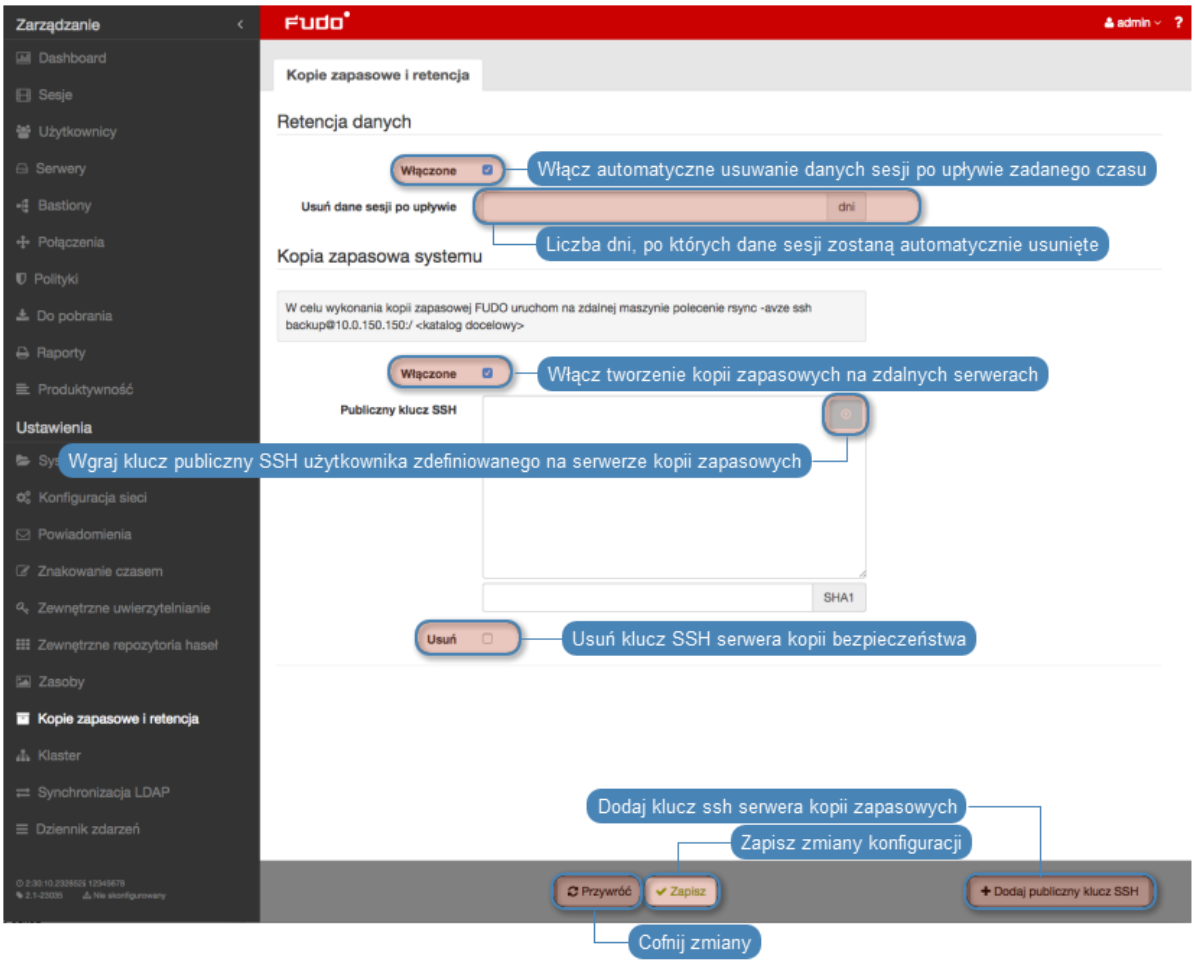
Ostrzeżenie: Kopia zapasowa systemu zawiera poufne informacje.

Automatyczne tworzenie kopii zapasowych danych przechowywanych na Wheel Fudo PAM wymaga skonfigurowania usługi `rsync` na zdalnym serwerze kopii zapasowych i przyznania prawa dostępu do danych przechowywanych na Wheel Fudo PAM, poprzez wgranie klucza publicznego serwera.

Informacja: Dane sesji przechowywane są w systemie plików z domyślnie włączoną kompresją o współczynniku sięgającym 12:1. Podczas kopiowania, dane podlegają dekompresji, stąd na serwerze kopii bezpieczeństwa mogą zajmować więcej miejsca niż wskazuje zajętość macierzy dyskowej Wheel Fudo PAM. Upewnij się, że serwer docelowy dysponuje odpowiednio dużą przestrzenią dyskową zdolną do przechowywania zdekompresowanych danych.

Aby włączyć usługę tworzenia kopii zapasowych, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Kopie zapasowe i retencja*.
2. W sekcji *Kopia zapasowa systemu*, zaznacz opcję *Włączone*.
3. Kliknij *Dodaj publiczny klucz SSH*.
4. Wprowadź lub wgraj klucz publiczny SSH użytkownika zdefiniowanego na serwerze kopii bezpieczeństwa.
5. Kliknij *Zapisz*.
6. Wykonaj na zdalnej maszynie polecenie: `rsync -avze ssh backup@adres_ip_fudo:/<katalog docelowy>`.



Odtwarzanie stanu systemu z kopii bezpieczeństwa

Usługa odtworzenia stanu systemu z kopii bezpieczeństwa świadczona jest przez dział wsparcia technicznego firmy Wheel Systems, na zasadach określonych w SLA.

Tematy pokrewne:

- *Mechanizmy bezpieczeństwa*
- *Eksportowanie/importowanie konfiguracji systemu*

6.11 Eksportowanie/importowanie konfiguracji systemu

Wheel Fudo PAM pozwala eksportować aktualny stan systemu, zdefiniowane obiekty jak i ustawienia konfiguracyjne, które później mogą zostać użyte do ponownego zainicjowania maszyny.

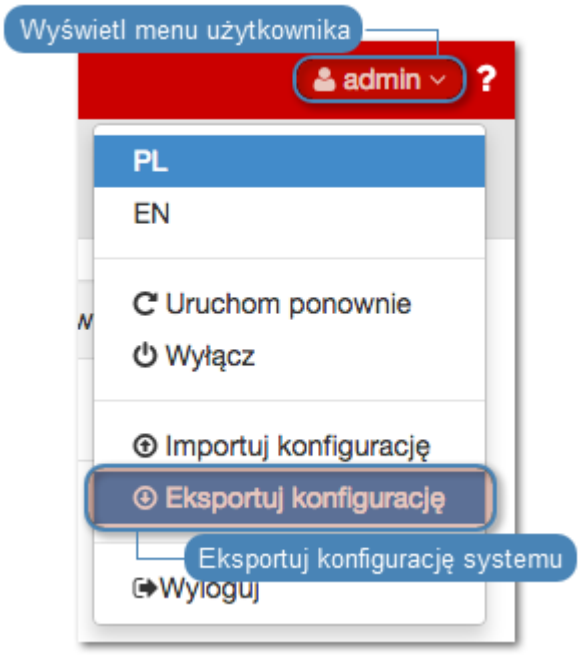
Ostrzeżenie: Wyeksportowana konfiguracja zawiera poufne informacje.

Informacja: Opcje importowania i eksportowania konfiguracji dostępne są dla użytkowników o przypisanej roli *superadmin*.

6.11.1 Eksportowanie konfiguracji

Aby wyeksportować konfigurację systemu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z menu użytkownika opcję *Eksportuj konfigurację*.
2. Zapisz plik konfiguracji.

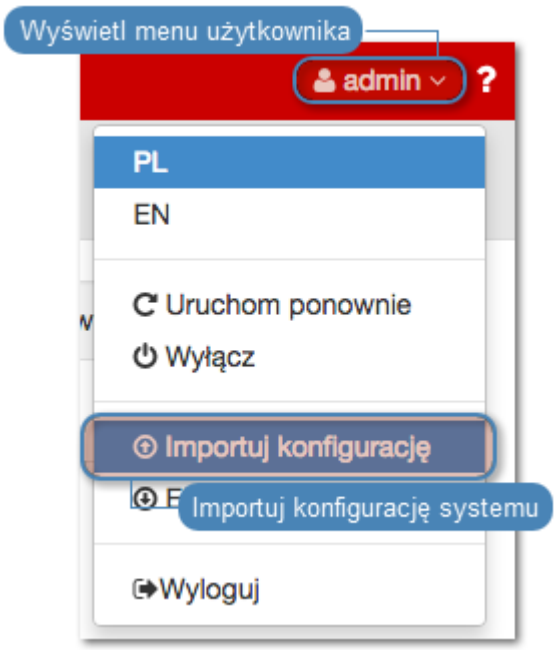


6.11.2 Importowanie konfiguracji

Ostrzeżenie: Zainicjowanie systemu wcześniej zapisaną konfiguracją spowoduje utratę wszystkich danych sesji.

Aby zaimportować konfigurację systemu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z menu użytkownika opcję *Importuj konfigurację*.



2. Wskaż plik konfiguracji i kliknij *Zatwierdź*.
3. Zatwierdź zainicjowanie systemu danymi z pliku.

Tematy pokrewne:

- *Kopie zapasowe i retencja*
- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

6.12 Konfiguracja klastrowa

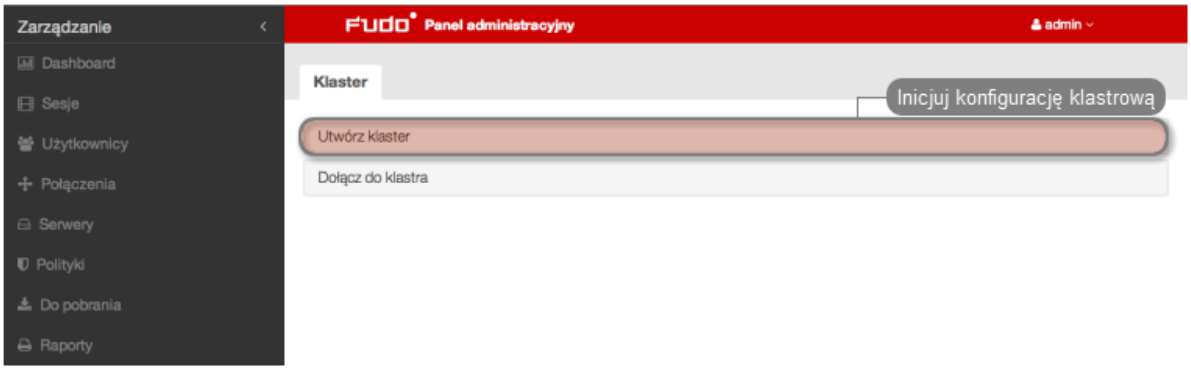
Klaster Wheel Fudo PAM zapewnia nieprzerwany dostęp do serwerów, w przypadku awarii jednego z węzłów systemu, a także pozwala na implementację scenariuszy statycznego balansowania obciążeniem zapytaniami użytkowników.

Ostrzeżenie: Konfiguracja klastrowa nie jest mechanizmem tworzenia kopii zapasowych danych. Dane sesji usunięte z jednego węzła, zostaną również usunięte z pozostałych węzłów klastra.

6.12.1 Inicjowanie klastra

Aby zainicjować klaster Wheel Fudo PAM postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Wybierz opcję *Utwórz klaster*, aby wyświetlić parametry inicjowania klastra.



3. Wprowadź nazwę węzła oraz opis ułatwiający identyfikację obiektu.
4. Z listy rozwijalnej *Adres* wybierz adres IP do komunikacji z innymi węzłami klastra.

5. Kliknij *Zatwierdź*, aby zainicjować klaster.

Informacja: Komunikat o konieczności skopiowania klucza może zostać pominięty przy inicjacji klastra.

Tematy pokrewne:

- *Bezpieczeństwo: Konfiguracja klastrowa*
- *Grupy redundancji*
- *Konfiguracja klastrowa*

6.12.2 Węzły klastra

Dodawanie węzłów klastra

Ostrzeżenie:

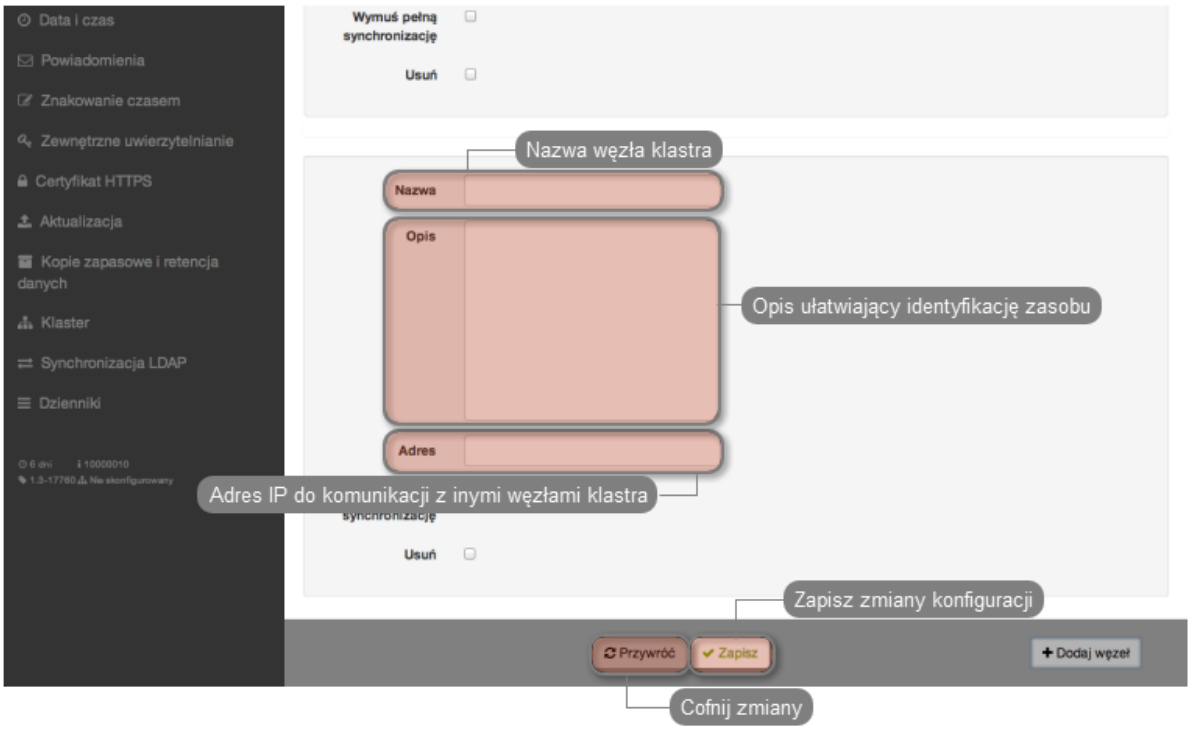
- Dane sesji oraz parametry konfiguracyjne (połączenia, serwery, użytkownicy, zewnętrzne serwery uwierzytelniania) węzła dołączanego są usuwane i inicjowane na nowo danymi zreplikowanymi z klastra.
- Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z węzłów. W przypadku problemów z relpikacją danych, skontaktuj się z działem wsparcia technicznego.

Aby dodać węzeł do klastra Wheel Fudo PAM, postępuj zgodnie z poniższą instrukcją.

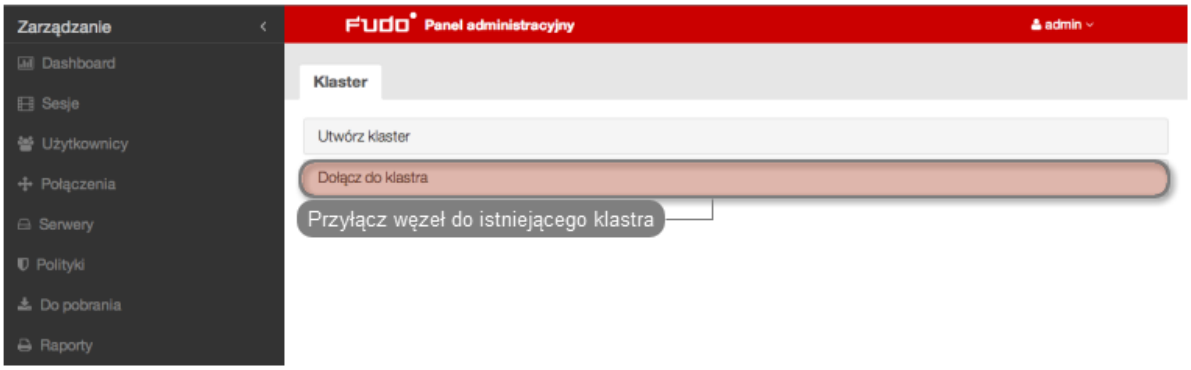
1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM, na którym został *zainicjowany klaster*.
2. Wybierz z lewego menu *Ustawienia* > *Klaster*.
3. Kliknij *Dodaj węzeł*.

4. Wprowadź nazwę węzła oraz opis, ułatwiający identyfikację obiektu.
5. Podaj adres IP węzła dołączanego.

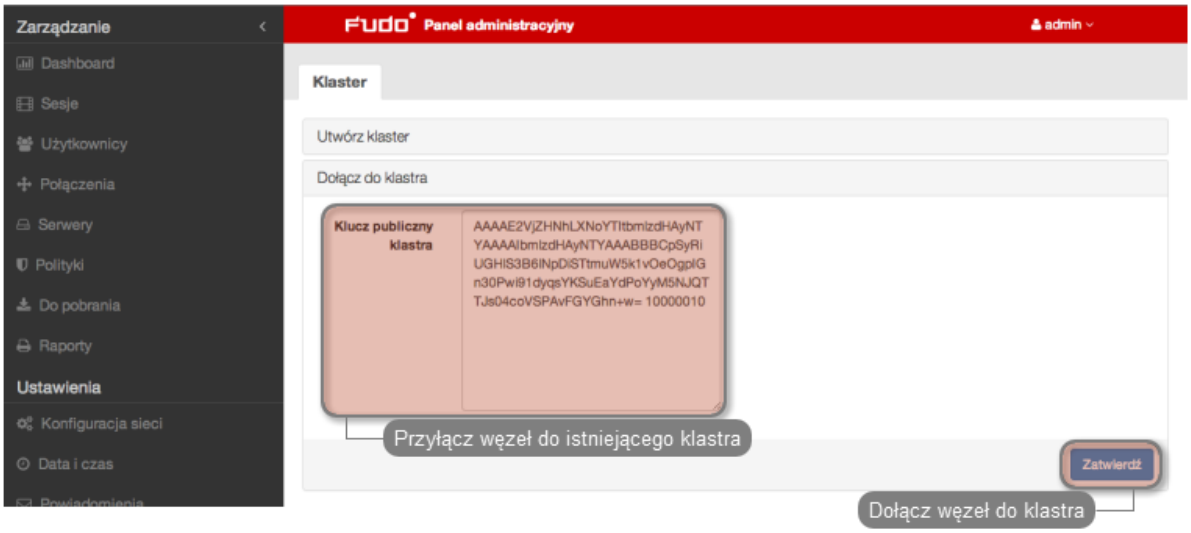
Informacja: Na wskazanym interfejsie sieciowym dołączanego węzła musi być aktywna opcja zarządzania urządzeniem. Informacje na temat konfigurowania ustawień sieciowych znajdziesz w rozdziale *Ustawienia sieci: Konfiguracja interfejsów sieciowych*.



6. Kliknij *Zapisz*, aby dodać definicję węzła i wygenerować klucz publiczny SSH.
7. Skopiuj wygenerowany klucz.
8. Zaloguj się do panelu administracyjnego węzła dołączanego.
9. Wybierz z lewego menu *Ustawienia* > *Klaster*.
10. Wybierz opcję *Dołącz do klastra*.



11. Wklej wygenerowany wcześniej klucz i kliknij *Zatwierdź*.



Edytowanie węzłów klastra

Aby zmodyfikować konfigurację węzła klastra Wheel Fudo PAM, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Znajdź i zmodyfikuj dane żądanego węzła.
3. Kliknij *Zapisz*.

Wymuszanie pełnej synchronizacji węzła klastra

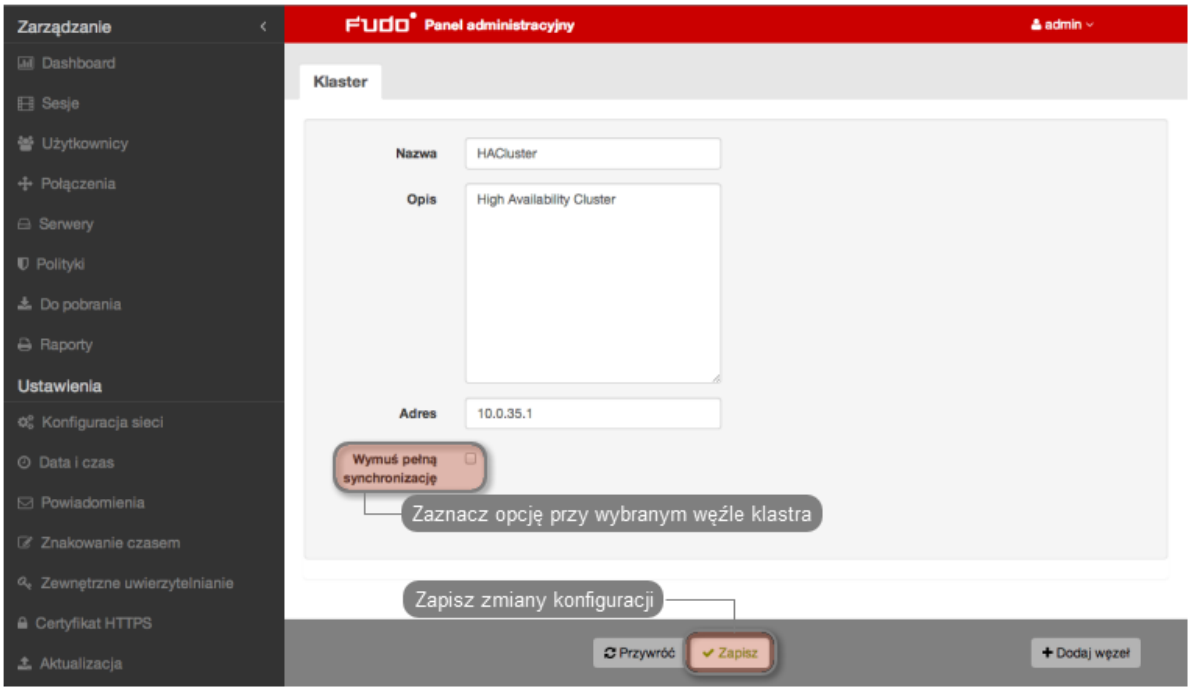
Ostrzeżenie: Przed wymuszeniem pełnej synchronizacji węzła klastra skontaktuj się z działem wsparcia technicznego Wheel Systems.

W sytuacji gdy dane przechowywane na jednym z węzłów klastra uległy desynchronizacji, należy przeprowadzić wymuszoną synchronizację danych, na wskazanym węźle.

Informacja: Wskazany węzeł zostanie zainicjowany danymi z innego węzła klastra.

Aby wymusić pełną synchronizację danych na węźle klastra, postępuje zgodnie z poniższą instrukcją.

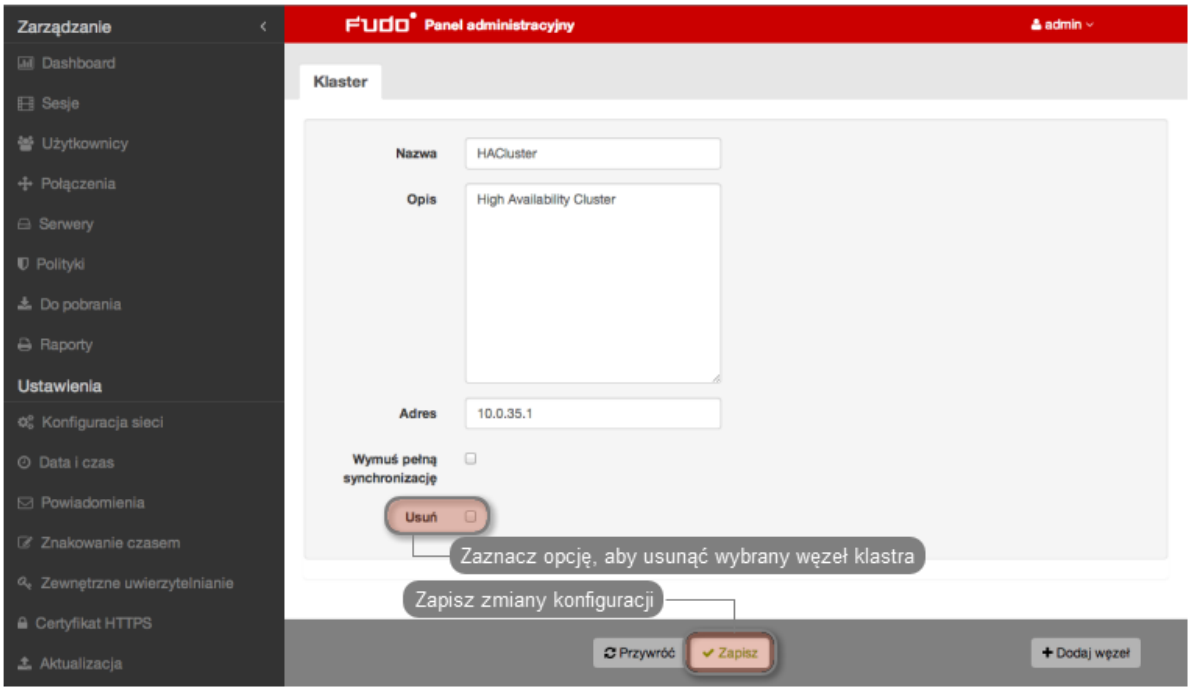
1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM na węźle innym, niż ten który wymaga synchronizacji danych.
2. Wybierz z lewego menu *Ustawienia* > *Klaster*.
3. Zaznacz opcję Wymuś pełną synchronizację przy węźle, który wymaga synchronizacji danych i kliknij *Zapisz*.



Usuwanie węzłów klastra

Aby usunąć węzeł klastra Wheel Fudo PAM, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Zaznaczy opcję *Usuń* przy wybranym węźle klastra i kliknij *Zapisz*.



Tematy pokrewne:

- *Bezpieczeństwo: Konfiguracja klastrowa*
- *Inicjowanie klastra*
- *Konfiguracja klastrowa*

6.12.3 Grupy redundancji

Grupy redundancji agregują adresy IP przypisane do interfejsów sieciowych. Nadanie różnym grupom odpowiednich priorytetów na poszczególnych węzłach klastra pozwala na statyczne balansowanie obciążeniem węzłów przy zachowaniu funkcjonalności klastra niezawodnościowego.

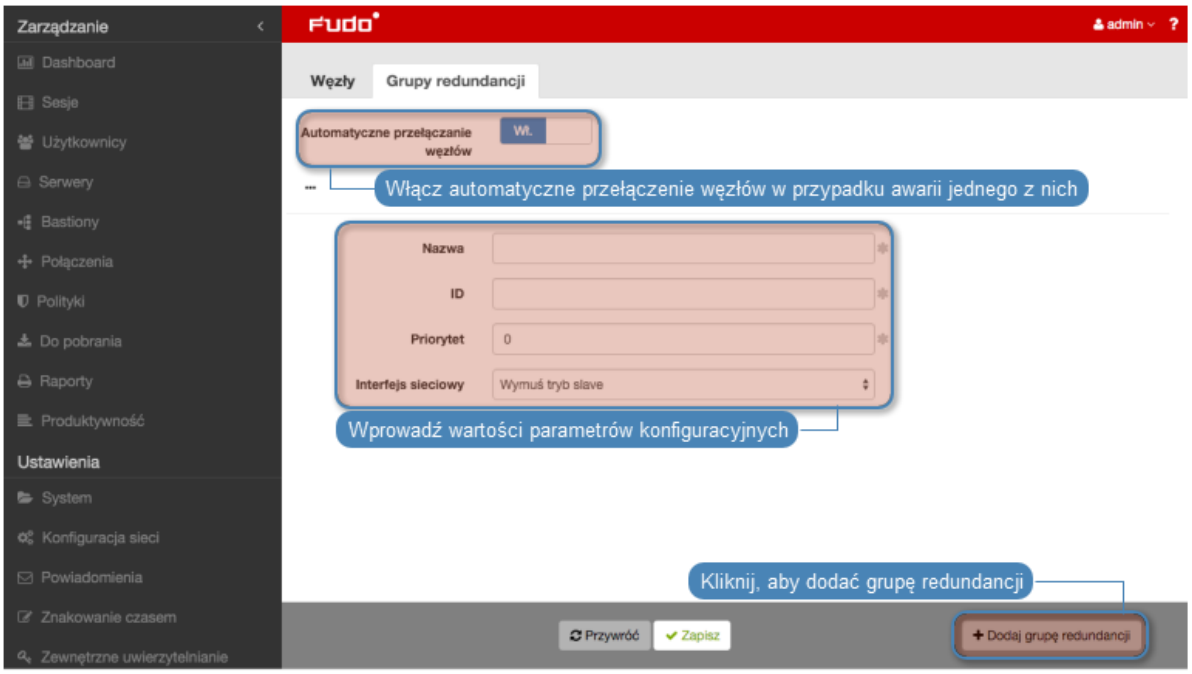
Informacja: Opcje konfigurowania grup redundancji dostępne są po zainicjowaniu klastra.

Dodawanie grup redundancji

Aby dodać grupę redundancji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Kliknij *+ Dodaj grupę redundancji*.
4. Zdefiniuj parametry grupy.

Parametr	Opis
Nazwa	Nazwa grupy redundancji.
ID	Identyfikator grupy redundancji (1-255).
Priorytet	Priorytet grupy redundancji (0-254), mniejsza wartość parametru oznacza wyższy priorytet.
	Grupa redundancji o wyższym priorytecie przyjmuje rolę *master* i obsługuje żądania dostępu do serwerów o adresach IP przypisanych do grupy. W przypadku awarii takiego węzła, zapytania kierowane są do węzła o najwyższym priorytecie wśród pozostałych.
Interfejs sieciowy	Interfejs sieciowy używany przez grupę redundancji do komunikacji z pozostałymi węzłami klastra.

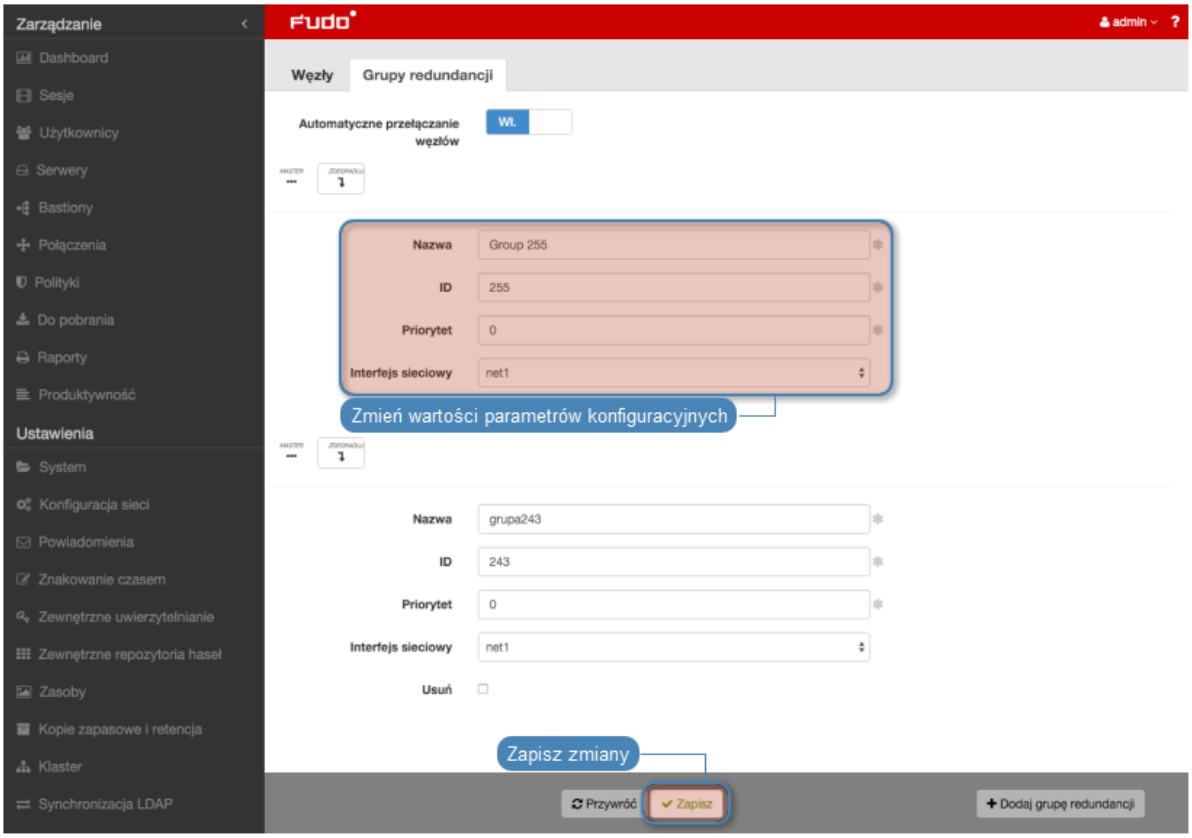


5. Kliknij *Zapisz*.

Edytowanie grup redundancji

Aby zmodyfikować grupę redundancji, postępuj zgodnie z poniższą instrukcją.

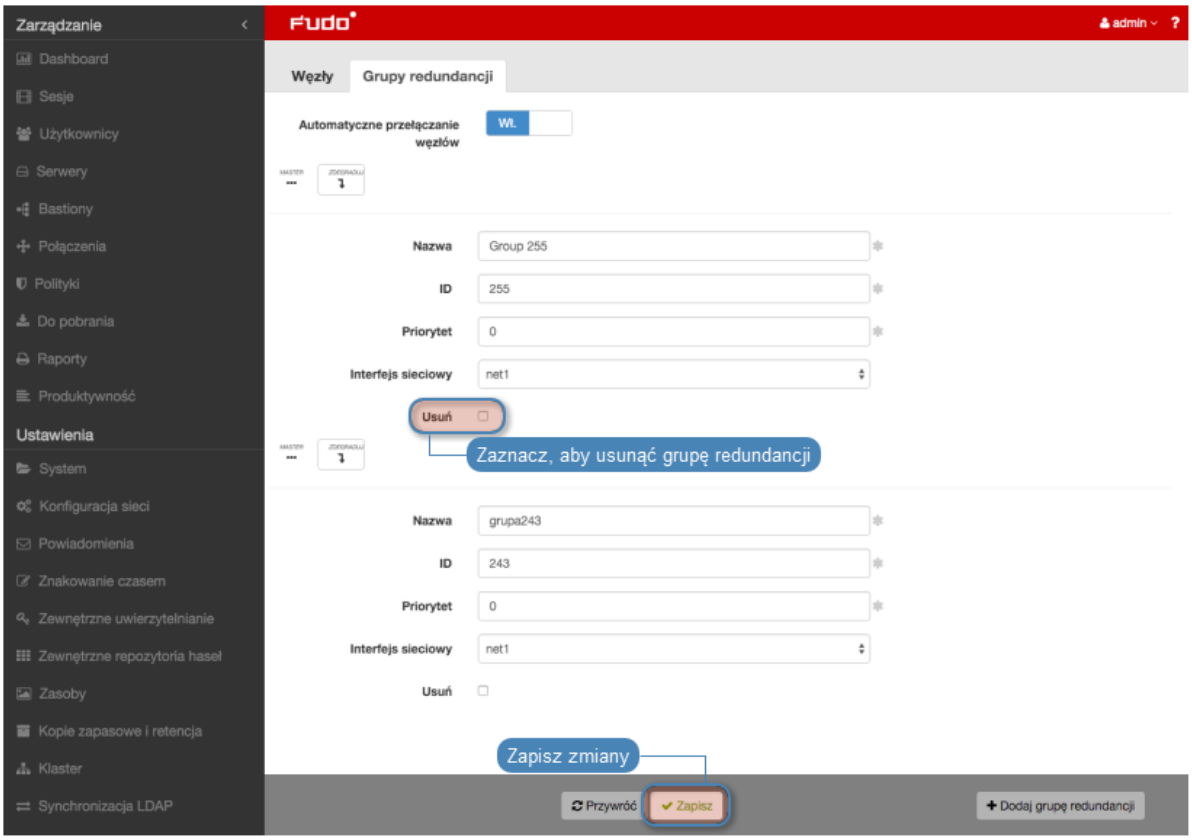
1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Zmień parametry wybranej grupy redundancji.
4. Kliknij *Zapisz*.



Usuwanie grup redundancji

Aby usunąć grupę redundancji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Zaznacz opcję *Usuń* przy wybranej grupie redundancji.
4. Kliknij *Zapisz*.

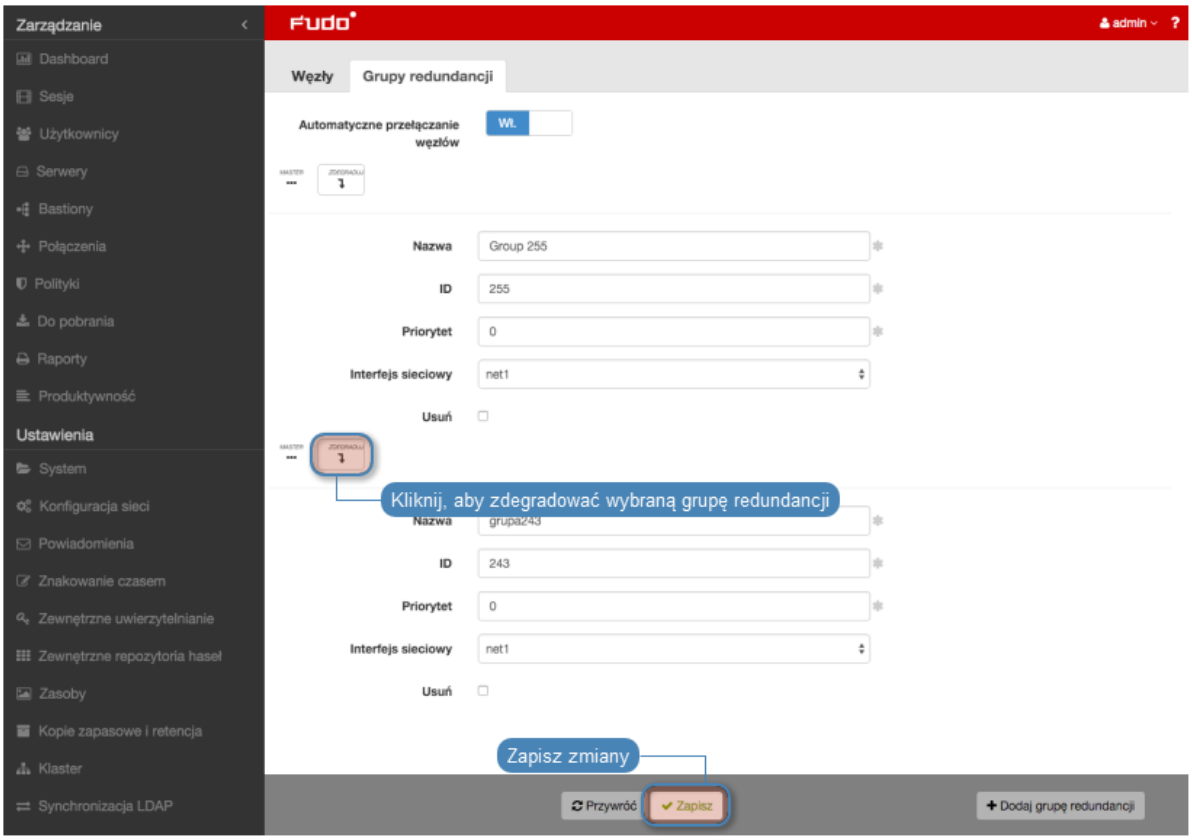


Degradowanie grupy redundancji

Informacja: Degradowanie grupy służy przełączeniu roli nadrzędnej dla danej grupy redundancji na inny węzeł klastra. Rolę nadrzędną dla grupy przejmie węzeł, na którym wybrana grupa redundancji ma najwyższy priorytet.

Aby zdegradować grupę redundancji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Kliknij *Degraduj* przy wybranej grupie redundancji.
4. Kliknij *Zatwierdź*.



Informacja: Jeśli po zdegradowaniu grupy żaden z pozostałych węzłów nie przejmie dla niej roli nadrzędnej, ta zostanie przywrócona grupie redundancji na edytowanym węźle.

Wymuszanie roli podrzędnej

Informacja: Wymuszenie roli podrzędnej spowoduje, że grupa redundancji nigdy nie przejdzie w tryb nadrzędny, niezależnie od stanu pozostałych węzłów klastra. Wymuszanie roli podrzędnej zalecane jest przed wykonywaniem prac serwisowych, aby ruch sieciowy kierowany był do pozostałych węzłów klastra.

Aby wymusić rolę podrzędną wybranej grupy redundancji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Odszukaj grupę redundancji i z listy rozwijalnej *Interfejs* wybierz `Wymuś tryb slave`.
4. Kliknij *Zapisz*.

Tematy pokrewne:

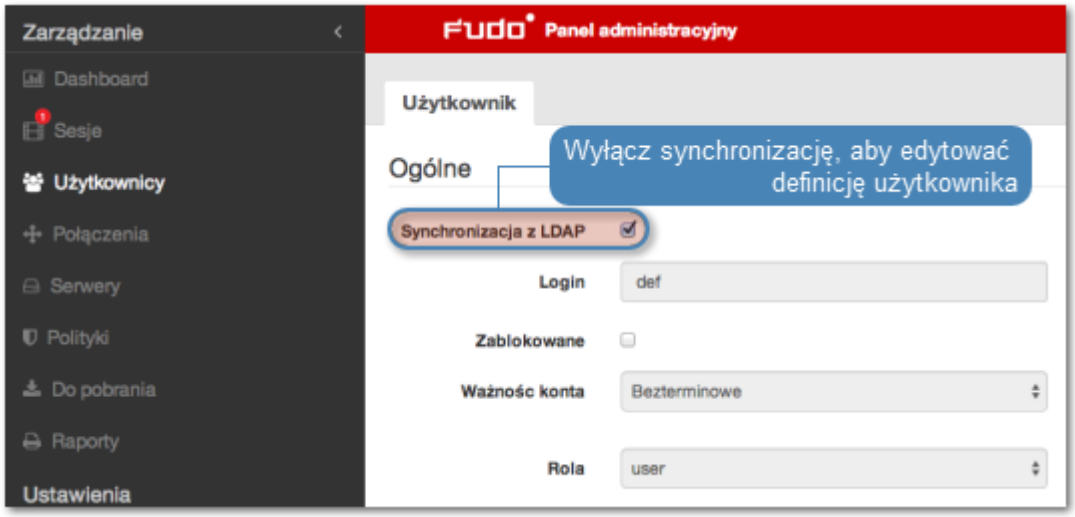
- *Bezpieczeństwo: Konfiguracja klastrowa*
- *Inicjowanie klastra*
- *Konfiguracja klastrowa*

6.13 Synchronizacja użytkowników

Użytkownik jest jednym z podstawowych elementów *modelu danych*. Tylko zdefiniowani użytkownicy mogą nawiązywać połączenia z monitorowanymi serwerami. Wheel Fudo PAM pozwala na automatyczną synchronizację definicji użytkowników z serwerem Active Directory.

Definicje nowych użytkowników oraz zmiany w istniejących obiektach pobierane są z serwera usług katalogowych co 5 minut. Odzwierciedlenie zmiany polegającej na usunięciu użytkownika z serwera AD lub LDAP wymaga pełnej synchronizacji. Pełna synchronizacja wyzwalana jest automatycznie raz na dobę, w czasie do 5 minut po godzinie 00:00, lub może zostać wyzwolona ręcznie.

Informacja: Dane użytkowników synchronizowanych z serwerem usług katalogowych nie mogą być poddawane edycji. Aby zmienić definicję użytkownika synchronizowanego z serwerem LDAP lub AD, wyłącz opcję `Synchronizacja z LDAP` dla danego użytkownika.



Konfiguracja usługi synchronizacji użytkowników

1. Wybierz z lewego menu *Ustawienia* > *Synchronizacja LDAP*.
2. Zaznacz opcję *Włączone*.
3. Wybierz z listy rozwijalnej *Rodaj serwera* typ usługi katalogowej.
4. Podaj informacje uwierzytelniające użytkownika uprawnionego do przeglądania katalogu.
5. Zdefiniuj adres serwera oraz port, na którym dostępna jest usługa katalogowa.
6. Podaj nazwę domeny, do której należą użytkownicy podlegający synchronizacji.
7. Określ bazowy parametr DN struktury katalogowej (np. `dc=devel,dc=whl`).

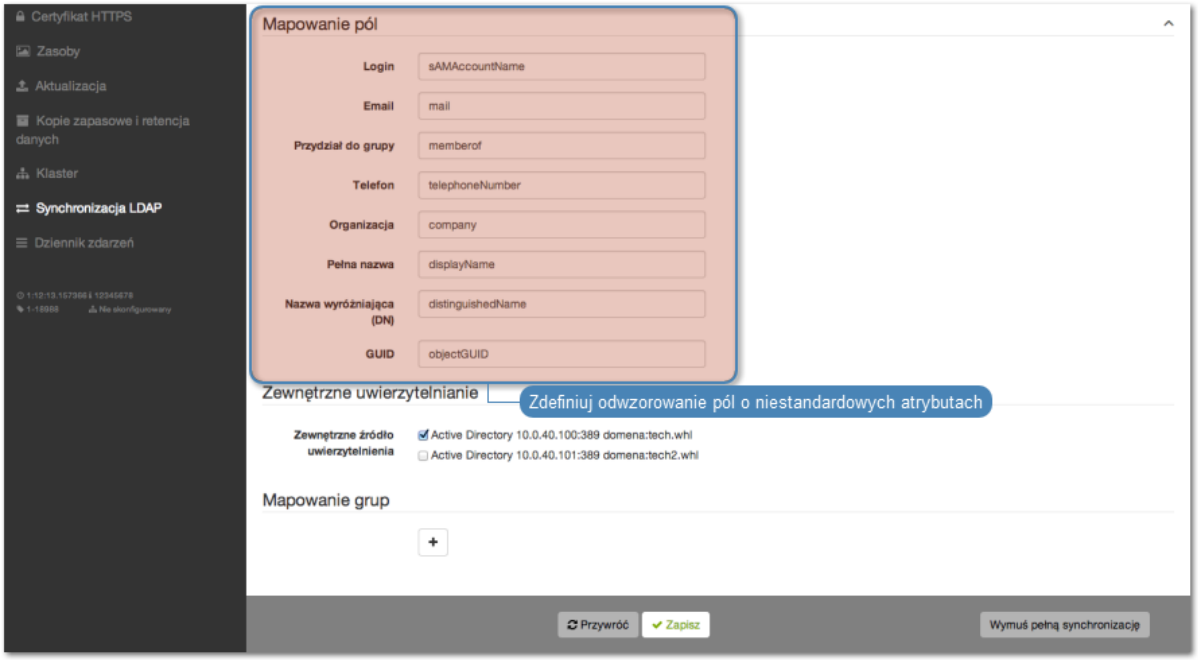
Informacja: Synchronizacja użytkowników przechowywanych w strukturze LDAP wymaga:

- użycia nakładki *memberOf*
- użycia grup *objectClass*: `groupOfNames`
- zdefiniowania ciągu parametru base DN w postaci: `uid=##username##,ou=people,dc=ldap,dc=test`.

Informacja: Parametr DN nie powinien zawierać zbędnych znaków białych, tj. spacji, tabulatorów, itp.

8. Zdefiniuj filtr dla rekordów użytkowników, których definicje mają zostać zsynchronizowane.
9. Zdefiniuj filtr dla grup użytkowników, których definicje mają zostać zsynchronizowane.
10. Zdefiniuj mapowanie pól definicji użytkowników.

Informacja: Mapowanie pól pozwala na pobranie informacji o użytkownikach z atrybutów o niestandardowych nazwach, np. numeru telefonu zdefiniowanego w atrybucie *mobile* zamiast standardowego *telephoneNumber*.

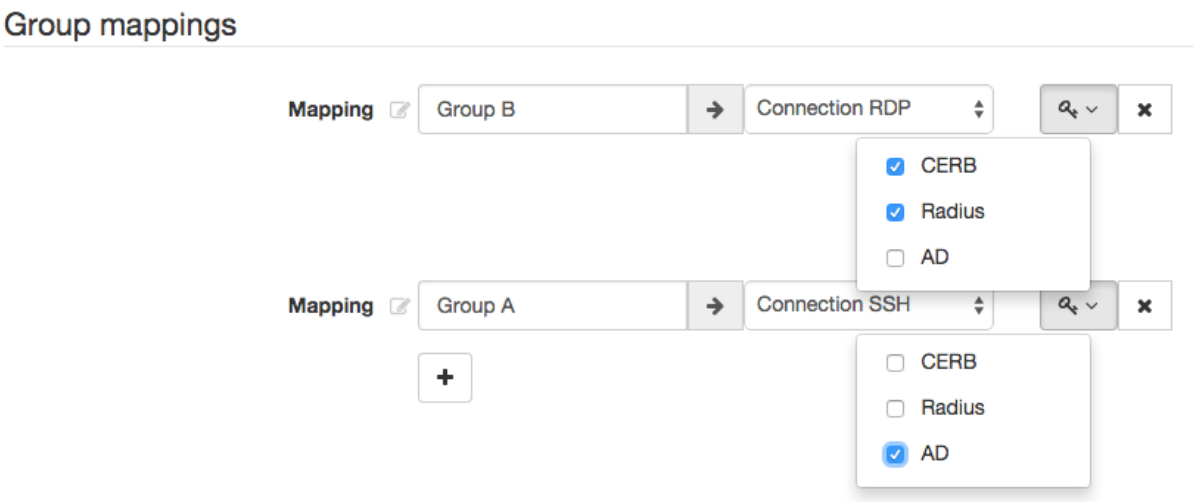


11. Zaznacz zewnętrzne źródła uwierzytelniania, jakie zostaną przypisane do definicji użytkowników synchronizowanych z serwerem usług katalogowych.
12. Określ przypisanie grup użytkowników do sejfów.
13. Przypisz źródła uwierzytelnienia do grup użytkowników.

Informacja: Źródła uwierzytelnienia przypisywane są użytkownikom w kolejności definiowania mapowań. Jeśli użytkownik znajduje się w więcej niż jednej grupie, w pierwszej kolejności będzie uwierzytelniany w oparciu o źródła uwierzytelniania przypisane do pierwszego zdefiniowanego mapowania, w którym się znajduje.

Na przykład:

Użytkownik przypisany jest do grup A i B. Dla grupy B, zdefiniowane jest mapowanie z połączeniem `Sejf RDP` i przypisanymi źródłami uwierzytelnienia `CERB` i `Radius`. Grupa A, mapowana jest w drugiej kolejności, na połączenie `Sejf SSH` i ma przypisane źródło uwierzytelnienia `AD`.



Wheel Fudo PAM uwierzytelniając użytkownika będzie wysyłać zapytania do zewnętrznych źródeł uwierzytelniania w następującej kolejności:

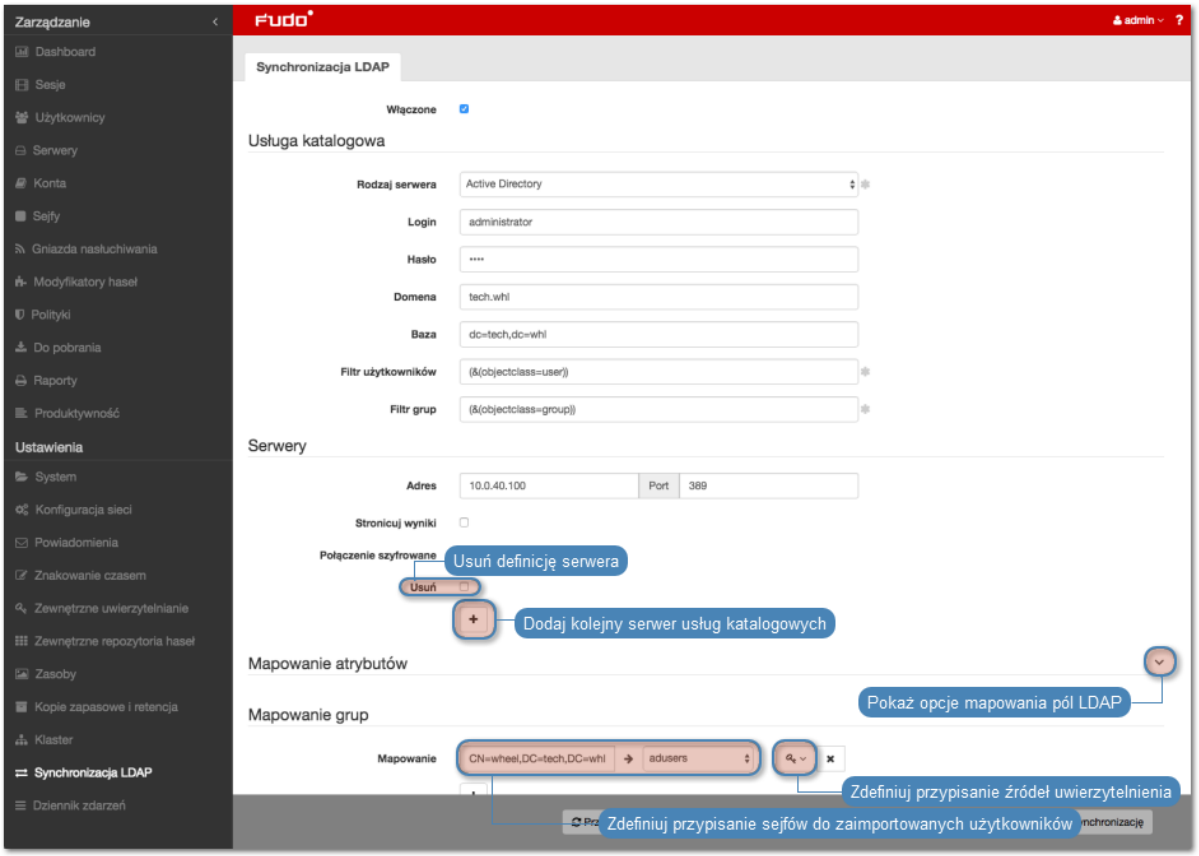
1. CERB.
2. Radius.
3. AD.

---

14. Kliknij *Zapisz*.

Informacja: Opcja *Wymuś pełną synchronizację* pozwala na przetworzenie zmian po stronie serwera usług katalogowych, które nie są odwzorowywane w procesie okresowej synchronizacji, tj. usunięcie zdefiniowanej grupy, lub usunięcie obiektu użytkownika.

Pełna synchronizacja wyzwalana jest automatycznie raz na dobę, w czasie do 5 minut po godzinie 00:00.



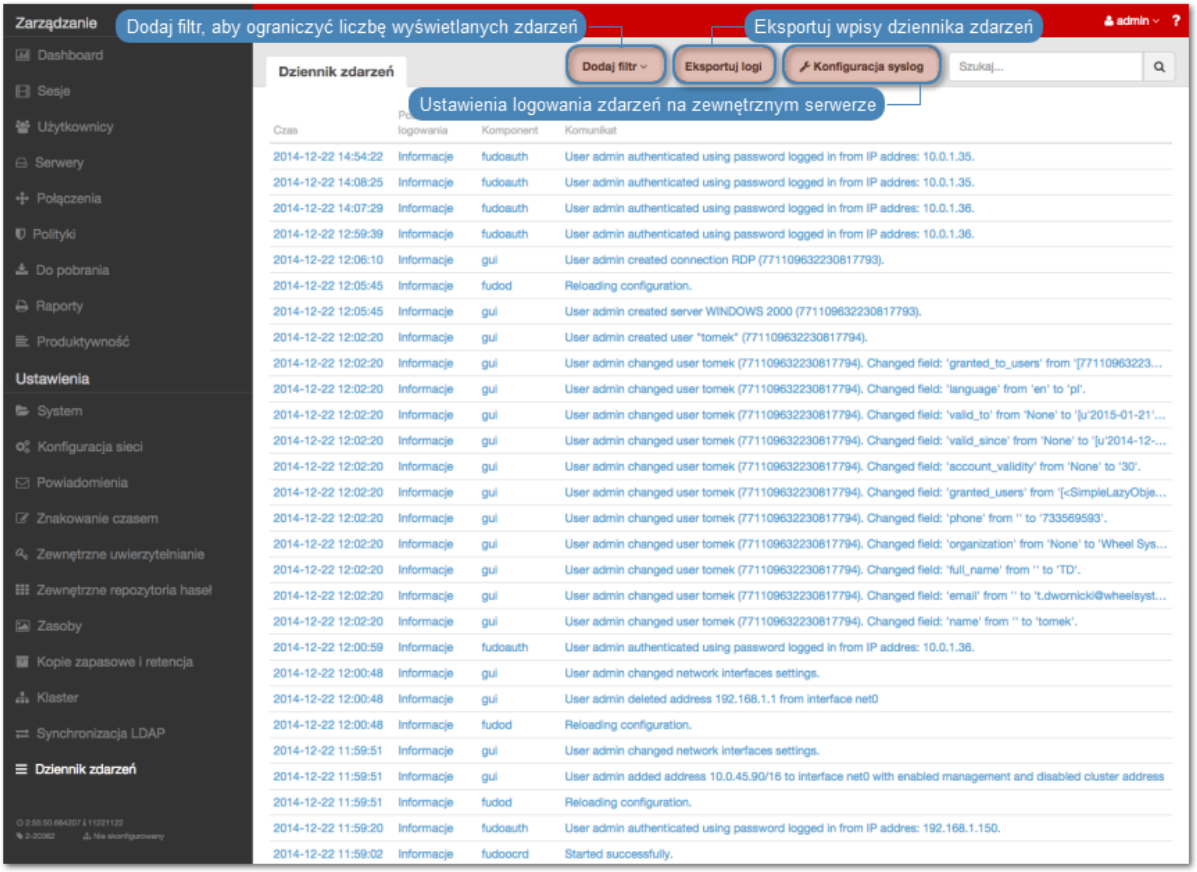
Tematy pokrewne:

- *Model danych*
- *Zarządzanie użytkownikami*
- *Zarządzanie serwerami*
- *Gniazda nasłuchiwania*

6.14 Dziennik zdarzeń

Dziennik zdarzeń stanowi wewnętrzny zapis akcji użytkowników mających wpływ na stan systemu (logowanie użytkowników, czynności administracyjne, itp.).

W celu wyświetlenia listy zdarzeń, wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.



Zewnętrzne serwery syslog

Wheel Fudo PAM pozwala na przesyłanie rejestrowanych zdarzeń do zewnętrznych serwerów syslog.

Dodawanie serwera Syslog

Aby skonfigurować usługę rejestrowania zdarzeń na zewnętrznych serwerach *Syslog*, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Konfiguracja syslog*, aby wyświetlić opcje konfiguracji rejestrowania zdarzeń na serwerach syslog.
3. Zaznacz opcję *Włącz logowanie zdarzeń na serwerach syslog*.
4. Kliknij *+*.
5. Wprowadź adres IP oraz numer portu serwera syslog.
6. Kliknij *Zapisz*.

Informacja: Wpisy dziennika zdarzeń przesyłane do serwerów syslog, przyjmują następującą postać:

```
[<poziom_logowania>] (<nazwa_komponentu>) (nazwa_obiektu: id_obiektu)
<treść_komunikatu>
```

Na przykład:

```
[INFO] (fudordp) (fudo_server: 848388532111147015) (fudo_session:
```

```
848388532111147219)          (fudo_user:  848388532111147012) (fudo_connection:
848388532111147014)    User user0 authenticated using password logged in from IP
addres:  10.0.40.101.
```

Lista komponentów

Komponent
cfuploadcert
cluster
confapply
confget
confimport
confset
datasendd
dbconfd
dbrecvd
dbsendd
eventd
fudoauth
fudod
fudodump
fudogeneric
fudohttp
fudomail
fudomysql
fudoocrd
fudooracle
fudordp
fudoretention
fudossh
fudossl
fudotelnet
fudotn3270
fudovnc
license
notify
pmonitor
timestampd
upgrade

Lista obiektów

Obiekt
fudo_configuration
fudo_connection
fudo_connection_attribute
fudo_connection_grant
fudo_connection_network
fudo_erpm

Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

Obiekt
fudo_external_authentication
fudo_http_request
fudo_ldap_address
fudo_ldap_connection
fudo_ldap_server
fudo_ldap_server_external_authentication_method
fudo_log_entry
fudo_log_object
fudo_node
fudo_node_replication
fudo_notification_filter
fudo_policy
fudo_regexp
fudo_regexp_policy
fudo_sensitive_feature_user
fudo_server
fudo_server_attribute
fudo_server_connection
fudo_server_grant
fudo_session
fudo_session_access
fudo_session_attribute
fudo_session_comment
fudo_session_event
fudo_session_share
fudo_session_text
fudo_user
fudo_user_attribute
fudo_user_authentication_method
fudo_user_connection
fudo_user_grant
reports_definedreport
reports_definedreportfilter
reports_definedreportsubscription
reports_report
reports_reportcriteria

Modyfikowanie serwera Syslog

Aby zmodyfikować definicję serwera *Syslog*, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Konfiguracja syslog*, aby wyświetlić opcje konfiguracji rejestrowania zdarzeń na serwerach syslog.
3. Wyszukaj żądaną definicję serwera syslog i zmień żądaną wartość parametru.
4. Kliknij *Zapisz*.

Usuwanie serwera Syslog

Aby usunąć serwer *Syslog*, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Konfiguracja syslog*, aby wyświetlić listę zdefiniowanych serwerów Syslog.
3. Wyszukaj i zaznacz żądany wpis.
4. Kliknij *Zapisz*.

Eksportowanie dziennika zdarzeń

Aby wyeksportować zdarzenia zapisane w dzienniku zdarzeń, postepuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Eksportuj logi*, i wskaż miejsce, w którym zostanie zapisany plik z logami.

Tematy pokrewne:

- *Bezpieczeństwo*
- *Zarządzanie serwerami*

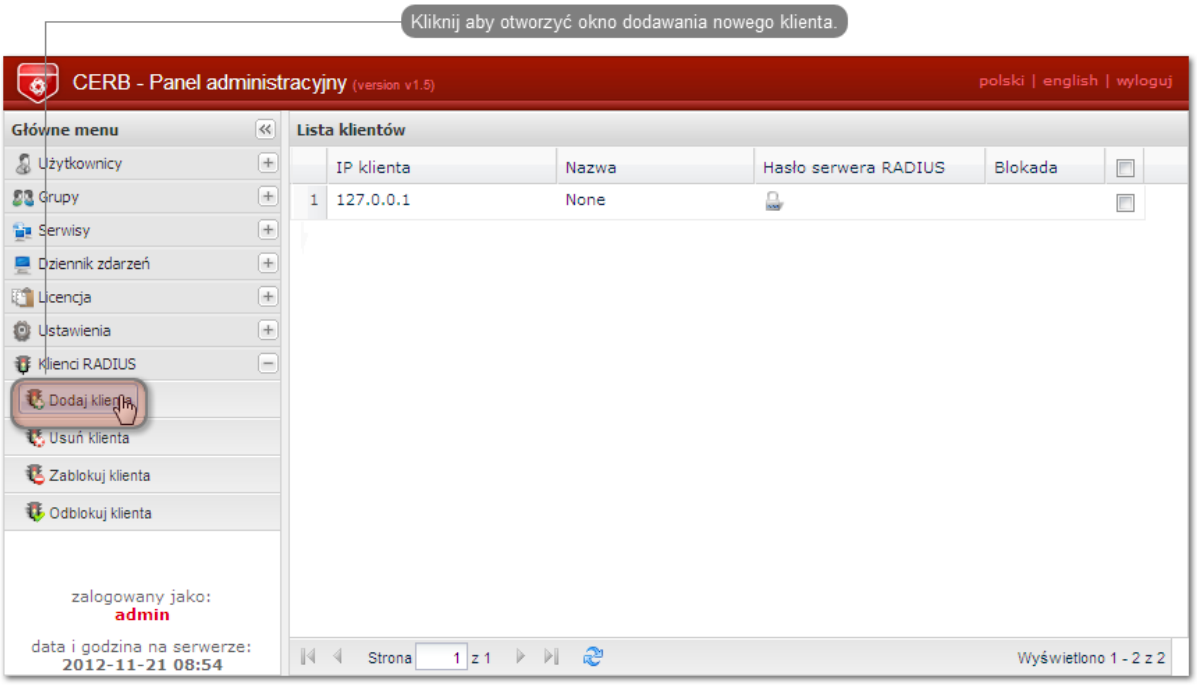
6.15 Integracja z serwerem CERB

CERB jest zewnętrznym serwerem uwierzytelniania wspierającym wiele mechanizmów weryfikacji tożsamości użytkowników (tj. token mobilny czasowy i zdarzeniowy, hasła jednorazowe, itp.). Poniższa instrukcja przestawia kroki konfiguracyjne jakie należy przeprowadzić aby użytkownicy nawiązujący połączenia zdalne za pośrednictwem Wheel Fudo PAM, uwierzytelniany byli przez zewnętrzny serwer CERB.

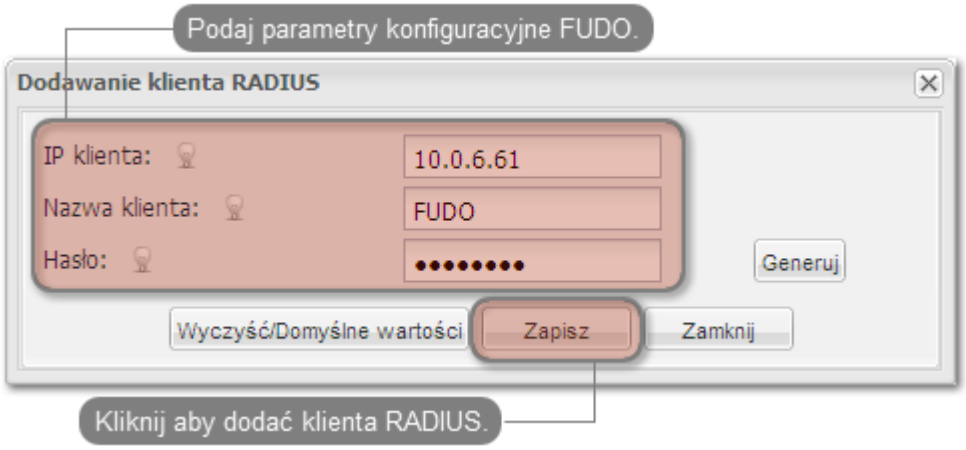
Konfiguracja serwera CERB

1. Dodanie klienta RADIUS.

- Wybierz z lewego menu *Klienci RADIUS* > *Dodaj klienta*, aby dodać Wheel Fudo PAM jako klienta RADIUS.



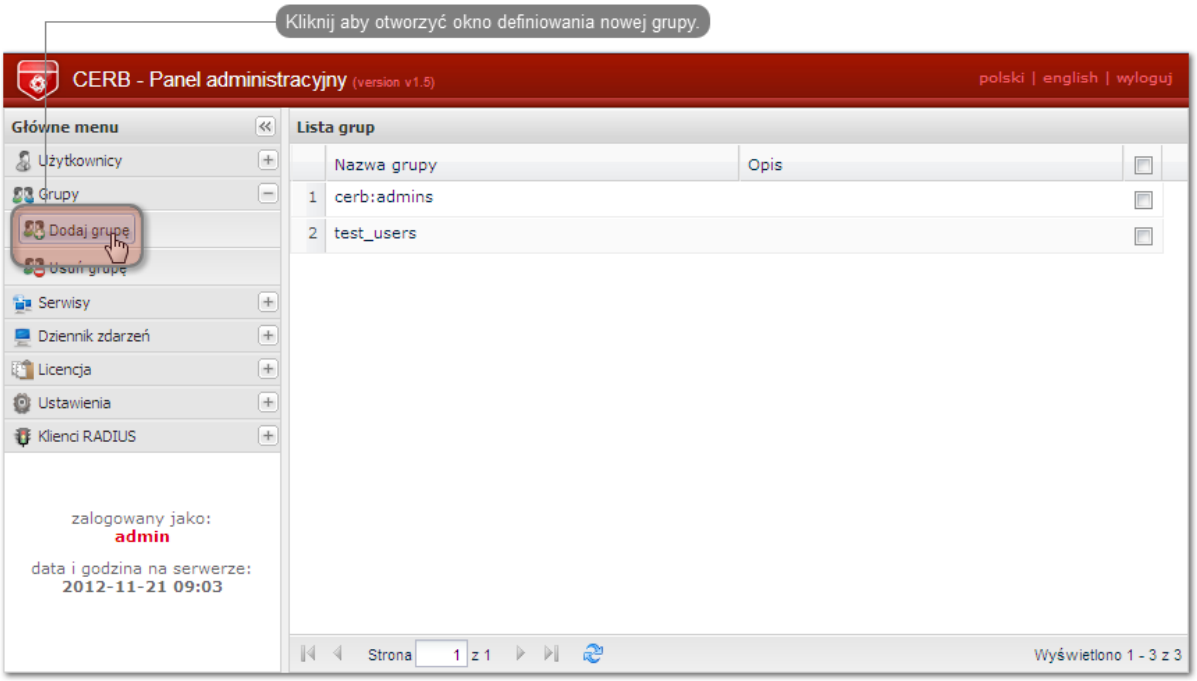
- Podaj adres IP serwera Wheel Fudo PAM, nazwę klienta oraz hasło i kliknij *Zapisz*.



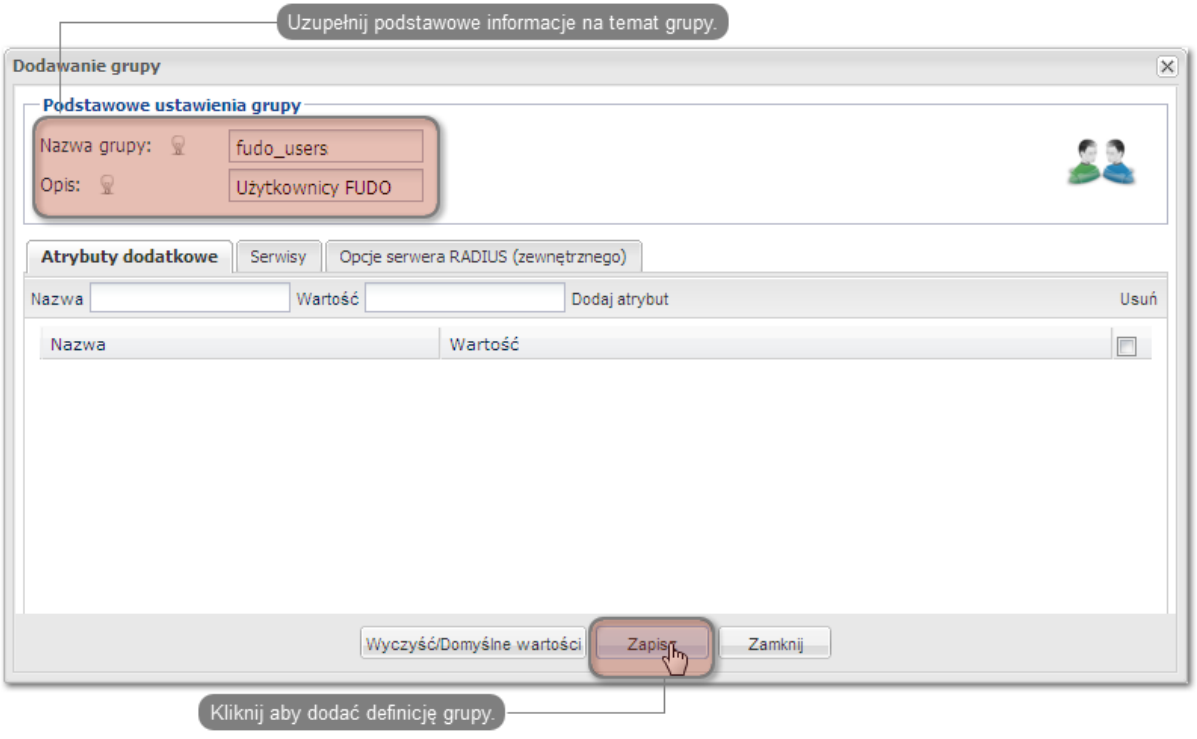
Informacja: Hasło będzie wymagane do skonfigurowania zewnętrznego serwera uwierzytelniania w panelu administracyjnym Wheel Fudo PAM.

2. Dodanie grupy użytkowników.

- Wybierz z lewego menu *Grupy* > *Dodaj grupę*, aby zdefiniować grupę użytkowników Wheel Fudo PAM, którzy będą autoryzowani poprzez serwer CERB.

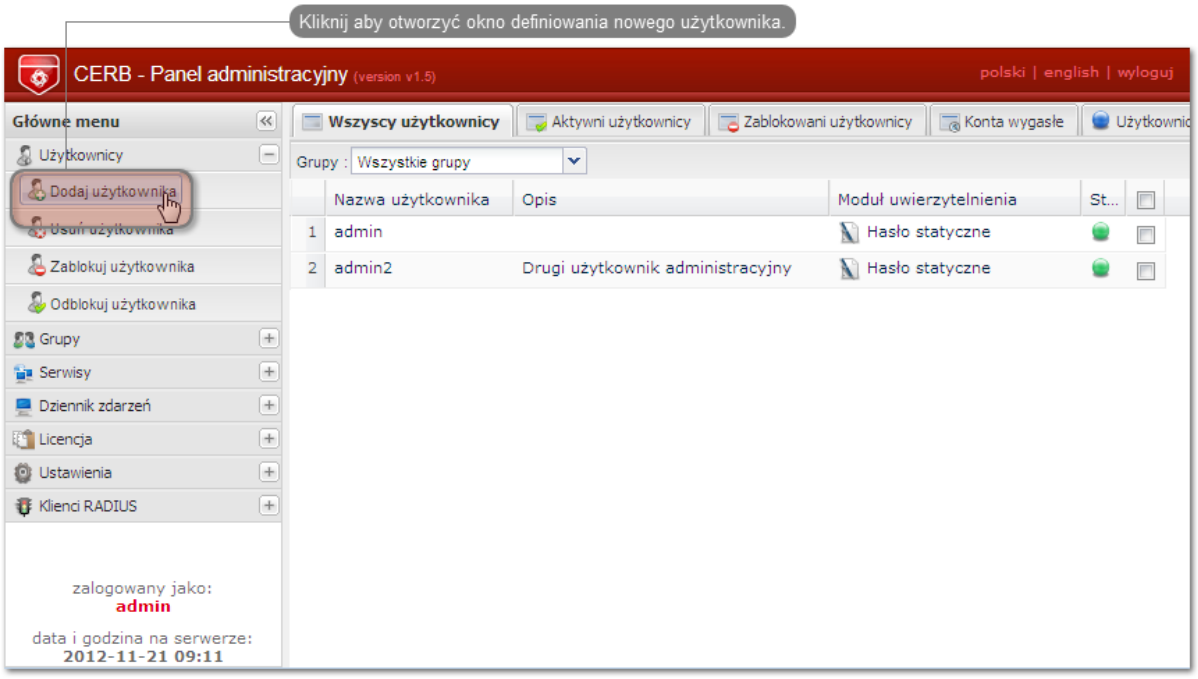


- Podaj nazwę grupy (`fudo_users`) i kliknij *Zapisz*.

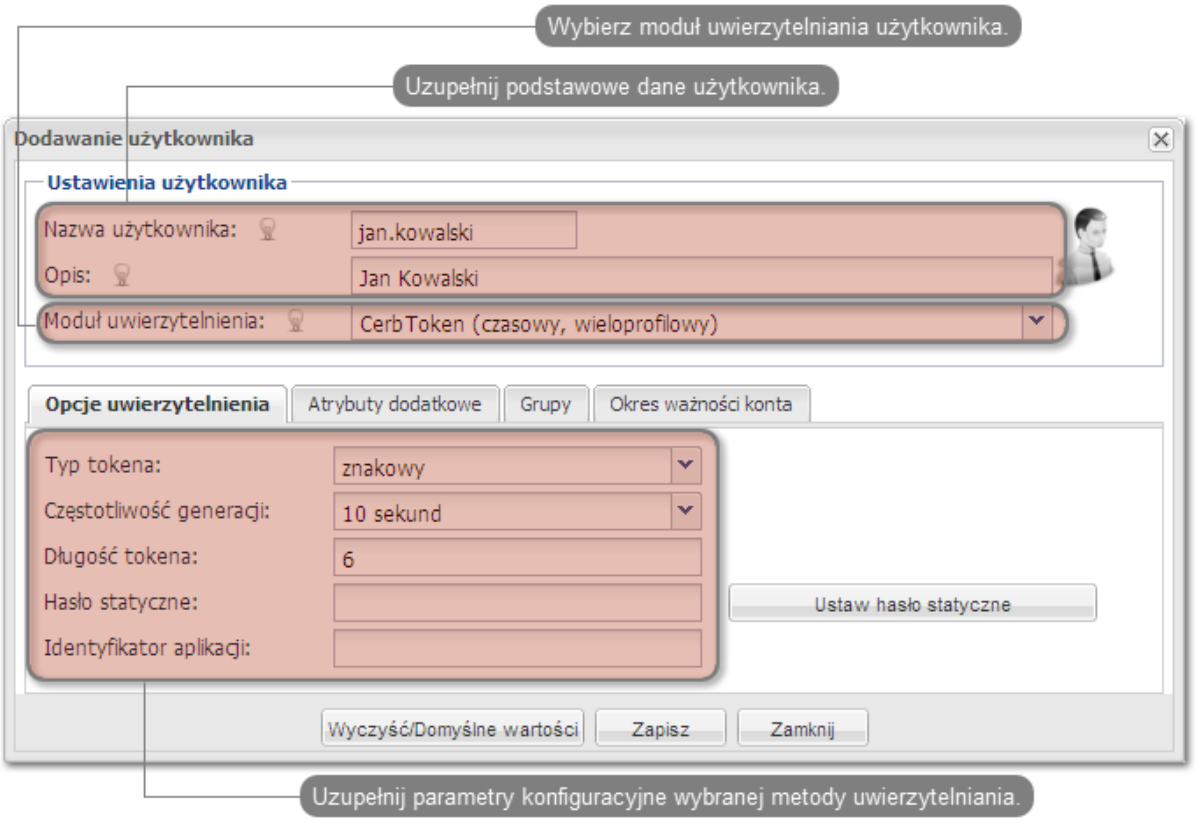


3. Dodanie użytkownika.

- Wybierz z lewego menu *Użytkownicy* > *Dodaj użytkownika*, aby otworzyć okno definiowania nowego użytkownika.

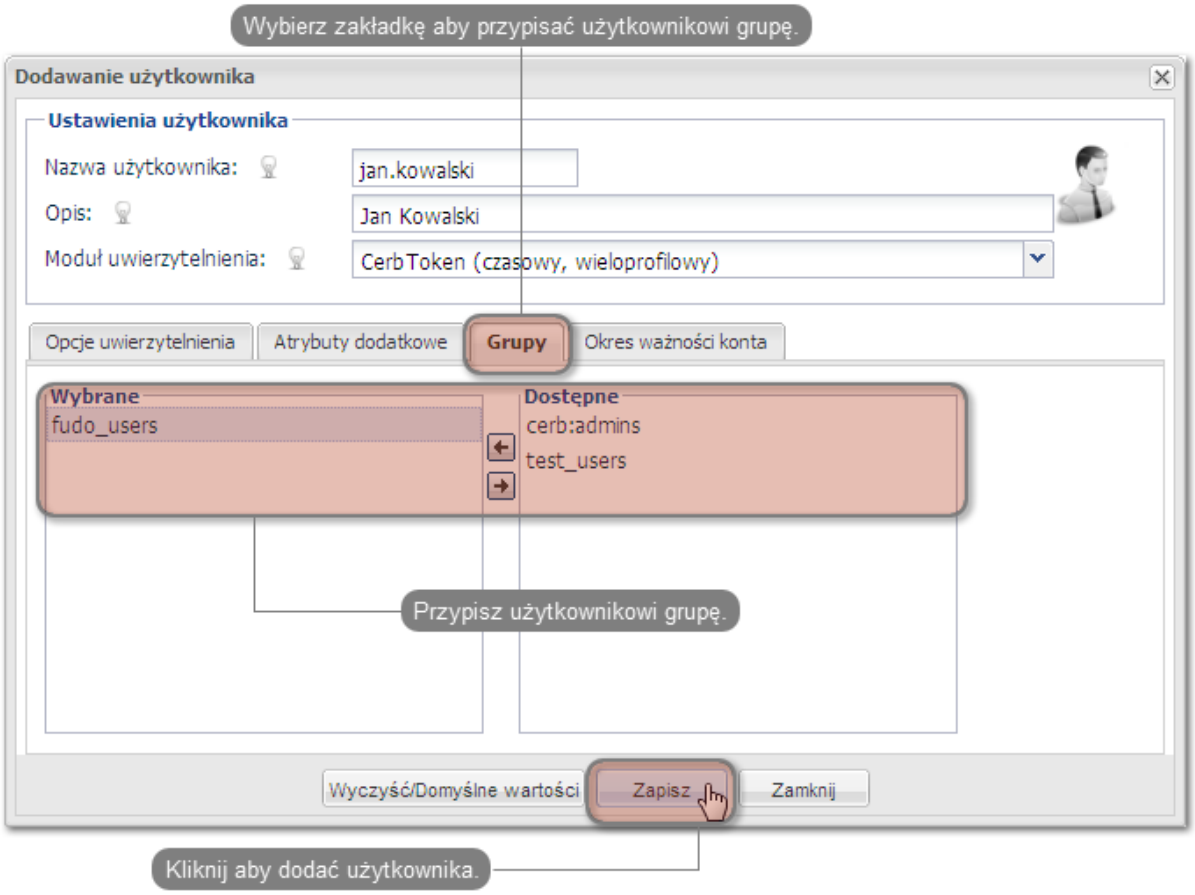


- Podaj nazwę użytkownika, opis oraz wybierz stosowny moduł uwierzytelniania (więcej informacji na temat modułów uwierzytelniania znajdziesz w dokumentacji serwera CERB).



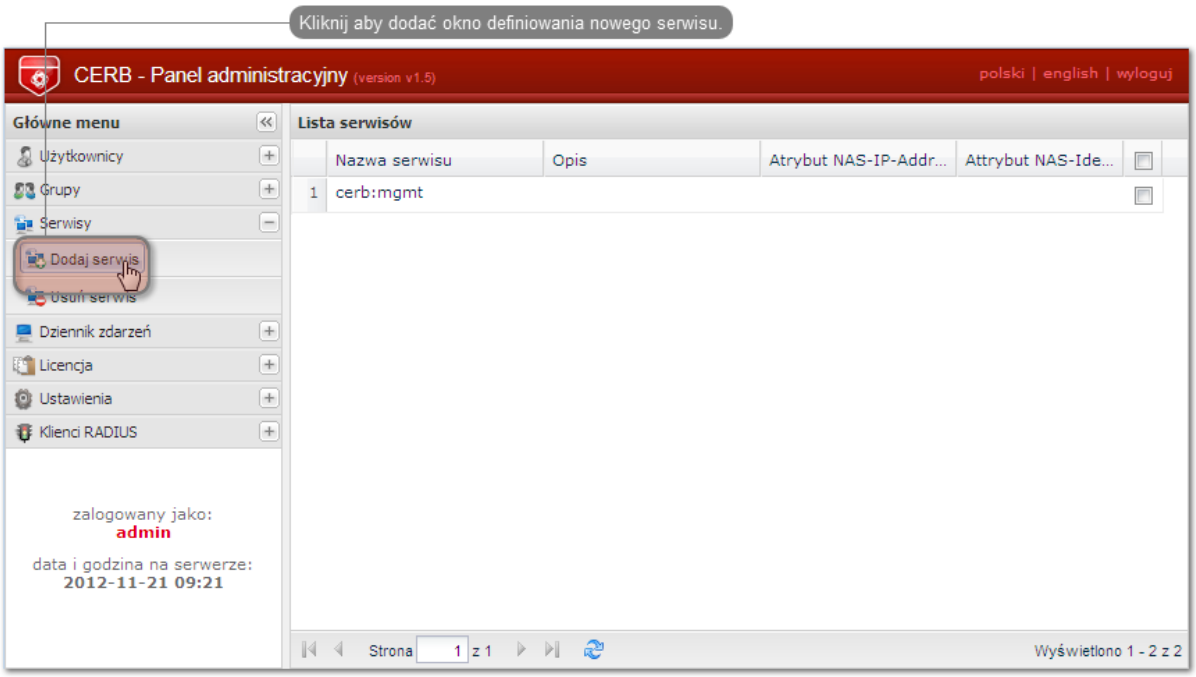
Informacja: Nazwa użytkownika wykorzystywana jest w procesie uwierzytelniania użytkowników łączących się z Wheel Fudo PAM.

- Przypisz do użytkownika wcześniej dodaną grupę `fudo_users` i kliknij *Zapisz*.

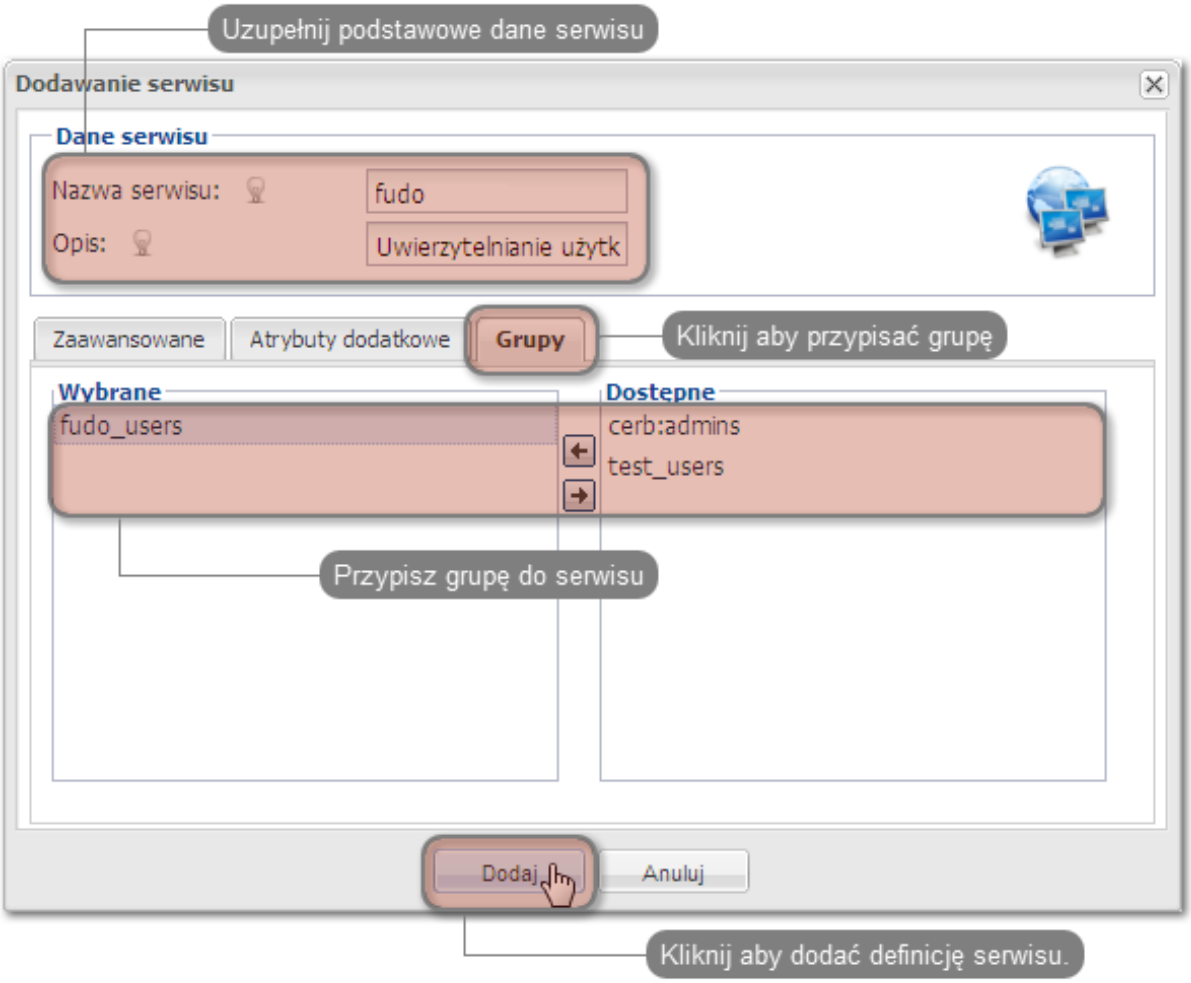


4. Skonfigurowanie serwisu.

- Wybierz z lewego menu *Serwisy* > *Dodaj serwis*, aby otworzyć okno definiowania nowego serwisu.



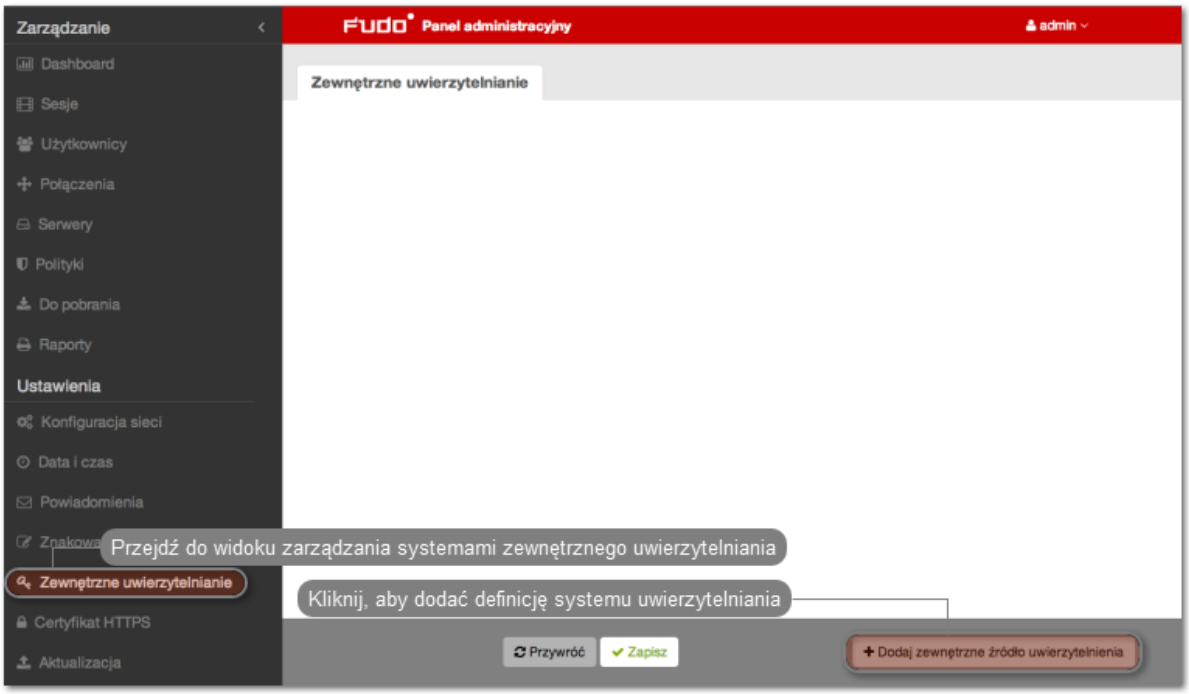
- Wpisz nazwę pod jaką identyfikowana będzie usługa uwierzytelniania (`cerb_fudo`) oraz opis serwisu.
- Dodaj do serwisu grupę `fudo_users` i kliknij *Dodaj*.



Konfiguracja serwera Wheel Fudo PAM

1. Dodanie serwera zewnętrznego uwierzytelniania CERB.

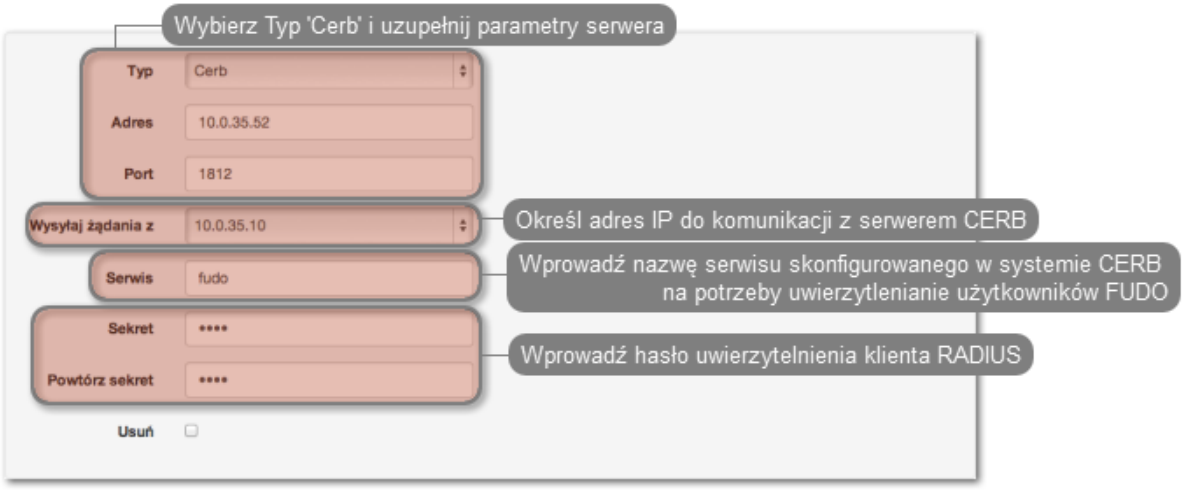
- Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
- Kliknij + *Dodaj zewnętrzne źródło uwierzytelnienia*, aby dodać definicję serwera CERB.



- Podaj adres IP serwera uwierzytelniania CERB, *sekret* oraz nazwę serwisu pod jaką identyfikowana będzie usługa uwierzytelniania.

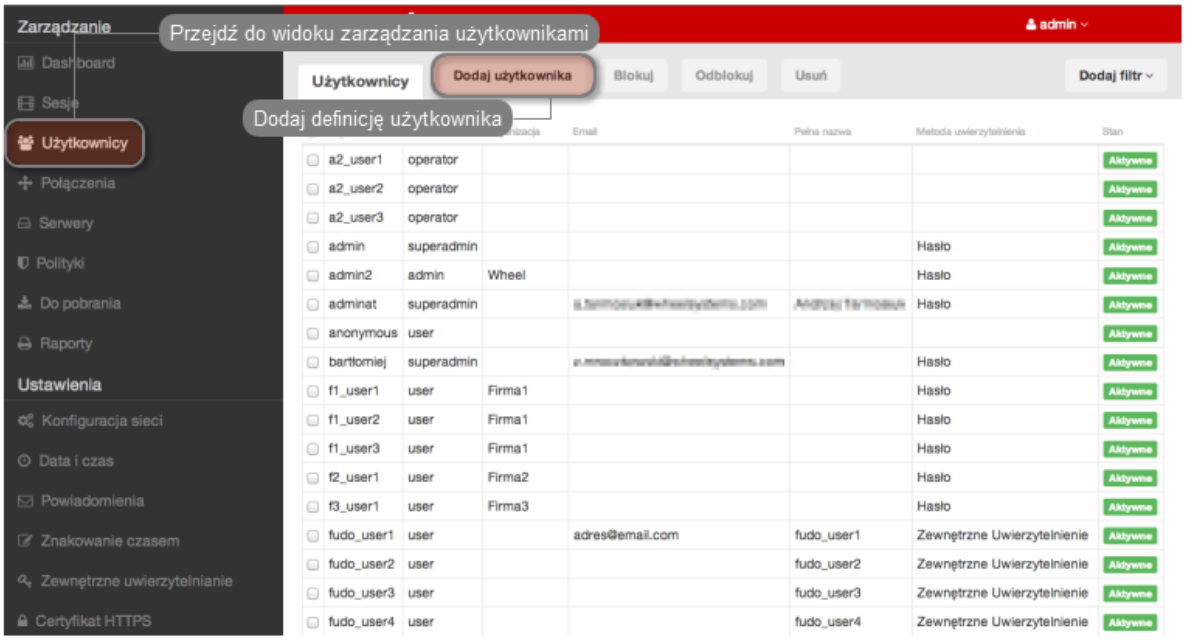
Informacja: Sekret odpowiada hasłu, które zostało podane przy konfigurowaniu klienta RADIUS na serwerze CERB. Nazwa serwisu musi być zgodna z nazwą nadaną przy konfigurowaniu serwisu na serwerze CERB.

- Kliknij *Zapisz*.



2. Dodanie użytkownika.

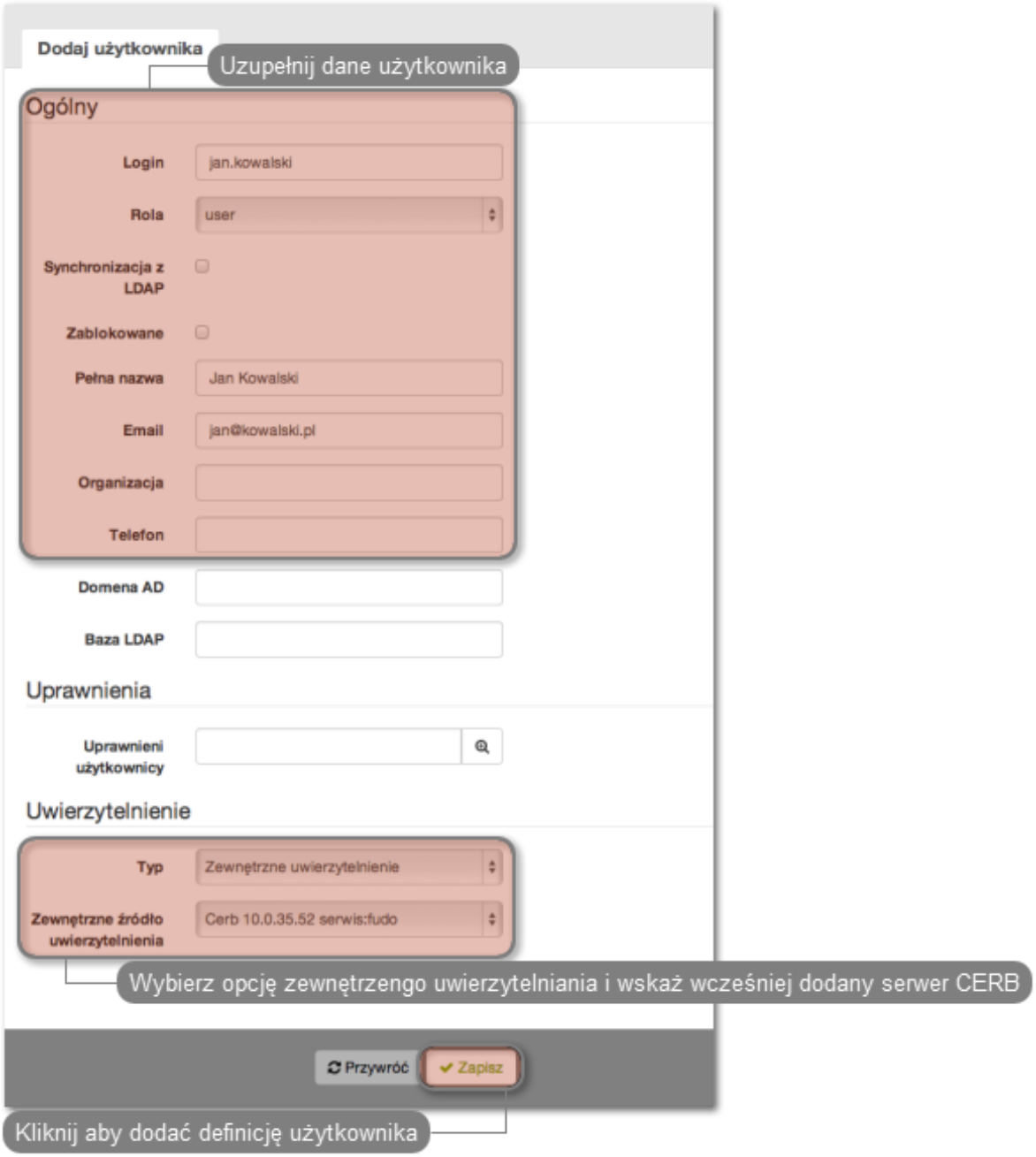
- Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
- Kliknij *+ Dodaj*.



- Podaj podstawowe dane użytkownika.

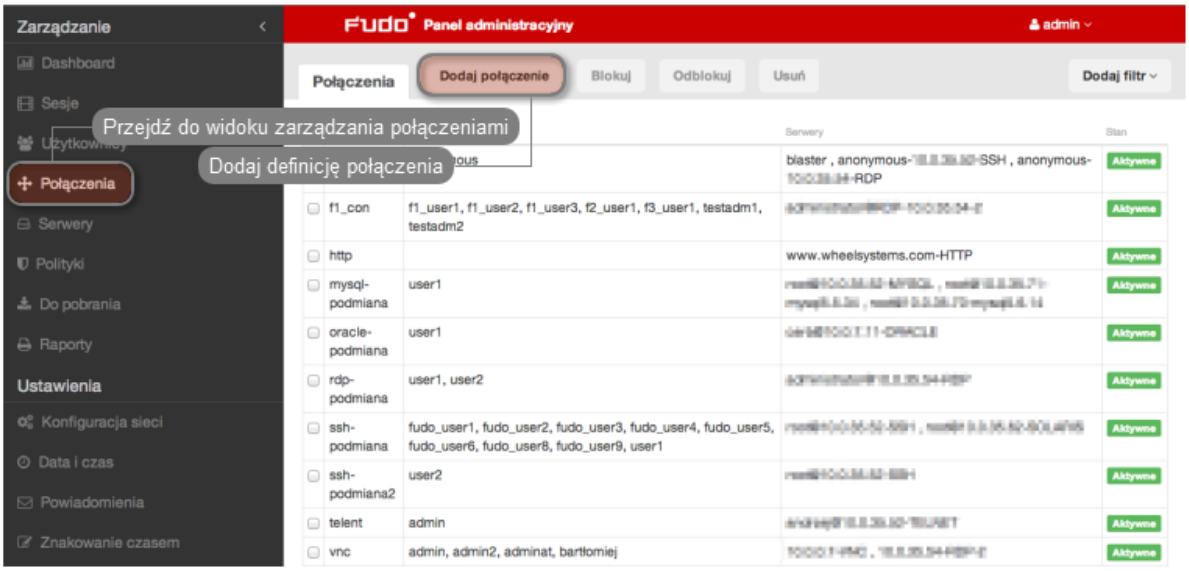
Informacja: Login użytkownika musi odpowiadać nazwie nadanej użytkownikowi na serwerze CERB.

- Z listy rozwijalnej wybierz `CERB` jako metodę uwierzytelniania i wskaż wcześniej dodany serwer uwierzytelniania.
- Kliknij *Zapisz*.

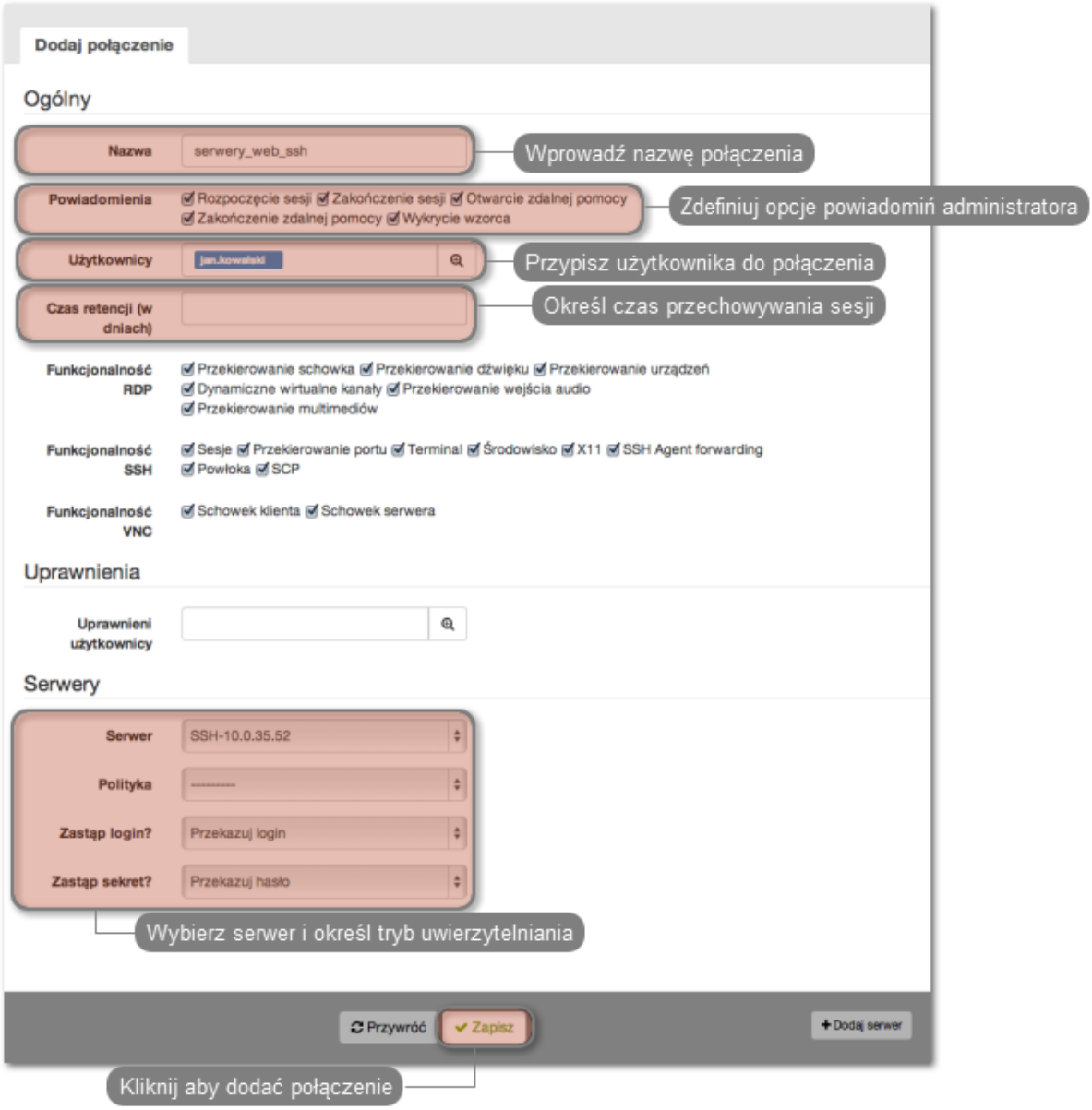


3. Dodanie połączenia.

- Wybierz z lewego menu *Zarządzanie* > *Połączenia*.
- Kliknij + *Dodaj*.



- Podaj podstawowe parametry połączenia.
- Wybierz z listy wcześniej dodanego użytkownika.
- Wybierz serwer, z którym użytkownik będzie się łączył w ramach tego połączenia.
- Wybierz tryb uwierzytelniania użytkownika (*Tryby uwierzytelniania*).
- Kliknij *Zapisz*.



Tematy pokrewne:

- *Zarządzanie użytkownikami*
- *Konfigurowanie serwerów uwierzytelniania*
- *Metody i tryby uwierzytelniania użytkowników*

6.16 Czynności serwisowe

Poniższy rozdział zawiera opisy czynności serwisowych.

6.16.1 Monitorowanie stanu systemu

Monitorowanie stanu Wheel Fudo PAM pozwala zapewnić prawidłową pracę systemu i zapobiegać przeciążeniom i awariom.

Monitorowanie aktywnych sesji

1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM.
2. Wybierz z lewego menu *Zarządzanie* > *Dashboard*.
3. Sprawdź bieżącą liczbę aktualnie aktywnych połączeń użytkowników.

Informacja: Konfiguracja Wheel Fudo PAM pozwala na jednoczesną obsługę 300 połączeń RDP.

Monitorowanie przepustowości łącza sieciowego

1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM.
2. Wybierz z lewego menu *Zarządzanie* > *Dashboard*.
3. Sprawdź bieżącą aktywność interfejsów sieciowych.

Informacja: Wheel Fudo PAM jest wyposażone w interfejsy sieciowe o przepustowości 1Gbps. W przypadku gdy bieżąca wartość transferu przekracza 500Mbps, użytkownicy mogą zauważyć spadek wydajności komunikacji z systemem.

Tematy pokrewne:

- *Dziennik zdarzeń*
- *Często zadawane pytania*

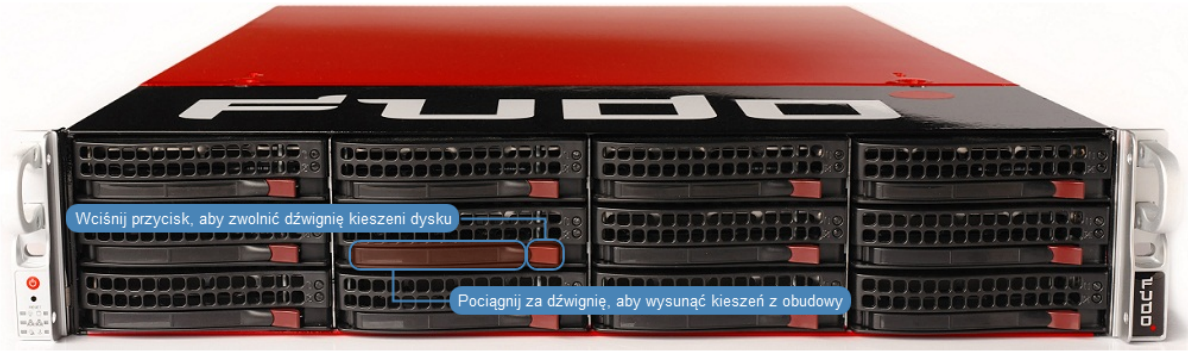
6.16.2 Wymiana dysku macierzy

W domyślnej konfiguracji, macierz dyskowa Wheel Fudo PAM składa się z 12 dysków twardych a zastosowany system plików pozwala na kontynuowanie świadczenia usług w przypadku awarii dwóch nośników.

Wymiana dysku macierzy

1. Przesuń w lewo dźwignię zwalniającą przedni panel, aby zdjąć go z obudowy.

2. Wciśnij przycisk zwalniający dźwignię kieszeni dysku twardego i pociągnij za dźwignię, aby wyjąć kieszeń z obudowy.



3. Odkręć śruby mocujące dysk twardy i wyjmij dysk z kieszeni.
4. Włóż nowy dysk twardy i wkręć śruby mocujące.
5. Włóż kieszeń z dyskiem twardym do serwera.

Informacja: System automatycznie wykryje zmianę stanu macierzy i przystąpi do odbudowywania struktury danych. Czas trwania procesu zależy od liczby danych przechowywanych w systemie.

Tematy pokrewne:

- *Urządzenie*

- *Często zadawane pytania*

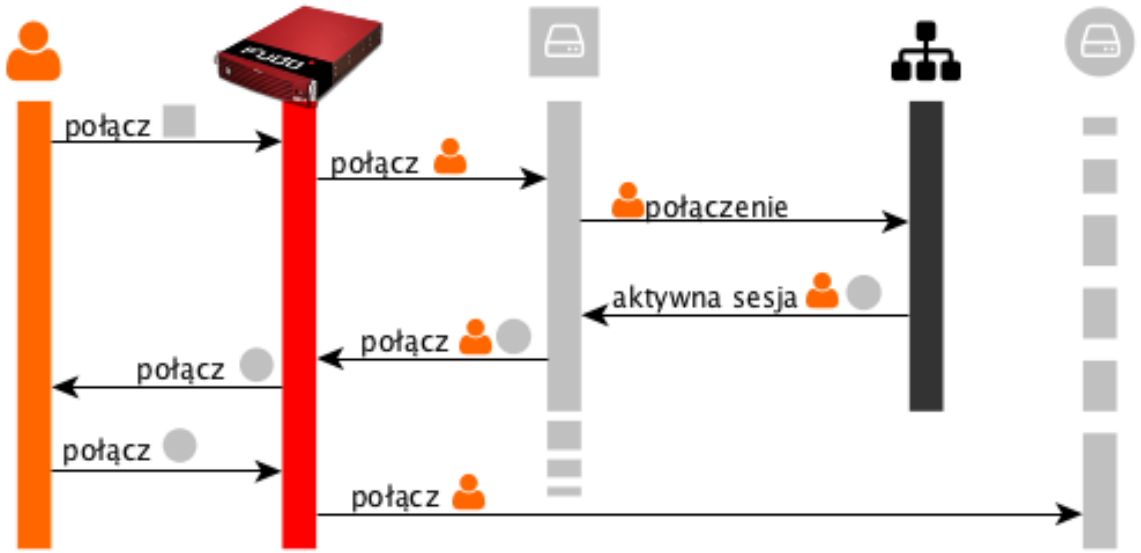
ROZDZIAŁ 7

Informacje uzupełniające

7.1 Broker połączeń RDP

Broker połączeń zdalnych umożliwia ponowne połączenie do istniejącej sesji w farmie serwerów z mechanizmem balansowania obciążeniem.

Jeśli broker stwierdzi aktywną sesję użytkownika na serwerze innym niż ten, z którym się połączył, połączenie zostanie przekierowane na serwer z istniejącą aktywną sesją a użytkownik zostanie poproszony o ponowne uwierzytelnienie.



Informacja: Aby proces przekierowania użytkownika się powiódł, wskazany przez broker serwer, musi być zdefiniowany na Fudo i nasłuchiwać na domyślnym porcie RDP (3389) a użytkownik musi być uprawniony do łączenia się z tym zasobem.

Tematy pokrewne:

- *Model danych*
- *RDP*
- *Zarządzanie serwerami*
- *Zarządzanie połączeniami*

7.2 Kody błędów

Kod błędu	Treść komunikatu i opis
FSE0001	*Internal system error*
FSE0002	*FUDO certificate error.*
FSE0003	*Unable to change configuration settings.*
FSE0004	*Configuration import error*
FSE0005	*Unable to initialize ${disk}.* Wymień dysk twardy, który sygnalizuje błąd. **Informacja:** Numeracja dysków zaczyna się od 0. Jeżeli błąd zgłasza dysk numer 1, fizycznie jest to drugi dysk w górnym rzędzie.
FSE0006	*Invalid license*
FSE0007	*Unable to find license file* System nie mógł zlokalizować licencji. Wgraj ponownie plik licencji zgodnie z procedurą opisaną w rozdziale *Administracja > System > Licencja*. Jeśli problem będzie się powtarzał skontaktuj się z działem wsparcia technicznego.
FSE0008	*Unable to attach hard drive ${disk}.*
FSE0009	*Upgrade failed.* Wystąpił błąd w procedurze aktualizacji systemu. Wgraj raz jeszcze plik z aktualizacją i ponownie wywołaj procedurę aktualizacji. Jeśli problem się powtórzy, skontaktuj się z działem wsparcia technicznego.
FSE0010	*License expired.* Skontaktuj się z działem wsparcia technicznego, aby otrzymać nową licencję.
FSE0020	*System backup error.*
FSE0024	*Hard drive belongs to another FUDO (${diskserial}) ${disk}.* Wskazany dysk twardy pochodzi z innej instancji Wheel Fudo PAM. Wymień dysk na właściwy. **Informacja:** Numeracja dysków zaczyna się od 0. Jeżeli błąd zgłasza dysk numer 1, fizycznie jest to drugi dysk w górnym rzędzie.
FSE0026	*Cluster communication error.*
FSE0028	*Unable to join node to cluster.*
FSE0031	*Timestamping service communication error*

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod błędu	Treść komunikatu i opis
FSE0032	*Unable to timestamp session.*
FSE0033	*Unknown timestamping service provider.*
FSE0040	*Cluster communication error. Local FUDO version is %s than %s FUDO version.*
FSE0046	*There is no filter called %s.*
FSE0048	*Error authenticating user over RADIUS.*
FUE0057	*Authentication method «password», required by MySQL, requested by the user %s, logging in from IP address %s, was not found.*
FUE0058	*Authentication method «password», required by MySQL, requested by the user %s, was not found.*
FSE0061	*Incorrect password repository configuration: login is empty.*
FSE0062	*Incorrect password repository configuration: password is empty.*
FSE0063	*Incorrect server configuration: ERPM namespace is empty.*
FSE0064	*Incorrect server configuration: ERPM name is empty.*
FSE0065	*License configuration error.*
FSE0066	*Unable to block user %jd.*
FSE0067	*Error connecting to Lieberman ERPM server %s: incorrect URL in configuration.*
FSE0068	*Error connecting to Lieberman ERPM server %s: incorrect protocol specified.*
FSE0069	*Error fetching password from Lieberman ERPM server %s: unable to get sessid for user %s.*
FSE0070	*Error fetching password from Lieberman ERPM server %s: unable to get password for user %s for the %s/%s server.*
FSE0076	*Unable to establish connection, could not find specified transparent server (tcp://%s:%u).*
FSE0077	*LDAP authentication error.*
FSE0078	*LDAP authentication error: unable to connect from %s to %s.*
FUE0079	*Authentication timeout after %ju key attempt%s and %ju password attempt%s.*
FUE0080	*Authentication timeout after %lu key attempt%s.*
FUE0081	*Authentication timeout after %lu password attempt%s.*
FSE0082	*Unable to establish connection to server %s (%s).*
FSE0083	*Unable to establish connection from %s to server %s (%s).*
FUE0089	*Authentication timeout.*
FSE0090	*Unable to connect to the passwords repository server %s.*
FSE0091	*Unable to add server %s.*
FSE0092	*Passwords repository server %s communication error.*
FSE0093	*Error connecting to Thycotic server %s: incorrect URL in configuration.*
FSE0094	*Error connecting to Thycotic server %s: incorrect protocol specified.*
FSE0095	*Error fetching password from Thycotic server %s: unable to get sessid for user %s.*
FSE0096	*Error fetching password from Thycotic server %s.*
FSE0097	*Error fetching password from Thycotic server %s: unable to get secretid for server %s.*
FSE0098	*Error fetching password from Thycotic server %s: unable to get password for user %s for the %s server.*

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod błędu	Treść komunikatu i opis
FUE0099	*Connection terminated.*
FUE0101	*Unable to find matching HTTP connection.*
FUE0103	*HTTP connection error.*
FUE0106	*Authentication failed: %s.*
FUE0108	*MySQL connection error.*
FUE0110	*Oracle connection error.*
FUE0112	*RDP connection error.*
FUE0113	*TLS Security configured, but missing TLS private key.*
FUE0114	*TLS Security configured, but missing TLS certificate.*
FUE0115	*Standard RDP Security configured, but missing private key.*
FUE0116	*TLS certificate verification failed.*
FUE0117	*RSA key verification failed.*
FUE0124	*SSH connection error.*
FUE0125	*User %s failed to authenticate after %d attempts, disconnecting.*
FUE0127	*Invalid authentication method: expected passwordor sshkey, got %s.*
FUE0129	*Failed to authenticate against the server as user %s using %s.*
FUE0130	*Failed to authenticate against the server as user %s using %s (received %s).*
FUE0132	*Client requested incorrect terminal dimensions (%dx%d).*
FUE0133	*MSSQL connection error.*
FUE0134	*TN3270 connection error.*
FUE0135	*Unknown TN3270 command: %02x.*
FUE0136	*Telnet connection error.*
FSE0137	*Unable to read private key.*
FSE0138	*Server's certificate does not match configured certificate.*
FUE0139	*VNC connection error.*
FUE0140	*Client version: %s is higher than the client integrated in FUDO: %s.*
FUE0141	*VNC connection error. Client answered with unsupported security type: %hhu.*
FUE0142	*VNC connection error. Server version: %s is lower than client version: %s.*
FUE0144	*User %s failed to authorize logging in from IP address: %s.*
FUE0145	*User %s failed to authorize.*
FUE0146	*User %s failed to authenticate logging in from IP address: %s.*
FUE0147	*User %s failed to authenticate.*
FSE0148	*Listening on %s:%u failed while adding bastion %s.*
FAE0153	*Session indexing failure.*
FAE0154	*Session conversion failure for session %s.*
FAE0165	*Error authenticating user <user_name>.*
FAE0189	*Error saving NTP servers: <server_name>.*
FAE0232	*MySQL session playback error.*
FAE0267	*Error generating report %d: %s.*
FSE0283	*Unable to process pattern: %s.*
FSE0285	*Unable to read certificate.*
FSE0286	*No peer certificate received.*
FSE0290	*Unable to add server %s because %s is listening on same IP address and port.*

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod błędu	Treść komunikatu i opis
FUE0305	*Client connection closed: encryption is not available.*
FUE0306	*Client connection closed.*
FSE0307	*Error fetching password from HiPAM server %s: unable to get sessid for user %s.*
FSE0308	*HiPAM server internal error.*
FSE0309	*Error fetching password from HiPAM server %s: unable to get sessdat for user %s.*
FSE0310	*Incorrect server configuration: HiPAM name is empty.*
FSE0311	*Unable to fetch password from HiPAM.*
FSE0312	*Error connecting to HiPAM server %s: incorrect URL in configuration.*
FSE0313	*Error connecting to HiPAM server %s: incorrect protocol specified.*
FUE0314	*Invalid pixel format.*
FUE0315	*Unable to fetch standard RDP certificate.*
FUE0316	*Protocol security negotiation failure.*
FUE0317	*Unable to establish connection to server %s.*
FUE0318	*Unable to fetch SSL certificate.*
FSE0330	*Bad login field configured on server. Error while processing user %s.*
FSE0331	*Error while processing userAccountControl value of user %s.*
FUE0346	*Client sent a packet bigger than %d bytes.*
FSE0347	*Cluster communication error. Local FUDO version: ${lversion}, remote FUDO version: ${rversion}.*
FSE0348	*Unable to get configuration settings.*
FUE0351	*Client sent unsupported NTLM v1 response.*
FSE0352	*Bastion requires login and server delimited with one of «%s» (%s).*
FSE0355	*Inconsistent data, starting recovery replication to node ${name}.*
FUE0359	*Server rejected X11 connection: %.*s.*
FUE0360	*Server requires unsupported X11 authentication: %.*s.*
FSE0362	*Unable to propagate ARP.*
FUE0363	*User %s has no access to host %s:%u.*
FUE0365	*RDP server %s:%u has to listen on the default RDP port in order to redirect sessions.*
FSE0366	*Error connecting to CyberArk server %s: incorrect URL in configuration.*
FSE0367	*Error connecting to CyberArk server %s: incorrect protocol specified.*
FSE0368	*Error fetching password from CyberArk server %s.*
FSE0369	*Error fetching password from CyberArk server %s: unable to get password for user %s for server %s.*
FSE0372	*Unable to invalidate OTP password %jd.*
FSE0375	*Unable to add listener %s.*
FSE0376	*Unable to add listener %s because %s is listening on same IP address and port.*
FSE0377	*Bastion requires login and server delimited with a «%s» character (login: %s).*
FSE0378	*Unable to establish connection, could not find a server (login: %s).*
FSE0379	*Unable to establish connection, could not find specified transparent server (tcp://%s:%u) (login: %s).*
FSE0380	*Unable to authenticate user %s: server is blocked.*
FSE0381	*Unable to authenticate user %s: account not found.*

Kontynuacja na następnej stronie

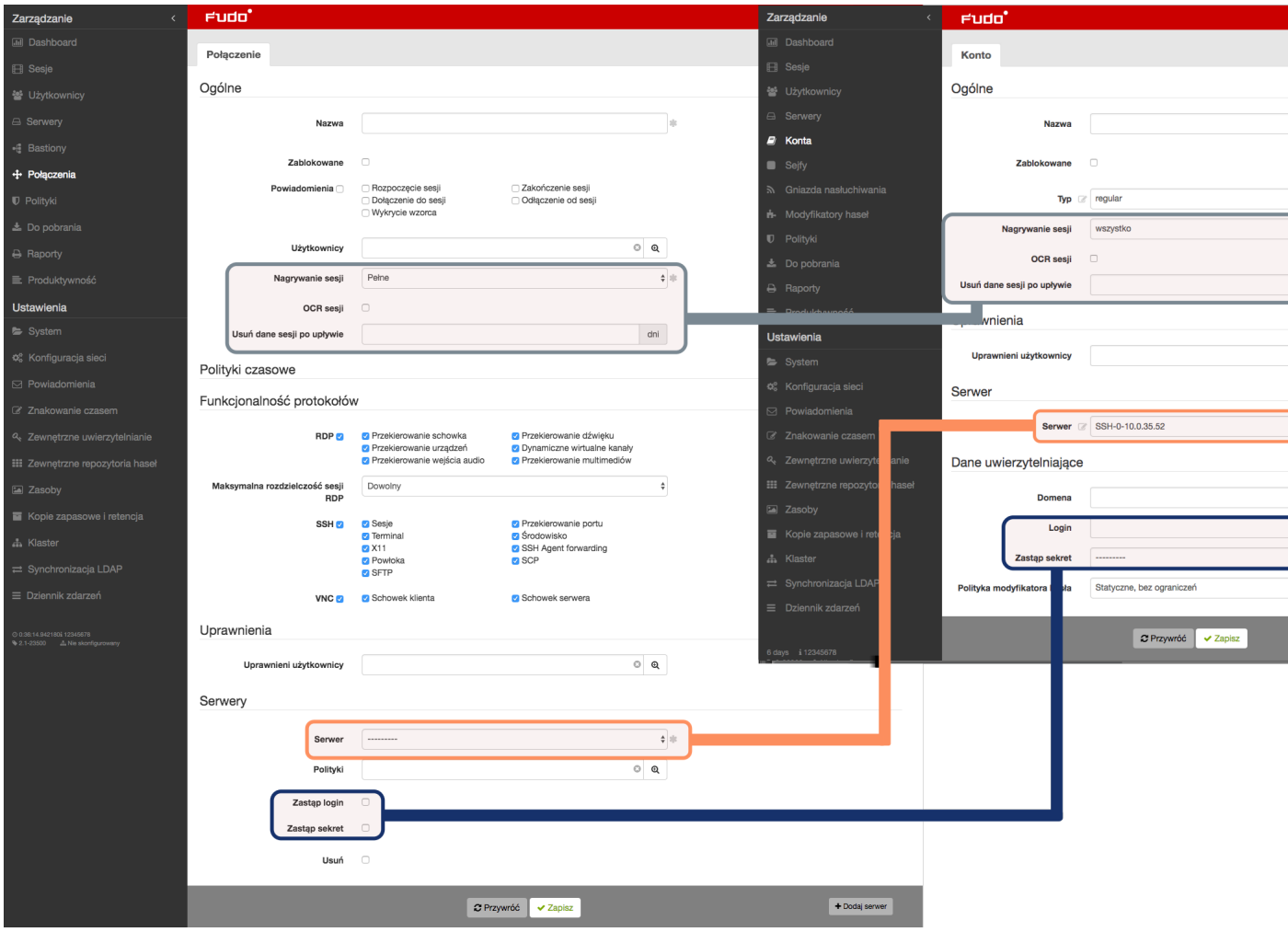
Tabela 1 – kontynuacja poprzedniej strony

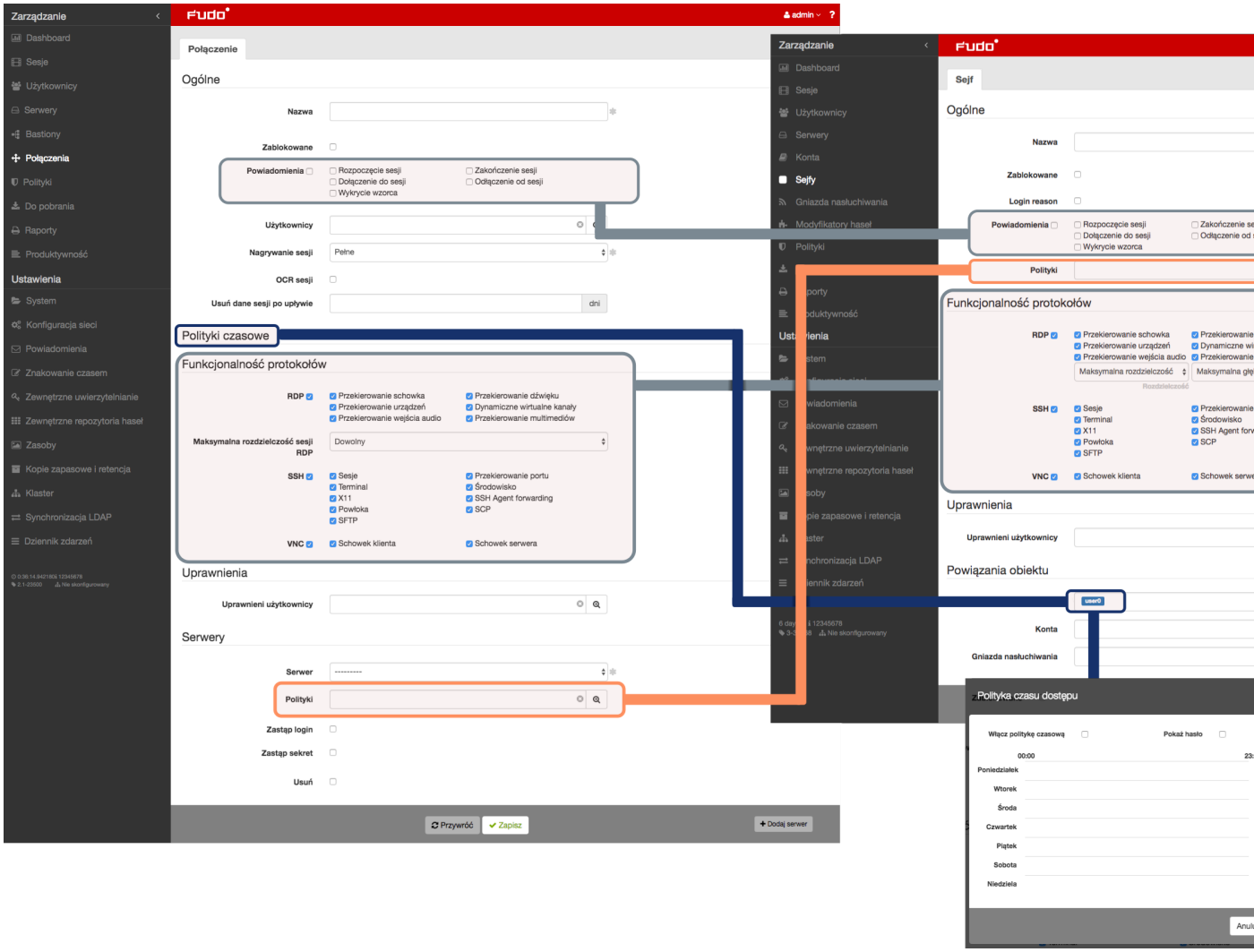
Kod błędu	Treść komunikatu i opis
FSE0382	*Unable to authenticate user %s: account is blocked.*
FSE0383	*Unable to authenticate user %s: user not found.*
FSE0384	*Unable to authenticate user %s: user is blocked.*
FSE0385	*Unable to authenticate user %s: safe not found.*
FSE0386	*Unable to authenticate user %s: safe is blocked.*
FSE0420	*Unable to authenticate user %s against server %s.*
FSE0461	*Invalid data from AD server.*
FAE0464	*User %s is not allowed to login from address %s.*

7.3 Mapowanie parametrów Wheel Fudo PAM 2.2 na Wheel Fudo PAM 3.0

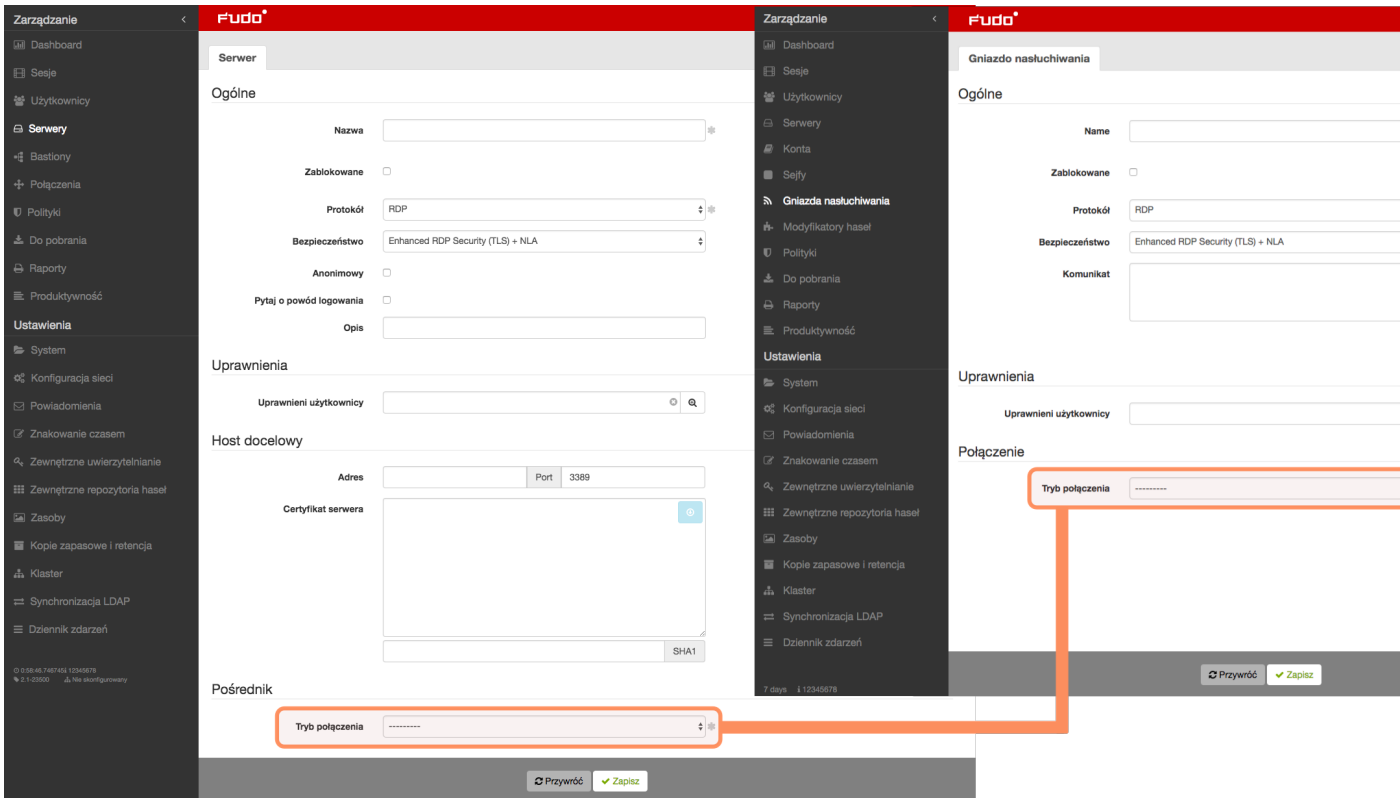
Ten rozdział zawiera opis odwzorowania parametrów obiektów w Wheel Fudo PAM 2.2 na nowy model danych Wheel Fudo PAM 3.0.

7.3.1 Połączenie




Zarządzanie
Dashboard
Sesje
Użytkownicy
Serwery
Bastiony
Połączenia
Polityki
Do pobrania
Raporty
Produktywność
Ustawienia
System
Konfiguracja sieci
Powiadomienia
Znakowanie czasem
Zewnętrzne uwierzytelnianie
Zewnętrzne repozytoria haseł
Zasoby
Kopie zapasowe i retencja
Klaster
Synchronizacja LDAP
Dziennik zdarzeń
admin
Połączenie
Ogólne
Nazwa
Zablokowane
Powiadomienia
Rozpoczęcie sesji
Dołączenie do sesji
Wykrycie wzorca
Zakończenie sesji
Odłączenie od sesji
Użytkownicy
Nagrywanie sesji
Pełne
OCR sesji
Usuń dane sesji po upływie
dni
Polityki czasowe
Funkcjonalność protokołów
RDP
Przekierowanie schowka
Przekierowanie urządzeń
Przekierowanie wejścia audio
Przekierowanie dźwięku
Dynamiczne wirtualne kanały
Przekierowanie multimediów
Maksymalna rozdzielczość sesji RDP
Dowolny
SSH
Sesje
Terminal
X11
Powłoka
SFTP
Przekierowanie portu
Środowisko
SSH Agent forwarding
SCP
VNC
Schowek klienta
Schowek serwera
Uprawnienia
Uprawnieni użytkownicy
Serwery
Serwer
Polityki
Zastąp login
Zastąp sekret
Usuń
Przywróć
Zapisz
Dodaj serwer
Sejf
Login reason
Konta
Sejfy
Gniazda nasłuchiwania
Modyfikatory haseł
Powiązania obiektu
Konta
Gniazda nasłuchiwania
Polityka czasu dostępu
Włącz politykę czasową
Pokaż hasło
Poniedziałek
Wtorek
Środa
Czwartek
Piątek
Sobota
Niedziela

7.3.2 Serwer



7.4 Migracja modelu danych wersji 2.2 do 3.0

Ten rozdział opisuje mechanizmy migracji obiektów modelu danych Wheel Fudo PAM 2.2 do wersji 3.0.

Informacja: W przypadku niepowodzenia aktualizacji Wheel Fudo PAM do wersji 3.0, nieprawidłowości, które uniemożliwiły prawidłowe zakończenie migracji danych, zostaną zapisane w dzienniku zdarzeń.

7.4.1 Serwer

Serwery o tym samym adresie IP i numerze portu zostają zastąpione jednym obiektem. Nazwa powstałego obiektu stanowi konkatenację nazw serwerów, posortowanych rosnąco i oddzielonych przecinkiem.

Ostrzeżenie: Jeżeli dwa serwery o tym samym adresie docelowym i porcie mają przypisane różne protokoły, opisy, ustawienia zewnętrznego repozytorium haseł, poziom bezpieczeństwa RDP, ustawienia HTTP, ustawienia TLS, certyfikaty lub klucze publiczne, aktualizacja nie powiedzie się.

7.4.2 Sejf (dawniej *połączenie*)

- Połączenie anonimowe staje się obiektem typu sejf, który może zostać usunięty.
- Dla każdego bastionu (tj. grupy serwerów w trybie *bastion*, przypisanych do tego samego bastionu) z danego połączenia zostaje utworzony obiekt typu *sejf* o nazwie `<nazwa połączenia> > <nazwa bastionu>`.
- Dla każdego serwera w trybie *gateway*, *proxy* lub *transparent* z danego połączenia zostaje utworzony obiekt typu *sejf* o nazwie `<nazwa połączenia> > <nazwa serwera>`.
- Sejf utworzony na podstawie połączenia dziedziczy po nim jego prawa dostępu, uprawnienia, ustawienia powiadomień, ustawienia protokołów, a także mapowania LDAP.
- Ustawienia OCR, nagrywania sesji i retencji danych sesji nie są dziedziczone po połączeniu, ale znajdują swoje odzwierciedlenie w obiekcie typu *konto*.
- Polityki czasowe połączeń odwzorowane są na dostęp użytkownika do sejfu utworzonego na podstawie danego połączenia.
- Polityki danych logowania połączenia są odwzorowane na polityki sejfu.

7.4.3 Konto (dawniej *dane logowania*)

Dla każdych danych logowania z połączenia powstaje obiekt typu *konto*.

- Jeżeli dane logowania zawierają login to konto dostaje typ regular. Nazwa takiego konta to `<login> @ <ostateczna nazwa serwera>`.
- Jeżeli dane logowania nie zawierają loginu i dotyczą połączenia nieanonimowego, to konto dostaje typ forward. Nazwa takiego konta to `forward for <ostateczna nazwa serwera>`.
- Jeżeli dane logowania nie zawierają loginu i dotyczą połączenia anonimowego to konto będące wynikiem migracji danych będzie typu *anonymous*. Nazwa takiego konta to `anonymous for <ostateczna nazwa serwera>`.
- Zduplikowane dane logowania zostają zastąpione jednym kontem. Uprawnienia do zarządzania obiektem, ustawienia OCR, ustawienia nagrywania sesji, ustawienia retencji danych sesji konta zostają odziedziczone po połączeniu, z którego pochodziły dane logowania, na podstawie których konto zostało utworzone.

Ostrzeżenie: Jeżeli dane logowania zawierają login, ale nie zawierają sekretu, tzn. zastępują login, ale nie przekazują sekretu to aktualizacja zakończy się niepowodzeniem.

7.4.4 Gniazdo nasłuchiwania (dawniej *bastion* lub część serwera)

- Dla każdego serwera w trybie *proxy*, *transparent* lub *gateway* zostaje utworzone gniazdo nasłuchiwania z tym samym trybem.
- Obiekt dziedziczy po serwerze uprawnienia, ustawienia TLS i poziom bezpieczeństwa RDP.
- Komunikat i klucze prywatne przechodzą na gniazdo.

- Obiekt zostaje przypisany do wszystkich sejfów, które zostały utworzone na podstawie połączeń, do których należał serwer, z którego powstało gniazdo.
- Bastion staje się gniazdem nasłuchiwania w trybie *bastion*. Prawa dostępu i ustawienia bastionu przechodzą na gniazdo. Gniazdo zostaje dodane do wszystkich sejfów, które zostały utworzone na podstawie połączeń, do których należał przynajmniej jeden serwer z bastionu, z którego powstało gniazdo.

7.4.5 Sesje

- Dla każdej sesji zaktualizowany jest identyfikator sejfu, serwera i konta. Jeżeli sesja dotyczyła serwera, który nie działał w trybie bastion to również ustawiony jest identyfikator gniazda nasłuchiwania.

7.5 Obsługa wspieranych protokołów

Ten rozdział zawiera szczegółowy opis zakresu w jakim wspierane są obsługiwane protokoły.

7.5.1 Citrix StoreFront (HTTP)

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Odtwarzacz prezentuje surowy tekst, bez renderowania graficznego.
- Brak wsparcia dla trybu bastion wynika z ograniczeń protokołu. Citrix StoreFront sam w sobie daje dostęp do bastionu maszyn. Użytkownik logując się do Citrix StoreFront może wybrać w swoim panelu maszynę, z którą chce się połączyć za pomocą protokołu ICA.

7.5.2 HTTP

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Odtwarzacz prezentuje surowy tekst, bez renderowania graficznego.
- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.
- Brak monitorowania ściąganych zasobów z zewnętrznych.
- Brak śledzenia przekierowań.

7.5.3 ICA

Wspierane tryby połączenia:

- Bastion (możliwość wpisania konta lub serwera docelowego w pliku ICA),
- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- Citrix Receiver.

7.5.4 Modbus

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.

7.5.5 MS SQL (TDS)

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- SQL Server Management Studio,
- sqsh.

7.5.6 MySQL

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- Oficjalny klient MySQL,

- Biblioteki PyMySQL dla Pythona.

Uwagi:

- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.
- Brak wsparcia uwierzytelnienia z użyciem AD lub innych zewnętrznych źródeł uwierzytelnienia.

7.5.7 Oracle

Protokół Oracle jest zamkniętym protokołem, którego implementacja wymaga reverse engineeringu, co ogranicza możliwości techniczne w zakresie rozbudowy i poprawy ewentualnych problemów.

Wspierane tryby połączenia:

- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- SQLDeveloper 4.1.3.20.78,
- SQL*Plus: Release 11.2.0.4.0 Production.

Uwagi:

- Brak wsparcia uwierzytelnienia z użyciem AD lub innych zewnętrznych źródeł uwierzytelnienia.
- Odtwarzacz uwzględnia tylko zapytania klientów (w podglądzie sesji nie wyświetlamy odpowiedzi serwera).
- Wspierane wersje 10 i 11.
- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.

7.5.8 RDP

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- Wszystkie oficjalne Microsoft – Windows, macOS,
- FreeRDP 2.0 i nowsze.

Uwagi:

- W przypadku uwierzytelnienia użytkowników Fudo przed AD (lub innym zewnętrznym źródłem) tryb bezpieczeństwa TLS+NLA (Network Level Authentication) nie jest obsługiwany; zamiast niego stosowany jest tryb TLS. Wsparcie dla trybu NLA po stronie serwera docelowego jest zapewnione.
- Trwają prace nad wsparciem dla mechanizmu RemoteApp.

7.5.9 SSH

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Wybrane wspierane funkcje:

- Multipleksowanie połączeń,
- SCP,
- SFTP – brak podglądu sesji i plików SFTP w Fudo,
- Przekierowanie portów.

Uwagi:

- Brak możliwości przekazywania (forwardowania) klucza SSH.

7.5.10 Telnet

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

7.5.11 Telnet 3270

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

Wspierane aplikacje klienckie:

- IBM Personal Communications,
- c3270.

7.5.12 Telnet 5250

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

Wspierane aplikacje klienckie:

- IBM Personal Communications,
- tn5250.

7.5.13 VNC

Wspierane tryby połączenia:

- Bastion,
- Brama,
- Pośrednik,
- Przezroczysty.

Wspierane aplikacje klienckie:

- TightVNC,
- RealVNC.

7.5.14 X11

Protokół X11 wspierany jest w ramach protokołu SSH.

Wspierane serwery:

- Xorg,
- Xming,
- XQuartz.

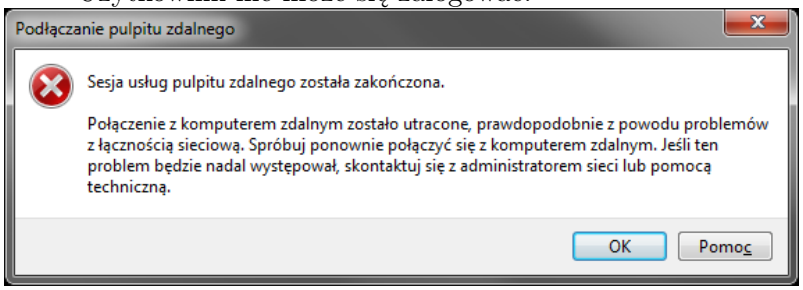
ROZDZIAŁ 8

Rozwiązywanie problemów

8.1 Uruchamianie Wheel Fudo PAM

Problem	Objawy i opis rozwiązania
Wheel Fudo PAM nie uruchamia się	• Sprawdź czy oba zasilacze są podłączone do instalacji elektrycznej 230V. Brak odpowiedniego podłączenia komunikowany jest sygnałem dźwiękowym. • Upewnij się czy podłączony został klucz szyfrujący. Brak klucza komunikowany jest sygnałem dźwiękowym. • W przypadku gdy problem wynika z nieudanej próby aktualizacji systemu, odczekaj kilka minut, podczas których urządzenie wykryje problem i uruchomi się ponownie przywracając poprzednią wersję systemu.

8.2 Połączenia z serwerami

Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem	**Objawy:** • Użytkownik nie może się zalogować.  • Wpis w dzienniku zdarzeń: `Authentication failed: Invalid username kowalski or password.`
	Rozwiązanie: • Sprawdź czy definicja użytkownika istnieje w systemie Wheel Fudo PAM. • Zweryfikuj poprawność danych logowania użytkownika. • Upewnij się, że w kliencie za pośrednictwem którego realizowane jest połączenie z serwerem, nie są zapamiętane nieaktualne dane logowania.
	Objawy: komunikat w dzienniku zdarzeń: `Unable to establish connection to server zbigniew (10.0.35.53:3399).`
	Przyczyna: błędna konfiguracja serwera.
	Rozwiązanie: • Zweryfikuj poprawność definicji danego serwera (adres IP, numer portu). • Sprawdź, czy serwer osiągalny jest przez Wheel Fudo PAM:
	1. Zaloguj się do panelu administracyjnego Wheel Fudo PAM. 2. Wybierz *Ustawienia* > *System*, zakładka *Diagnostyka*. 3. Wprowadź adres serwera w sekcji *Ping* i wykonaj polecenie, żeby sprawdzić osiągalność hosta.

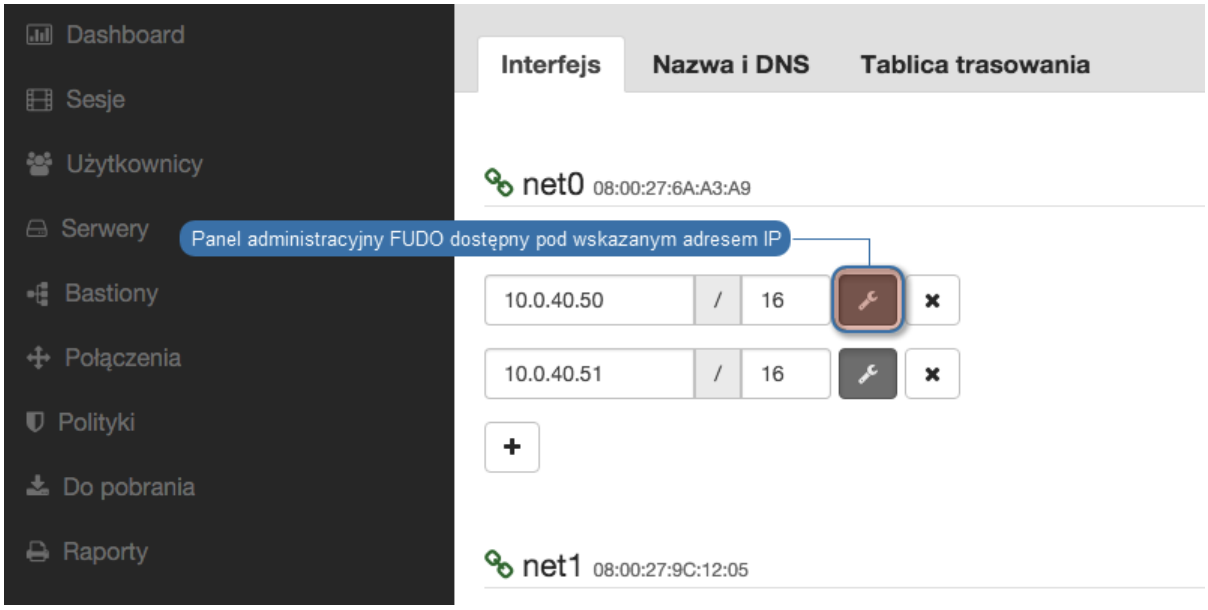
Problem	Objawy i opis rozwiązania
Przy próbie logowania nie wszyscy użytkownicy widzą ekran logowania Wheel Fudo PAM (standardowy, z szarym tłem).	**Przyczyna:** • Zapisane poświadczenia w skrócie RDP skutkują ukryciem ekranu Wheel Fudo PAM i bezpośrednim zalogowaniem do serwera docelowego. • Zapisane poświadczenia w skrócie RDP, użytkownik używa poświadczeń lokalnych na Wheel Fudo PAM tak więc przed Wheel Fudo PAM jest poprawnie uwierzytelniany i nie pokazuje mu się ekran logowania. Następnie gdy Wheel Fudo PAM robi forward uwierzytelnień do docelowej maszyny to są one nie poprawne i użytkownikowi pokazuje się gina Windows gdzie sam się musi uwierzytelnić.
	Objawy: • Komunikat klienta: `Connection closed by remote host.` • Wpis w dzienniku zdarzeń: `Failed to authenticate against the server as user root using password.`
	Przyczyna: niepoprawne dane logowania do serwera docelowego.
	Rozwiązanie: zmień dane logowania w konfiguracji obiektu serwera.
	Objawy: • Komunikat klienta RDP: `Connection refused`. • Komunikat klienta SSH: `ssh: connect to host 10.0.1.111 port 10011: Connection refused`
	Przyczyna: serwer jest zablokowany.
	Rozwiązanie: odblokuj serwer w panelu administracyjnym Wheel Fudo PAM.

Problem	Objawy i opis rozwiązania
Połączenie jest zrywane	**Objawy:** • Użytkownik próbuje się połączyć z serwerem przez Wheel Fudo PAM, po wpisaniu nazwy użytkownika i hasła sesja od razu się zrywa. • Komunikat w dzienniku zdarzeń: `TLS certificate verification failed.`
	Rozwiązanie:
	Pobierz nowy certyfikat serwera docelowego w sekcji *Host docelowy*.
	
	Objawy: • Po wpisaniu nazwy użytkownika i hasła następuje zerwanie połączenia. • Wpis w dzienniku zdarzeń: `RDP connection error.`
	Rozwiązanie: sprawdź czy w zakładce *General* we właściwościach TCP-Rdp, opcja *Encryption level* nie jest ustawiona na `FIPS Compliant`.
Brak połączenia z serwerem	**Objawy:** • Nie można zalogować się do serwera, komunikat `User user0 not allowed to connect to server.` • w dzienniku zdarzeń wpis: `Authentication failed: User user0 not allowed to connect to server.`
	Przyczyna: użytkownik nie jest dodany do połączenia.
	Rozwiązanie: dodaj użytkownika do odpowiedniego obiektu połączenia.

Problem	Objawy i opis rozwiązania
	Objawy: • Po wpisaniu nazwy użytkownika i hasła następuje jakby zamrożenie ekranu logowania. • Wpis w dzienniku zdarzeń `Terminating session: User user0 (id=848388532111147010) is blocked.`
	Przyczyna: użytkownik jest zablokowany w Wheel Fudo PAM.
	Rozwiązanie: odblokuj użytkownika.
Użytkownik musi logować się dwukrotnie	**Objawy:** użytkownik łącząc się poprzez protokół RDP wpisuje login i hasło po czym po chwili jest proszony o ponowne wprowadzenie danych autoryzujących.
	Przyczyna: serwer stanowi część infrastruktury zarządzanej przez broker połączeń, który wykrył istniejącą aktywną sesję użytkownika na innym serwerze.
	Objawy: użytkownik nawiązując połączenie SSH wprowadza dane logowania po czym ponownie proszony jest o ich podanie.
	Przyczyna: w obiekcie *połączenie* włączone są opcje zastępowania loginu i hasła, ale te pola ich definicji pozostawione są puste, co skutkuje podwójnym uwierzytelnieniem - w pierwszej kolejności przed Fudo, w drugiej przed serwerem docelowym.
Nie można nawiązać połączenia z serwerem RDP	**Objawy:** • użytkownik nawiązując połączenie RDP zostaje rozłączony chwilę po uwierzytelnieniu. • w dzienniku zdarzeń wpis: `RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.`
	Przyczyna: serwer docelowy, na który następuje przekierowanie, nie nasłuchuje na porcie 3389.
	Rozwiązanie: skonfiguruj serwer docelowy tak, by oczekiwał na połączenia użytkowników na porcie 3389.
	Objawy: • w dzienniku zdarzeń wpis: `User user0 has no access to host 192.168.0.1:3389`
	Przyczyna: broker stwierdza, że użytkownik ma aktywną sesję na innym serwerze i inicjuje przekierowanie, ale docelowy serwer nie jest skonfigurowany na Wheel Fudo PAM lub użytkownik nie jest uprawniony do nawiązywania połączeń z wybranym zasobem.
	Rozwiązanie: • Upewnij się, że obiekt serwera jest dodany do Fudo. • Dodaj użytkownika do odpowiedniego *połączenia*.

8.3 Logowanie do panelu administracyjnego

Problem	Objawi i opis rozwiązania
Nie można zalogować się do panelu administracyjnego	• Zweryfikuj czy wprowadzony adres Wheel Fudo PAM jest poprawny. • Ustaw adres IP Wheel Fudo PAM z poziomu konsoli, postępując zgodnie z instrukcją w rozdziale *Konfiguracja interfejsów sieciowych* w dokumentacji systemu Wheel Fudo PAM. • Upewnij się, że adres IP ma włączoną funkcję zarządzania Wheel Fudo PAM.



8.4 Odtwarzanie sesji

Problem	Objawy i opis rozwiązania
Nie można odtworzyć wyeksportowanego materiału	**Przyczyna:** brak odpowiednich kodeków wideo.
	Rozwiązanie: zweryfikuj czy masz zainstalowane odpowiednie oprogramowanie.
Użytkownik administrator nie widzi sesji	**Objawy:** na liście sesji nie ma spodziewanych pozycji.
	Przyczyna: brak stosownych uprawnień.
	Rozwiązanie: nadaj użytkownikowi uprawnienia do określonego obiektu połączenia, serwera oraz użytkownika.
Nie można odtworzyć sesji w odtwarzaczu	**Objawy:** komunikat: `Nie można odnaleźć danych sesji.`
	Przyczyna: połączenie miało miejsce przy wyłączonej opcji rejestrowania sesji.
	Rozwiązanie: włącz opcję rejestrowania sesji, aby w przyszłości mieć możliwość odtworzenia materiału.

8.5 Konfiguracja klastrowa

Problem	Objawy i opis rozwiązania
Obiekty nie replikują się na drugi węzeł	**Objawy:** Obiekty utworzone na jednym węźlę, nie pojawiają się automatycznie na pozostałych węzłach klastra. **Rozwiązanie:** Skontaktuj się z działem wspracia technicznego.

ROZDZIAŁ 9

Często zadawane pytania

1. Jaka jest maksymalna ilość nagranych sesji na Wheel Fudo PAM dostępna z poziomu systemu?

2. W jaki sposób Wheel Fudo PAM obsługuje archiwizację sesji?

3. Jak wyliczyć wielkość przestrzeni dyskowej do archiwizacji?

4. W jaki sposób użytkownicy mogą ukrywać swoje działania na serwerach do których mają skonfigurowane połączenia na Wheel Fudo PAM?

5. W jaki sposób można stwierdzić próby uzyskania nieuprawionego dostępu do monitorowanych serwerów?

6. Czy możliwe jest ukrycie ekranu logowania podczas nawiązywania połączeń RDP?

7. Dlaczego lista użytkowników we właściwościach połączenia jest niekompletna?

8. Dlaczego użytkownik usunięty z serwera LDAP/AD w dalszym ciągu widoczny jest na Wheel Fudo PAM?

9. Jak często ma miejsce synchronizacja użytkowników z serwerem LDAP/AD?

*10. W odtwarzaczu sesji zamiast wprowadzonych znaków klawiatury wyświetlane są *. W jaki sposób zobaczyć dane wejścia klawiatury?*

11. Czy można unieważnić odnośnik do sesji?

1. Jaka jest maksymalna ilość nagranych sesji na Wheel Fudo PAM dostępna z poziomu systemu?

Urządzenie dysponuje 20TB przestrzeni dyskowej dedykowanej do przechowywania sesji.

Rozmiar sesji determinowany jest aktywnością użytkownika. Średnie wartości dla jednej minuty zarejestrowanego połączenia wynoszą:

RDP	1 MB aktywnej sesji (brak aktywności ze strony użytkownika generuje pomijalnie niewielkie ilości danych). Ostateczny rozmiar sesji uzależniony jest od rozdzielczości ekranu, głębi kolorów i aktywności użytkownika w sesji.
SSH	50 kB aktywnej sesji.

Przy takich założeniach, 20 TB pozwala na zarejestrowanie:

- około 36 lat sesji RDP;
- około 760 lat sesji SSH.

Informacja: Wheel Fudo PAM pozwala określić, jak długo sesje mają być przechowywane i automatycznie usuwa dane sesji po upłynięciu czasu określonego parametrem *retencji*.

---

2. W jaki sposób Wheel Fudo PAM obsługuje archiwizację sesji?

Wszystkie sesje archiwizowane są na 20 TB przestrzeni dyskowej urządzenia, przeznaczonej na rejestrowanie zdalnych połączeń. Dodatkowo Wheel Fudo PAM daje możliwość eksportu sesji w natywnym formacie lub w postaci nagrania video.

3. Jak wyliczyć wielkość przestrzeni dyskowej do archiwizacji?

Rozmiar plików w formacie natywnym jest zgodny z odpowiedzią z punktu 1. W przypadki eksportu do formatu video, rozmiar wynikowy pliku zależy od wybranego kodowania strumienia video oraz wybranej rozdzielczości nagrania.

4. W jaki sposób użytkownicy mogą ukrywać swoje działania na serwerach, do których mają skonfigurowane połączenia na Wheel Fudo PAM?

W przypadku protokołu SSH, obsługiwany jest kanał SCP przez co wszystkie pliki, w tym skrypty, również podlegają monitorowaniu. Dzięki temu można audytować daną sesję również pod kątem złośliwego kodu zamieszczanego w programach wysłanych na serwer, których zawartość nie jest wyświetlana na ekranie.

Ochrona innych kanałów komunikacji użytkownika z serwerem (np. przeglądarka internetowa lub inne programy) to zadanie dla rozwiązań innego rodzaju. Żadne rozwiązania jak Wheel Fudo PAM nie mogą monitorować tych kanałów, dlatego ważne jest stworzenie odpowiedniej konfiguracji serwera przez administratora systemu.

5. W jaki sposób można stwierdzić nieuprawnione próby uzyskania dostępu do monitorowanych serwerów?

Próby nadużyć (nieuprawniony dostęp, atak DoS), można stwierdzić na podstawie analizy wpisów w dzienniku zdarzeń. Wszelkie wpisy o poziomie logowania ERROR i WARNING powinny być dokładnie analizowane. Przypadki wystąpienia błędu przekroczenia limitu czasu logowania, mogą świadczyć o próbie dokonania ataku DoS.

6. Czy możliwe jest ukrycie ekranu logowania podczas nawiązywania połączeń RDP?

Ukrycie ekranu logowania wymaga zdefiniowania trybu bezpieczeństwa `Enhanced RDP Security (TLS) + NLA` monitorowanego serwera.

7. Dlaczego lista użytkowników we właściwościach połączenia jest niekompletna?

Lista użytkowników we właściwościach połączenia nie zawiera użytkowników synchronizowanych z serwerem usług katalogowych. Aby dodać takiego użytkownika do połączenia, zdefiniuj mapowanie grup we *właściwościach synchronizacji LDAP* lub wyłącz synchronizację LDAP dla wybranego użytkownika.

8. Dlaczego użytkownik usunięty z serwera LDAP/AD w dalszym ciągu widoczny jest na Wheel Fudo PAM?

Odwzorowanie zmiany polegającej na usunięciu użytkownika z serwera LDAP lub AD wymaga pełnej synchronizacji. Proces pełnej synchronizacji wyzwalany jest automatycznie raz na dobę, w czasie do 5 minut po godzinie 00:00, lub może zostać wyzwolony ręcznie z poziomu widoku ustawień *synchronizacji LDAP*.

9. Jak często ma miejsce synchronizacja użytkowników z serwerem LDAP/AD?

Definicje nowych użytkowników oraz zmiany w istniejących obiektach pobierane są okresowo w odstępie czasowym wynoszącym 5 minut. Pełna synchronizacja wyzwalana jest automatycznie raz na dobę, w czasie do 5 minut po godzinie 00:00.

10. W odtwarzaczu sesji zamiast wprowadzonych znaków klawiatury wyświetlane są *. W jaki sposób zobaczyć dane wejścia klawiatury?

Wejście klawiatury należy do grupy funkcjonalności wrażliwych i jest domyślnie ukryte. Włączenie pokazywania znaków wprowadzonych na klawiaturze wymaga decyzji dwóch użytkowników `superadmin`. Procedura aktywacji funkcjonalności opisana jest w rozdziale *Funkcjonalności wrażliwe*.

11. Czy można unieważnić odnośnik do sesji?

Aktywny odnośnik do sesji może zostać w każdej chwili unieważniony. Procedura unieważnienia odnośników opisana jest w rozdziale *Udostępnianie sesji*.

ROZDZIAŁ 10

Słownik pojęć

DNS Domain Name Server - serwer nazw, tłumaczy mnemoniczne nazwy hostów na adresy IP.

SSH Secure Shell - protokół sieciowy do bezpiecznej komunikacji ze zdalnymi urządzeniami.

Syslog Standard logowania zdarzeń w systemach komputerowych. Serwer Syslog zbiera i przechowuje centralnie dane dzienników zdarzeń (log) urządzeń sieciowych, które mogą zostać wykorzystane w celach raportowania i analizowania.

Odcisk Palca Fingerprint - ciąg znaków będący działaniem funkcji skrótu na danych wejściowych, pozwalający jednoznacznie stwierdzić, czy dane nie zostały zmienione.

RDP Remote Desktop Protocol - protokół zdalnego dostępu do graficznych interfejsów użytkownika w systemach operacyjnych firmy Microsoft.

VNC Protokół graficznego dostępu do zdalnych zasobów komputerowych.

RADIUS Remote Authentication Dial In User Service - protokół sieciowy służący regulowaniu dostępu do określonych usług udostępnianych w sieci informatycznej.

Hasło statyczne Podstawowa metoda uwierzytelniania użytkowników, w której do potwierdzenia tożsamości używana jest kombinacja ciągów znakowych w postaci loginu i hasła.

Klucz publiczny Metoda uwierzytelniania, w której tożsamość użytkownika ustalana jest na podstawie pary kluczy - prywatny (będący tylko w posiadaniu użytkownika) i publiczny (udostępniany innym podmiotom).

CERB Kompleksowe rozwiązanie uwierzytelniania i autoryzacji użytkowników, wspierające metody uwierzytelniania tj. token mobilny (aplikacja na telefon komórkowy), hasło statyczne, hasła jednorazowe SMS.

LDAP Lightweight Directory Access Protocol - protokół dostępu i zarządzania rozproszonymi usługami katalogowymi w sieciach IP.

Active Directory Usługa uwierzytelniania i autoryzacji użytkowników w domenie Windows.

AD Active Directory - usługa uwierzytelnienia i autoryzacji użytkowników w domenie Windows.

notacja CIDR Skrócona notacja adresów sieciowych, w której adres IP zapisywany jest zgodnie z notacją IPv4, a maska podawana jest w postaci liczby wiądących cyfr «1» w zapisie bitowym (192.168.1.1 - 255.255.255.0; 192.168.1.1/24).

DoS (Denial of Service) Próba ataku na system polegająca na wysłaniu znacznej ilości zapytań do serwera, tak aby zaprzestał przetwarzać kolejne żądania użytkowników.

heartbeat Pakiet służący informowaniu innych węzłów klastra o stanie maszyny. W przypadku gdy drugi węzeł klastra nie otrzyma pakietu heartbeat przez określony czas, przejmuje rolę węzła głównego i przetwarza zapytania użytkowników.

PSM (Privileged Session Management) Moduł Wheel Fudo PAM służący rejestracji zdalnych sesji dostępowych.

sejf anonimowy Sejf anonimowy ma przypisane co najmniej jedno konto typu `anonymous` i może mieć przypisane jedynie konta tego typu. Do sejfów anonimowych nie można przypisać użytkowników.

AAPM Moduł AAPM (Application to Application Password Manager) umożliwiający bezpieczną wymianę haseł pomiędzy aplikacjami.

Efficiency Analyzer Moduł Efficiency Analyzer dostarcza danych statystycznych na temat aktywności użytkowników.

serwer

Serwery Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

gniazdo nasłuchiwania Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

użytkownik Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (indywidualny login, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzilnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

konto Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykłe (z podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

sejf Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

hot-swap Mechanizm umożliwiający wymianę komponentu bez wyłączania urządzenia.

polityka czasowa Mechanizm definiowania przedziałów czasu, w których użytkownicy mają dostęp do serwerów.

modyfikator haseł Narzędzie służące do zmiany hasła do konta na monitorowanym serwerze.

polityka Mechanizm pozwalający definiować wzorce i automatyczne akcje, które podejmie system w przypadku wykrycia danego wzorca.

sesja współdzielona Sesja użytkownika, do której dołączył inny użytkownik.

fudopv Skrypt modułu AAPM, rezydujący na serwerze, umożliwiający wymianę haseł pomiędzy aplikacjami.

dostęp SSH Dostęp serwisowy do Wheel Fudo PAM poprzez protokół SSH.

VLAN Mechanizm sieci wirtualnych, umożliwiający separację domen rozgłoszeniowych.

DHCP Mechanizm dynamicznego zarządzania adresacją w sieciach LAN.

znacznik czasu Znacznik będący skrótem danych, pozwalający zweryfikować czy dane nie zostały zmienione.

zewnętrzny serwer uwierzytelnienia Serwer przechowujący dane użytkowników, używany do weryfikacji tożsamości w procesie logowania do Wheel Fudo PAM lub nawiązywania połączenia z serwerami docelowymi.

repozytorium haseł Repozytorium haseł zarządza hasłami do serwerów docelowych, w dostępie do których, pośredniczy Wheel Fudo PAM.

retencja Retencja danych to mechanizm, który usuwa dane sesji po upływie zdefiniowanego czasu.

grupa redundancji Zdefiniowana grupa adresów IP, które w przypadku awarii jednego z węzłów, zostaną przypisane do drugiego serwera, dla zachowania ciągłości świadczenia usług.

broker połączeń RDP Mechanizm zarządzania sesjami dostępowymi do maszyn będących częścią farmy serwerów.

Indeks

A

AAPM, **220**
Active Directory, **219**
Active Directory
    systemy zewnętrznego
        uwierzytelniania, 150
AD, **219**
administracja
    aktualizacja systemu, 130
    import/eksport konfiguracji, 160
    pierwsze uruchomienie, 16
    ponowne uruchomienie, 157
    przywracanie poprzedniej wersji, 156

B

broker połączeń RDP, **221**
broker połączeń RDP, 193

C

CERB, **219**
CERB
    systemy zewnętrznego
        uwierzytelniania, 150

D

DHCP, **221**
DNS, **219**
DNS
    konfiguracja, 146
DoS (*Denial of Service*), **220**
dostęp SSH, **221**

E

Efficiency Analyzer, **220**
Efficiency Analyzer, 4

F

fudopv, **220**

G

gniazda nasłuchiwania
    konfiguracja, 75
gniazdo nasłuchiwania, **220**
grupa redundancji, **221**

H

Hasło statyczne, **219**
heartbeat, **220**
hot-swap, **220**

K

Klucz publiczny, **219**
konfiguracja
    gniazda nasłuchiwania, 75
    model danych, 4
    powiadomienia, 148
    serwery, 62
    synchronizacja użytkowników, 171
    ustawienia sieciowe, 135
    użytkownicy, 56
konto, **220**

L

LDAP, **219**
LDAP
    systemy zewnętrznego
        uwierzytelniania, 150

M

model danych
    serwer, 5
    użytkownik, 5
moduł
    AAPM, 4
    Efficiency Analyzer, 4
    PSM, 2
    Secret Manager, 3
modyfikator haseł, **220**

N

notacja CIDR, **220**

O

Odcisk Palca, **219**

P

polityka, **220**
polityka czasowa, **220**
Portal użytkownika, 4
PSM, 2
PSM (*Privileged Session Management*), **220**

R

RADIUS, **219**
RADIUS
    systemy zewnętrznego uwierzytelniania, 150
RDP, **219**
repozytorium haseł, **221**
retencja, **221**

S

scenariusze wdrożenia
    bastion, 8
    brama, 7
    most, 6
    pośrednik, 8
    wymuszony routing, 6
sejf, **220**
sejf anonimowy, **220**
serwer, **220**
Serwery, **220**
serwery
    konfiguracja, 62
sesja współdzielona, **220**
sesje, 87
    dołączanie do trwającej sesji, 100
    eksportowanie, 106
    filtrowanie, 88
    komentowanie, 104
    na żywo, 98
    odtwarzanie i podgląd, 95
SSH, **219**
synchronizacja użytkowników, 171
    konfiguracja, 171
Syslog, **219**
systemy zewnętrznego uwierzytelniania, 150
    dodawanie serwera, 151
    modyfikowanie serwera, 152
    usuwanie serwera, 152

T

tryb połączenia
    transparentny, 7

U

ustawienia sieciowe
    konfiguracja interfejsów, 135
    serwery DNS, 146
    trasa routingu, 144
użytkownicy, 56
    blokowanie, 60
    konfiguracja, 56
    prawa dostępu, 61, 63
    role, 61
    usuwanie, 60
    zewnętrzne uwierzytelnianie, 150
użytkownik, **220**

V

VLAN, **221**
VNC, **219**

Z

zewnętrzny serwer uwierzytelnienia, **221**
znacznik czasu, **221**