Fudo PAM 5.2 - Dokumentacja Systemu

Fudo Security

08.03.2024

Spis treści

ROZDZIAŁ 1

O dokumentacji

Ten dokument skierowany jest do administratorów i operatorów systemu Fudo, odpowiedzialnych za konfigurację urządzenia i nadzorowanie zdalnych sesji uprzywilejowanych.

Struktura dokumentacji

1. O dokumentacji

Rozdział zawiera informacje na temat tej dokumentacji.

2. Motywy kolorystyczne Panelu Administracyjnego

Rozdział zawiera informacje na temat dostępnych motywów kolorystycznych Fudo PAM.

3. Wstęp

Rozdział zawiera informacje na temat poszczególnych modułów Fudo PAM, opisuje scenariusze wdrożenia, a także tryby połączenia oraz metody uwierzytelnienia użytkowników.

4. Instalacja i pierwsze uruchomienie

Rozdział opisuje procedurę wdrożenia Fudo PAM wraz z inicjalizacją systemu.

5. Szybki start

Rozdział zawiera przykłady konfiguracji typowych przypadków użycia.

6. Użytkownicy

Rozdział zawiera tematy związane z zarządzaniem użytkownikami.

7. Serwery

Rozdział zawiera tematy związane z zarządzaniem serwerami.

8. Konta

Rozdział zawiera tematy związane z zarządzaniem kontami.

9. Gniazda nasłuchiwania

Rozdział zawiera tematy związane z zarządzaniem gniazdami nasłuchiwania.

10. Sejfy

Rozdział zawiera tematy związane z zarządzaniem sejfami.

11. Żądania dostępu

Rozdział zawiera opis funkcjonalności wysyłania żądań dostępu do zasobów.

12. Wykrywanie (Discovery)

Rozdział zawiera opis funkcjonalności automatycznego wykrywania kont oraz serwerów.

13. Modyfikatory haseł

Rozdział opisuje zagadnienia automatycznej zmiany haseł w systemach docelowych.

14. Polityki

Rozdział opisuje zagadnienia związane z proaktywnym monitoringiem.

15. Aktywność konta w Portalu Użytkownika

Rozdział zawiera informacje dotyczące funkcjonalności informowania o zajętości zasobów.

16. Sesje

Rozdział zawiera informacje dotyczące rejestrowanych sesji dostępowych.

17. Raporty

Rozdział zawiera informacje na temat generowania raportów.

18. Produktywność

Rozdział opisuje w szczegółach moduł analizy produktywności użytkowników w monitorowanych sesjach.

19. Administracja

Rozdział zawiera opisy procedur administracyjnych.

20. Informacje uzupełniające

Rozdział zawiera informacje uzupełniające bezpośrednio związane z procedurami zarządzania.

21. Fudo Officer 1.0

Rozdział zawiera informacje na temat aplikacji mobilnej Fudo Officer 1.0, pozwalającej administratorom Fudo PAM zarządzać żądaniami użytkowników o dostęp do serwera.

22. AAPM (Application to Application Password Manager)

Rozdział zawiera opis modułu zmiany haseł w aplikacjach trzecich.

23. Systemy zgłoszeń

Rozdział zawiera opis integracji Fudo PAM z systemem zarządzania zgłoszeniami *Service Now*.

24. Aplikacje klienckie

Rozdział zawiera opisy konfigurowania aplikacji klienckich dla wybranych protokołów.

25. Rozwiązywanie problemów

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

26. Często zadawane pytania

Rozdział zawiera odpowiedzi na często zadawane pytania.

27. Słownik pojęć

Rozdział zawiera listę pojęć technicznych 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.

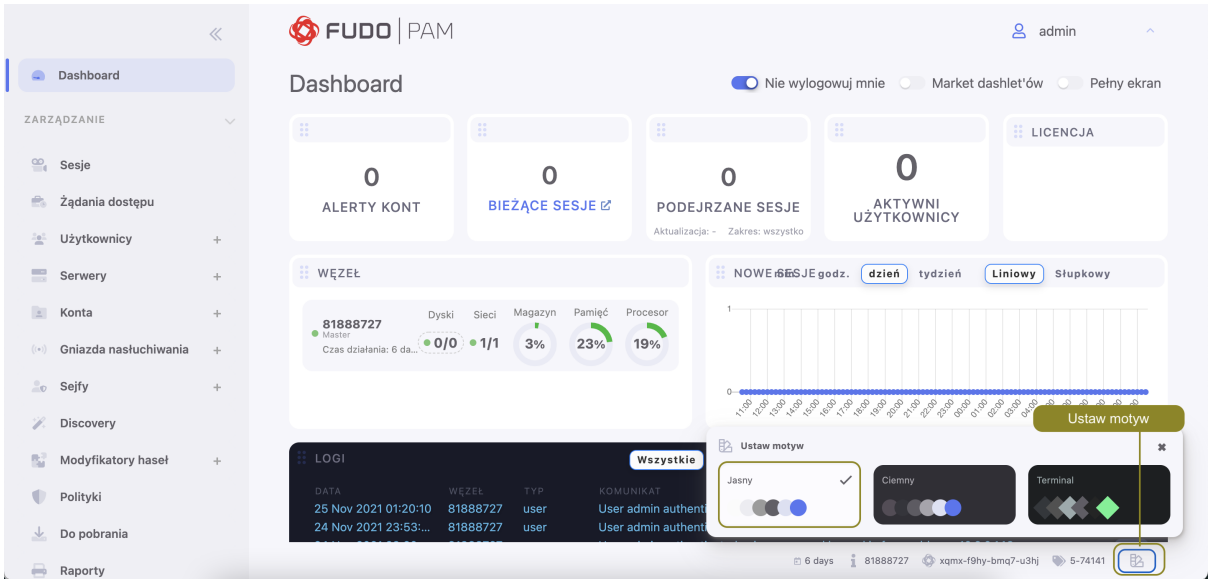
Nota prawna

ROZDZIAŁ 2

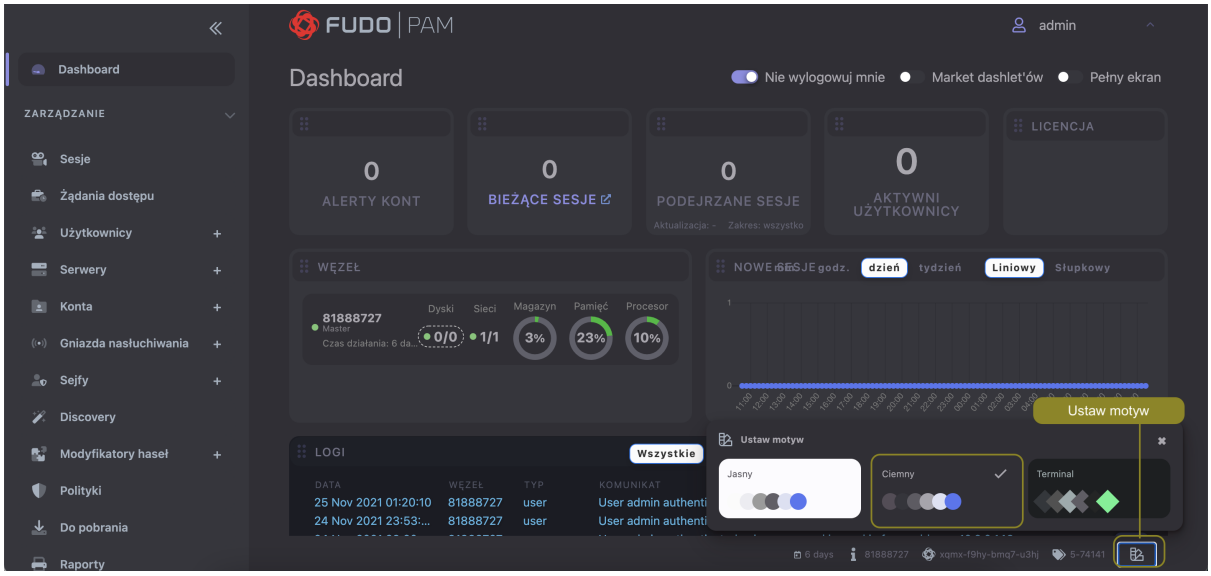
Motywy Panelu Administracyjnego

Fudo PAM 5.1 jest dostępny w trzech szatach graficznych dla Panelu Administracyjnego.

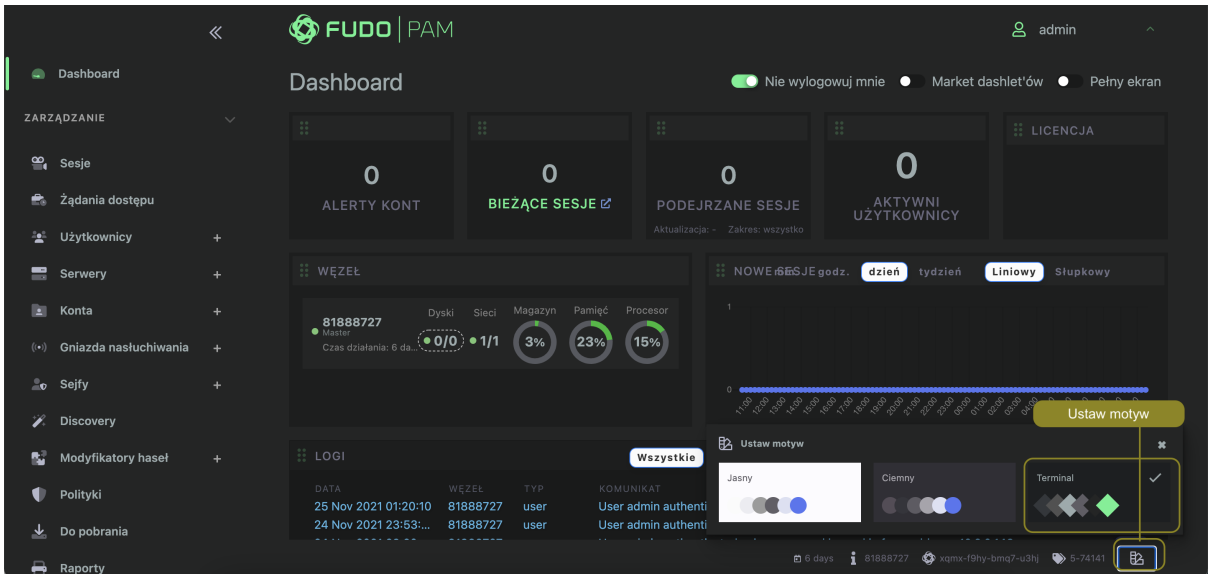
Jasny:



Ciemny:



Terminal:



Tematy pokrewne:

- *Wstęp*

ROZDZIAŁ 3

Wstęp

3.1 Opis systemu

Fudo PAM jest kompletnym rozwiązaniem do zarządzania zdalnym dostępem uprzywilejowanym. Fudo PAM składa się z czterech modułów, z których każdy odpowiedzialny jest za inny aspekt zarządzania dostępem uprzywilejowanym.

- *Privileged Sessions Management (PSM)*
- *Skarbiec haseł*
- *Analiza produktywności*
- *Application to Application Password Manager*

Zarządzanie sesjami uprzywilejowanymi *(ang. Privileged Sessions Management (PSM))*

Moduł PSM służy do stałego monitorowania zdalnych sesji dostępu do infrastruktury IT. 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.

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

Fudo PAM wspiera następujące konfiguracje systemowe:

- Linux,
- FreeBSD,

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

Skarbiec haseł *(ang. 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 *Modyfikatory haseł*.
Analiza produktywności

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

Więcej na temat modułu analizy produktywności znajdziesz w rozdziale *Produktywność*.

Application to Application Password Manager (AAPM)

Moduł *AAPM* umożliwia bezpieczną wymianę haseł pomiędzy aplikacjami.

Systemy operacyjne wspierane przez moduł AAPM:

- systemy operacyjne Microsoft Windows
- systemy operacyjne rodziny Linux
- systemy operacyjne rodziny BSD

Wiecej informacji na temat modułu AAPM znajdziesz w rozdziale *AAPM (Application to Application Password Manager)*.

Tematy pokrewne:

- *Wspierane protokoły*
- *Wymagania*
- *Model danych*
- *Mechanizmy bezpieczeństwa*

3.2 Wspierane protokoły

3.2.1 Citrix StoreFront (HTTP)

Ostrzeżenie: Wsparcie protokołu `Citrix` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Wspierane algorytmy kiedy szyfrowanie TLS jest włączone, a opcja *Starsze algorytmy kryptograficzne* wyłączona:

- `ecdhe-ecdsa-aes256-gcm-sha384`
- `ecdhe-rsa-aes256-gcm-sha384`
- `ecdhe-ecdsa-chacha20-poly1305`
- `ecdhe-rsa-chacha20-poly1305`
- `ecdhe-ecdsa-aes256-sha384`
- `dhe-rsa-aes256-gcm-sha384`

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.
- 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.

3.2.2 HTTP

Wspierane tryby połączenia:

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

Wspierane języki OCR renderowanej sesji HTTP:

- angielski,

- niemiecki,
- norweski,
- ukraiński,
- polski,
- węgierski,
- rosyjski.

Wspierane algorytmy kiedy szyfrowanie TLS jest włączone, a opcja *Starsze algorytmy kryptograficzne* wyłączona:

- `ecdhe-ecdsa-aes256-gcm-sha384`
- `ecdhe-rsa-aes256-gcm-sha384`
- `ecdhe-ecdsa-chacha20-poly1305`
- `ecdhe-rsa-chacha20-poly1305`
- `ecdhe-ecdsa-aes256-sha384`
- `dhe-rsa-aes256-gcm-sha384`

Uwagi:

Ostrzeżenie: Renderowanie sesji HTTP jest wymagającym procesem i może mieć negatywny wpływ na ogólną wydajność systemu. Monitorowanie rednerowanych połączeń HTTP zaleca się na maszynach fizycznych, z uwzględnieniem następujących limitów dla jednoczesnych połączeń HTTP.

Model	Maksymalna zalecana liczba jednoczesnych połączeń HTTP*
F100x	2
F300x	5
F500x	10

* Rzeczywista maksymalna liczba obsługiwanych sesji HTTP uwarunkowana jest konfiguracją danej instacji Fudo PAM.

- Brak wsparcia mechanizmu dołączania do sesji.
- Brak wsparcia wymagania podania powodu logowania.

Dodatkowo, w przypadku sesji nierenderowanych:

- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.
- Brak monitorowania ściąganych zasobów z zewnętrznych.
- Brak śledzenia przekierowań.
- Brak przekierowania danych do logowania.

Dodatkowo, w przypadku sesji renderowanych:

- Surowy ruch HTTP nie jest zapisywany.
- Lista czcionek dostępnych w systemie Fudo PAM dla renderowanych sesji HTTP.

3.2.3 ICA

Ostrzeżenie: Wsparcie protokołu `ICA` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

Wspierane tryby połączenia:

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

Wspierane aplikacje klienckie:

- Citrix Receiver.

Wspierane algorytmy szyfrujące:

- Basic
- TLS

Wspierane języki OCR:

- angielski,
- niemiecki,
- norweski,
- ukraiński,
- polski,
- węgierski,
- rosyjski.

Wspierane algorytmy kiedy szyfrowanie TLS jest włączone, a opcja *Starsze algorytmy kryptograficzne* wyłączona:

- `ecdhe-ecdsa-aes256-gcm-sha384`
- `ecdhe-rsa-aes256-gcm-sha384`
- `ecdhe-ecdsa-chacha20-poly1305`
- `ecdhe-rsa-chacha20-poly1305`
- `ecdhe-ecdsa-aes256-sha384`
- `dhe-rsa-aes256-gcm-sha384`

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.

- Obsługa połączeń ICA poprzez interfejs *Citrix StoreFront* wymaga użycia kont typu *anonymous* lub *forward*.
- Nawiązanie bezpośredniego połączenia z serwerem (z pominięciem *Citrix StoreFront*) wymaga utworzyenia pliku konfiguracyjnego `.ica`. Więcej informacji znajdziesz w rozdziale *Plik konfiguracyjny połączenia ICA*.

3.2.4 Modbus

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.
- Brak wsparcia dla trybu bastion z powodu ograniczeń protokołu.

3.2.5 MS SQL (TDS)

Ponieważ MS SQL Studio może nawiązywać wiele niezależnych połączeń dla przesłania zapytań, sesje, nawiązane przez protokół TDS korzystając z MS SQL Studio są agregowane przez Fudo PAM.

Fudo PAM działa według algorytmu, weryfikującego, czy obiekty nowej sesji (`gniazdo nasłuchiwania`, `konto`, `adres serwera (serwer)`, `użytkownik`, oraz `sejf`) są takie same, jak obiekty którejś z już trwających sesji. Jeśli tak jest, sesje są agregowane w jedną.

Natomiast, jeśli algorytm nie wykrywa żadnej trwającej sesji z obiektami nowej sesji, system tworzy nową sesję.

To powoduje, że w ramach jednej sesji wiele zapytań są zgrupowane. Każde zapytanie jest oznaczone tagiem, co pozwala wyświetlić w playerze tylko te połączenia, które są istotne (na przykład, zawierają zapytania, które faktycznie wykonał użytkownik).

Wspierane tryby połączenia:

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

Wspierane aplikacje klienckie:

- SQL Server Management Studio,
- sqsh.

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.

3.2.6 MySQL

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Wspierane aplikacje klienckie:

- Oficjalny klient MySQL,
- Biblioteki PyMySQL dla Pythona.

Uwagi:

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

3.2.7 RDP

Wspierane tryby połączenia:

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

Wspierane aplikacje klienckie:

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

Wspierane języki OCR:

- angielski,
- niemiecki,
- norweski,
- ukraiński,
- polski,
- węgierski,
- rosyjski.

Wspierane algorytmy kiedy jest wybrany poziom bezpieczeństwa TLS, a opcja *Starsze algorytmy kryptograficzne* wyłączona:

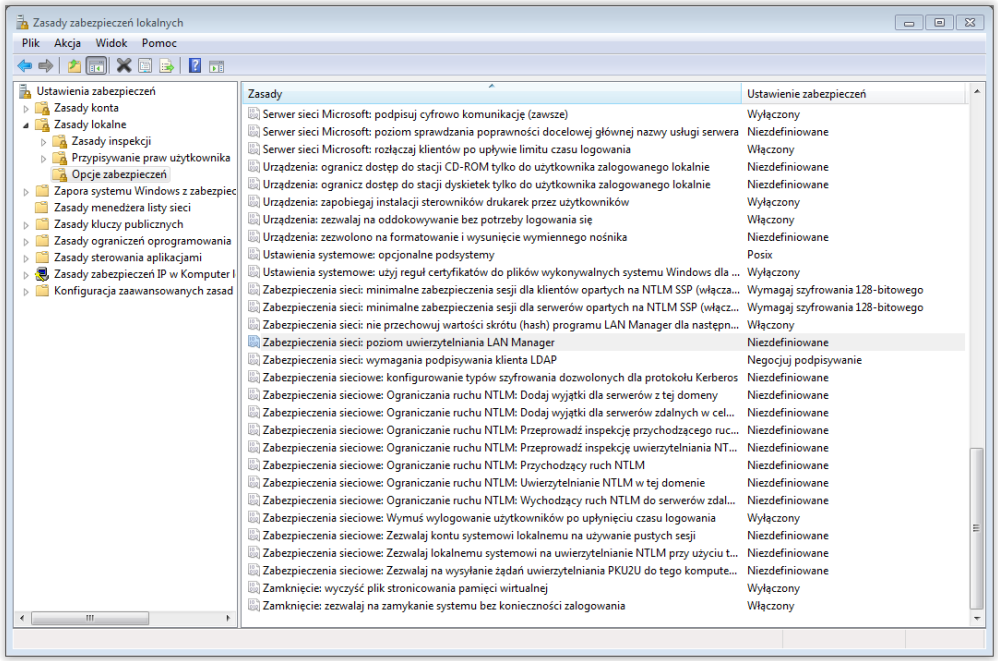
- `ecdhe-ecdsa-chacha20-poly1305`
- `ecdhe-rsa-chacha20-poly1305`

- `ecdhe-ecdsa-aes256-gcm-sha384`
- `ecdhe-rsa-aes256-gcm-sha384`
- `ecdhe-ecdsa-aes256-sha384`
- `ecdhe-rsa-aes256-sha384`
- `dhe-rsa-aes256-gcm-sha384`
- `aes256-gcm-sha384`
- `aes128-gcm-sha256`
- `aes128-sha256`

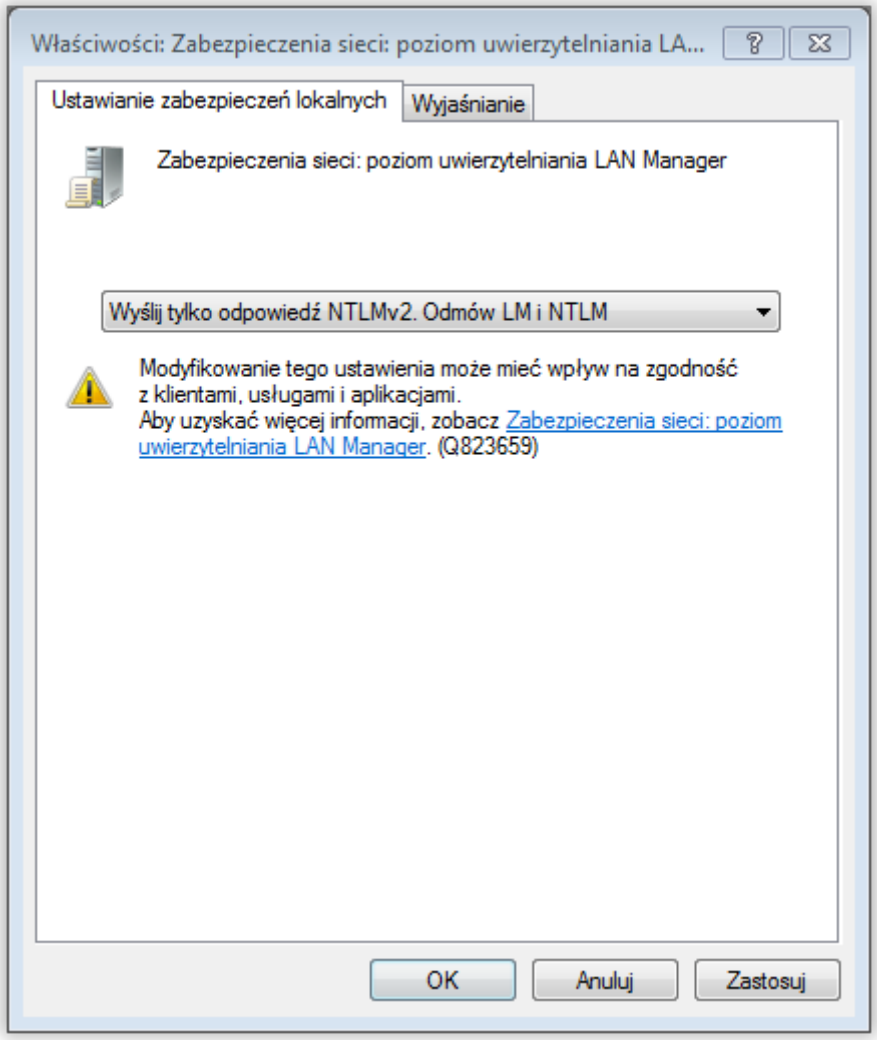
Uwagi:

- Implementacja wsparcia dla protokołu RDP umożliwia uwierzytelnienie poprzez protokół RADIUS, w trybie *challenge-response*.
- 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.
- W przypakdu uwierzytelnienia *Enhanced RDP Security (TLS) + NLA* Fudo PAM wymaga użycia protokołu NTML w wersji v2 lub nowszej. Aby poprawnie obsłużyć logowanie NLA włącz, po stronie klienta oraz serwera, opcję wysyłania tylko odpowiedzi NTLMv2:

  1. Kliknij *Start* > *Wszystkie Programy* > *Akcesoria* > *Uruchom*.
  2. Wpisz `secpol.msc` i kliknij *OK*.
  3. Wybierz *Zasady Lokalne* > *Opcje zabezpieczeń* i kliknij dwukrotnie *Zabezpieczenia sieci: poziom uwierzytelnienia LAN Manager*.



  4. Z listy rozwijalnej wybierz *Wyślij tylko odpowiedzi NTLMv2. Odmów LM i NTML*.



- Fudo PAM sprawdza i ustawia język wprowadzania danych w chwili zestawienia połączenia i nie wspiera dynamicznej zmiany języka na ekranie logowania.

RemoteApp

Fudo PAM natywnie wspiera mechnizm RemoteApp, nagrywając okna aplikacji tak samo jak połączenia RDP, z zachowaniem wszelkich restrykcji bezpieczeństwa.

Monitorowanie RemoteApp wymaga, aby połączenie było nawiązane poprzez odpowiednio przygotowany plik konfiguracyjny `*.rdp`, w którym zdefiniowany jest adres IP oraz numer portu Fudo PAM. Połączenia inicjowane poprzez *Remote Desktop Web Access* mogą być monitorowane jedynie w trybie transparentnym/bramy.

3.2.8 SSH

Wspierane tryby połączenia:

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

Wybrane wspierane funkcje:

- Multipleksowanie połączeń (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- SCP (surowy ruch, przerwanie sesji, możliwość wyodrębnienia poszczególnych plików),
- SFTP,
- 2FA,
- Przekierowanie portów (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- SSH Agent forwarding (przeźroczysty, nie rejestrujemy),
- X11 - w ramach protokołu SSH (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- Shell (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- Terminal (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch).

Wspierane algorytmy szyfrujące:

- Serwer: RSA, DSA
- Gniazdo nasłuchiwania: RSA, DSA

Wspierane funkcje skrótu (algorytmy hashujące):

- MD5
- SHA256

Wspierane typy kluczy SSH:

- RSA
- ED25519, ED25519-SK
- ECDSA, ECDSA-SK
- DSA (z włączoną opcją *Starsze algorytmy kryptograficzne*)

Wspierane kodowanie: UTF-8

Wspierane algorytmy kryptograficzne:

- Wspierane algorytmy *key exchange*:
  - `curve25519-sha256`
  - `curve25519-sha256@libssh.org`
  - `ecdh-sha2-nistp256`
  - `ecdh-sha2-nistp384`
  - `ecdh-sha2-nistp521`
  - `diffie-hellman-group-exchange-sha256`
  - `diffie-hellman-group16-sha512`
  - `diffie-hellman-group18-sha512`
  - `diffie-hellman-group14-sha256`
  - `diffie-hellman-group14-sha1`

- dodatkowo dochodzą 2 algorytmy *key exchange*, kiedy opcja *Starsze algorytmy kryptograficzne* zostaje włączona:
  - `diffie-hellman-group1-sha1`
  - `diffie-hellman-group-exchange-sha1`
- Wspierane algorytmy *host key*:
  - `ecdsa-sha2-nistp256-cert-v01@openssh.com`
  - `ecdsa-sha2-nistp384-cert-v01@openssh.com`
  - `ecdsa-sha2-nistp521-cert-v01@openssh.com`
  - `ssh-ed25519-cert-v01@openssh.com`
  - `rsa-sha2-512-cert-v01@openssh.com`
  - `rsa-sha2-256-cert-v01@openssh.com`
  - `ssh-rsa-cert-v01@openssh.com`
  - `ecdsa-sha2-nistp256`
  - `ecdsa-sha2-nistp384`
  - `ecdsa-sha2-nistp521`
  - `ssh-ed25519`
  - `rsa-sha2-512`
  - `rsa-sha2-256`
  - `ssh-rsa`
- dodatkowo dochodzą 2 algorytmy *host key*, kiedy opcja *Starsze algorytmy kryptograficzne* zostaje włączona:
  - `ssh-dss`
  - `ssh-dss-cert-v01@openssh.com`
- Wspierane algorytmy *encryption*:
  - `chacha20-poly1305@openssh.com`
  - `aes128-ctr`
  - `aes192-ctr`
  - `aes256-ctr`
  - `aes128-gcm@openssh.com`
  - `aes256-gcm@openssh.com`
- dodatkowo dochodzą 10 algorytmów *encryption*, kiedy opcja *Starsze algorytmy kryptograficzne* zostaje włączona:
  - `aes128-cbc`
  - `aes192-cbc`
  - `aes256-cbc`

  - `rijndael-cbc@lysator.liu.se`
  - `3des-cbc`
  - `arcfour256`
  - `arcfour128`
  - `arcfour`
  - `blowfish-cbc`
  - `cast128-cbc`
- Wspierane algorytmy *MAC*:
  - `umac-64-etm@openssh.com`
  - `umac-128-etm@openssh.com`
  - `hmac-sha2-256-etm@openssh.com`
  - `hmac-sha2-512-etm@openssh.com`
  - `hmac-sha1-etm@openssh.com`
  - `umac-64@openssh.com`
  - `umac-128@openssh.com`
  - `hmac-sha2-256`
  - `hmac-sha2-512`
  - `hmac-sha1`
- dodatkowo dochodzą 10 algorytmów *MAC*, kiedy opcja *Starsze algorytmy kryptograficzne* zostaje włączona:
  - `hmac-sha1-etm@openssh.com`
  - `hmac-sha1-96-etm@openssh.com`
  - `hmac-sha1-96`
  - `hmac-ripemd160`
  - `hmac-ripemd160@openssh.com`
  - `hmac-ripemd160-etm@openssh.com`
  - `hmac-md5`
  - `hmac-md5-96`
  - `hmac-md5-etm@openssh.com`
  - `mac-md5-96-etm@openssh.com`

Uwagi:

- Implementacja wsparcia dla protokołu SSH umożliwia uwierzytelnienie poprzez protokół RADIUS, w trybie *challenge-response*.

3.2.9 Telnet 3270

Wspierane tryby połączenia:

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

Wspierane aplikacje klienckie:

- IBM Personal Communications,
- c3270.

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.
- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

Informacja: Terminalowy klient `telnet(1)` dostępny w systemie operacyjnym FreeBSD, w przeciwieństwie do wersji dostępnych na dystrybucjach Linuxa (np. Debian), podczas nawiązywania sesji automatycznie przekazuje login użytkownika do serwera docelowego. Jest to związane z domyślnie włączonym parametrem `-a`, odpowiadającym za przekazywanie loginu. W konsekwencji, uwierzytelniając się przed serwerem docelowym, użytkownik nie będzie poproszony o login. Aby wyłączyć domyślne przekazywanie loginu, należy użyć parametru `-K` bądź parametru `-l` z pustym loginem. Zatem należy pamiętać, aby zwrócić uwagę na domyślne zachowanie używanego programu klienckiego.

3.2.10 Telnet 5250

Wspierane tryby połączenia:

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

Wspierane aplikacje klienckie:

- IBM Personal Communications,
- tn5250.

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.
- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

Informacja: Terminalowy klient `telnet(1)` dostępny w systemie operacyjnym FreeBSD, w przeciwieństwie do wersji dostępnych na dystrybucjach Linuxa (np. Debian), podczas nawiązywania sesji automatycznie przekazuje login użytkownika do serwera docelowego. Jest to związane z domyślnie włączonym parametrem `-a`, odpowiadającym za przekazywanie loginu. W konsekwencji, uwierzytelniając się przed serwerem docelowym, użytkownik nie będzie poproszony o login. Aby wyłączyć domyślne przekazywanie loginu, należy użyć parametru `-K` bądź parametru `-l` z pustym loginem. Zatem należy pamiętać, aby zwrócić uwagę na domyślne zachowanie używanego programu klienckiego.

3.2.11 Telnet

Wspierane tryby połączenia:

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

Uwagi:

- Konieczność dwukrotnego uwierzytelnienia - przed Fudo i bezpośrednio przed serwerem.

Informacja: Terminalowy klient `telnet(1)` dostępny w systemie operacyjnym FreeBSD, w przeciwieństwie do wersji dostępnych na dystrybucjach Linuxa (np. Debian), podczas nawiązywania sesji automatycznie przekazuje login użytkownika do serwera docelowego. Jest to związane z domyślnie włączonym parametrem `-a`, odpowiadającym za przekazywanie loginu. W konsekwencji, uwierzytelniając się przed serwerem docelowym, użytkownik nie będzie poproszony o login. Aby wyłączyć domyślne przekazywanie loginu, należy użyć parametru `-K` bądź parametru `-l` z pustym loginem. Zatem należy pamiętać, aby zwrócić uwagę na domyślne zachowanie używanego programu klienckiego.

3.2.12 VNC

Wspierane tryby połączenia:

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

Wspierane aplikacje klienckie:

- TightVNC,
- RealVNC.

Wspierane języki OCR:

- angielski,
- niemiecki,
- norweski,
- ukraiński,
- polski,
- węgierski,
- rosyjski.

Uwagi:

- Implementacja wsparcia dla protokołu VNC umożliwia uwierzytelnienie poprzez protokół RADIUS, w trybie *challenge-response*.

Charakterystyka połączenia - serwer wymaga uwierzytelnienia

- Konto typu *anonymous*: wymaga podania hasła logowania do serwera VNC.
- Konto typu *regular*: wymaga podania loginu i hasła (uwierzytelnienie przed Fudo); ciąg znaków, na który podmieniana jest nazwa użytkownika jest ignorowany.
- Konto typu *forward*: hasło uwierzytelniające zgodne ze zdefiniowanym po stronie serwera VNC.

Charakterystyka połączenia - serwer nie wymaga uwierzytelnienia

- Konto typu *anonymous*: nie wymaga podawania jakichkolwiek danych na ekranie logowania.
- Konto typu *regular*: wymaga podania loginu i hasła (uwierzytelnienie przed Fudo); ciąg znaków określający hasło przekazywane do systemu docelowego może być pusty.
- Konto typu *forward*: wymaga podania loginu i hasła (uwierzytelnienie przed Fudo);

3.2.13 X11

Protokół X11 wspierany jest w ramach protokołu SSH.

Informacja: Funkcja *dołączania do sesji* nie jest dostępna dla połączeń realizowanych za pośrednictwem protokołu X11.

Wspierane serwery:

- Xorg,
- Xming,
- XQuartz.

Wspierane czcionki:

Lista czcionek dostępnych w systemie Fudo PAM dla aplikacji korzystających z podstawowego protokołu X11 do rysowania tekstu. |

3.2.14 TCP

TCP to generyczny typ protokołu, służący do monitorowania połączeń nieszyfrowanych.

Wspierane tryby połączenia:

- *Brama*,
- *Pośrednik*,
- *Przezroczysty*.

Uwagi:

- Odtwarzacz prezentuje surowy tekst, bez renderowania graficznego.
- Brak możliwości dołączenia do sesji.
- Brak wsparcia szyfrowania SSL.

3.2.15 Pobranie hasła

Protokół sesji **Pobrania Hasła** jest protokołem wirtualnym i służy do nawiązania sesji dostępowej do hasła konta. W ramach tej sesji użytkownik wypożycza hasło poprzez funkcję *Rezerwuj hasło* na portalu i zwraca go używając opcji *Zdaj hasło* czym informuje system, że hasło już nie jest potrzebne.

Informacja: Protokół ten jest nazywany wirtualnym przez brak sesji TCP/IP, ponieważ są przechowywane same metadane sesji (na przykład, czas pobrania hasła, czas zdania hasła, kto dostał dostęp do hasła). Z związku z brakiem sesji TCP/IP oraz danych, które mogą później zostać odtworzone, sesje pobrania hasła są mniej obciążone zasobami, porównując z sesjami w oparciu o inne protokoły.

W przypadku przechwycenia hasła, nagranie sesji umożliwia wskazanie konkretnych użytkowników, którzy uzyskali dostęp do hasła.

Żądanie na pobranie hasła jest wysyłane użytkownikiem poprzez portal. Administrator może zaakceptować bądź odrzucić żądanie użytkownika w przypadku ustawienia opcji *Wymagaj potwierdzenia* w ustawieniach dostępowych Sejfu. Po zatwierdzeniu sesji użytkownik może podglądać oraz kopiować hasło w każdym momencie aktywnej sesji. Sesja przestaje być aktywna w momencie zdania hasła bądź jego wygaśnięcia (na przykład, przy ustawieniu opcji *Limit czasu rezerwacji hasła* dla konkretnego konta).

Hasło może zostać zwrócone automatycznie we wskazanym czasie bądź zdane manualnie przez użytkownika. Więcej informacji o konfiguracji czasu trwania sesji pobrania hasła na stronie *Dodawanie sejfu* pod zakładką *Użytkownicy* oraz na stronie *Dodawanie konta typu regular* w sekcji *Dane uwierzytelniające*.

Kiedy *Limit czasu rezerwacji hasła* jest skonfigurowany dla konta z trwającą obecnie sesją, inny użytkownik może pobrać jego hasło. W tym przypadku użytkownik powinien potwierdzić operację, wymuszając rezerwację hasła dla siebie.

Po zdaniu, hasło może zostać automatycznie zmienione na nowe, wygenerowane zgodnie z wybraną polityką modyfikatora hasła dla konta.

Uwagi:

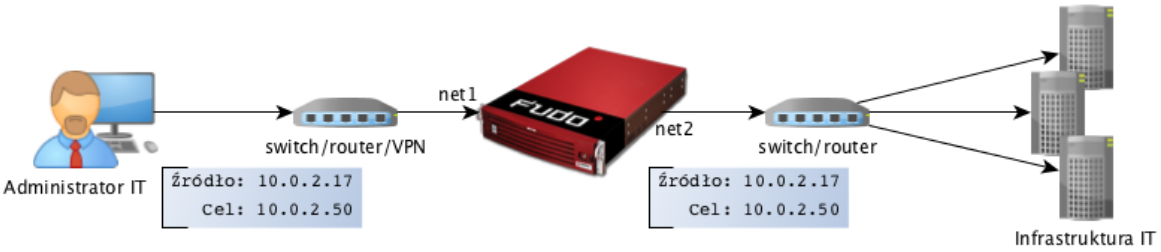
- Brak wsparcia mechanizmu dołączania do sesji.
- Brak wsparcia odtwarzacza.

3.3 Scenariusze wdrożenia

Informacja: Zaleca się umiejscowienie 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 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.



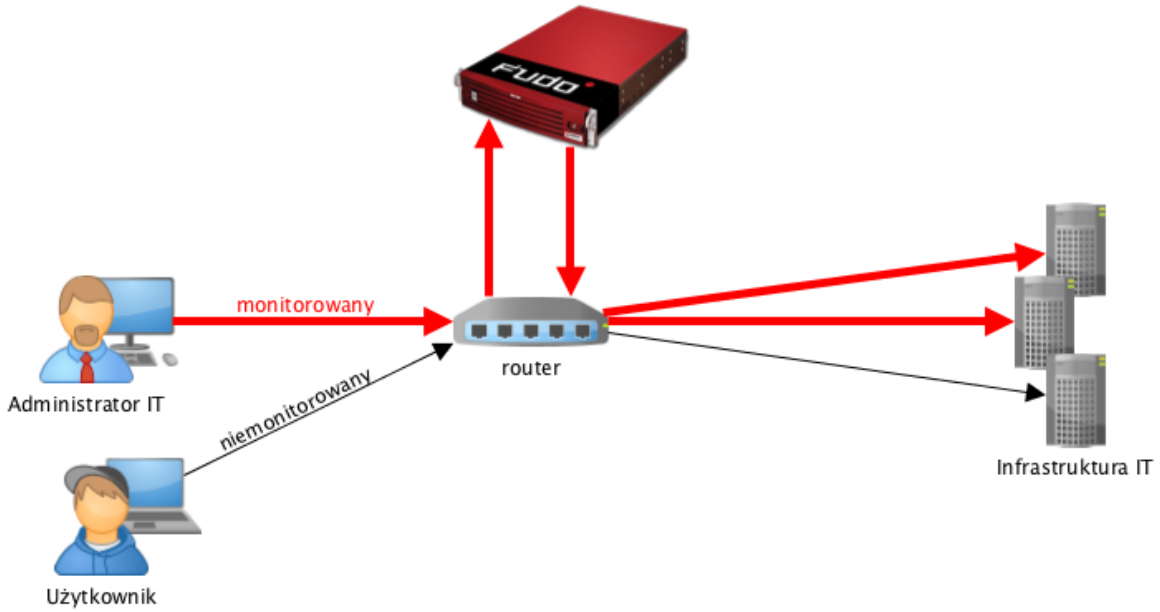
Fudo PAM pośrednicząc w przekazywaniu ruchu, zachowuje źródłowy adres IP klienta wysyłającego zapytania do serwerów.

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 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.

Tematy pokrewne:

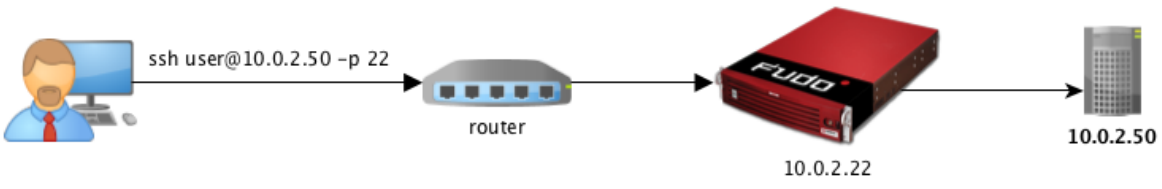
- *Tryby połączenia*
- *Zarządzanie serwerami*
- *Metody i tryby uwierzytelniania użytkowników*
- *Opis systemu*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*
- *Pierwsze uruchomienie*

3.4 Tryby połączenia

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

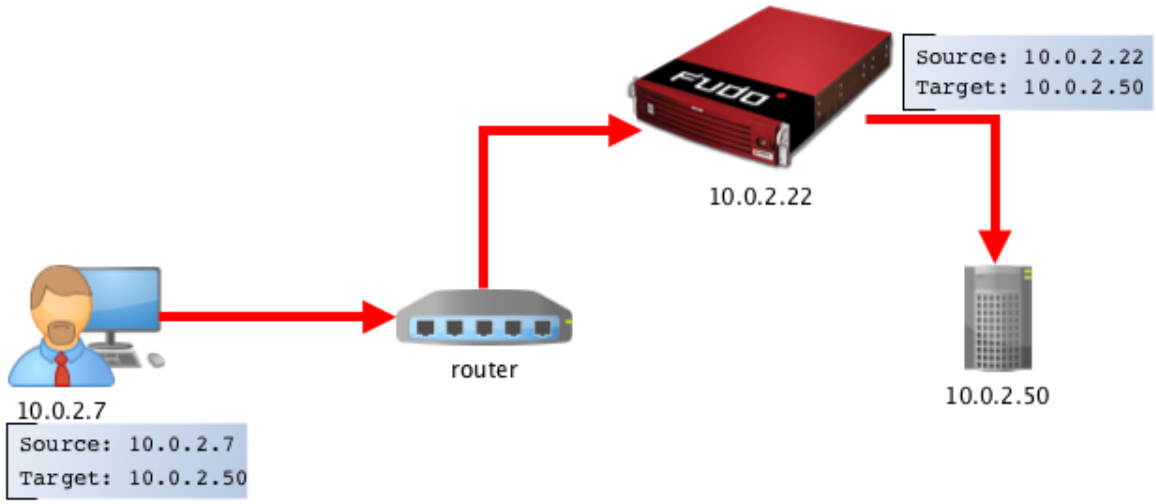
Przezroczysty

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



Brama

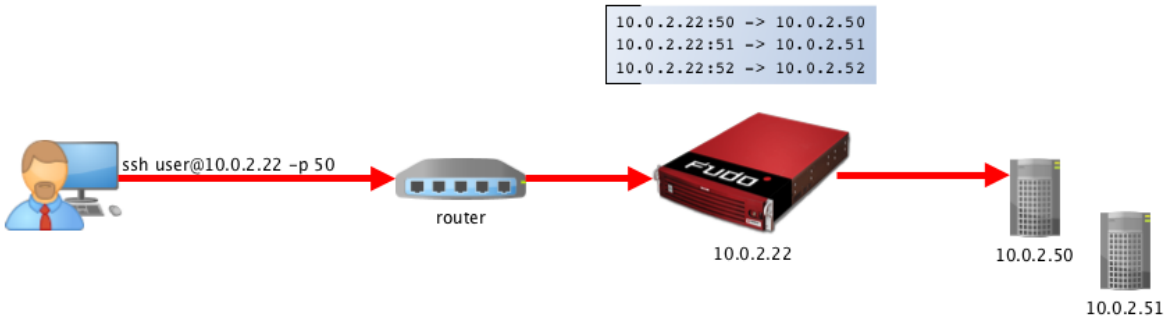
W trybie bramy, klient łączy się z serwerem docelowym wskazując bezpośrednio jego adres IP. Fudo PAM zestawiając połączenie z monitorowanym zasobem używa własnego adresu IP. Tryb pracy bramy pozwala na sterowanie ruchem sieciowym, by ten stale przechodził przez Fudo PAM, w przypadku gdy zastosowanie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



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

Pośrednik

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



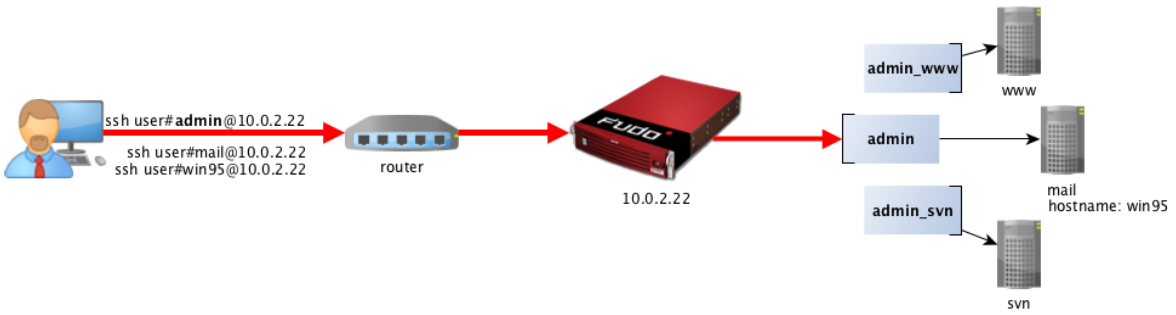
Takie rozwiązanie ukrywa faktyczną adresację serwerów, a odpowiednie ich skonfigurowanie pozwala na odrzucanie zapytań ze źródłowym adresem IP innym niż adres IP Fudo PAM.

Bastion

Informacja: Tryb bastion wspierany jest w połączeniach realizowanych za pośrednictwem protokołów: SSH, RDP, VNC, Telnet, Telnet 3270, Telnet 5250, MS SQL, ICA.

W trybie bastionu, konto na serwerze docelowym (lub sam serwer) zdefiniowane jest w ciągu identyfikującym użytkownika, np. `ssh user#mail@10.0.2.22`. 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: Ciąg wskazujący obiekt docelowy, musi jednoznacznie identyfikować konto lub serwer.

Sekwencja dopasowania obiektu docelowego:

1. Dokładne dopasowanie nazwy konta - Fudo PAM dokonuje próby dopasowania ciągu znaków do nazwy obiektu typu konto.
2. Dokładne dopasowanie nazwy serwera - Fudo PAM dokonuje próby dopasowania ciągu znaków do nazwy obiektu typu serwer.
3. Dokładne dopasowanie adresu serwera - Fudo PAM dokonuje próby dopasowania ciągu znaków do adresu IP lokalnie zdefiniowanego serwera.
4. Adres IP zwrócony przez usługę DNS - Fudo PAM odpytuje usługę DNS o nazwę hosta i dokonuje próby dopasowania zwróconego adresu IP z adresem IP lokalnie zdefiniowanego serwera.
5. Nazwa hosta zwrócona przez usługę DNS - Fudo PAM odpytuje usługę odwróconego DNS i dokonuje próby dopasowania zwrócenej nazwy hosta z lokalnie zdefiniowanym obiektem.

Informacja: Ze względu na szczególną interpretację znaku \ przez niektóre powłoki systemowe (np. bash), w celu prawidłowego zinterpretowania nazwy użytkownika i domeny podczas nawiązywania połączenia, należy odpowiednio sformatować ciąg znaków:

- „domena\uzytkownik”#bsd01@10.0.60.138
- «domena\uzytkownik»#bsd01@10.0.60.138
- domena\uzytkownik#bsd01@10.0.60.138

Tematy pokrewne:

- *Scenariusze wdrożenia*
- *Zarządzanie serwerami*
- *Metody i tryby uwierzytelniania użytkowników*
- *Opis systemu*
- *Szybki start - konfiguracja połączenia SSH*

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

3.5 Metody i tryby uwierzytelniania użytkowników

Metody uwierzytelniania użytkowników

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

Wspierane metody uwierzytelnienia:

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

Informacja:

- Zewnętrzne serwery uwierzytelniania CERB, RADIUS, LDAP, Active Directory, SMS oraz DUO, wymagają wcześniejszego skonfigurowania. Szczegółowe informacje na ten temat znajdziesz w rozdziale *Zarządzanie zewnętrznymi serwerami uwierzytelnienia*.
- W protokołach RDP, SSH i VNC, uwierzytelnienie RADIUS wspiera tryb *pytanie-odpowiedź* (ang. *challange-response*).

Tryby uwierzytelnienia

Po uwierzytelnieniu użytkownika, 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, Fudo PAM przekazuje wprowadzone przez użytkownika dane i wykorzystuje je w stanie niezmienionym do zestawienia połączenia z serwerem.

Informacja:

- Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, wprowadzony przez użytkownika login jest ignorowany przy zestawianiu połączenia.

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*.
- 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.
- Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, login zdefiniowany w koncie typu *regular* jest ignorowany przy zestawianiu połączenia.

Podwójne uwierzytelnienie

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

Uwierzytelnianie z podmianą hasła

W tym trybie, podczas zestawiania połączenia, Fudo PAM przekazuje wprowadzony przez użytkownika login i podmienia podane hasło.

Informacja:

- Hasło dostępu do serwera docelowego może być zdefiniowane w obiekcie, lub każdorazowo pobierane z zewnętrznego repozytorium haseł. Więcej informacji znajdziesz w rozdziale *Zewnętrzne repozytoria haseł*.
- Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, login użytownika jest ignorowany przy zestawianiu połączenia.

Uwierzytelnienie przez serwer docelowy

W tym trybie, Fudo PAM przekazuje dane logowania do serwera docelowego, który weryfikuje ich poprawność i przekazuje status weryfikacji do Fudo PAM. Tryb uwierzytelnienia przez serwer docelowy dostępny jest dla połączeń *ssh* oraz *RDP* w trybie NLA.

Autoryzacja dostępu przez administratora

Fudo PAM umożliwia skonfigurowanie sejfu tak, aby każde żądanie połączenia realizowane za pośrednictwem danego obiektu, wymagało potwierdzenia przez administratora z poziomu interfejsu administracyjnego.

Tematy pokrewne:

- *Dodawanie sejfu*
- *Akceptowanie żądań użytkowników*
- *Odrzucanie żądań użytkowników*
- *Opis systemu*
- *Mechanizmy bezpieczeństwa*

3.6 Mechanizmy bezpieczeństwa

3.6.1 Szyfrowanie danych

Dane przechowywane na 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 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 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 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.

Baza danych

Dane wrażliwe, takie jak hasła, klucze, loginy itp., są dodatkowo szyfrowane w bazie danych Fudo. Klucz szyfrujący, zwany Master Key, to losowy ciąg 256 bitów i służy do uzyskiwania dalszych kluczy używanych do szyfrowania każdej sekcji bazy danych, takich jak informacje konfiguracyjne (dane użytkownika, konta, sejfy itp.), kopia zapasowa bazy danych i system plików na zewnętrznej macierzy. Ponadto, Fudo wykorzystuje kod HMAC do „zapieczętowania" zaszyfrowanych danych. Klucz główny (Master Key) może zostać wyeksportowany przez superadministratora, ale tylko wtedy, gdy ten przed eksportem prześle do Fudo klucz do zaszyfrowania samego klucza głównego. Dopiero wtedy będzie możliwe odtworzenie Master Key, a co za tym idzie danych zaszyfrowanych kluczami wynikającymi z klucza głównego.

3.6.2 Kopie zapasowe

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

3.6.3 Uprawnienia użytkowników

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

Więcej informacji na temat uprawnień użytkowników znajdziesz w rozdziale *Role użytkownika*.

3.6.4 Sandboxing

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

3.6.5 Niezawodność

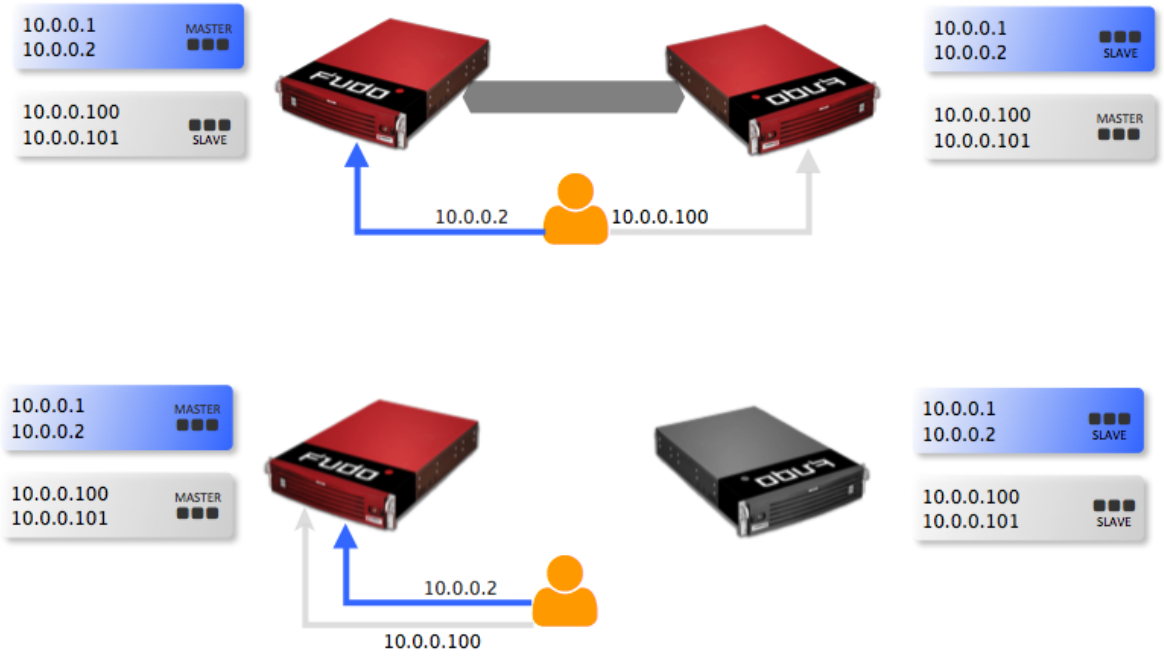
Fudo PAM dostarczane jest w konfiguracji sprzętowej zapewniającej optymalną wydajność i wysoką niezawodność systemu.

3.6.6 Konfiguracja klastrowa

Fudo PAM może pracować w konfiguracji klastrowej. Układ klastrowy pracuje w trybie multi-master, 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*

3.7 Model danych

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 (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

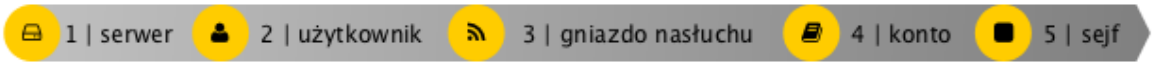
Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

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.

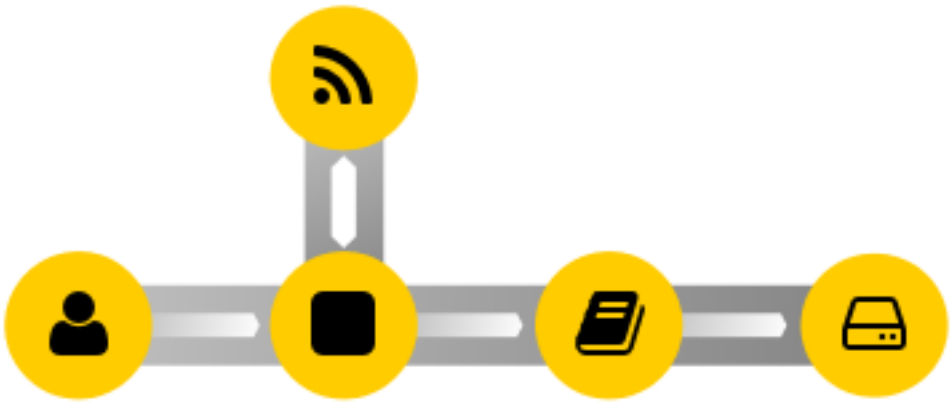
Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

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



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 replikacją danych, skontaktuj się z działem wsparcia technicznego.

Schemat relacji obiektów



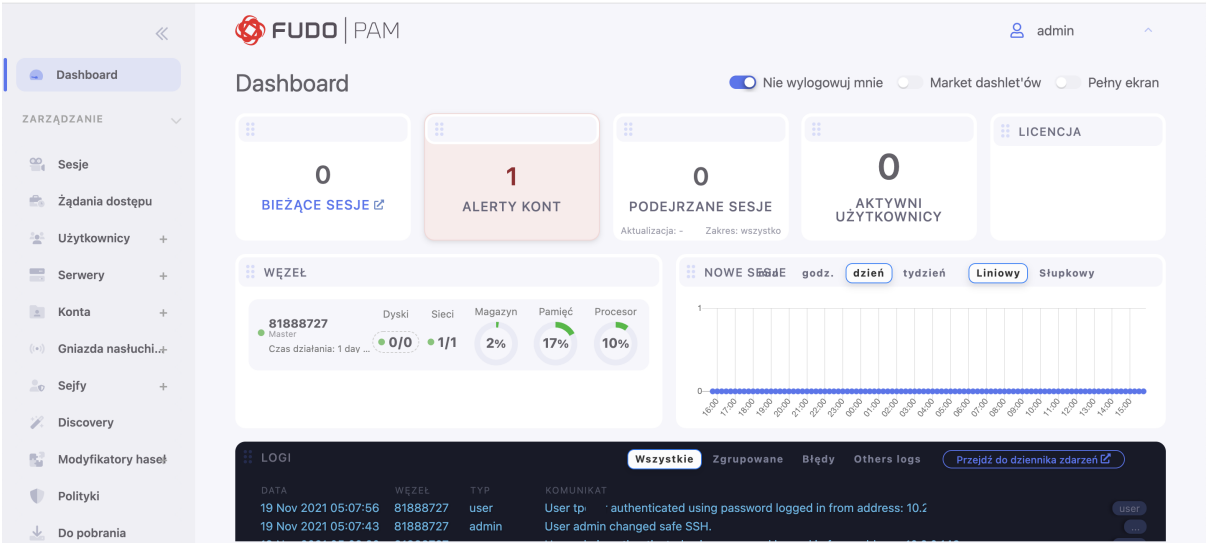
Sejf jest centralnym obiektem modelu danych, który reguluje dostęp do monitorowanych serwerów. Wskazuje konta uprzywilejowane na systemach docelowych, wraz z gniazdami nasłuchiwania określającymi właściwe dla *wybranego trybu* parametry połączenia (np. adres IP, numer portu). Taki model danych pozwala na optymalne zarządzanie obiektami. Jeden serwer może być dostępny w kilku różnych trybach połączenia, określonych przez gniazdo nasłuchiwania. Sejf grupuje konta pozwalając na wygodne regulowanie dostępnu do monitorowanych zasobów.

Tematy pokrewne:

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

3.8 Dashboard

Widok główny panelu administracyjnego Fudo PAM umożliwia szybki dostęp do informacji o stanie urządzenia. Układ elementów jest konfigurowalny co pozwala na dostosowanie prezentowanych informacji do potrzeb użytkownika.



Informacja:

- Zaznacz opcję *Nie wylogowuj mnie*, aby sesja nie wygasła, tak długo jak użytkownik pozostaje na ekranie startowym.
- Zaznacz opcję *Pełen ekran*, aby włączyć widok pełnoekranowy.

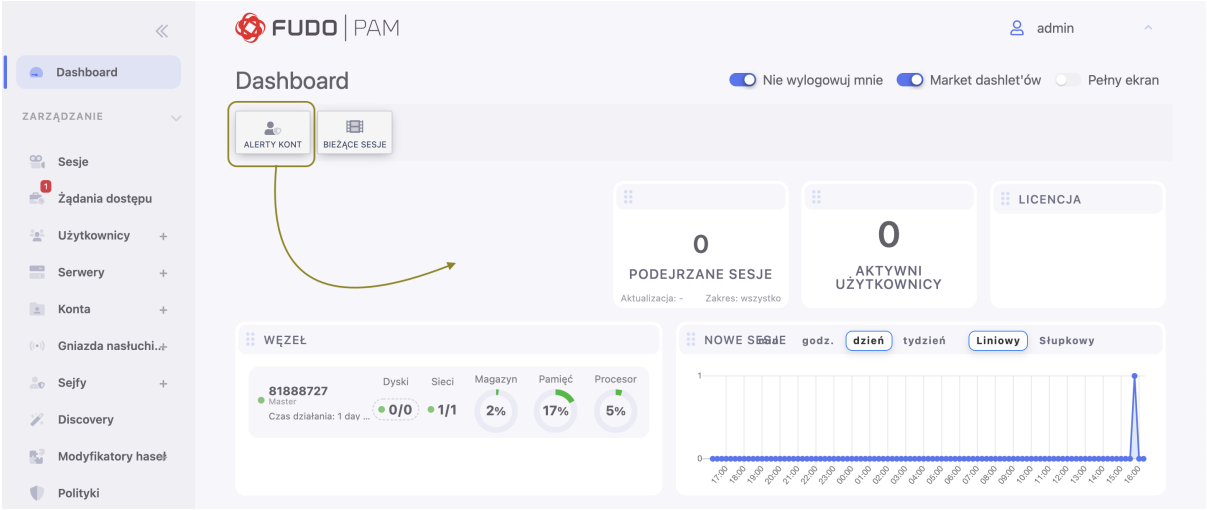
3.8.1 Widgety

Nowe sesje	Wykres obrazujący liczbę nowo nawiązanych połączeń w jednostce czasu.
Aktualne sesje	Liczba aktualnie zestawionych połączeń.
Sesje podejrzane	Liczba sesji o wysokim stopniu zagrożenia. Widget pozwala wyświetlać podejrzane sesje według następujących konfiguracji czasowych: z ostatnich 12 godzin, ostatniego dnia, ostatniego tygodnia, lub z ostatniego miesiąca.
Account alerts	Number of accounts at risk of a security breach.
Alerty konta	Konta, w przypadku których wystąpiło zagrożenie naruszenia bezpieczeństwa.
Aktywni użytkownicy	Liczba aktualnie połączonych użytkowników.
Licencja	Informacje dotyczące aktywnej licencji.
Węzeł	Informacje statusowe dotyczące instancji Fudo PAM oraz pozostałych węzłów klastra.
Logi systemowe	Ostatnie wpisy systemowego dziennika zdarzeń.

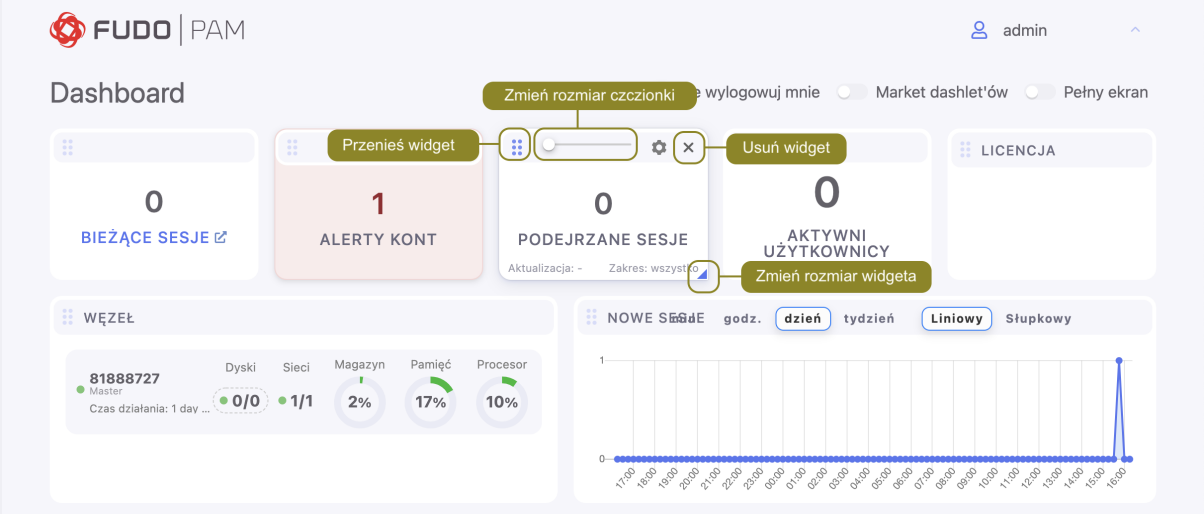
Informacja: Dostępność widgetów zależy od *roli przypisanej użytkownikowi*.

3.8.2 Zarządzanie widgetami

1. Kliknij *Market dashlet'ow*, aby wyświetlić dostępne elementy.
2. Kliknij wybrany widget i przeciągnij go na obszar roboczy.



3. Kliknij i przeciągnij prawy dolny róg widgetu, aby zmienić jego rozmiar.
4. Kliknij i przciągnij lewy górny róg widgetu, aby zmienić jego pozycję.
5. Kliknij suwak pod wartością liczbową, aby zmienić rozmiar czcionki.
6. Kliknij ✖ w prawym górnym roku elementu, który chcesz usunąć.

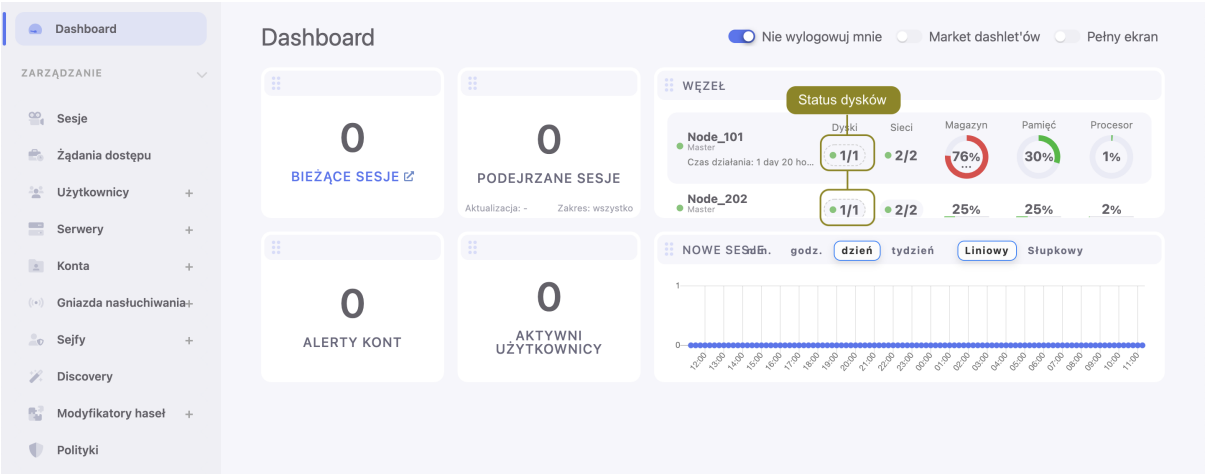


- Kliknij *Usuń*, aby potwierdzić usunięcie widgetu.

Informacja: Usunięte widgety dostępne są do ponownego wybrania w *Markecie dashlet'ow*.

3.8.3 Status dysków

Aby wyświetlić status dysków twardych macierzy, kliknij ikonę statusu dysków na widgecie *WĘZEŁ*.



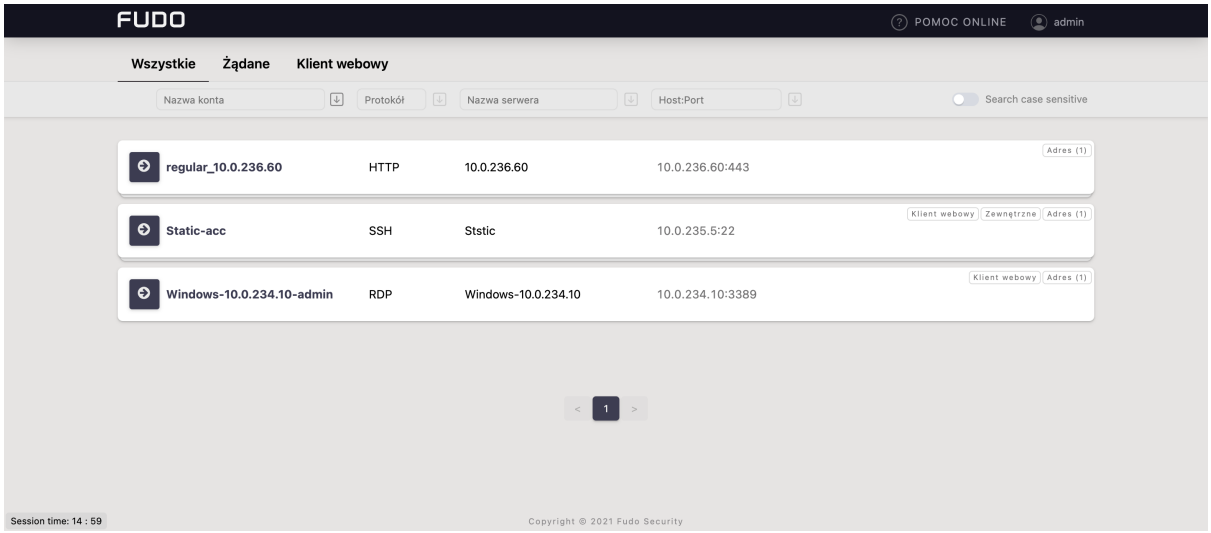
●	Dysk pracuje prawidłowo.
●	Dysk w trakcie synchronizacji danych.
●	Błędy odczytu/zapisu danych - dysk nie działa prawidłowo i może wkrótce ulec awarii - skontaktuj się z działem wsparcia technicznego w celu omówienia dalszych kroków mających na celu przywrócenie urządzenia do pełnej sprawności.
●	Awaria dysku - dysk wymaga wymiany, skontaktuj się z działem wsparcia technicznego w celu omówienia dalszych kroków mających na celu przywrócenie urządzenia do pełnej sprawności.

Tematy pokrewne:

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

3.9 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.



3.10 Licencje produktów stron trzecich

Rozdział zawiera informacje na temat licencji produktów stron trzecich wykorzystywanych przez Fudo PAM

Zbiór licencji najważniejszych narzędzi, z których korzystamy podczas rozwoju naszego produktu dostępny jest pod tym adresem. Przejdź do wskazanej lokalizacji w celu zapoznania się z ich treścią.

Jeśli szukana licencja nie jest dostępna w katalogu, to oznacza, że nie została udostępniona przez producenta.

ROZDZIAŁ 4

Instalacja i pierwsze uruchomienie

Ten rozdział opisuje urządzenie fizyczne i procedurę pierwszego uruchomienia.

4.1 Wymagania

Panel zarządzający

Zarządzanie systemem odbywa się za pomocą panelu administracyjnego dostępnego z poziomu przeglądarki internetowej. Zalecanymi przeglądarkami są Google Chrome, Mozilla Firefox oraz Microsoft Edge (wersja oparta na Chromium).

Wymagania sieciowe

Poprawne działanie Fudo PAM wymaga:

- Możliwości wykonywania połączeń dla sesji administracyjnych na port 443 urządzenia.
- Możliwości wykonywania połączeń do Fudo PAM przez klientów oraz z Fudo PAM do maszyn docelowych.
- Prawidłowo działającego *serwera czasu*.

Wymagania sprzętowe

Fudo PAM jest całościowym rozwiązaniem sprzętowo-programowym. Zainstalowanie urządzenia wymaga fizycznej przestrzeni 2U (model F100x) lub 3U (model F300x) w szafie serwerowej oraz podłączenie do infrastruktury sieciowej.

Wymagania dla maszyny wirtualnej

	100 sesji jednoczesnych*	200 sesji jednoczesnych*	300 sesji jednoczesnych*
CPU	6 rdzeni 3.60 GHz	20 rdzeni 2.40 GHz	28 rdzeni 2.60 GHz
RAM	32 GB	64 GB	128 GB

	6 miesięcy użytkowania**	2 lata użytkowania**	7 lat użytkowania**
Przechowywanie danych	24 TB	96 TB	288 TB

* 30% sesji graficznych FullHD 32bit, 70% połączeń terminalowych

** średnio 50 sesji dziennie, 70% RDP - FullHD 32bit, 30% SSH

Docelowe środowiska wirtualizacji:

- VMware Tools
- VirtualBox
- Proxmox
- Hyper-V
- Azure

Wymagania dla klienta VNC

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

4.2 Urządzenie

Fudo PAM dostarczane jest w obudowie do montażu w standardowej szafie serwerowej 19", w rozmiarze 2U (model F100x), 3U (model F300x) lub 4U (model F500x).

Fudo PAM F1002

- Obudowa: 19" 2U
- Wymiary: 89 mm (wysokość), 437 mm (szerokość), 647 mm (głębokość)
- Zasilanie: 2x 920 W
- Pamięć systemowa: 32 GB
- Wewnętrzna przestrzeń danych: 12x 2 TB, 2x 480 GB SSD
- Interfejsy sieciowe:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

  Sytuacja może różnić się w zależności od zastosowania kart rozszerzeń.

Fudo PAM F3002

- Obudowa: 19” 3U
- Wymiary: 132 mm (wysokość), 437 mm (szerokość), 647 mm (głębokość)
- Zasilanie: 2x 1000 W
- Pamięć systemowa: 64 GB
- Wewnętrzna przestrzeń danych: 16x 6 TB, 2x 480 GB SSD
- Interfejsy sieciowe:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

Sytuacja może różnić się w zależności od zastosowania kart rozszerzeń.

Fudo PAM F5000

- Obudowa: 19” 4U
- Wymiary: 178 mm (wysokość), 437 mm (szerokość), 699 mm (głębokość)
- Zasilanie: 2x 1280 W
- Pamięć systemowa: 128 GB
- Wewnętrzna przestrzeń danych: 36x 8 TB, 2x 480 GB SSD
- Interfejsy sieciowe:
  - 4 x RJ45 Gigabit Ethernet LAN ports
  - 1 x RJ45 Dedicated IPMI LAN port

  Sytuacja może różnić się w zależności od zastosowania kart rozszerzeń.

Tematy pokrewne:

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

4.3 Pierwsze uruchomienie

Urządzenie fizyczne

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, zgodnie z procedurą opisaną w rozdziale *Sporządzanie kopii zapasowej kluczy szyfrujących*.

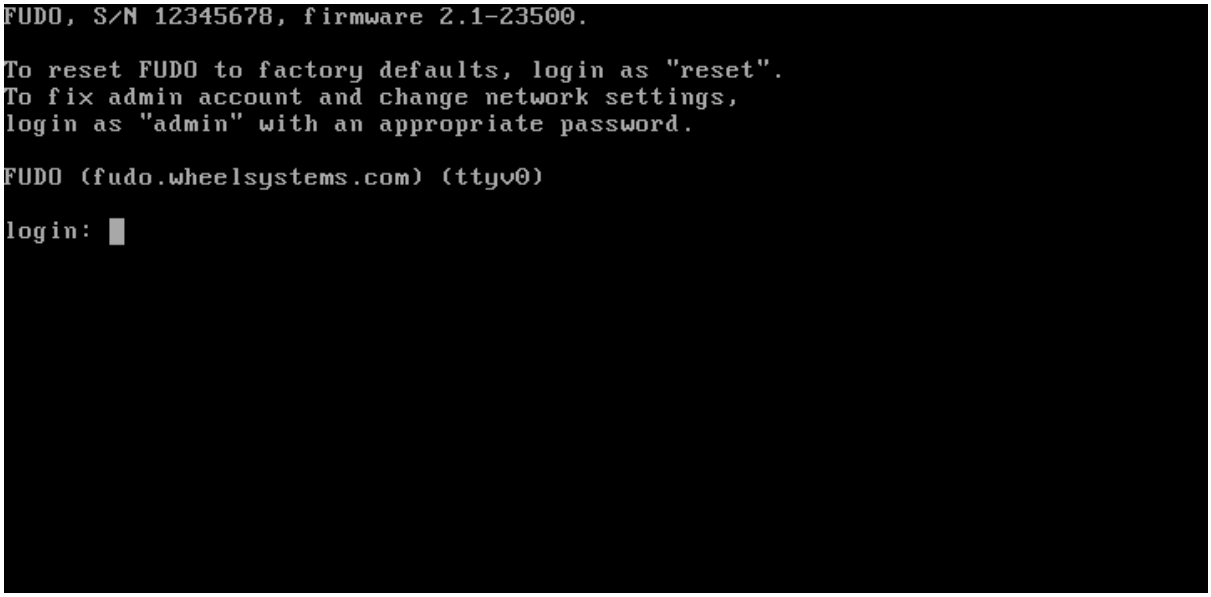
Ustawienie adresu IP z konsoli

1. Podłącz do urządzenia monitor i klawiaturę.
2. Wprowadź login konta administratora.

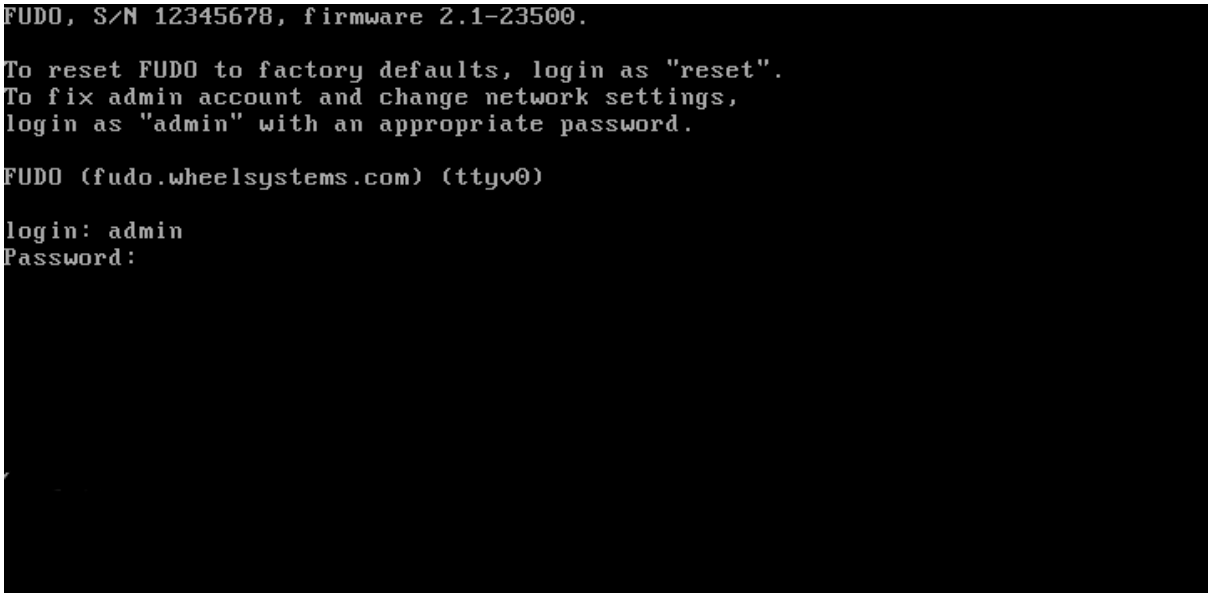
Informacja: Domyślne dane logowania:

login: admin
hasło: proxycrypto

Dla wersji w chmurze domyślnym hasłem jest zazwyczaj identyfikator maszyny wirtualnej dostarczanej z Fudo PAM. Skontaktuj się ze sprzedawcą lub wsparciem technicznym, aby dowiedzieć się więcej.



3. Wprowadź hasło do konta administratora.



4. Wpisz 2 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):
```

5. 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):
```

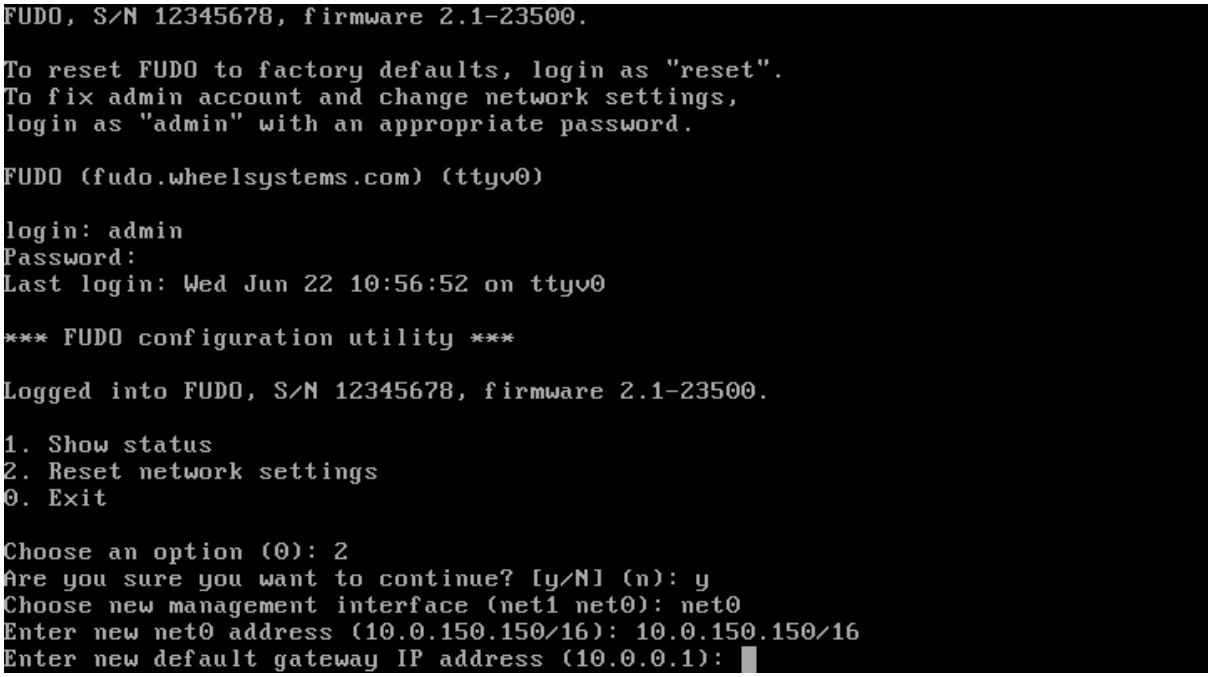
6. Wprowadź nazwę interfejsu zarządzającego (poprzez interfejs zarządzający udostępniany jest panel administracyjny Fudo PAM) i naciśnij klawisz *Enter*.

```
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):
```

7. 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
```

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



Tematy pokrewne:

- *Wymagania*
- *Sporządzanie kopii zapasowej kluczy szyfrujących*
- *Szybki start - konfiguracja połączenia SSH*
- *Szybki start - konfiguracja połączenia RDP*
- *Opis systemu*
- *Mechanizmy bezpieczeństwa*

ROZDZIAŁ 5

Szybki start

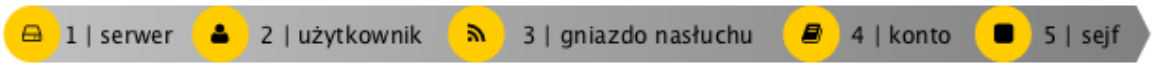
5.1 SSH

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji 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 Fudo PAM używając własnego loginu i hasła (`john_smith`/`john`). Fudo PAM zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `root`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

5.1.1 Założenia

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

5.1.2 Konfiguracja



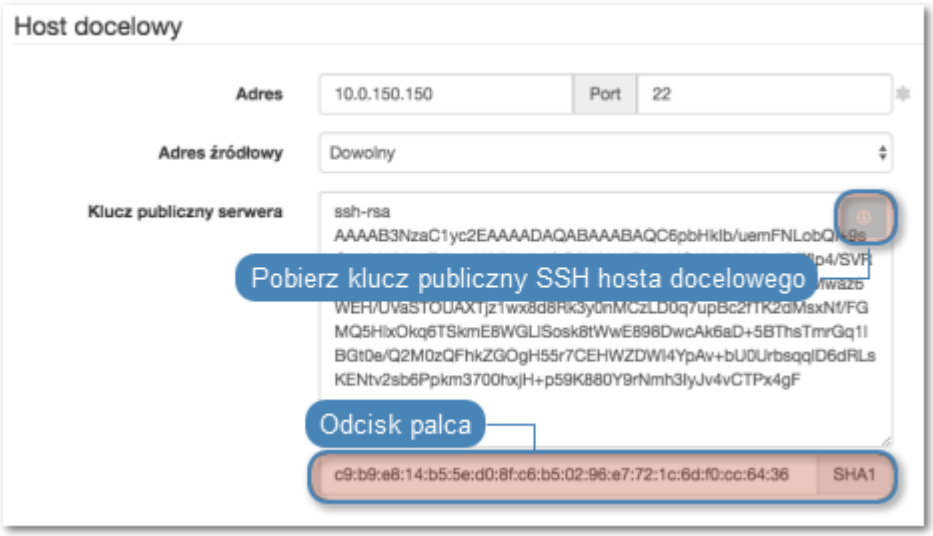
Dodanie serwera

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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	ssh_server
Opis	✘
Zablokowane	✘
Protokół	`SSH`
Starsze algorytmy kryptograficzne	✘
Adres źródłowy	`Dowolny`
Uprawnienia	
Uprawnieni użytkownicy	✘
Adresy serwerów	
Adres IP	`10.0.150.150`
Port	`22`

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 (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Ogólne	
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	✗
Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

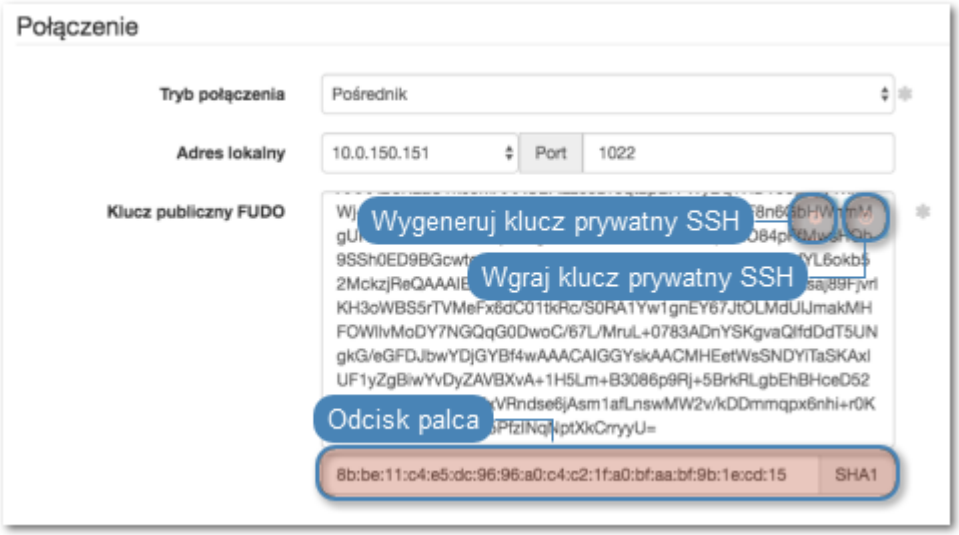
Dodanie gniazda nasłuchiwania

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`
Starsze algorytmy kryptograficzne	✗
Nierozróżnianie wielkości liter	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`1022`
Adres zewnętrzny	✗
Port zewnętrzny	✗

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`
Notatki	✘
Retencja danych	
Nadpisz globalne ustawienia retencji	✘
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	✘

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	✘
Powiadomienia	✘
Powód logowania	✘
Wymagaj potwierdzenia	✘
Polityki	✘
Note access	`No access`

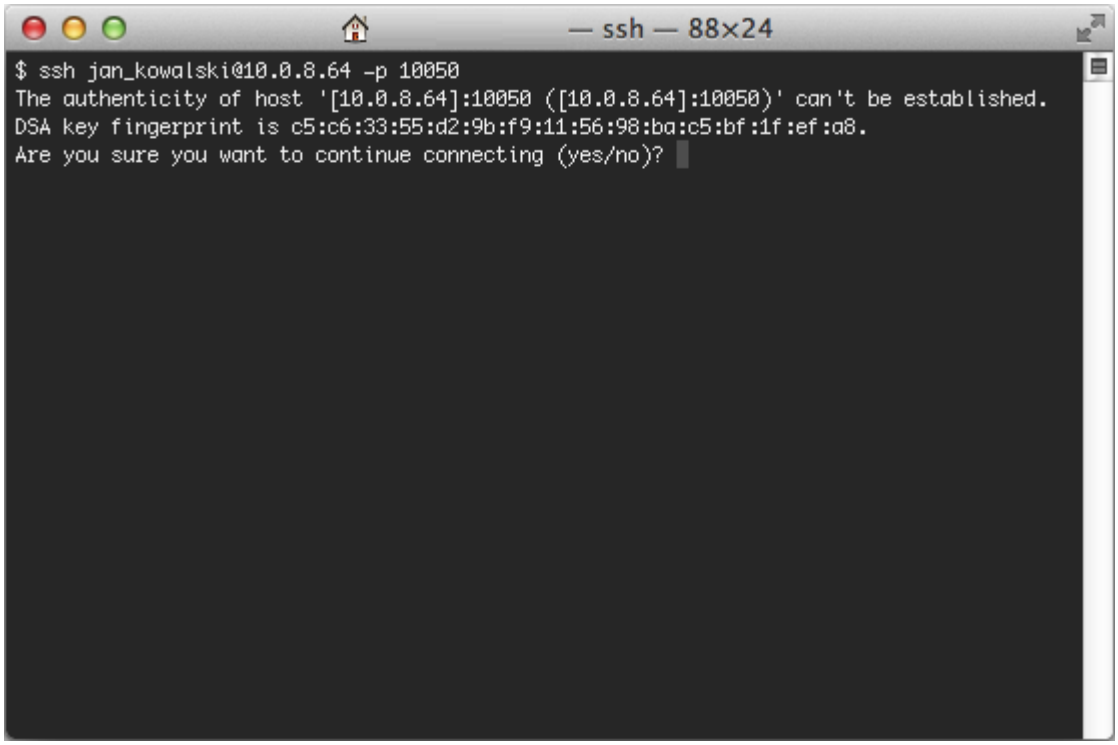
Funkcjonalność protokołów	
RDP	✘
SSH	✔
VNC	✘

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_ssh_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `ssh_listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.1.3 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.

5.1.4 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 Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.

Tematy pokrewne:

- *Aplikacje klienckie - PuTTY*
- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Wymagania*
- *Model danych*

5.2 SSH w trybie bastionu

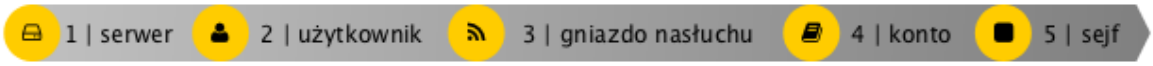
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo PAM, której celem jest monitorowanie połączeń SSH ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *SSH* uwierzytelnia się przed Fudo PAM używając własnego loginu i hasła (`john_smith`/`john`). Nawiązując połączenie, użytkownik wskazuje konto `admin_ssh_server` i adres IP Fudo PAM. Połączenie realizowane jest za pośrednictwem portu numer 22, domyślnego dla protokołu SSH.

Fudo PAM zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `root`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

5.2.1 Założenia

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

5.2.2 Konfiguracja



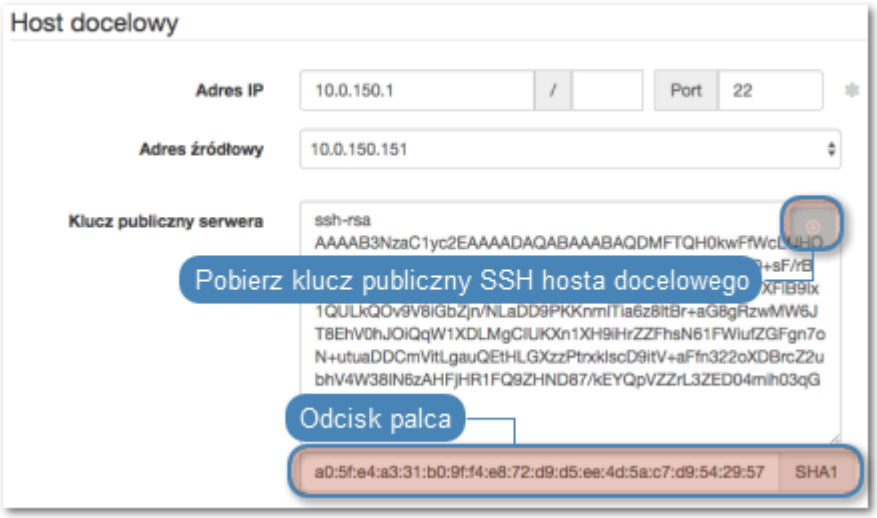
Dodanie serwera

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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	ssh_server
Opis	✗
Zablokowane	✗
Protokół	`SSH`
Starsze algorytmy kryptograficzne	✗
Adres źródłowy	`Dowolny`
Uprawnienia	
Uprawnieni użytkownicy	✗
Adresy serwerów	
Adres IP	`10.0.150.1`
Port	22

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 (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗
Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

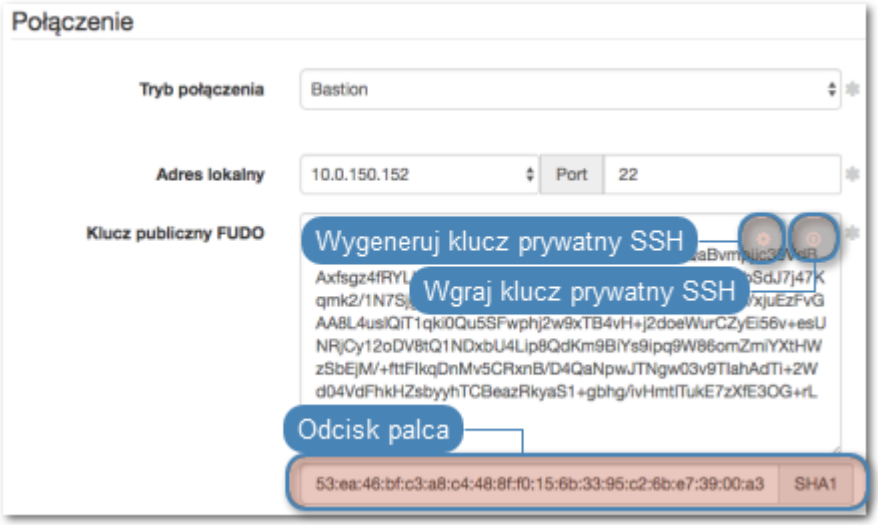
Dodanie gniazda nasłuchiwania

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`
Starsze algorytmy kryptograficzne	✗
Nierozróżnianie wielkości liter	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Tryb połączenia	`Bastion`
Adres lokalny	`10.0.150.151`
Port	22
Adres zewnętrzny	✗
Port zewnętrzny	✗

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*.

Informacja: Upewnij się, że w ustawieniach sieciowych, na wskazanym adresie IP nie jest włączona opcja dostępu administracyjnego .

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`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
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	`Statyczne, bez ograniczeń`

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	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

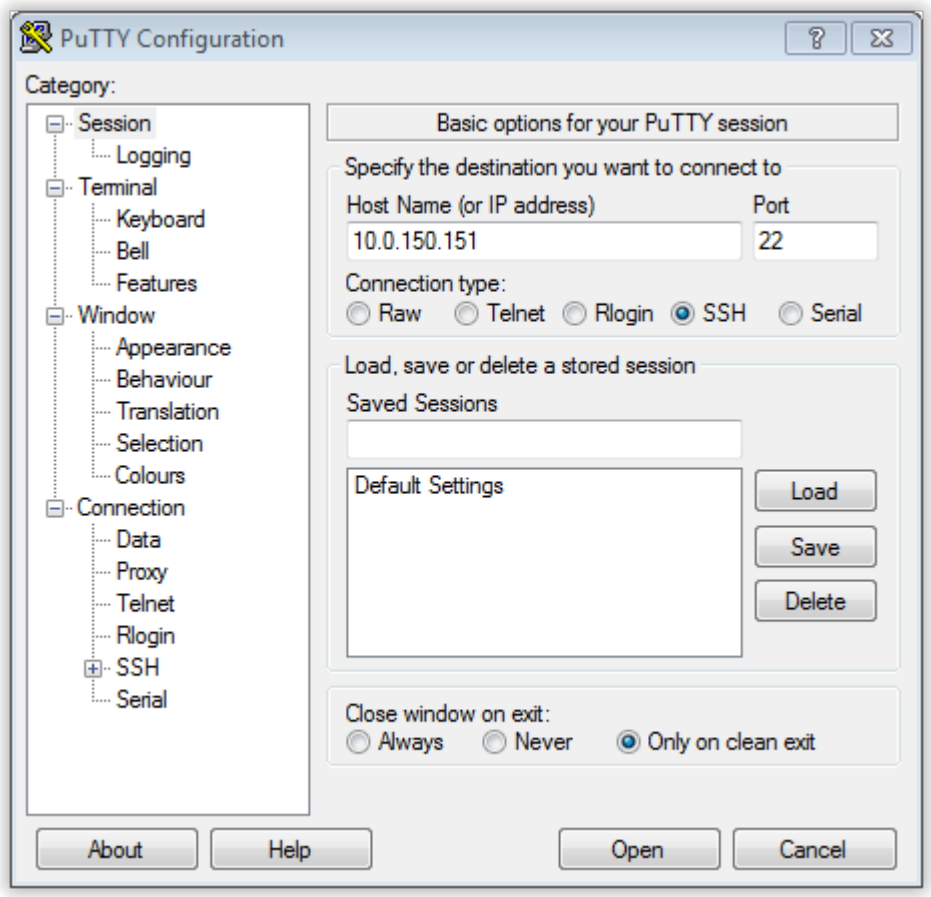
Funkcjonalność protokołów	
RDP	✗
SSH	✓
VNC	✗

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_ssh_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `ssh_listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

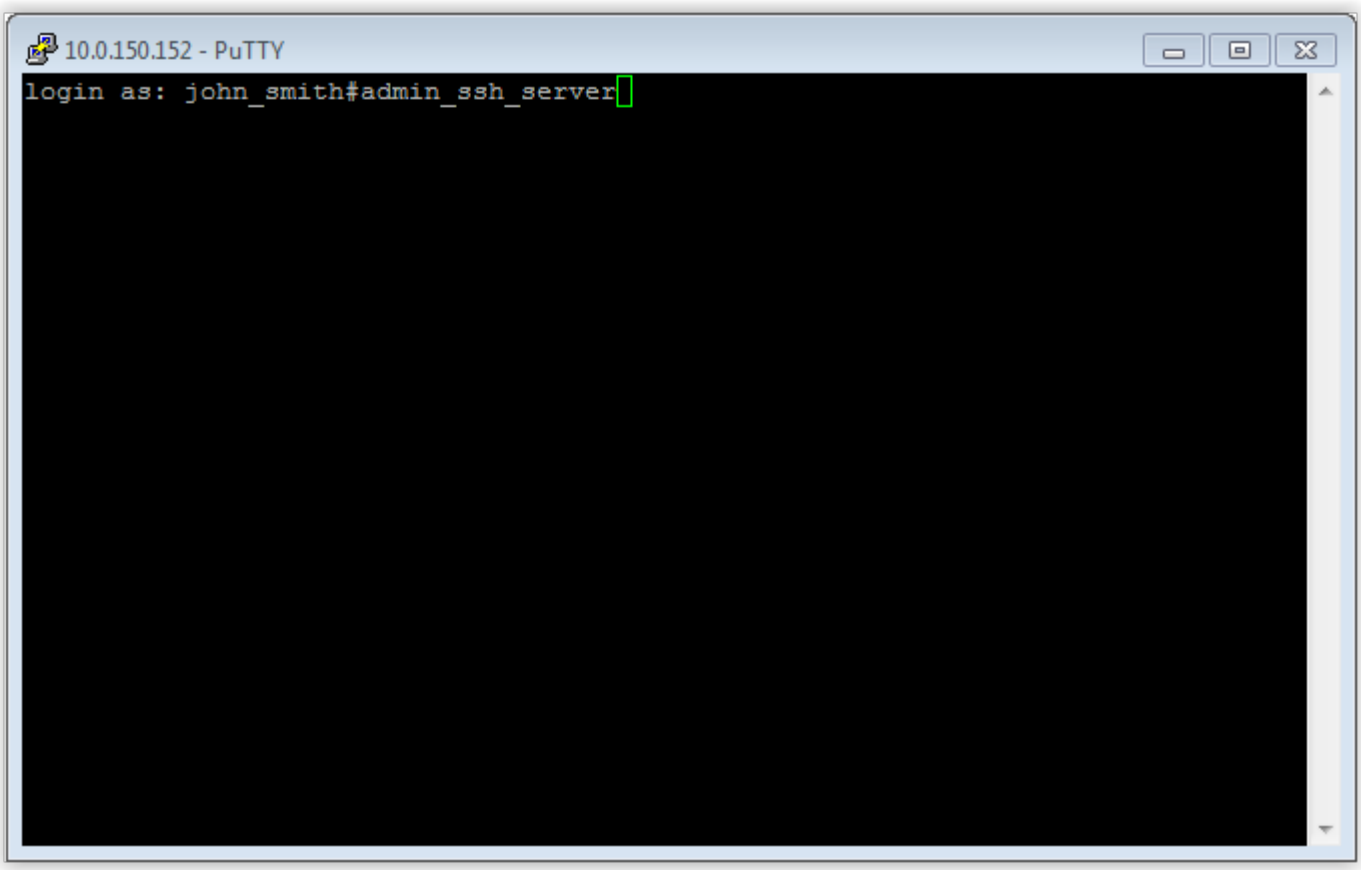
5.2.3 Nawiązanie połączenia

PuTTY - klient SSH dla systemu operacyjnego Microsoft Windows

1. Pobierz i uruchom PuTTY.
2. W polu *Host Name (or IP address)* wprowadź adres `10.0.150.151`.
3. Określ typ połączenia `SSH` i pozostaw domyślny numer portu.



4. Kliknij *Open*.
5. Wprowadź nazwę użytkownika wraz z nazwą konta, na serwerze docelowym.



Informacja: Alternatywnie, zamiast nazwy konta, możesz wskazać nazwę obiektu serwera tj. `john_smith#ssh_server`.

6. Wprowadź hasło użytkownika.

Interfejs linii komend

Wykonaj komendę:

```
ssh john_smith#admin_ssh_server@10.0.150.151
```

Informacja: Ze względu na szczególną interpretację znaku \ przez niektóre powłoki systemowe (np. bash), w celu prawidłowego zinterpretowania nazwy użytkownika i domeny podczas nawiązywania połączenia, należy odpowiednio sformatować ciąg znaków:

- „domena\uzytkownik”#bsd01@10.0.60.138
- «domena\uzytkownik»#bsd01@10.0.60.138
- domena\uzytkownik#bsd01@10.0.60.138

5.2.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres `10.0.150.150`.

2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego 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*

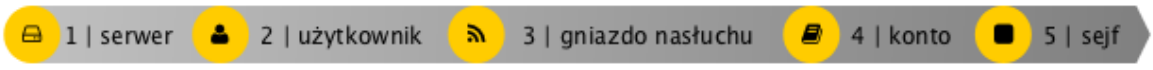
5.3 RDP

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji 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. 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*).

5.3.1 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*.

5.3.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	rdp_server
Opis	`Serwer RDP`
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Adres źródłowy	`Dowolny`

Uprawnienia	
Uprawnieni użytkownicy	✗

Adresy serwerów	
Adres IP	`10.0.35.10`
Port	`3389`

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

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Ogólne	
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	✗
Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

4. Kliknij *Zapisz*.

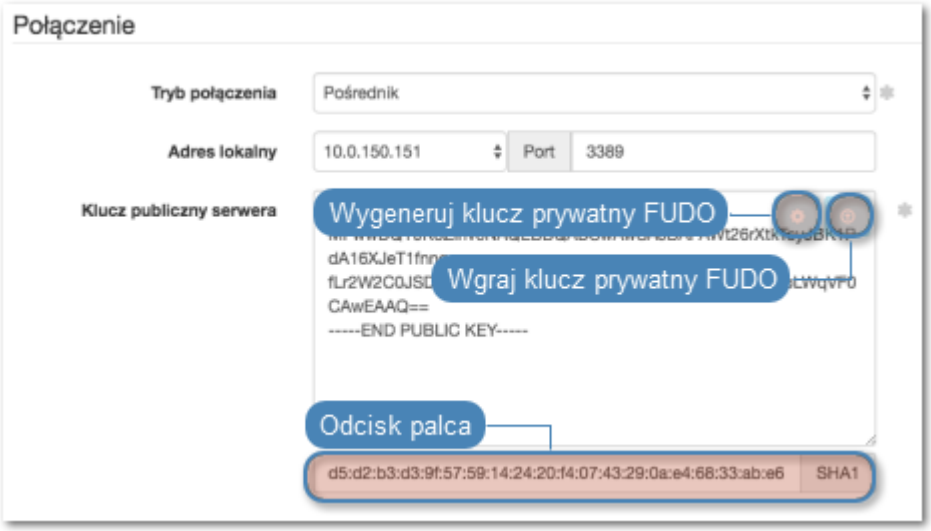
Dodanie gniazda nasłuchiwania

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	`proxy`
Adres lokalny	`10.0.150.151`
Port	`3389`
Adres zewnętrzny	✗
Port zewnętrzny	✗

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	✓
Język OCR	`Angielski`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
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	✗

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:

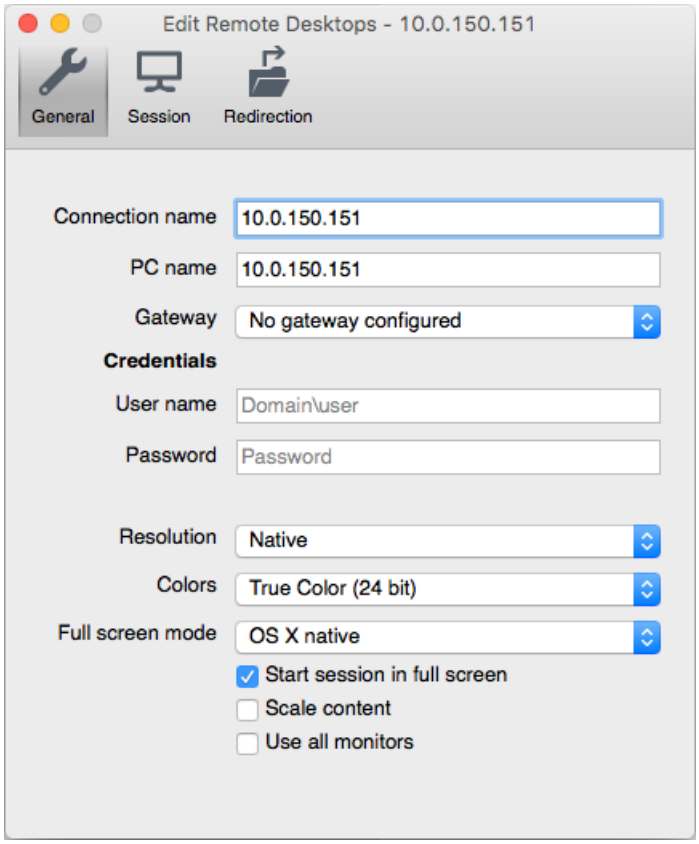
Parametr	Wartość
Ogólne	
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✓
SSH	✗
VNC	✗
Uprawnienia	
Uprawniani użytkownicy	✗
Konta	
`admin_rdp_server`	`rdp_listener`

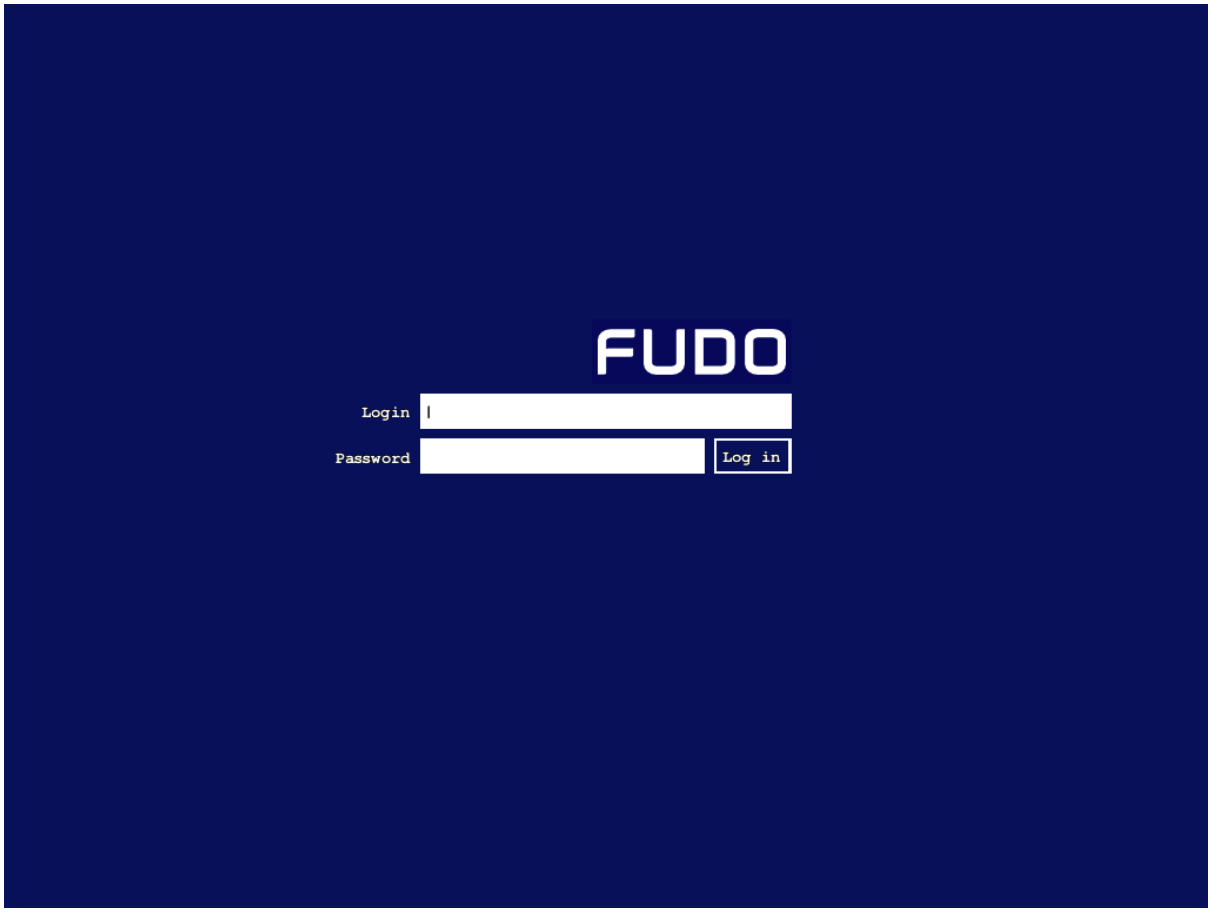
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_ smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_rdp_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `rdp_listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.3.3 Nawiązanie połączenia

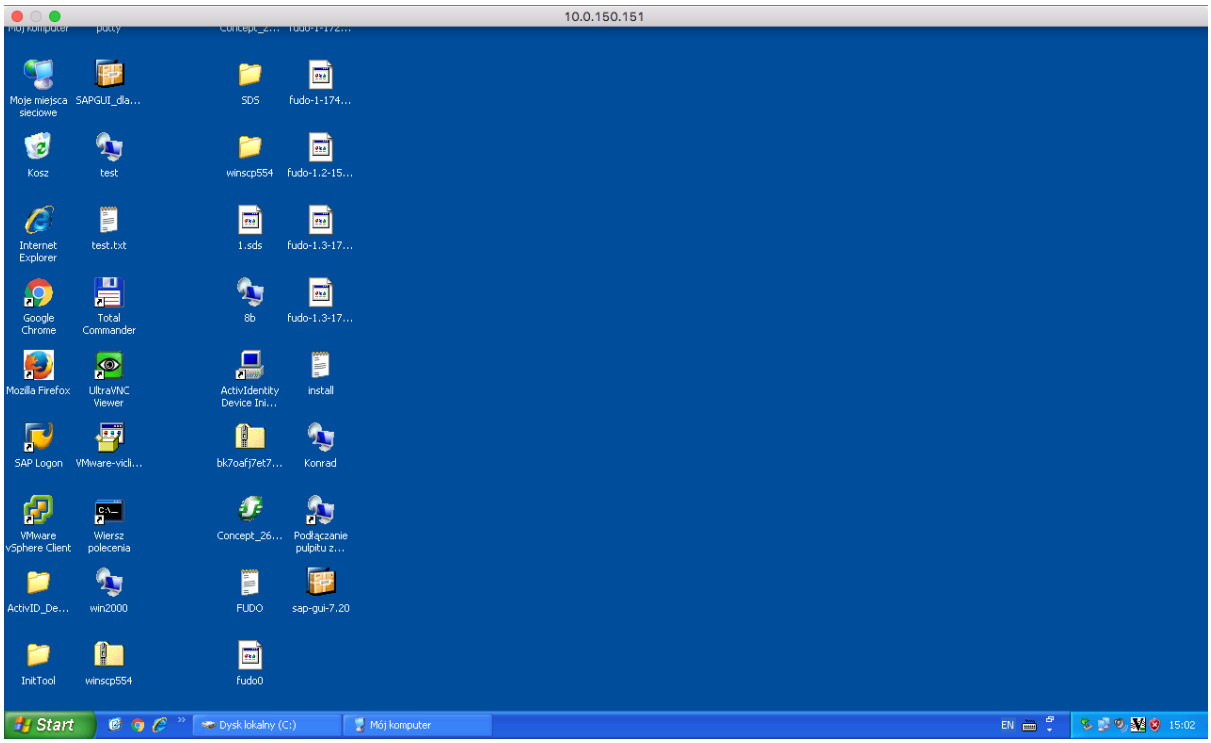
1. Uruchom klienta połączeń RDP.
2. Skonfiguruj połączenie zdalnego pulpitu.



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



Informacja: Fudo PAM pozwala na zastosowanie własnego logotypu na ekranie logowania. Więcej informacji na temat konfigurowania ekranów dla połączeń graficznych, znajdziesz w sekcji *Zasoby*.

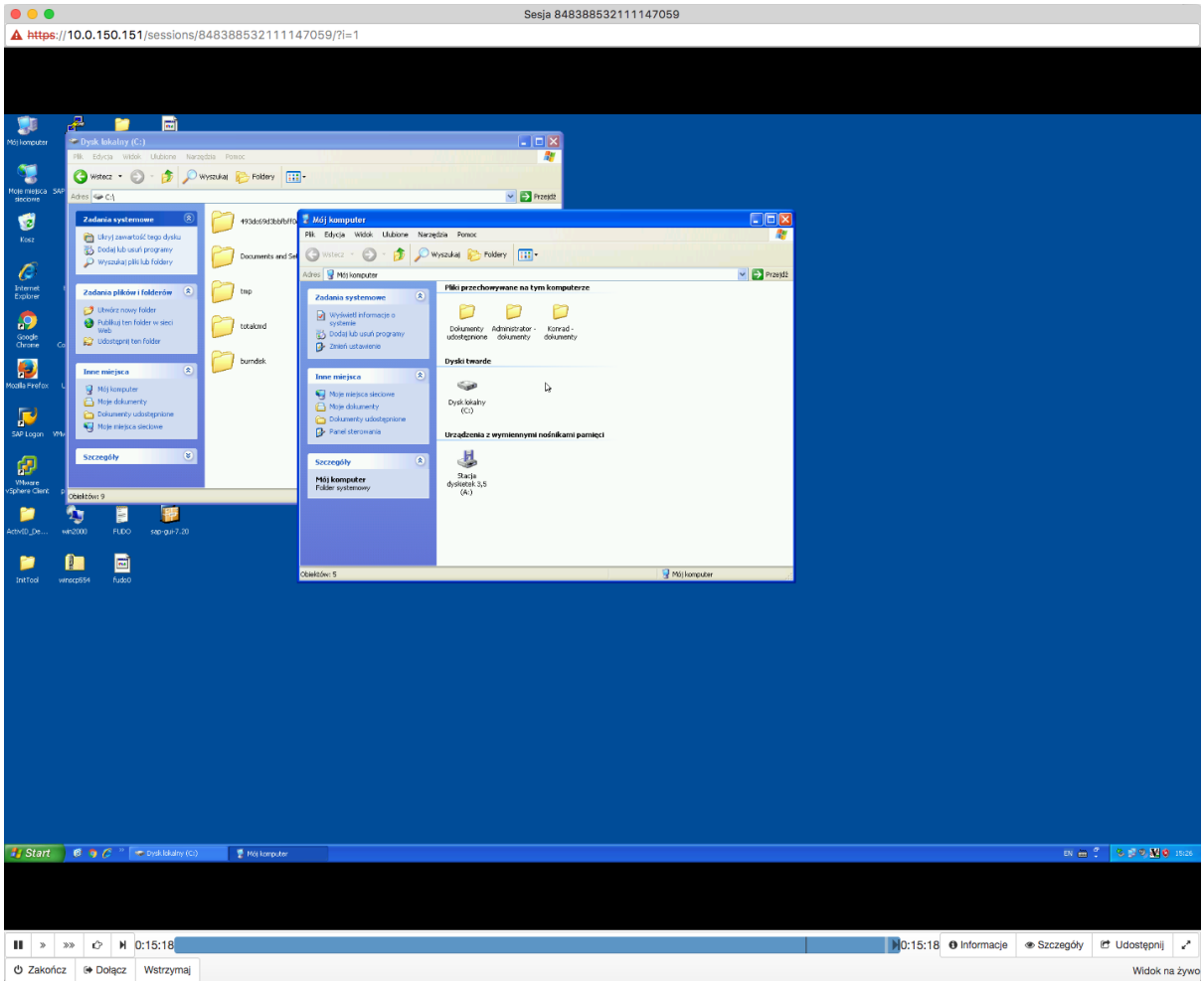


5.3.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający 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 Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *Aplikacje klienckie - Microsoft Remote Desktop*
- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia VNC*
- *Zasoby*
- *Model danych*
- *Broker połączeń RDP*

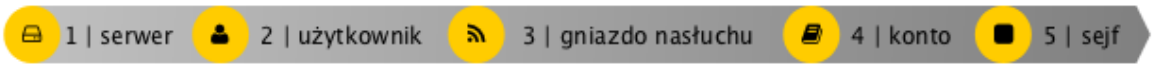
5.4 RDP w trybie bastionu

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo PAM, której celem jest monitorowanie połączeń RDP ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem w trybie bastionu, wskazując w nazwie użytkownika konto uprzywilejowane, na które chce się dostać. Fudo PAM uwierzytelnia użytkownika na podstawie danych zapisanych w lokalnej bazie danych i zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na ciągi zdefiniowane w koncie uprzywilejowanym (obiekt *konto* skonfigurowane w trybie *regular*).

5.4.1 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*.

5.4.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	rdp_server
Opis	`Serwer RDP`
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Adres źródłowy	`Dowolny`
Uprawnienia	
Uprawnieni użytkownicy	✗
Adresy serwerów	
Adres IP	`10.0.234.6/32`
Port	`3389`

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

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗
Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
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_bastion`
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Komunikat	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`bastion`
Adres lokalny	`10.0.150.151`
Port	`3389`
Adres zewnętrzny	✗
Port zewnętrzny	✗

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	✔
Język OCR	`Angielski`
Notatki	✘
Retencja danych	
Nadpisz globalne ustawienia retencji	✘
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	`Statyczne, bez ograniczeń`

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:

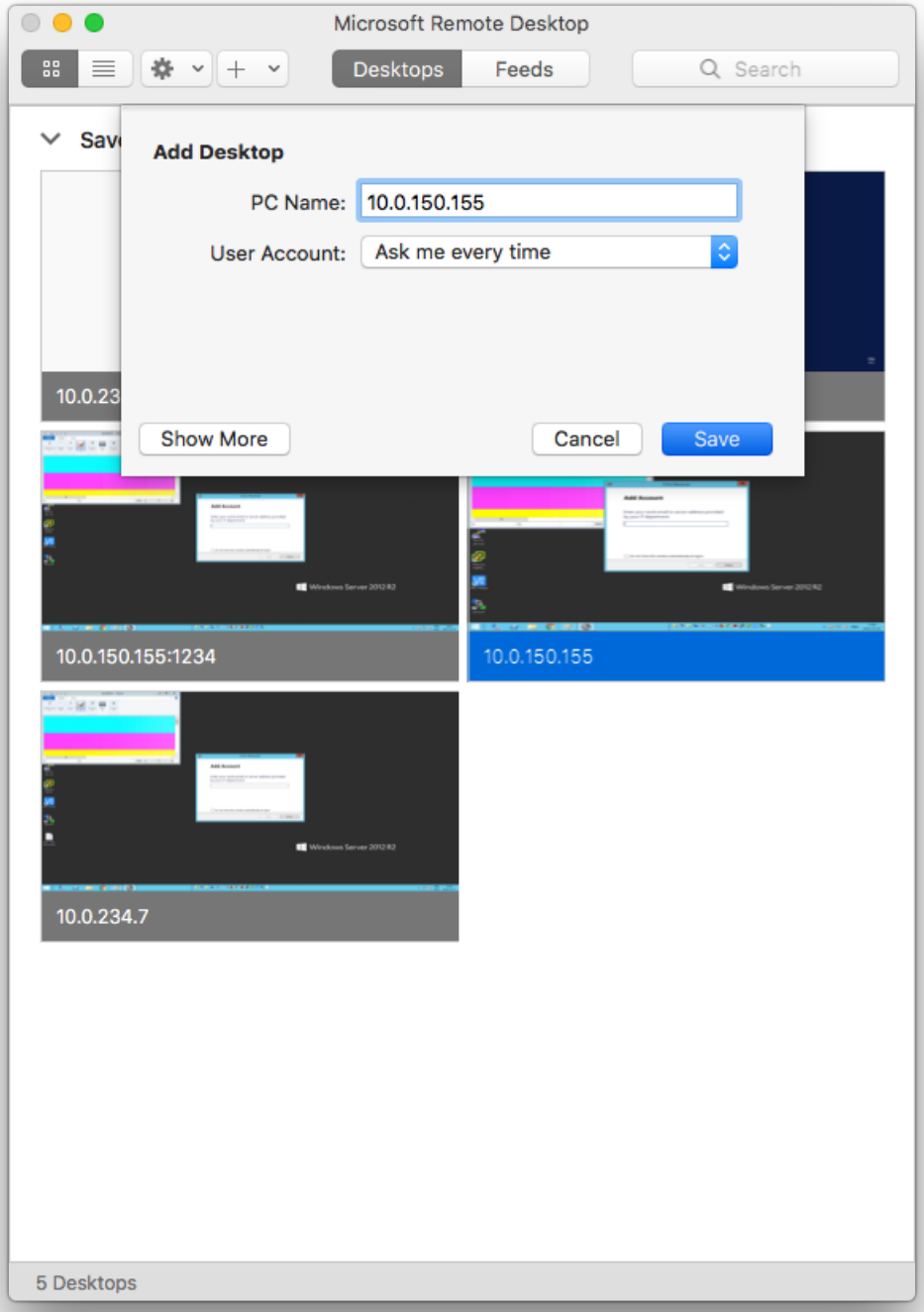
Parametr	Wartość
Ogólne	
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✓
SSH	✗
VNC	✗

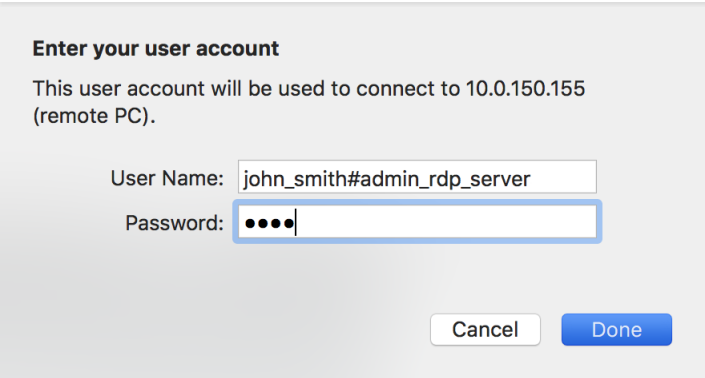
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij [+].
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_rdp_server` i kliknij [+].
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `rdp_listener_bastion` i kliknij [+].
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.4.3 Nawiązanie połączenia

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

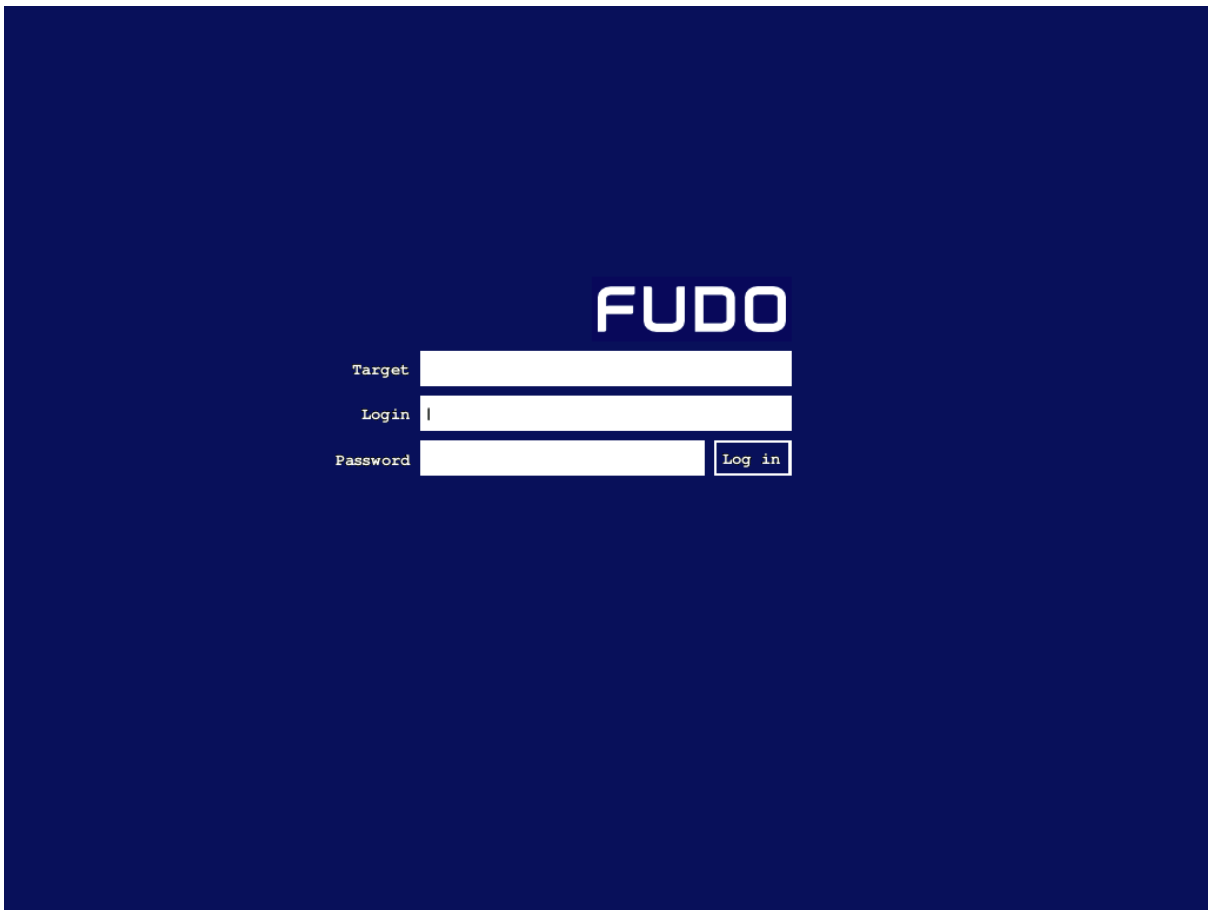


3. Wpisz login, uzupełniony o nazwę konta (john_smith#admin_rdp_server) oraz hasło użytkownika.

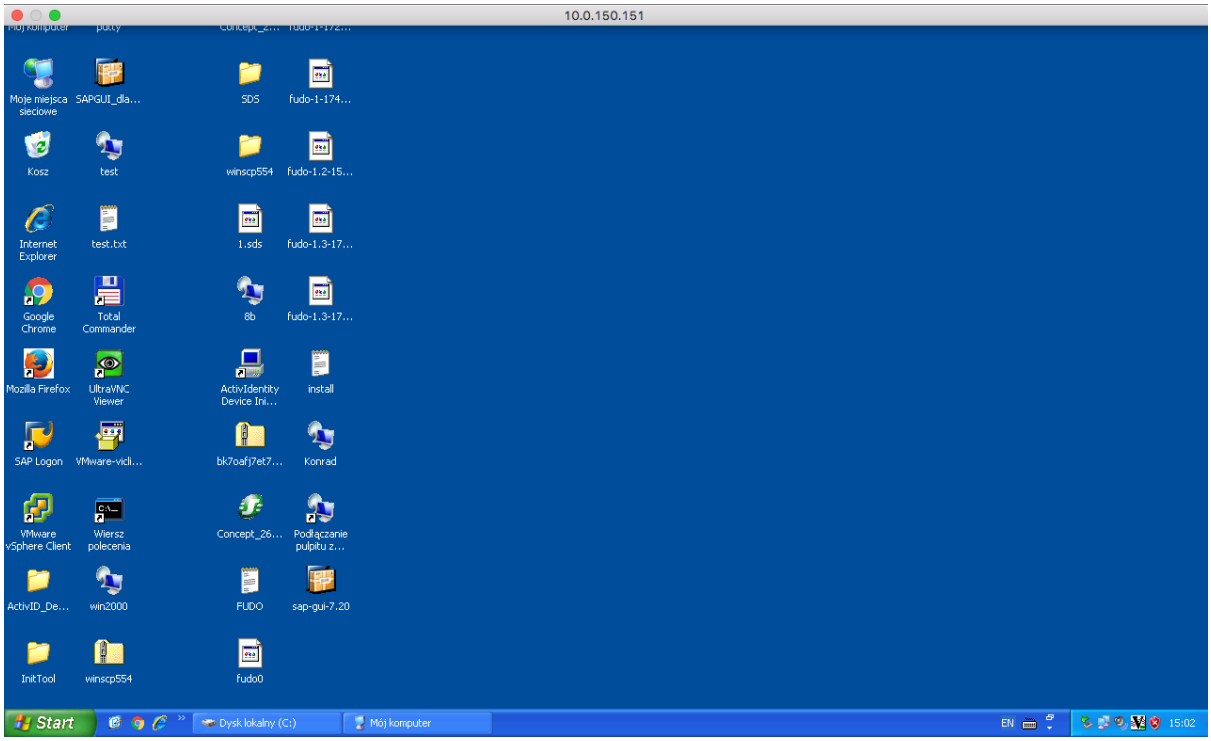


Informacja:

- Jeśli użytkownik nie wyspecyfikuje danych logowania w kliencie RDP, Fudo wyświetli własny ekran logowania, który należy uzupełnić nazwą konta uprzywilejowanego oraz danymi logowania użytkownika.



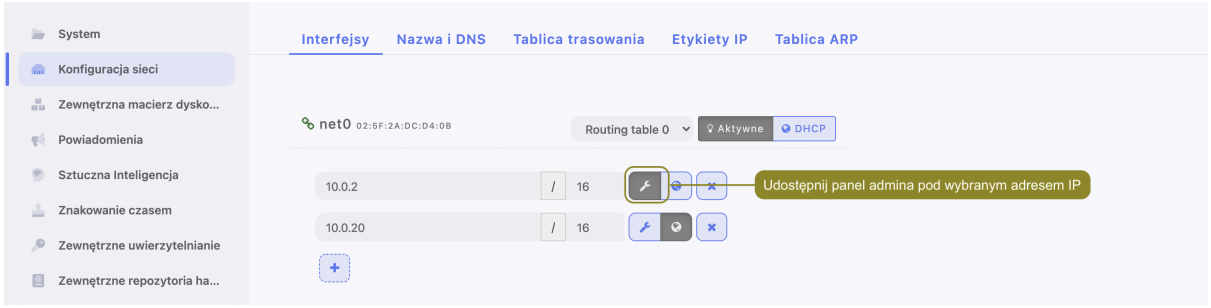
- W przypadku gdy wskazane konto nie istnieje, Fudo PAM dokona próby dopasowania podanego ciągu znaków do nazwy serwera. Jeśli system nie stwierdzi istnienia obiektu serwera o takiej nazwie, spróbuje dokonać dopasowania na podstawie nazwy DNS hosta.
- Fudo PAM pozwala na zastosowanie własnego logotypu na ekranie logowania. Więcej informacji na temat konfigurowania ekranów dla połączeń graficznych, znajdziesz w sekcji *Zasoby*.



5.4.4 Podgląd sesji połączeniowej

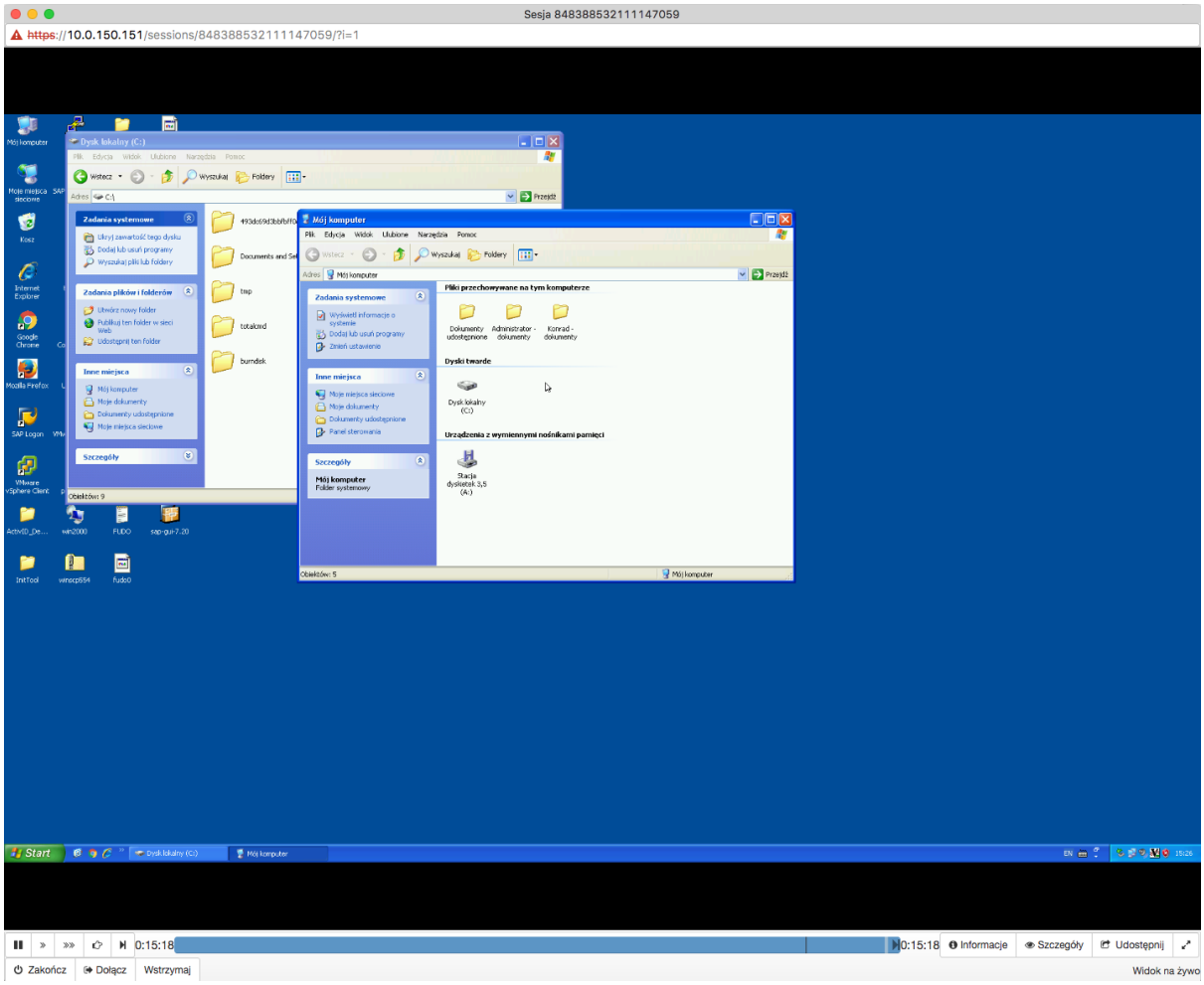
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Fudo PAM.

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



---

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



Tematy pokrewne:

- *Aplikacje klienckie - Microsoft Remote Desktop*
- *Szybki start - konfigurowanie połączenia SSH*
- *Szybki start - konfigurowanie połączenia VNC*
- *Zasoby*
- *Model danych*
- *Broker połączeń RDP*

5.5 Telnet

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji 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. Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników, zestawia połączenie ze zdalnym zasobem i rozpoczyna rejestrowanie akcji użytkownika.

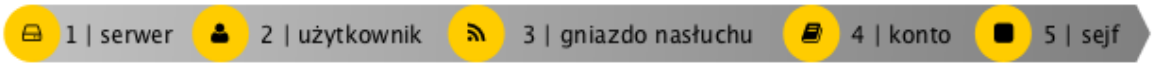
Informacja: Połączenia telnet realizowane za pośrednictwem Fudo PAM nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu przez Fudo

PAM musi uwierzytelnić się na serwerze docelowym po zestawieniu połączenia.

5.5.1 Założenia

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

5.5.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	telnet_server
Opis	✗
Zablokowane	✗
Protokół	`Telnet`
Adres źródłowy	`Dowolny`
Użyj szyfrowania TLS	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Adresy serwerów	
Adres IP	`10.0.35.137`
Port	`23`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres

email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗

Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
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`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`23`
Użyj szyfrowania 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`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
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	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij + *Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij + *Dodaj konto*.
10. Znajdź konto `admin_telnet_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `telnet_listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.5.3 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 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.

5.5.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający 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 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 SSH*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia RDP*
- *Zasoby*
- *Model danych*

5.6 Telnet 5250

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo PAM, której celem jest monitorowanie połączeń Telnet 5250 ze zdalnym serwerem. Scenariusz zakłada, że użytkow-

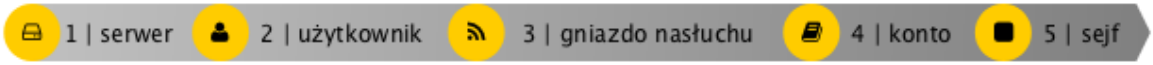
nik łączy się ze zdalnym serwerem za pomocą klienta protokołu Telnet używając indywidualnego loginu i hasła. Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników, zestawia połączenie ze zdalnym zasobem i rozpoczyna rejestrowanie akcji użytkownika.

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

5.6.1 Założenia

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

5.6.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	telnet_server
Opis	✗
Zablokowane	✗
Protokół	`Telnet 5250`
Adres źródłowy	`Dowolny`
Użyj szyfrowania TLS	✗

Uprawnienia	
Uprawnieni użytkownicy	✗

Adresy serwerów	
Adres IP	`10.0.35.137`
Port	`23`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗

Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
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 5250`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`23`
Użyj szyfrowania 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`
Notatki	✘
Retencja danych	
Nadpisz globalne ustawienia retencji	✘
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	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

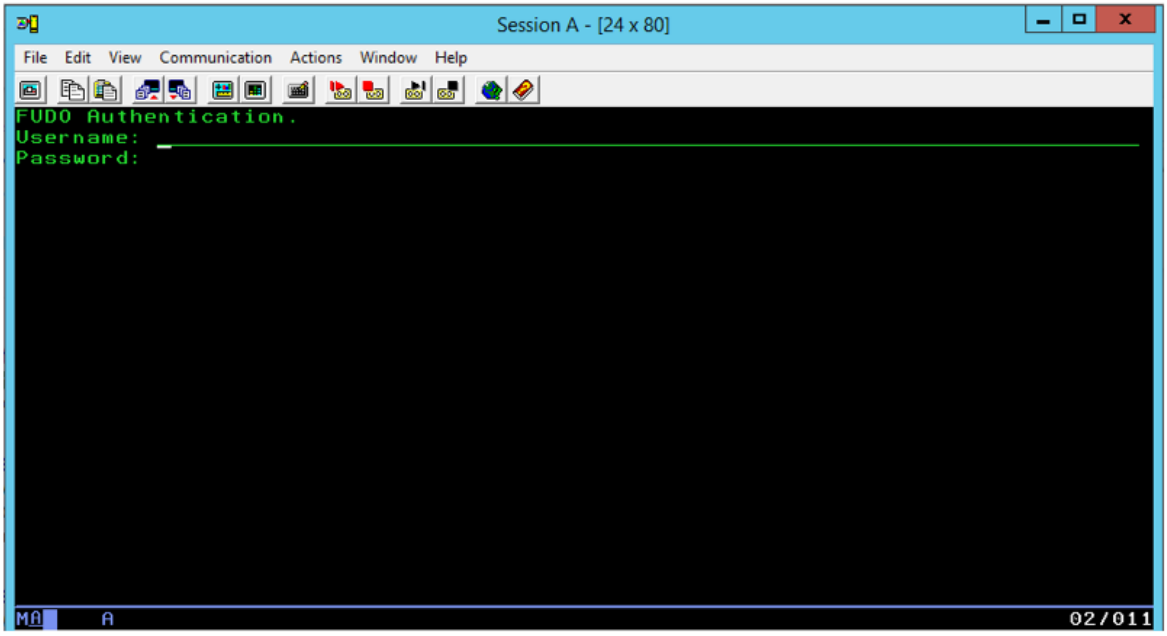
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_telnet_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `telnet_listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.6.3 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 '^]'.
```

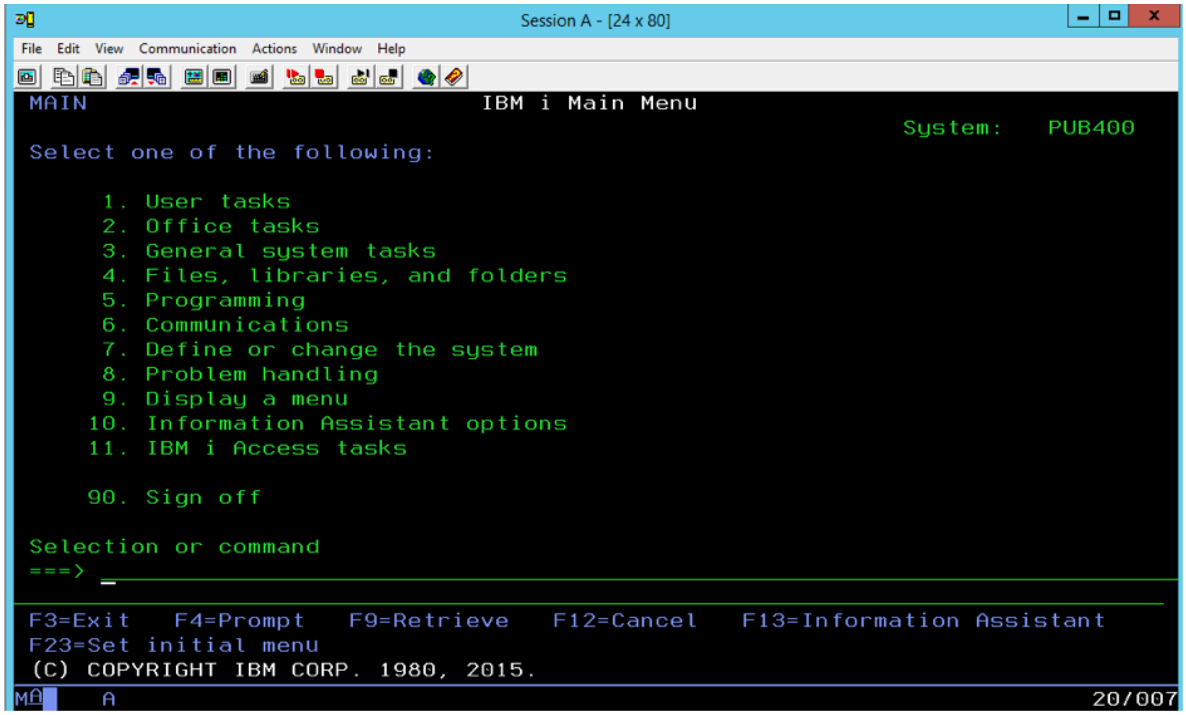
3. Wprowadź dane uwierzytelniające użytkownika na Fudo PAM.



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.



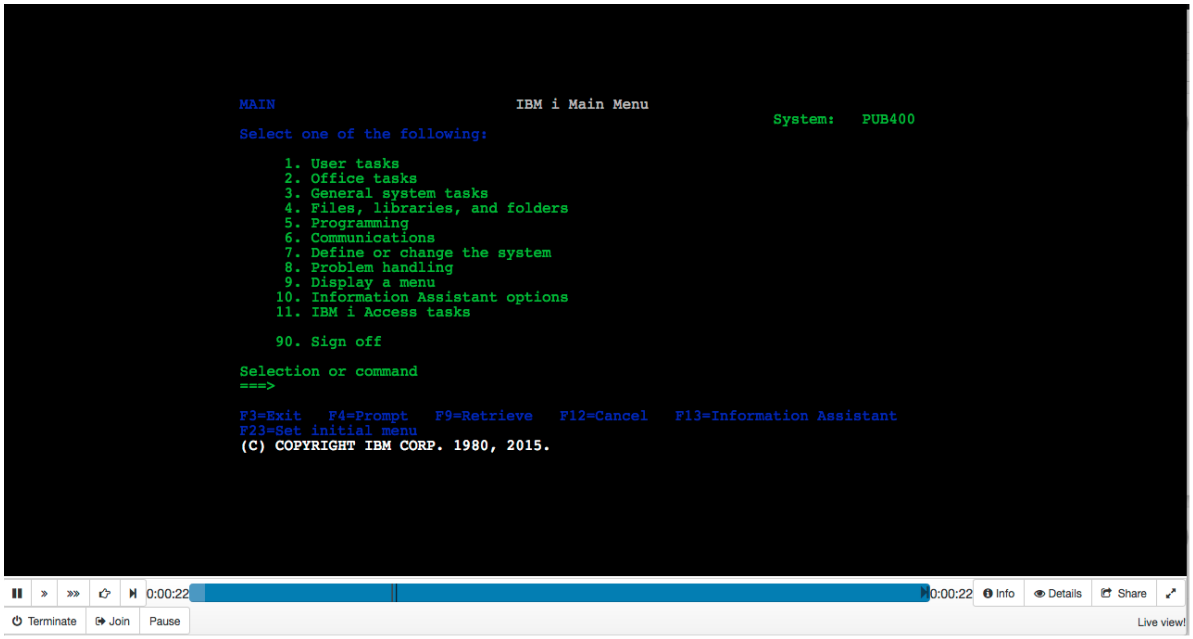
5.6.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający 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 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 SSH*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia RDP*
- *Zasoby*
- *Model danych*

5.7 MySQL

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji 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

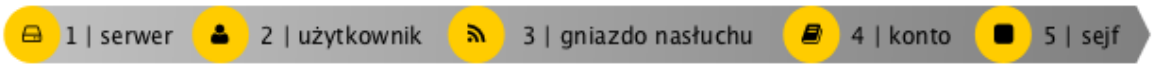
loginu i hasła. Fudo PAM uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników i zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `admin`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).

Ostrzeżenie: Domyślny plugin serwera MySQL `caching_sha2_password` nie jest obecnie wspierany przez Fudo PAM. Wspierane plugin'y dla połączeń MySQL przez Fudo PAM - to są `mysql_native_password` oraz `mysql_old_password`. Plugin Serwera powinien być ustawiony do `mysql_native_password` w `/etc/mysql/mysql.conf.d/mysqld.cnf` oraz Użytkownik stworzony z plugin'em `mysql_native_password`.

5.7.1 Założenia

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

5.7.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	mysql_server
Opis	✗
Zablokowane	✗
Protokół	`MySQL`
Adres źródłowy	`Dowolny`

Uprawnienia	
Uprawnieni użytkownicy	✗

Adresy serwerów	
Adres IP	`10.0.1.35`
Port	`3306`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗

Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
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`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
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	✗

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:

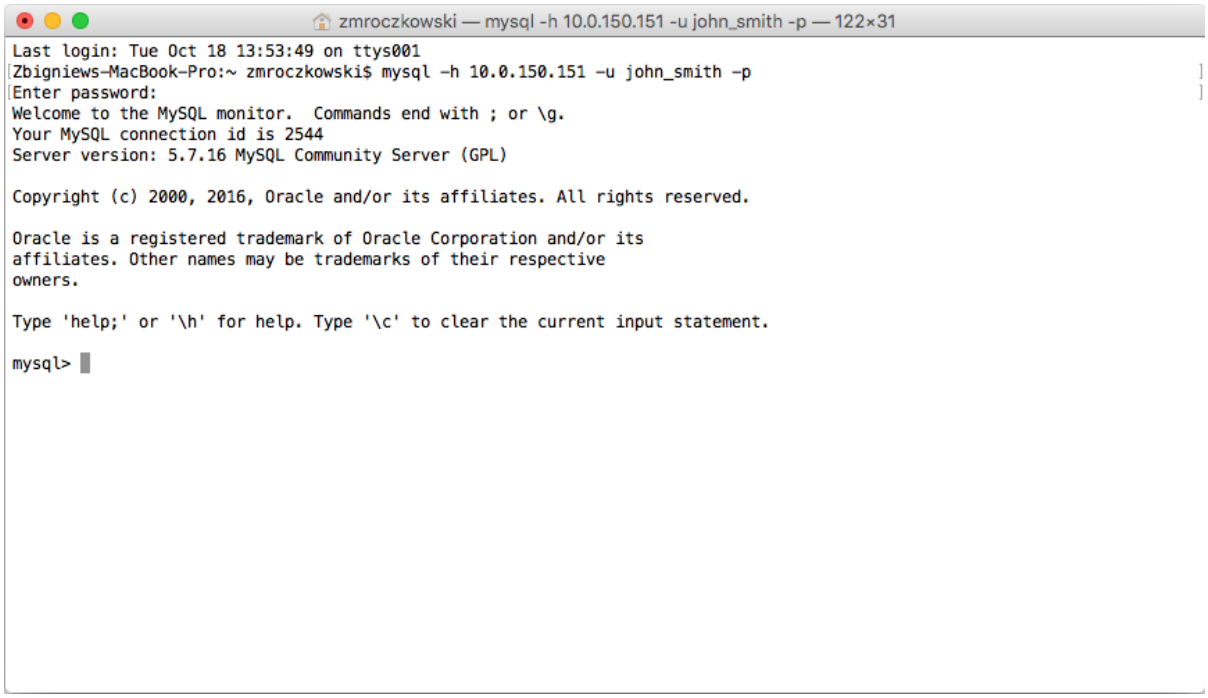
Parametr	Wartość
Ogólne	
Nazwa	`msyql_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_ smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_mysql_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `mysql_listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.7.3 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.

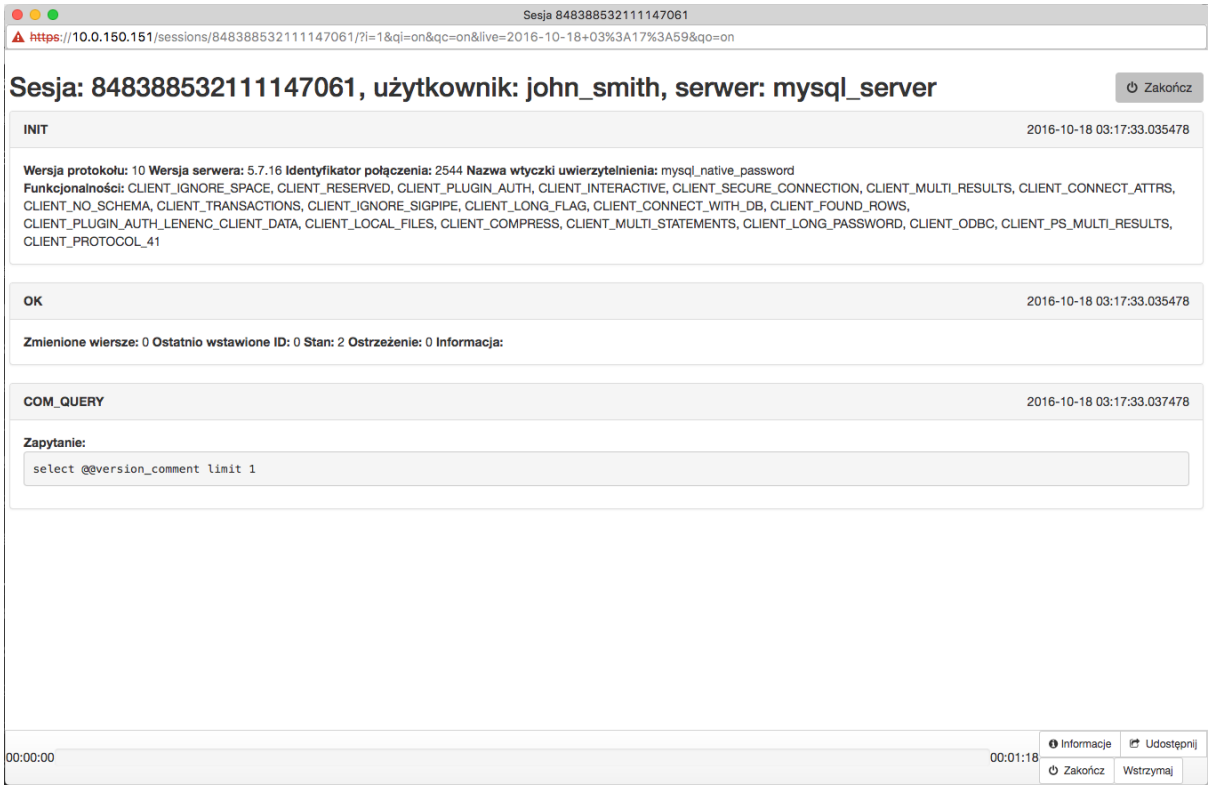
5.7.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający 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 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 SSH*
- *Szybki start - konfigurowanie połączenia RDP*
- *Szybki start - konfigurowanie połączenia HTTP*
- *Szybki start - konfigurowanie połączenia Telnet*
- *Telnet*
- *Wymagania*
- *Model danych*

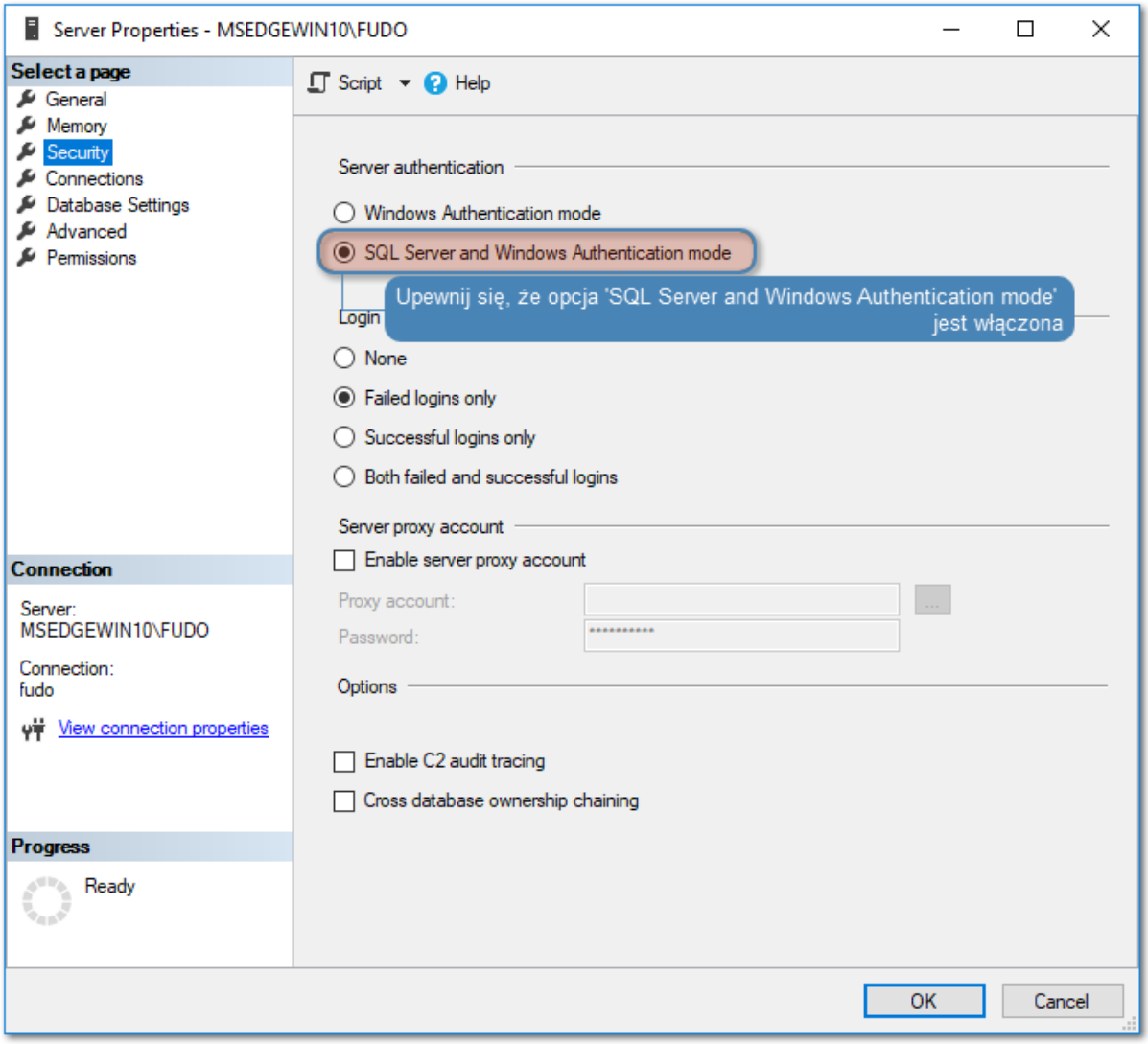
5.8 MS SQL

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

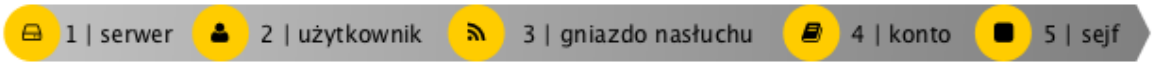
5.8.1 Założenia

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

Informacja: Upewnij się, że serwer SQL ma włączony tryb uwierzytelnienia *SQL Server and Windows Authentication*.



5.8.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	mssql_server
Opis	✗
Zablokowane	✗
Protokół	`MS SQL (TDS)`
Adres źródłowy	`Dowolny`
Uprawnienia	
Uprawnieni użytkownicy	✗
Adresy serwerów	
Adres IP	`10.0.150.154`
Port	`1433`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗

Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
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	`MSSQL_proxy`
Zablokowane	✗
Protokół	`MS SQL (TDS)`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`proxy`
Adres lokalny	`10.0.150.150`
Port	`1433`

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_mssql_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`mssql_server`
Dane uwierzytelniające	
Domena	✗
Login	`fudo`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗

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:

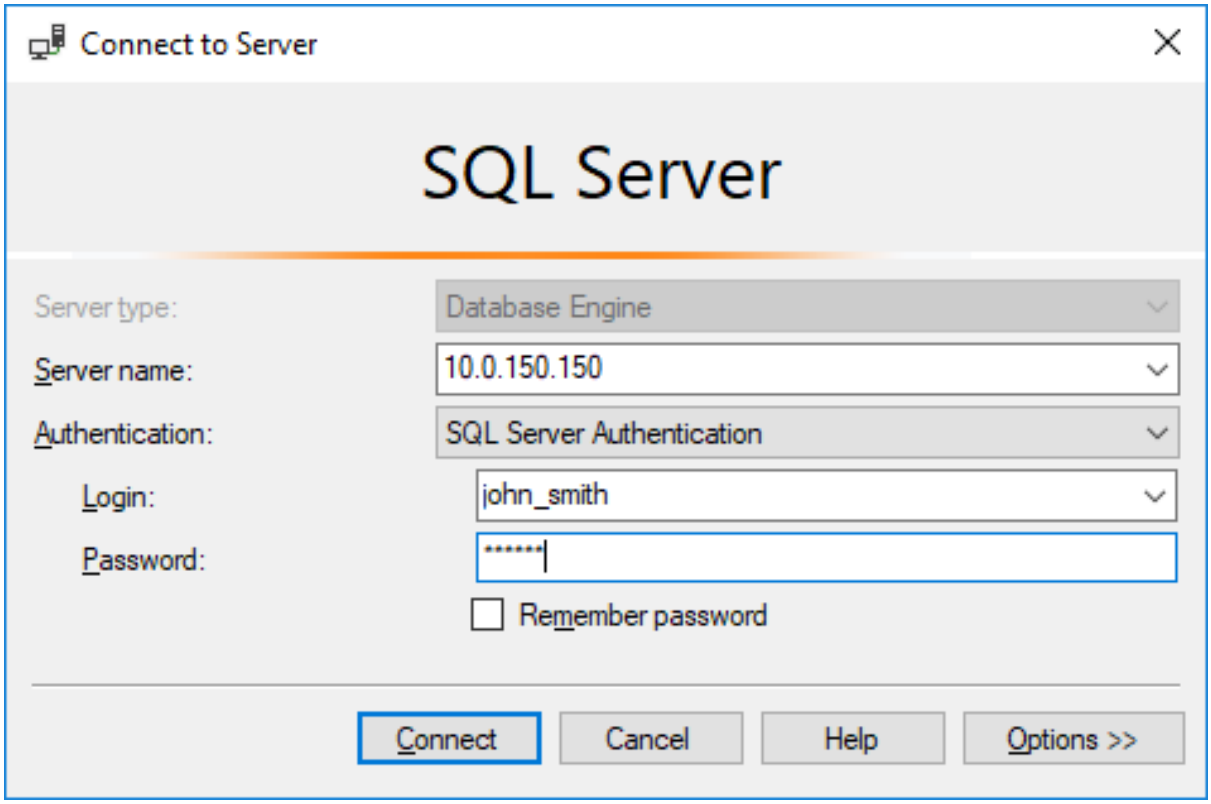
Parametr	Wartość
Ogólne	
Nazwa	`mssql_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

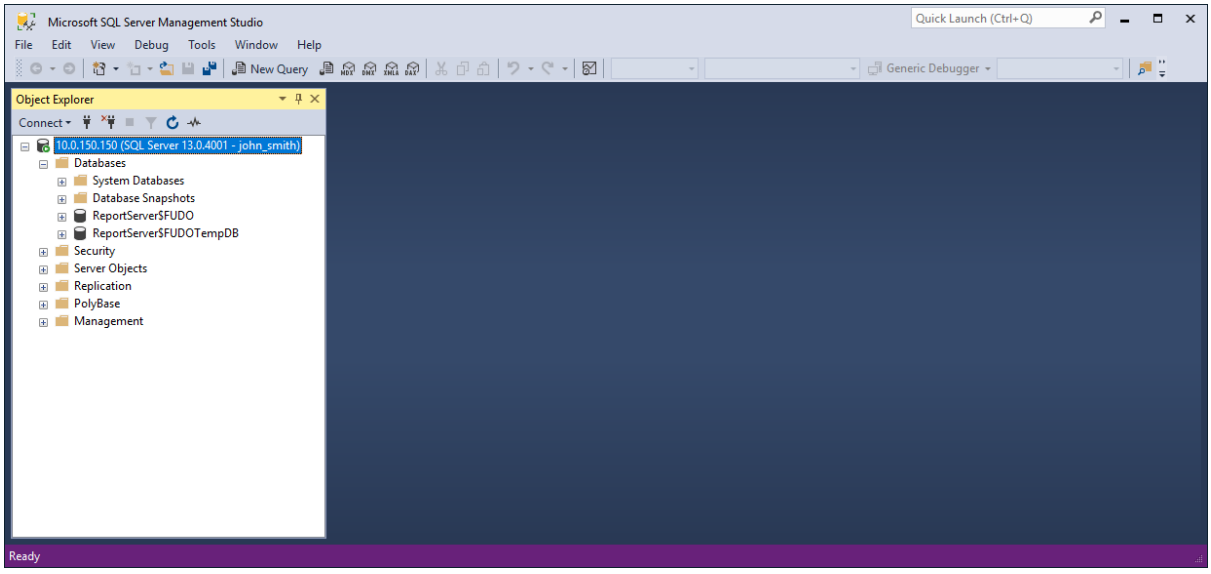
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_mssql_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `MSSQL_proxy` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.8.3 Nawiązanie połączenia

1. Uruchom *SQL Server Management Studio*.
2. Wprowadź wcześniej skonfigurowany adres proxy, na którym Fudo oczekuje na połączenia z serwerem MS SQL (10.0.150.150).
3. Z listy rozwijalnej *Authentication*, wybierz *SQL Server Authentication*.
4. Wprowadź nazwę użytkownika oraz hasło.
5. Kliknij *Connect*.





5.8.4 Podgląd sesji połączeniowej

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

3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ▶.

Informacja: Ponieważ MS SQL Studio może nawiązywać wiele niezależnych połączeń dla przesłania zapytań, sesje, nawiązane przez protokół TDS korzystając z MS SQL Studio są agregowane przez Fudo PAM.

Fudo PAM działa według algorytmu, weryfikującego, czy obiekty nowej sesji (`gniazdo nasłuchiwania`, `konto`, `adres serwera (serwer)`, `użytkownik`, oraz `sejf`) są takie same, jak obiekty którejś z już trwających sesji. Jeśli tak jest, sesje są agregowane w jedną.

Natomiast, jeśli algorytm nie wykrywa żadnej trwającej sesji z obiektami nowej sesji, system tworzy nową.

To powoduje, że w ramach jednej sesji wiele zapytań są zgrupowane. Każde zapytanie jest oznaczone tagiem, co pozwala wyświetlić w playerze tylko te połączenia, które są istotne (na przykład, zawierają zapytania, które faktycznie wykonał użytkownik).

Tematy pokrewne:

- *SQL Server Management Studio*
- *Szybki start - konfigurowanie połączenia MySQL*
- *Szybki start - konfigurowanie połączenia SSH*
- *Telnet*
- *Wymagania*
- *Model danych*

5.9 HTTP

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo PAM, której celem jest monitorowanie połączeń HTTPS z serwisem Twitter. Scenariusz zakłada, że użytkownik uwierzytelnia się za pomocą indywidualnej kombinacji loginu i hasła, które podmieniane są na poświadczenia monitorowanego konta w serwisie docelowym. Sesja połączeniowa będzie wymagała ponownego uwierzytelnienia po 15 minutach (900 sekund) braku aktywności.

Ostrzeżenie: Renderowanie sesji HTTP jest wymagającym procesem i może mieć negatywny wpływ na ogólną wydajność systemu. Monitorowanie rednerowanych połączeń HTTP zaleca się na maszynach fizycznych, z uwzględnieniem następujących limitów dla jednoczesnych połączeń HTTP.

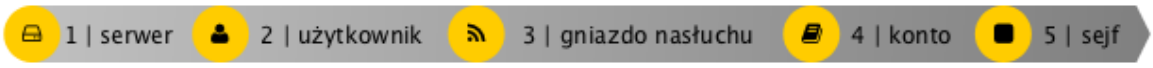
Model	Maksymalna zalecana liczba jednoczesnych połączeń HTTP*
F100x	2
F300x	5
F500x	10

* Rzeczywista maksymalna liczba obsługiwanych sesji HTTP uwarunkowana jest konfiguracją danej instacji Fudo PAM.

5.9.1 Założenia

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

5.9.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	twitter
Opis	✗
Zablokowane	✗
Protokół	`HTTP`
Czas oczekiwania HTTP	`900`
Adres źródłowy	`10.0.236.70`
Użyj szyfrowania TLS	✓
Starsze algorytmy kryptograficzne	✗
Używaj zaufanych certyfikatów	✓
Certyfikat CA	Kliknij w celu wgrania CA certyfikatu.
Uprawnienia	
Uprawnieni użytkownicy	✗
Adresy serwerów	
Adres	`twitter.com`
Port	`443`
Certyfikat serwera	Kliknij i pobierz certyfikat serwera.
Host HTTP	✗
Metoda uwierzytelnienia	`Twitter`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗

Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
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	`twitter_listener`
Zablokowane	✘
Protokół	`HTTP`
Renderuj sesje	✔
Uprawnienia	
Uprawnieni użytkownicy	✘
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.236.70`
Port	`997`
Użyj szyfrowania TLS	✔
Starsze algorytmy kryptograficzne	✔
Certyfikat TLS	Kliknij  i wygeneruj certyfikat 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	`twitter_admin`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`twitter`
Dane uwierzytelniające	
Domena	✗
Login	`Tweety`
Zastąp sekret	`hasłem`
Hasło	`*****`
Powtórz hasło	`*****`
Polityka modyfikatora hasła	`Statyczne, bez ograniczeń`

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 zakładki *Ogólne*.

Parametr	Wartość
Ogólne	
Nazwa	`http_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

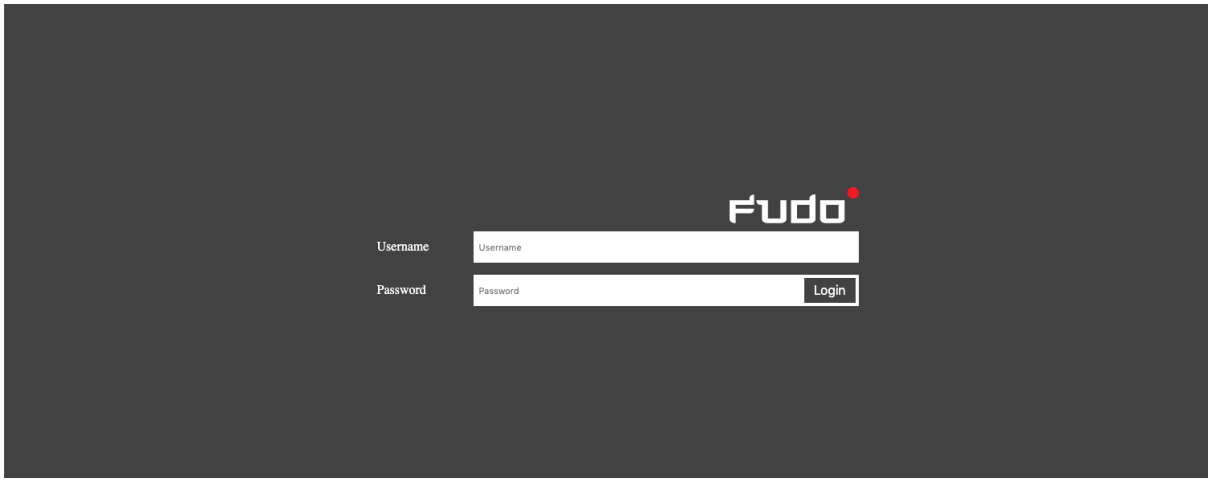
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `twitter_admin` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `twitter_listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.9.3 Nawiązanie połączenia

1. Uruchom przeglądarkę internetową.
2. W pasku adresu wprowadź 10.0.236.70:997.
3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter] lub klikając przycisk *Login*.

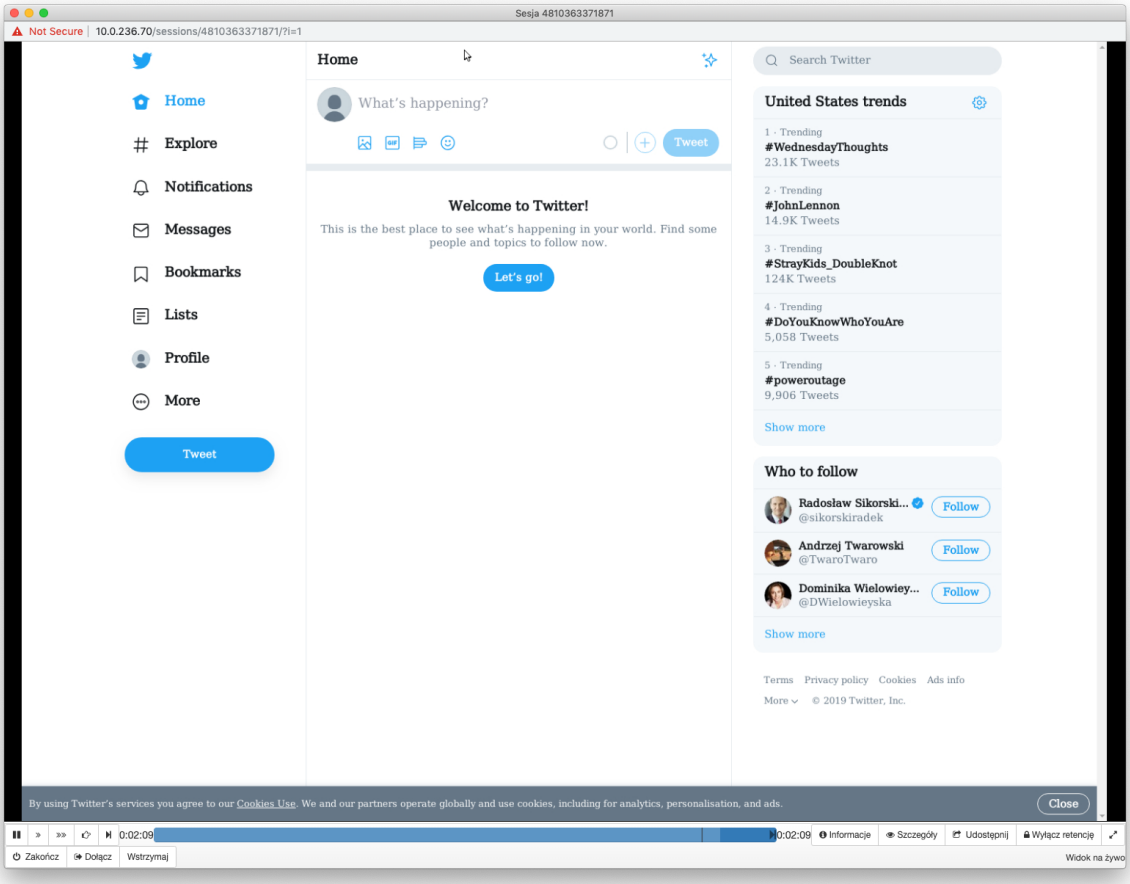
Informacja: W przypadku uwierzytelniania dwuskładnikowego, wprowadź hasło statyczne wraz ze składnikiem dynamicznym (wskazanie tokena) jako jeden ciąg znaków.



4. Kontynuuj przeglądanie serwisu.

5.9.4 Podgląd sesji połączeniowej

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



Tematy pokrewne:

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

5.10 Citrix

Ostrzeżenie: Wsparcie protokołów `ICA` oraz `Citrix` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianymi protokołami (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

Połączenia administracyjne realizowane z wykorzystniem protokołu ICA mogą być nawiązywane bezpośrednio za pomocą aplikacji klienckiej lub za pośrednictwem intefejsu Citrix StoreFront.

5.10.1 ICA

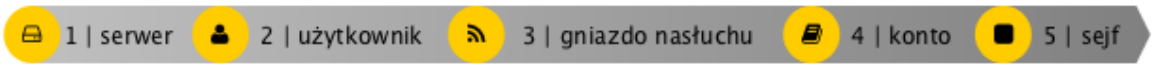
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo PAM, której celem jest monitorowanie połączeń ICA ze zdalnym serwerem, z wykorzystaniem aplikacji klienckiej protokołu ICA. Klient nawiązuje połączenie używając indywidualnej nazwy użytkownika i hasła (john_smith/john), które zostają zamienione na parametry konta uprzywilejowanego (citrixuser/password) w momencie zestawiania połączenia z serwerem docelowym.

Ostrzeżenie: Wsparcie protokołu `ICA` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

5.10.1.1 Założenia

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

5.10.1.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	ica_server
Opis	✗
Zablokowane	✗
Protokół	`ICA`
Adres źródłowy	`Dowolny`
Użyj szyfrowania TLS	✗

Uprawnienia	
Uprawnieni użytkownicy	✗

Adresy serwerów	
Adres IP	`10.0.0.21`
Port	`1494`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej 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	`ICA`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`2494`
Użyj szyfrowania 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.

Informacja: Połączenia bezpośrednie z serwerami ICA wspierają wszystkie typy kont.

---

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

Parametr	Wartość
Ogólne	
Nazwa	`admin_ica_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`ica_server`
Dane uwierzytelniające	
Domena	✗
Login	`citrixuser`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora hasła	Statyczne, bez ograniczeń

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	`ica_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_ica_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `ica_listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

Informacja: W przypadku połączeń szyfrowanych protokołem TLS, Fudo zwraca klientowi Citrix *plik konfiguracyjny .ica*, w którym adresem serwera (*Address*) jest nazwa zwyczajowa (*Common Name*) z certyfikatu TLS.

5.10.1.3 Zdefiniowanie połączenia w pliku .ica

Bezpośrednie połączenie ze zdalnym serwerem za pośrednictwem protokołu ICA wymaga utworzenia pliku konfiguracyjnego, zawierającego parametry połączenia. Plik konfiguracyjny powinien wskazywać gniazdo nasłuchiwania za pomocą którego nawiązane zostanie połączenie z monitorowanym serwerem.

Informacja: Szczegółowe informacje na temat pliku konfiguracyjnego znajdziesz w rozdziale *Plik konfiguracyjny połączenia ICA*.

1. Utwórz plik tekstowy o następującej treści:

```
[ApplicationServers]
ica_connection_example=

[ica_connection_example]
ProxyType=SOCKSV5
ProxyHost=10.0.150.151:2494
ProxyUsername=*
ProxyPassword=*
Address=john_smith
Username=john_smith
ClearPassword=john
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

2. Zapisz plik z dowolną nazwą, nadając mu rozszerzenie `.ica`.

5.10.1.4 Nawiązanie połączenia

1. Kliknij dwukrotnie plik z parametrami połączenia, aby uruchomić klienta protokołu ICA.
2. Kontynuuj korzystanie z usługi.

5.10.1.5 Podgląd sesji połączeniowej

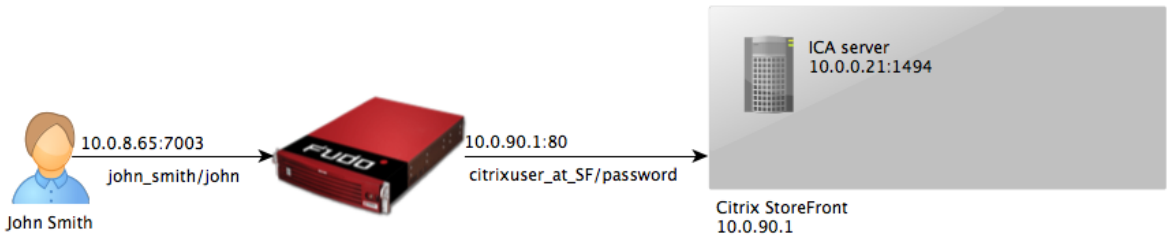
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Fudo PAM.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith*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

Tematy pokrewne:

- *Plik konfiguracyjny połączenia ICA*
- *Model danych*
- *Dodawanie serwera ICA*
- *Dodawanie gniazda nasłuchiwania ICA*
- *Protokół ICA*

5.10.2 Citrix StoreFront

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo PAM, której celem jest monitorowanie połączeń ICA ze zdalnym serwerem, w przypadku której inicjowanie połączenia następuje za pośrednictwem Citrix StoreFront.

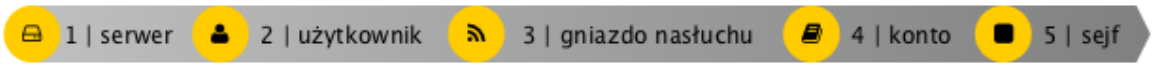


Ostrzeżenie: Wsparcie protokołu `Citrix` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

5.10.2.1 Założenia

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

5.10.2.2 Konfiguracja



Dodanie serwera ICA

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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Ogólne	
Nazwa	`ica_server`
Opis	✘
Zablokowane	✘
Protokół	`ICA`
Adres źródłowy	`Dowolny`
Użyj szyfrowania TLS	✘

Uprawnienia	
Uprawnieni użytkownicy	✘

Adresy serwerów	
Adres IP	`10.0.0.21`
Port	`1494`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania dla serwera ICA

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	`ica_listener`
Zablokowane	✘
Protokół	`ICA`
Uprawnienia	
Uprawnieni użytkownicy	✘
Połączenie	
Tryb połączenia	`proxy`
Adres lokalny	`10.0.150.151`
Port	`2494`
Użyj szyfrowania TLS	✘

4. Kliknij *Zapisz*.

Dodanie konta dla serwera ICA

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.

Informacja: Połączenia z serwerami ICA za pośrednictwem Citrix StoreFront wymagają konta

skonfigurowanego w trybie *anonymous* lub *forward*.

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

Parametr	Wartość
Ogólne	
Nazwa	`ICA_forward`
Zablokowane	✗
Typ	`forward`
Nagrywanie sesji	`wszystko`
Notatki	✗

Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`ica_server`
Dane uwierzytelniające	
Zastąp sekret	✗
Przekazuj domenę	✓

4. Kliknij *Zapisz*.

Dodanie serwera Citrix StoreFront

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	`citrix_storefront`
Zablokowane	✗
Protokół	`Citrix StoreFront (HTTP)`
Czas oczekiwania HTTP	`900`
Opis	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Host docelowy	
Adres IP	`10.0.90.1`
Port	`80`
Adres źródłowy	`Dowolny`
Użyj szyfrowania TLS	✗
URL	`http://10.0.90.1/Citrix/StoreWeb/`

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania dla serwera Citrix StoreFront

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	`citrix_storefront_listener`
Zablokowane	✗
Protokół	`Citrix StoreFront (HTTP)`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`proxy`
Adres lokalny	`10.0.8.65`
Port	`7003`
Adres zewnętrzny	✗
Port zewnętrzny	✗
Użyj szyfrowania TLS	✗

4. Kliknij *Zapisz*.

Dodanie konta dla Citrix StoreFront

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	`citrixuser_at_SF`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`citrix_storefront`
Dane uwierzytelniające	
Domena	`tech.whl`
Login	`citrixuser`
Zastąp sekret	`hasłem`
Hasło	password
Powtórz hasło	password
Polityka modyfikatora hasła	`Statyczne, bez ograniczeń`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗

Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
Typ	`Hasło`
Hasło	`john`
Powtórz hasło	`john`

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.

Informacja: Przy wybieraniu listenera ICA, którego adres ma być zwrócony do klienta przeszukiwane są jedynie sejfy, w których znajduje się listener Citrix StoreFront, z którego użytkownik aktualnie korzysta.

---

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

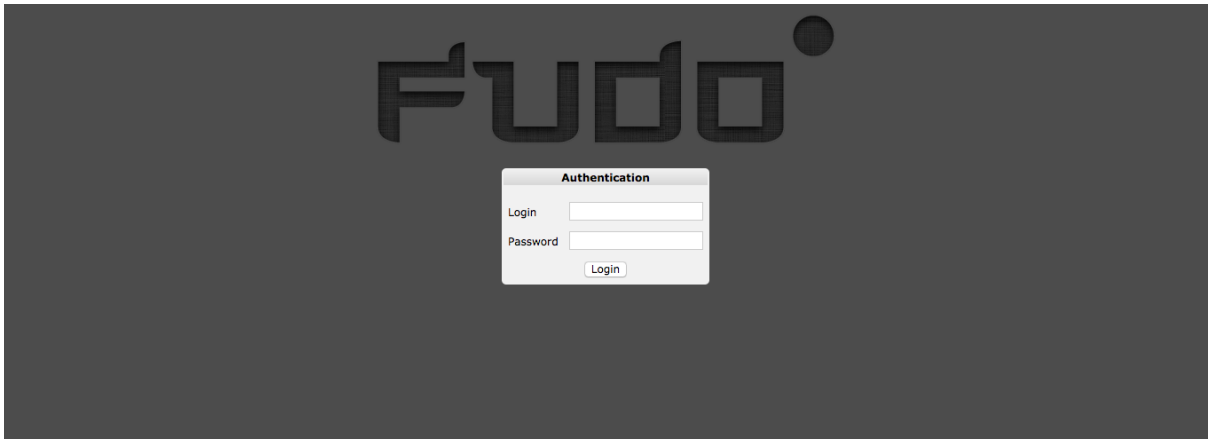
Parametr	Wartość
Ogólne	
Nazwa	`ica_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

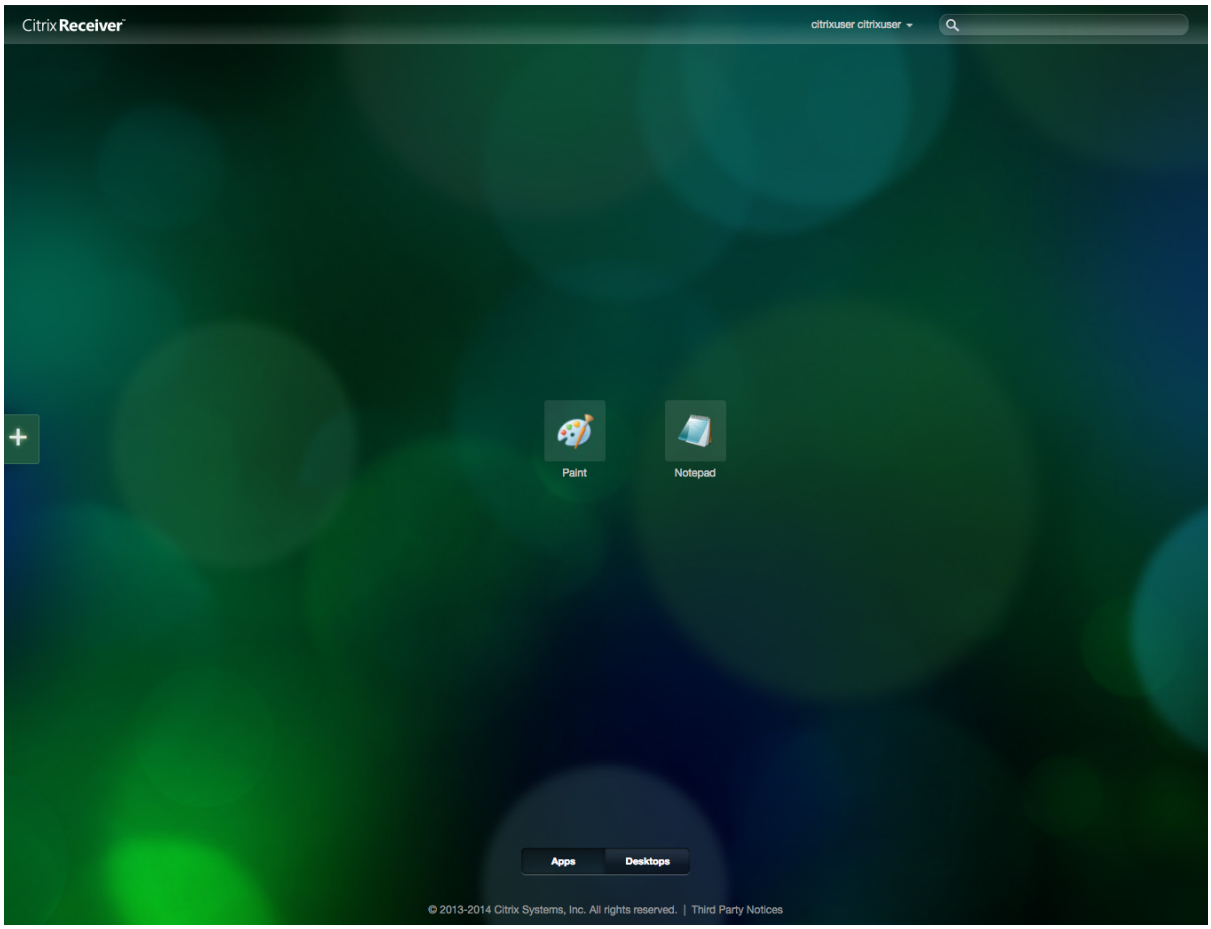
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_ smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `citrixuser_at_SF` i kliknij +.
11. Znajdź konto `ICA_forward` i kliknij +.
12. Kliknij *OK*.
13. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania* w wierszu konta *citrixuser_ at_ SF*.
14. Znajdź obiekt `citrix_storefront_listener` i kliknij +.
15. Kliknij *OK*.
16. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania* w wierszu konta *ICA_ forward*.
17. Znajdź obiekt `ica_listener` i kliknij +.
18. Kliknij *OK*.
19. Kliknij *Zapisz*.

Nawiązanie połączenia

1. W przeglądarce internetowej wprowadź adres IP `10.0.8.65:7003`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu Citrix StoreFront.



3. Kliknij wybrany element, aby nawiązać połączenie z zasobem.



Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP `10.0.8.65`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu panelu zarządzającego Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.

Tematy pokrewne:

- *Model danych*

- *Dodawanie serwera Citrix*
- *Dodawanie gniazda nasłuchiwania Citrix*
- *Citrix StoreFront (HTTP)*

5.11 VNC

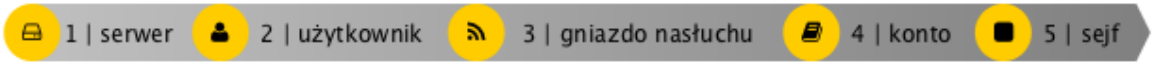
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo PAM, której celem jest monitorowanie połączeń VNC ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *VNC* uwierzytelnia się na Fudo PAM używając własnego loginu i hasła (`john_smith`/`john`). Fudo PAM zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła.

Informacja: Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, login zdefiniowany w koncie typu *regular* jest ignorowany przy zestawianiu połączenia.

5.11.1 Założenia

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

5.11.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	vnc_server
Opis	✗
Zablokowane	✗
Protokół	`VNC`
Adres źródłowy	`Dowolny`

Uprawnienia	
Uprawnieni użytkownicy	✗

Adresy serwerów	
Adres IP	`10.0.40.230`
Port	`5900`

4. Kliknij *Zapisz*.

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗

Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
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	`vnc_listener`
Zablokowane	✗
Protokół	`VNC`
Komunikat	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`proxy`
Adres lokalny	`10.0.150.151`
Port	`5900`
Adres zewnętrzny	✗
Port zewnętrzny	✗

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_vnc_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✓
Język OCR	`Angielski`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`vnc_server`
Dane uwierzytelniające	
Domena	✗
Login	✗
Zastąp sekret	`hasłem`
Hasło	`root`
Powtórz hasło	`root`
Polityka modyfikatora haseł	✗

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:

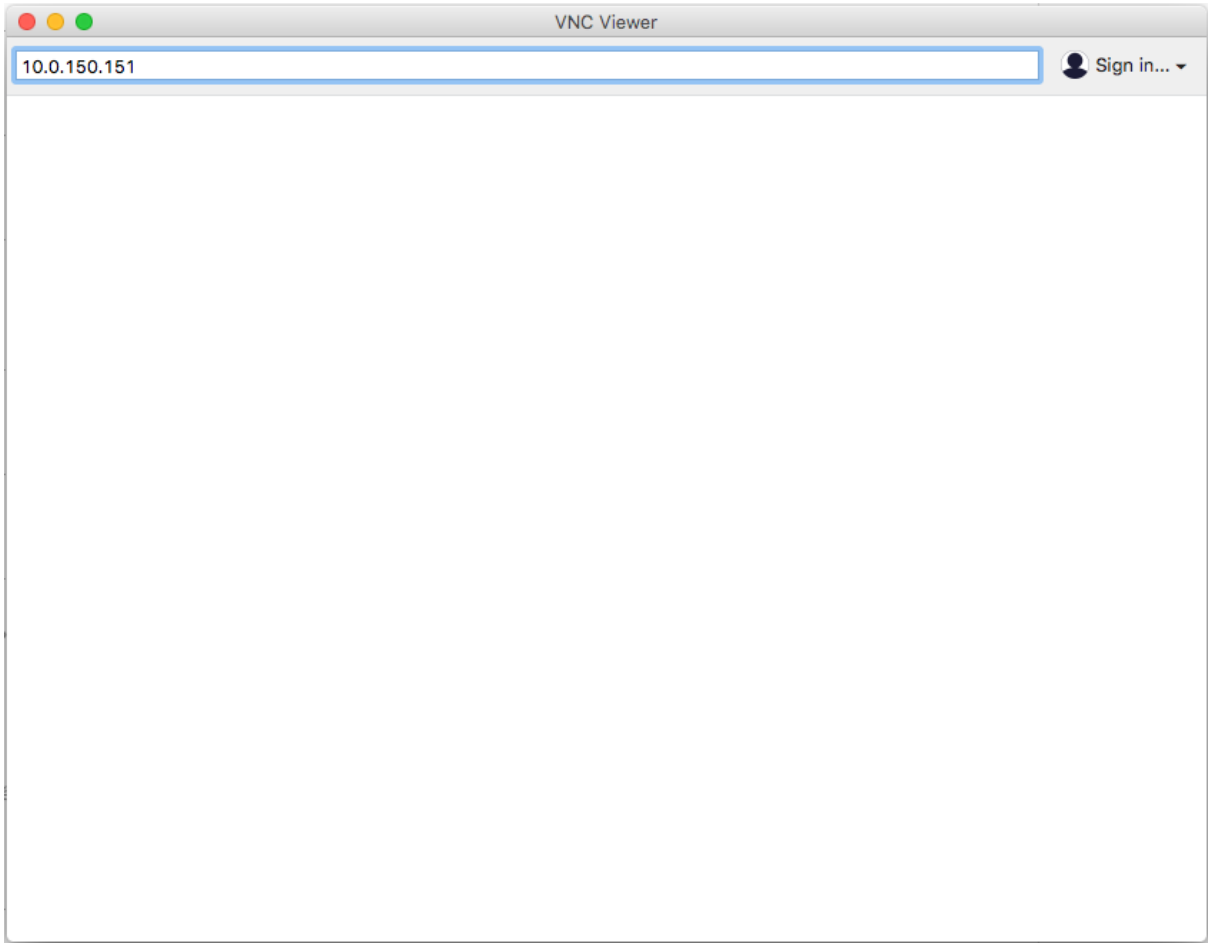
Parametr	Wartość
Nazwa	`vnc_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✓
Uprawnienia	
Uprawnieni użytkownicy	✗
Powiązania obiektu	
`admin_vnc_server`	`vnc_listener`

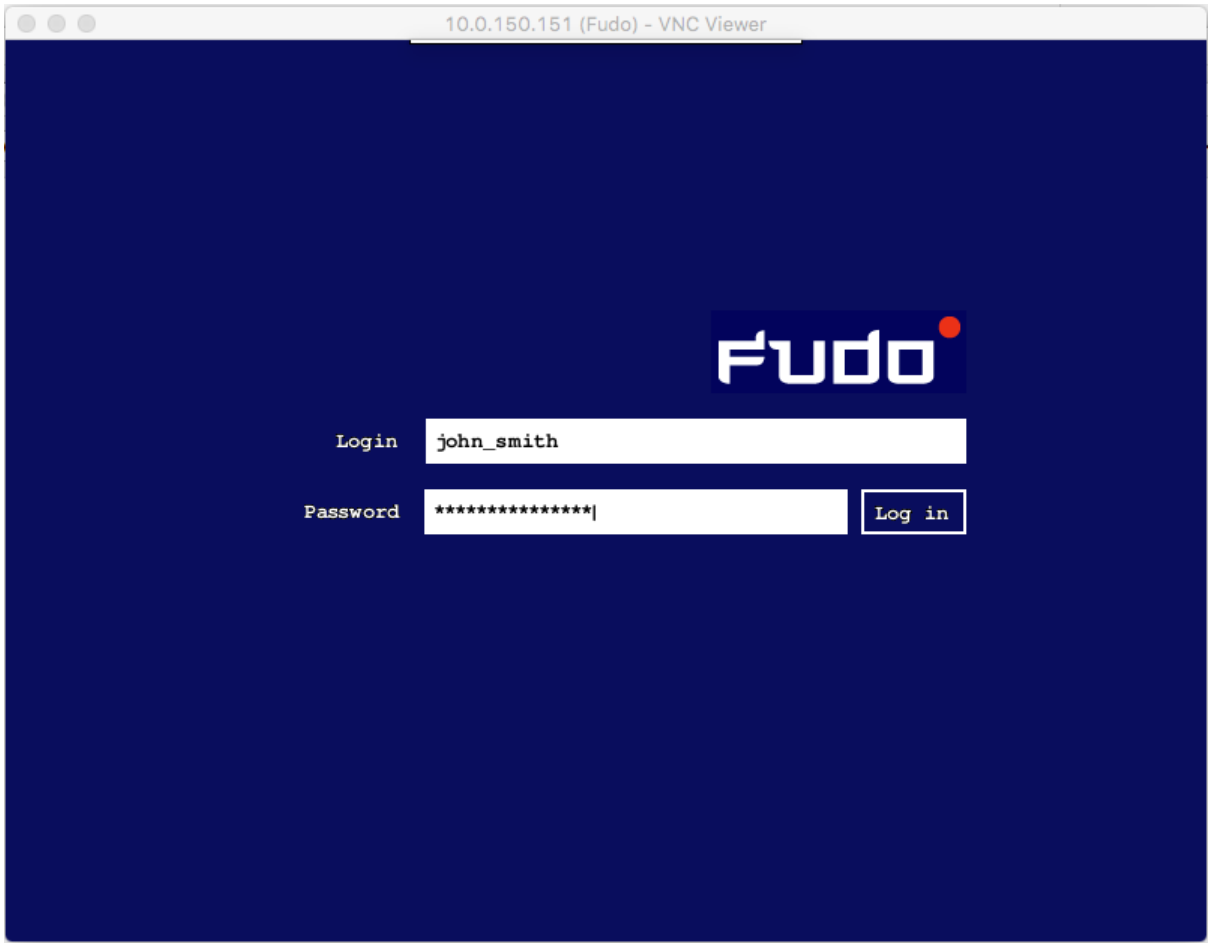
4. Kliknij *Zapisz*.

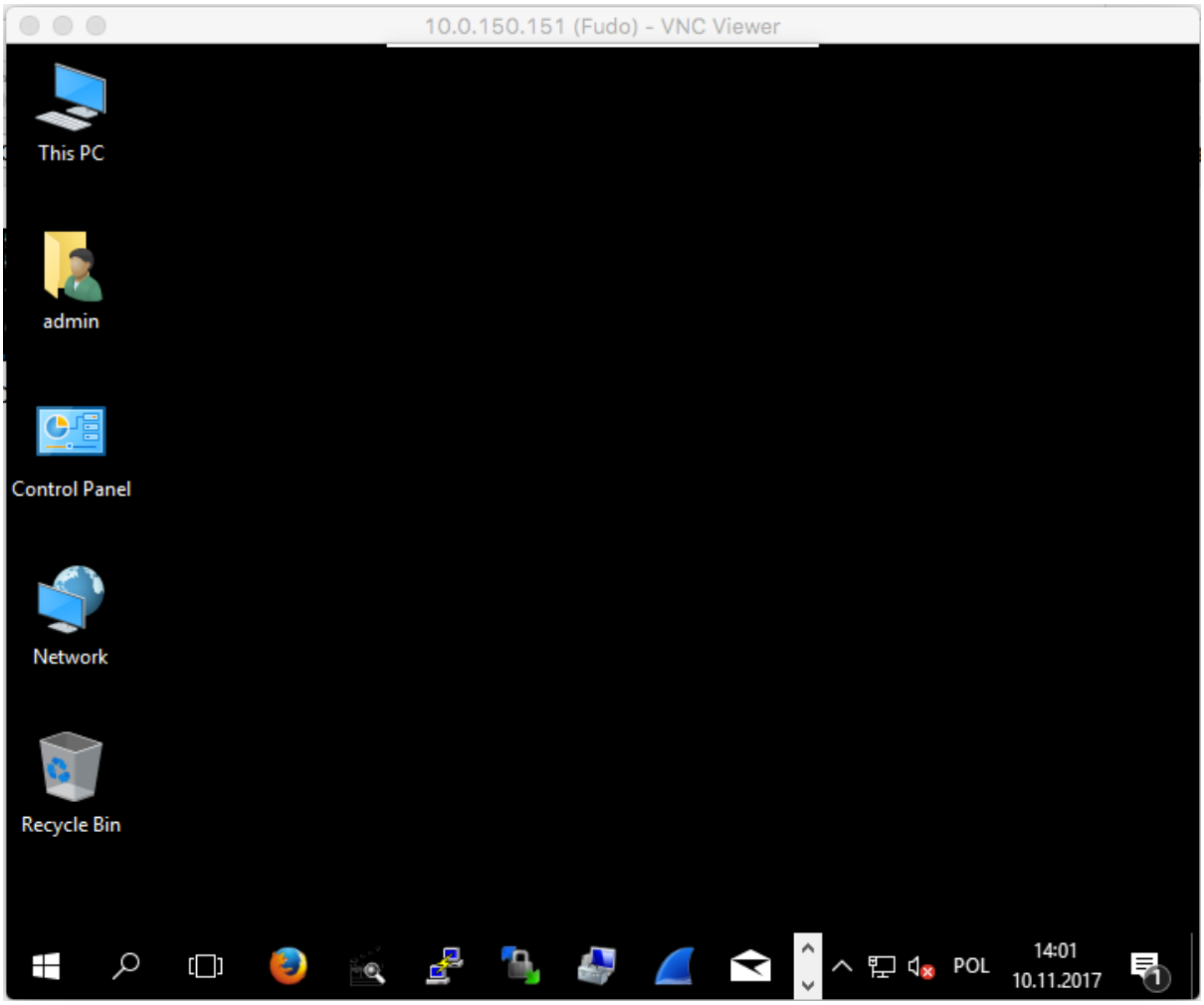
5.11.3 Nawiązanie połączenia

1. Uruchom aplikację kliencką *VNC Viewer* i w polu adresu wprowadź `10.0.150.151`.



2. Wprowadź nazwę użytkownika, hasło i zatwierdź klawiszem enter.


10.0.150.151 (Fudo) - VNC Viewer
Login
john_smith
Password
Log in



5.11.4 Podgląd sesji połączeniowej

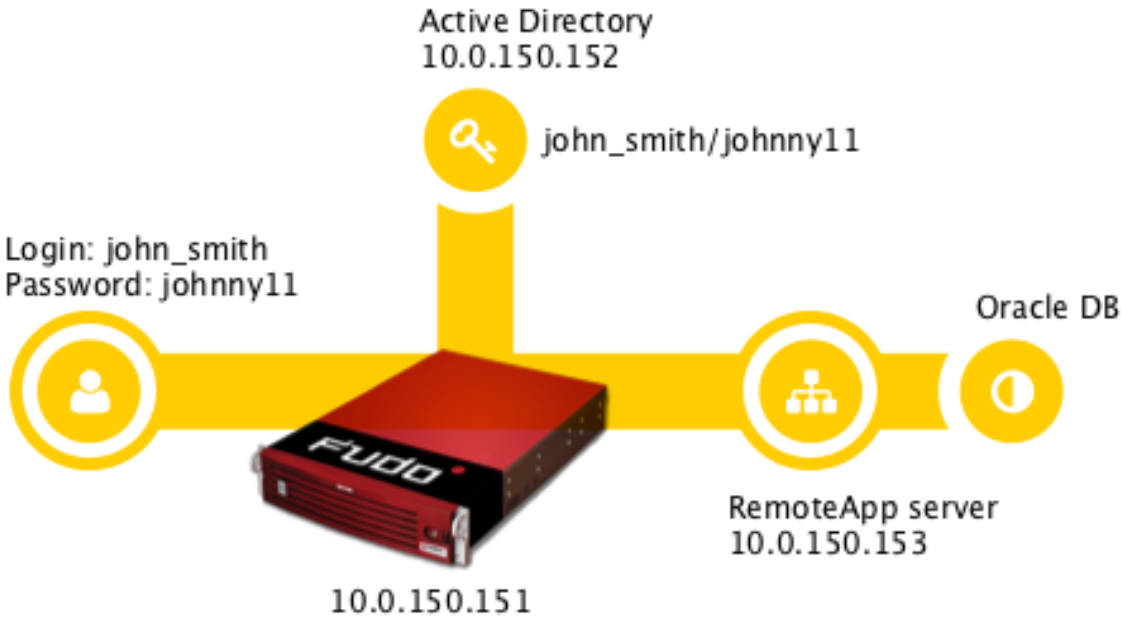
1. W przeglądarce internetowej wpisz adres `10.0.150.151`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Fudo PAM.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.

Tematy pokrewne:

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

5.12 Oracle poprzez RemoteApp

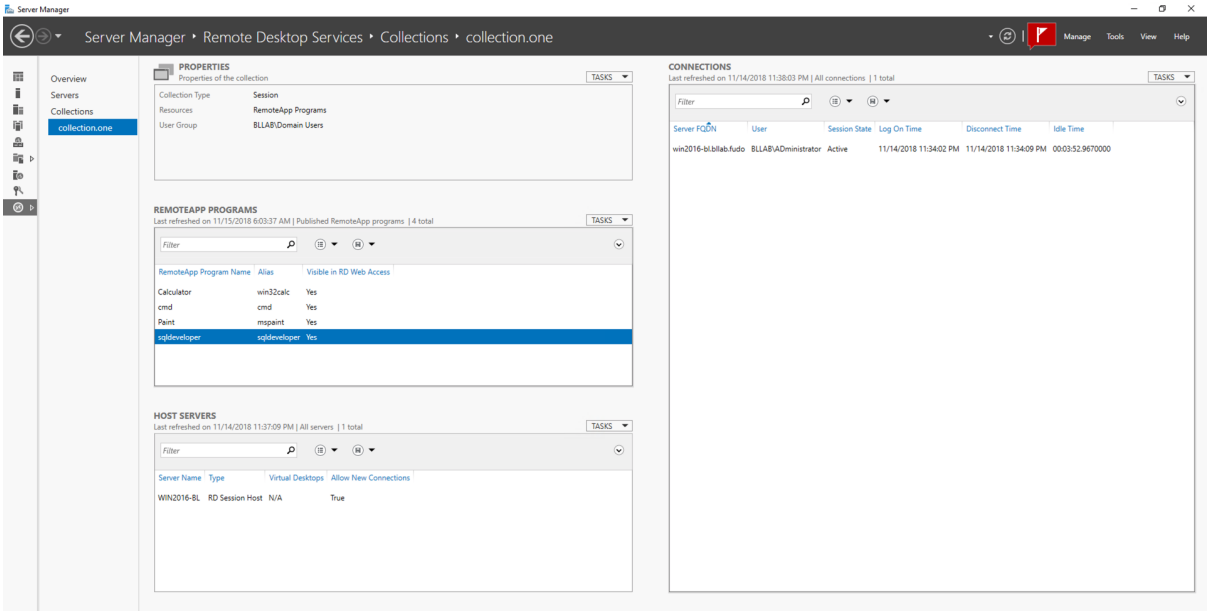
W tym rozdziale przedstawiony jest przykład konfiguracji Fudo PAM, której celem jest monitorowanie połączeń z bazą danych Oracle poprzez serwer RemoteApp. Scenariusz zakłada, że użytkownik łączy się z serwerem RemoteApp poprzez protokół *RDP*. Tożsamość użytkownika weryfikowana jest w Active Directory, a dane logowania przesyłane są *do serwera docelowego*. Połączenie następuje poprzez Fudo, w *trybie pośrednika*.



Ostrzeżenie: Wsparcie protokołu `Oracle` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

5.12.1 Wymagania

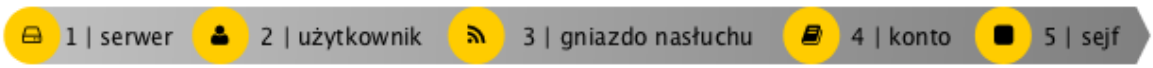
- Wdrożona i skonfigurowana usługa RDS na systemie Windows Server 2012/2012 RE/2016.
- Skonfigurowana kolekcja z aplikacją SQL Developer.



- Wdrożona usługa Active Directory do uwierzytelnienia tożsamości użytkowników.

Poniższy opis zakłada, że pierwsze uruchomienie Fudo zostało prawidłowo przeprowadzone, w środowisku informatycznym, funkcjonuje prawidłowo skonfigurowana usługa RemoteApp oraz Active Directory. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

5.12.2 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* i wybierz opcję *Serwer statyczny*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Ogólne	
Nazwa	RemoteApp Server
Opis	✘
Zablokowane	✘
Protokół	`RDP`
Bezpieczeństwo	`Enhanced RDP Security (TLS) + NLA`
Starsze algorytmy kryptograficzne	✘
Adres źródłowy	`Dowolny`

Uprawnienia	
Uprawnieni użytkownicy	✘

Adresy serwerów	
Adres IP	`10.0.150.153`
Port	`3389`

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

Dodanie użytkownika

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
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	✗

Uwierzytelnienie	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła statycznego	✗
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	`RemoteApp-listener`
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Enhanced RDP Security (TLS) + NLA`
Komunikat	✗

Uprawnienia	
Uprawnieni użytkownicy	✗

Połączenie	
Tryb połączenia	`proxy`
Adres lokalny	`10.0.150.151`
Port	`10025`
Adres zewnętrzny	✗
Port zewnętrzny	✗

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	`RemoteApp-account`
Zablokowane	✗
Typ	`forward`
Nagrywanie sesji	`wszystko`
OCR sesji	✓
Język OCR	`Angielski`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`RemoteApp_server`
Dane uwierzytelniające	
Zastąp sekret	✗
Przekazuj domenę	✓

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	`RemoteApp-safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✓
SSH	✗
VNC	✗

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `RemoteApp-account` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź obiekt `RemoteApp-listener` i kliknij +.
14. Kliknij *OK*.
15. Kliknij *Zapisz*.

5.12.3 Zmiana wpisów w rejestrze systemowym na kontrolerze domeny RDS

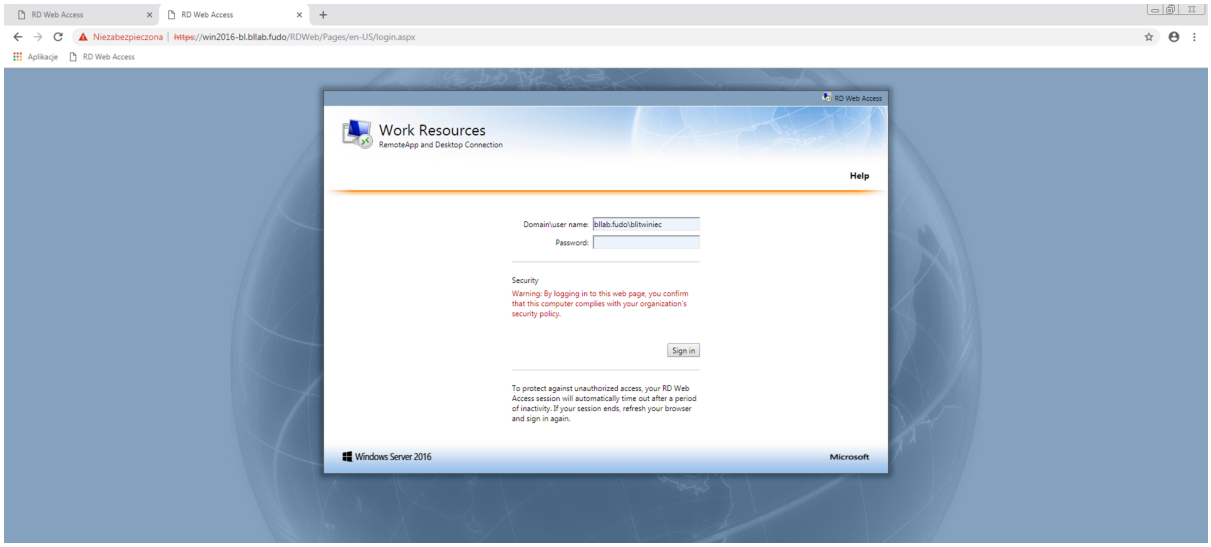
1. Zaloguj się na konto administratora na serwerze, na których uruchomiona jest usługa RDS.
2. Uruchom edytor rejestru systemowego.
3. Odszukaj klucz

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\TerminalServer\
CentralPublishedResources\PublishedFarms\collectionone\Applications\sqldeveloper
```

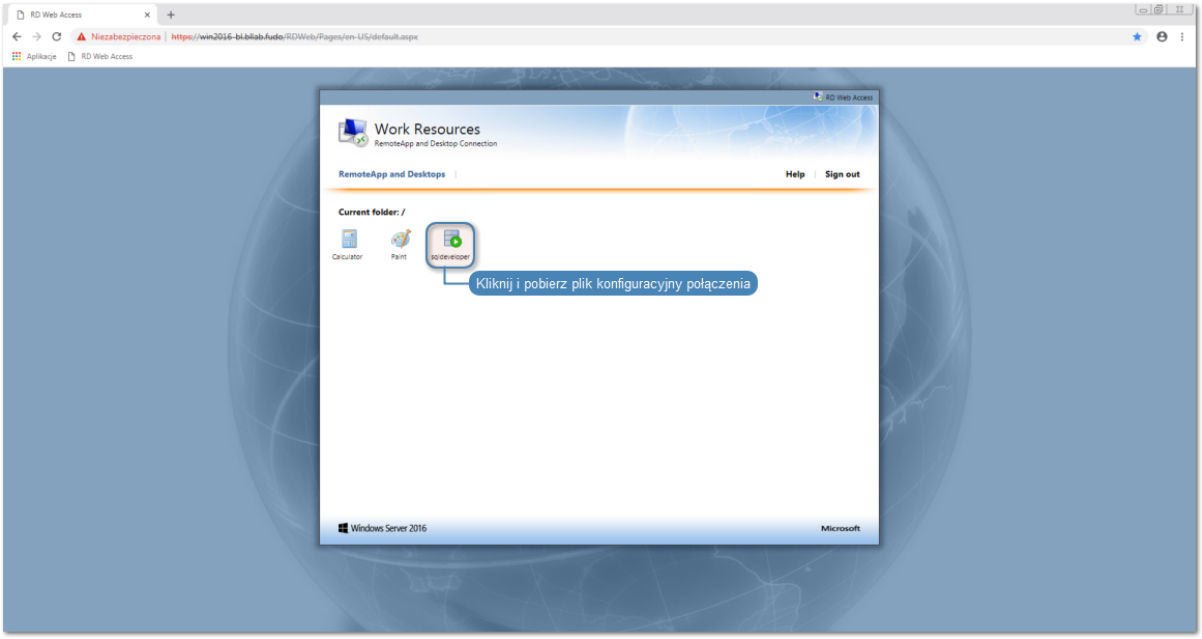
4. W parametrze *RDPFileContent*, znajdź atrybut *full address:s:* i zmień jego wartość na adres IP i numer portu gniazda nasłuchiwania, tj. `full address:s:10.0.150.151:10025`

5.12.4 Nawiązanie połączenia

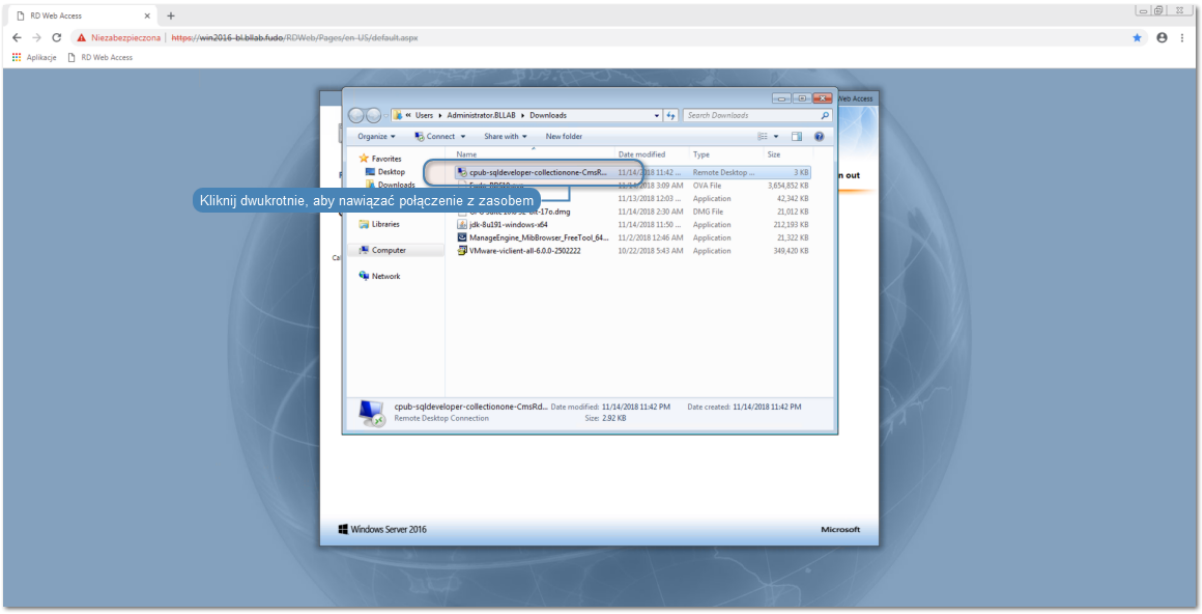
1. Uruchom przeglądarkę na systemie użytkownika, wprowadź adres kontrolera domeny RDS i zaloguj się do portalu.



2. Kliknij aplikację *SQL Developer*, aby pobrać plik konfiguracyjny RemoteApp.

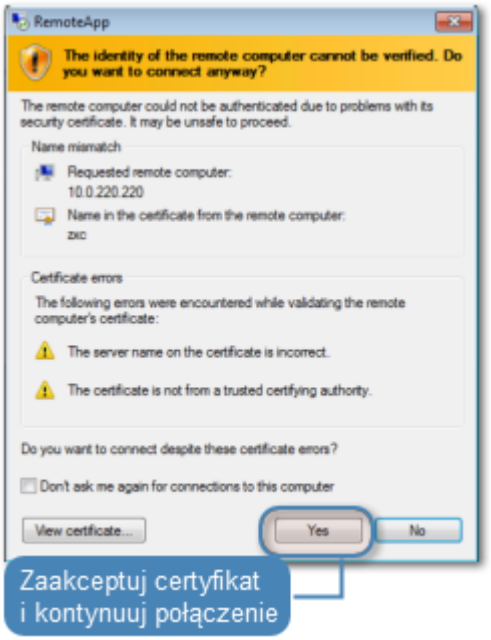


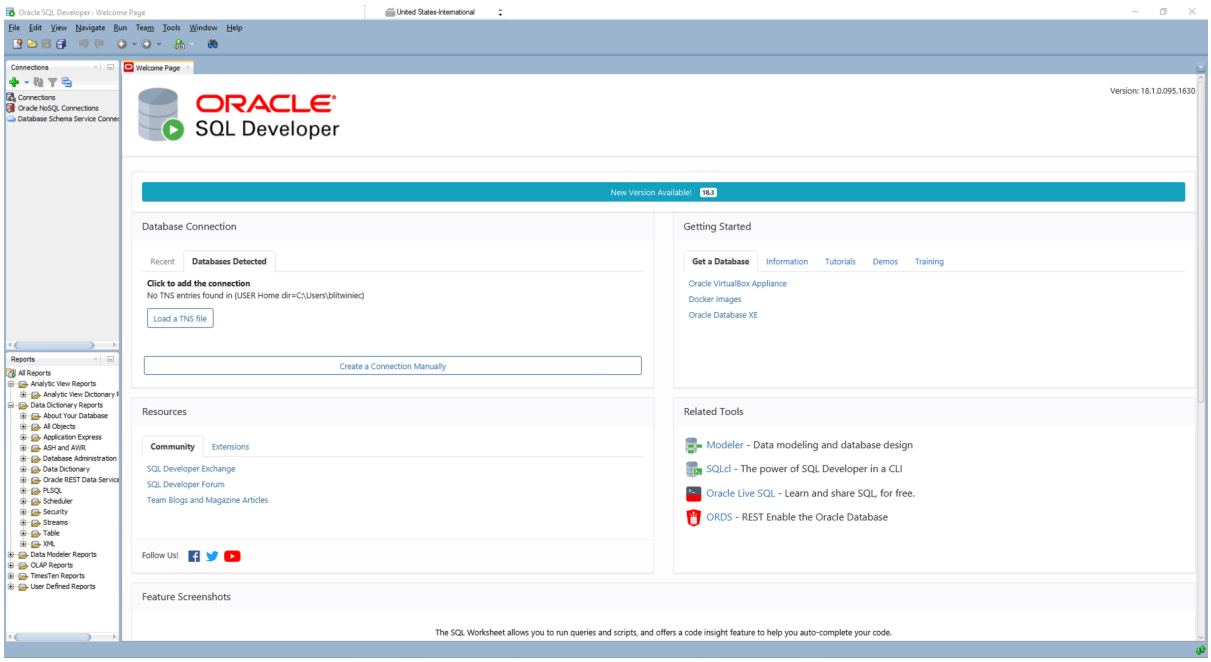
3. Kliknij dwukrotnie pobrany plik konfiguracyjny.



4. Kliknij Connect, aby połączyć się z wybranym zasobem zasobem.

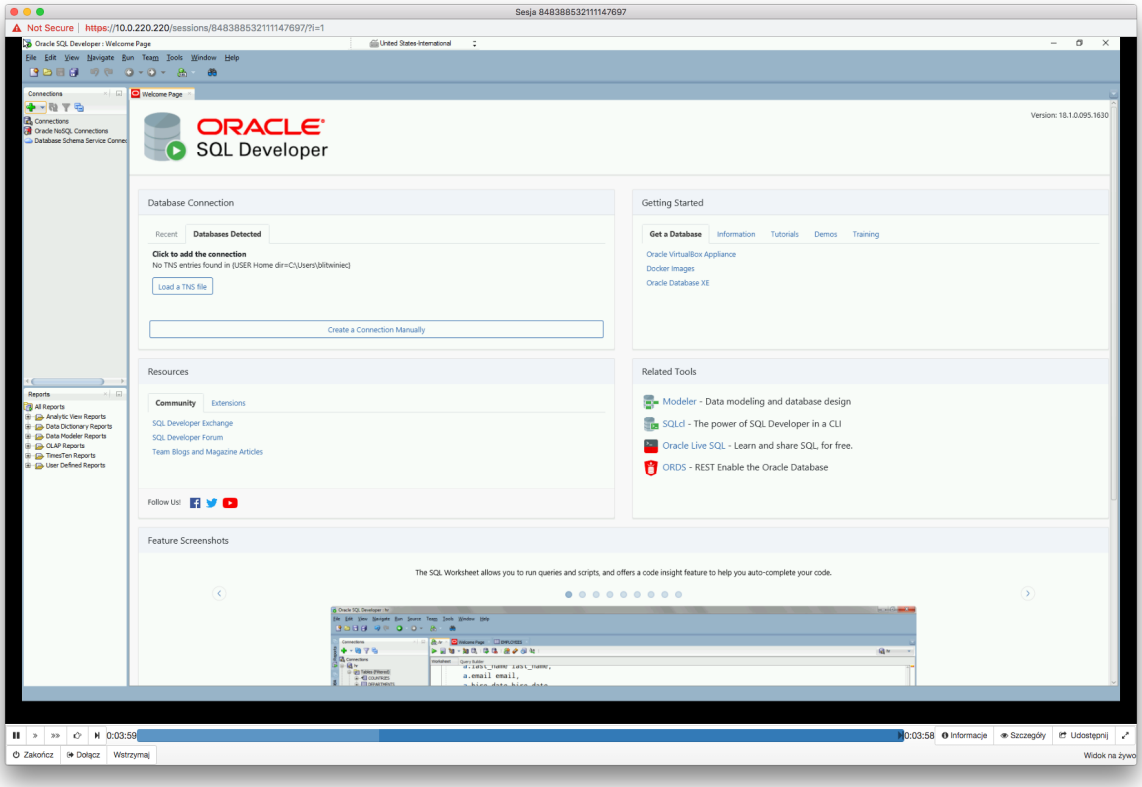
5. Wprowadź dane logowania użytkownika.
6. Zaakceptuj certyfikat i potwierdź nawiązanie połączenia.





5.12.5 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wprowadź adres panelu administracjnego Fudo.
2. Wprowadź nazwę użytkownika oraz hasło.
3. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
4. Znajdź na liście sesję użytkownika *John Smith* i kliknij ikonę odtwarzania sesji.



Tematy pokrewne:

- *RDP*
- *Szybki start - konfigurowanie połączenia RDP*
- *Wymagania*
- *Model danych*

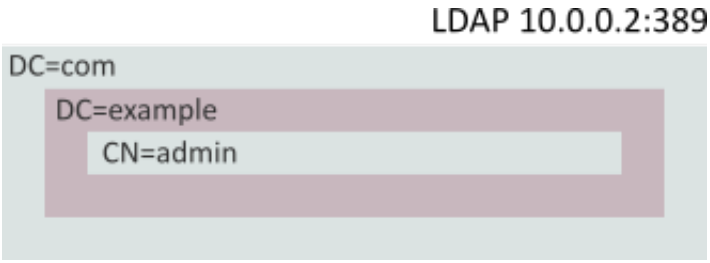
5.13 Uwierzytelnienie użytkowników w katalogu LDAP

W tym rozdziale przedstawiony jest przykład konfigurowania usługi LDAP jako zewnętrznego źródła uwierzytelnienia i wykorzystanie definicji do uwierzytelnienia użytkownika zdefiniowanego w lokalnym modelu danych systemu Fudo PAM.

5.13.1 Założenia

Poniższy opis zakłada, że dane uwierzytelniające użytkownika `admin` sprawdzane są na serwerze LDAP, dostępnym pod adresem 10.0.0.2 i na domyślnym numerze portu usługi LDAP tj. 389.

Definicja użytkownika znajduje się pod ścieżką `cn=admin,dc=example,dc=com`.



5.13.2 Konfiguracja

Dodanie zewnętrznego źródła uwierzytelnienia

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnienie*.
2. Kliknij *+ Dodaj zewnętrzne źródło uwierzytelnienia*.
3. Uzupełnij parametry konfiguracyjne usługi:

Parametr	Wartość
Typ	`LDAP`
Adres hosta	`10.0.0.2`
Port	`389`
Wysyłaj żądania z	`10.0.0.10`
Bind DN	`dc=example,dc=com` **Informacja:** Alternatywnie, określ pełną ścieżkę miejsca przechowywania definicji kont użytkowników `cn=##username##, dc=example,dc=com` i pozostaw pole *Baza LDAP* w konfiguracji użytkowników puste.
Połączenie szyfrowane	✘
Usuń	✘

4. Kliknij *Zapisz*.

Dodanie metody uwierzytelnienia użytkownika

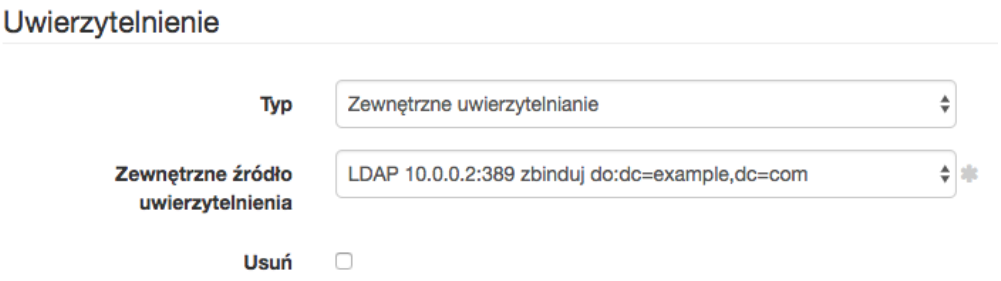
1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.

2. Odszukaj na liście i kliknij użytkownika `admin`.
3. W polu *Baza LDAP* wprowadź ciąg definiujący obiekt *admin* w strutkurze katalogowej `cn=admin,dc=example,dc=com`.

Informacja: Pozostaw pole *Baza LDAP* puste, jeśli w konfiguracji zewnętrznego źródła uwierzytelnienia podana została pełna ścieżka miejsca przechowywania kont użytkowników w drzewie katalogów (`cn=##username##,dc=example,dc=com`).

---

4. Kliknij *+ Dodaj metodę uwierzytelnienia*.
5. Z listy rozwijalnej *Typ*, wybierz `Zewnętrzne uwierzytelnienie`.
6. Z listy rozwijalnej *Zewnętrzne źródło uwierzytelnienia*, wybierz `LDAP 10.0.0.10:389 zbinduj do:dc=example,dc=com`.



7. Kliknij *Zapisz*.

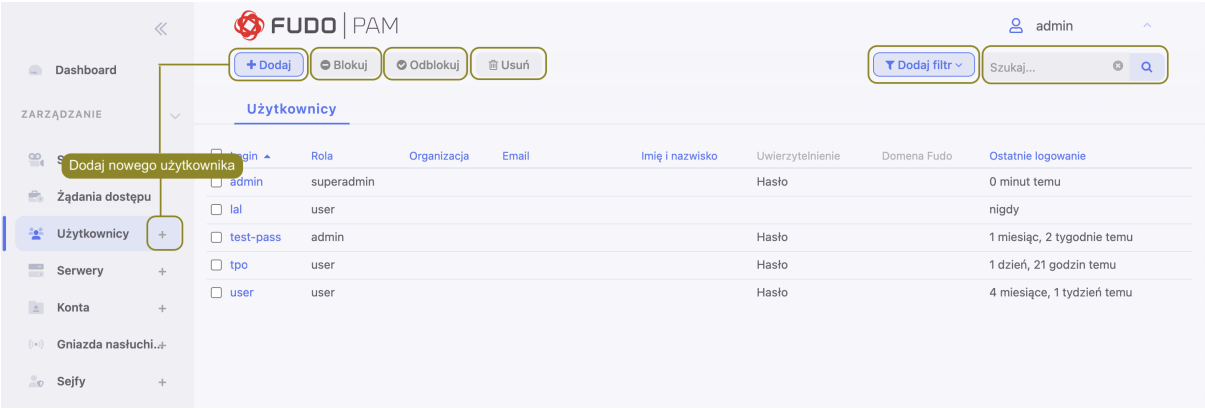
Tematy pokrewne:

- *Zewnętrzne serwery uwierzytelniania*
- *Dodawanie użytkownika*
- *Konfigurowanie monitorowania połączeń SSH*

ROZDZIAŁ 6

Użytkownicy

Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.



6.1 Dodawanie użytkownika

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 replikacją danych, skontaktuj się z działem wsparcia technicznego.

Ostrzeżenie: Tworząc obiekt Użytkownik dla połączeń MySQL, miej na uwadze, że domyślny plugin MySQL `caching_sha2_password` nie jest obecnie wspierany przez Fudo PAM. Wspierane plugin'y dla połączeń MySQL przez Fudo PAM - to są

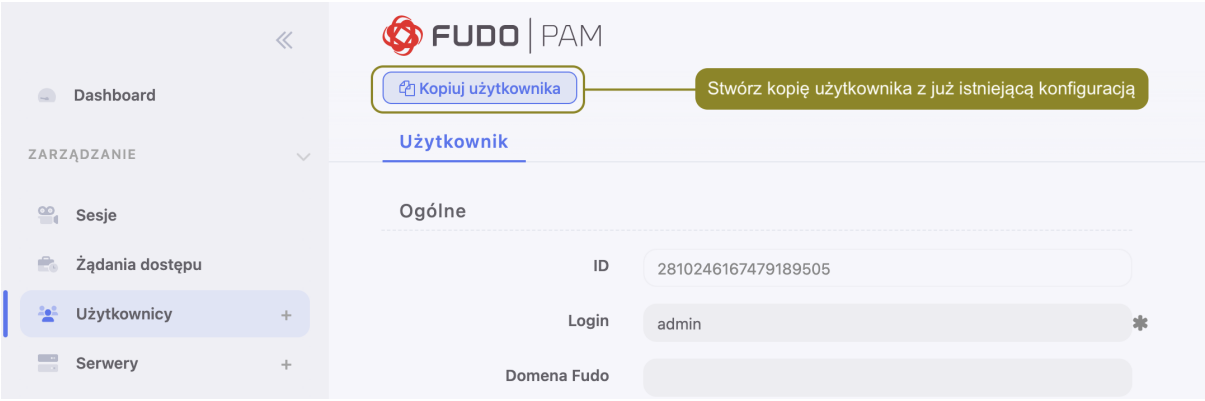
`mysql_native_password` oraz `mysql_old_password`. Plugin Serwera powinien być ustawiony do `mysql_native_password` w `/etc/mysql/mysql.conf.d/mysqld.cnf` oraz Użytkownik stworzony z plugin'em `mysql_native_password`.

Aby dodać definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

1. Kliknij + obok zakładki *Użytkownicy*, albo

Wybierz z lewego menu *Zarządzanie* > *Użytkownicy* i kliknij + *Dodaj*.

Informacja: 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.



---

2. Wprowadź nazwę użytkownika.

Informacja:

- Model danych dopuszcza istnienie więcej niż jednego obiektu o tym samym loginie, z zachowaniem unikalności kombinacji loginu i domeny.
- Pole *Login* nie rozróżnia wielkości liter.

---

3. Określ domenę Fudo.

Informacja:

- W przypadku zdefiniowania domeny Fudo, użytkownik będzie musiał ją podać przy logowaniu do panelu administracyjnego Fudo oraz podczas nawiązywania połączeń z monitorowanymi serwerami.
- *Domena domyślna* dopuszcza dowolność - użytkownik może ją wskazać podczas logowania ale nie jest to konieczne.

---

4. Zaznacz opcję *Zablokowane*, aby uniemożliwić użytkownikowi zalogowanie zaraz po utworzeniu konta.
5. Określ ważność tworzonego konta.

6. Zdefiniuj rolę, determinującą prawa dostępu użytkownika.

Informacja: Określone rolą uprawnienia, dotyczą także dostępu do modelu danych poprzez interfejs API.

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).
service	• monitorowanie stanu systemu poprzez protokół SNMP.
operator	• logowanie do panelu administracyjnego, • przeglądanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, • blokowanie/odblokowywanie wybranych obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, • generowanie i subskrybowanie raportów, • zarządzanie powiadomieniami, • konwersja sesji, w której pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • pobieranie haseł do serwerów (wymaga stosownego uprawnienia), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych.

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, w której pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału, • włączanie/wyłączanie powiadomień email, • zarządzanie politykami, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, • zarządzanie modyfikatorami haseł, • pobieranie haseł do serwerów (wymaga stosownego uprawnienia), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych.
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), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych, licencja, dziennik zdarzeń systemowych.

7. Określ preferowany język panelu administracyjnego Fudo PAM.
8. Dodaj sejfy z kontami uprzywilejowanymi, do których użytkownik będzie miał dostęp.

Informacja:

- Przeciągnij i upuść sejf, żeby określić kolejność użycia danych przechowywanych w sejfie przy zestawianiu połączenia.
- Kliknij sejf, aby zdefiniować *politykę czasu dostępu*.

9. Wprowadź pełną nazwę użytkownika, która umożliwi jego jednoznaczną identyfikację.
10. Wprowadź adres email użytkownika.

Informacja: Na podany adres email, Fudo PAM wysyła subskrybowane raporty cykliczne.

11. Wprowadź nazwę organizacji, do której przynależy użytkownik.
12. Podaj numer telefonu użytkownika.
13. Wprowadź domenę *AD*, do której należy konto użytkownika.

Informacja: Fudo PAM nie jest w stanie rozróżnić przypadków, w którym istnieją dwaj użytkownicy o tym samym loginie, z których jeden ma zdefiniowaną domenę taką samą jak *domena domyślna* a drugi nie ma określonej domeny. Takie sytuacje będą skutkowały brakiem możliwości zalogowania konfliktujących użytkowników.

14. Wprowadź parametr bazowy usługi katalogowej LDAP (*Base DN*).

Informacja:

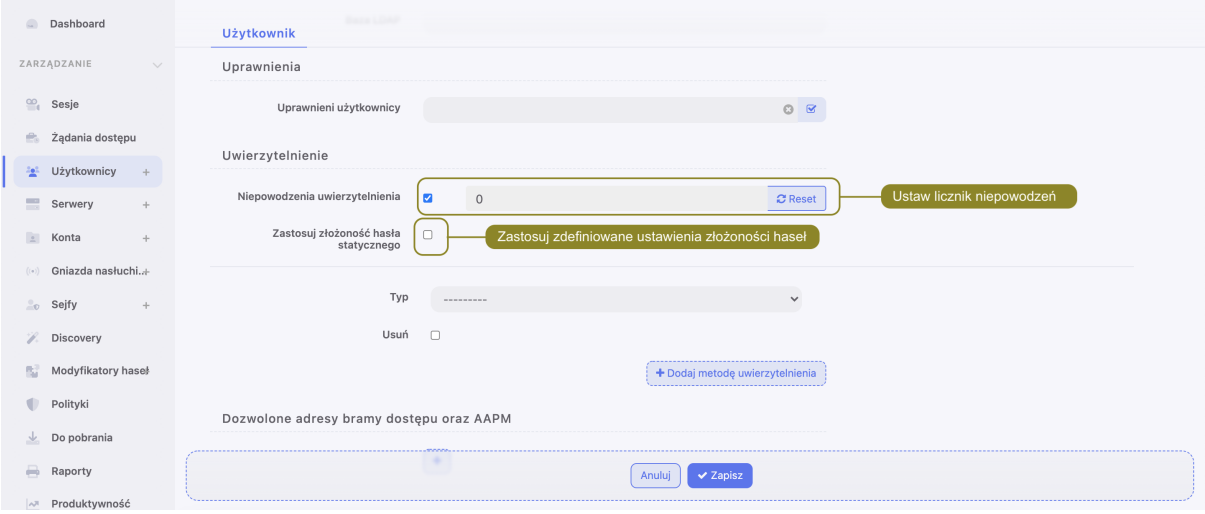
- Parametr bazowy LDAP jest wymagany do uwierzytelnienia użytkownika w usłudze Active Directory.
- Dla użytkownika `admin` w przykładowej domenie `example.com`, parametr powinien przyjąć postać `cn=admin,dc=example,dc=com`.

15. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania tworzonym obiektem, a w przypadku użytkowników o roli *admin* i *operator*, zdefiniuj prawo do zarządzania obiektami modelu danych.

Informacja: Aby operator lub administrator miał możliwość podglądu wybranej sesji, musi mieć przypisane prawo dostępu do: serwera, konta, sejfu i użytkownika związanych z określonym połączeniem.

16. W sekcji *Uwierzytelnienie*, zaznacz opcję *Niepowodzenia uwierzytelnienia*, aby konto zostało automatycznie zablokowane w przypadku przekroczenia limitu nieudanych prób logowania.

Informacja: Nieudane próby logowania są rejestrowane, jeśli włączona jest opcja Niepowodzenia uwierzytelnienia dla konkretnego użytkownika oraz w zakładce *Ustawienia* > *System*, w sekcji *Uwierzytelnianie użytkowników i sesje*.



17. Zaznacz opcję *Zastosuj złożoność hasła statycznego*, aby wymusić zgodność hasła z ustawieniami systemowymi.

Informacja: Złożoność hasła definiowana jest w menu *Ustawienia* > *System*, w sekcji *Uwierzytelnianie użytkowników i sesje*.

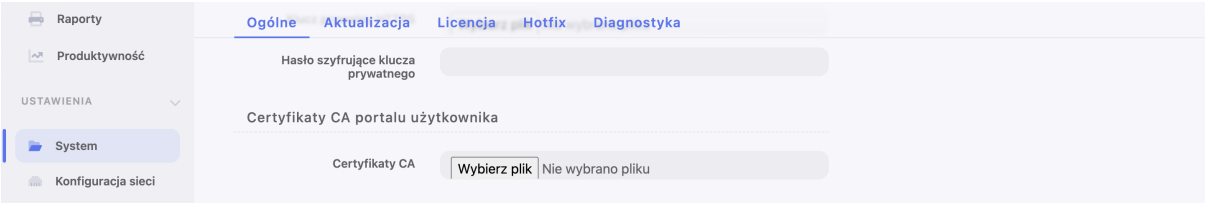
---

18. W sekcji *Uwierzytelnienie*, określ sposób uwierzytelnienia użytkownika.

Certyfikat

- Wprowadź *Podmiot*, zgodny z RFC 2253 lub RFC 4514.

Informacja: Metoda uwierzytelnienia `certyfikat` wymaga dodatkowego wgrania pliku z certyfikatami CA w zakładce *Ustawienia* > *System* sekcji *Ogólne*.



Więcej informacji na temat konfiguracji Certyfikatu jako metody uwierzytelnienia znajdziesz pod linkiem: *Model uwierzytelniania w oparciu o certyfikaty*.

DUO

- Z listy **Pierwszy składnik** wybierz *Hasło statyczne* albo *Zewnętrzne uwierzytelnianie* (AD albo LDAP).
- Wprowadź *Użytkownik DUO*.
- Wprowadź *ID użytkownika DUO*.

Informacja: Więcej informacji na temat konfiguracji DUO jako metody uwierzytelnienia znajdziesz pod linkiem: *Definicja uwierzytelnienia DUO*.

SMS

- Wprowadź numer telefonu w polu **Telefon**.
- Z listy **Pierwszy składnik** wybierz *Hasło statyczne* albo *Zewnętrzne uwierzytelnianie* (AD albo LDAP).

Informacja: Więcej informacji na temat konfiguracji SMS jako metody uwierzytelnienia znajdziesz pod linkiem: *Definicja uwierzytelnienia SMS*.

Hasło

- Z listy rozwijalnej *Typ*, wybierz `Hasło`.
- Wprowadź hasło w polu *Hasło*.
- Powtórnie wprowadź hasło w polu *Powtórz hasło*.
- Zaznacz opcję *Wymagaj zmiany hasła przy kolejnym logowaniu*, aby wymusić na użytkowniku zmianę hasła przy następnym logowaniu do *Portalu Użytkownika*.

Informacja: Zaznaczenie opcji *Wymagaj zmiany hasła przy kolejnym logowaniu* uniemożliwi bezpośrednie (z pominięciem *Portalu Użytkownika*) zalogowanie się do monitorowanych serwerów za pomocą aplikacji klienckiej wybranego protokołu. Użytkownik będzie musiał zmienić hasło poprzez *Portal użytkownika*.

Zewnętrzne uwierzytelnienie

- Z listy rozwijalnej *Typ*, wybierz `Zewnętrzne uwierzytelnienie`.
- Z listy rozwijalnej *Zewnętrzne źródło uwierzytelnienia* wybierz źródło, które zostanie użyte do uwierzytelnienia użytkownika.

Informacja: Procedura definiowanie zewnętrznych źródeł uwierzytelnienia opisana jest w rozdziale *Zewnętrzne serwery uwierzytelniania*.

Klucz SSH

- Z listy rozwijalnej *Typ*, wybierz `Klucz SSH`.
- Kliknij ikonę w polu tekstowym *Klucz publiczny* i wskaż plik z definicją klucza publicznego użytkownika, który zostanie użyty do zweryfikowania jego tożsamości.

Hasło jednorazowe

Ostrzeżenie: Opcja logowania za pomocą hasła jednorazowego ma zastosowanie w implementacjach mechanizmu bezpiecznej wymiany haseł pomiędzy aplikacjami (*AAPM*).

- Z listy rozwijalnej *Typ*, wybierz `Hasło jednorazowe`.

19. Kliknij *+ Dodaj metodę uwierzytelnienia*, aby zdefiniować kolejną metodę uwierzytelnienia.

Informacja: W procesie uwierzytelnienia, Fudo PAM dokonuje sprawdzenia danych logowania użytkownika w oparciu o źródła uwierzytelnienia w kolejności w jakiej zostały zdefiniowane. W przypadku niepowodzenia uwierzytelnienia za pomocą pierwszej metody, Fudo PAM próbuje uwierzytelnić użytkownika za pomocą kolejnych.

20. W sekcji *API* kliknij [+], aby dodać adres IP wykorzystywany przez *Access Gateway* oraz *AAPM* do komunikacji z Fudo PAM.
21. Kliknij *Zapisz*.

Tematy pokrewne:

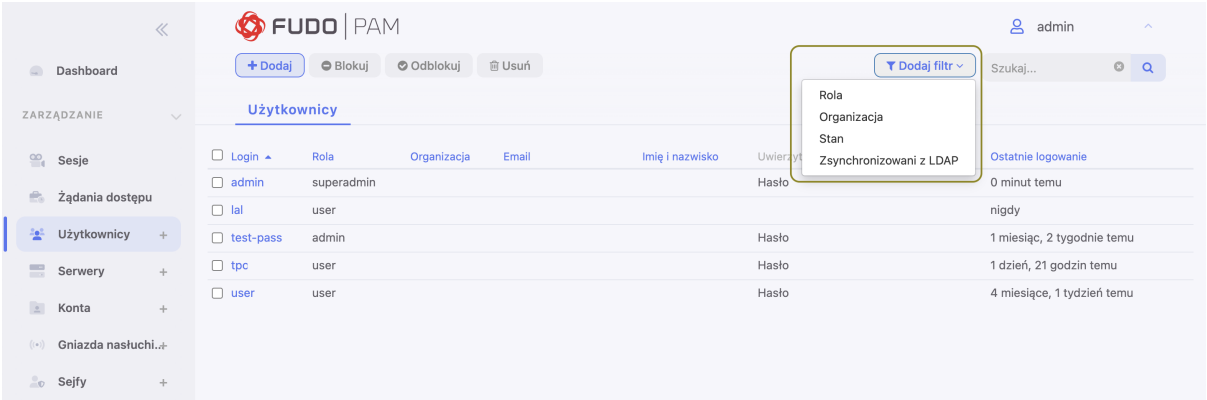
- *Zliczanie niepowodzeń uwierzytelnienia*
- *Synchronizacja użytkowników z LDAP*
- *Domyślna domena*
- *Polityka czasowa dostępu do sejfów*
- *Model danych*
- *Złożoność haseł*

6.2 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.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



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

Informacja:

- ID użytkowika jest identyfikatorem obiektu nadawanym automatycznie przez Fudo PAM i jest parametrem tylko do odczytu.

5. Kliknij *Zapisz*.

Tematy pokrewne:

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

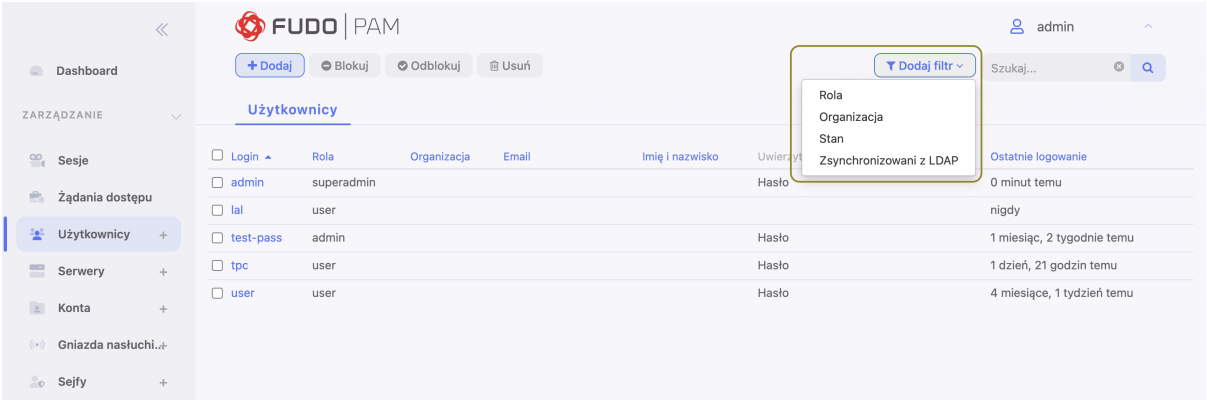
6.3 Blokowanie użytkownika

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

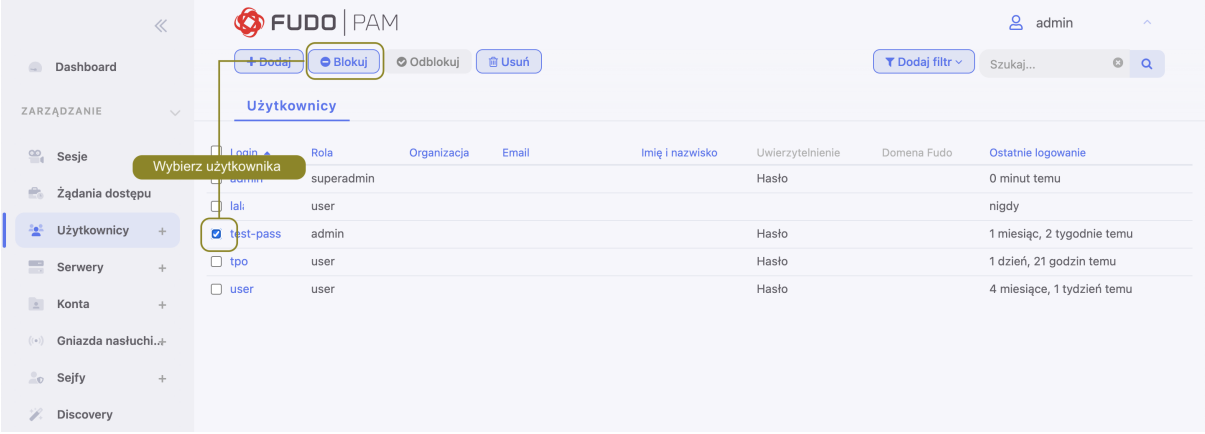
Ostrzeżenie: Zablokowanie użytkownika spowoduje przerwanie aktualnie nawiązanych przez niego połączeń.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i zaznacz użytkownika, którego chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



3. Kliknij *Blokuj*, aby zablokować użytkownikowi możliwość nawiązywania połączeń.



4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.

Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Informacja: Konto użytkownika może zostać również zablokowane z poziomu formularza edycji obiektu.

- Zaznacz opcję *Zablokowane*.
- Opcjonalnie, wprowadź powód zablokowania.
- Kliknij *Zapisz*.

Tematy pokrewne:

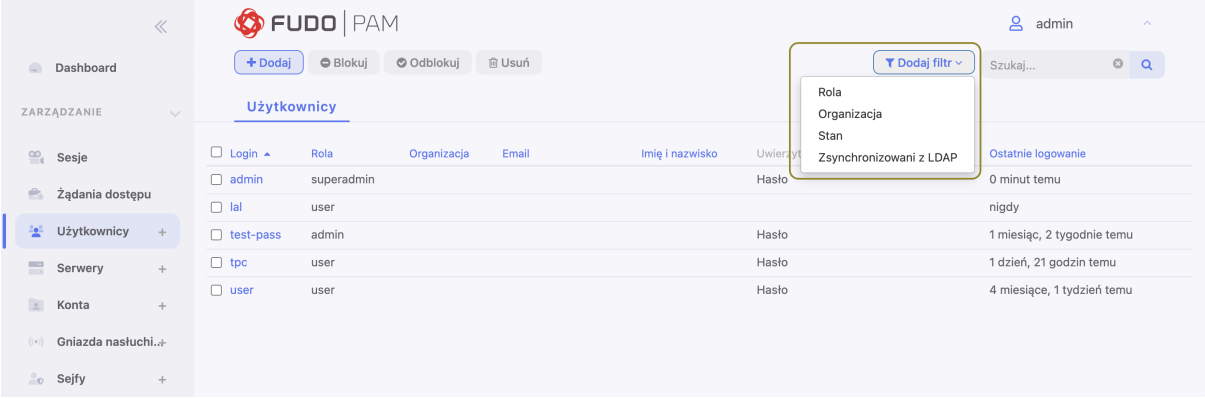
- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*

6.4 Odblokowanie użytkownika

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

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



3. Kliknij *Odblokuj*, aby umożliwić użytkownikowi nawiązywanie połączeń.
4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektu.

Tematy pokrewne:

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

6.5 Usuwanie użytkownika

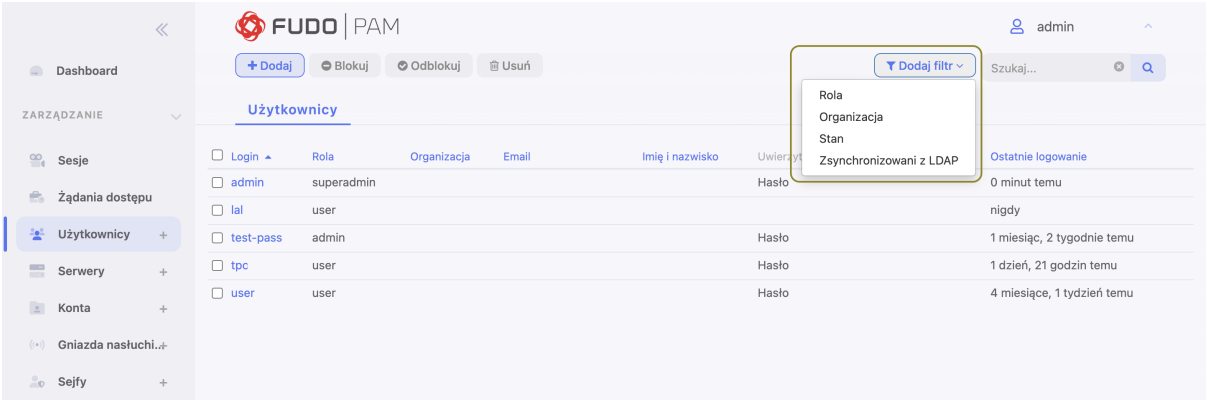
Aby usunąć definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

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

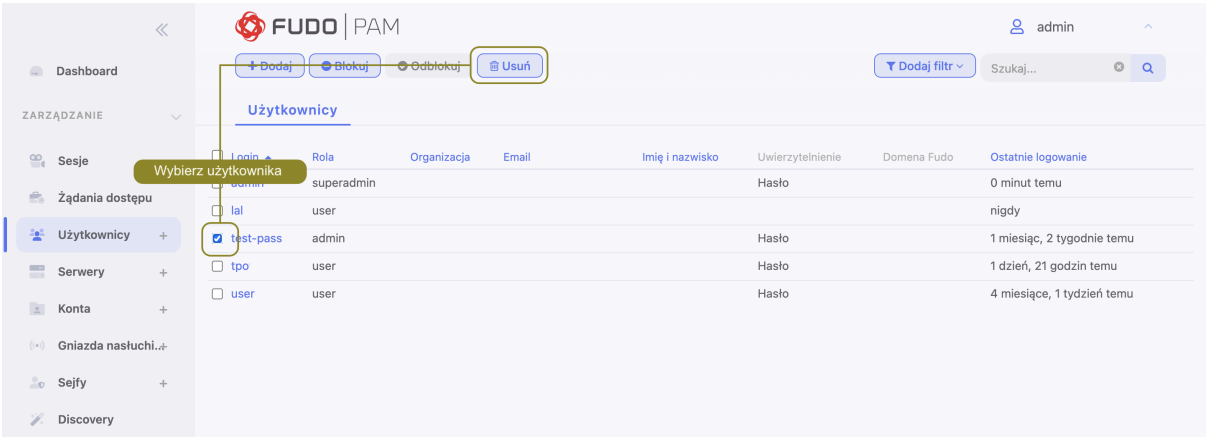
Ostrzeżenie: Usunięcie użytkownika spowoduje przerwanie aktualnie nawiązanych przez niego połączeń.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i zaznacz konta, które chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



3. Kliknij *Usuń*.



4. Potwierdź operację usunięcia zaznaczonych obiektów.

Tematy pokrewne:

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

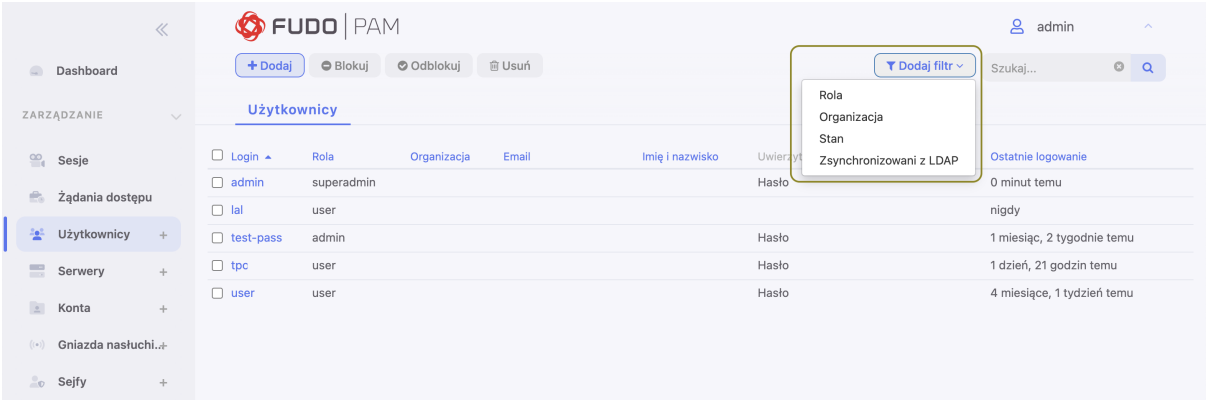
6.6 Polityka czasowa dostępu do sejfów

Fudo PAM pozwala na regulowanie dostępu do sejfów na podstawie definiowanych ram czasowych.

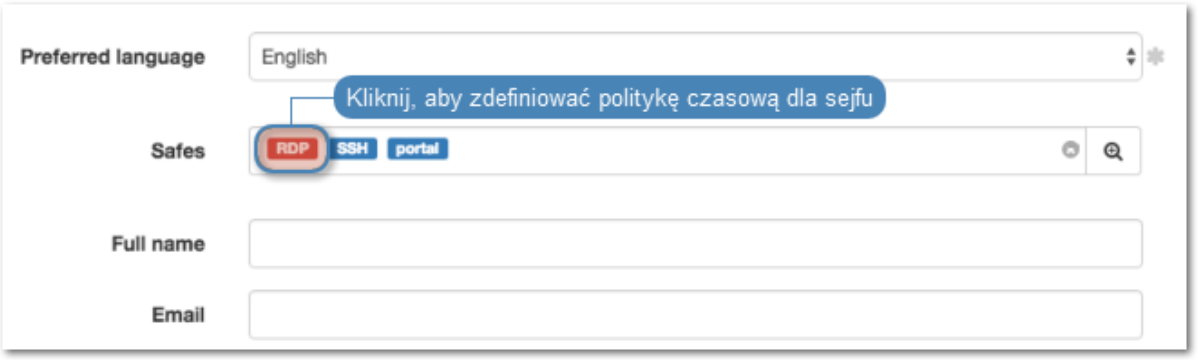
Aby zdefiniować politykę czasu dostępu do sejfu, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście definicję użytkownika.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



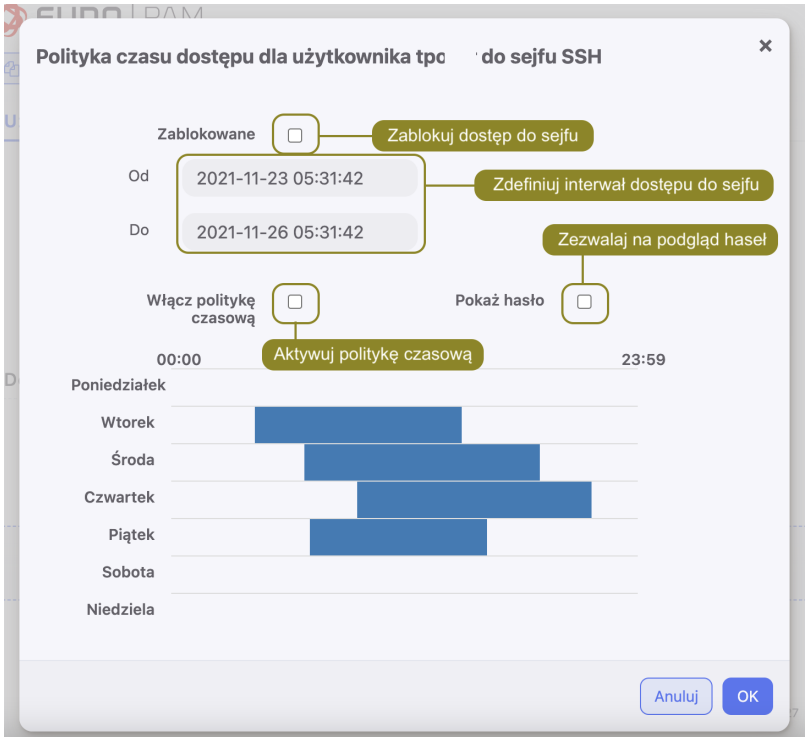
3. Kliknij nazwę użytkownika.
4. Kliknij wybrany sejf.



5. Zaznacz opcję *Zablokowane*, jeśli chcesz uniemożliwić użytkownikowi nawiązywanie połączeń poprzez wybrany sejf. Użytkownik będzie miał zablokowany dostęp, dopóki administrator nie wyłączy opcję *Zablokowane*, albo nie kliknie *Odblokuj dostęp* w konfiguracji sejfu.
6. Uzupełnij pola *Od* and *Do* interwałem czasu, w którym użytkownik będzie mógł nawiązywać połączenia za pośrednictwem wybranego sejfu. Kiedy podany czas nadejdzie, dostęp do sejfu zostanie przyznany użytkownikowi automatycznie. Opcja *Zablokowane* z poprzedniego kroku powinna być odznaczona.

Informacja: Pozostaw pola kalendarza puste, aby dostęp do sejfu był bezterminowy.

7. Zaznacz opcję *Włącz politykę czasową*, aby użytkownik mógł nawiązywać połączenia tylko w wyznaczonych godzinach.
8. Zaznacz opcję *Pokaż hasło*, aby zezwolić użytkownikowi na podgląd haseł w *Portalu Użytkownika*.
9. Kliknij kalendarz, aby zdefiniować przedziały czasowe, w których użytkownik będzie mógł się łączyć poprzez konta przypisane do wybranego sejfu.



10. Kliknij *OK*.
11. Kliknij *Zapisz*.

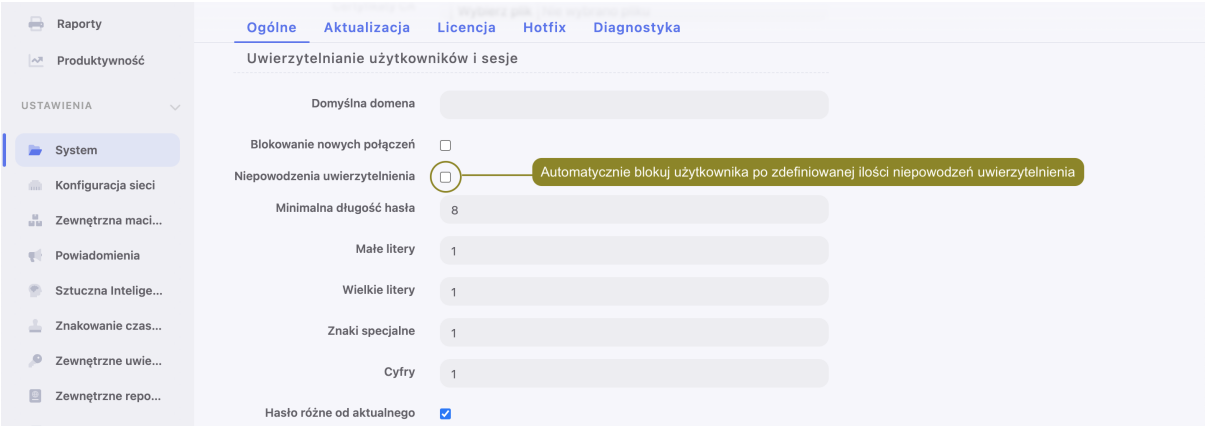
Tematy pokrewne:

- *Dodawanie użytkownika*
- *Sejfy*

6.7 Zliczanie niepowodzień uwierzytelnienia

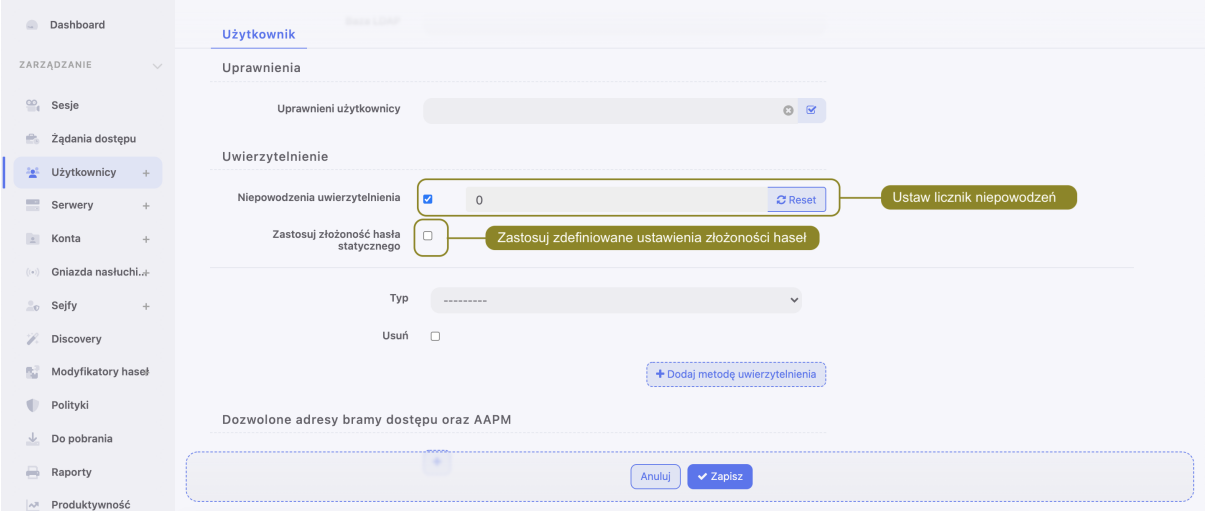
Fudo może zliczać niepowodzenia logowania i automatycznie blokować konto użytkownika, z chwilą gdy licznik nieudanych prób uwierzytelnienia osiągnie zdefiniowaną wartość.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Uwierzytelnianie użytkowników i sesje*, zaznacz opcję *Niepowodzenia uwierzytelnienia*.
3. Określ liczbę niepowodzeń uwierzytelnienia, po której konto użytkownika zostanie zablokowane.



4. Kliknij *Zapisz*.
5. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
6. Odszukaj na liście i kliknij użytkownika, dla którego chcesz włączyć opcję automatycznego blokowania.
7. W sekcji *Uwierzytelnienie*, zaznacz opcję *Niepowodzenia uwierzytelnienia*.
8. Kliknij *Zapisz*.

Informacja: Kliknij Reset aby zresetować wskazanie licznika.



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*

6.8 Role użytkownika

Role użytkownika umożliwiają regulowanie dostępu do obiektów zarządzanych i monitorowanych przez Fudo PAM.

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).
service	• monitorowanie stanu systemu poprzez protokół SNMP.
operator	• logowanie do panelu administracyjnego, • przeglądanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, • blokowanie/odblokowywanie wybranych obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, • generowanie i subskrybowanie raportów, • zarządzanie powiadomieniami, • konwersja sesji, w której pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • pobieranie haseł do serwerów (wymaga stosownego uprawnienia), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych.

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, w której pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału, • włączanie/wyłączanie powiadomień email, • zarządzanie politykami, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, • zarządzanie modyfikatorami haseł, • pobieranie haseł do serwerów (wymaga stosownego uprawnienia), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych.
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), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych, licencja, dziennik zdarzeń systemowych.

Tematy pokrewne:

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

6.9 Synchronizacja użytkowników z LDAP

Użytkownik jest jednym z podstawowych elementów *modelu danych*. Tylko zdefiniowani użytkownicy mogą nawiązywać połączenia z monitorowanymi serwerami. Fudo PAM pozwala na

automatyczną synchronizację definicji użytkowników z serwerem *Active Directory* lub innymi zgodnymi z protokołem *LDAP*.

Ostrzeżenie: Dla skutecznej konfiguracji synchronizacji opartej o protokół LDAP jest konieczne wsparcie parametru `memberOf` na serwerze LDAP. Atrybut ten służy do wskazania grup, do których należy użytkownik.

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: Opcja *Synchronizacja z LDAP* umożliwia synchronizację danych użytkownika z serwerem usług katalogowych dla danego użytkownika. Kiedy ta opcja jest zaznaczona, administrator nie może edytować danych użytkownika manualnie, tylko dodawać bądź edytować jego metody uwierzytelniania.

Jeśli opcja *Synchronizacja z LDAP* zostaje odznaczona, użytkownik już nie jest synchronizowany ze źródłem LDAP, i może być edytowany przez administratora.

Administrator może znowu zaznaczyć opcję i przywrócić synchronizację LDAP-ową, ale wszystkie zmiany, naniesione manualnie znikną przy następnej próbie synchronizacji. Tylko dodane bądź zmienione metody uwierzytelniania zostaną.

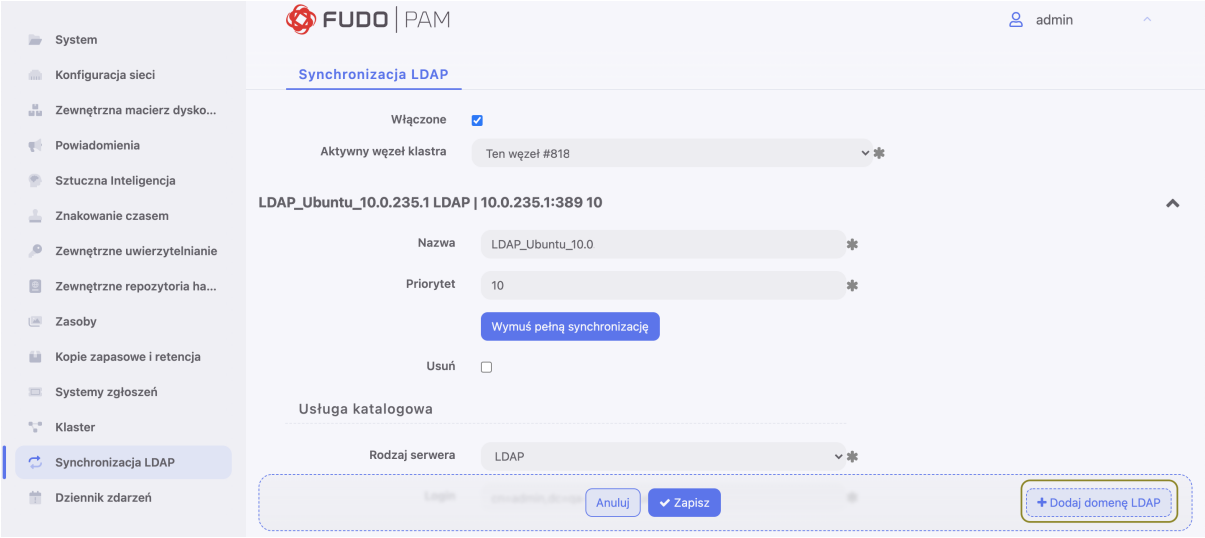
Konfiguracja usługi synchronizacji użytkowników

1. Wybierz z lewego menu *Ustawienia* > *Synchronizacja LDAP*.
2. Zaznacz opcję *Włączone*.
3. W przypadku *konfiguracji klastrowej*, z listy rozwijalnej *Aktywny węzeł klastra*, wybierz węzeł, który będzie dokonywał synchronizacji obiektów z usługą LDAP.

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.
- W przypadku analizowania problemów z komunikacją z serwerem LDAP, skorzystaj z *narzędzi diagnostycznych*.
- Fudo PAM wspiera zagnieżdżone grupy LDAP.



4. Kliknij *+ Dodaj domenę LDAP*.
5. Nadaj nazwę konfigurowanej domenie.
6. Określ priorytet, który determinuje kolejność odpytywania domen.

Informacja: Mniejsza liczba oznacza wyższy priorytet.

7. W sekcji *Usługa katalogowa*, wybierz z listy rozwijalnej *Rodzaj serwera* typ usługi katalogowej.
8. W polach *Login*, *Hasło* wprowadź dane uwierzytelniające użytkownika uprawnionego do przeglądania katalogu.
9. W polu *Domena AD/LDAP* wprowadź nazwę domeny, do której należy użytkownik uprawniony do przeglądania zawartości katalogu.
10. W polu *Domena Fudo* podaj nazwę domeny, która zostanie przypisana zsynchronizowanym użytkownikom.

Informacja:

- Pole *Domena* na formularzu użytkownika pobranego z katalogu przyjmie wartość określoną parametrem *Domena Fudo*.
- Tak zdefiniowaną domenę, użytkownik będzie musiał podać tak zdefiniowaną nazwę domeny podczas logowania do systemów monitorowanych przez Fudo.

11. Określ miejsce przechowywania użytkowników w strukturze katalogowej (np. `dc=devel, dc=whl`).

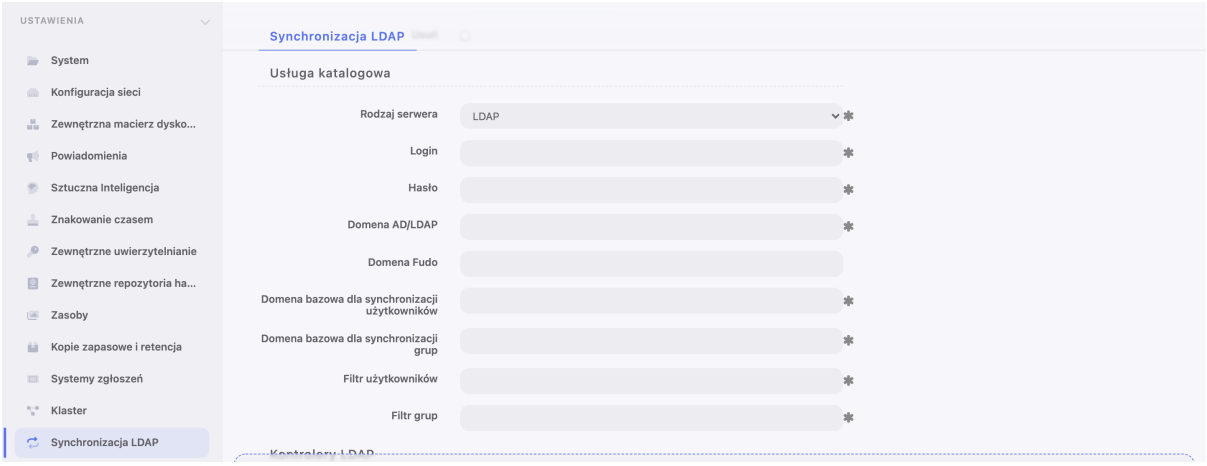
Informacja: Synchronizacja użytkowników przechowywanych w strukturze LDAP wymaga:

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

12. Określ miejsce przechowywania grup w strukturze katalogowej.

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

12. Zdefiniuj filtr dla rekordów użytkowników, których definicje mają zostać zsynchronizowane (lub pozostaw wartość domyślną).
13. Zdefiniuj filtr dla grup użytkowników, których definicje mają zostać zsynchronizowane (lub pozostaw wartość domyślną).



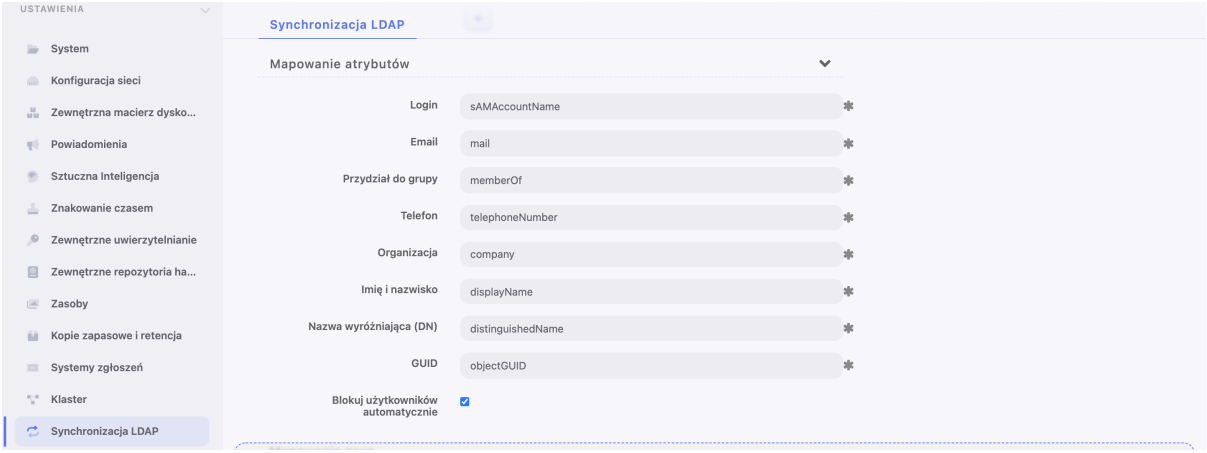
14. Zaznacz opcję *Zablokuj automatycznie*, aby Fudo automatycznie zablokowało lokalne konta użytkowników, zablokowanych w usłudze katalogowej.
15. Kliknij + w sekcji *Kontrolery LDAP*, aby zdefiniować host usługi katalogowej.
16. Wprowadź adres IP serwera oraz numer portu, na którym dostępna jest usługa katalogowa.

Informacja: W przypadku połączeń szyfrowanych, w polu adresu serwera, wprowadź jego nazwę domenową (np. `tech.ldap.com`) zamiast adresu IP, aby zapewnić poprawność weryfikacji certyfikatu serwera. Upewnij się, że nazwa domenowa jest ujęta w polu *Common Name* w certyfikacie.

17. Zaznacz ocję *Stronicuj wyniki LDAP*, aby włączyć stronicowanie danych zwracanych przez serwer LDAP.
18. Zaznacz opcję *Połączenie szyfrowane* i wgraj certyfkat CA, aby włączyć szyfrowanie transmisji z serwerem LDAP.

Informacja: Kliknij [+], aby wskazać kolejny serwer usług katalogowych.

19. Zdefiniuj mapowanie pól atrybutów 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*.

20. Kliknij [+] w sekcji *Mapowanie grup*, aby dodać mapowanie grupy użytkowników.
21. Wprowadź nazwę grupy i kliknij wybrany element na liście.
22. Określ przypisanie grup użytkowników do sejfów.
23. 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`.

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

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

24. Kliknij *Zapisz*.

Tematy pokrewne:

- *Uwierzytelnienie użytkowników w katalogu LDAP*
- *Zarządzanie użytkownikami*
- *Diagnostyka*

6.10 Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator

Google Authenticator umożliwia poprawę bezpieczeństwa kont użytkowników poprzez dodanie dynamicznego komponentu do hasła statycznego.

6.10.1 Protokoły obsługujące OATH

Podczas logowania, uwierzytelnienie przy użyciu OATH może być przeprowadzone w trybie „Challenge-Response" lub poprzez dołączenie dynamicznego kodu wygenerowanego przez Google Authenticator na końcu hasła statycznego (np: `password481418`). Uwaga: nie wszystkie protokoły wspierają tę metodę uwierzytelnienia.

Tabela 1: `Dostępność OATH`

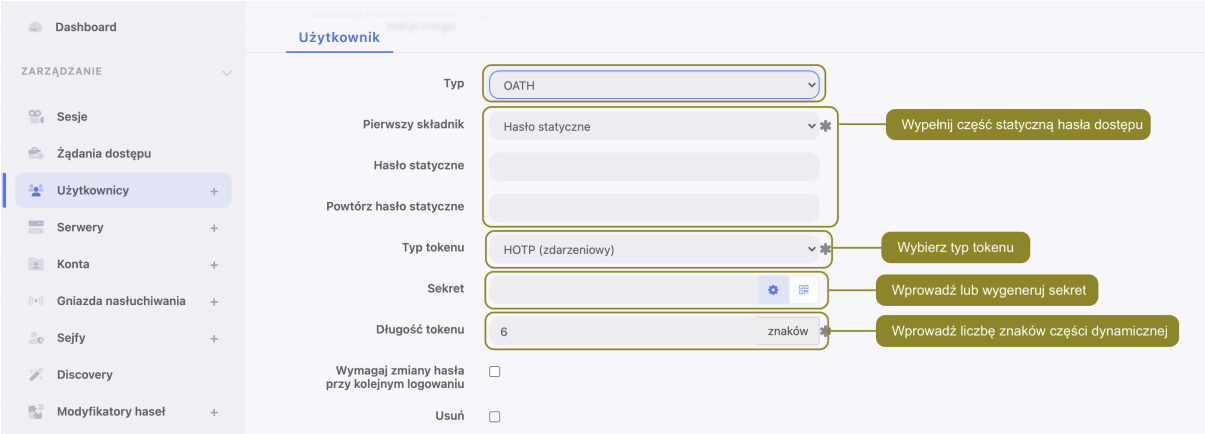
Platforma / Protokół	Tryb Challenge-Response	Hasło + Wygenerowany kod
Logowanie do Portalu Użytkownika	dostępne	dostępne
Logowanie do Panelu Administratora	dostępne	dostępne
VNC	dostępne	dostępne
SSH	dostępne	dostępne
RDP	dostępne	dostępne
Telnet 3270	nie dostępne	dostępne
Telnet 5250	nie dostępne	dostępne
Telnet	nie dostępne	dostępne
MS SQL(TDS)	nie dostępne	nie dostępne
HTTP/S	nie dostępne	nie dostępne
TCP	nie dostępne	nie dostępne
MySQL	nie dostępne	nie dostępne
X11	nie dostępne	nie dostępne
Modbus	nie dostępne	nie dostępne

6.10.2 Konfiguracja domyślnych wartości OATH

Fudo PAM pozwala zdefiniować wartości domyślne dla użytkownika, uwierzytelniającego metodą OATH.

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

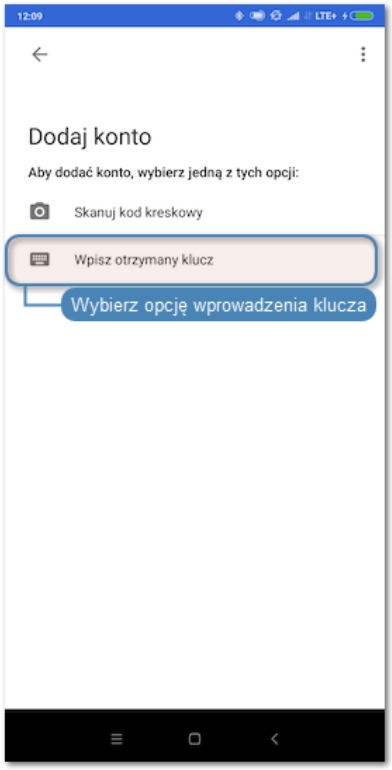
2. Odszukaj i kliknij użytkownika, dla którego chcesz włączyć dwuskładnikowe uwierzytelnienie.
3. Kliknij *+ Dodaj metodę uwierzytelnienia*.
4. Z listy rozwijalnej *Typ*, wybierz `OATH`.
5. Wprowadź część statyczną hasła.
6. Z listy rozwijalnej *Typ tokenu*, wybierz `HOTP (zdarzeniowy)`.
7. Wprowadź lub wygeneruj sekret, który będzie użyty do generowania części dynamicznej hasła przez aplikację *Google Authenticator*.
8. W polu *Długość tokenu*, wprowadź `6`.



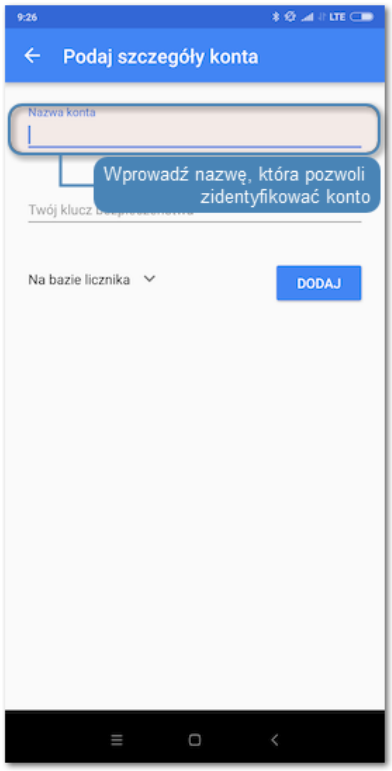
9. Kliknij *Zapisz*.
10. Uruchom aplikację *Google Authenticator* i dodaj konto ręcznie lub skanując kod QR.

Ręczne wprowadzenie danych	Kod QR

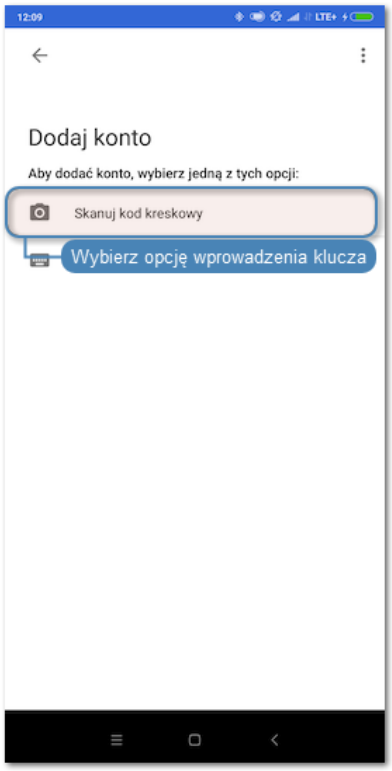
- Na ekranie dodawania konta, wybierz *Wpisz otrzymany klucz*.



- Nadaj nazwę konta.

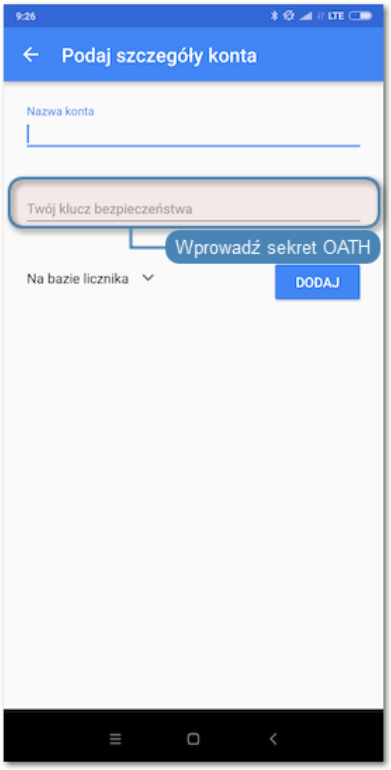


- Kliknij ikonę na formularzu konfiguracji użytkownika, w sekcji *Uwierzytelnienie*, w polu *Sekret*.
- Wybierz *Skanuj kod kreskowy* i zeskanuj wyświetlony kod QR, aby dodać konto.

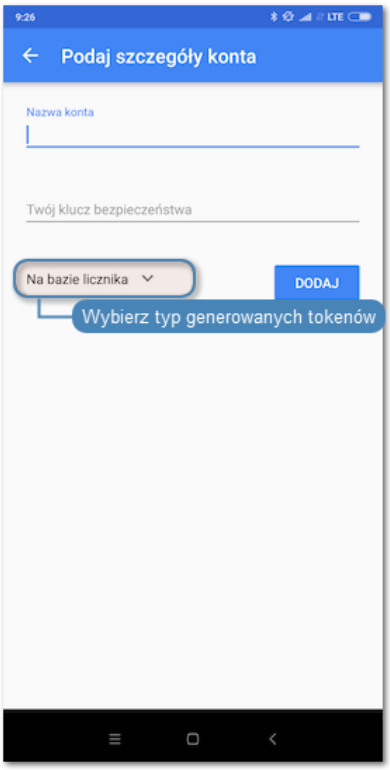


Ręczne wprowadzenie danych	Kod QR

- W polu *Twój klucz bezpieczeństwa*, wprowadź sekret z formularza konfiguracji metody uwierzytelnienia OATH.

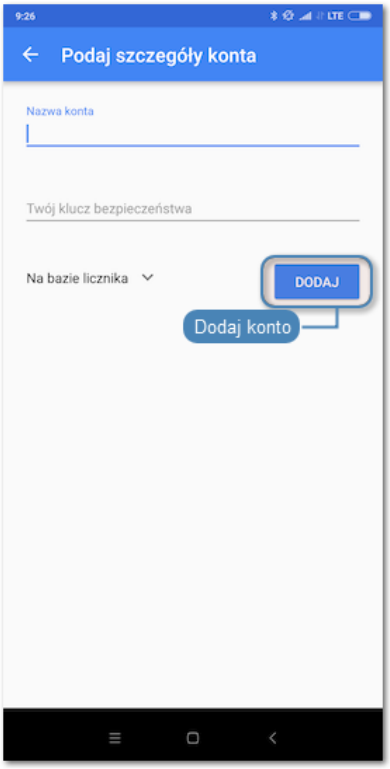


- Z listy rozwijalnej wybierz *Na bazie licznika*.

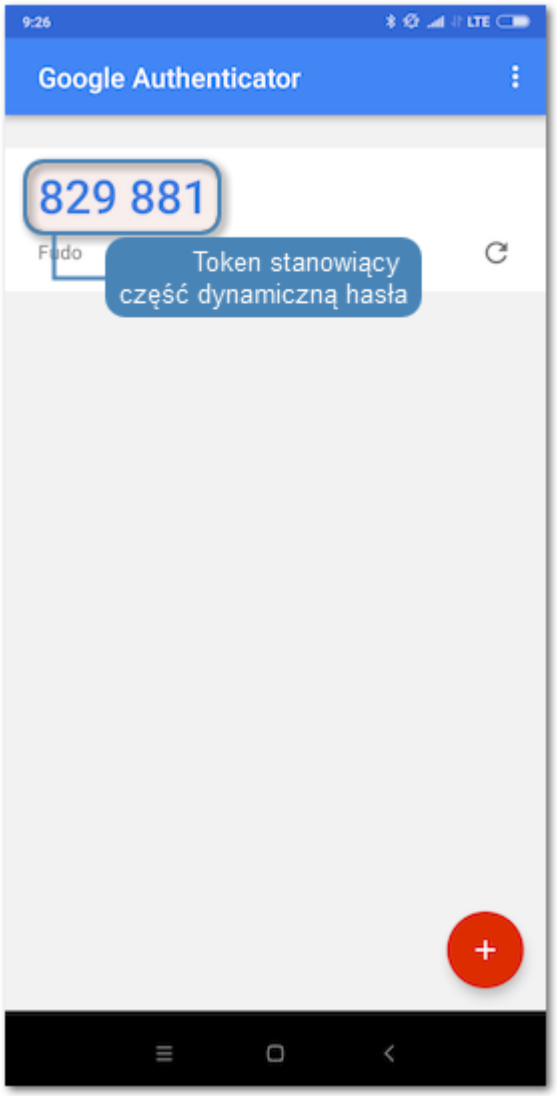


Ręczne wprowadzenie danych	Kod QR

- Wybierz DODAJ.



11. W procesie uwierzytelnienia, hasło stanowi sklejenie części statycznej z kodem wyświetlonym w aplikacji, np. `password829881`.



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*

ROZDZIAŁ 7

Serwery

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

7.1 Dodawanie 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 replikacją danych, skontaktuj się z działem wsparcia technicznego.

7.1.1 Serwery statyczne

7.1.1.1 Dodawanie serwera Citrix

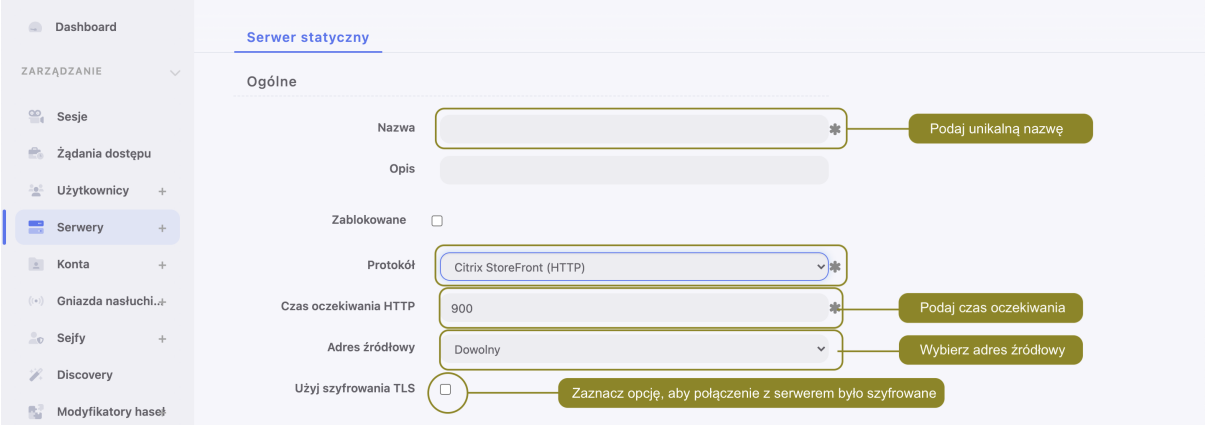
Ostrzeżenie: Wsparcie protokołu `Citrix` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.

4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `Citrix StoreFront (HTTP)`.
6. Wprowadź wartość parametru *Czas oczekiwania HTTP* - wyrażony w sekundach czas bezczynności, po upłynięciu którego, połączenie będzie wymagało ponownego uwierzytelnienia.
7. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

8. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem było szyfrowane.

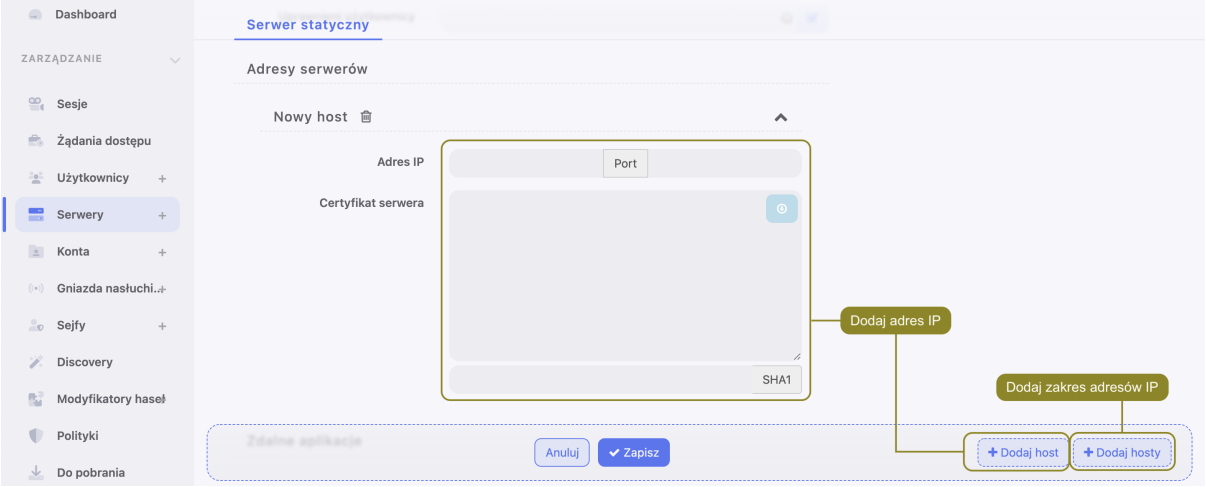
- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- Kliknij  , aby wgrać *Certyfikat CA*.

9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. Kliknij przycisk *Dodaj host* w celu dodania adresu do sekcji *Adresy serwerów*.

- Wprowadź Adres IP oraz port.
- Jeśli opcja wyżej *Użyj szyfrowania TLS* została wybrana, dodatkowo kliknij  , aby pobrać klucz serwera, lub wprowadź wartość klucza w polu *Certyfikat serwera*.

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

- W polu *URL* wprowadź bazowy URL Citrix StoreFront.



11. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.
    - Wprowadź Adres IP początkowy oraz Adres IP końcowy.
    - Podaj Port.
    - Kliknij *Dodaj hosty*.
12. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Dodawanie gniazda nasłuchiwania Citrix*
- *Citrix StoreFront*
- *Plik konfiguracyjny połączenia ICA*

7.1.1.2 Dodawanie serwera HTTP

Informacja:

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

Ostrzeżenie: Renderowanie sesji HTTP jest wymagającym procesem i może mieć negatywny wpływ na ogólną wydajność systemu. Monitorowanie rednerowanych połączeń HTTP zaleca się na maszynach fizycznych, z uwzględnieniem następujących limitów dla jednoczesnych połączeń HTTP.

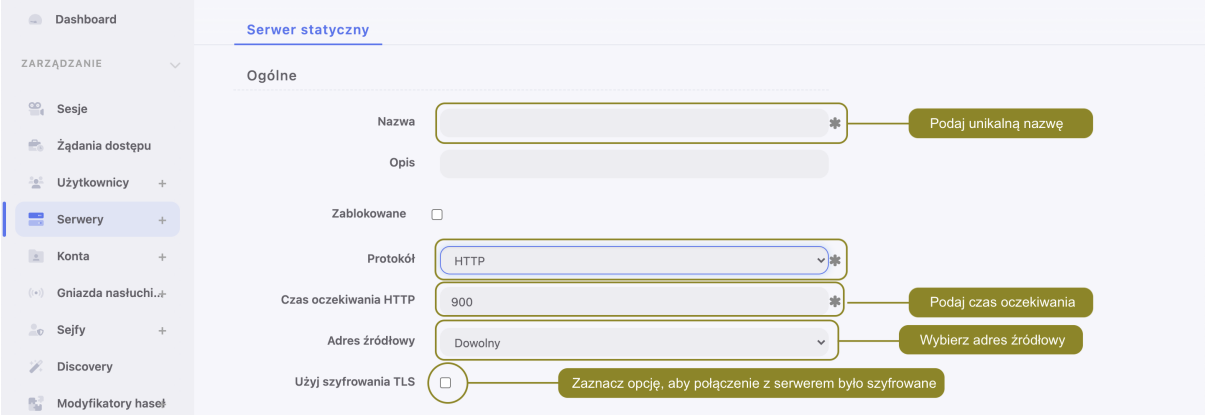
Model	Maksymalna zalecana liczba jednoczesnych połączeń HTTP*
F100x	2
F300x	5
F500x	10

* Rzeczywista maksymalna liczba obsługiwanych sesji HTTP uwarunkowana jest konfiguracją danej instacji Fudo PAM.

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `HTTP`.
6. Wprowadź wartość parametru *Czas oczekiwania HTTP* - wyrażony w sekundach czas bezczynności, po upłynięciu którego, połączenie będzie wymagało ponownego uwierzytelnienia.
7. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

8. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem było szyfrowane.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- Zaznacz opcję *Używaj zaufanych certyfikatów*.
- Kliknij , aby wgrać *Certyfikat CA*.

9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.

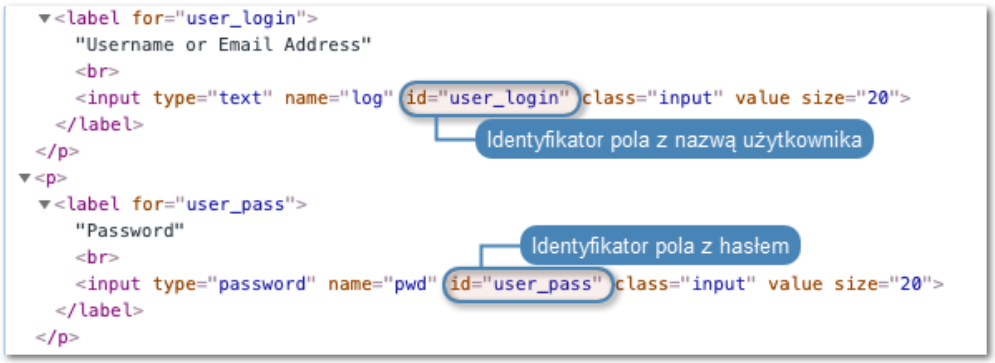
- Wprowadź Adres oraz port.
- Jeśli opcja wyżej *Użyj szyfrowania TLS* została wybrana, dodatkowo kliknij  , aby pobrać klucz serwera, lub wprowadź wartość klucza w polu *Certyfikat serwera*.

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

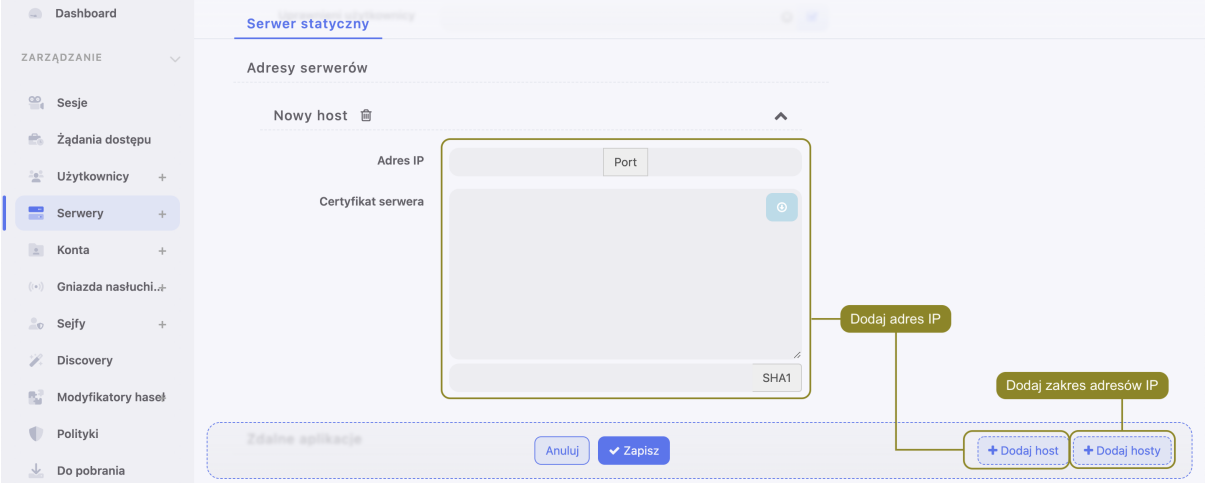
- W polu *Host HTTP*, wprowadź nagłówek HTTP. Nagłówek HTTP wskazuje zasób na serwerze, na którym hostowanych jest wiele stron internetowych.
- Z listy rozwijalnej *Metoda uwierzytelnienia*, wybierz jedną z predefiniowanych serwisów, lub wybierz opcję `Inne` i określ parametry logowania.

Informacja: Metody uwierzytelnienia umożliwiają podmianę danych logowania użytkownika podczas nawiązywania monitorowanego połączenia HTTP.

W przypadku definiowania własnych parametrów logowania, pola login i hasło identyfikowane są na podstawie selektorów CSS.



Więcej informacji na temat selektorów CSS znajdziesz na stronie https://www.w3.org/TR/selectors-3/



11. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.
    - Wprowadź Adres IP początkowy oraz Adres IP końcowy.
    - Podaj Port.
    - Kliknij *Dodaj hosty*.
12. Kliknij *Zapisz*.

Tematy pokrewne:

- *Protokoły - HTTP*
- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

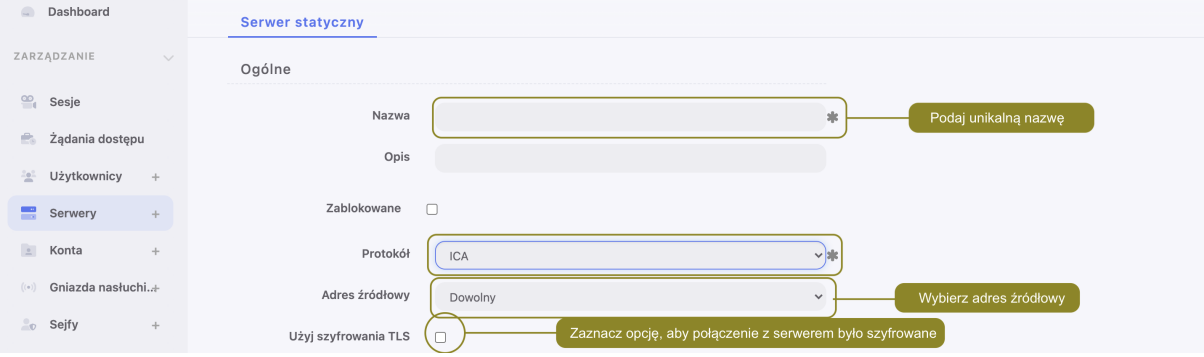
7.1.1.3 Dodawanie serwera ICA

Ostrzeżenie: Wsparcie protokołu `ICA` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `ICA`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

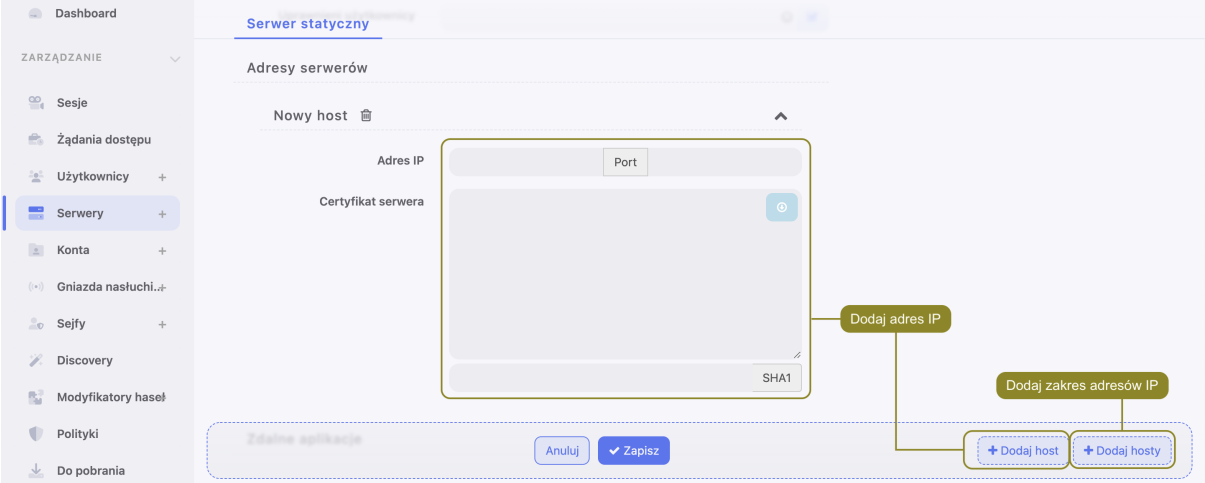
7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem było szyfrowane.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- Kliknij  , aby wgrać *Certyfikat CA*.

8. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
9. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.

- Wprowadź Adres IP oraz port.
- Jeśli opcja wyżej *Użyj szyfrowania TLS* została wybrana, dodatkowo kliknij  , aby pobrać klucz serwera, lub wprowadź wartość klucza w polu *Certyfikat serwera*.

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



10. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.
    - Wprowadź Adres IP początkowy oraz Adres IP końcowy.
    - Podaj Port.
    - Kliknij *Dodaj hosty*.
11. Kliknij *Zapisz*.

Tematy pokrewne:

- *Protokół ICA*
- *Model danych*
- *Dodawanie gniazda nasłuchiwania ICA*
- *Plik konfiguracyjny połączenia ICA*
- *Szybki start - ICA*

7.1.1.4 Dodawanie serwera Modbus

Informacja:

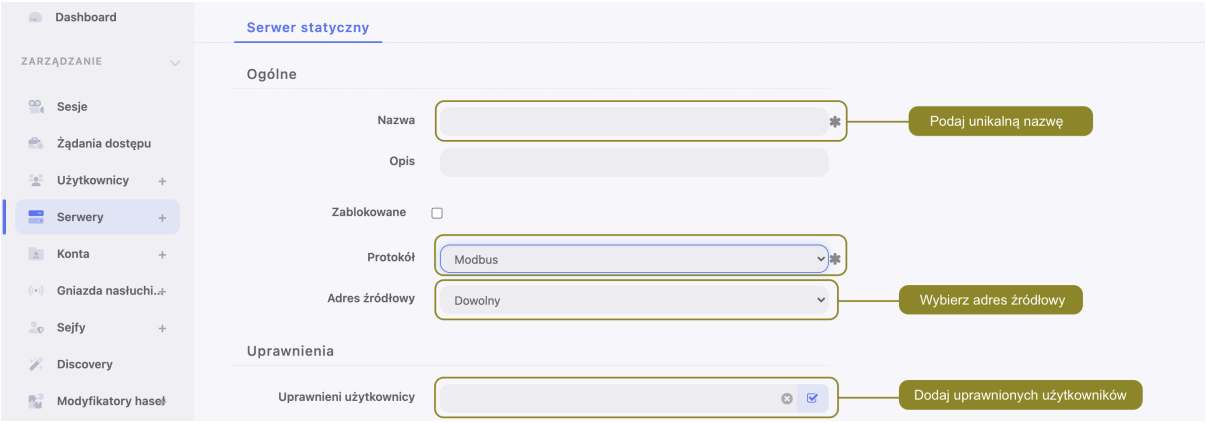
- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

---

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `Modbus`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

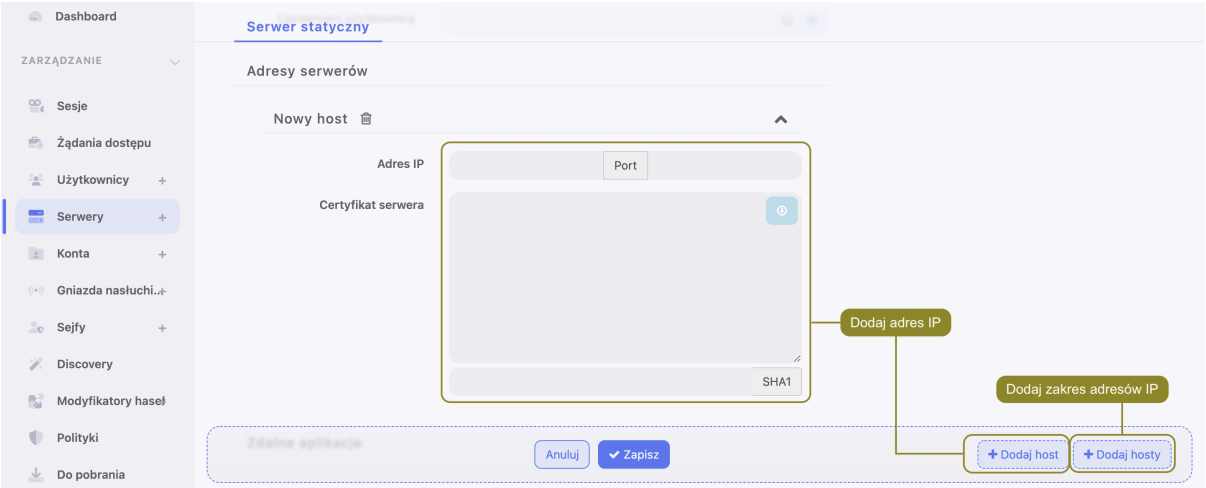
Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.

- Wprowadź Adres IP oraz port.



9. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.

- Wprowadź Adres IP początkowy oraz Adres IP końcowy.
- Podaj Port.

- Kliknij *Dodaj hosty*.

10. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

7.1.1.5 Dodawanie serwera MS SQL

Informacja:

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

---

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.

5. Z listy rozwijalnej *Protokół* wybierz `MS SQL (TDS)`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.
   - Wprowadź Adres IP oraz port.

9. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.
   - Wprowadź Adres IP początkowy oraz Adres IP końcowy.
   - Podaj Port.
   - Kliknij *Dodaj hosty*.
10. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

7.1.1.6 Dodawanie serwera MySQL

Ostrzeżenie: Domyślny plugin serwera MySQL `caching_sha2_password` nie jest obecnie wspierany przez Fudo PAM. Wspierane plugin'y dla połączeń MySQL przez Fudo PAM - to są `mysql_native_password` oraz `mysql_old_password`. Plugin Serwera powinien być ustawiony do `mysql_native_password` w `/etc/mysql/mysql.conf.d/mysqld.cnf` oraz Użytkownik stworzony z plugin'em `mysql_native_password`.

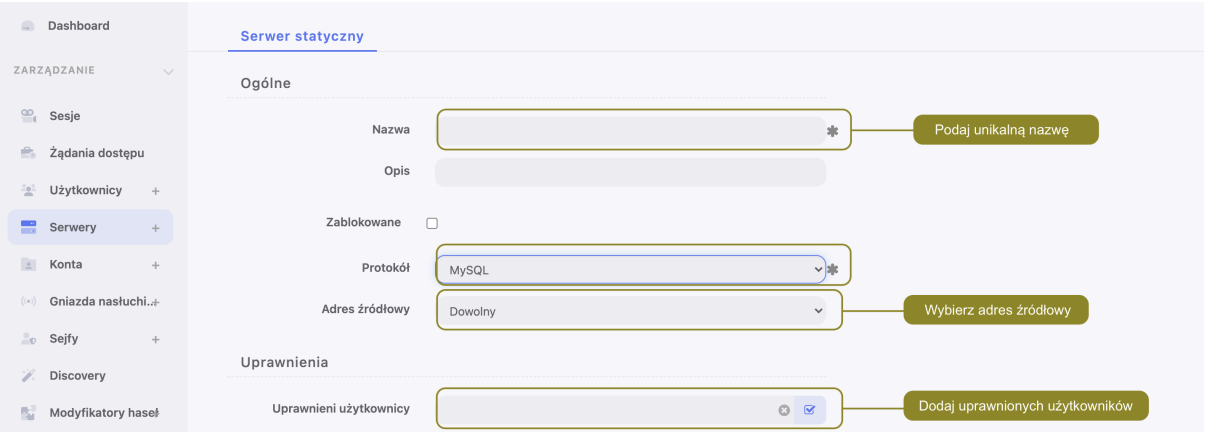
Informacja:

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

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.

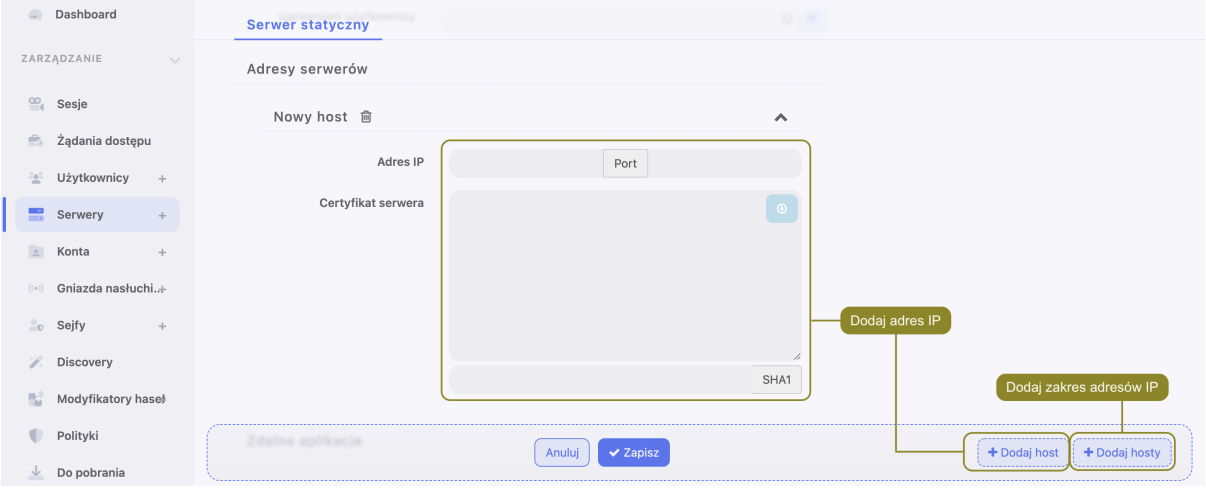


5. Z listy rozwijalnej *Protokół* wybierz `MySQL`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.
   - Wprowadź Adres IP oraz port.



9. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.
   - Wprowadź Adres IP początkowy oraz Adres IP końcowy.
   - Podaj Port.
   - Kliknij *Dodaj hosty*.
10. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

7.1.1.7 Dodawanie serwera RDP

Informacja:

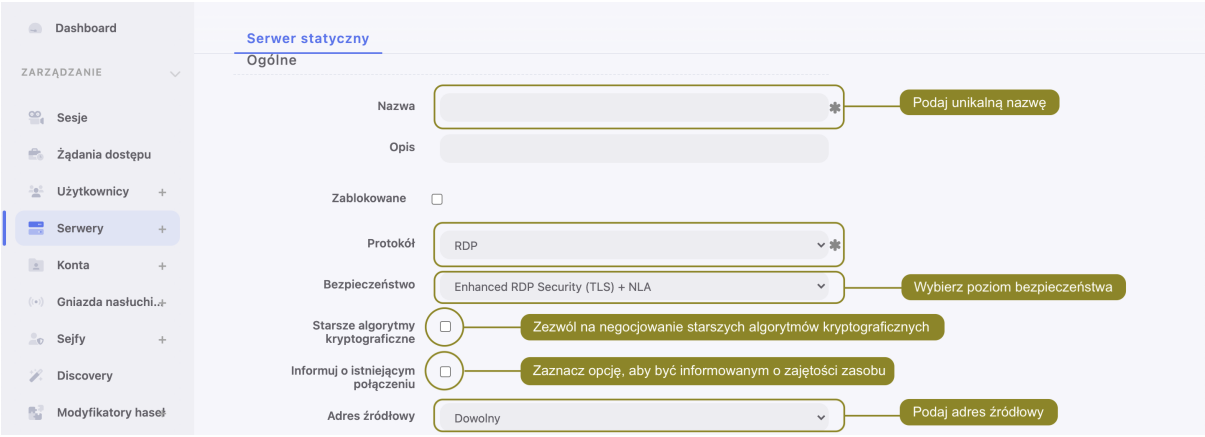
- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

---

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `RDP`.
6. Z listy rozwijalnej *Bezpieczeństwo*, wybierz tryb bezpieczeństwa protokołu RDP.

Informacja: Tryb bezpieczeństwa serwera RDP musi być zgodny z trybem bezpieczeństwa *gniazda nasłuchiwania RDP*.

W przypadku jeśli zostały wybrane opcje *Enhanced RDP Security (TLS)* albo *Enhanced RDP Security (TLS) + NLA*, zaznacz dodatkowo opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).

---

7. Zaznacz *Informuj o istniejącym połączeniu*, aby użytkownik, łączący się do serwera, był informowany o tym, że inny użytkownik jest obecnie połączony z danym serwerem. Więcej o konfiguracji **Zajętości zasobów** znajdziesz pod linkiem:
8. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

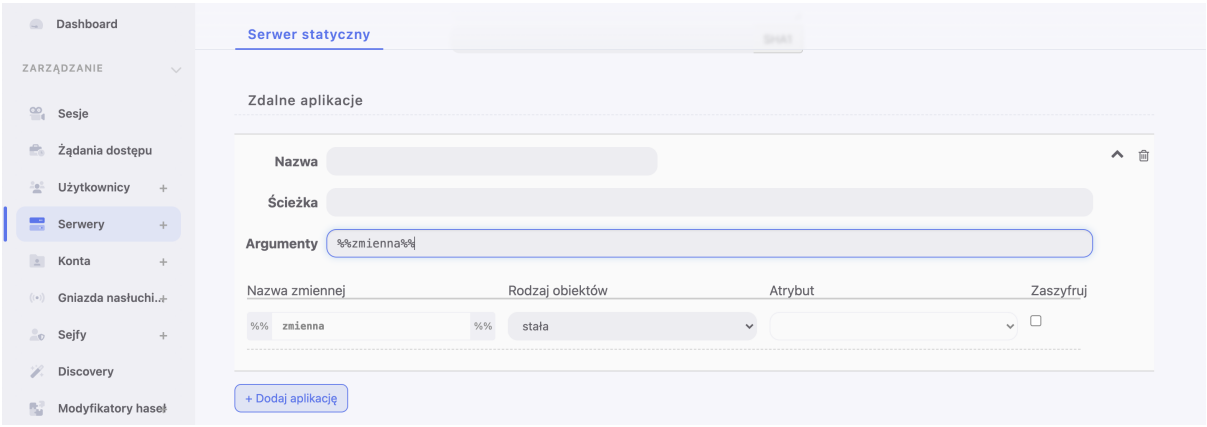
---

9. Kliknij  , aby wgrać certyfikat CA.

Informacja: Kliknij specyfikator funkcji skrótu, aby przełączyć pomiędzy wyświetlaniem skrótu

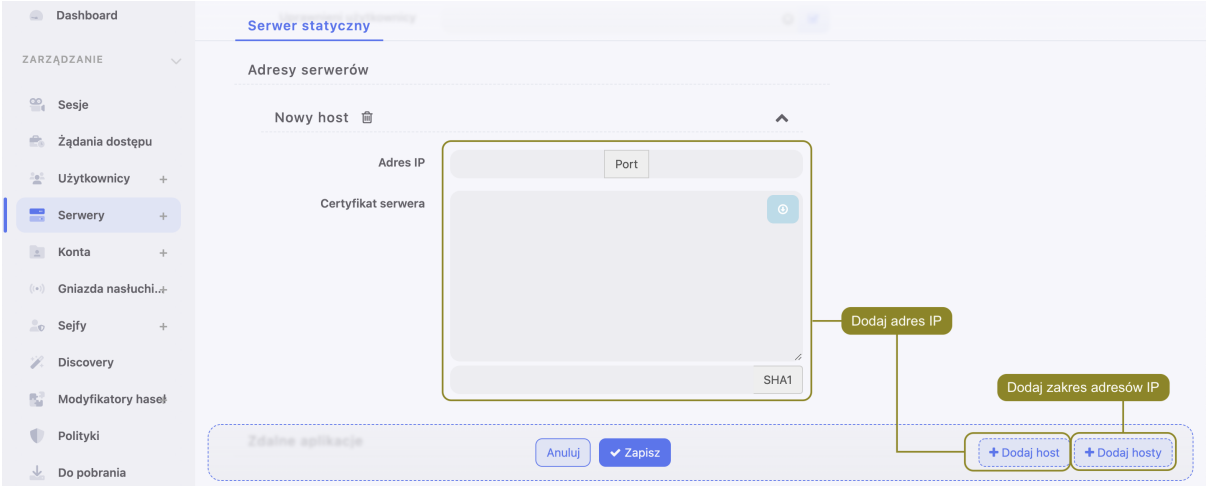
klucza wygenerowanego przez algorytm SHA1 lub MD5.

10. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
11. W sekcji *Remote applications* kliknij +Dodaj aplikację aby dodać aplikację Windows, która będzie dostępna dla użytkownika zdalnego.
    - Wprowadź *Nazwę* aplikacji, *Ścieżkę* do pliku wykonywalnego oraz nazwę *Argumentu* między dwóch znaków %%, na przykład, `%%zmienna%%`.
    - Wybierz *Rodzaj obiektów* oraz *Atrybut* dla każdego zdefiniowanego Argumentu. Można też zaszyfrować każdy argument stosując opcję *Zaszyfruj*.



12. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.
    - Wprowadź Adres IP oraz port.
    - Kliknij  , aby pobrać klucz serwera, lub wprowadź wartość klucza w polu *Certyfikat serwera*.

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



13. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.

- Wprowadź Adres IP początkowy oraz Adres IP końcowy.
- Podaj Port.
- Kliknij *Dodaj hosty*.

14. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

7.1.1.8 Dodawanie serwera SSH

Informacja:

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

---

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz `SSH`.

6. Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
7. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

8. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
9. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.
   - Wprowadź Adres IP oraz port.
   - Kliknij , aby pobrać klucz serwera, lub wprowadź wartość klucza w polu *Klucz publiczny serwera*.

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

10. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.
    - Wprowadź Adres IP początkowy oraz Adres IP końcowy.
    - Podaj Port.
    - Kliknij *Dodaj hosty*.
11. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*

- *Odblokowanie serwera*
- *Usuwanie serwera*

7.1.1.9 Dodawanie serwera Telnet

Dodawanie definicji serwera

Informacja:

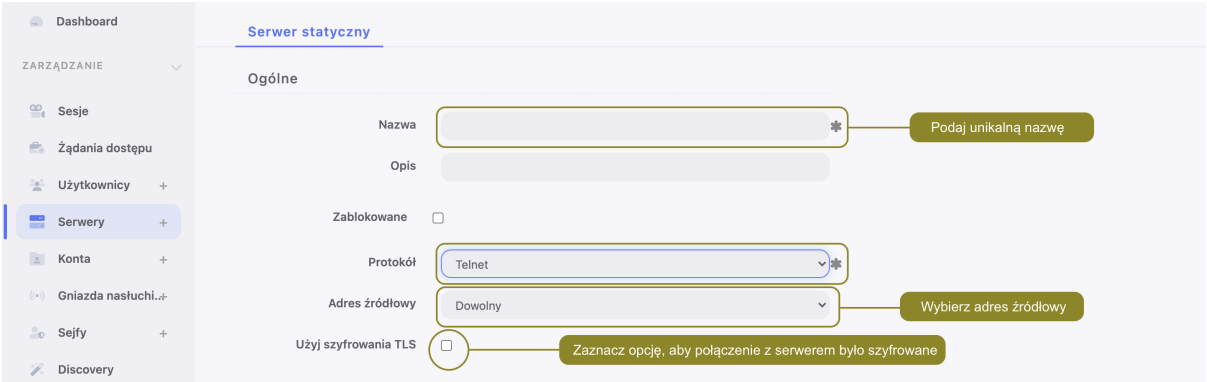
- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.
- Połączenia Telnet poprzez konto typu *forward* i *regular* wymagają dwukrotnego uwierzytelnienia. Pierwsze weryfikuje tożsamość użytkownika w lokalnej bazie Fudo PAM, drugie sprawdza dane logowanie przez serwer docelowy w celu zestawienia połączenia.

---

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `Telnet`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem było szyfrowane.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- Kliknij , aby wgrać *Certyfikat CA*.

8. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
9. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.

- Wprowadź Adres IP oraz port.
- Jeśli opcja wyżej *Użyj szyfrowania TLS* została wybrana, dodatkowo kliknij , aby pobrać klucz serwera, lub wprowadź wartość klucza w polu *Certyfikat serwera*.

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

10. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.

- Wprowadź Adres IP początkowy oraz Adres IP końcowy.
- Podaj Port.
- Kliknij *Dodaj hosty*.

11. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

7.1.1.10 Dodawanie serwera Telnet 3270

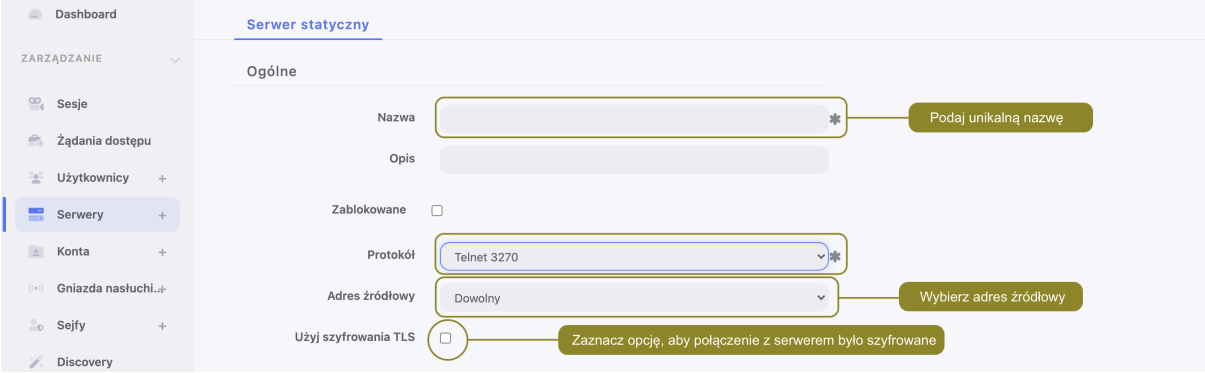
Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.
- Połączenia Telnet poprzez konto typu *forward* i *regular* wymagają dwukrotnego uwierzytelnienia. Pierwsze weryfikuje tożsamość użytkownika w lokalnej bazie Fudo PAM, drugie sprawdza dane logowanie przez serwer docelowy w celu zestawienia połączenia.

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `Telnet 3270`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem było szyfrowane.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).

- Kliknij  , aby wgrać *Certyfikat CA*.

8. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
9. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.

- Wprowadź Adres IP oraz port.
- Jeśli opcja wyżej *Użyj szyfrowania TLS* została wybrana, dodatkowo kliknij  , aby pobrać klucz serwera, lub wprowadź wartość klucza w polu *Certyfikat serwera*.

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

10. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.

- Wprowadź Adres IP początkowy oraz Adres IP końcowy.
- Podaj Port.
- Kliknij *Dodaj hosty*.

11. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

7.1.1.11 Dodawanie serwera Telnet 5250

Informacja:

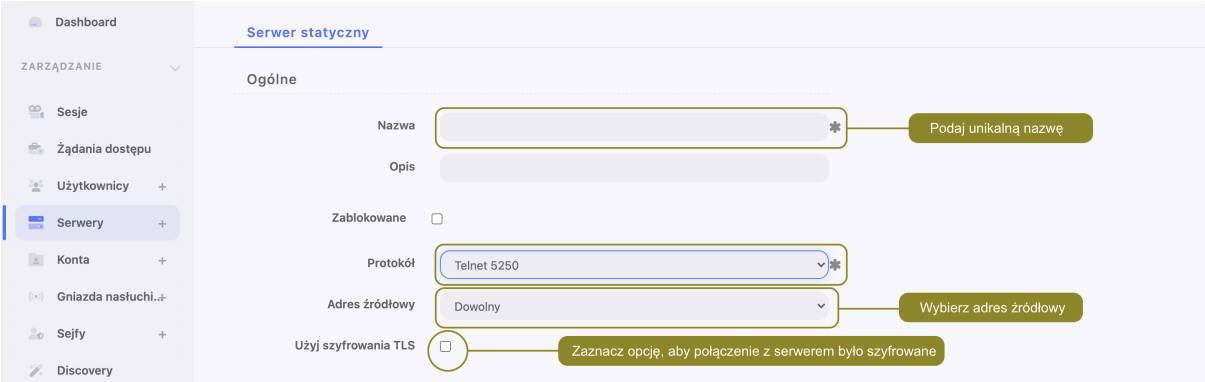
- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.
- Połączenia Telnet poprzez konto typu *forward* i *regular* wymagają dwukrotnego uwierzytelnienia. Pierwsze weryfikuje tożsamość użytkownika w lokalnej bazie Fudo PAM, drugie sprawdza dane logowanie przez serwer docelowy w celu zestawienia połączenia.

---

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `Telnet 5250`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem było szyfrowane.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- Kliknij  , aby wgrać *Certyfikat CA*.

8. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.

9. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.

- Wprowadź Adres IP oraz port.
- Jeśli opcja wyżej *Użyj szyfrowania TLS* została wybrana, dodatkowo kliknij  , aby pobrać klucz serwera, lub wprowadź wartość klucza w polu *Certyfikat serwera*.

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

10. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.

- Wprowadź Adres IP początkowy oraz Adres IP końcowy.
- Podaj Port.
- Kliknij *Dodaj hosty*.

11. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

7.1.1.12 Dodawanie serwera VNC

Informacja:

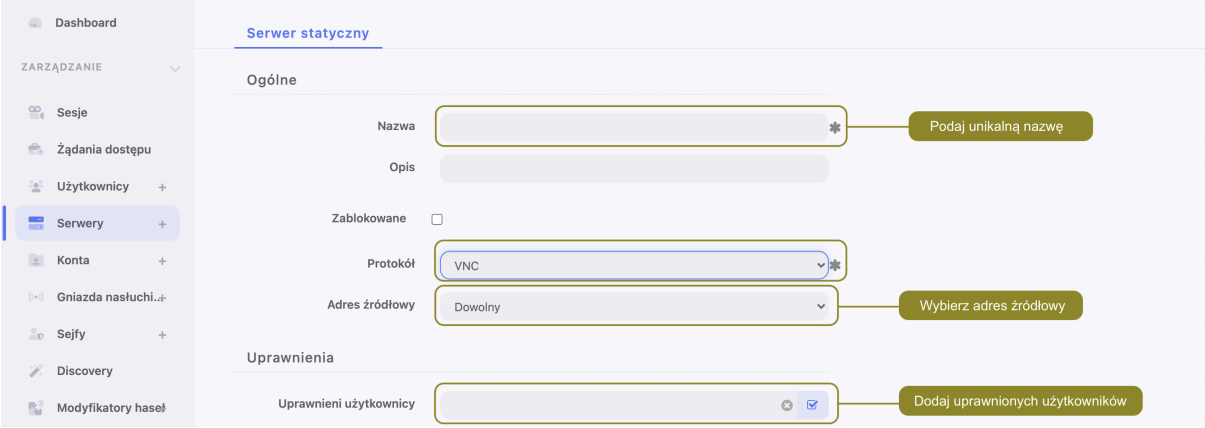
- Serwer może posiadać tylko jedno konto typu *anonymous*.
- Serwer może posiadać tylko jedno konto typu *forward*.

---

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.



5. Z listy rozwijalnej *Protokół* wybierz `VNC`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

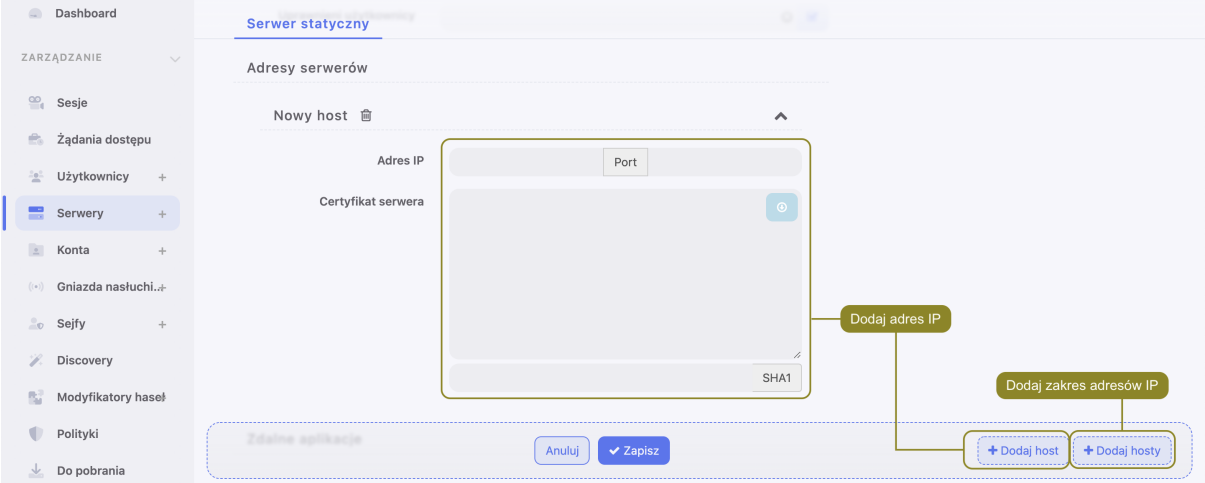
Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.

- Wprowadź Adres IP oraz port.



9. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.
   - Wprowadź Adres IP początkowy oraz Adres IP końcowy.
   - Podaj Port.
   - Kliknij *Dodaj hosty*.
10. Kliknij *Zapisz*.

Tematy pokrewne:

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

7.1.1.13 Dodawanie serwera TCP

1. Kliknij + obok zakładki *Serwery*, albo

Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*.

2. Wpisz nazwę obiektu serwera.
3. Wprowadź opcjonalnie opis, który ułatwi identyfikację zasobu infrastruktury.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.

5. Z listy rozwijalnej *Protokół* wybierz `TCP`.
6. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. Kliknij przycisk *Dodaj host* w celu dodania adresu bądź kilku adresów do sekcji *Adresy serwerów*.

- Wprowadź Adres IP oraz port.

9. Kliknij przycisk *Dodaj hosty* w celu dodania zakresu adresów IP dla serwera statycznego.

- Wprowadź Adres IP początkowy oraz Adres IP końcowy.
- Podaj Port.

- Kliknij *Dodaj hosty*.

10. Kliknij *Zapisz*.

Tematy pokrewne:

- *TCP*
- *Dodawanie gniazda nasłuchiwania TCP*
- *Model danych*

7.1.2 Serwery dynamiczne

Fudo PAM umożliwia zdefiniowanie grupy serwerów w postaci podsieci, w której znajdują się maszyny docelowe. Z chwilą gdy użytkownik dokonuje próby nawiązania połączenia z systemem znajdującym się w wybranej podsieci, Fudo PAM dokona sprawdzenia czy dany podmiot ma stosowne prawa dostępu, automatycznie doda definicję serwera w ramach istniejącego obiektu, pobierze certyfikat serwera i zestawi monitorowane połączenie.

7.1.2.1 Definiowanie grupy serwerów

Aby dodać dynamiczną grupę serwerów, postępuj zgodnie z poniższą procedurą.

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Kliknij + *Dodaj* i wybierz opcję *Serwer dynamiczny*.
3. Wpisz nazwę obiektu serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
5. Z listy rozwijalnej *Protokół* wybierz protokół serwera i skonfiguruj parametry charakterystyczne dla wybranego typu.
6. W sekcji *Host docelowy*, wprowadź adres podsieci, maskę w notacji CIDR i numer portu.
7. Z listy rozwijalnej *Adres źródłowy*, wybierz adres IP, z którego będą wysyłane pakiety do monitorowanego serwera.

Informacja: Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych*.

---

8. Uzupełnij pozostałe właściwości protokołu i kliknij *Zapisz*.

7.1.2.2 Definiowanie pojedynczego hosta w ramach grupy serwerów

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj i kliknij definicję grupy dynamicznych serwerów.

Informacja: Obiekty grupujące serwery wyróżnione są ikoną .

---

3. Kliknij przycisk + *Dodaj host*.

4. Wprowadź adres IP serwera.
5. Kliknij ikonę  , aby pobrać klucz serwera.
6. Zdefiniuj dodatkowe parametry konfiguracji.
7. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Serwery statyczne*

7.2 Modyfikowanie serwera

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

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

---

3. Kliknij nazwę obiektu.
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.
5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Dodawanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

7.3 Blokowanie serwera

Blokowanie i odblokowanie serwera

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.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z wybranymi zasobami.
4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.

Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę  .

Tematy pokrewne:

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

7.4 Odblokowanie serwera

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj*, aby przywrócić możliwość nawiązywania połączeń z serwerami.
4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektów.

Tematy pokrewne:

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

7.5 Usuwanie serwera

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

7.5.1 Usuwanie definicji serwera

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i zaznacz serwer, które chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.
4. Potwierdź operację usunięcia zaznaczonych obiektów.

7.5.2 Usuwanie wybranego hosta z grupy serwerów dynamicznych

1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i kliknij obiekt reprezentujący serwery dynamiczne.
3. W sekcji *Host docelowy* znajdź wybrany serwer i kliknij ikonę .
4. Kliknij *Zapisz*.

Tematy pokrewne:

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

ROZDZIAŁ 8

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.

8.1 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 replikacją danych, skontaktuj się z działem wsparcia technicznego.

8.1.1 Dodawanie konta typu *anonymous*

1. Kliknij + obok zakładki *Konta*, albo

   Wybierz z lewego menu *Zarządzanie* > *Konta* i kliknij + *Dodaj*.
2. W sekcji *Ogólne*, wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Typ*, wybierz `anonymous`.
5. Z listy rozwijalnej *Nagrywanie sesji*, wybierz żądaną opcję rejestrowania ruchu.

   - `wszystko` - Fudo PAM zapisuje metadane (podstawowe informacje o sesji), rejestruje surowy ruch sieciowy (plik RAW) a także zapisuje przebieg sesji w wewnętrznym formacie danych (plik FBS), umożliwiając późniejsze odtworzenie materiału w formie graficznej, w odtwarzaczu sesji oraz konwersję do wybranego formatu wideo.

- `raw` - Fudo PAM zapisuje metadane (podstawowe informacje o sesji), rejestruje surowy ruch sieciowy (plik RAW), umożliwiając późniejsze pobranie surowych danych, bez możliwości odtworzenia materiału w formie graficznej (odtwarzanie ogranicza się do wyświetlenia przebiegu wymiany pakietów sieciowych pomiędzy klientem i serwerem) ani konwersji do formatu wideo.
- `noraw` - Fudo PAM nagrywa sesję w formacie, dostępnym do odtworzenia w playerze.
- `brak` - Fudo PAM zapisuje tylko metadane (podstawowe informacje o sesji).

6. W polu *Notatki*, wprowadź treść komunikatu dla użytkowników *Portalu Użytkownika*. Jeśli uprawnienia są nadane, notatki można też edytować. Uprawnienia są nadawane z poziomu Sejfa.
7. W polu *Kategoria* wybierz `uprzywilejowany` albo `nieuprzywilejowany`. Kategoria ma charakter informacyjny.
8. W sekcji *Retencja danych*, skonfiguruj ustawienia automatycznego usuwania danych sesji.
   - Zaznacz opcję *Nadpisz globalne ustawienia retencji*, aby dla sesji nawiązanych za pośrednictwem tego konta określić *ustawienia retencji inne niż globalne*.
   - Zaznacz opcję *Usuń dane sesji*, aby wykluczyć sesje z mechanizmu retencji.
   - W polu *Usuń dane sesji*, określ liczbę dni, po których dane sesji zostaną przeniesione z lokalnego systemu plików na zewnętrzną macierz. Wartość domyślna dla zaznaczonej opcji to 30 dni.
9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Serwer*, z listy rozwijalnej *Serwer*, wybierz host docelowy, z którym skojarzone będzie definiowane konto.
11. Dla serwerów SSH oraz RDP, wybierz opcję *SSH Agent forwarding* w celu uwierzytelnienia na serwerze docelowym wykorzystując klucz SSH klienta.

Informacja: Ta opcja jest dostępna tylko przy wyborze serwera SSH. Zastosuj opcję -A w celu połączenia z serwerem SSH.

---

12. Kliknij *Zapisz*.

Tematy pokrewne:

- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowanie konta*
- *Usuwanie konta*

8.1.2 Dodawanie konta typu *forward*

1. Kliknij + obok zakładki *Konta*, albo

   Wybierz z lewego menu *Zarządzanie* > *Konta* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Typ*, wybierz `forward`.
5. Z listy rozwijalnej *Nagrywanie sesji*, wybierz żądaną opcję rejestrowania ruchu.
    - `wszystko` - Fudo PAM zapisuje metadane (podstawowe informacje o sesji), rejestruje surowy ruch sieciowy (plik RAW) a także zapisuje przebieg sesji w wewnętrznym formacie danych (plik FBS), umożliwiając późniejsze odtworzenie materiału w formie graficznej, w odtwarzaczu sesji oraz konwersję do wybranego formatu wideo.
    - `raw` - Fudo PAM zapisuje metadane (podstawowe informacje o sesji), rejestruje surowy ruch sieciowy (plik RAW), umożliwiając późniejsze pobranie surowych danych, bez możliwości odtworzenia materiału w formie graficznej (odtwarzanie ogranicza się do wyświetlenia przebiegu wymiany pakietów sieciowych pomiędzy klientem i serwerem) ani konwersji do formatu wideo.
    - `noraw` - Fudo PAM nagrywa sesję w formacie, dostępnym do odtworzenia w playerze.
    - `brak` - Fudo PAM zapisuje tylko metadane (podstawowe informacje o sesji).
6. W polu *Notatki*, wprowadź treść komunikatu dla użytkowników *Portalu Użytkownika*. Jeśli uprawnienia są nadane, notatki można też edytować. Uprawnienia są nadawane z poziomu Sejfa.
7. W polu *Kategoria* wybierz `uprzywilejowany` albo `nieuprzywilejowany`. Kategoria ma charakter informacyjny.
8. W sekcji *Retencja danych*, skonfiguruj ustawienia automatycznego usuwania danych sesji.
    - Zaznacz opcję *Nadpisz globalne ustawienia retencji*, aby dla sesji nawiązanych za pośrednictwem tego konta określić *ustawienia retencji inne niż globalne*.
    - Zaznacz opcję *Usuń dane sesji*, aby wykluczyć sesje z mechanizmu retencji.
    - W polu *Usuń dane sesji*, określ liczbę dni, po których dane sesji zostaną przeniesione z lokalnego systemu plików na zewnętrzną macierz. Wartość domyślna dla zaznaczonej opcji to 30 dni.
9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Serwer*, z listy rozwijalnej *Serwer*, wybierz host docelowy, z którym skojarzone będzie definiowane konto.
11. W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastąp sekret*, wybierz żądaną opcję.

`sekretem z innego konta`

- Z listy rozwijalnej *Konto* wybierz obiekt, z którego pobrane zostanie hasło w celu uwierzytelnienia użytkownika podczas zestawiania połączenia.

Informacja: Lista zawiera obiekty, do których zalogowany użytkownik ma stosowne prawa dostępu.

`kluczem`

- Kliknij ikonę  i wybierz typ klucza SSH.
- Kliknij ikonę  i wskaż plik z kluczem do wgrania.

`hasłem`

- W polu *Hasło*, wprowadź hasło, na które podmieniony zostanie ciąg wprowadzony przez użytkownika.
- W polu *Powtórz hasło*, wprowadź ponownie hasło, na które podmieniony zostanie ciąg wprowadzony przez użytkownika.

Informacja: *Podwójne uwierzytelnienie*

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

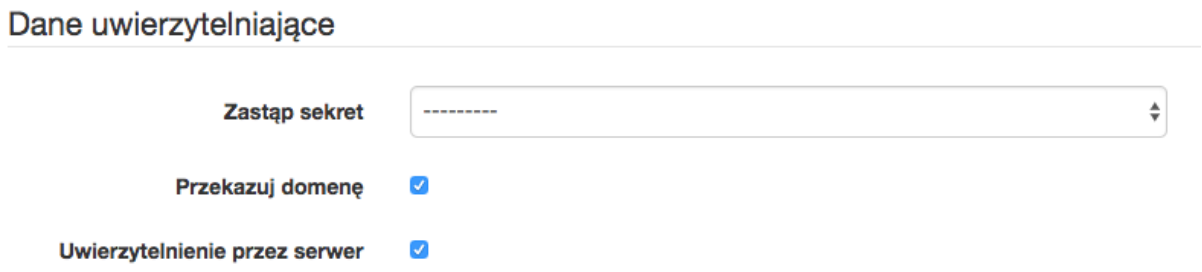
Aby aktywować funkcję podwójnego uwierzytelnienia, z listy rozwijalnej *Zastąp sekret* wybierz opcję `hasłem` i nie wypełniaj pól definiujących hasło oraz login.

`hasłem z zewnętrznego repozytorium`

- Z listy rozwijalnej, wybierz zewnętrzne repozytorium haseł, z którego pobrane zostanie hasło podczas zestawiania połączenia.

Informacja: *Uwierzytelnienie przez serwer*

W trybie uwierzytelnienia przez serwer, Fudo nie weryfikuje poprawności danych logowania, tylko przekazuje je do serwera docelowego, który przeprowadza proces uwierzytelnienia. Aby włączyć uwierzytelnienie przez serwer, zaznacz opcję *Uwierzytelnienie przez serwer* w sekcji *Dane uwierzytelniające* (dostępne tylko dla serwerów SSH oraz RDP w trybie bezpieczeństwa *Enhanced RDP Security (TLS) + NLA*.



W przypadku połączenia użytkownika, który uwierzytelnia się jedną z metod dwuskładnikowych, jak na przykład OATH+AD, Fudo nie poprosi o przekazanie części dynamicznej – w tym wypadku tokena OATH – tak jak zwykle robi to podczas łączenia się z serwerem (niebieski ekran po połączeniu z Fudo, a przed połączeniem z serwerem). To ograniczenie dotyczy tylko konta typu „forward".

---

12. Zaznacz opcję *Przekazuj domenę*, aby nazwa domeny była przekazywana razem z ciągiem identyfikującym użytkownika.

13. Dla serwerów SSH, zaznacz opcję *SSH Agent forwarding*, aby uwierzytelnić użytkownika przed serwerem z użyciem klucza klienta.

Informacja: Opcja *SSH Agent forwarding* dostępna jest w przypadku wybrania serwera SSH. Zastosuj opcję -A w celu połączenia z serwerem SSH.

---

14. Kliknij *Zapisz*.

Tematy pokrewne:

- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowanie konta*
- *Usuwanie konta*

8.1.3 Dodawanie konta typu *regular*

1. Kliknij *+* obok zakładki *Konta*, albo

   Wybierz z lewego menu *Zarządzanie* > *Konta* i kliknij *+ Dodaj*.

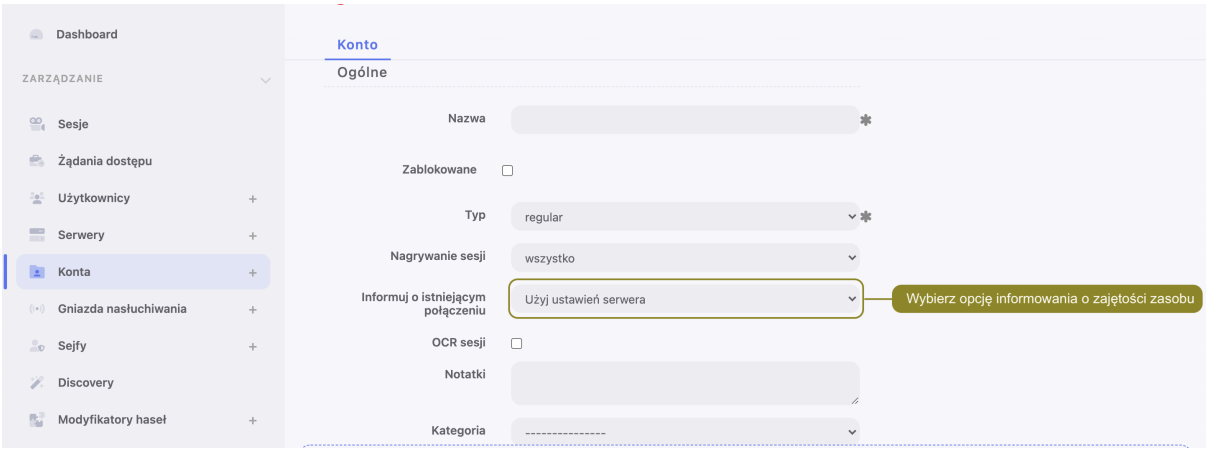
2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Typ*, wybierz `regular`.
5. Z listy rozwijalnej *Nagrywanie sesji*, wybierz żądaną opcję rejestrowania ruchu.

   - `wszystko` - Fudo PAM zapisuje metadane (podstawowe informacje o sesji), rejestruje surowy ruch sieciowy (plik RAW) a także zapisuje przebieg sesji w wewnętrznym formacie danych (plik FBS), umożliwiając późniejsze odtworzenie materiału w formie graficznej, w odtwarzaczu sesji oraz konwersję do wybranego formatu wideo.
   - `raw` - Fudo PAM zapisuje metadane (podstawowe informacje o sesji), rejestruje surowy ruch sieciowy (plik RAW), umożliwiając późniejsze pobranie surowych danych, bez możliwości odtworzenia materiału w formie graficznej (odtwarzanie ogranicza się do wyświetlenia przebiegu wymiany pakietów sieciowych pomiędzy klientem i serwerem) ani konwersji do formatu wideo.
   - `noraw` - Fudo PAM nagrywa sesję w formacie, dostępnym do odtworzenia w playerze.
   - `brak` - Fudo PAM zapisuje tylko metadane (podstawowe informacje o sesji).

6. W polu *Notatki*, wprowadź treść komunikatu dla użytkowników *Portalu Użytkownika*. Jeśli uprawnienia są nadane, notatki można też edytować.
7. W polu *Kategoria* wybierz `uprzywilejowany` albo `nieuprzywilejowany`. Kategoria ma charakter informacyjny.
8. W sekcji *Retencja danych*, skonfiguruj ustawienia automatycznego usuwania danych sesji.

- Zaznacz opcję *Nadpisz globalne ustawienia retencji*, aby dla sesji nawiązanych za pośrednictwem tego konta określić *ustawienia retencji inne niż globalne*.
- Zaznacz opcję *Usuń dane sesji*, aby wykluczyć sesje z mechanizmu retencji.
- W polu *Usuń dane sesji*, określ liczbę dni, po których dane sesji zostaną przeniesione z lokalnego systemu plików na zewnętrzną macierz. Wartość domyślna dla zaznaczonej opcji to 30 dni.

9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Serwer*, z listy rozwijalnej *Serwer*, wybierz host docelowy, z którym skojarzone będzie definiowane konto.
11. W przypadku wybrania serwera RDP, pojawi się dodatkowa opcja, pozwalająca być informowanym, kiedy inny użytkownik będzie już połączony z wybranym serwerem. W celu zmiany / wyłączenia / potwierdzenia tej funkcjonalności, wybierz jedną z wartości w polu *Informuj o istniejącym połączeniu*: `Użyj ustawienia serwera`, `nie`, albo `tak`.



12. W sekcji *Dane uwierzytelniające*, w polu *Domena*, wprowadź domenę konta użytkownika uprzywilejowanego, na serwerze docelowym.
13. W polu *Login*, wprowadź login użytkownika uprzywilejowanego na serwerze docelowym.
14. Z listy rozwijalnej *Zastąp sekret*, wybierz żądaną opcję.

`sekretem z innego konta`

- Z listy rozwijalnej *Konto* wybierz obiekt, z którego pobrane zostanie hasło w celu uwierzytelnienia użytkownika podczas zestawiania połączenia.

`kluczem`

- Kliknij ikonę  i wybierz typ klucza SSH.
- Kliknij ikonę  i wskaż plik z kluczem prywatnym, niezabezpieczony frazą szyfrującą.

`hasłem`

- W polu *Hasło*, wprowadź hasło, na które podmieniony zostanie ciąg wprowadzony przez użytkownika.

- W polu *Powtórz hasło*, wprowadź ponownie hasło, na które podmieniony zostanie ciąg wprowadzony przez użytkownika.

Informacja: *Podwójne uwierzytelnienie*

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

Aby aktywować funkcję podwójnego uwierzytelnienia, z listy rozwijalnej *Zastąp sekret* wybierz opcję `hasłem` i nie wypełniaj pól definiujących hasło oraz login.

`hasłem z zewnętrzengo repozytorium`

- Z listy rozwijalnej, wybierz zewnętrzne repozytorium haseł, z którego pobrane zostanie hasło podczas zestawiania połączenia.

15. W polu *Limit czasu rezerwacji hasła* określ limit czasu, po którym hasło zostanie automatycznie zdane.

Informacja: Zdefniowanie limitu czasu rezerwacji hasła powoduje włączenie dla wybranego konta funkcji rezerwacji na wyłączność.

---

16. Zaznacz opcję *Zmień hasło po ostatnim zdaniu hasła*, aby hasło zostało automatycznie zmienione po tym jak zda je ostatni użytkownik.

Informacja: Opcja automatycznej zmiany hasła jest dostępna po podaniu limitu czasu rezerwacji hasła.

---

17. Zaznacz opcję *Zmień hasło po zakończeniu sesji*, aby hasło zostało automatycznie zmienione po tym jak sesja zostanie zakończona.

Informacja: Z listy rozwijalnej Polityka modyfikatora haseł, wybierz odpowiednią. Uwaga: nie może być wybrana polityka *Statyczne, bez ograniczeń.*

Przejdź do tematu *polityki modyfikatora haseł* w celu uzyskania więcej informacji o definiowaniu modyfikatora haseł.

Wybierz co najmniej jeden Modyfikator hasła.

---

18. Zaznacz opcję SSH Agent forwarding, aby uwierzytelnić użytkownika przed serwerem z użyciem klucza klienta.

Informacja: Opcja SSH Agent forwarding dostępna jest w przypadku wybrania serwera SSH. Zastosuj opcję -A w celu połączenia z serwerem SSH.

---

19. Zaznacz opcję *Odzyskiwanie hasła*, aby włączyć uruchomienie Modyfikatora Hasła w sytuacji, gdy Weryfikator Hasła wykryje zmianę hasła, które nie zostało zapisane w systemie

Fudo PAM.

Informacja: Kiedy ta opcja jest włączona, Weryfikator Hasła uruchamia Modyfikator Hasła. Kiedy jest wyłączona, Weryfikator Hasła wysyła komunikat: „Nie udało się zweryfikować hasła dla konta <nazwa_konta>”.

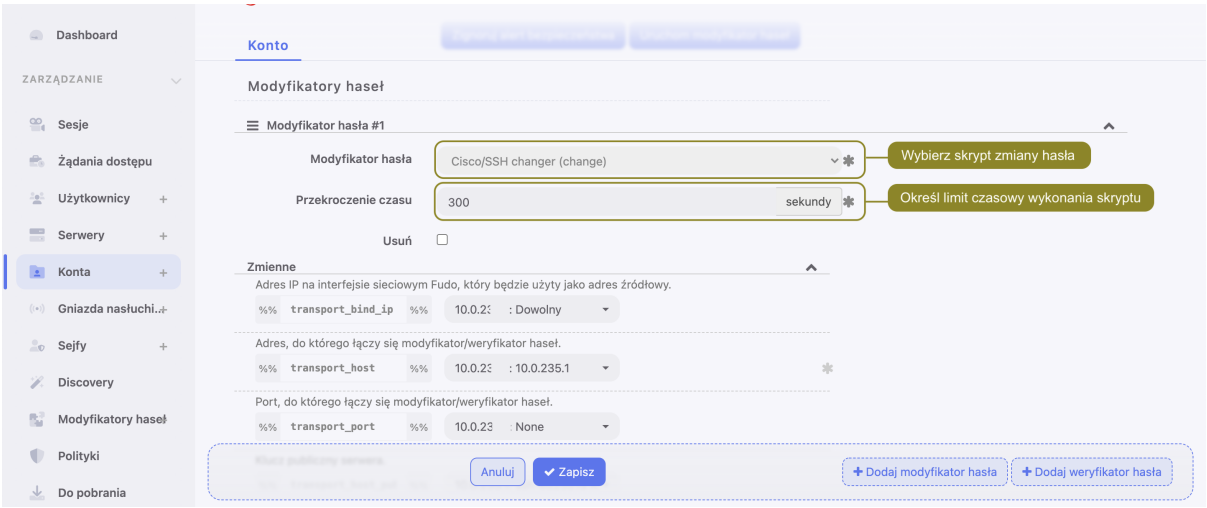
---

20. Kliknij *+ Dodaj modyfikator hasła*, aby hasło do konta było zmieniane automatycznie, zgodnie z *polityką modyfikatora haseł*.

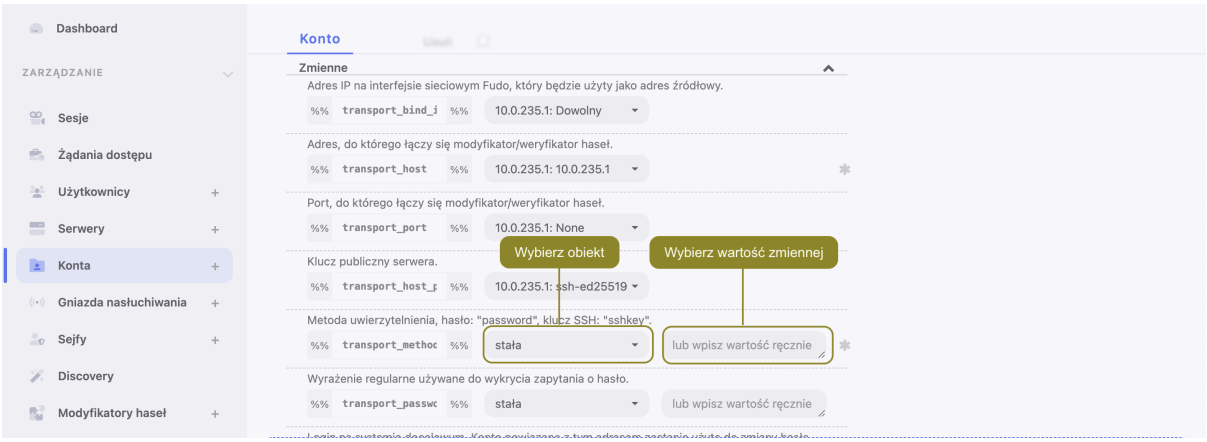
Informacja: Opcja dodania modyfikatora dostępna jest po wybraniu opcji zastąpienia sekretu hasłem.

---

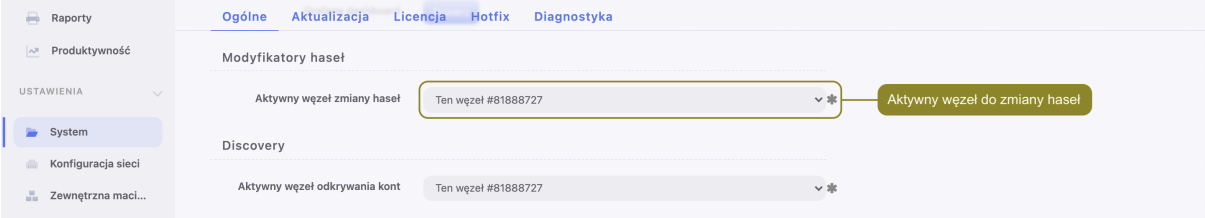
21. Z listy rozwijalnej *Modyfikator hasła*, wybierz właściwy dla hosta docelowego sposób zmiany haseł i uzupełnij parametry konfiguracyjne.
22. W polu *Przekroczenie czasu* określ limit czasowy wykonania skryptu.



23. W sekcji *Zmienne*, sparametryzuj zmienne skryptu.

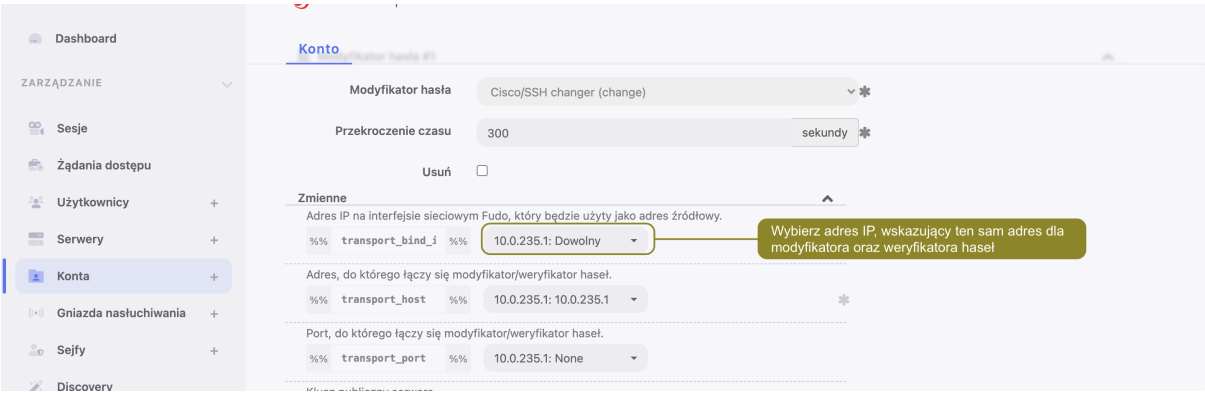


Fudo PAM umożliwia zmianę hasła na innym węźle klastra, niż ten, który jest wskazany jako aktywny węzeł klastra dla Modyfikatorów haseł.



W celu konfiguracji powyższego scenariusza, następujący warunek powinien zostać spełniony:

Definiując Modyfikator / Weryfikator hasła dla konta, wartość zmiennej `transport_bind_ip` powinna wskazywać ten sam węzeł dla wszystkich Modyfikatorów oraz Weryfikatorów hasła.



Jeśli wartości zmiennej `transport_bind_ip` będą wskazywać różne węzły klastra, Modyfikator / Weryfikator hasła będą działać na węźle, wskazanym jako *aktywny węzeł klastra dla Modyfikatorów haseł*.

Więcej informacji na temat pracy węzłów klastra w ramach zmiany haseł znajdziesz pod linkiem: *Modyfikatory haseł - aktywny węzeł klastra*

Tematy pokrewne:

- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowanie konta*
- *Usuwanie konta*

8.2 Edytowanie 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.
5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie konta*
- *Edytowanie konta*
- *Odblokowanie konta*
- *Usuwanie konta*

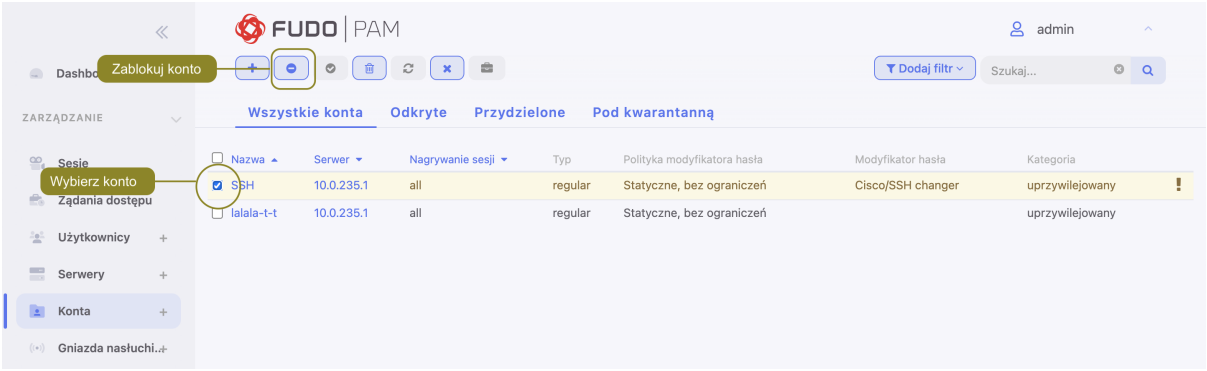
8.3 Blokowanie konta

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.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Blokuj*, aby zablokować możliwość nawiązywania połączeń z serwerem za pośrednictwem z wybranego konta.



4. Opcjonalnie wprowadź powód zablokowania zasobu i kliknij *Zatwierdź*.

Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Tematy pokrewne:

- *Odblokowanie konta*
- *Dodawanie konta*
- *Edytowanie konta*

- *Usuwanie konta*

8.4 Odblokowanie konta

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj*, aby umożliwić nawiązywanie połączeń za pośrednictwem wybranego konta.
4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektu.

Tematy pokrewne:

- *Blokowanie konta*
- *Dodawanie konta*
- *Edytowanie konta*
- *Usuwanie konta*

8.5 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.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.

4. Potwierdź operację usunięcia zaznaczonych obiektów.

Tematy pokrewne:

- *Dodawanie konta*
- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowanie konta*

8.6 Zarządzanie ostrzeżeniami bezpieczeństwa

Fudo PAM śledzi akcje użytkowników *portalu* i rejestruje każdą próbę podglądu hasła do monitorowanego konta uprzywilejowanego. Zablokowanie użytkownika, który poznał aktualne hasło do konta, stanowi potencjalne zagrożenie bezpieczeństwa. Fudo PAM identyfikuje takie zdarzenia i komunikuje administratorom systemu.

Administrator może zignorować alarm dla wybranego konta lub wymusić zmianę hasła za pomocą przypisanego *modyfikatora haseł*.

8.6.1 Zmiana hasła konta

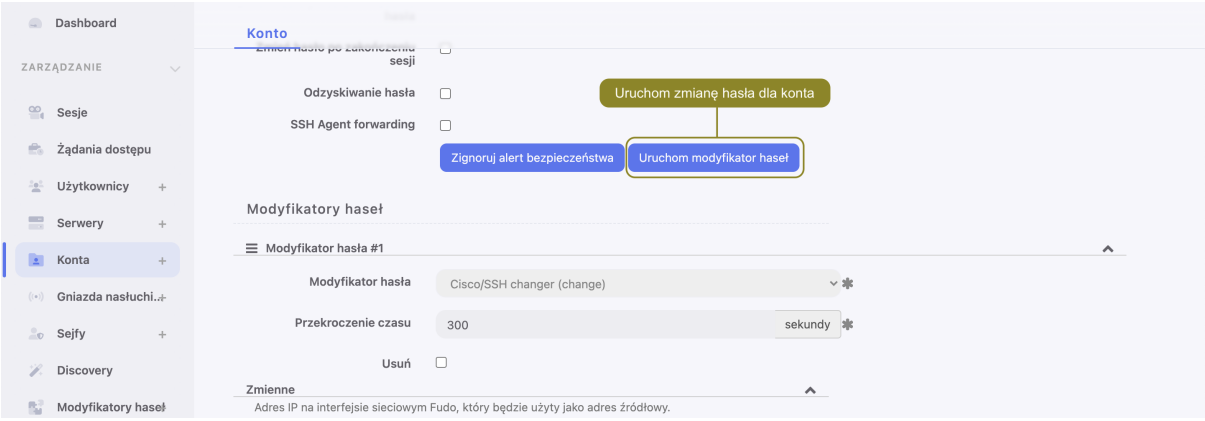
Zmiana hasła z poziomu listy kont

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz konta, dla których chcesz zmienić hasło.
3. Kliknij *Zmień hasło*.

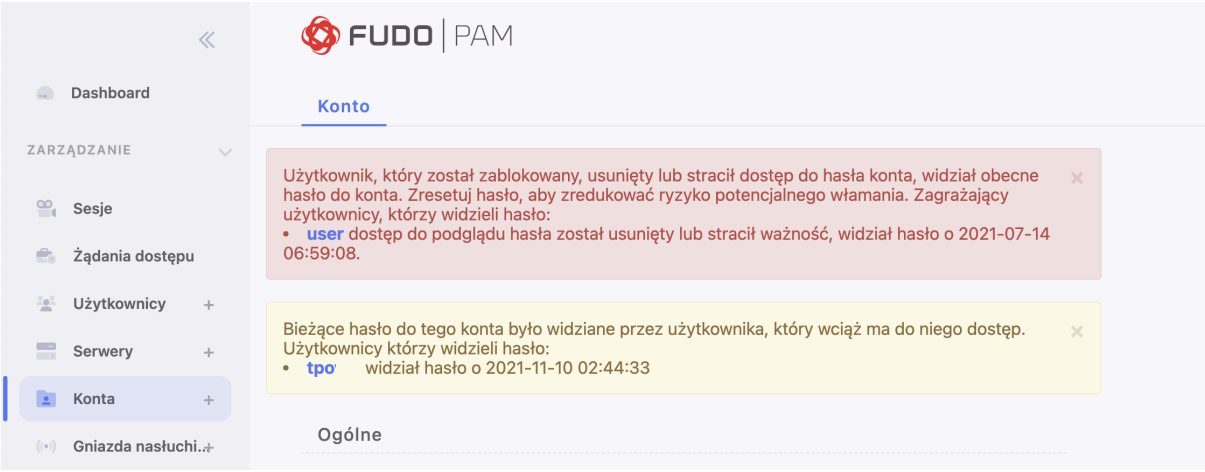
4. Kliknij *Zatwierdź*.

Zmiana hasła z poziomu formularza edycji konta

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i kliknij wybrane konto, aby otworzyć formularz edycji.
3. W sekcji *Dane uwierzytelniające*, kliknij *Uruchom modyfikator haseł*.



Informacja: Formularz edycji konta zawiera listę zablokowanych użytkowników, którzy widzieli aktualne hasło.



8.6.2 Zignorowanie ostrzeżenia

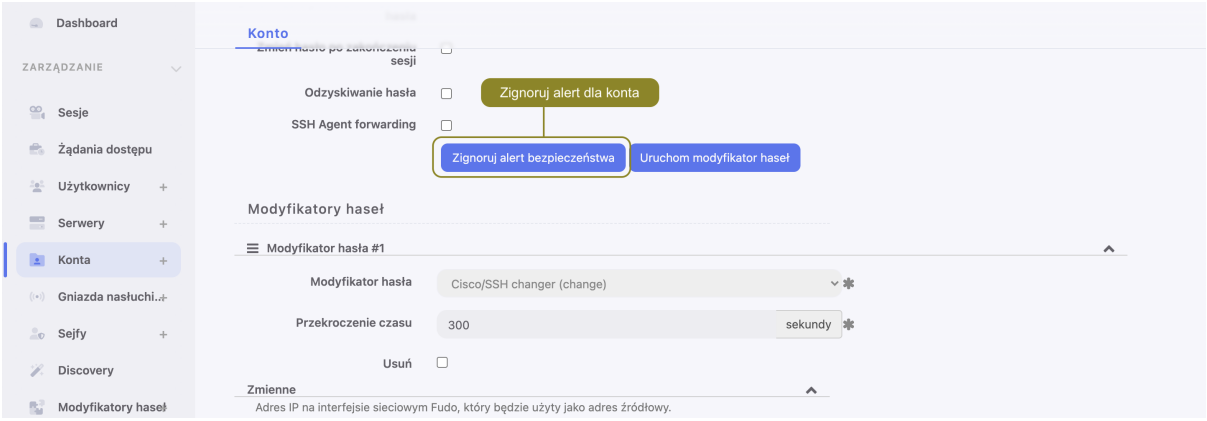
Zignorowanie ostrzeżenia z poziomu listy kont

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz konta, dla których chcesz zignorować ostrzeżenie.
3. Kliknij *Ignoruj alert*.

4. Kliknij *Zatwierdź*.

Zignorowanie ostrzeżenia z poziomu formularza edycji konta

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i kliknij wybrane konto, aby otworzyć formularz edycji.
3. W sekcji *Dane uwierzytelniające*, kliknij *Zignoruj alert bezpieczeństwa*.



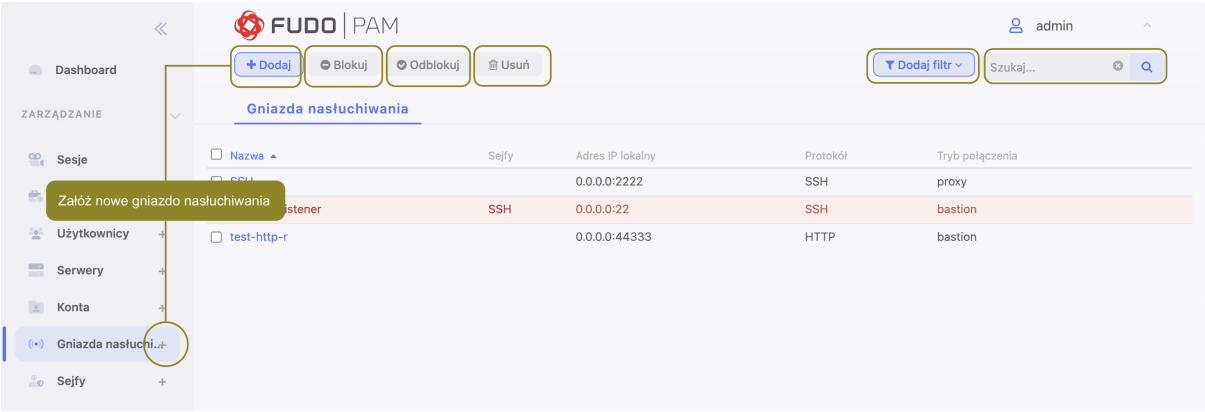
Tematy pokrewne:

- *Modyfikatory haseł*
- *Portal użytkownika*

ROZDZIAŁ 9

Gniazda nasłuchiwania

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



9.1 Dodawanie 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 replikacją danych, skontaktuj się z działem wsparcia technicznego.

Informacja:

- Gniazdo nasłuchiwania nie może być skojarzone z kontem przypisanym do serwera o protokole innym niż protokół gniazda nasłuchiwania.
- Gniazdo nasłuchiwania typu *pośrednik* może być skojarzone tylko z jednym serwerem.

- Gniazdo nasłuchiwania typu *bastion* nie może być skojarzone z kontem anonimowym.
- Gniazdo nasłuchiwania nie może być przypisane do jednego konta anonimowego poprzez dwa sejfy.
- 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 być przypisane do dwóch kont do tego samego serwera o tym samym protokole, co protokół gniazda nasłuchiwania, do których jeden użytkownik ma dostęp.

9.1.1 Dodawanie gniazda nasłuchiwania Citrix

Ostrzeżenie: Wsparcie protokołu `Citrix` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

1. Kliknij ikonkę *+* w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij *+ Dodaj*.
2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `Citrix StoreFront (HTTP)`.
5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem docelowym za pośrednictwem wybranego gniazda nasłuchiwania podlegało szyfrowaniu.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- W polu *Certyfikat TLS*, kliknij  , aby wygenerować certyfikat TLS, albo kliknij  , aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwolony format pliku z certyfikatem serwera - to PEM, jednak poza rozszerzeniem `.pem` akceptowane są też `.txt` oraz `.cert`.

  Informacja: W przypadku gdy wgrywany certyfikat jest zaszyfrowany, wprowadź hasło, które odszyfruje klucz.

  ---

8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Citrix StoreFront*
- *ICA*
- *Plik konfiguracyjny połączenia ICA*

9.1.2 Dodawanie gniazda nasłuchiwania HTTP

Użytkownicy portalu łącząc się do gniazda nasłuchiwania HTTP nie muszą wprowadzać loginu oraz hasła na stronie logowania HTTP. Ponieważ są już uwierzytelnieni na portalu, ich sesja jest automatycznie uwierzytelniona.

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `HTTP`.
5. Zaznacz opcję *Renderuj sesje*, aby połączenia HTTP przez wybrane gniazdo nasłuchiwania były renderowane graficznie.

Ostrzeżenie: Renderowanie sesji HTTP jest wymagającym procesem i może mieć negatywny wpływ na ogólną wydajność systemu. Monitorowanie rednerowanych połączeń HTTP zaleca się na maszynach fizycznych, z uwzględnieniem następujących limitów dla jednoczesnych połączeń HTTP.

Model	Maksymalna zalecana liczba jednoczesnych połączeń HTTP*
F100x	2
F300x	5
F500x	10

* Rzeczywista maksymalna liczba obsługiwanych sesji HTTP uwarunkowana jest konfiguracją danej instacji Fudo PAM.

Informacja: W przypadku renderowanych sesji HTTP, surowy ruch nie jest rejestrowany.

6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Bastion

Informacja:

- Tryb Bastion jest dostępny tylko przy zaznaczonej opcji *Renderuj sesje*.
- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.
- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.

- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Informacja: Adres zewnętrzny jest uwzględniony na liście kont w *portalu użytkownika* i umożliwia nawiązywanie sesji inicjowanych z sieci zewnętrznej.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

8. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie było szyfrowane.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- W polu *Certyfikat TLS*, kliknij , aby wygenerować certyfikat TLS, albo kliknij , aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwolony format pliku z certyfikatem serwera - to PEM, jednak poza rozszerzeniem `.pem` akceptowane są też `.txt` oraz `.cert`.

Informacja: W przypadku gdy wgrywany certyfikat jest zaszyfrowany, wprowadź hasło, które odszyfruje klucz.

---

9. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.3 Dodawanie gniazda nasłuchiwania ICA

Ostrzeżenie: Wsparcie protokołu `ICA` zostanie wycofane w następnej wersji Fudo PAM 5.3. Aby proces aktualizacji systemu przebiegł pomyślnie, jest wymagane usunięcie powiązanych sesji ze wspomnianym protokołem (poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `ICA`.
5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem docelowym za pośrednictwem wybranego gniazda nasłuchiwania podlegało szyfrowaniu.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- W polu *Certyfikat TLS*, kliknij  , aby wygenerować certyfikat TLS, albo kliknij  , aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwolony format pliku z certyfikatem serwera - to PEM, jednak poza rozszerzeniem `.pem` akceptowane są też `.txt` oraz `.cert`.

  Informacja:

- W przypadku gdy wgrywany certyfikat jest zaszyfrowany, wprowadź hasło, które odszyfruje klucz.
- W przypadku połączeń szyfrowanych, Fudo zwraca klientowi ICA *plik konfiguracyjny .ica*, w którym adresem FQDN serwera (*Address*) jest nazwa zwyczajowa (*Common Name*) z certyfikatu TLS.

8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tryby połączenia*
- *ICA*
- *Model danych*
- *Citrix StoreFront*
- *ICA*
- *Plik konfiguracyjny połączenia ICA*

9.1.4 Dodawanie gniazda nasłuchiwania Modbus

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `Modbus`.
5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.5 Dodawanie gniazda nasłuchiwania MySQL

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.

3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `MySQL`.
5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp > Tryby połączenia*.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.6 Dodawanie gniazda nasłuchiwania RDP

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `RDP`.
5. Z listy rozwijalnej *Bezpieczeństwo*, wybierz tryb bezpieczeństwa protokołu RDP.

Informacja: Tryb bezpieczeństwa gniazda nasłuchiwania RDP musi być zgodny z trybem bezpieczeństwa *serwera RDP*.

W przypadku jeśli zostały wybrane opcje *Enhanced RDP Security (TLS)* albo *Enhanced RDP Security (TLS) + NLA*, zaznacz dodatkowo opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).

6. W polu *Komunikat*, wprowadź informację, która będzie wyświetlana użytkownikom na ekranie logowania.
7. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
8. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Informacja: Adres zewnętrzny jest uwzględniony na liście kont w *portalu użytkownika* i umożliwia nawiązywanie sesji inicjowanych z sieci zewnętrznej.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

9. W polu *Certyfikat TLS*, kliknij  , aby wygenerować certyfikat TLS, albo kliknij  , aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwolony format pliku z certyfikatem serwera - to PEM, jednak poza rozszerzeniem `.pem` akceptowane są też `.txt` oraz `.cert`.

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

---

10. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*

- *Sejfy*
- *Konta*

9.1.7 Dodawanie gniazda nasłuchiwania SSH

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Zaznacz opcję *Nierozróżnianie wielkości liter*, aby proces uwierzytelnienia nie rozróżniał wielkości liter w nazwie użytkownika.
5. Z listy rozwijalnej *Protokół*, wybierz `SSH`.
6. Zaznacz opcję *ProxyJump*, która pozwala na wskazanie systemu pośredniczącego przez który można będzie łączyć się do docelowego serwera.
7. Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
8. W polu *Komunikat*, wprowadź informację, która będzie wyświetlana użytkownikom na ekranie logowania.
9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łączy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

Ze względu na szczególną interpretację znaku \ przez niektóre powłoki systemowe (np. bash), w celu prawidłowego zinterpretowania nazwy użytkownika i domeny podczas nawiązywania połączenia, należy odpowiednio sformatować ciąg znaków:

- „domena\uzytkownik”#bsd01@10.0.60.138
- «domena\uzytkownik»#bsd01@10.0.60.138
- domena\uzytkownik#bsd01@10.0.60.138

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.

- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Informacja: Adres zewnętrzny jest uwzględniony na liście kont w *portalu użytkownika* i umożliwia nawiązywanie sesji inicjowanych z sieci zewnętrznej.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

11. Kliknij ikonę  , aby wgrać *Klucz publiczny Fudo* (opcjonalnie, wprowadź hasło deszyfrujące), lub kliknij ikonę  , aby wygenerować klucz.

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

---

12. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.8 Dodawanie gniazda nasłuchiwania MS SQL

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.

4. Z listy rozwijalnej *Protokół*, wybierz `MS SQL (TDS)`.
5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp > Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.9 Dodawanie gniazda nasłuchiwania Telnet

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `Telnet`.
5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem docelowym za pośrednictwem wybranego gniazda nasłuchiwania podlegało szyfrowaniu.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- W polu *Certyfikat TLS*, kliknij , aby wygenerować certyfikat TLS, albo kliknij , aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwolony format pliku z certyfikatem serwera - to PEM, jednak poza rozszerzeniem `.pem` akceptowane są też `.txt` oraz `.cert`.

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

8. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.10 Dodawanie gniazda nasłuchiwania Telnet 3270

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.

3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.

4. Z listy rozwijalnej *Protokół*, wybierz `Telnet 3270`.

5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.

6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem docelowym za pośrednictwem wybranego gniazda nasłuchiwania podlegało szyfrowaniu.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- W polu *Certyfikat TLS*, kliknij  , aby wygenerować certyfikat TLS, albo kliknij  , aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwolony format

pliku z certyfikatem serwera - to PEM, jednak poza rozszerzeniem `.pem` akceptowane są też `.txt` oraz `.cert`.

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

---

8. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.11 Dodawanie gniazda nasłuchiwania Telnet 5250

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `Telnet 5250`.
5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Zaznacz opcję *Użyj szyfrowania TLS*, aby połączenie z serwerem docelowym za pośrednictwem wybranego gniazda nasłuchiwania podlegało szyfrowaniu.

- Zaznacz opcję *Starsze algorytmy kryptograficzne*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
- W polu *Certyfikat TLS*, kliknij , aby wygenerować certyfikat TLS, albo kliknij , aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwolony format pliku z certyfikatem serwera - to PEM, jednak poza rozszerzeniem `.pem` akceptowane są też `.txt` oraz `.cert`.

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

8. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.12 Dodawanie gniazda nasłuchiwania VNC

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `VNC`.
5. W polu *Komunikat*, wprowadź informację, która będzie wyświetlana użytkownikom na ekranie logowania.
6. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
7. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp > Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Informacja: Adres zewnętrzny jest uwzględniony na liście kont w *portalu użytkownika* i umożliwia nawiązywanie sesji inicjowanych z sieci zewnętrznej.

Brama (gateway)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.

- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

- W polu *Adres zewnętrzny* wprowadź adres IP (lub nazwę domenową FQDN) i numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

8. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.1.13 Dodawanie gniazda nasłuchiwania TCP

1. Kliknij ikonkę + w menu obok zakładki *Gniazda nasłuchiwania*, albo Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj*.

2. Wprowadź nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby konto było niedostępne po utworzeniu.
4. Z listy rozwijalnej *Protokół*, wybierz `TCP`.
5. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
6. W sekcji *Połączenie*, z listy rozwijalnej *Tryby połączenia*, wybierz sposób obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale *Wstęp* > *Tryby połączenia*.

Bastion

Informacja:

- Użytkownik łaczy się z serwerem docelowym podając jego nazwę w ciągu definiującym login, np. `ssh john_smith#mail_server@10.0.35.10`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Bastion`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Brama (gateway)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM zestawiając połączenie z serwerem używa własnego adresu IP. Ten tryb wymaga wdrożenia Fudo PAM w *trybie bramy*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Brama`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

Pośrednik (proxy)

Informacja:

- Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo PAM i numer portu, który jednoznacznie wskazuje docelową maszynę.
- Tryb *pośrednik* nie jest wspierany przez *serwery dodawane dynamicznie*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Pośrednik`.
- Z listy rozwijalnej *Adres lokalny*, wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia połączenia.

Informacja:

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykiety adresów IP*.
- Wybranie opcji `Dowolny`, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

Przezroczysty (transparent)

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP. Fudo PAM pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo PAM w *trybie mostu*.

- Z listy rozwijalnej *Tryb połączenia*, wybierz `Przezroczysty`.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

7. Kliknij *Zapisz*.

Tematy pokrewne:

- *Protokół TCP*
- *Dodawanie serwera TCP*
- *Model danych*

9.2 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.
5. Kliknij *Zapisz*.

Tematy pokrewne:

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

9.3 Blokowanie gniazda nasłuchiwania

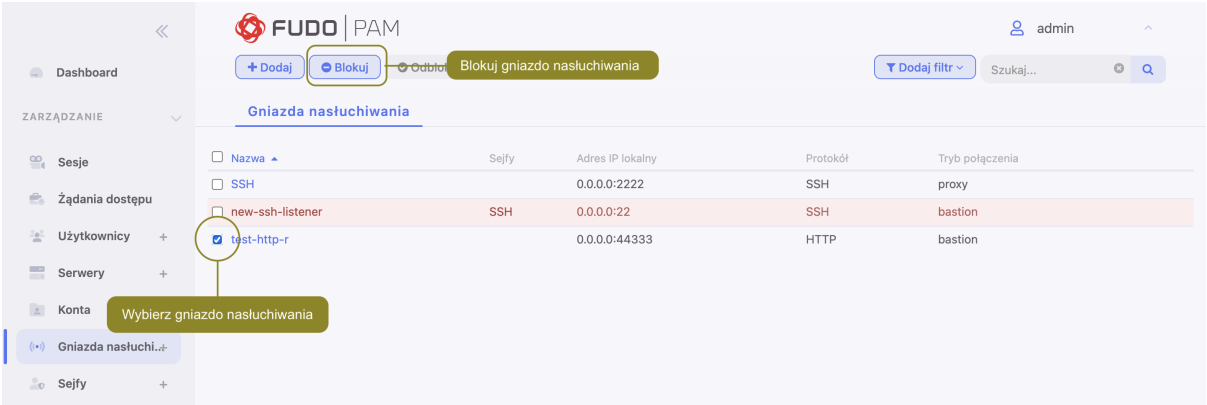
Ostrzeżenie: Zablokowanie gniazda spowoduje zerwanie aktualnie trwających sesji z serwerami, w połączeniach z którymi pośredniczy wybrane gniazdo nasłuchiwania.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

---

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*.

Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Tematy pokrewne:

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

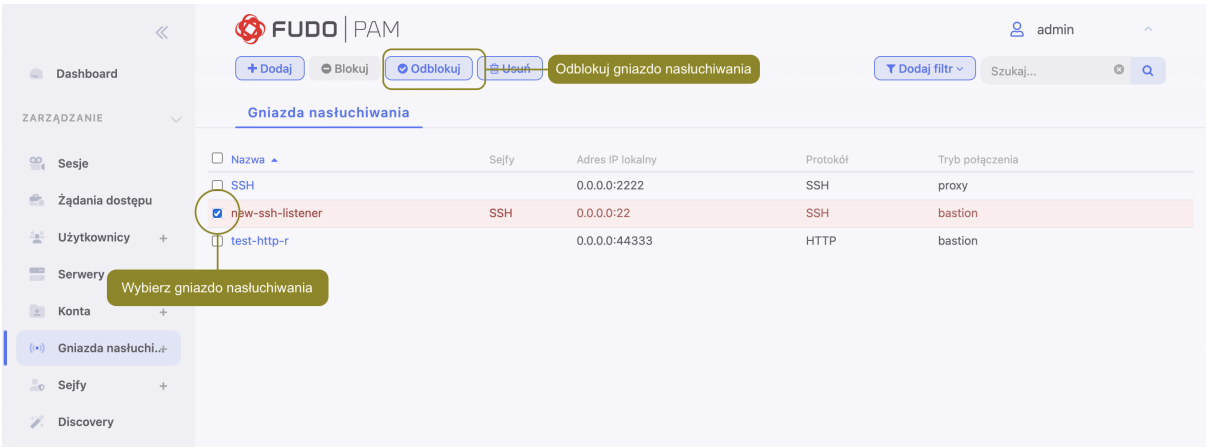
9.4 Odblokowanie gniazda nasłuchiwania

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

---

3. Kliknij *Odblokuj*.



4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektu.

Tematy pokrewne:

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

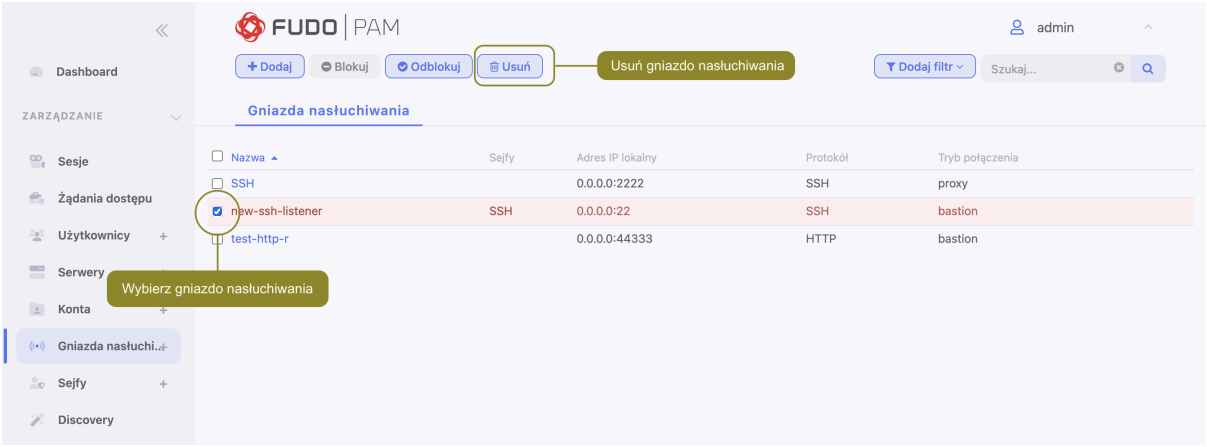
9.5 Usuwanie gniazda nasłuchiwania

Ostrzeżenie: Usunięcie gniazda nasłuchiwania spowoduje przerwanie aktualnie trwających sesji połączeniowych korzystających z usuniętego obiektu.

1. Wybierz z lewego menu *Zarządzanie* > *Gniazda nasłuchiwania*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.



4. Kliknij *Zatwierdź*, aby potwierdzić usunięcie zaznaczonych obiektów.

Tematy pokrewne:

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

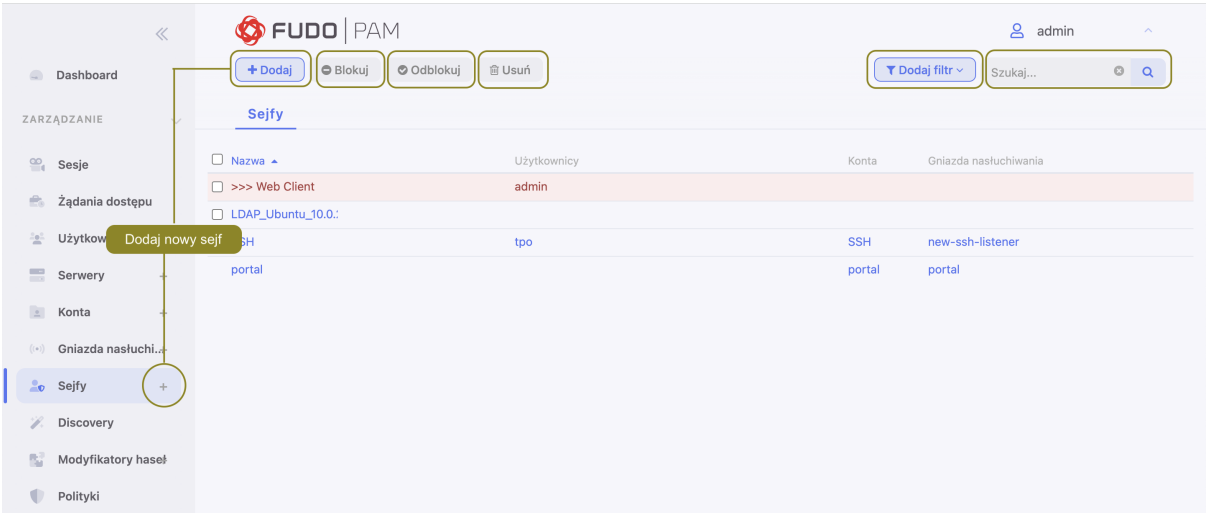
ROZDZIAŁ 10

Sejfy

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

Informacja:

- Sejf `system` może mieć przypisane tylko konto `system`.
- Sejf `portal` może mieć przypisane 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`.
- Użytkownik anonimowy musi mieć dostęp do sejfów, które zawierają konta anonimowe.



10.1 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 replikacją danych, skontaktuj się z działem wsparcia technicznego.

1. Kliknij + obok zakładki *Sejfy*, albo

Wybierz z lewego menu *Zarządzanie* > *Sejfy* i kliknij + *Dodaj*.

2. Wpisz nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby użytkownicy nie mieli dostępu do kont przypisanych do sejfu, zaraz po jego utworzeniu.
4. Zaznacz opcję *Powód logowania*, aby wyświetlić użytkownikowi monit o podanie powodu logowania do systemu docelowego.

Informacja: Wymaganie podania powodu logowania nie jest wspierane w połączeniach *HTTP*.

5. Zaznacz opcję *Głosy wymagane do uzyskania dostępu*, żeby uruchomić wysłanie żądań o dostęp do zasobów. Podaj liczbę głosów, które będą się liczyć do akceptacji bądź odrzucenia żądania użytkownika. Więcej informacji na temat udzielenia dostępu do zasobów pod linkiem *Żądania dostępu*.
6. Zaznacz opcję *Wymagaj potwierdzenia*, aby połączenia z serwerami realizowane za pośrednictwem wybranego sejfu, wymagały potwierdzenia przez osobę do tego upoważnioną. Podaj ile czasu (w minutach) administrator ma na potwierdzenie / odrzucenie.
7. Przypisz do sejfu *polityki bezpieczeństwa*.
8. Z listy rozwijalnej *Dostęp do notatek*, wybierz poziom dostępu użytkowników sejfu do notatek przypisanych dotyczących kont.

Informacja: Notatki dostępne są z poziomu formularza konta oraz w *Portalu Użytkownika*.

9. Wybierz opcję *Limit trwania sesji* oraz wprowadź wartość w minutach.
10. Wybierz opcję *Limit nieaktywności sesji* oraz wprowadź wartość w minutach.
11. Opcja *OTP w Portalu Użytkownika* jest domyślnie włączona i służy do generowania OTP w Portalu Użytkownika.

Ostrzeżenie: Wyłączenie opcji *OTP w Portalu Użytkownika* uniemożliwi połączenie przez Klienta Natywnego oraz Klienta Webowego w Portalu Użytkownika. Tylko dostęp przez *Żądania dostępu* będzie wtedy dostępny.

12. W przypadku sejfów opartych o RDP, VNC oraz SSH protokoły, wybierz opcję *Klient Webowy* w celu połączenia z serwerem w przeglądarce.

Informacja: Opcja *Klient Webowy* nie może być włączona kiedy opcja *OTP w Portalu Użytkownika* jest wyłączona.

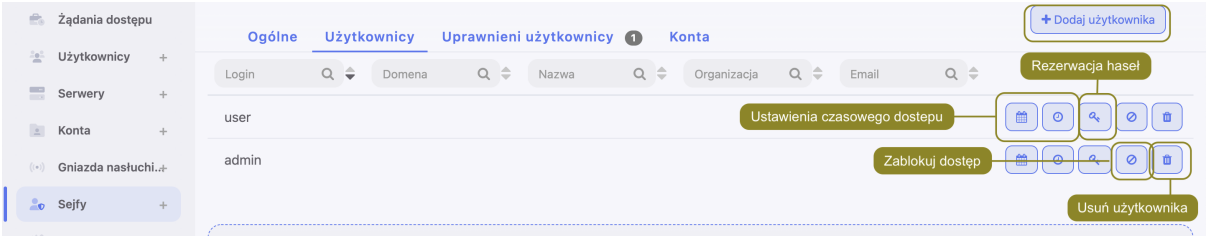
13. Z listy rozwijanej *Miejsce docelowe kopii zapasowej* wybierz skonfigurowane miejsce docelowe dla przechowania kopii zapasowych. Konfiguracja jest dostępna pod linkiem *Kopie zapasowe i retencja*.
14. W sekcji *Funkcjonalność protokołów*, zaznacz funkcje dozwolone w połączeniach.

Informacja: Zaznaczenie opcji *Wstrzymanie aktualizacji sesji* dla sesji RDP, spowoduje, że treść sesji nie będzie dostępna w odtwarzaczu przez okres, w którym aplikacja kliencka będzie zminimalizowana.

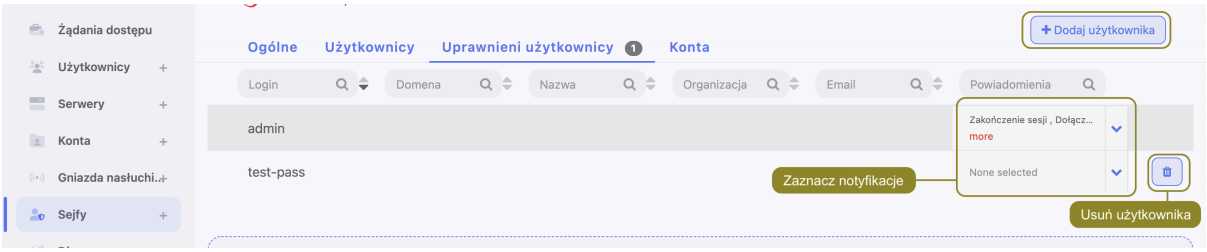
Zaznaczenie opcji *Client Cut Text* dla sesji VNC, umożliwi użytkownikowi wklejanie danych ze schowka do komputera serwera VNC.

Zaznaczenie opcji *Server Cut Text* dla sesji VNC, umożliwi użytkownikowi kopiowanie oraz wklejanie danych z komputera serwera VNC do swojego komputera.

15. Wybierz zakładkę *Użytkownicy*, aby nadać użytkownikom uprawnienia dostępu do sejfu.
    - Kliknij *+ Dodaj użytkownika*.
    - Kliknij [+] przy użytkowniku, któremu chcesz przyznać dostęp do sejfu.

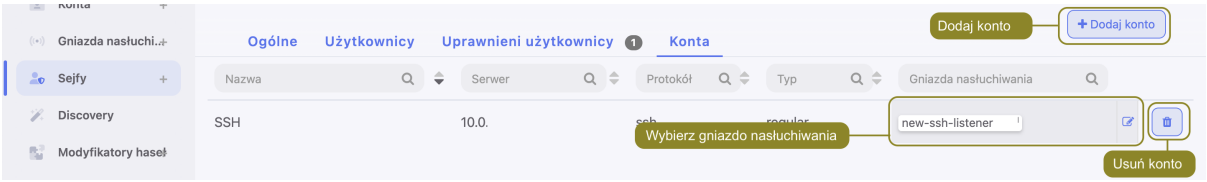


    - Kliknij *ok*, aby zamknąć okno modalu.
    - Zdefiniuj opcje dostępu do sejfu.
        - Kliknij [📅], aby przyznać dostęp w zadanym przedziale czasu. Opcja *okresu dostępu* jest nieaktywna, kiedy opcja *głosowania do uzyskania dostępu* jest włączona.
        - Kliknij [🕐], aby *zdefiniować dobową politykę czasu dostępu*. Opcja *dobowej polityki dostępu* jest nieaktywna, kiedy opcja *głosowania do uzyskania dostępu* jest włączona.
        - Kliknij [🔑], aby zezwolić użytkownikowi na rezerwację i podgląd haseł w Portalu Użytkownika.
        - Kliknij [⊘], aby zablokować użytkownikowi dostęp do sejfu.
        - Kliknij 🗑, aby usunąć użytkownika z sejfu.
16. Wybierz zakładkę *Uprawnieni użytkownicy*, aby nadać uprawnienia do zarządzania obiektem.



- Kliknij *+ Dodaj użytkownika*.
- Kliknij [+] przy użytkowniku, któremu chcesz przyznać prawo do zarządzania obiektem.
- Kliknij *ok*, aby zamknąć okno modalu.
- Ustaw powiadomienia dla konkretnego użytkownika. Ustawienia notyfikacji znajdziesz pod linkiem *Powiadomienia*.

17. Wybierz zakładkę Konta.



- Kliknij *+ Dodaj konto*.
- Kliknij [+] przy kontach, które chcesz dodać do sejfu.
- Kliknij *ok*, aby zamknąć okno modalu.
- Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*, aby dodać gniazda nasłuchiwania pośredniczące w nawiązywaniu połączenia.
- Kliknij [+] przy gnieździe nasłuchiwania, aby utworzyć powiązanie z wybranym kontem w ramach konfigurowanego sejfu.
- Kliknij *ok*, aby zamknąć okno modalu.

18. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie sejfu*
- *Blokowanie sejfu*
- *Usuwanie sejfu*
- *Żądania dostępu*

10.2 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.
5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Dodawanie sejfu*
- *Blokowanie sejfu*
- *Usuwanie sejfu*

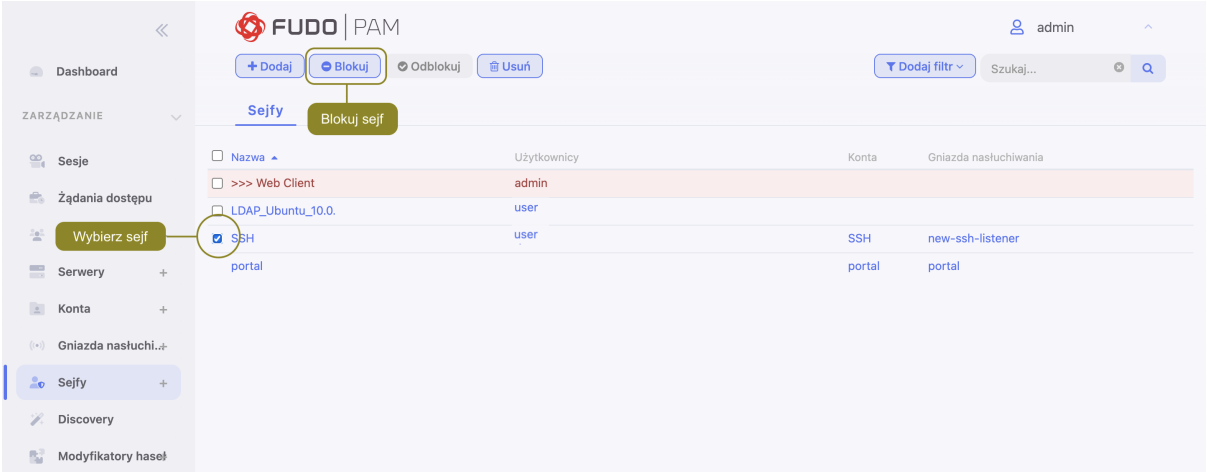
10.3 Blokowanie sejfu

Ostrzeżenie: Zablokowanie sejfu spowoduje zerwanie aktualnie trwających sesji połączeniowych, wykorzystujących konta przypisane wybranego obiektu.

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

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*.

Informacja: Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę .

Tematy pokrewne:

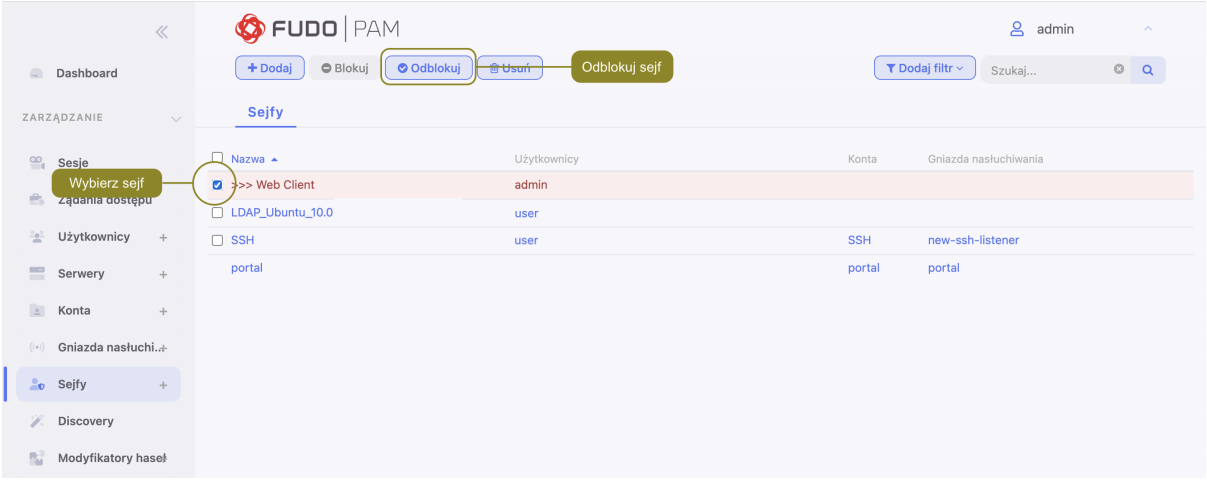
- *Odblokowanie sejfu*
- *Model danych*
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*

10.4 Odblokowanie sejfu

1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj*, aby przywrócić możliwość nawiązywania połączeń z serwerami z wykorzystaniem kont uprzywilejowanych przypisanych do wybranego sejfu.



4. Kliknij *Zatwierdź*, aby potwierdzić odblokowanie obiektów.

Tematy pokrewne:

- *Model danych*
- *Blokowanie sejfu*
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*
- *Usuwanie sejfu*

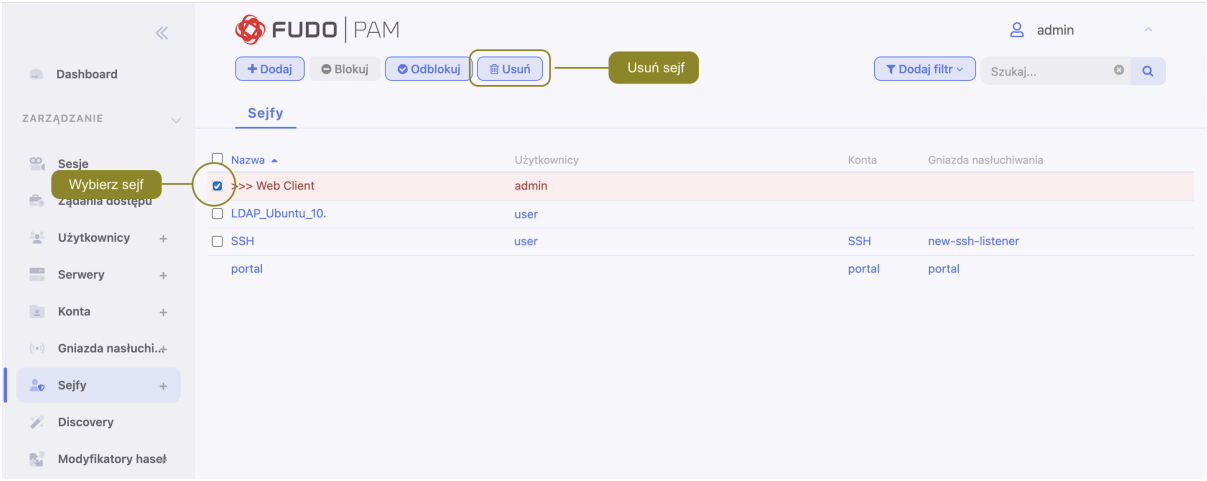
10.5 Usuwanie sejfu

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.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Usuń*.



4. Potwierdź operację usunięcia zaznaczonych obiektów.

Tematy pokrewne:

- *Model danych*
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*
- *Blokowanie sejfu*
- *Odblokowanie sejfu*

ROZDZIAŁ 11

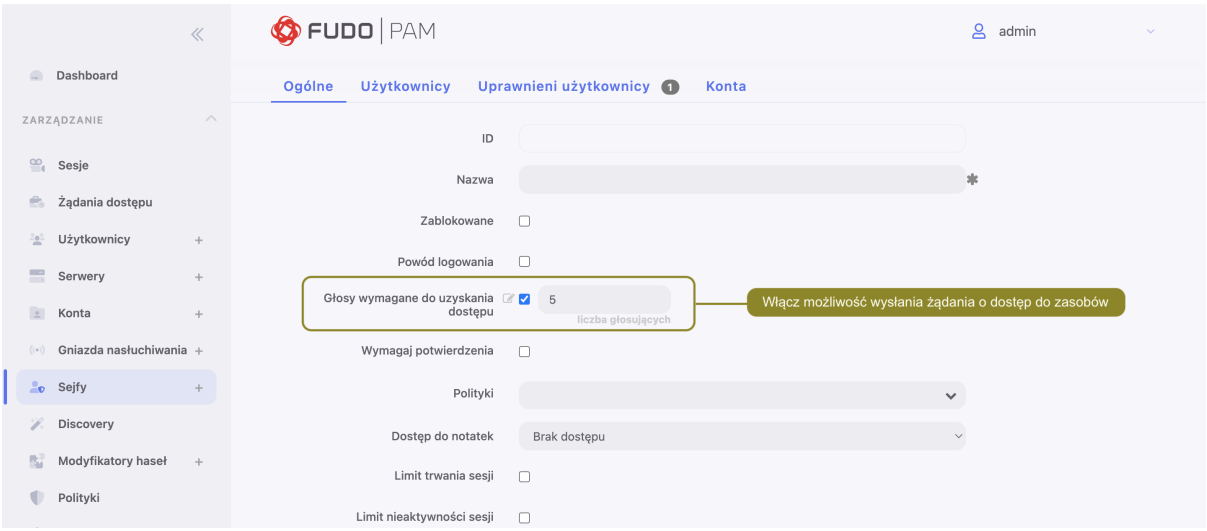
Żądania dostępu

Wysłanie żądania na potrzeby dostępu do zasobów jest podstawą funkcjonalności **Just In Time**.

Żądania są wysyłane użytkownikiem przez Portal Użytkownika, a osoby uprawnione do udzielenia dostępu, mogą zaakceptować bądź odrzucić żądanie w zakładce *Żądania dostępu* pod sekcją *Zarządzanie*.

Aby włączyć tę funkcjonalność, postępuj zgodnie z instrukcją:

1. Wybierz *Zarządzanie* > *Sejfy* i znajdź żądany sejf, bądź stwórz nowy.
2. W sekcji *Ogólne* ustawień sejfu zaznacz opcję *Głosy wymagane do uzyskania dostępu*. Razem z włączonym checkboxem pojawi się pole do wprowadzenia ilości tak zwanych głosów, które będą się liczyć do akceptacji bądź odrzucenia żądania użytkownika.



Informacja: Użytkownicy o rolach *Admin* oraz użytkownicy dodani do sejfu jako *Uprawnieni użytkownicy* mogą głosować o udzielenie dostępu.

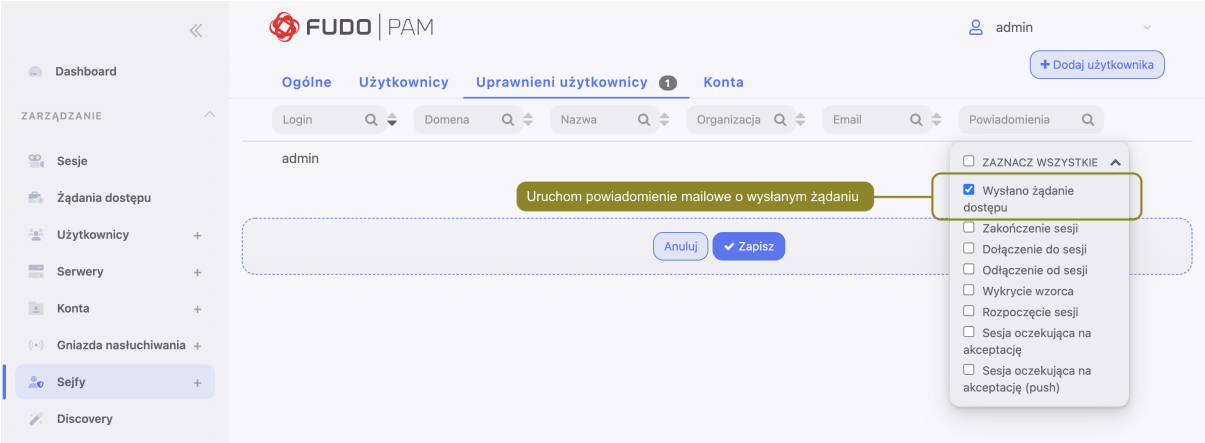
Użytkownik, który wysłał żądanie o dostęp nie może udzielać dostępu na swoje własne żądanie,

więc wysłane przez niego żądania nie są dla niego widoczne.

W przypadku ustawienia liczby osób głosujących większej niż 1, żądanie będzie musiało być zaakceptowane przez zdefiniowaną liczbę osób. Natomiast, jeśli jeden z głosujących zagłosuje na odrzucenie, całe żądanie zostanie odrzucone.

3. Teraz przejdź do pod-zakładki **Uprawnieni użytkownicy** i dodaj typ notyfikacji *Wysłano żądanie dostępu* dla użytkowników, którzy będą dostawać powiadomienia o wysłanych żądaniach.

Informacja: Notyfikacje są ustawiane per węzeł - zgodnie z ustawieniami w zakładce *Powiadomienia*. W przypadku wybrania notyfikacji typu *Wysłano żądanie dostępu*, powiadomienie mailowe zostanie wysłane z tego węzła, z którego zostało wysłane żądanie. Więcej na temat wysłania notyfikacji znajdziesz pod linkiem *Powiadomienia*.



4. Kliknij *Zapisz*.

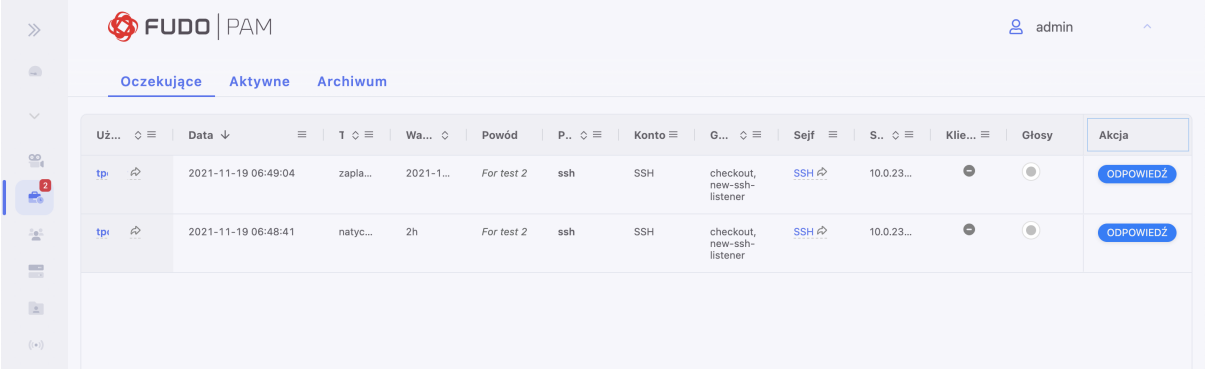
11.1 Żądania oczekujące

Użytkownik wysyłający ma do wyboru dwa typy żądania: **natychmiastowy** lub **zaplanowany**.

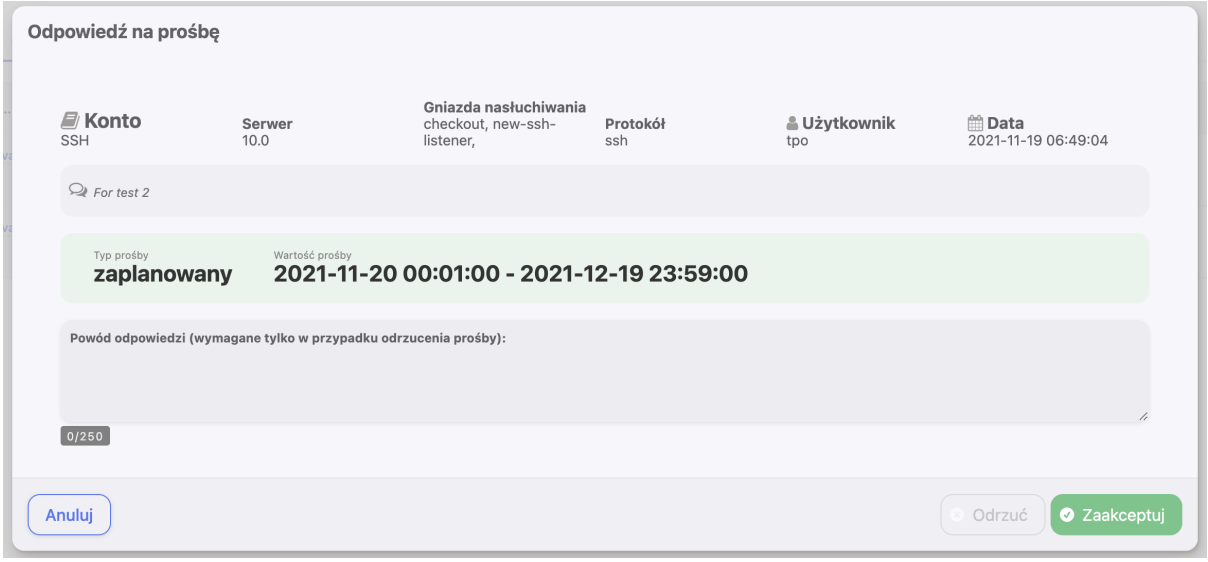
W przypadku wybrania **natychmiastowego** typu żądania, użytkownik może ustalić okres dostępu od zaraz do maksymalnie 24 godzin. Okres dostępu użytkownika zaczyna się w momencie zatwierdzenia żądania przez administratora - wtedy ma on 24 godziny na rozpoczęcie sesji. Kiedy użytkownik rozpoczyna sesję, system odlicza czas dostępu i przerywa połączenie, kiedy czas ten się skończy. Natomiast, jeśli użytkownik nie łączy się w ciągu bliższych 24 godzin, jego dostęp zostaje cofnięty.

Zaplanowany typ żądania polega na wyborze daty rozpoczęcia oraz daty zakończenia trwania dostępu.

Żądania oczekujące decyzji uprawnionych osób są widoczne w zakładce *Żądania dostępu* pod sekcją *Zarządzanie*.



Żeby zagłosować, wciśnij przycisk *Odpowiedź*. W modalu będzie widoczna szczegółowa informacja o wysłanym żądaniu. Wprowadź *Powód odpowiedzi* oraz wybierz opcję akceptacji albo odrzucenia.

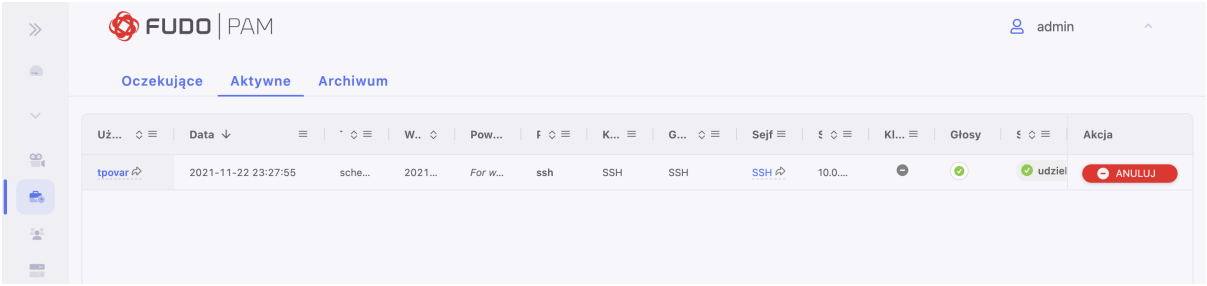


Informacja:

- Użytkownicy, którzy wysłali żądanie o dostęp oraz mają skonfigurowane adresy mailowe w Panelu Admina, dostaną powiadomienie, kiedy ich żądanie zostanie zaakceptowane bądź odrzucone.
- Jeśli użytkownik próbuje się połączyć do serwera (przykładowo, o protokole SSH) korzystając z opcji *klient natywny*, ale nie wysłał żądania o dostęp, stosowny komunikat o błędzie uwierzytelnienia będzie zapisany w Dzienniku zdarzeń: `Unable to authenticate user: safe requires acceptance`.

11.2 Żądania aktywne

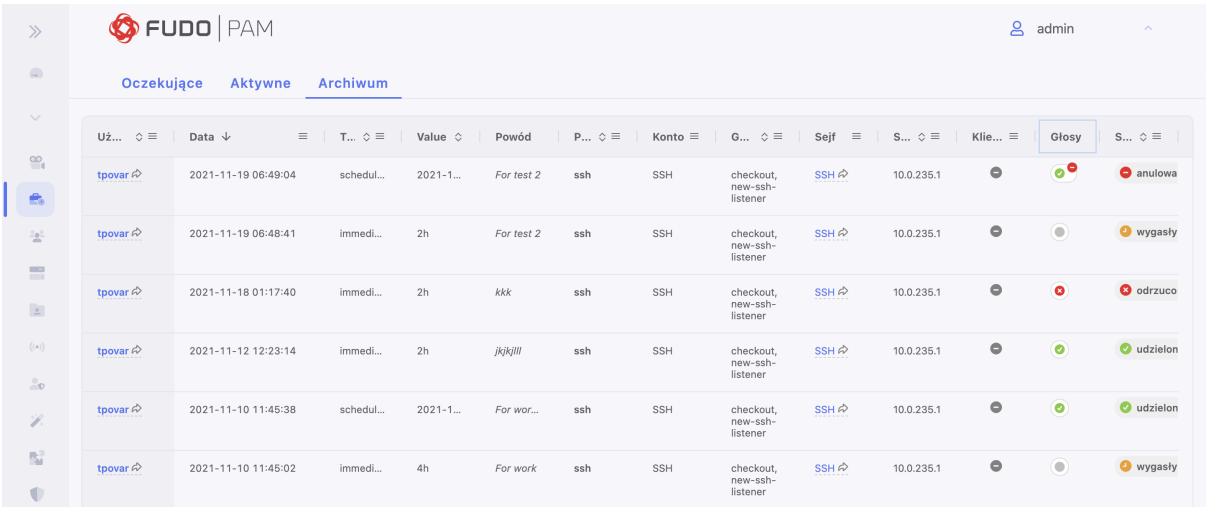
Pod zakładką *Aktywne* są widoczne dwa typy żądań: 1) te, które zostały zaakceptowane, i je sesje obecnie trwają, oraz 2) te, które dalej oczekują na część głosów. W kolumnie *Głosy* można sprawdzić aktualny stan żądania oraz ile głosów konkretne żądanie potrzebuje.



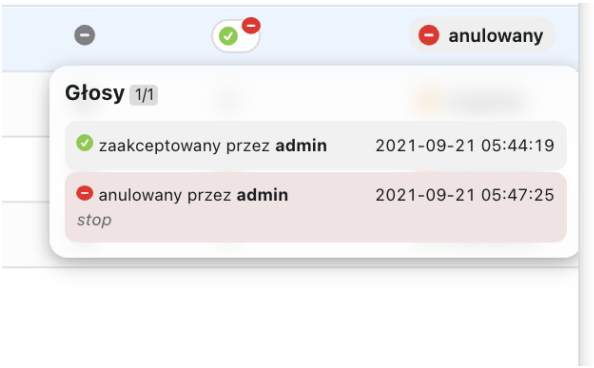
Stąd też można odwołać dostęp użytkownikowi poprzez wciśnięcie przycisku *Anuluj*, dostępnego dla żądań z już uznanym dostępem. Ta opcja też jest przydatna w sytuacji, kiedy użytkownik skończył pracę wcześniej - administrator może odwołać dostęp w celu uniknięcia nadużycia zasobów.

11.3 Archiwum żądań

Historia skompletowanych żądań jest widoczna w zakładce *Archiwum*.



Informacja o dokonanych głosach na konkretne żądanie jest dostępna po najechaniu na rekord kolumny *Głosy*.



Funkcjonalność **Just In Time** działa też w obrębie klastra połączonych instancji Fudo. Żądania oraz głosy są replikowane na poszczególnych węzłach klastra.

Informacja: W przypadku, gdy użytkownik zagłosował na kilku maszynach w obrębie klastra,

i jego głosy były sprzeczne, system potraktuje żądanie jako odrzucone.

Tematy pokrewne:

- *Dodawanie sejfu*

ROZDZIAŁ 12

Wykrywanie (Discovery)

Funkcjonalność Wykrywanie polega na przeszukiwaniu serwera kontrolera domeny pod kątem kont o różnym stopniu uprzywilejowania i przyznania im dostępu poprzez dodanie do odpowiednich gniazd nasłuchiwania oraz / lub sejfów. Alternatywnie, wysłania kont do kwarantanny. Proces przyznania wykrytym kontom dostępu nazywa się *przydzieleniem*.

Dodatkowe nazewnictwo, które zostało wprowadzone w ramach tej funkcjonalności do zakładki *Wykrywanie* oraz zakładki *Konta*:

Skaner - główny komponent, służący do wykrywania kont na serwerze docelowym. Może, ale nie musi posiadać reguły, definiujące akcje stosowane do wykrytych kont. Skaner może być uruchamiany manualnie lub automatycznie według ustawionego harmonogramu.

Reguła pozwala ustawić kryteria do spełnienia dla kont, które mają zostać wykryte oraz akcje, następnie do nie stosowane.

Kategoria konta - poziom uprzywilejowania konta.

Konta Odkryte - konta, które zostały wykryte na serwerze docelowym przez skaner.

Konta Przydzielone - konta, które zostały dodane do sejfu oraz / lub gniazda nasłuchiwania.

Konta pod kwarantanną - konta, które zostały zablokowane na serwerze docelowym.

Informacja: Funkcja Wykrywanie wykonuje skanowanie serwera Active Directory stosując tryb połączenia LDAP.

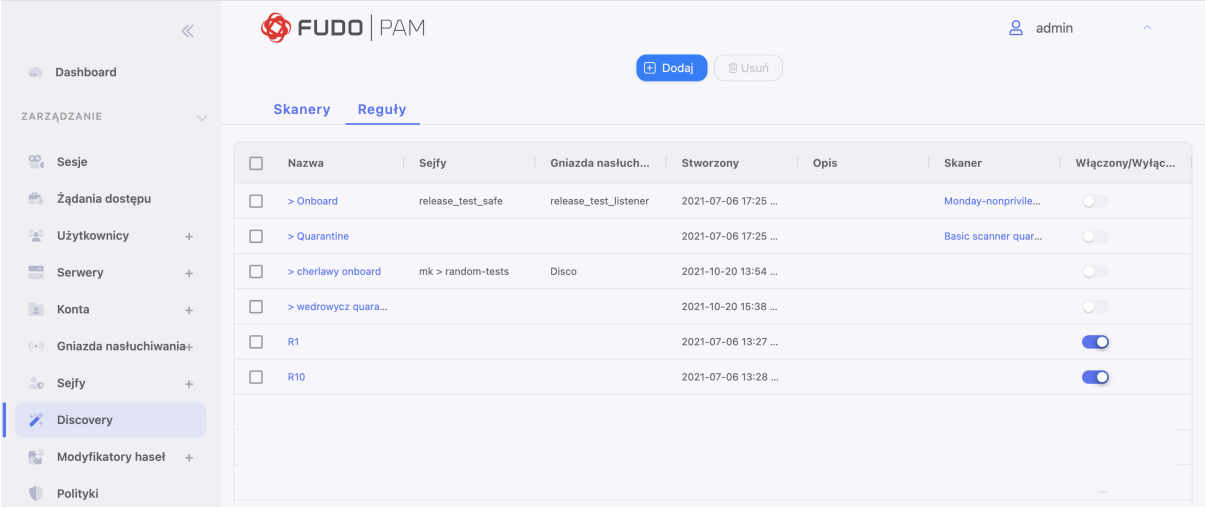
Funkcja Wykrywanie działa najskuteczniej ze skonfigurowanym skanerem oraz regulą. Reguła ma na celu zidentyfikowanie konta oraz wykonanie odpowiednich akcji. Skaner z kolei przeszukuje serwer docelowy pod kątem kont do wykrycia oraz przy dodanej regule wykonuje automatyczne przydzielenie.

Dla szybszeij konfiguracji jest wskazane najpierw stworzyć Regułę, później Skaner. Jednak ponieważ, skaner może ale nie musi posiadać reguły, krok tworzenia reguły może zostać pominięty. Wtedy wykryte konta będą musiały być przydzielone przez administratora manualnie.

Informacja: Aktywny węzeł odkrywania kont jest ustawiony w sekcji *Discovery* zakładki *Ustawienia* > *System*.

12.1 Tworzenie reguły

Każda reguła może być włączona albo wyłączona. Kiedy reguła jest włączona, system automatycznie przydziela bądź wysyła do kwarantanny konta, które spełniają zadane kryteria. Reguły działaja na kontach **odkrytych**, lecz nie na kontach, które już zostały przydzielone albo wysłane do kwarantanny. W praktyce to oznacza, że jeśli działająca reguła została zmieniona, jej zmiany wejdą "w życie" już dla nowo odkrytych kont.



W celu stworzenia reguły postępuj zgodnie z poniższą instrukcją:

1. Wybierz *Zarządzanie* > *Wykrywanie* > *Reguły*.
2. Kliknij + *Dodaj*.
3. Wprowadź nazwę reguły.
4. Opcjonalnie, wprowadź opis reguły.
5. W sekcji *Konfiguracja*:

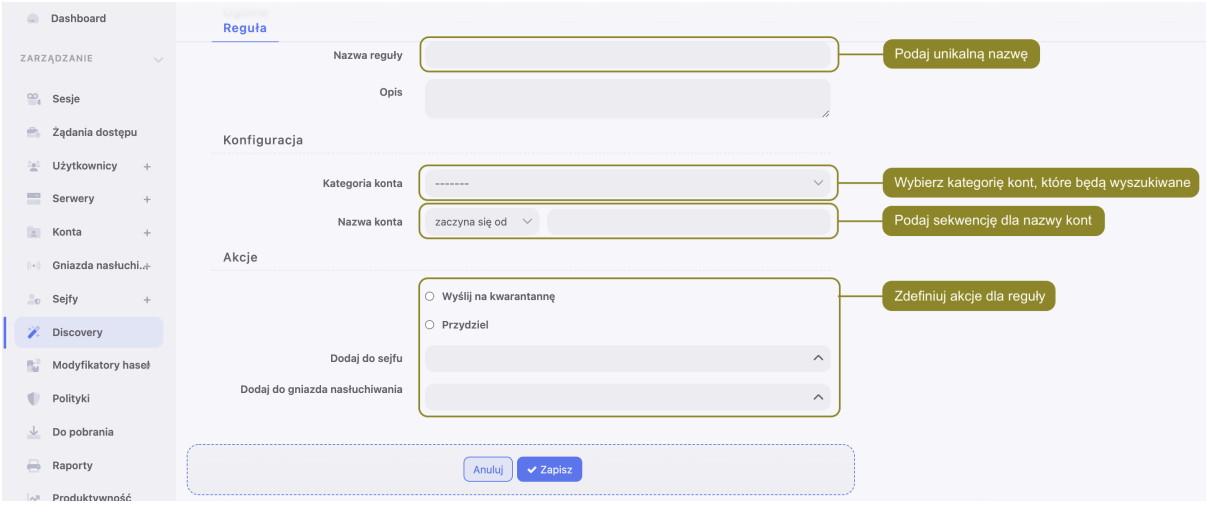
   5.1. Wybierz *Kategorię konta* (`uprzywilejowany`, `nieuprzywilejowany` albo `wszystko`).

   5.2. W polu *Nazwa konta* wybierz `zawiera`, `zaczyna się od` albo `kończy się`, aby doprecyzować nazwę kont do wykrycia.

   5.3. Ustaw *Akcje*:

5.3.1. **Wyślij na kwarantannę**, albo

5.3.2. **Przydziel** dodając konta do konkretnych sejfów oraz / albo gniazd nasłuchiwania. **Tylko gniazda nasłuchiwania o trybie połączenia bastion są wspierane**.



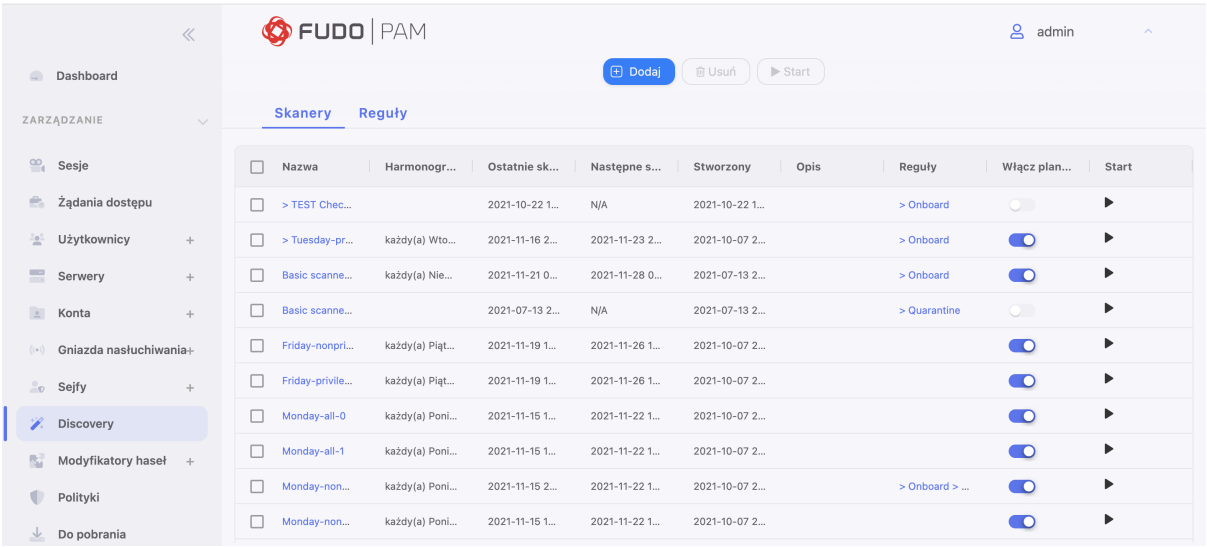
6. Kliknij *Zapisz*.

Related topics:

- *Tworzenie skanera*
- *Zarządzanie kontami*

12.2 Tworzenie skanera

Skanery ze zdefiniowanym harmonogramem mogą być włączone albo wyłączone. Jeśli skaner ma harmonogram włączony, system automatycznie wykona zadaną konfigurację. Jeśli natomiast skaner ma harmonogram wyłączony, system będzie czekać na decyzję administratora przed tym, jak wykonać zdefiniowaną akcję.



W celu stworzenia skanera postępuj zgodnie z poniższą instrukcją:

1. Wybierz *Zarządzanie* > *Wykrywanie* > *Skanery*.
2. Kliknij *+ Dodaj*.
3. Wprowadź nazwę skanera.
4. Pole *Typ skanera* ma domyślnie wybraną wartość `Kontroler Domeny`.
5. Opcjonalnie, wprowadź opis skanera.
6. W sekcji *Harmonogram* wybierz dzień oraz czas, kiedy co tydzień skaner będzie się uruchamiał przez system. Ten krok może zostać pominięty, jeśli administrator chcę uruchamiać skaner manualnie.
7. W sekcji *Konfiguracja*:

   7.1. Wybierz *Serwer docelowy*.

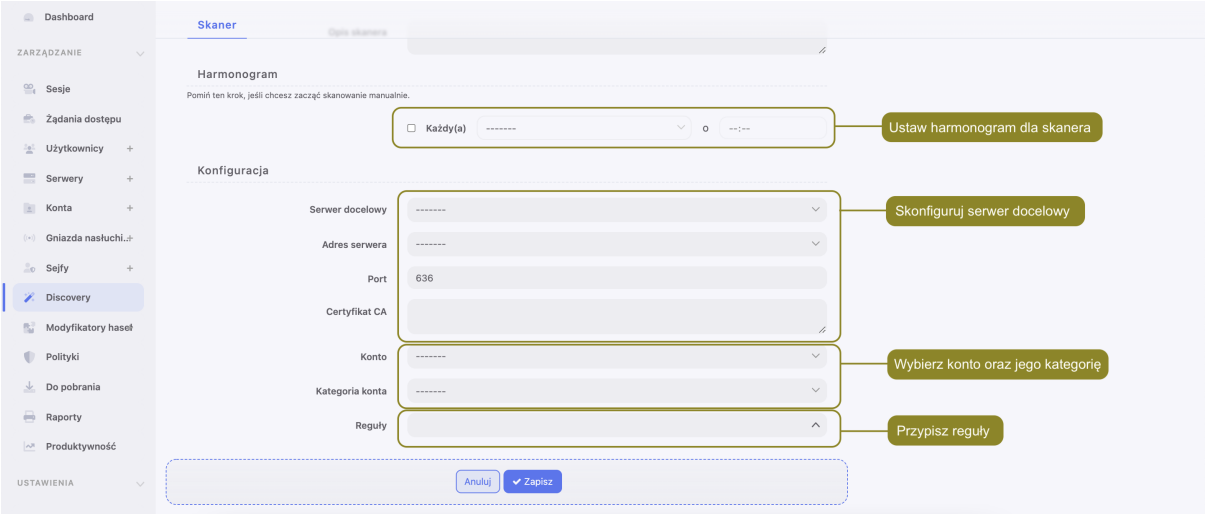
   7.2. Wybierz *Adres serwera* oraz *Port*.

   7.3. Wprowadź *Certyfikat CA*.

   7.4. Wybierz *Konto* do połączenia z serwerem docelowym.

   7.5. Wybierz *Kategorię konta* (`uprzywilejowany`, `nieuprzywilejowany` albo `wszystko`).

   7.6. Wybierz *Reguły*. **W przypadku dodania więcej niż jednej reguły, ich kolejność będzie miała znaczenie. Jeśli działania reguł będą się pokrywać, system zastosuje pierwszą z kolejki**.



8. Kliknij *Zapisz*.

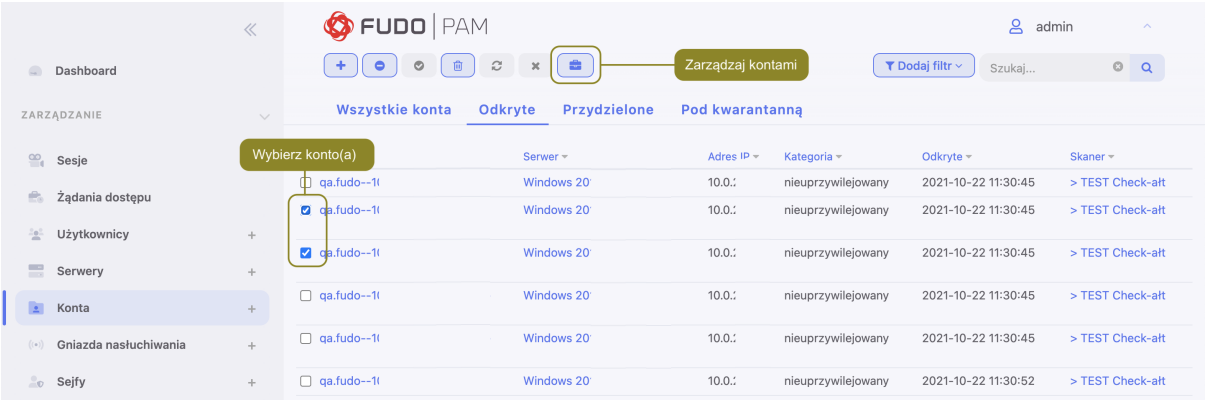
Related topics:

- *Tworzenie reguły*
- *Zarządzanie kontami*

12.3 Zarządzanie kontami

Odkryte, *przydzielone* konta oraz konta *pod kwarantanną* są dostępne w głównym widoku zakładki *Konta*.

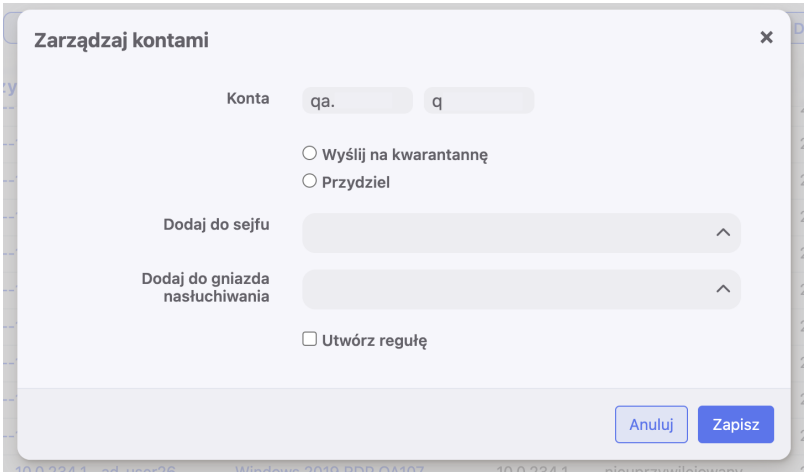
Konta, które się znajdą w zakładce *Odkryte* zostaną wykryte przez skaner, lecz nie zostaną ani przydzielone, ani wysłane do kwarantanny. Będzie to spowodowane brakiem automatycznego ustawienia skanera albo reguły. Administrator może przydzielić albo wysłać do kwarantanny je manualnie korzystając z opcji *Zarządzaj kontami* z górnego menu.



1. Wybierz *Zarządzanie* > *Konta* > *Odkryte*
2. Zaznacz konto lub konta, które chcesz przydzielić albo wysłać do kwarantanny.
3. Wybierz opcję *Zarządzaj kontami*.
4. Wybierz akcję:

   4.1 **Wyślij na kwarantannę** (opcjonalnie, podaj powód) albo

   4.2 **Przydziel** dodając konta do konkretnych sejfów oraz / albo gniazd nasłuchiwania. **Tylko gniazda nasłuchiwania o trybie połączenia bastion są wspierane**.
5. Kliknij *Utwórz regułę*, jeśli chcesz uruchomić powtarzanie zdefiniowanej czynności.



6. Kliknij *Zapisz*.

Related topics:

- *Tworzenie reguły*
- *Tworzenie skanera*

ROZDZIAŁ 13

Modyfikatory haseł

Fudo PAM umożliwia zarządzanie hasłami dostępu do kont uprzywilejowanych zdefiniowanych na monitorowanych systemach.

Modyfikatory haseł operują na wyodrębnionej warstwie transportowej SSH, LDAP, Telnet oraz WinRM i dają możliwość skorzystania z predefiniowanych skryptów lub *napisania własnych*. Modyfikatory mogą przyjąć również *postać wtyczek wgrywanych na* Fudo PAM.

Wbydowane modyfikatory haseł obejmują następujące scenariusze:

- Unix poprzez SSH
- MySQL na serwerze Unix poprzez SSH
- Cisco poprzez SSH i Telnet
- Cisco Enable Password poprzez SSH i Telnet
- WinRM
- LDAP

13.1 Polityki haseł

Polityka zmiany haseł określa częstotliwość zmiany hasła oraz jego złożoność.

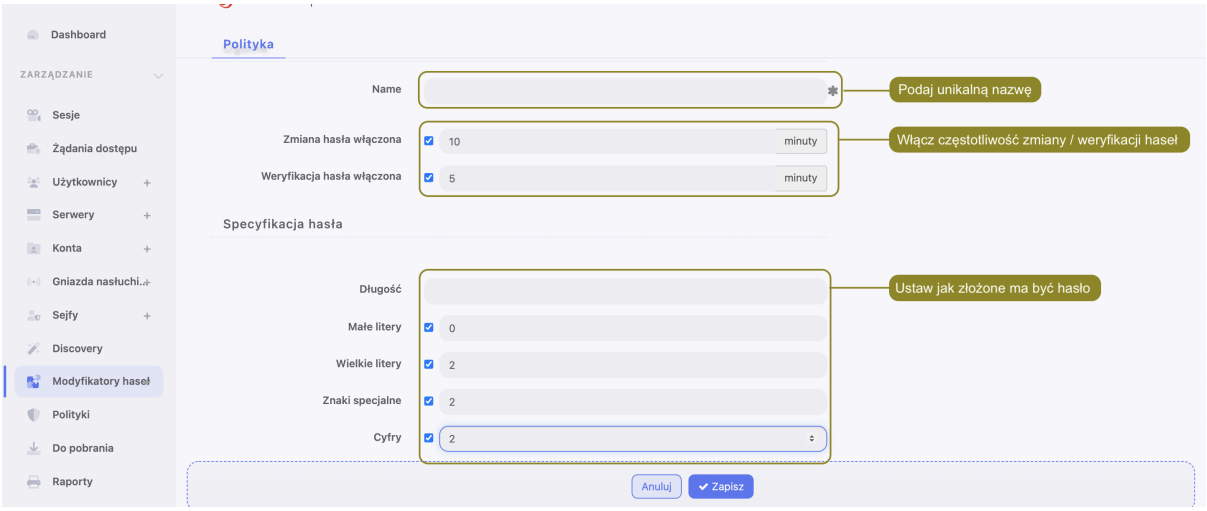
13.1.1 Dodawanie polityki zmiany haseł

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Kliknij + *Dodaj*.
3. Wprowadź nazwę dla modyfikatora haseł.
4. Zaznacz opcję *Zmiana hasła włączona* i zdefiniuj jak często hasło ma być zmieniane.

5. Zaznacz opcję *Weryfikacja hasła włączona* i zdefiniuj jak często sprawdzane będzie, czy hasło nie zostało zmienione w sposób nieuprawiony.
6. W sekcji *Specyfikacja hasła*, określ złożoność generowanego ciągu znaków.

Parametr	Opis
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.

7. Kliknij *Zapisz*.



13.1.2 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*.

13.1.3 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.

Tematy pokrewne:

- *Model danych*

- *Konta*
- *Uniwersalne modyfikatory haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

13.2 Uniwersalne modyfikatory haseł

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

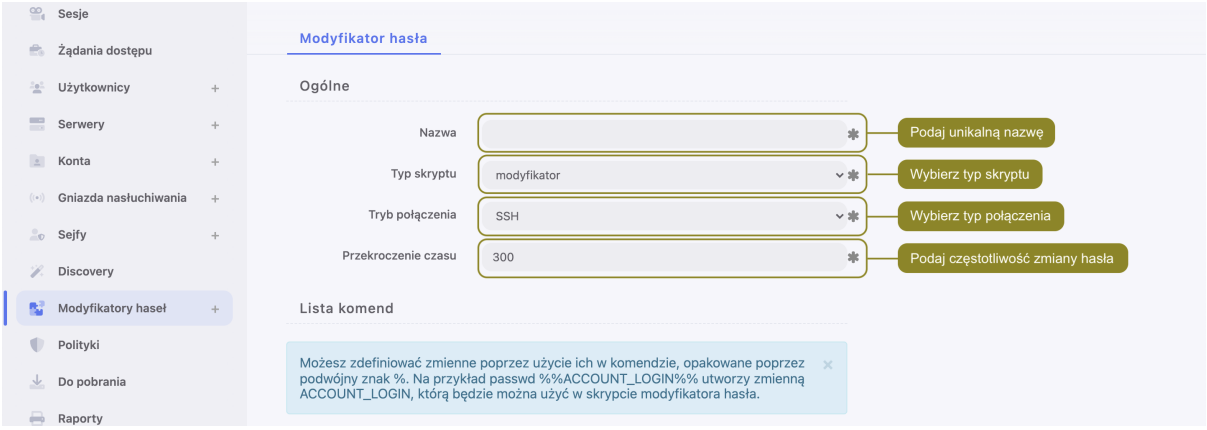
Informacja: W konfiguracji klastrowej, zmiana haseł realizowana jest przez wybrany węzeł, wskazany w ustawieniach systemowych. Więcej informacji na temat zmiany aktywnego węzła klastra, znajdziesz w rozdziale *Modyfikatory haseł - aktywny węzeł klastra*.

13.2.1 Definiowanie modyfikatora haseł

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

---

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.
3. Kliknij *+ Dodaj*.
4. W sekcji *Ogólne*, wprowadź nazwę modyfikatora haseł.
5. Z listy rozwijalnej *Typ skryptu*, wybierz czy definiowany obiekt jest modyfikatorem czy weryfikatorem hasła.
6. Z listy rozwijalnej *Tryb połączenia*, wybierz protokół komunikacji z systemem docelowym.
7. W polu *Limit czasowy*, określ limit czasu na wykonanie skryptu.



8. W sekcji *Lista komend*, kliknij [+], aby dodać określoną komendę.

Informacja: Dostępne komendy zależą od wybranej warstwy transportowej.

- `INPUT` - komenda wykonywana po stronie serwera.
- `EXPECTED` - oczekiwany rezultat wykonania komendy.
- `ENTER`
- `DELAY` - opóźnienie wyrażone w sekundach.
- `DN` - parametr DN usługi katalogowej.
- `FILTER` - filtr użytkownika w usłudze katalogowej.

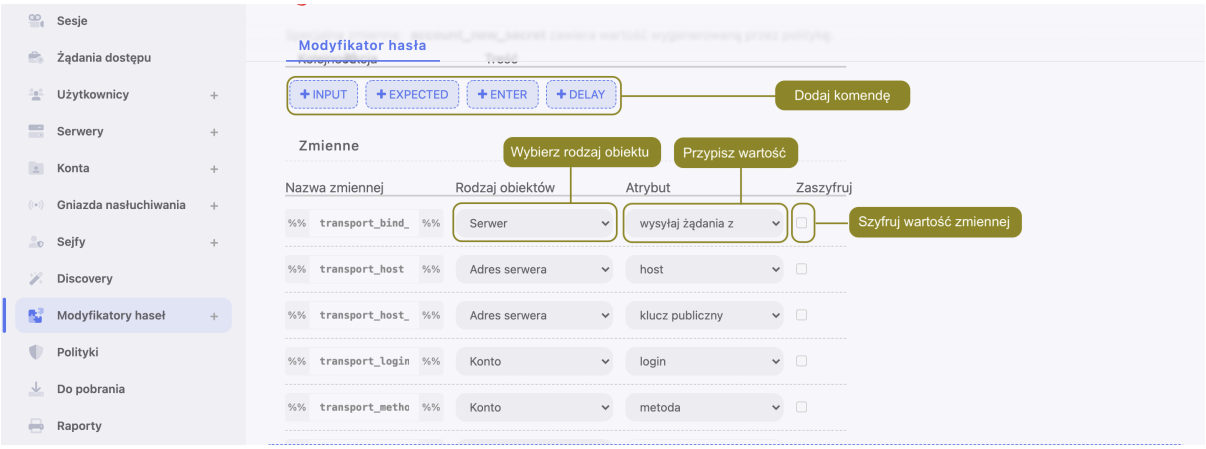
Ostrzeżenie: Aby skonfigurować modyfikator haseł **WinRM**, musisz podać dane uwierzytelniające użytkownika z uprawnieniami do zmiany haseł (zwykle konto na poziomie administratora). Nie należy używać tego konta do zmiany własnego hasła, ponieważ WinRM zwróci błąd, którego Fudo PAM nie może obsłużyć. **Upewnij się, że zmienne account_login i transport_login mają różne wartości.**

9. Wprowadź komendę lub sparametryzuj dodaną akcję.

Informacja: W komendach można stosować zmienne predefiniowane dla wybranej warstwy transportowej lub własne zmienne. Aby użyć lub zdefiniować zmienną w komendzie, umieść ciąg znaków pomiędzy znakami `%%`, np. `%%host%%`.

---

10. Kliknij [💬], aby dodać opcjonalny komentarz.
11. Powtarzaj kroki 8-10, aby dodać kolejne komendy.
12. W sekcji *Zmienne*, określ atrybuty zmiennych występujących w skrypcie.



13. Kliknij *Zapisz*.
14. *Zdefiniuj politykę haseł* i *dodaj modyfikator do konta*.

Informacja: Przykład

Przykładowy modyfikator haseł, dokonujący zmiany sekretu na systemie FreeBSD, za pomocą komendy `passwd` wykonanej z uprawnieniami *sudo*.

Lista komend

	Akcja	Treść	Komentarz
1	EXPECTED	`Password`	Spodziewany wyraz «Password» w treści konsoli.
2	INPUT	`%%transport_secret%%`	Zmienna `transport_secret` reprezentuje sekret uwierzytelniający konto, uprawnione do zmiany hasła.
3	EXPECTED	`\[john@john-laptop.*\]`	Spodziewana treść odpowiadająca wyrażeniu regularnemu przedstawiona na konsoli.
4	INPUT	`sudo passwd %%account_login%%`	Komenda zmiany hasła na koncie; zmienna `account_login` reprezentuje login użytkownika, któremu jest zmieniane hasło.
5	EXPECTED	`Password`	Spodziewany wyraz «Password» w treści konsoli.
6	INPUT	`%%transport_secret%%`	Zmienna `transport_secret` reprezentuje sekret uwierzytelniający konto, uprawnione do zmiany hasła.
7	EXPECTED	`Changing local password`	Spodziewany wyraz «Changing local password» w treści konsoli.
8	EXPECTED	`New Password`	Spodziewany wyraz «New Password» w treści konsoli.
9	INPUT	`%%account_new_secret%%`	Nowe hasło
10	EXPECTED	`Retype New Password`	Spodziewany wyraz «Retype New Password» w treści konsoli.
11	INPUT	`%%account_new_secret%%`	Nowe hasło
12	INPUT	`echo $?`	
13	EXPECTED	`0`	

Zmienne

Nazwa zmiennej	Rodzaj obiektu	Atrybut	Zaszyfruj
transport_method	constant		✗
transport_bind_to	server_property	bind_ip	✗
transport_user	account	login	✗
transport_host	server_address_property	host	✗
transport_port	server_property	port	✗
transport_secret	account	secret	✓
transport_host_public_key	constant		✗
account_login	account	login	✗

13.2.2 Edytowanie uniwersalnego modyfikatora haseł

Ostrzeżenie: Zmiana modyfikatora, który jest aktualnie w użyciu, może wymagać ręcznej korekty w kontach, do których jest przypisany. Lista kont, które potrzebują takiej zmiany zostanie wyświetlona.

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*.

13.2.3 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:

- *Modyfikatory haseł - aktywny węzeł klastra*
- *Konta*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

13.3 Tryby połączenia

Tryb połączenia określa warstwę transportową używaną w procesie zmiany hasła. Warstwa transportowa determinuje listę dostępnych komend oraz zmiennych systemowych dla modyfikatora oraz weryfikatora haseł.

13.3.1 SSH

Tryb połączenia SSH używa protokołu SSH w celu nawiązania połączenia ze zdalnym systemem.

Komendy

Komenda	Opis
INPUT	Komenda wykonana na zdalnym systemie.
EXPECTED	Oczekiwany rezultat wykonania komendy.
ENTER	
DELAY	Opóźnienie pomiędzy wykonanywanymi komendami.

Zmienne

Zmienna	Opis
transport_bind_ip	Adres IP używany przez Fudo przy komunikacji ze zdalnym systemem.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_host_public_key	Klucz publiczny zdalnego systemu.
transport_login	Nazwa konta na systemie docelowym, uprawnionego do zmiany hasła.
transport_method	Metoda uwierzytelnienia konta uprawnionego do zmiany hasła. Dopuszczalne wartości: `password` or `sshkey`.
transport_password_prompt	Wyrażenie regularne opisujące zapytanie systemowe o podanie hasła. **Informacja:** W przypadku zdefiniowania parametru jako wartość stałą, nie uzupełnienie wartości zmiennej po przypisaniu modyfikatora hasła do konta, poskutkuje przyjęciem domyślnej postaci wyrażenia.
transport_port	Numer portu, służący do nawiązania połączenia z systemem docelowym.
transport_secret	Sekret służący do uwierzytelnienia konta wykorzystywanego w procesie zmiany hasła.
account_login	Login użytkownika, któremu jest zmieniane hasło.
account_new_secret	Zmienna systemowa, inicjowana wartością automatycznie wygenerowaną przez Fudo.

13.3.2 LDAP

Warstwa transportowa LDAP wykonuje zapytanie LDAP do zmiany hasła obiektu zdefiniowanego w usłudze katalogowej.

Komendy

Komenda	Opis
DN	Parametr DN (Distinguished Name) usługi katalogowej.
FILTER	Filtr użytkowników usługi katalogowej.

Informacja: Modyfikatory haseł oparte o warstwę transportową LDAP, mogą mieć zdefinowaną tylko jedną komendę.

Zmienne

Zmienna	Opis
transport_base	Parametr *base DN* usługi katalogowej.
transport_bind_ip	Adres IP Fudo, wykorzystywany do nawiązania połączenia z systemem docelowym.
transport_ca_certificate	Certyfikat CA systemu docelowego.
transport_domain	Domena służąca do logowania do systemu docelowego.
transport_encoding	Kodowanie tekstu na systemie docelowym.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_login	Nazwa konta na systemie docelowym, uprawnionego do zmiany hasła.
transport_port	Numer portu, służący do nawiązania połączenia z systemem docelowym.
transport_secret	Sekret służący do uwierzytelnienia konta wykorzystywanego w procesie zmiany hasła.
transport_server_certificate	Certyfikat serwera docelowego.
account_domain	Domena użytkownika, któremu jest zmieniane hasło.
account_new_secret	Zmienna systemowa, inicjowana wartością automatycznie wygenerowaną przez Fudo.

13.3.3 Telnet

Tryb połączenia Telnet, wykorzystuje protokół *Telnet* w celu nawiązania połączenia ze zdalnym systemem w celu zmiany hasła.

Komendy

Komenda	Opis
INPUT	Komenda wykonana na zdalnym systemie.
EXPECTED	Oczekiwany rezultat wykonania komendy.
ENTER	
DELAY	Opóźnienie pomiędzy wykonanywanymi komendami.

Zmienne

Zmienna	Opis
transport_bind_ip	Adres IP używany przez Fudo przy komunikacji ze zdalnym systemem.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_login	Nazwa konta na systemie docelowym, uprawnionego do zmiany hasła.
transport_port	Numer portu, służący do nawiązania połączenia z systemem docelowym.
transport_secret	Sekret służący do uwierzytelnienia konta wykorzystywanego w procesie zmiany hasła.
account_login	Login użytkownika, któremu jest zmieniane hasło.
account_new_secret	Zmienna systemowa, inicjowana wartością automatycznie wygenerowaną przez Fudo.

13.3.4 WinRM

Warstwa transportowa WinRM wykorzystuje protokół Windows Remote Management w celu nawiązania połączenia ze zdalnym systemem. Warstwa transportowa WinRM jest kompatybilna z Listą unieważnionych certyfikatów (listą CRL), co powoduje, że używane certyfikaty są potwierdzone i ważne.

Informacja: Domyślnie, Modyfikator oraz Weryfikator haseł na bazie warstwy transportowej WinRM, działają tylko dla użytkowników *lokalnych*. W celu konfiguracji Modyfikatora oraz Weryfikatora haseł WinRM dla użytkowników *domenowych*, należy dodać ich do grupy "Allow log on locally".

Komendy

Komenda	Opis
INPUT	Komenda wykonana na zdalnym systemie.
EXPECTED	Oczekiwany rezultat wykonania komendy.
ENTER	
DELAY	Opóźnienie pomiędzy wykonanywanymi komendami.

Zmienne

Ostrzeżenie: Aby skonfigurować modyfikator haseł **WinRM**, musisz podać dane uwierzytelniające użytkownika z uprawnieniami do zmiany haseł (zwykle konto na poziomie administratora). Nie należy używać tego konta do zmiany własnego hasła, ponieważ WinRM zwróci błąd, którego Fudo PAM nie może obsłużyć. **Upewnij się, że zmienne account_login i transport_login mają różne wartości.**

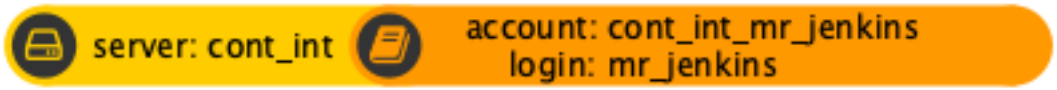
Zmienna	Opis
transport_bind_ip	Adres IP używany przez Fudo przy komunikacji ze zdalnym systemem.
transport_ca_certificate	Certyfikat CA systemu docelowego.
transport_encoding	Kodowanie tekstu na systemie docelowym.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_login	Nazwa konta na systemie docelowym, służącego do zmiany hasła. Wskazane konto musi być różne od konta, na którym jest zmieniane hasło (zmienna account_login).
transport_port	Numer portu, służący do nawiązania połączenia z systemem docelowym.
transport_secret	Sekret służący do uwierzytelnienia konta wykorzystywanego w procesie zmiany hasła.
account_login	Login użytkownika, któremu jest zmieniane hasło.
account_new_secret	Zmienna systemowa, inicjowana wartością automatycznie wygenerowaną przez Fudo.

Tematy pokrewne:

- *Uniwersalne modyfikatory haseł*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

13.4 Konfigurowanie modyfikatora haseł Unix poprzez SSH

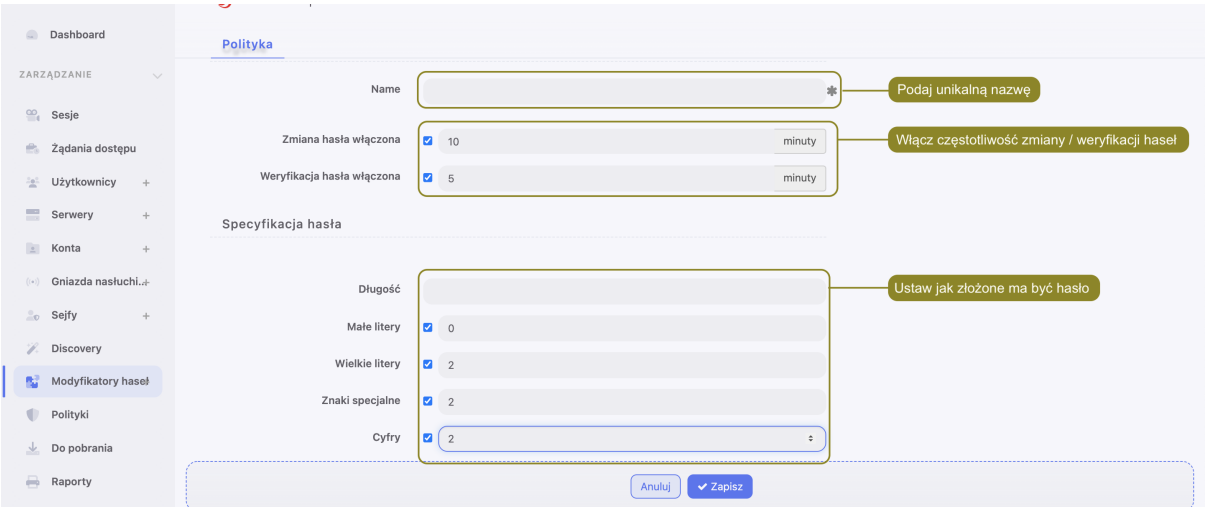
W tym rozdziale przedstawiony jest przykład konfigurowania automatycznej zmiany hasła konta *mr_jenkins* na serwerze Unix *cont_int*. Konto użytkownika *mr_jenkins*, w lokalnej bazie danych Fudo reprezentowane jest poprzez obiekt konta o nazwie *cont_int_mr_jenkins*.



Zmiana hasła zachodzi z użyciem konta uprzywilejowanego *root* zdefiniowanego ręcznie jako parametr warstwy transportowej.

Dodanie polityki zmiany haseł

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



3. Wprowadź nazwę polityki zmany haseł.

Informacja: Opisowa nazwa pozwoli osobom administrującym 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 i weryfikatora haseł do konta uprzywilejowanego

1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Znajdź i kliknij wybrany obiekt.
3. Kliknij *+ Dodaj modyfikator hasła*.
4. Wybierz z listy rozwijalnej *Modyfikator hasła*, wybierz `Unix/SSH changer`.
5. Określ limit czasowy wykonania skryptu.
6. Zweryfikuj domyślnie przypisane wartości zmiennych i w razie potrzeby, uzupełnij brakujące informacje.

Zmienna	Wartość
transport_bind_ip	`cont_int: Dowolny`
transport_host	`cont_int: 10.0.0.12`
transport_host_public_key	`cont_int: ssh-rsa AAA[...]`
transport_login	*Wprowadź ręcznie:* `root`
transport_method	*Wprowadź ręcznie:* `password`
transport_password_prompt	`stała`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`
account_login	`cont_int_mr_jenkins: mr_jenkins`

Informacja:

- Zmienne z przedrostkiem `transport_` stanowią parametry połączenia z serwerem docelowym, wykorzystywane przez warstwę transportową.
- Zmienne mogą być zainicjowane wartościami z innych obiektów, lub wprowadzone ręcznie.

7. Kliknij *+ Dodaj weryfikator hasła*.
8. Z listy rozwijalnej *Weryfikator hasła* wybierz opcję `Unix/SSH verifier (verify)`.
9. Określ limit czasowy wykonania skryptu.
10. Zweryfikuj domyślnie przypisane wartości zmiennych i w razie potrzeby, uzupełnij brakujące informacje.

Zmienna	Wartość
transport_bind_ip	`cont_int: Dowolny`
transport_host	`cont_int: 10.0.0.12`
transport_host_public_key	`cont_int: ssh-rsa AAA[...]`
transport_login	`cont_int_mr_jenkins: mr_jenkins`
transport_method	`cont_int_mr_jenkins: hasłem`
transport_password_prompt	`stała`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`

11. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tryby połączenia*
- *Uniwersalne modyfikatory haseł*

13.5 Wtyczki

Wtyczki umożliwiają wygodne tworzenie i wdrażenie zaawansowanych modyfikatorów haseł.

13.5.1 Tworzenie wtyczek

Wtyczki umożliwiają wygodne tworzenie i wdrażanie zaawansowanych modyfikatorów haseł.

13.5.1.1 Środowisko

Do tworzenia wtyczek niezbędne jest środowisko programistyczne, którego podstawę stanowi system operacyjny FreeBSD w wersji właściwej dla danego wydania Fudo (10.4 dla Fudo 3.11), oraz Python 3.6.

Struktura katalogowa środowiska:

```
  /
  |-- bin
  |-- dev
  |-- etc
  |-- lib
  |-- libexec
* |-- plugin
  |-- sbin
* |-- tmp
  `-- usr
          |-- bin
          |-- lib
*         |-- local
          `-- sbin
```

Archiwum wtyczki rozpakowane jest w katalogu `/plugin`. Interpreter języka Python znajduje się w `/usr/local`. Katalog `/tmp` może służyć do przechowywania plików tymczasowych. Jego rozmiar nie może przekroczyć 10 MB a zawartość jest czyszczona po każdym wykonaniu skryptu.

Tematy pokrewne:

- *Struktura wtyczki*
- *Przygotowanie wtyczki*
- *Uniwersalne modyfikatory haseł*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

13.5.1.2 Struktura wtyczki

Wtyczka stanowi archiwum plików, w skład którego wchodzą:

- *manifest.json*
- *skrypt change*
- *skrypt verify*
- *kod modyfikujący/weryfikujący hasło*

Ostrzeżenie: Rozmiar skompresowanego archiwum nie może przekraczać 10 MB. Po rozpakowaniu, sumaryczny rozmiar plików wtyczki nie może przekraczać 100 MB.

13.5.1.2.1 manifest.json

Manifest deklaruje kluczowe meta dane wtyczki oraz zmienne wykorzystywane przez modyfikator oraz weryfikator haseł.

Parametr	Opis
`name`	Unikatowa nazwa umożliwiająca jednoznaczną identyfikację wtyczki.
`plugin_version`	Wersja wtyczki. **Informacja:** Producent sugeruje zastosowanie wersjonowania semantycznego *MAJOR.MINOR.PATCH* opisanego na stronie https://semver.org/.
`type`	Zarówno w przypadku modyfikatora jak i weryfikatora, typem powinien być `password_changer`.
`engine_version`	Fudo PAM zapewnia środowisko wykonywania wtyczek w określonej wersji. Wtyczka wymaga zadeklarowania kompatybilnej wersji silnika.
`timeout`	Maksymalny czas wykonania skryptu, wyrażony w sekundach. W przypadku gdy skrypt modyfikujący/weryfikujący hasło nie wykona się prawidłowo w wyznaczonym czasie, proces odpowiedzialny za jego wykonanie zostanie zakończony a próba zmiany/weryfikacji hasła zostanie uznana za nieudaną.

Manifest definiuje także listę zmiennych modyfikatora i weryfikatora haseł odpowiednio w sekcji `change` i `verify`. Zmienne mogą odwoływać się do obiektów modelu danych lub być definiowane ręcznie. Definicja zmiennej opisana jest następującą strukturą:

Parametr	Typ	Wymagany	Opis
`name`	string	✔	Nazwa zmiennej.
`description`	string	✘	Opis zmiennej.
`required`	boolean	✔	Specyfikacja obowiązku zdefiniowania zmiennej.
`object_type`	string	✘	Typ obiektu, do której odwołuje się zmienna.
`object_property`	string	✘	Parametr obiektu, którego wartość zostanie użyta do zainicjowania zmiennej.
`encrypt`	boolean	?	Specyfikator szyfrowania zmiennej w bazie danych. Wymagane, w przypadku gdy nie zostały określone `object_type` oraz `object_property`.

Dostępne obiekty i ich właściwości

Obiekt/parametr	Opis
`server`	Obiekt *serwer* zdefiniowany w lokalnej bazie danych.
`name`	Nazwa obiektu.
`bind_ip`	Adres IP Fudo PAM wykorzystany do komunikacji z serwerem.
`ca_certificate`	Certyfikat CA.
`port`	Numer portu, na którym nasłuchuje serwer docelowy.
`protocol`	Protokół komunikacji z serwerem docelowym: `citrixsf`, `http`, `ica`, `modbus`, `mysql`, `oracle`, `rdp`, `ssh`, `system`, `tcp`, `tds`, `telnet`, `tn3270`, `tn5250`, `vnc`.
`secproto`	Protokół bezpieczeństwa używany przez serwer RDP: `nla`, `tls`, `std`.
`ssl_to_server`	`1` jeśli serwer korzysta z szyfrowania SSL/TLS, `0` jeśli SSL/TLS nie jest wykorzystywany.
`ssl_v2`	`1` jeśli protokół SSL w wersji 2.0 może zostać użyty do komunikacji z serwerem docelowym, `0` jeśli komunikacja z serwerem poprzez protokół SSL 2.0 nie jest dopuszczalna.
`ssl_v3`	`1` jeśli protokół SSL w wersji 3.0 może zostać użyty do komunikacji z serwerem docelowym, `0` jeśli komunikacja z serwerem poprzez protokół SSL 3.0 nie jest dopuszczalna.
`subnet`	Specyfikacja podsieci podawana w przypadku serwerów dynamicznych, np. `192.168.0.0/24`

Obiekt/parametr	Opis
`server_address`	Adres IP serwera. W przypadku serwerów dynamicznych, pojedynczy obiekt może mieć przypisanych wiele adresów IP.
`host`	Adres serwera.
`certificate`	Certyfikat dla danego adresu IP serwera.
`public_key`	Klucz publiczny SSH dla danego adresu IP.

`account`	Obiekt *konto* zdefiniowany w lokalnej bazie danych.
`name`	Nazwa obiektu.
`description`	Opis obiektu.
`login`	Login konta uprzywilejowanego na monitorowanym serwerze.
`method`	Metoda uwierzytelnienia, przyjmuje wartość hasła lub klucz SSH.
`secret`	Sekret używany w procesie uwierzytelnienia.

Przykład:

```
{
  "name": "Redmine",
  "plugin_version": "1.0.3",
  "type": "password changer",
  "engine_version": "1.0.0",
  "timeout": "300",
  "change":
  {
        "variables":
        [
          {
                "name": "transport_login",
                "description": "User name used to login to account.",
                "required": true,
                "object_type": "account",
                "object_property": "login"
          },
          {
                "name": "transport_secret",
                "description": "A secret to be used when logging in.",
                "required": true,
                "object_type": "account",
                "object_property": "secret"
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
          },
          {
                "name": "transport_host",
                "description": "Host name or IP address. IPv4 and IPv6 are both␣
↪supported.",
                "required": true,
                "object_type": "server_address",
                "object_property": "host"
          },
          {
                "name": "account_login",
                "description": "User name for which to change password.",
                "required": true,
                "object_type": "account",
                "object_property": "login"
          }
        ]
  },
  "verify":
  {
        "variables":
        [
          {
                "name": "transport_login",
                "description": "User name used to login to account. This user's␣
↪password will be verified.",
                "required": true,
                "object_type": "account",
                "object_property": "login"
          },
          {
                "name": "transport_secret",
                "description": "A secret that will be verified.",
                "required": true,
                "object_type": "account",
                "object_property": "secret"
          },
          {
                "name": "transport_host",
                "description": "Host name or IP address. IPv4 and IPv6 are both␣
↪supported.",
                "required": true,
                "object_type": "server_address",
                "object_property": "host"
          }
        ]
  }
}
```

13.5.1.2.2 Skrypt change

Skrypt inicjujący wykonanie właściwego kodu zmieniającego hasła.

Przykład:

```
#!/bin/sh
CURR_DIR="$(realpath $(dirname "${0}"))"

echo "Script located in '${CURR_DIR}' directory."

export PYTHONPATH="${CURR_DIR}/site-packages"
python3 "${CURR_DIR}/redmine_changer.py" change
```

13.5.1.2.3 Skrypt verify

Skrypt inicjujący wykonanie właściwego kodu weryfikującego hasła.

Przykład:

```
#!/bin/sh
CURR_DIR="$(realpath $(dirname "${0}"))"

echo "Script located in '${CURR_DIR}' directory."

export PYTHONPATH="${CURR_DIR}/site-packages"
python3 "${CURR_DIR}/redmine_changer.py" verify
```

13.5.1.2.4 Kod modyfikujący hasło

Informacja: Wszelkie zmienne zadeklarowane w pliku `manifest.json` dostępne są poprzez zmienne środowiskowe. Oprócz nich, funkcjonuje zmienna specjalna `account_new_secret`, dostępna tylko w skrypcie modyfikującym hasło. Zmienna inicjowana jest wartością wygenerowaną automatycznie przez Fudo PAM.

Przykład odwołania się do zmiennej:

```
import os

print('New secret: {}'.format(os.environ['account_new_secret']))
```

Przykład kodu w języku Python zmieniającego hasło do serwisu Redmine za pomocą REST API:

```
import os
import sys

import requests


MODE_CHANGE = 1
MODE_VERIFY = 2


def eprint(*args, **kwargs):
        print(*args, file=sys.stderr, **kwargs)
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
class RedmineChangerError(Exception):
        pass


def redmine_get_user_id(server_uri, admin_login, admin_password, user_login):
        req = requests.get(
                server_uri + '/users.json',
                params={'name': user_login},
                auth=(admin_login, admin_password),
                verify=False,
        )
        if req.status_code != 200:
                raise RedmineChangerError(
                        'HTTP status code {} from {}.'.format(req.status_code,␣
↪server_uri)
                )

        user_list = [x for x in req.json()['users'] if x['login'] == user_login]
        if len(user_list) > 1:
                raise RedmineChangerError(
                        'Ambigious answer from {}: Multiple users with "{}" login'.
↪format(
                                server_uri, user_login
                        )
                )
        if len(user_list) < 1:
                raise RedmineChangerError(
                        'Response from {} doesn\'t contain user with login "{}"'.
↪format(
                                server_uri, user_login
                        )
                )

        try:
                user_id = user_list[0]['id']
        except KeyError:
                raise RedmineChangerError(
                        'Response from {} doesn\'t contain "id".'.format(server_uri)
                )
        return user_id


def redmine_set_user_password(
        server_uri, admin_login, admin_password, user_id, user_password
):
        uri = '{}/users/{}.json'.format(server_uri, user_id)
        req = requests.put(
                uri,
                json={'user': {'password': user_password}},
                auth=(admin_login, admin_password),
                verify=False,
        )
        if req.status_code != 200:
                raise RedmineChangerError(
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
                        'HTTP status code {} from {}.'.format(req.status_code,␣
↪server_uri)
                )


# https://redmine.hostonly.vm/users/current.json
def redmine_get_current_user_login(server_uri, admin_login, admin_password):
        req = requests.get(
                server_uri + '/users/current.json',
                auth=(admin_login, admin_password),
                verify=False,
        )
        if req.status_code != 200:
                raise RedmineChangerError(
                        'HTTP status code {} from {}.'.format(req.status_code,␣
↪server_uri)
                )

        try:
                login = req.json()['user']['login']
        except KeyError:
                raise RedmineChangerError('Unable to get "user.login".')

        return login


def change(
        transport_login,
        transport_secret,
        transport_uri,
        account_login,
        account_new_secret,
):
        try:
                user_id = redmine_get_user_id(
                        transport_uri, transport_login, transport_secret, account_
↪login
                )
        except RedmineChangerError as err:
                print('Error getting user id: {}'.format(err), file=sys.stderr)
                return 1

        print('User "{}" has id {}.'.format(account_login, user_id))

        try:
                redmine_set_user_password(
                        transport_uri,
                        transport_login,
                        transport_secret,
                        user_id,
                        account_new_secret,
                )
        except RedmineChangerError as err:
                print('Error setting user password: {}'.format(err), file=sys.stderr)
                return 1
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        print('Successfully changed password for user "{}".'.format(account_login))
        return 0


def verify(transport_login, transport_secret, transport_uri):
        try:
                login = redmine_get_current_user_login(
                        transport_uri, transport_login, transport_secret
                )
        except RedmineChangerError as err:
                print(
                        'Error getting current user login: {}'.format(err), file=sys.
↪stderr
                )
                return 1

        if login != transport_login:
                print(
                        'Server {} returned wrong login "{}" - expected "{}".'.
↪format(
                                transport_uri, login, transport_login
                        ),
                        file=sys.stderr,
                )
                return 1

        print('Successfully logged in as "{}".'.format(transport_login))
        return 0


# TODO: There are some improvements that we can implement in future versions of
# plugin to test update procedure:
# - respect TLS: at the moment we assume TLS is on and connect using HTTPS,
# - verify server certificate,
# - optionally, get port of the server.
def main():
        if len(sys.argv) != 2:
                print('Provide "change" or "verify" as plugin mode', file=sys.stderr)
                sys.exit(1)

        if sys.argv[1] == 'change':
                mode = MODE_CHANGE
        elif sys.argv[1] == 'verify':
                mode = MODE_VERIFY
        else:
                print('Incorrect plugin mode: "{}".'.format(sys.argv[1]))
                sys.exit(1)

        transport_login = os.environ['transport_login']
        transport_secret = os.environ['transport_secret']
        transport_uri = 'https://' + os.environ['transport_host']
        if mode == MODE_CHANGE:
                account_login = os.environ['account_login']
                account_new_secret = os.environ['account_new_secret']

        result = 1
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
        if mode == MODE_CHANGE:
                result = change(
                        transport_login,
                        transport_secret,
                        transport_uri,
                        account_login,
                        account_new_secret,
                )
        else:
                result = verify(transport_login, transport_secret, transport_uri)

        sys.exit(result)


if __name__ == '__main__':
        main()
```

Informacja: Prawidłowo wykonany kod powinien na wyjściu zwrócić wartość 0. Każda inna wartość będzie zinterpretowana jako zmiana/weryfikacja wykonana niepomyślnie.

Tematy pokrewne:

- *Środowisko*
- *Przygotowanie wtyczki*
- *Uniwersalne modyfikatory haseł*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

13.5.1.3 Przygotowanie wtyczki

Przygotowanie przykładowej wtyczki do wgrania wymaga skopiowania skopiowania zawartości katalogu do katalogu roboczego i zainstalowania `requests` w podkatalogu `site-packages`.

```
mkdir /tmp/workdir-redmine
cp -a core/usr.local.share/plugins/ex02-redmine/* /tmp/workdir-redmine
cd /tmp/workdir-redmine
pip3 install -t site-packages requests
zip /tmp/ex02-redmine.zip -9r *
```

Tematy pokrewne:

- *Środowisko*
- *Struktura wtyczki*
- *Uniwersalne modyfikatory haseł*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

Tematy pokrewne:

- *Uniwersalne modyfikatory haseł*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

13.5.2 Wgrywanie wtyczek

1. Wybierz z lewego menu *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.
3. Kliknij *Wgraj*.
4. Wskaż plik wtyczki w lokalnym systemie plików.
5. *Zdefiniuj politykę haseł* i *dodaj modyfikator do konta*.

Tematy pokrewne:

- *Uniwersalne modyfikatory haseł*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

Tematy pokrewne:

- *Uniwersalne modyfikatory haseł*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

ROZDZIAŁ 14

Polityki

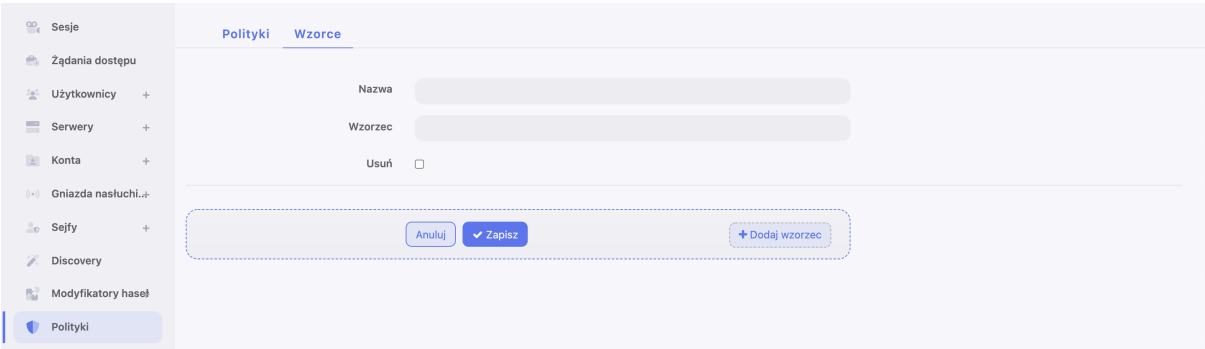
Polityki to grupy definicji wzorców pozwalające na proaktywny monitoring przebiegu sesji. W przypadku wykrycia wzorca, Fudo PAM pozwala na automatyczne wstrzymanie sesji, zakończenie połączenia, zablokowanie użytkownika i wysłanie stosownego powiadomienia do administratora.

Definiowanie wzorców

Informacja: Fudo PAM wspiera wyrażenia regularne opisane standardem *POSIX Extended*.

---

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



4. Zdefiniuj nazwę i ciąg znaków stanowiący wzorzec.

Informacja: 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 Fudo PAM podejmie z chwilą stwierdzenia wystąpienia któregoś ze wzorców.

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

Informacja:

- Wysyłanie powiadomień wymaga skonfigurowania *usługi powiadomień* oraz zaznaczonej opcji *Wykrycie wzorca* w *ustawieniach sejfu*.
- Zablokowanie użytkownika powoduje automatyczne przerwanie połączenia.

---

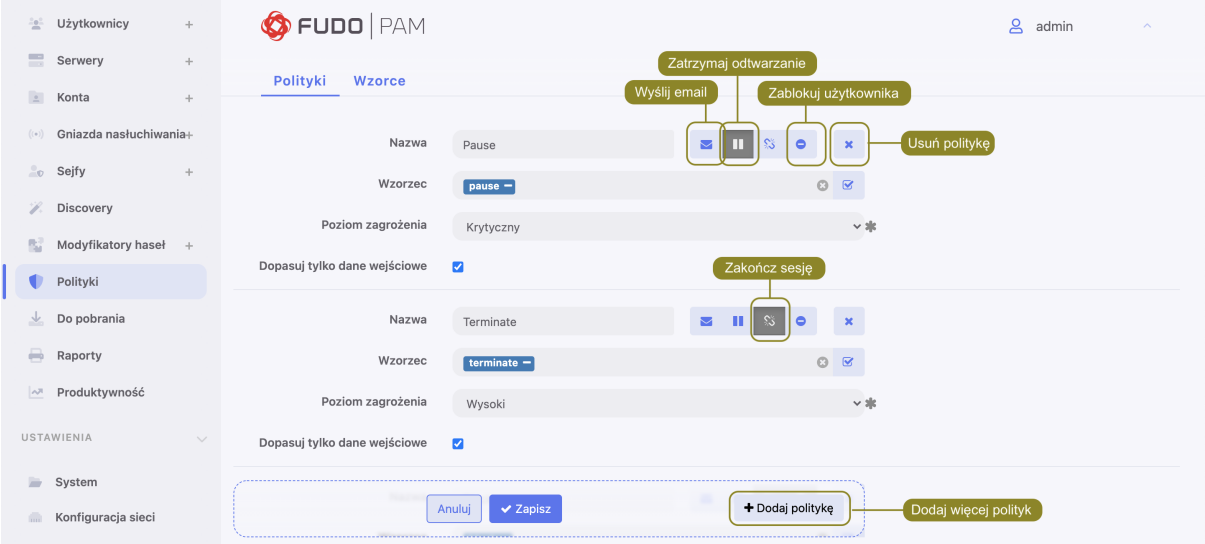
5. Wybierz wzorce śledzone w ramach danej polityki.
6. Określ poziom zagrożenia dla dodawanej polityki.

Informacja: Informacja o poziomie zagrożenia zawarta jest w treści powiadomienia.

---

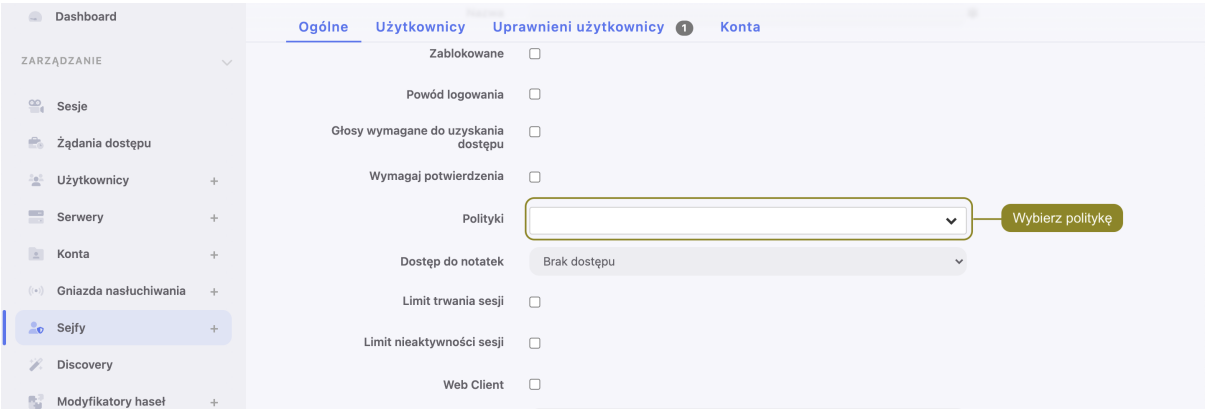
7. Zaznacz opcję *Dopasuj tylko dane wejściowe*, aby system reagował tylko na treści wprowadzone przez użytkownika.

Informacja: W przypadku protokołów RDP, VNC i MySQL, przetwarzaniu podlegają tylko dane wejściowe.



8. Kliknij *Zapisz*.

Informacja: Po utworzeniu polityki, przypisz ją do wybranego *sejfu*.



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:

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

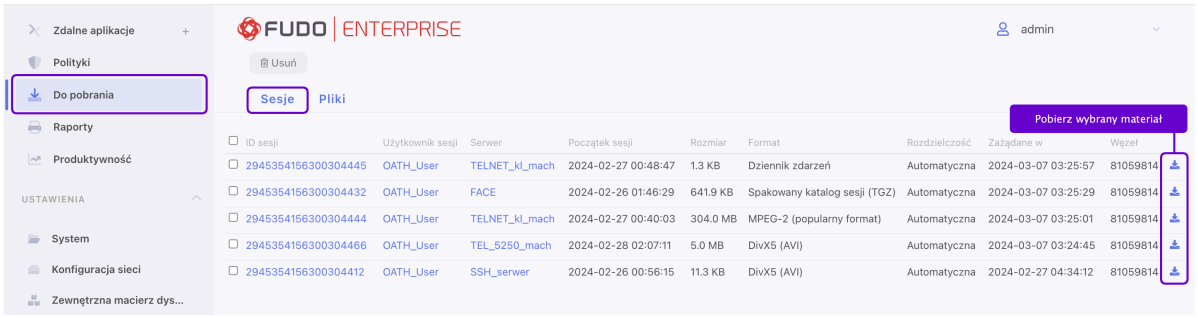
ROZDZIAŁ 15

Do pobrania

Zakładka **Do pobrania** umożliwia śledzenie postępu konwersji wskazanych wcześniej do pobrania nagrań sesji oraz plików przesyłanych podczas sesji SFTP.

15.1 Sesje

Fudo PAM pozwala na konwersję zapisanej sesji do jednego ze wspieranych formatów wyjściowych. Zakładka **Sesje** jest przeznaczona do zarządzania nagraniami sesji, które wcześniej zostały wybrane do pobrania w zakładce Zarządzanie > Sesje. Szczegółowa instrukcja eksportowania sesji znajduje się w rozdziale *Eksportowanie sesji*.



15.2 Pliki

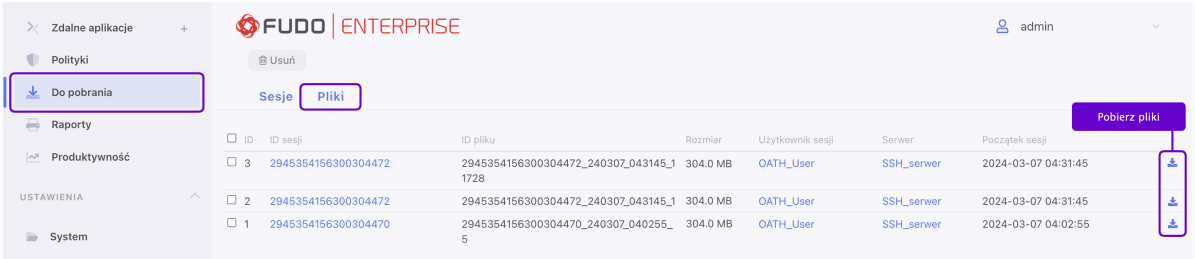
Zakładka **Pliki** jest przeznaczona do zarządzania pobieraniem dużych plików pochodzących z sesji SFTP. Jeśli rozmiar wybranego pliku przekracza 50 MB, przechodzi on proces konwersji i w następnym kroku jest gotowy do pobrania w zakładce **Pliki**. Pliki mniejsze niż 50 MB są pobierane bezpośrednio przez przeglądarkę bez konwersji.

Aby pobrać plik transferowany podczas sesji SFTP, należy zainicjować jego pobranie z poziomu odtwarzacza sesji. W celu wyświetlenia wybranej sesji SFTP, postępuj według poniższych kroków:

1. Wybierz *Zarządzanie* > *Sesje*.
2. Znajdź żądaną sesję SFTP i kliknij ikonę odtwarzania obok niej.
3. W oknie odtwarzacza prześledź historię sesji, aby odnaleźć żądany plik do pobrania, a następnie kliknij przycisk **File**, aby zainicjować proces.

Informacja: UWAGA: Aby pobrać cały plik, należy użyć przycisku **File**.

4. Wybierz *Zarządzanie* > *Do pobrania*.
5. Przejdź do zakładki **Pliki**.
6. Kliknij i, aby pobrać wybrany materiał.



Tematy pokrewne:

- *Eksportowanie sesji*
- *Sesje*

ROZDZIAŁ 16

Aktywność konta w Portalu Użytkownika

Fudo PAM pozwala być informowanym o istniejących połączeniach przez Portal Użytkownika.

Funkcjonalność ta działa podczas nawiązywania połączenia do serwera docelowego, kiedy inny użytkownik jest już do niego połączony. Jeśli użytkownik kontynuuje nawiązanie połączenia, obecna sesja zostaje przerwana.

Ostrzeżenie: Funkcjonalność jest dostępna tylko dla połączeń RDP.

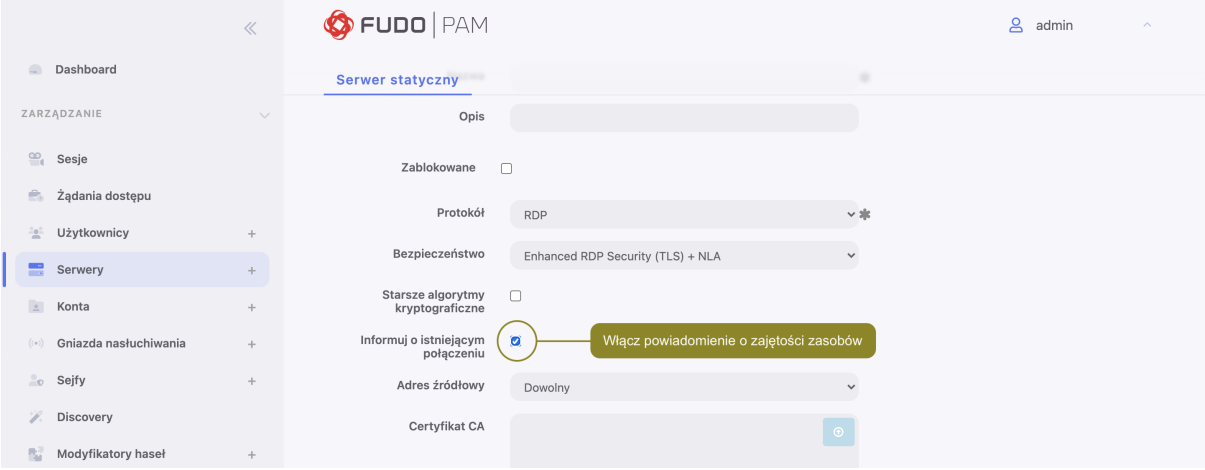
W celu konfiguracji funkcjonalności zajętości zasobów na poziomie serwera, postępuj zgodnie z instrukcją:

- Załóż nowy serwer, wybierając z lewego menu *Zarządzanie* > *Serwery*, kliknij + *Dodaj* i wybierz opcję *Serwer statyczny*. Skonfiguruj serwer RDP według procedury, opisanej na stronie *Dodawanie serwera RDP*,

  albo

  Wybierz serwer RDP, dla którego chcesz uruchomić tę opcję.

- W sekcji *Ogólne* zaznacz opcję *Informuj o istniejącym połączeniu*.

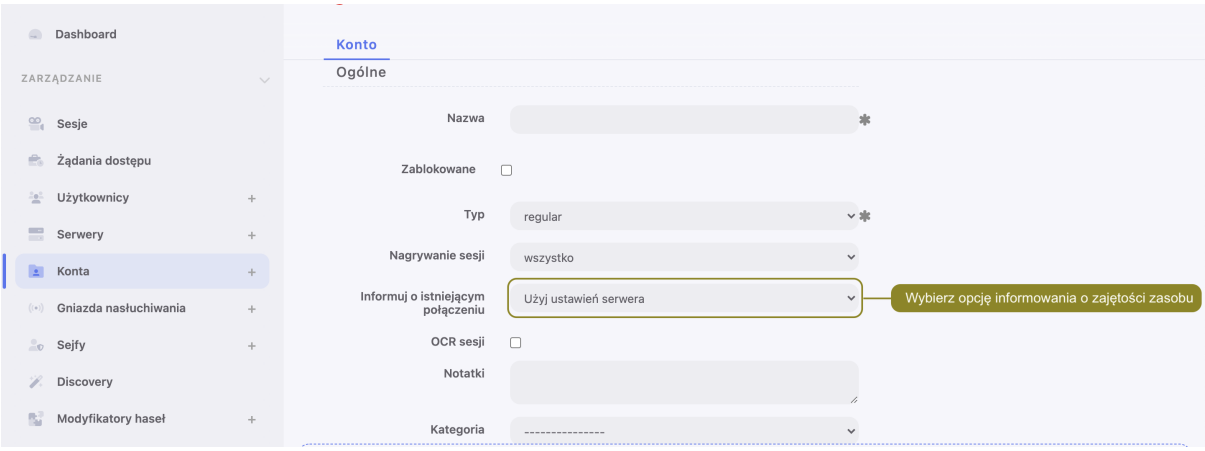


- Kliknij *Zapisz*.
- Konfigurując funkcjonalność zajętości zasobów na poziomie konta z dostępem do serwera RDP, w polu *Informuj o istniejącym połączeniu* ustaw jedną z trzech wartości:

`Użyj ustawień serwera` w celu użycia konfiguracji serwera RDP, dodanego w sekcji *Serwer*,

`Nie`, aby wyłączyć funkcjonalność,

`Tak`, aby włączyć funkcjonalność (niezależnie od ustawień serwera).



Informacja o zajętości zasobów będzie prezentowana na Portalu Użytkownika. Treść wiadomości jest domyślna, jednak też może być zdefiniowana przez administratora i dostosowana do potrzeb użytkownika. Dostosować treść wiadomości można zawierając zmienne `organization`, `phone`, `name`, `full_name`, albo `email` pomiędzy podwójnymi znakami %%. Na przykład, `%%email%%`.

- Wybierz *Ustawienia* > *Zasoby* > zakładkę *User portal*.
- Podaj tekst wiadomości w polu *Komunikat o zajętości zasobu*.
- Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie serwera RDP*
- *Ekran logowania Portalu użytkownika*

ROZDZIAŁ 17

Sesje

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 dostarcza także informacji statusowych na temat każdej z sesji oraz pozwala zarządzać wygenerowanymi wcześniej odnośnikami.

Informacja: Zawartość listy sesji uzależniona jest od uprawnień zalogowanego użytkownika. Aby użytkownik miał dostęp do określonej sesji, musi mieć stosowne uprawnienia do obiektów: serwera, konta, użytkownika i sejfu, wykorzystywanych w danym połączeniu.

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.
	Sprawdź status replikacji sesji.
	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*).
	Nazwa użytkownika, który zaakceptował sesję wymagającą autoryzacji.
✔	Akceptacja żądania oczekującego.
✖	Odrzucenie żądania oczekującego.
?	Żądanie oczekujące na akceptację.
✚	Element agregujący połączenia nawiązane w ramach tej samej sesji.
	Sesja *niepodlegająca retencji*.
	Status analizy behawioralnej sesji. *Jest to wersja ewaluacyjna komponentu AI.* ○ - sesja w trakcie analizy, wstępny wynik analizy - brak zagrożenia. ○ - sesja w trakcie analizy, wstępny wynik analizy - średni poziom zagrożenia. ○ - sesja w trakcie analizy, wstępny wynik analizy - wysoki poziom zagrożenia. ○ - sesja oczekuje na analizę lub jest wstępnie przetwarzana. - sesja nie poddana analizie z uwagi na brak wyuczonego modelu. ● - sesja przetworzona - brak zagrożenia. ● - sesja przetworzona - średni poziom zagrożenia. ● - sesja przetworzona - wysoki poziom zagrożenia. ● - sesja przetworzona - brak wyniku analizy.

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

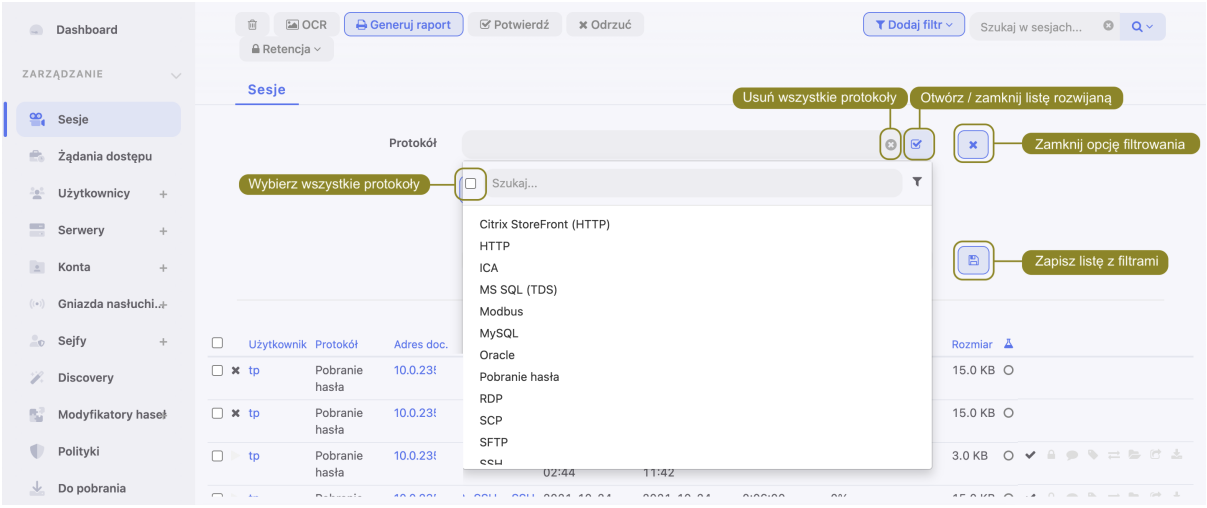
Informacja: Fudo PAM przechowuje materiał sesji w formie skompresowanej, z czego wynikać mogą różnice pomiędzy podawanym a faktycznym rozmiarem sesji.

17.1 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.

17.1.1 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.

---

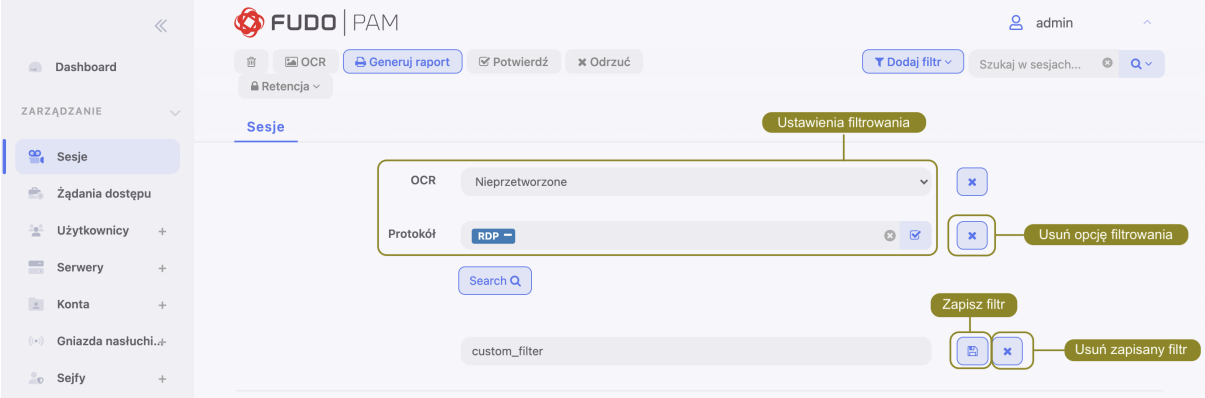
4. Kliknij *Dodaj filtr* i wybierz ponownie wcześniej zaznaczony parametr filtrowania, aby wyłączyć filtrowanie według zadanego parametru.

17.1.2 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 dyskietki, aby zapisać ustawienia.

Usuwanie definicji filtrowania

1. Kliknij *Dodaj filtr* i wybierz żądaną definicję filtrowania.
2. Kliknij ikonę usunięcia definicji filtrowania.
3. Potwierdź usunięcie wybranej definicji filtrowania.

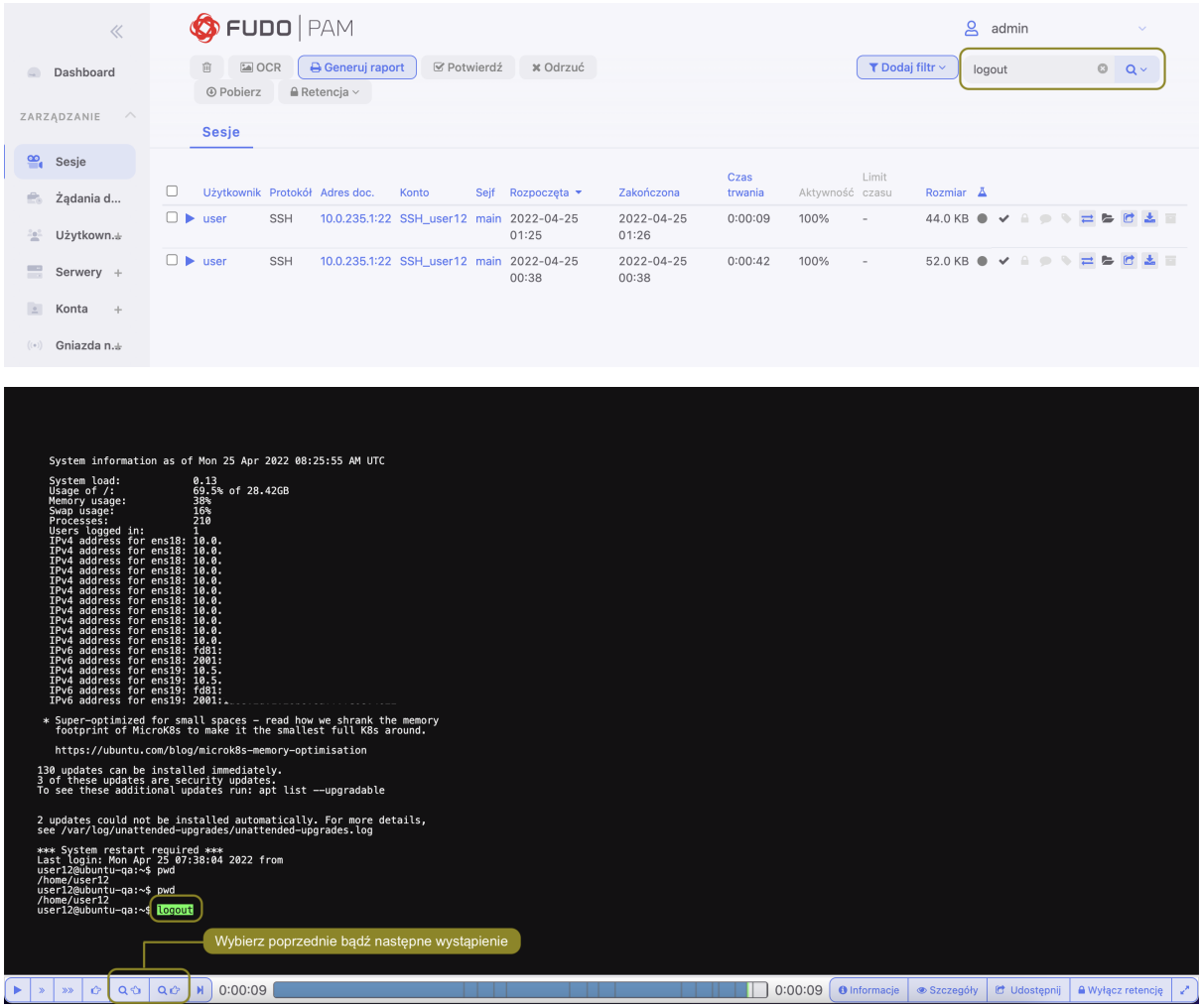
17.1.3 Przeszukiwanie pełnotekstowe

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

Informacja:

- Skorzystaj z wyszukiwarki listy Sesji, aby odnaleźć sesje zawierające ciąg znaków, np. „logout”.
- Odtwarzanie sesji znalezionych na podstawie wprowadzonej frazy rozpoczyna się w miejscu jej pierwszego wystąpienia.

Odtwarzacz pozwala na przeskakiwanie pomiędzy wystąpieniami wprowadzonego ciągu znaków.



Tematy pokrewne:

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

17.2 Odtwarzanie sesji

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

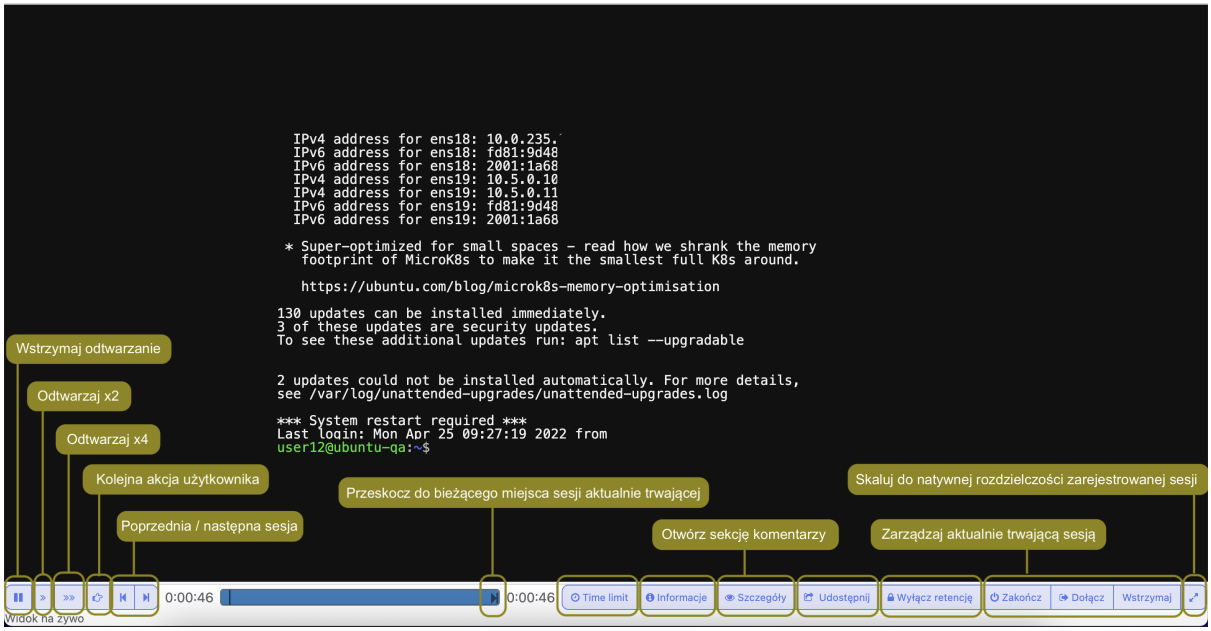
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Wyszukaj na liście żądaną sesję i kliknij ikonę rozpoczęcia odtwarzania.

Informacja: Użyj opcji filtrowania, aby wyświetlić sesje aktywne:

- Kliknij *Dodaj filtr* i z listy wybierz *Aktywne*.
- Z listy rozwijalnej wybierz *Tak*.

Opcje odtwarzacza

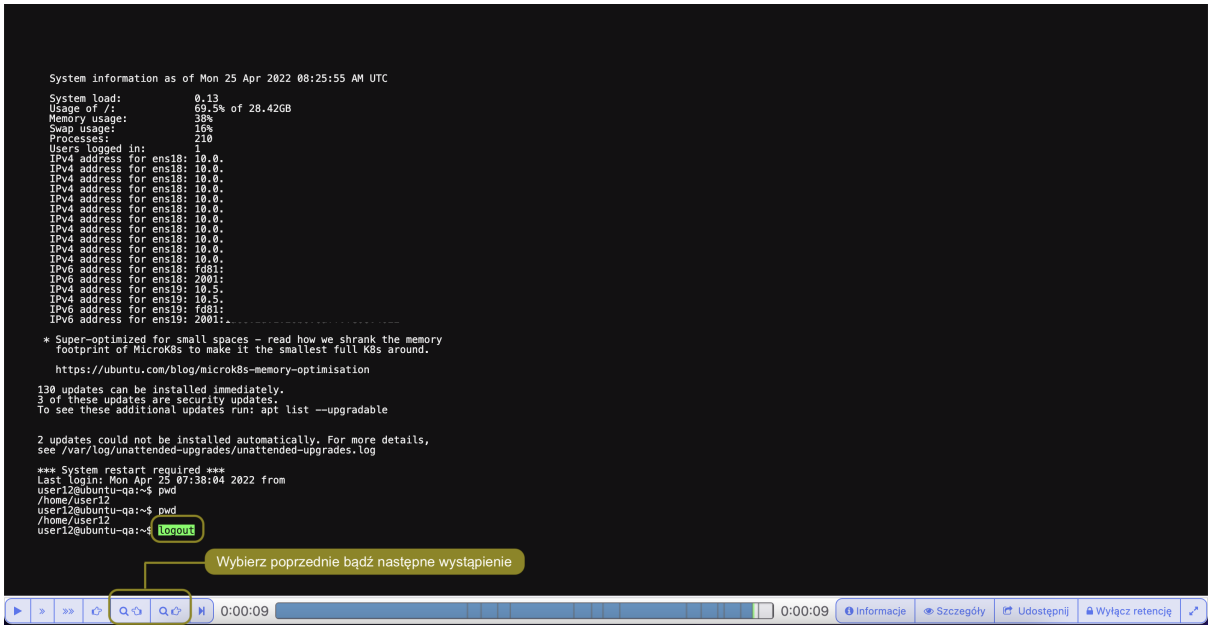
SSH, RDP, Telnet, X11



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

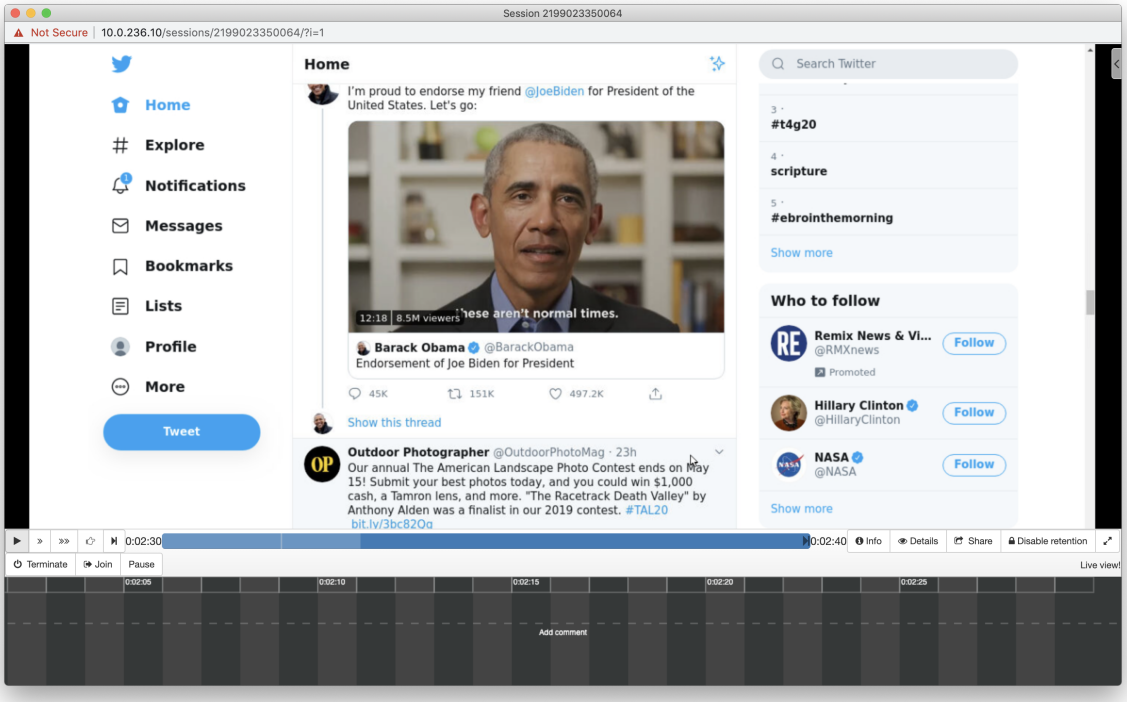
Informacja: Odtwarzanie sesji znalezionych na podstawie wprowadzonej frazy rozpoczyna się w miejscu jej pierwszego wystąpienia.

Odtwarzacz pozwala na przeskakiwanie pomiędzy wystąpieniami wprowadzonego ciągu znaków.



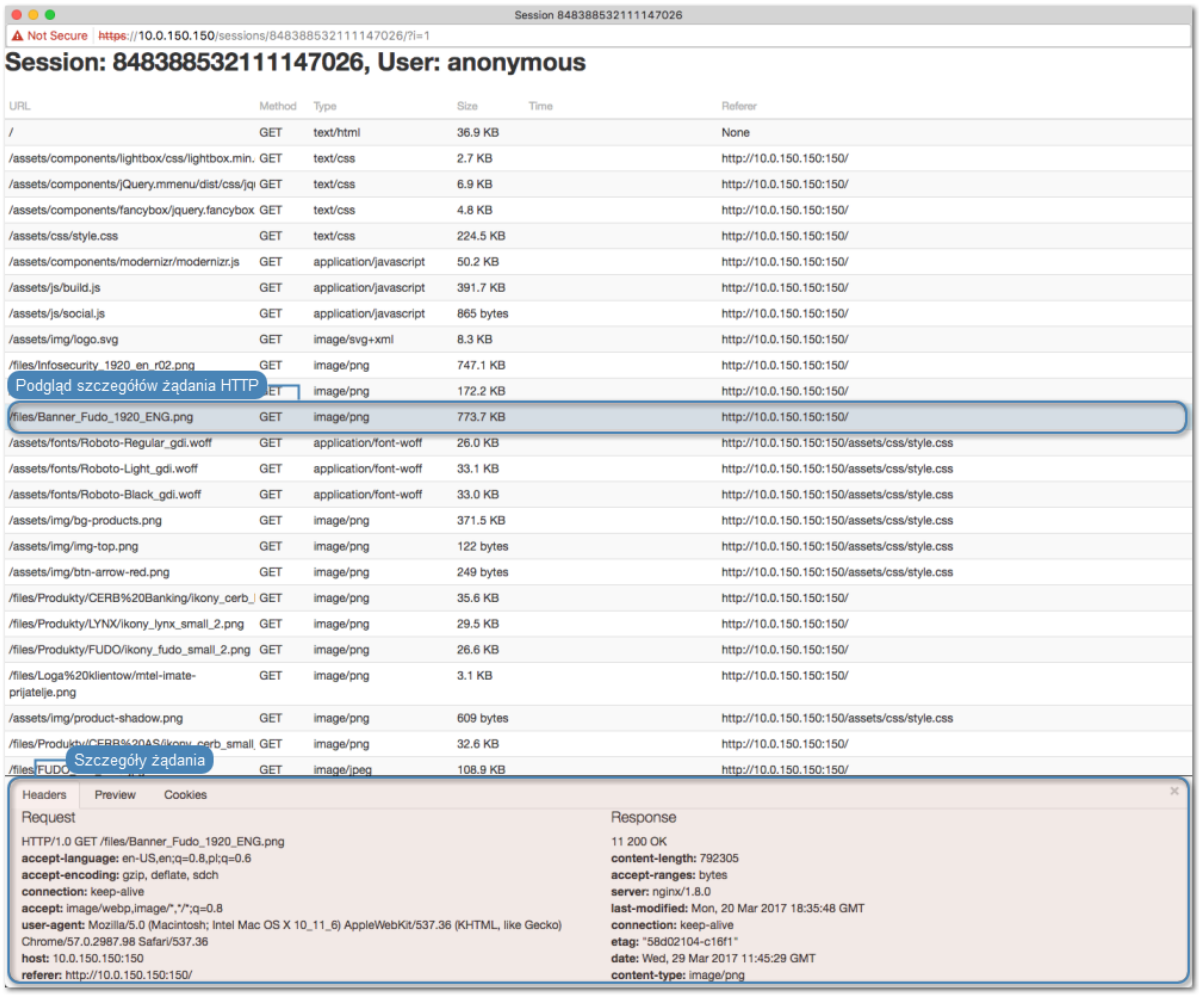
Informacja: Kliknij w zegar odmierzający czas odtwarzanej sesji, aby przełączyć pomiędzy czasem bezwzględnym i względnym.

HTTP - renderowane

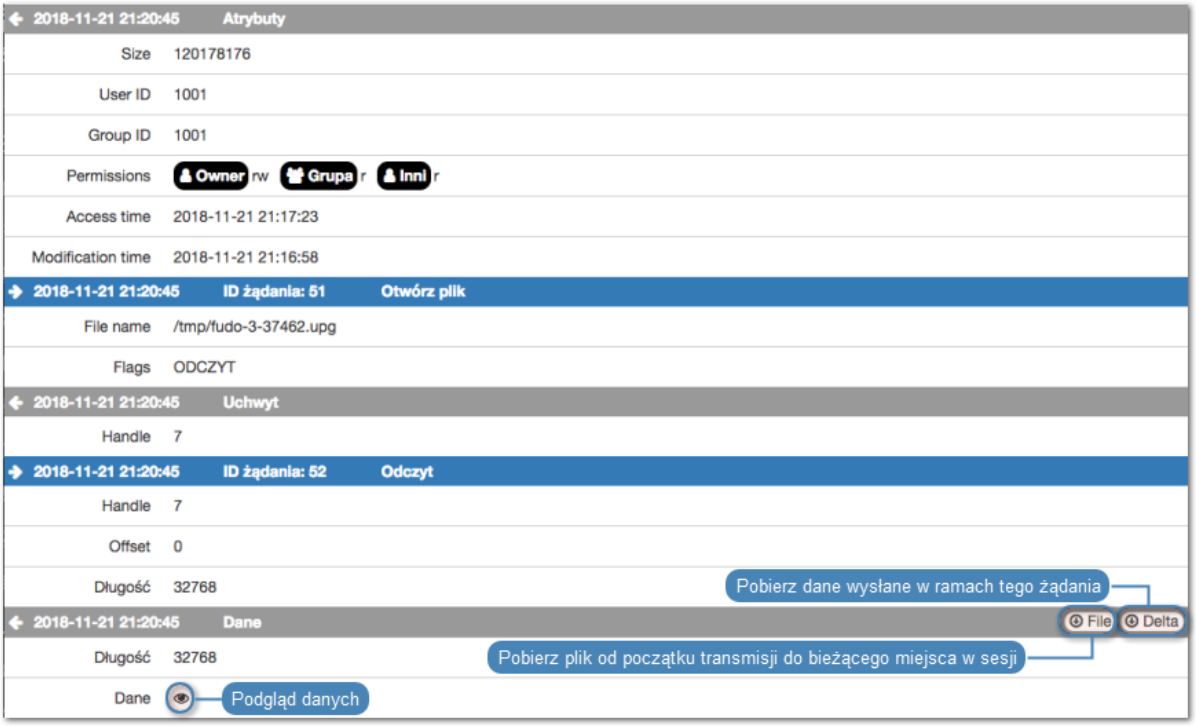


Informacja: W przypadku renderowanych sesji HTTP, surowy ruch nie jest rejestrowany.

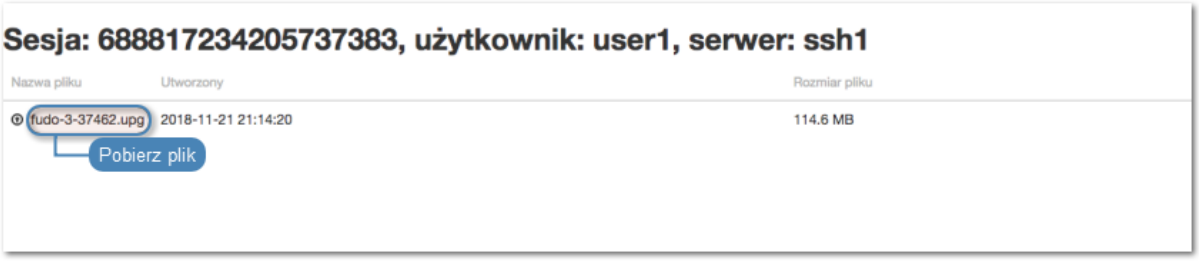
HTTP


Session 848388532111147026
Not Secure https://10.0.150.150/sessions/848388532111147026/?i=1
Session: 848388532111147026, User: anonymous
URL Method Type Size Time Referer
/ GET text/html 36.9 KB None
/assets/components/lightbox/css/lightbox.min. GET text/css 2.7 KB http://10.0.150.150:150/
/assets/components/jQuery.mmenu/dist/css/jq GET text/css 6.9 KB http://10.0.150.150:150/
/assets/components/fancybox/jquery.fancybox GET text/css 4.8 KB http://10.0.150.150:150/
/assets/css/style.css GET text/css 224.5 KB http://10.0.150.150:150/
/assets/components/modernizr/modernizr.js GET application/javascript 50.2 KB http://10.0.150.150:150/
/assets/js/build.js GET application/javascript 391.7 KB http://10.0.150.150:150/
/assets/js/social.js GET application/javascript 865 bytes http://10.0.150.150:150/
/assets/img/logo.svg GET image/svg+xml 8.3 KB http://10.0.150.150:150/
/files/Infosecurity_1920_en_r02.png GET image/png 747.1 KB http://10.0.150.150:150/
Podgląd szczegółów żądania HTTP
/files/Banner_Fudo_1920_ENG.png GET image/png 773.7 KB http://10.0.150.150:150/
/assets/fonts/Roboto-Regular_gdi.woff GET application/font-woff 26.0 KB http://10.0.150.150:150/assets/css/style.css
/assets/fonts/Roboto-Light_gdi.woff GET application/font-woff 33.1 KB http://10.0.150.150:150/assets/css/style.css
/assets/fonts/Roboto-Black_gdi.woff GET application/font-woff 33.0 KB http://10.0.150.150:150/assets/css/style.css
/assets/img/bg-products.png GET image/png 371.5 KB http://10.0.150.150:150/assets/css/style.css
/assets/img/img-top.png GET image/png 122 bytes http://10.0.150.150:150/assets/css/style.css
/assets/img/btn-arrow-red.png GET image/png 249 bytes http://10.0.150.150:150/assets/css/style.css
/files/Produkty/CERB%20Banking/ikony_cerb_ GET image/png 35.6 KB http://10.0.150.150:150/
/files/Produkty/LYNX/ikony_lynx_small_2.png GET image/png 29.5 KB http://10.0.150.150:150/
/files/Produkty/FUDO/ikony_fudo_small_2.png GET image/png 26.6 KB http://10.0.150.150:150/
/files/Loga%20klientow/mtel-imate-prijatelje.png GET image/png 3.1 KB http://10.0.150.150:150/
/assets/img/product-shadow.png GET image/png 609 bytes http://10.0.150.150:150/assets/css/style.css
GET image/png 32.6 KB http://10.0.150.150:150/
Szczegóły żądania
GET image/jpeg 108.9 KB http://10.0.150.150:150/
Headers Preview Cookies
Request
HTTP/1.0 GET /files/Banner_Fudo_1920_ENG.png
accept-language: en-US,en;q=0.8,pl;q=0.6
accept-encoding: gzip, deflate, sdch
connection: keep-alive
accept: image/webp,image/*,*/*;q=0.8
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.98 Safari/537.36
host: 10.0.150.150:150
referer: http://10.0.150.150:150/
Response
11 200 OK
content-length: 792305
accept-ranges: bytes
server: nginx/1.8.0
last-modified: Mon, 20 Mar 2017 18:35:48 GMT
connection: keep-alive
etag: "58d02104-c16f1"
date: Wed, 29 Mar 2017 11:45:29 GMT
content-type: image/png

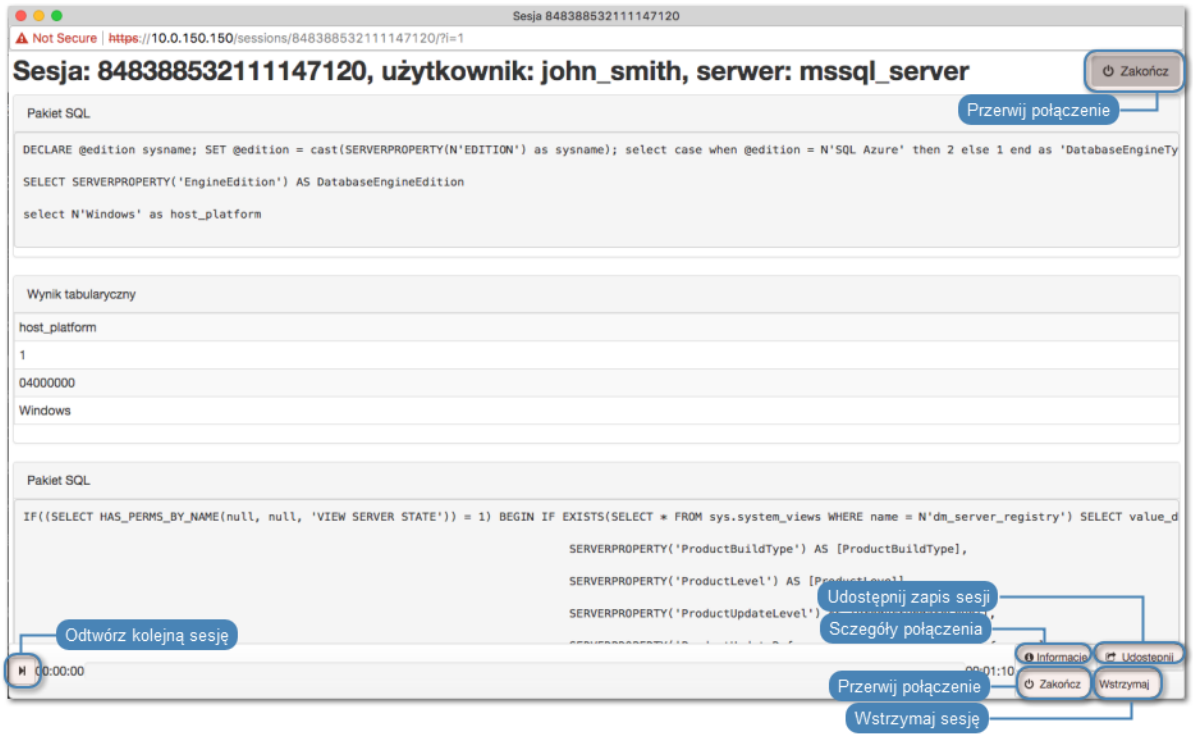
SFTP


2018-11-21 21:20:45 Atrybuty
Size 120178176
User ID 1001
Group ID 1001
Permissions Owner rw Grupa r Inni r
Access time 2018-11-21 21:17:23
Modification time 2018-11-21 21:16:58
2018-11-21 21:20:45 ID żądania: 51 Otwórz plik
File name /tmp/fudo-3-37462.upg
Flags ODCZYT
2018-11-21 21:20:45 Uchwyt
Handle 7
2018-11-21 21:20:45 ID żądania: 52 Odczyt
Handle 7
Offset 0
Długość 32768
Pobierz dane wysłane w ramach tego żądania
2018-11-21 21:20:45 Dane
File Delta
Długość 32768
Pobierz plik od początku transmisji do bieżącego miejsca w sesji
Dane
Podgląd danych

SCP



MySQL, MSSQL, Oracle



Modbus

Tematy pokrewne:

- *Funkcjonalności wrażliwe*

17.3 Wstrzymywanie połączenia

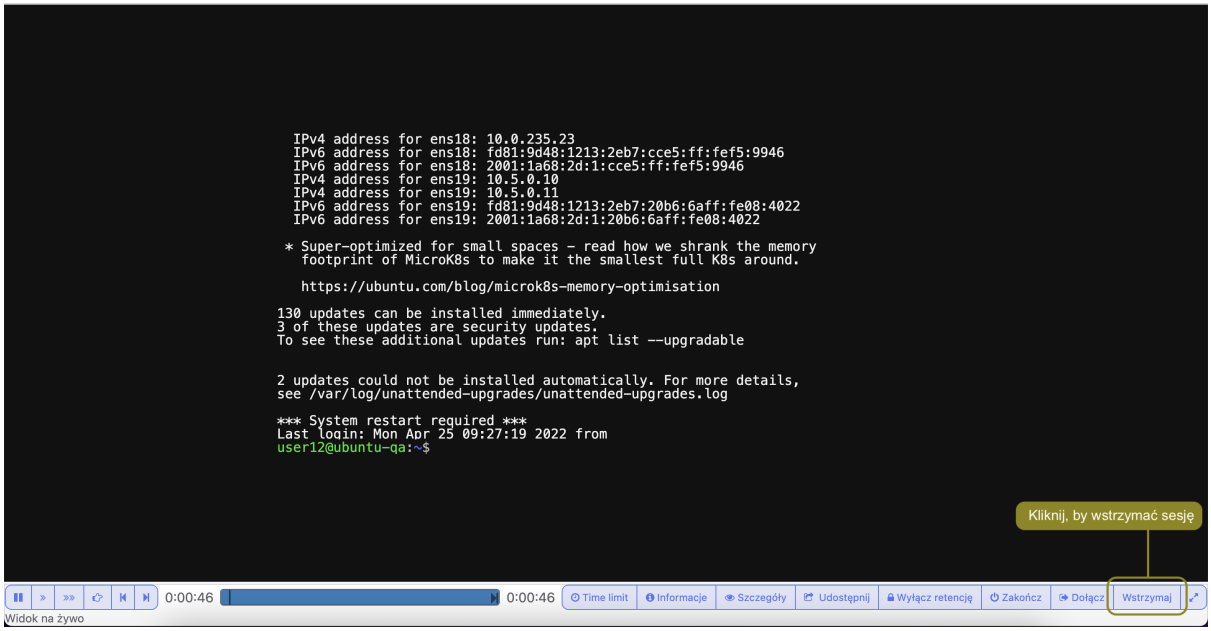
W przypadku gdy aktualne akcje użytkownika wymagają analizy, połączenie może zostać wstrzymane.

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 *Dodaj filtr* i z listy wybierz *Aktywne*.

3. Z listy rozwijalnej wybierz *Tak*.
4. Wyszukaj i kliknij żądaną sesję i kliknij ikonę rozpoczęcia odtwarzania.
5. Kliknij *Wstrzymaj*.



Tematy pokrewne:

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

17.4 Przerywanie połączenia

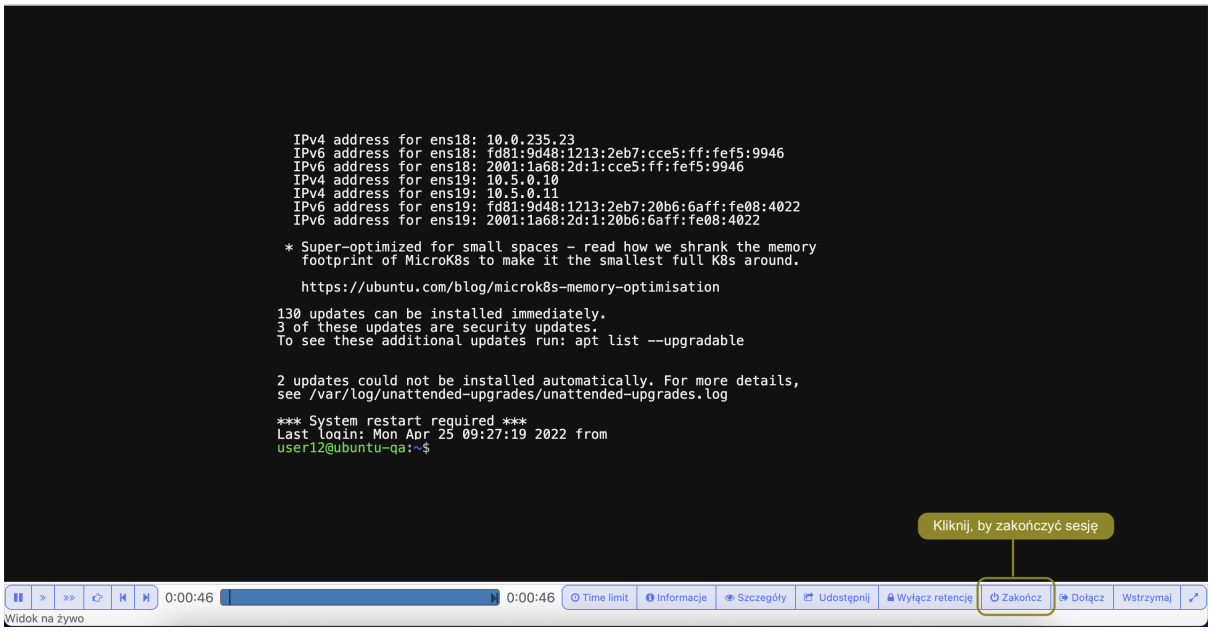
W przypadku gdy administrator stwierdzi nadużycie praw dostępu, może przerwać sesję połączeniową użytkownika.

Informacja: 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 *Dodaj filtr* i z listy wybierz *Aktywne*.
3. Z listy rozwijalnej wybierz *Tak*.
4. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
5. Kliknij *Zakończ*, aby przerwać połączenie.

Informacja: Zerwanie połączenia automatycznie blokuje konto użytkownika.



6. Zdecyduj czy użytkownik powinien pozostać zablokowany.

Tematy pokrewne:

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

17.5 Dołączanie do sesji

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

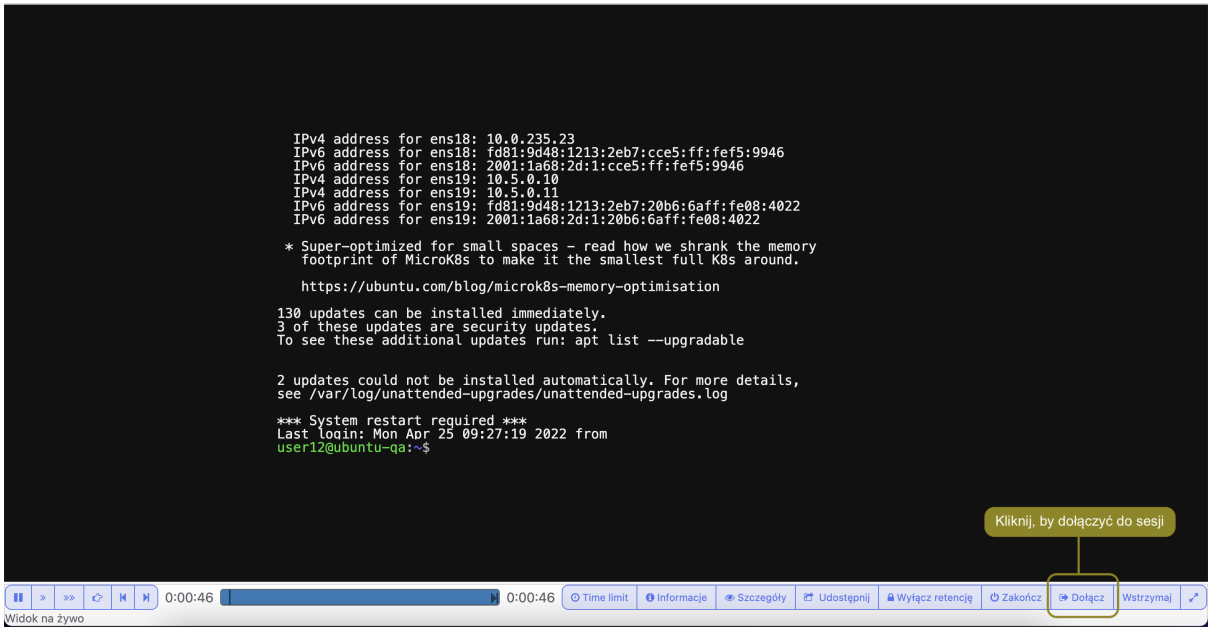
Informacja:

- Funkcja dołączania do sesji jest możliwa w połączeniach SSH, RDP, VNC oraz Telnet (z wyłączeniem Telnet 5250 oraz Telnet 3270).
- W przypadku konfiguracji klastrowej, dołączenie do sesji jest możliwe po zalogowaniu do panelu administracyjnego Fudo na węźle, który obsługuje daną sesję.

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

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij *Dodaj filtr* i z listy wybierz *Aktywne*.
3. Z listy rozwijalnej wybierz *Tak*.
4. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.

5. Kliknij przycisk *Dołącz*.



Tematy pokrewne:

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

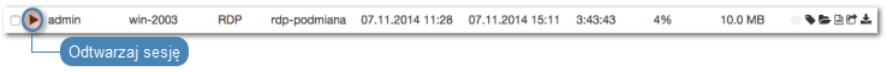
17.6 Udostępnianie sesji

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

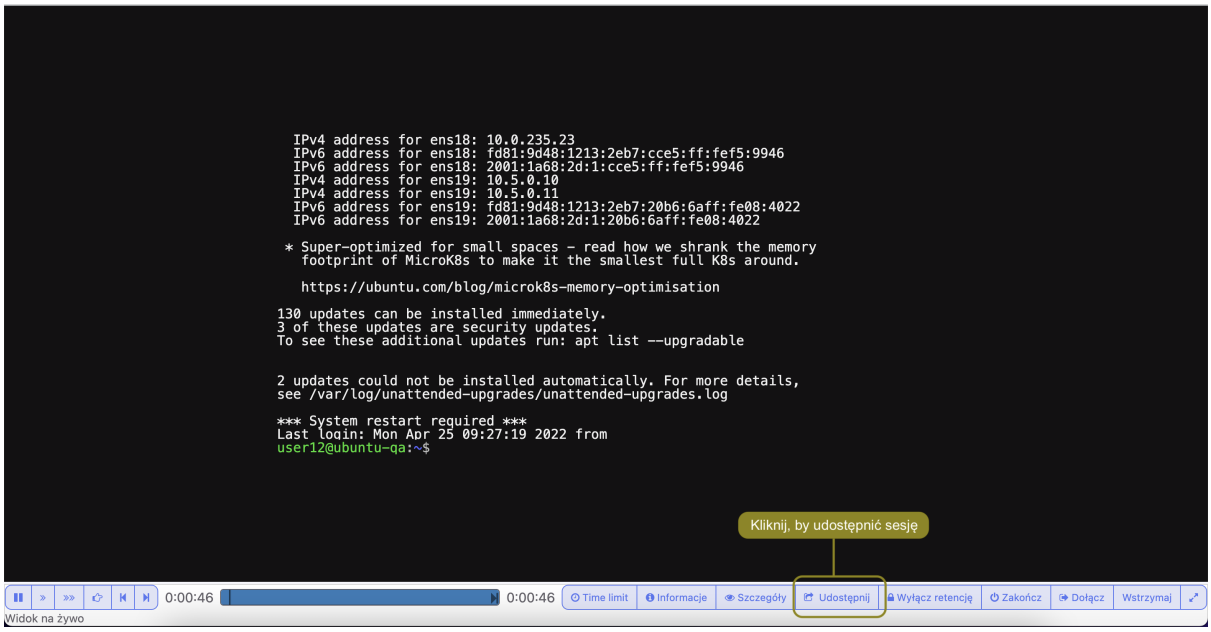
Udostępnianie sesji

Aby udostępnić sesję, postępuj zgodnie z poniższą instrukcją.

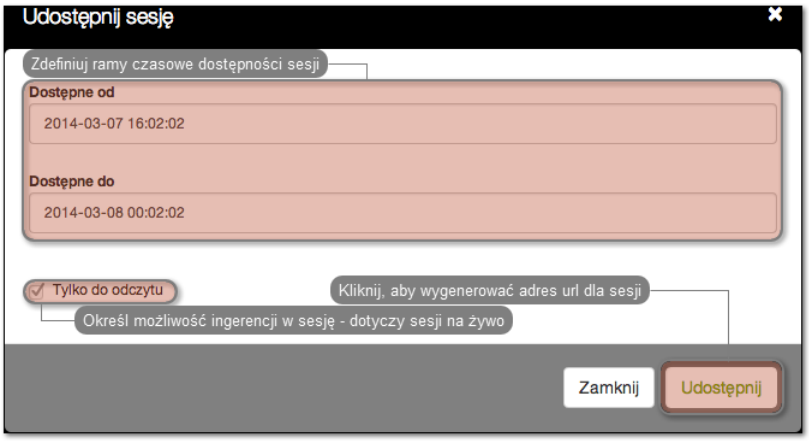
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.



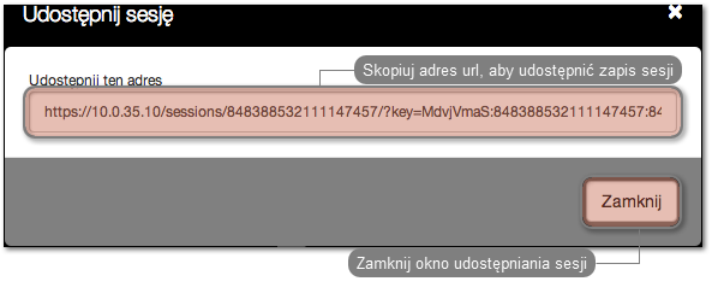
3. Kliknij *Udostępnij*.



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

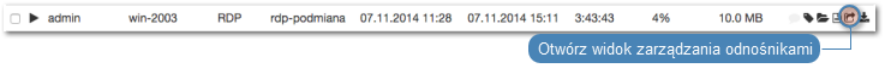


5. Skopiuj odnośnik i kliknij *Zamknij*.

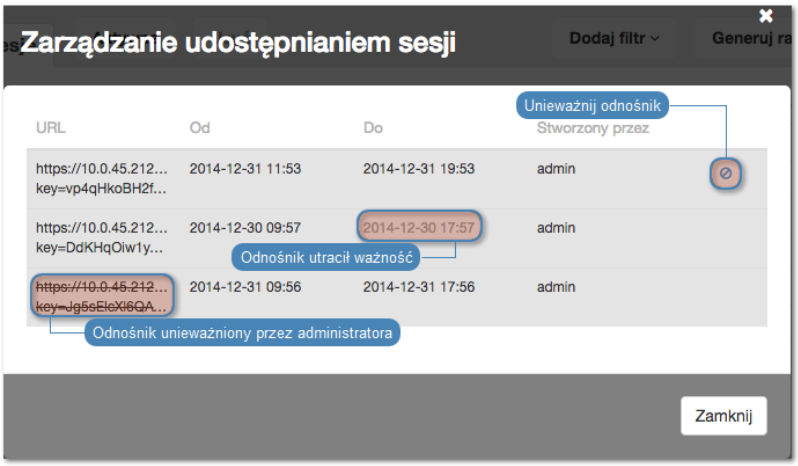


Unieważnienie odnośnika

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*

17.7 Komentowanie sesji

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

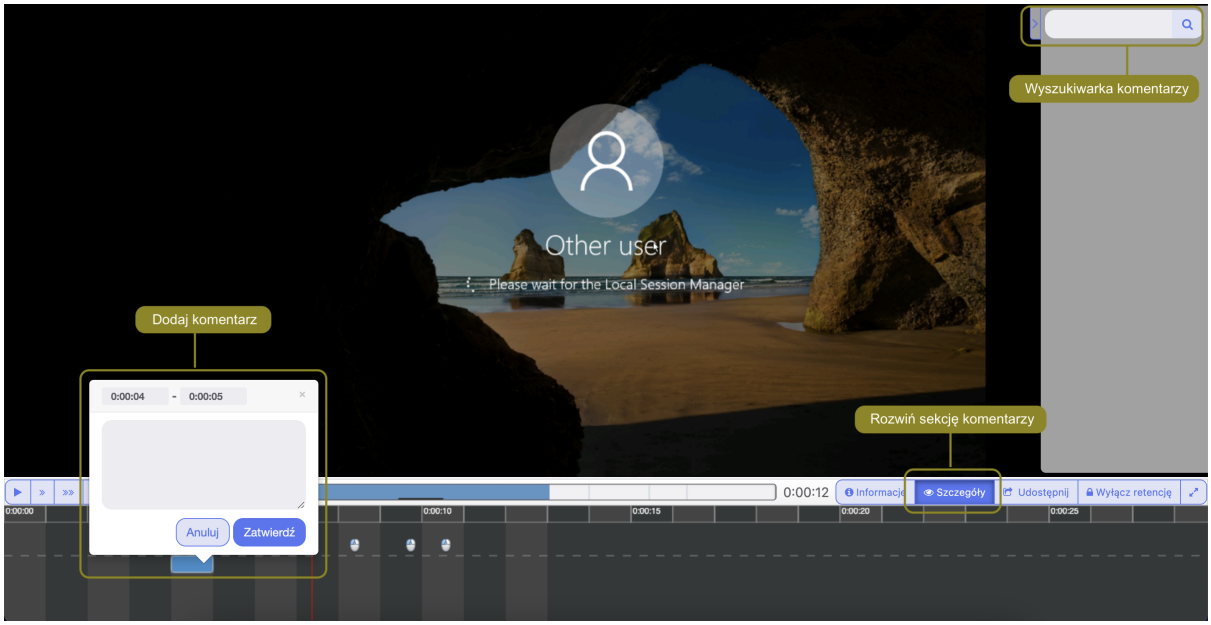
Dodawanie komentarza

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:

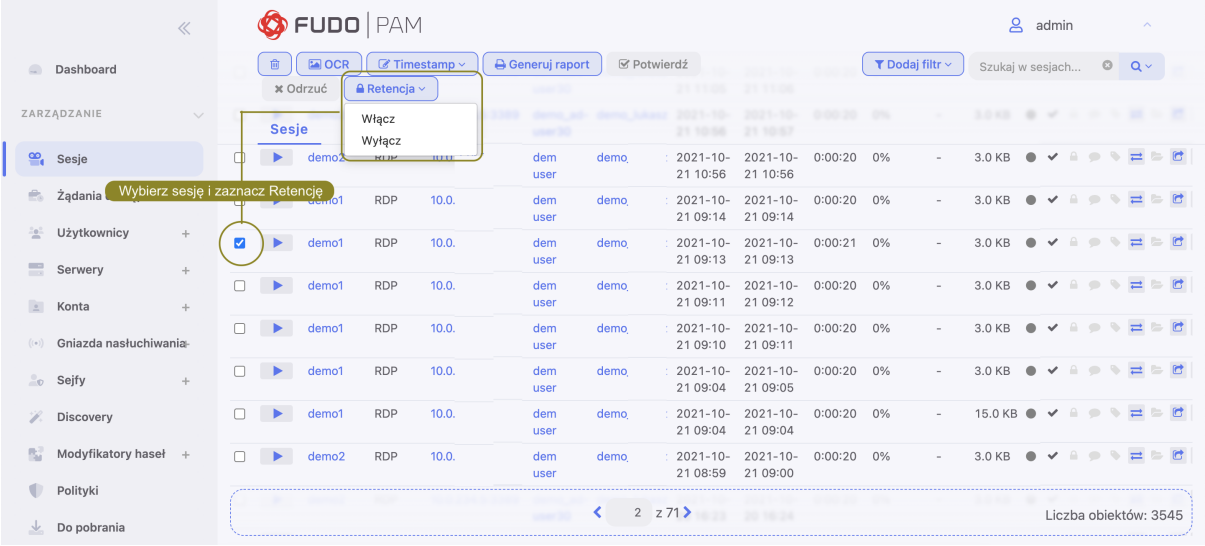
- *Funkcjonalności wrażliwe*

17.8 Zarządzanie retencją sesji

Mechanizm retencji danych automatycznie usuwa sesje po upływie zdefiniowanego interwału czasu. Fudo PAM umożliwia wykluczenie wybranych sesji z procesu retencji, aby nie zostały automatycznie usunięte.

Wyłączanie retencji dla wybranych sesji

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



3. Kliknij *Retencja* i wybierz opcję *Wyłącz retencję*.
4. Kliknij *Zatwierdź*, aby wyłączyć wybrane pozycje z retencji danych.

Włączanie retencji dla wybranych sesji

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Zaznacz żądane sesje.
3. Kliknij *Retencja* i wybierz opcję *Włącz retencję*.
4. Kliknij *Zatwierdź*, aby włączyć retencję dla wybranych pozycji.

Ostrzeżenie: Sesje zostaną usunięte zgodnie z bieżącymi parametrami retencji danych.

Tematy pokrewne:

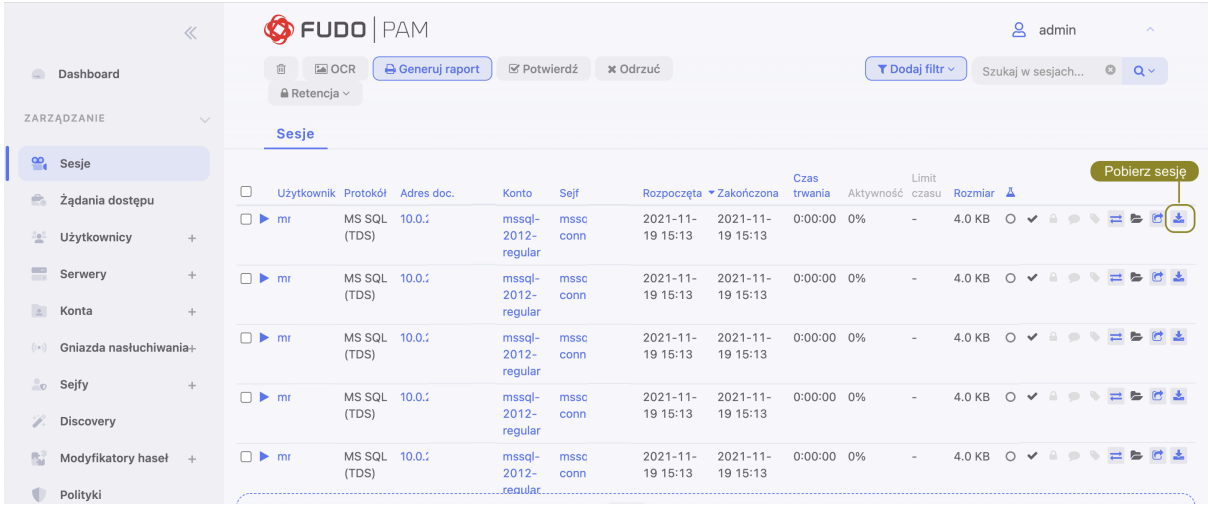
- *Kopie zapasowe i retencja*
- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

17.9 Eksportowanie sesji

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.

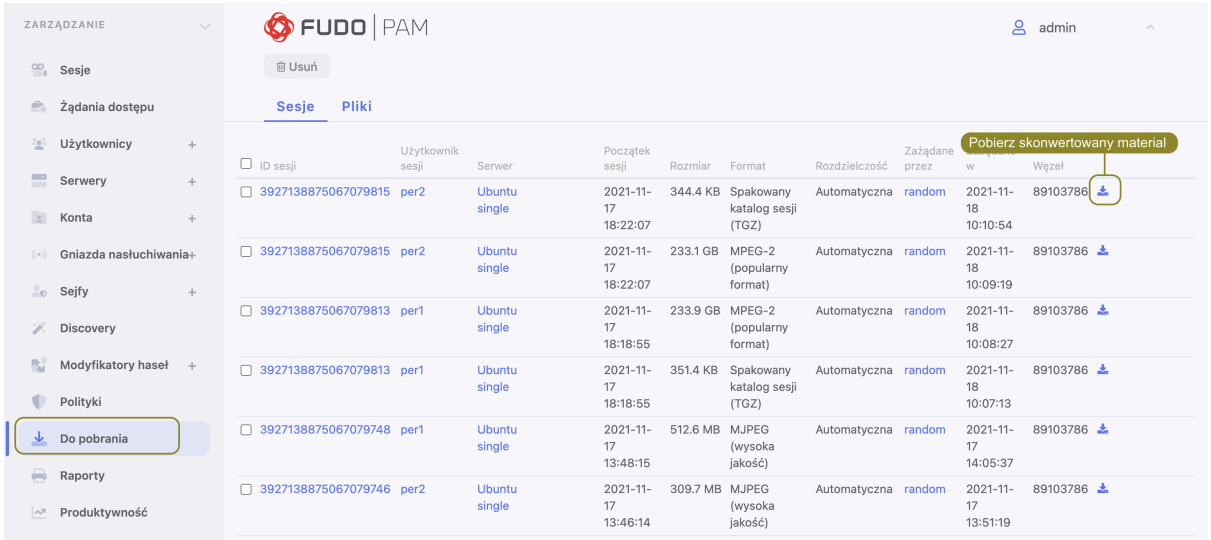
---

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

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

---

6. Kliknij ikonę pobrania sesji.



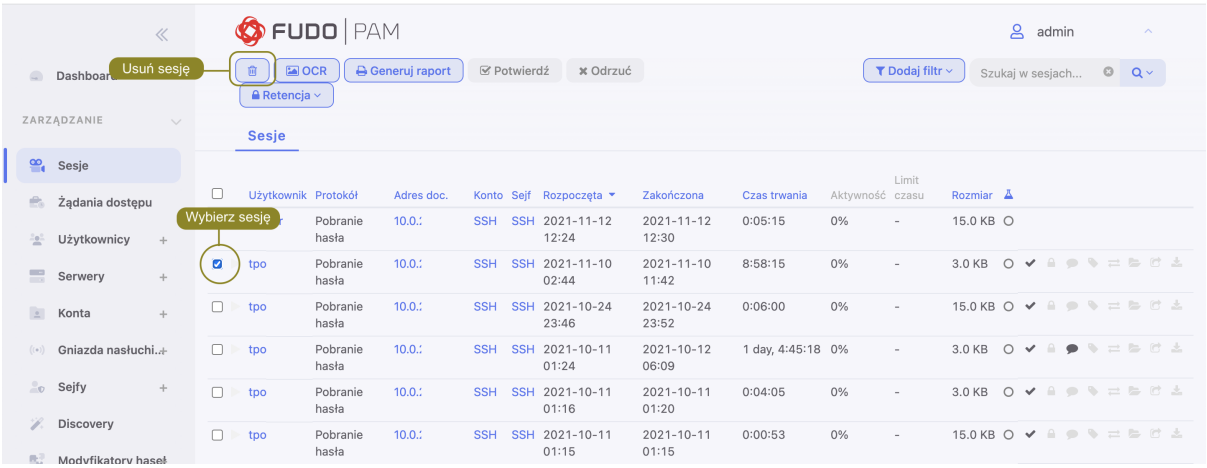
Tematy pokrewne:

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

17.10 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. Zaznacz opcję *Usuń powiązane zasoby*, aby usunąć również treści *wyeksportowane* dla wybranych sesji.
5. Potwierdź usunięcie sesji.

Informacja: 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*

17.11 Przetwarzanie OCR sesji

Zarejestrowany materiał sesji ICA, RDP i VNC oraz renderowanej sesji HTTP może być indeksowany na potrzeby przeszukiwania pełnotekstowego.

Informacja: Przetwarzanie OCR sesji jest wymagającym procesem i może mieć negatywny wpływ na wydajność systemu. Zaleca się, aby OCR ograniczyć do kont, które wymagają szczególnego nadzoru.

Automatyczne przetwarzanie OCR sesji w ramach wybranego połączenia

Aby włączyć przetwarzanie OCR sesji w ramach połączeń realizowanych za pomocą wybranego konta, postępuj zgodnie z poniższą instrukcją.

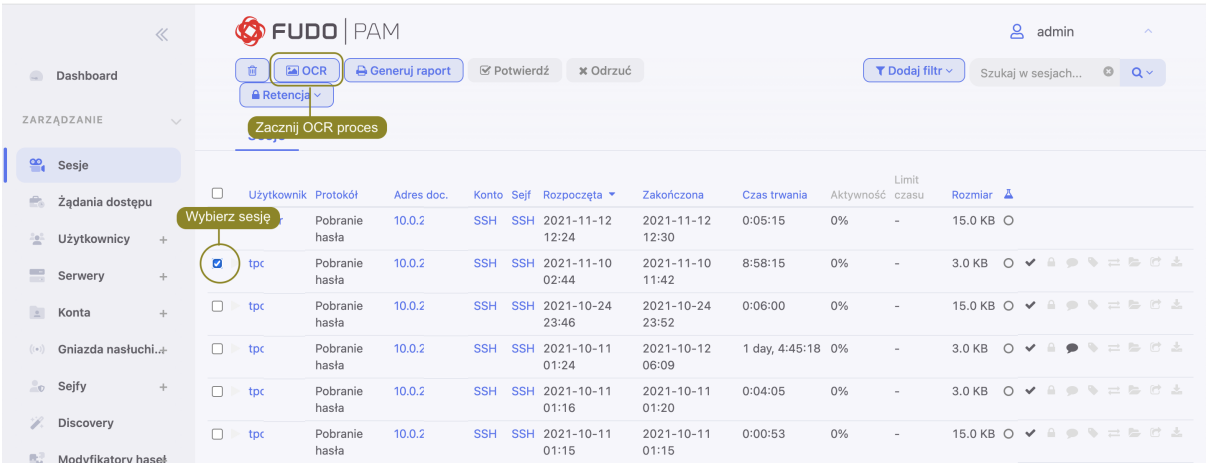
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Znajdź i wybierz żądane konto.
3. Zaznacz opcję *OCR sesji*.
4. Wybierz język przetwarzanych treści.

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*
- *Gniazda nasłuchiwania*

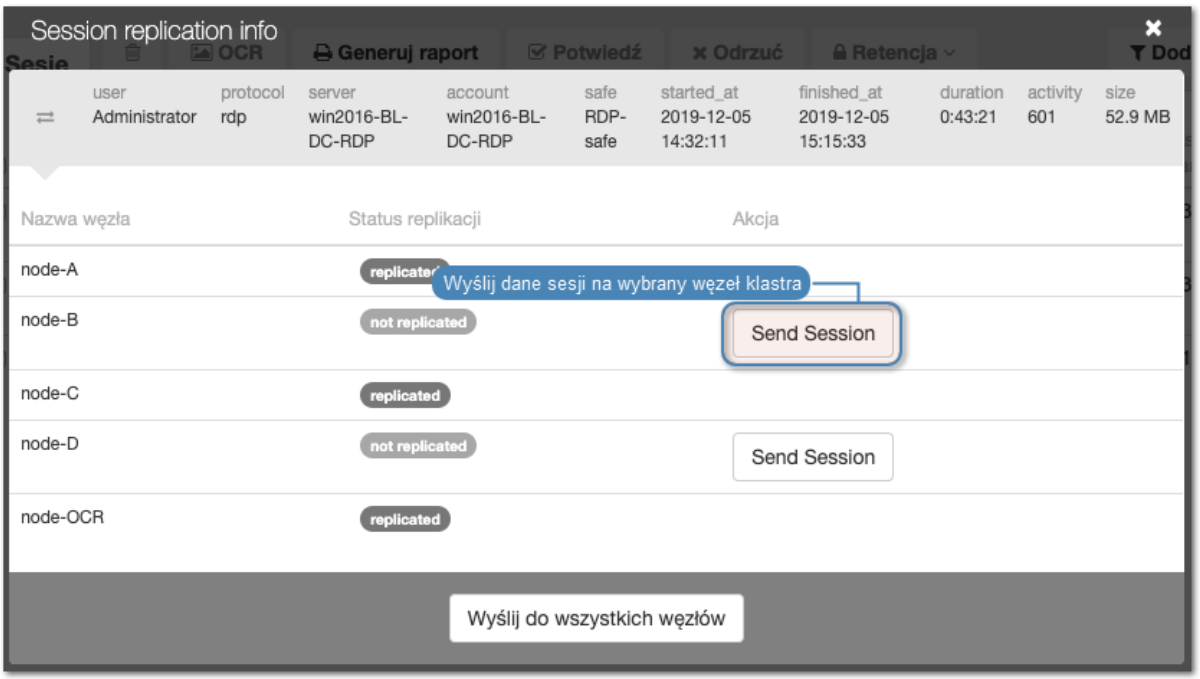
17.12 Replikacja sesji w konfiguracji klastrowej

Poza automatyczną replikacją danych w ramach konfiguracji klastrowej, Fudo PAM umożliwia ręczne zreplikowanie pojedynczych sesji na węzły, na które dana sesja nie jest przesyłana automatycznie.

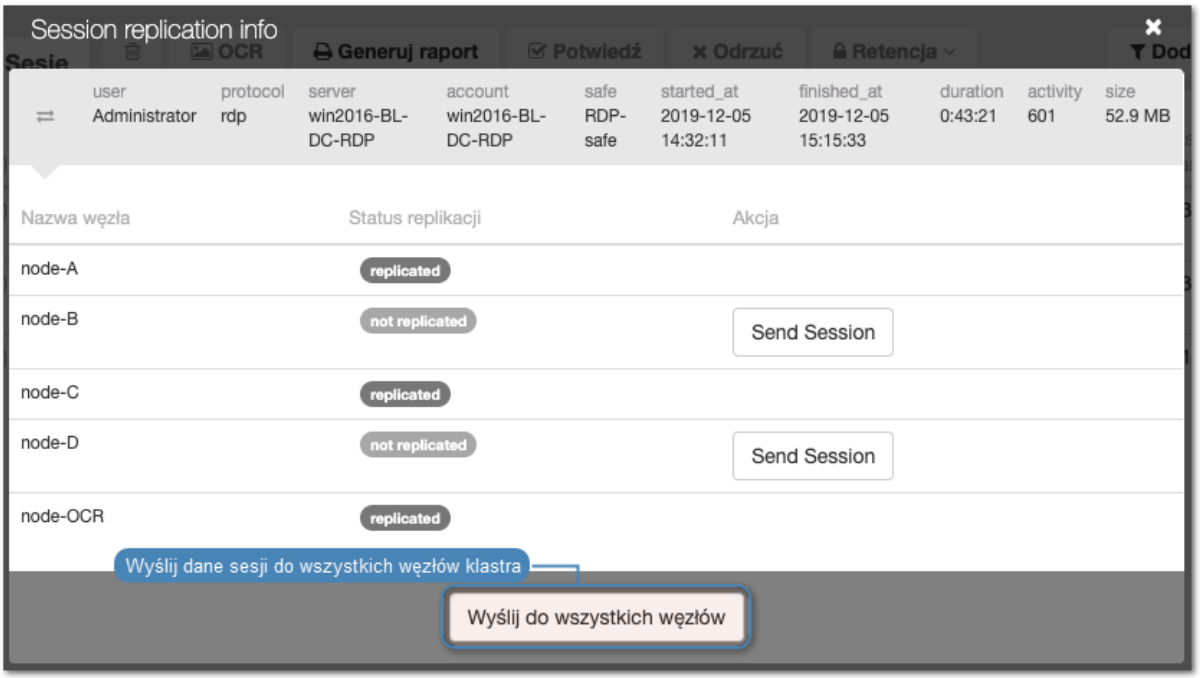
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij ⇄ przy wybranej sesji.

Informacja: Opcja wysłania sesji do wybranych instancji Fudo PAM dotyczy węzłów, na które dane wybranej sesji nie są replikowane automatycznie.

3. Kliknij *Wyślij sesję* przy wybranym węźle, aby zreplikować dane na wskazany węzeł



lub *Wyślij do wszystkich węzłów*, aby dane sesji zostały zreplikowane na wszystkie węzły klastra.



Tematy pokrewne:

- *Konfiguracja klastrowa*
- *Sesje*

17.13 Znakowanie czasem wybranych sesji

Informacja: Aby mieć możliwość opatrywania sesji znacznikiem czasu należy najpierw włączyć i skonfigurować tą opcję z poziomu menu *Ustawienia* > *Znakowanie czasem* zgodnie z instrukcją z rozdziału *Znakowanie czasem*.

Aby opatrzyć znacznikiem czasu wybrane sesje, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Zaznacz żądane sesje, kliknij *Timestamp* i wybierz *Oznakuj sesje*.

3. Kliknij *Zatwierdź*.

Informacja: Po włączeniu opcji znakowania czasem na liście sesji pojawi się dodatkowa kolumna zawierająca status znakowania. Sesje opatrzone znacznikiem czasu wyróżnione są aktywną ikoną zegara. Klikając na ikonę można przeglądać szczegółowe informacje o znaczniku oraz pobrać podpis.

17.14 Anulowanie znakowania czasem

Aby anulować znakowanie czasem wybranych sesji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Zaznacz żądane sesje, kliknij *Timestamp* i wybierz *Anuluj znakowanie*.
3. Kliknij *Zatwierdź*.

Tematy pokrewne:

- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

17.15 Akceptowanie żądań użytkowników

Informacja: Aby otrzymywać powiadomienia email o połączeniu oczekującym na akceptację, zaznacz opcję *Sesja oczekująca na akceptację* w konfiguracji powiadomień dla sejfu.

Informacja: Żądania mogą być akceptowane przez uprawnionych osób też w aplikacji *Fudo Officer 1.0*.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij ✔ przy wybranym połączeniu, lub zaznacz żądane sesje oczekujące i kliknij *Potwierdź*.

Tematy pokrewne:

- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

17.16 Odrzucanie żądań użytkowników

Informacja: Żądania mogą być odrzucane przez uprawnionych osób też w aplikacji *Fudo Officer 1.0*.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij ✖ przy wybranym połączeniu, lub zaznacz żądane sesje oczekujące i kliknij *Odrzuć*.

3. Opcjonalnie, wprowadź powód odrzucenia żądania.

Informacja: Powód odrzucenia wyświetlany jest na liście sesji po najechaniu kursorem na ikonę 💬.

---

4. Opcjonalnie, zaznacz opcję zablokowania konta użytkownika, aby trwale uniemożliwić użytkownikowi nawiązywanie połączeń.
5. Kliknij *Zatwierdź*.

Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Akceptowanie żądań użytkowników*
- *Przerywanie połączenia*
- *Blokowanie użytkownika*
- *Sesje*

17.17 Przetwarzanie sesji - uczenie maszynowe

Informacja: *Jest to wersja ewaluacyjna komponentu AI.*

Fudo PAM jest w stanie wykryć zmiany w zachowaniu użytkowników i pomóc w identyfikacji przypadków, w których dostęp do konta uprzywilejowanego został uzyskany przez osoby nieupoważnione. Fudo PAM śledzi także parametry ilościowe sesji i informuje administratora o nadmiernie dużej liczbie połączeń lub podejrzanie długo trwającej sesji.

17.17.1 Model zawartości

Model zawartości analizuje sesje RDP oraz SSH w celu zbudowania indywidualnych profili behawioralnych użytkowników. Na podstawie zebranych danych, Fudo PAM może wykryć najdrobniejsze zmiany w zachowaniach użytkowników i pomóc w zapobiegnięciu nadużycia praw dostępu.

Model RDP

Model zawartości RDP oparty jest na analizie ruchu kursora myszy.

Wymagania ilościowe modelu RDP:

Minimalne:

- 5 godzin nagranych sesji dla jednego predyktora,
- 5 unikatowych predyktorów (np. użytkowników).

Optymalne:

- 30 godzin nagranych sesji dla jednego predyktora,
- 10 unikatowych predyktorów.

Informacja: Jakość modelu RDP zależy od konsekwencji sposobu interakcji użytkownika z monitorowanym systemem. Jeśli użytkownik korzystał z różnych systemów operacyjnych i różnych urządzeń wejściowych (np. różne myszki, trackpad, trackball), model będący wynikiem analizy sesji nie będzie efektywny, z uwagi na wysoką tolerancję sposobu interakcji użytkownika z systemem.

Model SSH

Model SSH treści oparty jest na analizie komend wprowadzonych przez użytkownika.

Wymagania ilościowe modelu SSH:

Minimalne:

- 65 nagranych sesji (minimum 25 unikatowych komend w każdej sesji),
- 5 unikatowych predyktorów (np. użytkowników).

Optymalne:

- 300 nagranych sesji dla każdego predyktora,
- 10 unikatowych predyktorów.

17.17.2 Ocena sesji

Fudo PAM analizuje sesji w czasie rzeczywistym i wyznacza poziom zagrożenia (OK, NISKI, WYSOKI) w zależności od tego jak zachowanie użytkownika odbiega od schematu zapisanego w modelu.

Informacja: Sesje przetwarzane są w cząstkach o stałej liczbie zdarzeń. Przetwarzanie odbywa się w czasie rzeczywistym, o ile dostępne są zasoby odpowiedzialne za analizę sesji. W przypadku braku zasobów, bieżące sesje nie są analizowane.

Modele są kalibrowane indywidualnie a wyniki analizy prezentowane są na *liście sesji*.

Ikona	Opis
	Sesja w trakcie analizy, wstępny wynik - brak zagrożenia.
	Sesja w trakcie analizy, wstępny wynik - średni poziom zagrożenia.
	Sesja w trakcie analizy, wstępny wynik analizy - wysoki poziom zagrożenia.
	Sesja oczekuje na analizę lub jest wstępnie przetwarzana.
	Sesja nie poddana analizie z uwagi na brak wyuczonego modelu.
	Sesja przetworzona - brak zagrożenia.
	Sesja przetworzona - średni poziom zagrożenia.
	Sesja przetworzona - wysoki poziom zagrożenia.
	Sesja przetworzona - brak wyniku analizy.

Informacja: Efektywność modelu SSH ściśle zależy od jakości danych użytych w procesie trenowania. Jeśli użytkownik udostępniał dane logowania innym, powstały na tej podstawie model może nie być w stanie stwierdzić różnicy w zachowaniach użytkowników.

17.17.3 Modele ilościowe

Fudo PAM monitoruje liczbę połączeń oraz ich czas trwania i może zaalarmować administratora jeśli stwierdzi nadzwyczaj dużą liczbę połączeń jednoczesnych lub podejrzanie długo trwającą sesję.

Ocena bieżąca dokonywana jest w odniesieniu do danych historycznych, zebranych dla użytkowników, kont i serwerów dla każdego dnia tygodnia i każdej godziny.

Tematy pokrewne:

- *Sztuczna inteligencja*
- *Sesje*
- *Często zadawane pytania*

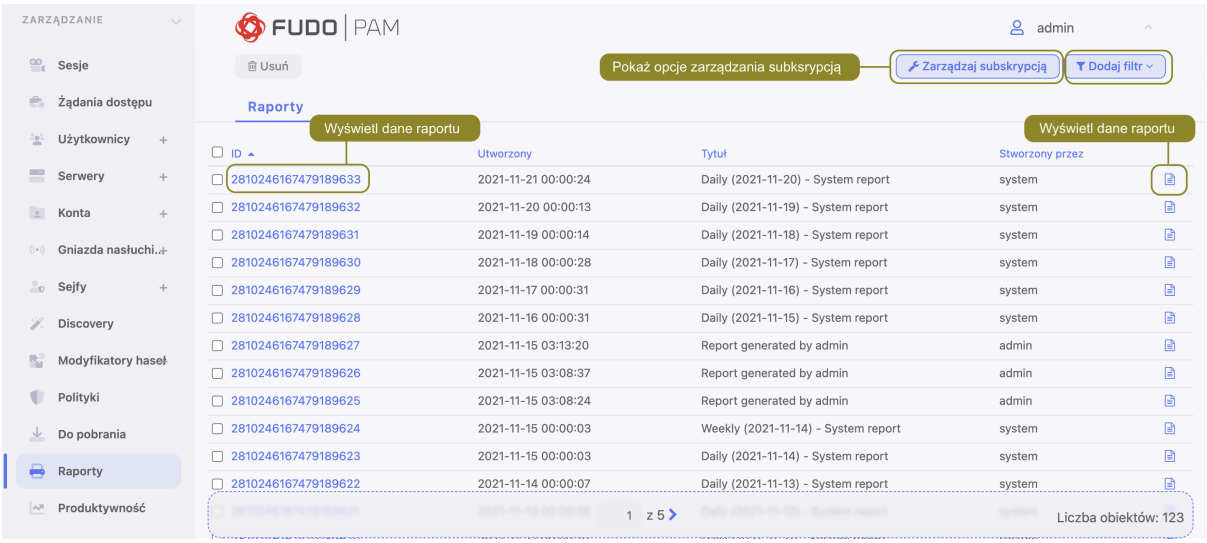
ROZDZIAŁ 18

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.



Raporty predefiniowane

Raport dostępu do kont	Raport zawiera konta, wraz ze skojarzonymi serwerami docelowymi oraz sejfami, do których dostęp miał miejsce w określonym przedziale czasu.
Raport dostępu do sejfów	Raport zawiera sejfy, wraz ze skojarzonymi serwerami, do których dostęp miał miejsce w określonym przedziale czasu.
Raport dostępu do serwerów	Raport zawiera serwery wraz ze skojarzonymi sejfami, do których dostęp miał miejsce w określonym przedziale czasu.
Sesje zatwierdzone przez użytkownika	Raport zawiera sesje zatwierdzone przez administratora.
Udostępnianie sesji	Raport zawiera sesje, których zapis został udostępniony osobom trzecim, w określonym przedziale czasu.
Podsumowanie sesji	Raport zawiera sesje zarejestrowane w określonym przedziale czasu.
Raport sesji per serwer	Raport zawiera listę zarejestrowanych sesji w zestawieniu z serwerami w określonym przedziale czasu.
Raport dostępu użytkownika	Raport zawiera użytkowników w zestawieniu z serwerami, do których się logowali, oraz w zestawieniu z sejfami, gniazdami nasłuchiwania oraz kontami, które pośredniczyły w zestawieniu połączenia.
Raport praw dostępu użytkownika	Raport zawiera użytkowników w zestawieniu z obiektami, do których posiadają uprawnienia dostępu.
Raport użytkownika	Raport zawiera zestawienie użytkowników wraz z podstawowymi informacjami: rolą, statusem, datą utworzenia, ostatnim logowaniem oraz użytkownikiem, który utworzył dany obiekt.

18.1 Subskrybowanie raportu cyklicznego

Subskrypcja powoduje wysłanie raportów poprzez e-mail, więc pamiętaj o konfiguracji serwera SMTP według informacji na stronie *Powiadomienia*. 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.

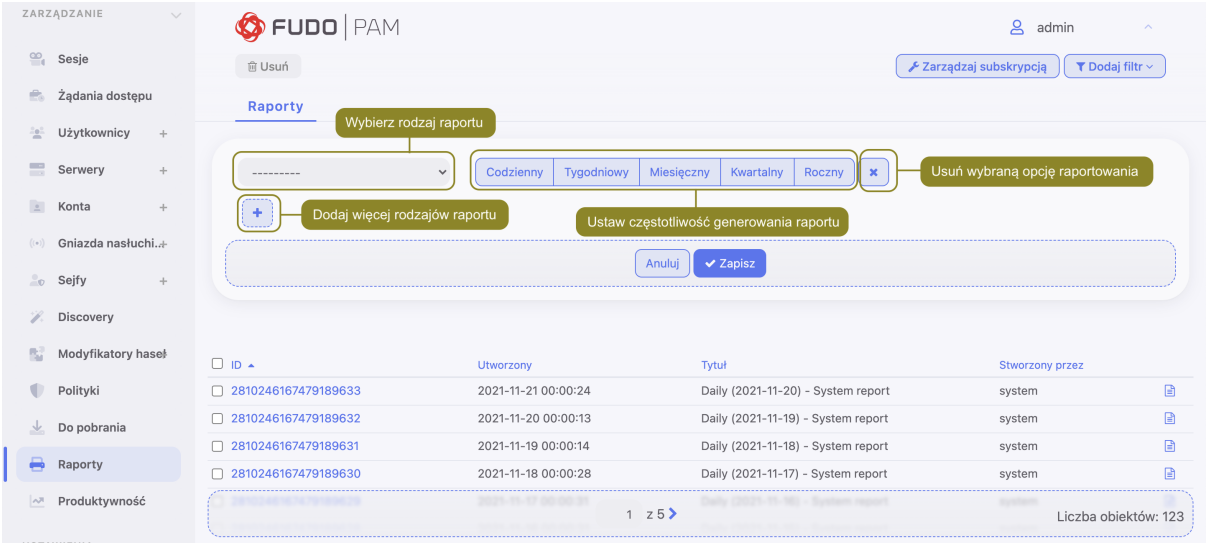
---

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 predefiniowane oraz zapisane przez użytkownika *definicje filtrowania*.

---

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



18.2 Rezygnacja z subskrypcji raportu cyklicznego

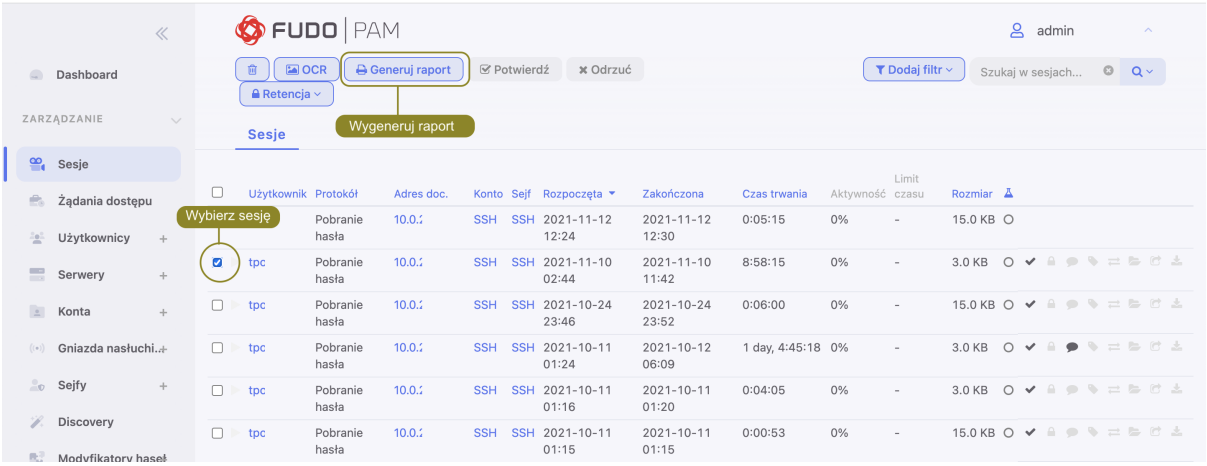
Aby zrezygnować z subskrypcji raportu cyklicznego, postępuj zgodnie z poniższą instrukcją.

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*.

18.3 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.

18.4 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.

18.5 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*

ROZDZIAŁ 19

Produktywność

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

19.1 Zestawienie

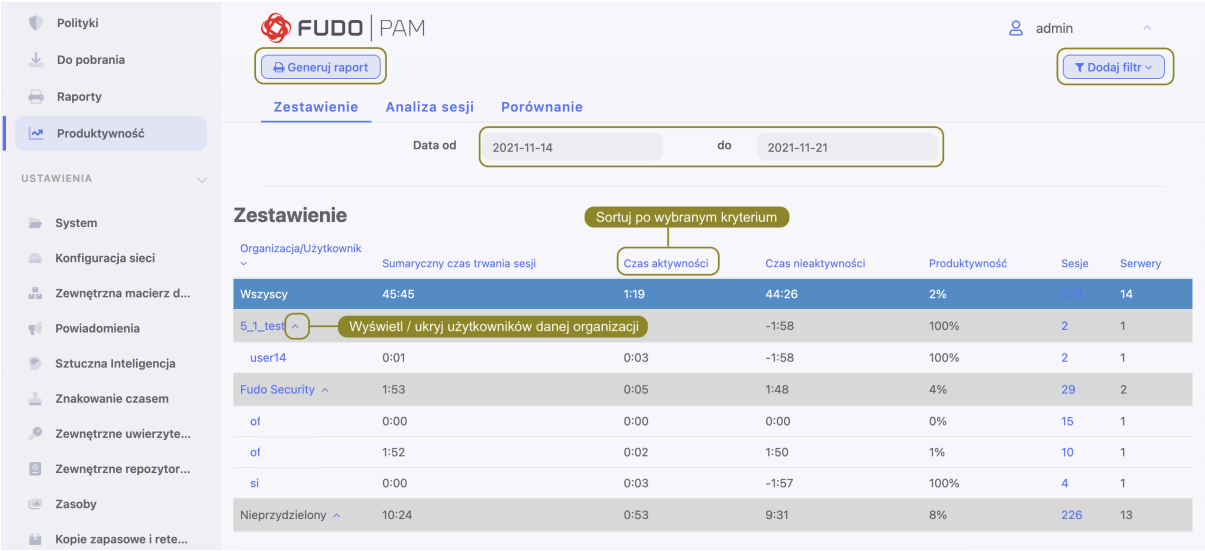
Zestawienie przedstawia dane o aktywności użytkowników i organizacji w wybranym przedziale czasu.

Informacja: Wskaźnik aktywności określany jest na podstawie interakcji użytkownika z systemem. 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*

19.2 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*

19.3 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 20

Administracja

Poniższy rozdział zawiera opisy czynności administracyjnych.

20.1 System

20.1.1 Data i czas

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

Ostrzeżenie:

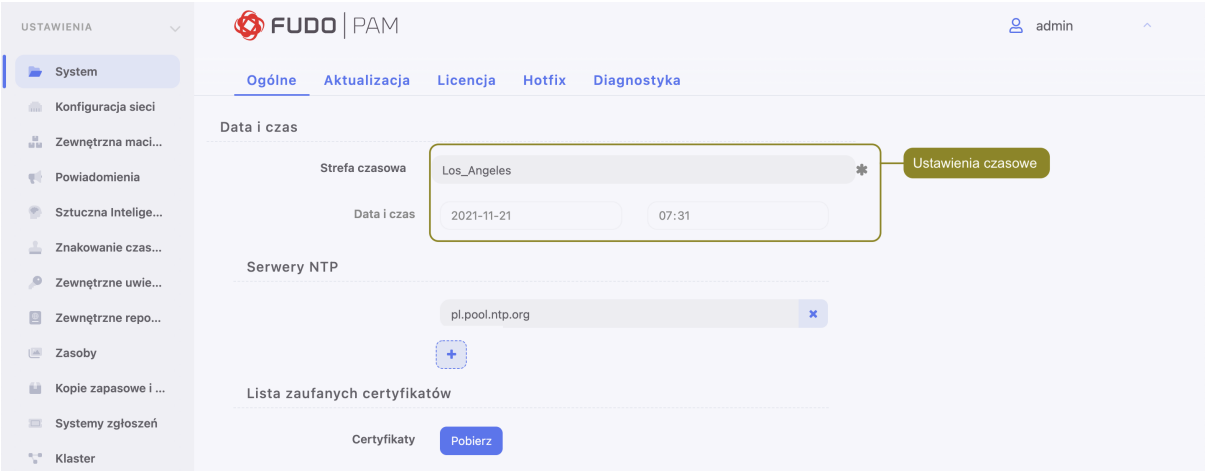
- Zaleca się, aby data i czas pobierane były z serwera NTP, będącego pewnym źródłem danych referencyjnych. Ręczna zmiana ustawień daty i czasu może spowodować nieprawidłowości w funkcjonowaniu urządzenia.
- Pobieranie czasu z serwera NTP jest wymagane w przypadku *konfiguracji klastrowych*.

Zmiana daty i czasu

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

Aby zmienić datę i czas serwera 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*.

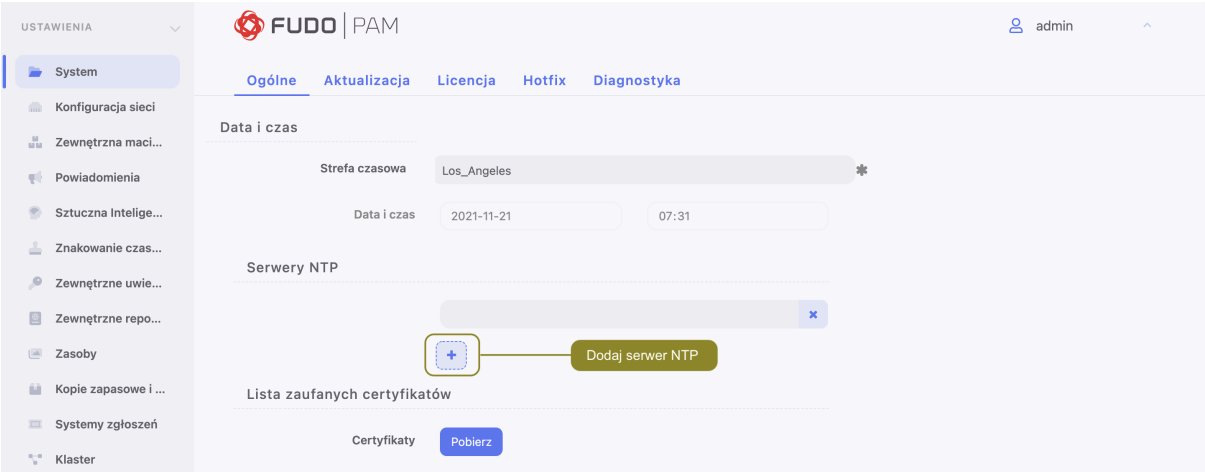
Konfiguracja serwerów czasu

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*.
5. Wybierz z menu użyktownika opcję *Uruchom ponownie*.

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*.
4. Wybierz z menu użyktownika opcję *Uruchom ponownie*.

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*

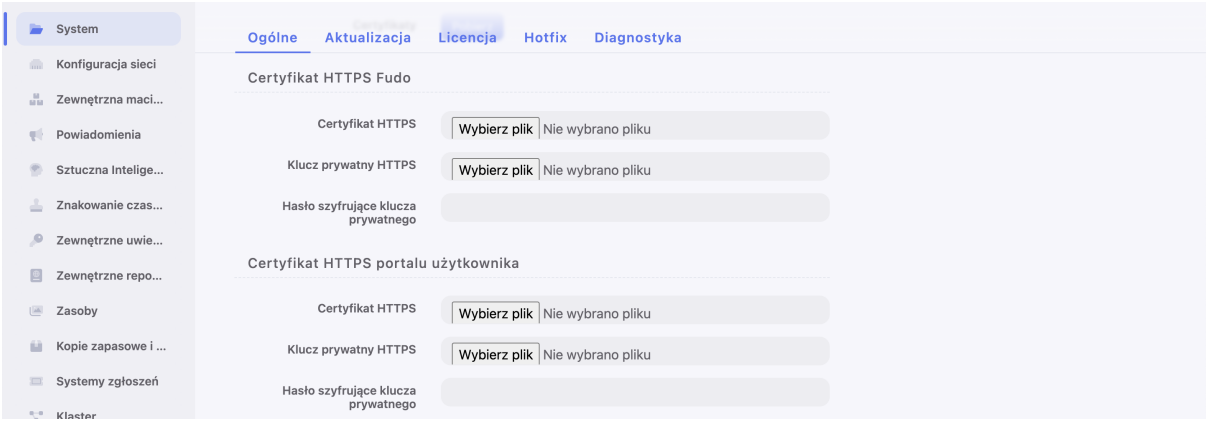
20.1.2 Certyfikaty HTTPS

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

Informacja: Fudo wymaga użycia niezaszyfrowanych kluczy certyfikatów. Sprawdź jak odszyfrować hasło zaszyfrowane kluczem RSA.

Konfigurowanie certyfikatu SSL panelu administracyjnego Fudo

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Certyfikat HTTPS Fudo*, 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*.

Konfigurowanie certyfikatu SSL portalu użytkownika

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Certyfikat HTTPS portalu użytkownika*, 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*

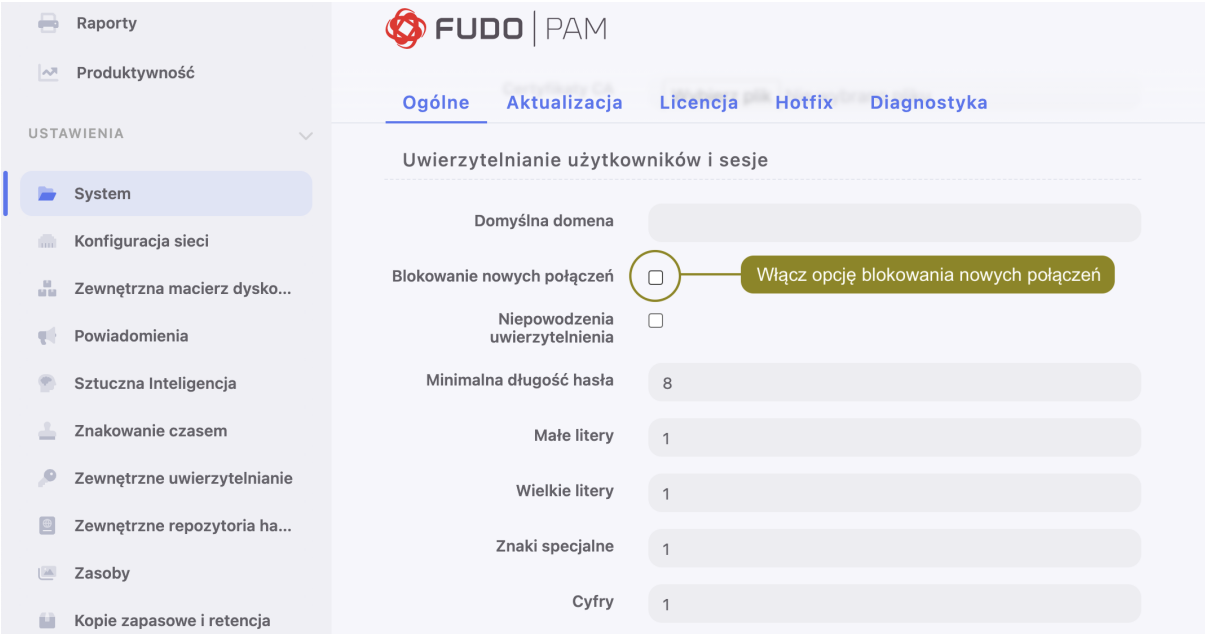
20.1.3 Blokowanie nowych połączeń

Opcja blokowania nowych połączeń umożliwia zablokowanie możliwości nawiązywania połączeń z monitorowanymi zasobami, np. w celu realizacji zaplanowanych prac serwisowych.

Włączenie blokowania nowych połączeń

Aby włączyć opcję blokowania nowych połączeń, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. W sekcji *Uwierzytelnianie użytkowników i sesje* zaznacz opcję *Blokowanie nowych połączeń*.



3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

20.1.4 Dostęp SSH

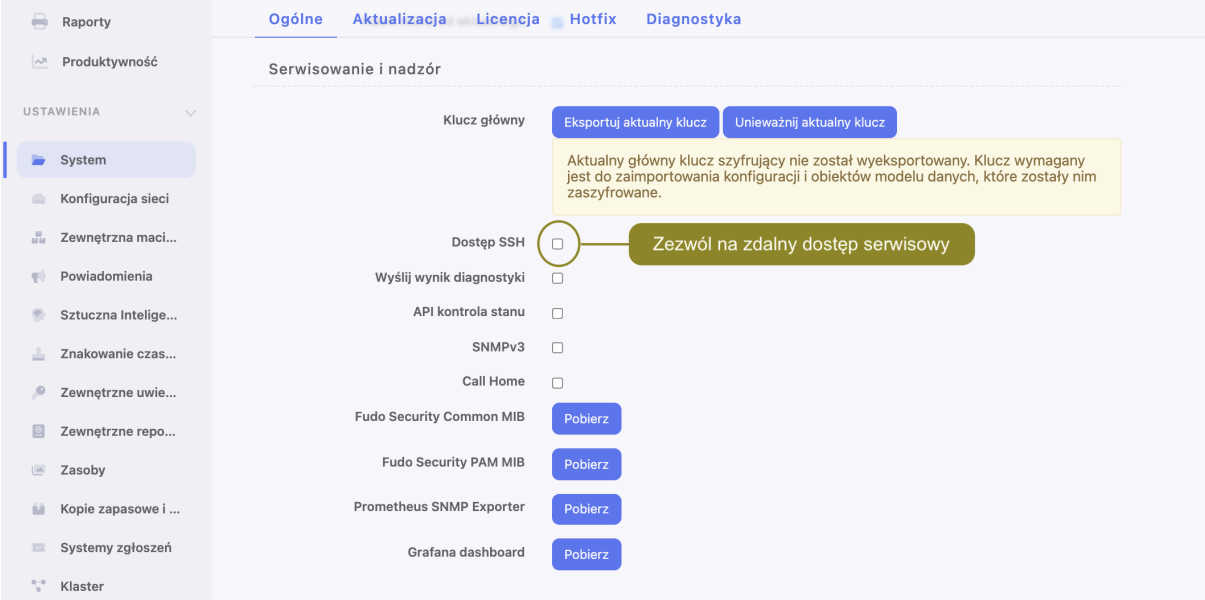
Opcja umożliwia zdalny dostęp serwisowy do Fudo PAM za pośrednictwem protokołu SSH.

Informacja: Domyślnym portem dostępu serwisowego poprzez protokół SSH jest port numer 65522.

Włączanie dostępu SSH

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

1. Wybierz z lewego menu opcję *Ustawienia* > *System*.
2. W sekcji *Serwisowanie i nadzór* zaznacz opcję *Dostęp SSH*.



3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

20.1.5 Funkcjonalności wrażliwe

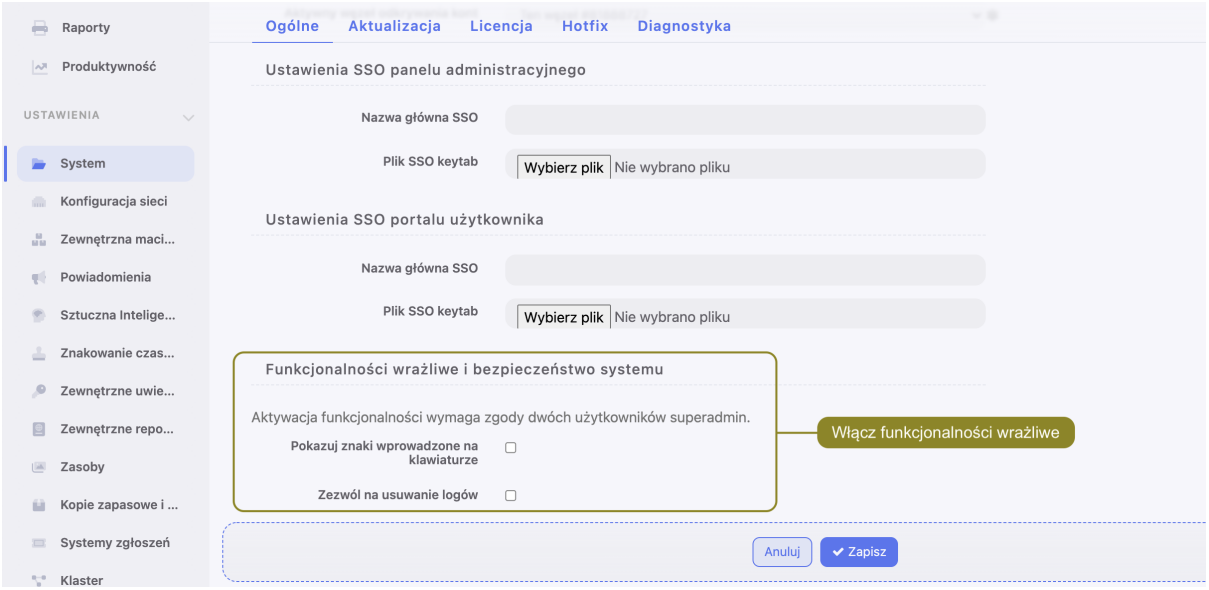
Funkcjonalności wrażliwe to zestaw opcji, których włączenie wymaga decyzji dwóch użytkowników o roli `superadmin`.

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 i bezpieczeństwo systemu*, aby zainicjować włączenie funkcji.
3. Kliknij Zapisz.



4. Zaznacz opcję *Zezwól na usuwanie logów*, powiązaną z funkcjonalnością Retencji logów: *Kopie zapasowe i retencja*.

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

Tematy pokrewne:

- *Odtwarzanie sesji*

20.1.6 Aktualizacja systemu

Ponieważ następna wersja systemu Fudo PAM 5.3 zawiera liczne zmiany w bazach danych, jest wymagane przeprowadzenie pracy przygotowawczej:

- Wsparcie protokołów `Citrix`, `ICA` and `Oracle` zostaje wycofane, więc jest wymagane usunięcie powiązanych sesji ze wspomnianymi protokołami(poza tymi, które już zostały wyeksportowane). Reszta powiązanych obiektów (konta, serwery, gniazda nasłuchiwania) zostaną usunięte przez skrypt aktualizacyjny automatycznie.
- Opcja *Używaj zaufanych certyfikatów* będzie domyślnie włączona dla serwerów HTTP w przyszłej wersji systemu, więc dla wszystkich istniejących serwerów HTTP ta opcja powinna zostać włączona. Więcej informacji pod linkiem *Dodawanie serwera HTTP*.
- *Hitachi ID Privileged Access Manager* oraz *Lieberman Enterprise Random Password* powinno zostać usunięte z konfiguracji Zewnętrznych repozytoriów haseł.
- Nazwy użytkowników zawierające «#» albo «%» , powinny zostać zmienione.
- Jeśli istnieje kilka serwerów z duplikowaną parą adres:port, ale o różnych protokołach, tylko jeden z nich powinien zostać.
- Konfiguracja Remote app powinna zostać usunięta dla serwerów oraz kont. Więcej informacji pod linkiem *Dodawanie serwera RDP*.
- Konfiguracja *Modyfikatorów haseł* dla serwerów przestaje wspierać `protocol`, `secproto`, `ssl_to_server`, `ssl_v2`, `ssl_v3`, `subnet`, więc one powinny być usunięte.

- Port numer 8888 jest teraz zarezerwowany. Istniejące gniazda nasłuchiwania, korzystające z tego portu powinny zostać odpowiednio zmodyfikowane.
- Porty powyżej albo równe 60000 są teraz zarezerwowane. Istniejące gniazda nasłuchiwania, korzystające z tych portów powinny zostać odpowiednio zmodyfikowane.

Informacja:

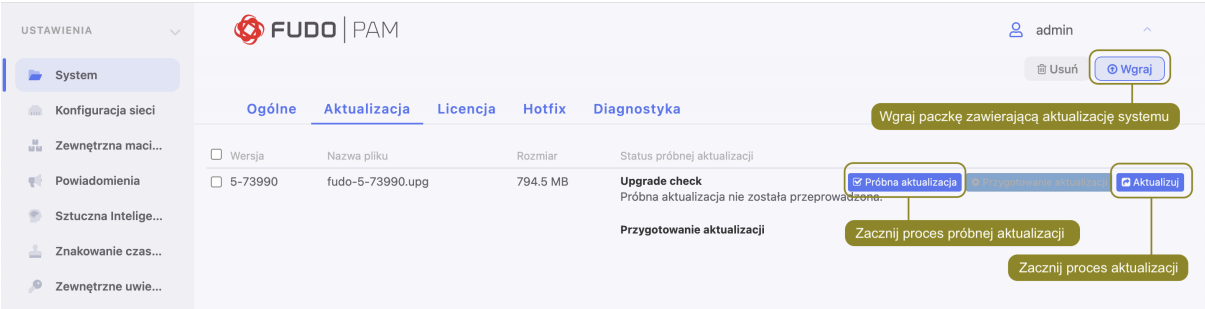
- Proces aktualizacji systemu nie dokonuje zmian w konfiguracji urządzenia ani nie narusza integralności zarejestrowanych sesji.
- Podczas aktualizacji systemu, zużycie wewnętrznej macierzy dyskowej może tymczasowo wzrosnąć.
- W przypadku konfiguracji klastrowej, w pierwszej kolejności dokonaj aktualizacji na węźlę podrzędnym.

20.1.6.1 Aktualizowanie systemu

Ostrzeżenie:

- W przypadku, gdy aktualizacja wymaga przygotowania, zaleca się aby proces przygotowawczy dobiegł końca. Pozwoli to zminimalizować czas przestoju maszyny podczas wykonywania właściwej aktualizacji.
- W przypadku, gdy zajętość wewnętrznej macierzy danych przekracza 85%, przed wykonaniem aktualizacji systemu, skontaktuj się ze wsparciem technicznym.
- W procesie aktualizacji, trwające połączenia użytkowników zostaną zerwane. Skorzystaj z opcji *Blokowanie nowych połączeń*, w sekcji *Sesja* ustawień systemowych, *aby ograniczyć liczbę* aktywnych użytkowników przed ponownym uruchomieniem systemu.
- Po aktualizacji systemu, Fudo PAM zostanie uruchomione ponownie. Ponowne uruchomienie maszyny fizycznej wymaga obecności klucza szyfrującego. Włóż nośnik z kluczem szyfrującym do portu USB. W przypadku instancji wirtualnej, ponowne uruchomienie wymaga podania hasła szyfrującego. Wprowadzenie błędnego hasła spowoduje ponowne uruchomienie systemu w poprzedniej wersji.
- Dla użytkowników, aktualizujących z wersji Fudo PAM 4.x, nowy klucz aktualny będzie wygenerowany podczas aktualizacji. Takim użytkownikom zaleca się wyeksportować i zachować nowy klucz. Więcej informacji o kluczach aktualnych znajdziesz pod linkiem: *Szyfrowanie konfiguracji*.

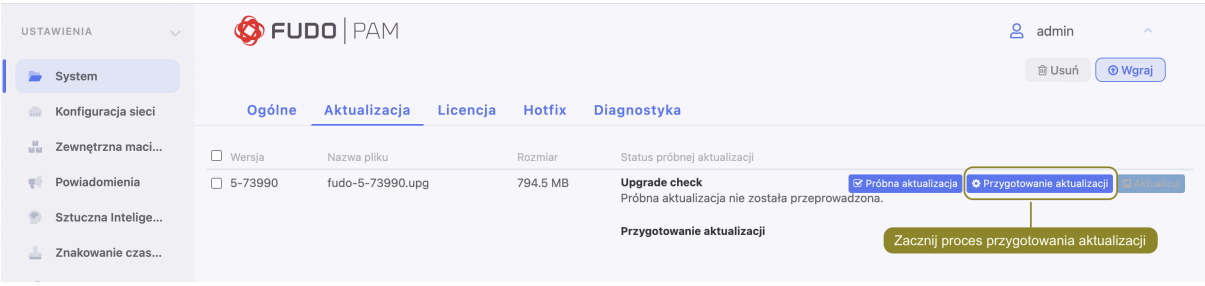
1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Aktualizacja*.
3. Kliknij *Wgraj*.
4. Wskaż plik zawierający aktualizację systemu (`.upg`).
5. Kliknij *Próbna aktualizacja* przy wybranym pliku obrazu, aby stwierdzić, czy obiekty modelu danych i bieżąca konfiguracja są kompatybilne z nową wersją systemu.



Informacja:

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

6. Jeśli aktualizacja wymaga przygotowania, kliknij *Przygotowanie aktualizacji*.



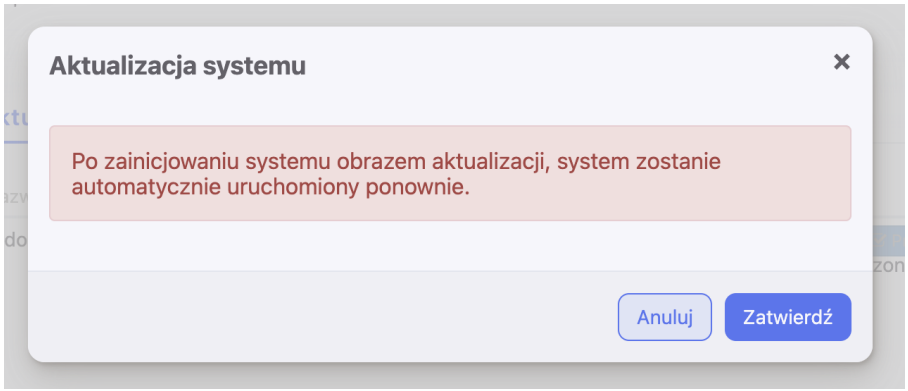
Informacja:

- Proces przygotowawczy pozwala na zminimalizowanie czasu potrzebnego na wykonanie właściwej aktualizacji.
- Kliknij *Stop*, aby przerwać proces przygotowawczy. Miej na uwadze, że aktualnie przetwarzany etap musi zostać zakończony, więc anulowanie procesu może zająć chwilę.
- Kliknij *Start*, aby wznowić proces przygotowawczy.

7. Kliknij *Aktualizacja*.

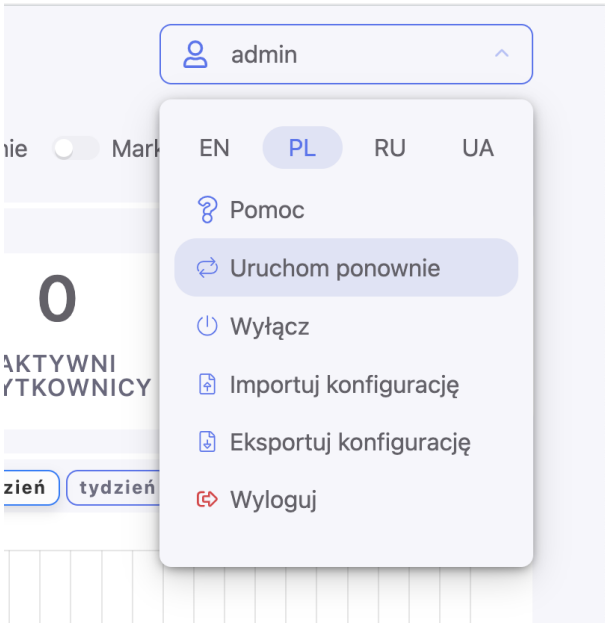
Informacja: W przypadku aktualizacji wymagających przygotowania, aktualizacja może zostać przeprowadzona po wykonaniu wstępnego przygotowania. Zalecane jest jednak, aby proces przygotowawczy dobiegł końca. Pozwoli to zminimalizować czas przestoju maszyny podczas wykonywania właściwej aktualizacji.

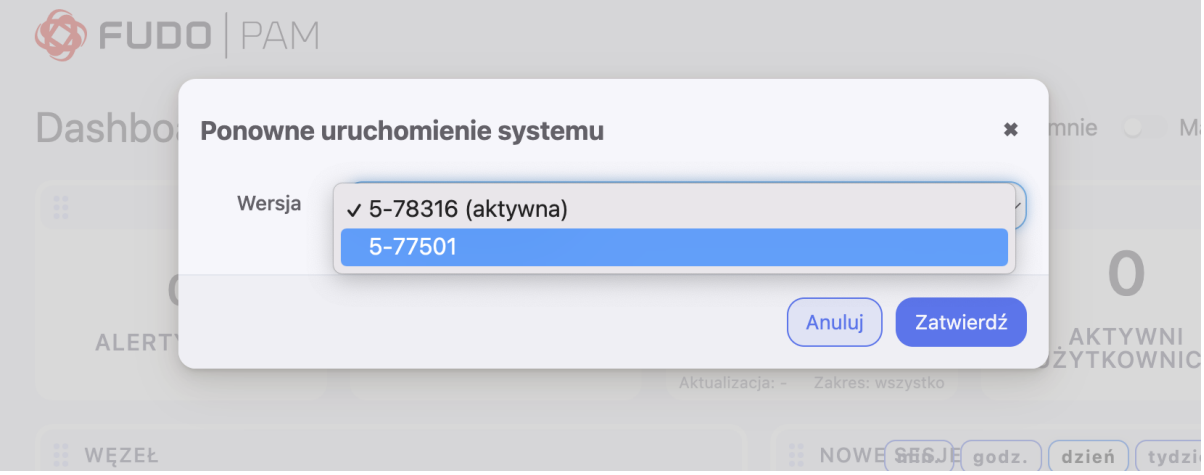
8. Kliknij *Zatwierdź*, aby wykonać aktualizację.



Informacja: Jeśli przed aktualizacją została włączona opcja systemowa *Blokowanie nowych połączeń*, pamiętaj żeby wyłączyć ją po ponownym uruchomieniu systemu.

Fudo PAM oprócz bieżącej wersji systemu, przechowuje jego poprzednią wersję, pozwalając na jej przywrócenie. W przypadku gdy uruchomienie systemu w nowej wersji nie powiedzie się, Fudo PAM wykryje problem i uruchomi system w poprzedniej wersji. Fudo PAM też umożliwia przywrócenie poprzedniej wersji systemu za pomocą opcji *Uruchom ponownie* z menu opcji użytkownika:





Ostrzeżenie: Przywrócenie poprzedniej wersji spowoduje odtworzenie stanu systemu sprzed jego aktualizacji. **Dane sesji** oraz **zmiany w konfiguracji** dokonane na nowej wersji systemu zostaną utracone. Obejmuje to także **aktywność modyfikatorów haseł**. Jeśli jakiekolwiek hasła zostały zmienione podczas korzystania z nowszej wersji, przywrócenie poprzedniej wersji spowoduje utratę dostępu do wybranych systemów.

Jeśli zostanie wybrana aktywna wersja, odbędzie się ponowne uruchomienie systemu, według opisu na stronie *Ponowne uruchomienie systemu*.

20.1.6.2 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*

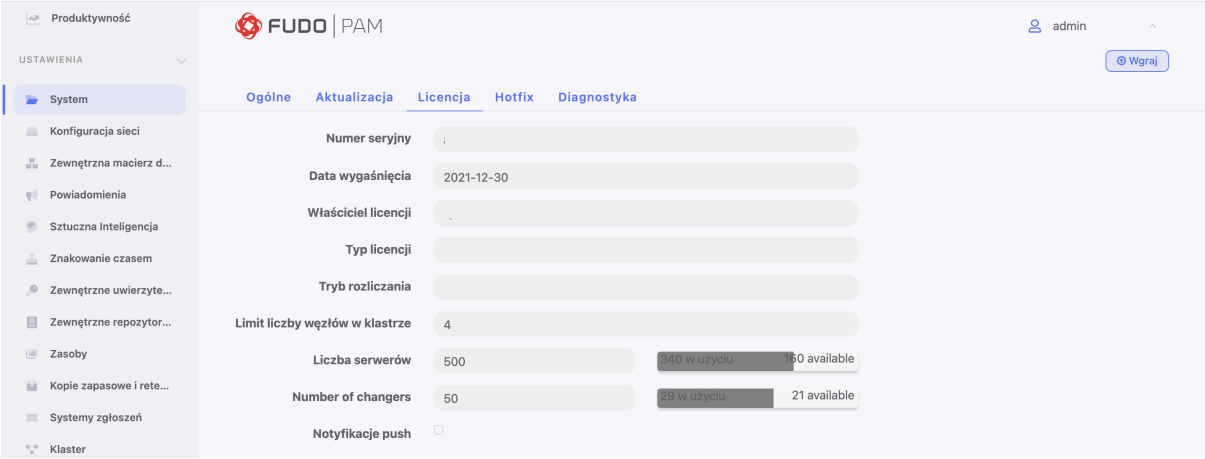
20.1.7 Licencja

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.

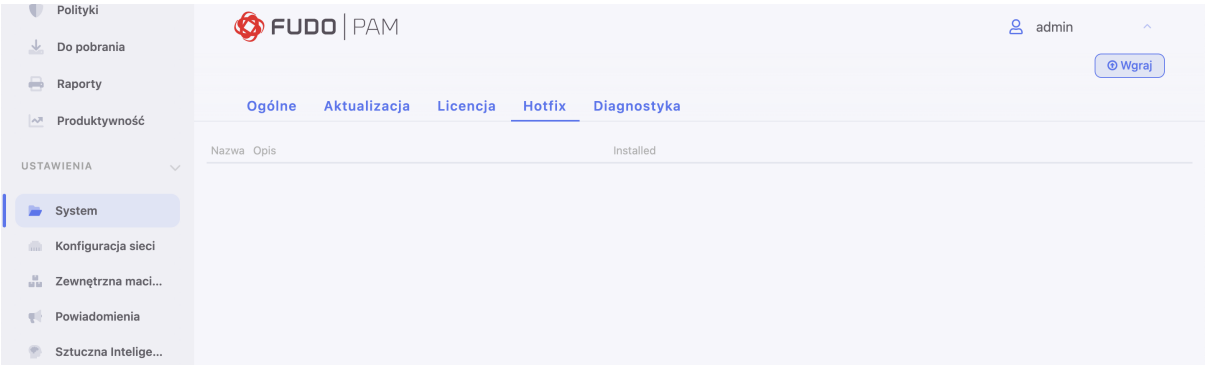
Tematy pokrewne:

- *Opis systemu*
- *Wymagania*

20.1.8 Hotfix

Funkcjonalność Hotfix pozwala administratorowi naprawić błędy systemowe poprzez wgranie paczki naprawczej w Panelu Administracyjnym. Paczka jest dostarczana przez Dział Wsparcia Technicznego Fudo PAM i nie wymaga nic więcej do konfiguracji.

Plik z paczką Hotfix ma rozszerzenie Fudo Security HotFix (`.fshf`), i może zostać wgrany przez Administratora z lewego menu w *Ustawienia* > *System* > *Hotfix*.



Hotfixy nie mogą zostać usunięte ani odinstalowane, gdyż znikają zaraz po aktualizacji systemu.

Related topics:

- *Aktualizacja systemu*

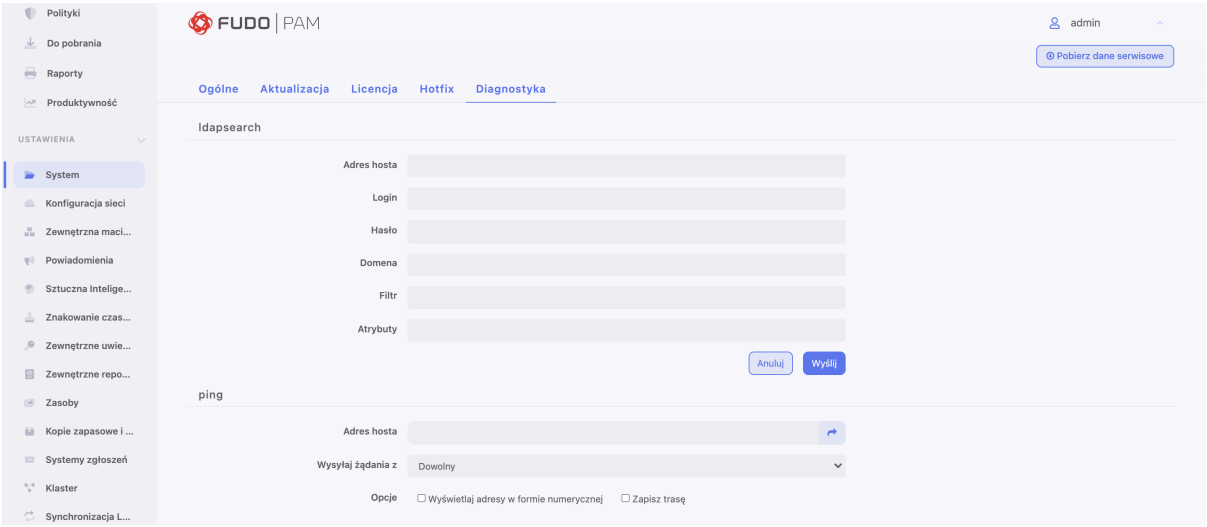
- *System*

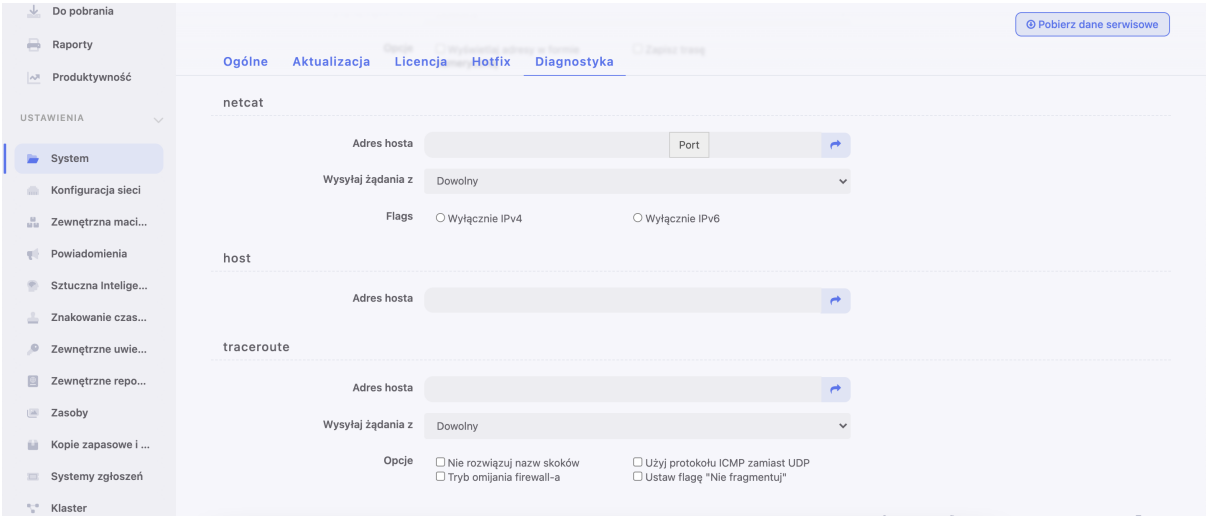
20.1.9 Diagnostyka

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
LDAP search	Narzędzie umożliwia bezpośrednie wysłanie zapytania do serwera LDAP.
Adres hosta	Adres IP serwera LDAP.
Login	Login użytkownika uprawnionego do przeglądania zawartości katalogu.
Hasło	Hasło użytkownika uprawnionego do przeglądania zawartości katalogu.
Domena	Domena, w której znajdują się żądane obiekty.
Filtr	Parametr filtrowania obiektów.
Atrybuty	Atrybuty zapytania LDAP.
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 Fudo PAM i hostem docelowym.
Nie rozwiązuj nazw skoków	Adresy kolejnych punktów przeskoku nie będą rozwiązywane do nazw mnemonicznych.
Użyj 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*

20.1.10 Szyfrowanie konfiguracji

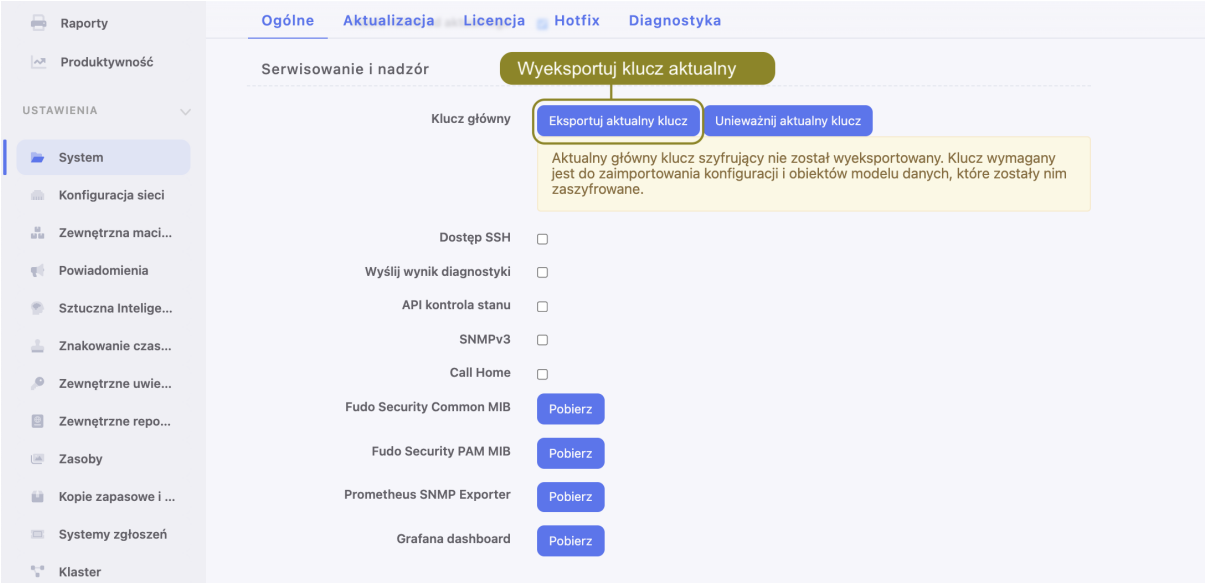
Główny klucz szyfrujący zapewnia bezpieczeństwo i poufność danych konfiguracyjnych, kopii zapasowych systemu i zewnętrznych wolumenów przechowywania danych. Klucz umożliwia również odzyskanie klucza szyfrującego wewnętrznego wolumenu danych w przypadku zaginięcia lub uszkodzenia kluczy zapisanych na nośnikach pamięci podczas inicjalizacji systemu.

Informacja:

- Klucz szyfrujący jest eksportowany do formatu PEM i szyfrowany SMIME z użyciem klucza publicznego/certyfikatu administratora.
- Aktualny *klucz główny* powinien być wyeksportowany i przechowywany w bezpiecznym miejscu.
- W przypadku skompromitowania *klucza głównego*, należy go unieważnić, co poskutkuje wygenerowaniem nowego klucza i ponownym zaszyfrowaniem danych.

Eksportowanie klucza głównego

1. Wybierz *Ustawienia* > *System*.
2. W sekcji *Serwisowanie i nadzór*, kliknij *Eksportuj aktualny klucz*.



3. Kliknij *Wybierz plik*, i wskaż plik z certyfikatem do zaszyfrowania klucza.

Informacja:

- Wygeneruj certyfikat i plik CSR (Certificate Signing Request) narzędziem `openssl`:

```
openssl req -newkey rsa:4096 -keyout privkey.pem -out req.pem
```

```
openssl req -nodes -newkey rsa:4096 -keyout privkey.pem -out req.pem # Do not prompt for a password.
```

- Podpisz wygenerowany plik CSR:

```
openssl x509 -req -in req.pem -signkey privkey.pem -out cert.pem
```

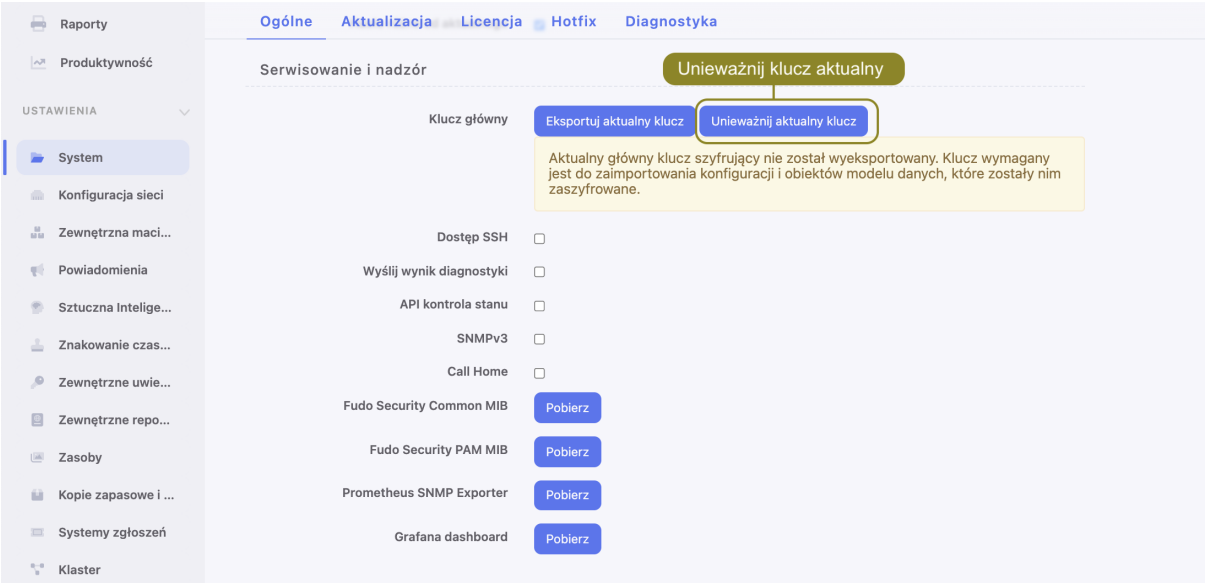
---

4. Kliknij *Zatwierdź* i zapisz plik z kluczem.

Unieważnienie klucza głównego

W przypadku skompromitowania *klucza głównego*, należy go unieważnić, co poskutkuje wygenerowaniem nowego klucza i ponownym zaszyfrowaniem danych.

1. Wybierz *Ustawienia* > *System*.
2. W sekcji *Serwisowanie i nadzór*, kliknij *Unieważnij aktualny klucz*.



3. Kliknij *Zatwierdź*.
4. Pamiętaj o konieczności *wyeksportowania nowego klucza*.

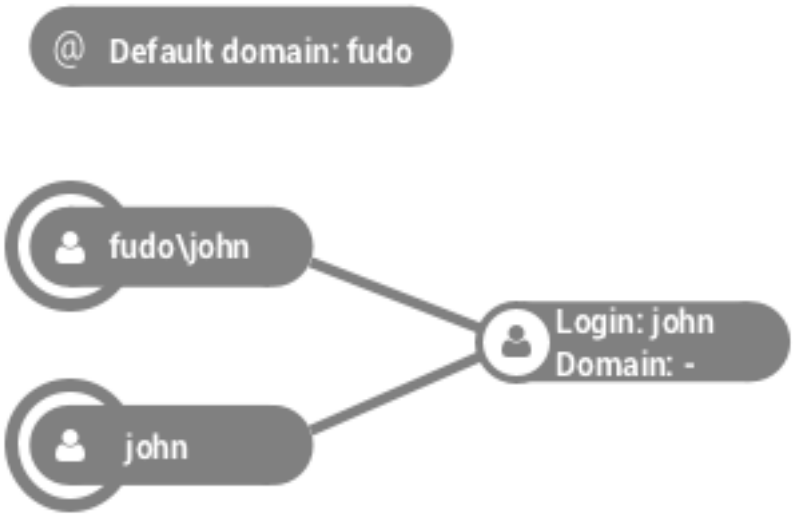
Tematy pokrewne:

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

20.1.11 Domyślna domena

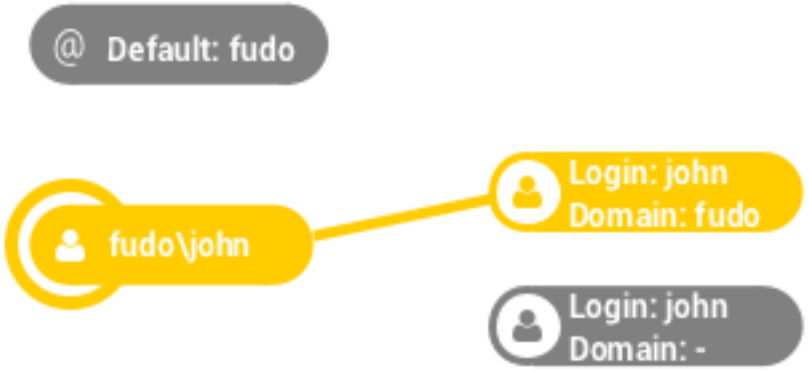
Informacja:

- W przypadku gdy została zdefiniowana domena domyślna a użytkownik nie ma przypisanej domeny, może uwierzytelniać się podając domenę domyślną lub jej nie wskazywać.

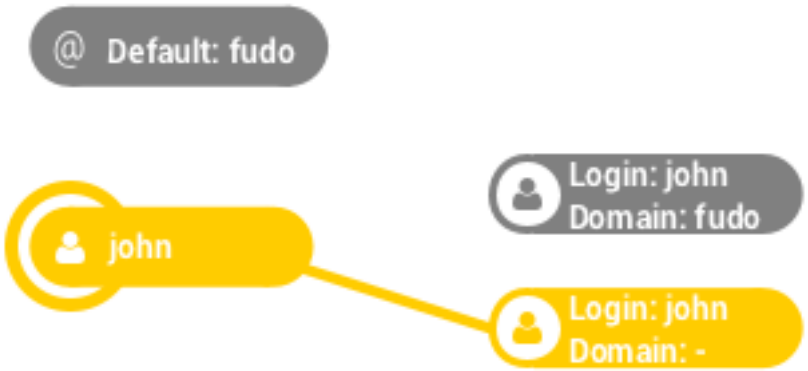


- W sytuacji, w której istnieją dwaj użytkownicy o tym samym loginie, z których jeden ma zdefiniowaną domenę taką samą jak domena domyślna, a drugi nie ma określonej domeny,

logując się z podaniem domeny, zostanie dopasowany użytkownik ze zdefiniowaną domeną.



W przypadku nie podania domeny, nastąpi dopasowanie użytkownika, który nie miał określonej domeny.



Definiowanie domeny domyślnej

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Uwierzytelnienie użytkowników i sesje*, wprowadź domenę domyślną.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

20.1.12 Złożoność haseł

Fudo PAM umożliwia definiowanie złożoności haseł, aby te były zgodne z polityką bezpieczeństwa organizacji.

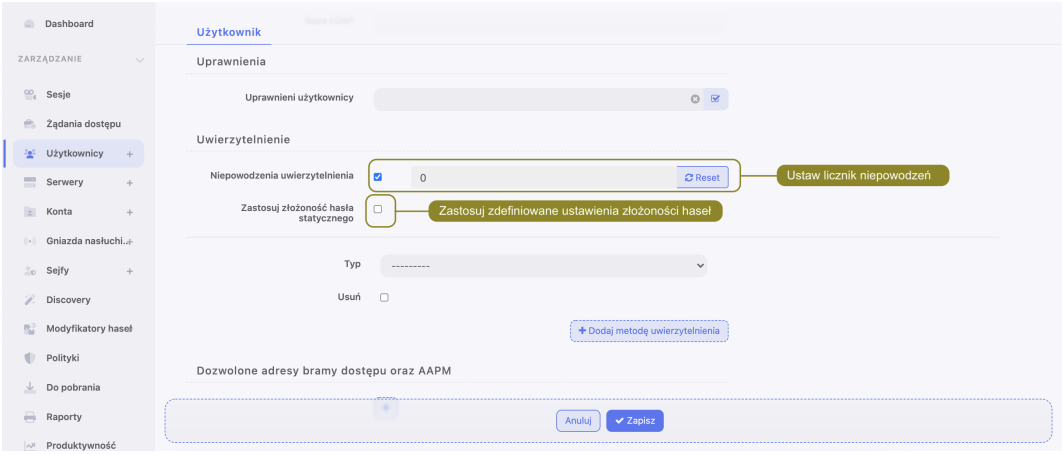
Definiowanie złożoności haseł

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Uwierzytelnienie użytkowników i sesje*, zaznacz opcję *Złożoność hasła*.

Informacja: Włączenie opcji *Złożoność hasła* spowoduje wymuszenie zmiany hasła u użytkowników, którzy mają włączoną opcję wymuszenia złożoności hasła statycznego, w przypadku których aktualne hasło nie jest zgodne z wymaganiami. Hasło będzie musiało zostać zmienione przy najbliższym logowaniu do *Portalu Użytkownika*.

3. Określ minimalną długość hasła.
4. Zaznacz *Małe litery* i określi minimalną liczbę małych liter.
5. Zaznacz *Wielkie litery* i określi minimalną liczbę wielkich liter.
6. Zaznacz *Znaki specjalne* i określi minimalną liczbę znaków specjalnych.
7. Zaznacz *Cyfry* i określi minimalną liczbę cyfr.
8. Zaznacz opcję *Hasło różne od aktualnego*, aby nowe hasło było różne od bieżącego.
9. Kliknij *Zapisz*.

Informacja: Aby wymusić złożoność haseł dla wybranego użytkownika, zaznacz opcję *Zastosuj złożoność hasła statycznego* w sekcji *Uwierzytelnienie*.



Tematy pokrewne:

- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

20.1.13 Single Sign On

Opcja Single Sign On umożliwia automatyczne zalogowanie do systemu. Fudo PAM pozwala uruchomić usługę Single Sign On dla Panelu Administracyjnego oraz Portalu Użytkownika.

20.1.13.1 Konfiguracja Fudo PAM

1. Skonfiguruj nazwę hosta `hostname.yourdomain.local`.
    - Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.

- Przejdź do zakładki *Nazwa i DNS*.
- W polu *Nazwa hosta*, wprowadź `hostname.yourdomain.local`.

2. Skonfiguruj serwer DNS wskazujący serwer DNS w domenie *yourdomain.local*.
   - Kliknij *+ Dodaj serwer DNS*, aby zdefiniować nowy serwer DNS.
   - Wprowadź adres IP serwera DNS.
   - Kliknij *Zapisz*.
3. Dodaj użytkownika, który posiada konto w rejestrze Active Directory.
   - *Zsynchronizuj konta użytkowników* lub
   - *dodaj konto ręcznie*, ze wskazaniem usługi Active Directory jako zewnętrznej metody uwierzytelnienia.

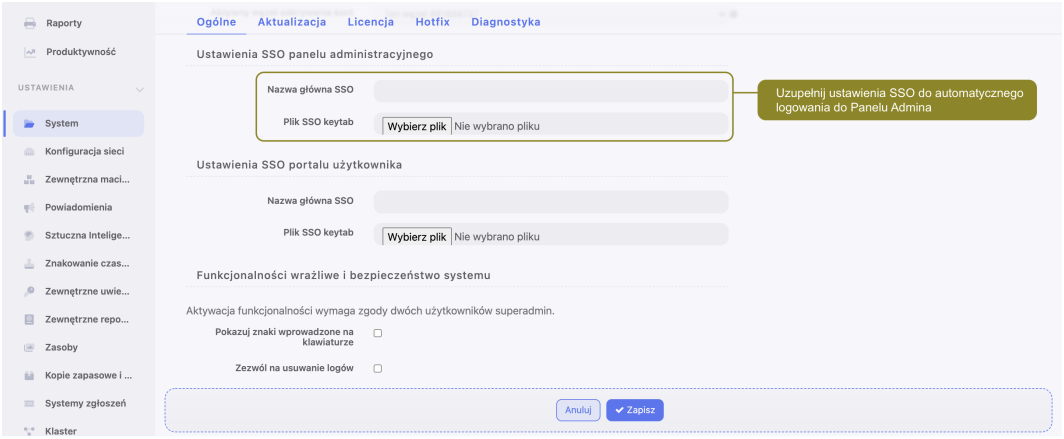
Informacja: W przypadku ręcznego dodania użytkownika, parametry *Fudo Domain* oraz *AD domain* powinny pokrywać się z nazwą domenową zdefiniowaną w identyfikatorze Kerberos.

20.1.13.2 Single Sign On do Panelu Administracyjnego

Ostrzeżenie: Usługa Single Sign On do Panelu Administracyjnego jest dostępna do konfiguracji tylko dla użytkowników o roli `superadmin`, natomiast mogą z niej korzystać użytkownicy z rolami `operator`, `admin` oraz `superadmin`.

Aby zdefiniować parametry usługi w ustawieniach systemowych, postępuj zgodnie z instrukcją:

- Wybierz z lewego menu *Ustawienia* > *System*.
- W sekcji *Ustawienia SSO panelu administracyjnego*, w polu *Nazwa główna SSO*, wprowadź identyfikator: `HTTP/hostname.yourdomain.local@yourdomain.local`.
- Wgraj plik `hostname.yourdomain.local.keytab` z identyfikatorem konta użytkownika w Active Directory oraz kluczami do szyfrowania i deszyfrowania żądań Kerberos.

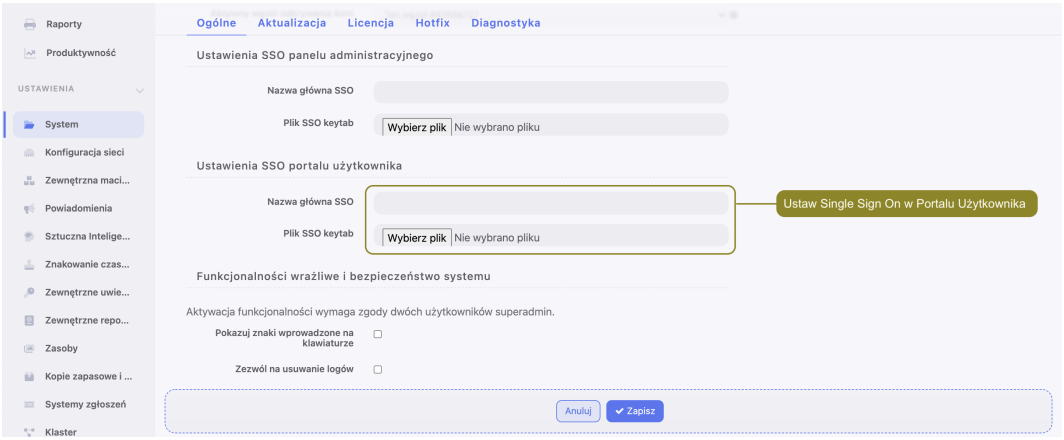


- Kliknij *Zapisz*.

20.1.13.3 Single Sign On do Portalu Użytkownika

Aby zdefiniować parametry usługi w ustawieniach systemowych, postępuj zgodnie z instrukcją:

- Wybierz z lewego menu *Ustawienia* > *System*.
- W sekcji *Ustawienia SSO portalu użytkownika*, w polu *Nazwa główna SSO*, wprowadź identyfikator: `HTTP/hostname.yourdomain.local@yourdomain.local`.
- Wgraj plik `hostname.yourdomain.local.keytab` z identyfikatorem konta użytkownika w Active Directory oraz kluczami do szyfrowania i deszyfrowania żądań Kerberos.



- Kliknij *Zapisz*.

20.1.13.4 Konfiguracja kontrolera domeny

1. Dodaj konto użytkownika za pomocą którego *Portal użytkownika* albo *Panel Admina* dostępne pod adresem *hostname.yourdomain.local*, będą komunikowały się z domeną *yourdomain.local*.

Informacja: Dodając konto, zaznacz opcję *Hasło nigdy nie wygasa*.

---

2. Na serwerze DNS dodaj wpisy forward oraz reverse DNS dla adresu *hostname.yourdomain.local*.
3. Utwórz identyfikator Kerberos dla Fudo PAM wykonując komendę w konsoli CMD lub PowerShell:

```
ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.local -mapuser
sso\nazwa_uzytkownika -pass    hasło_uzytkownika. - ptype KRB5_NT_PRINCIPAL -out
hostname.yourdomain.local.keytab
```

20.1.13.5 Konfiguracja stacji roboczej

1. Zaloguj się na konto użytkownika, który będzie łączył się z monitorowanymi systemami.

2. Uruchom przeglądarkę *Internet Explorer*.
3. Otwórz ustawienia *Internet options*.
4. Przejdź do zakładki *Security*.
5. Zaznacz opcję *Local intranet* i kliknij przycisk *Sites*.
6. Kliknij przycisk *Zaawansowane*.
7. Dodaj adres `hostname.yourdomain.local`.
8. Zamknij okno ustawień.

Tematy pokrewne:

- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

20.1.14 Modyfikatory haseł - aktywny węzeł klastra

Opcja wyboru aktywnego węzła klastra wskazuje instancję Fudo PAM, która realizuje zmianę haseł na monitorowanych systemach.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Modyfikatory haseł*, z listy rozwijalnej *Aktywny węzeł zmiany haseł*, wybierz węzeł odpowiedzialny za wykonanie skryptów modyfikujących hasła.

3. Kliknij *Zapisz*.

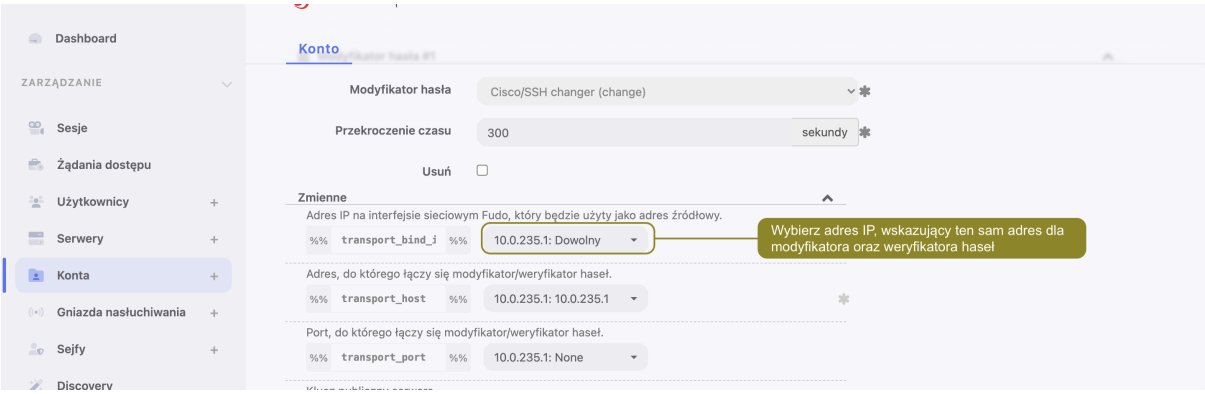
Informacja: W sytuacji, w której wskazany węzeł ulegnie awarii, zadanie zmiany haseł nie zostanie automatycznie podjęte przez inną instancję Fudo PAM. Automatyczna zmiana haseł wymaga zmiany przypisania aktywnego węzła lub przywrócenie działania uszkodzonej jednostki.

20.1.14.1 Manager haseł w klastrze

Fudo PAM umożliwia zmianę hasła na innym węźle klastra, niż ten, który jest wskazany jako aktywny węzeł klastra dla Modyfikatorów haseł.

W celu konfiguracji powyższego scenariusza, następujący warunek powinien zostać spełniony:

Definiując Modyfikator / Weryfikator hasła dla konta, wartość zmiennej `transport_bind_ip` powinna wskazywać ten sam węzeł dla wszystkich Modyfikatorów oraz Weryfikatorów hasła.



Jeśli wartości zmiennej `transport_bind_ip` będą wskazywać różne węzły klastra, Modyfikator / Weryfikator hasła będą działać na węźle, wskazanym jako *aktywny węzeł klastra dla Modyfikatorów haseł*.

Tematy pokrewne:

- *Modyfikatory haseł*
- *Uniwersalne modyfikatory haseł*

20.2 Konfiguracja sieci

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

20.2.1 Konfiguracja ustawień sieciowych

W specyfikacji domyślnej, 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.

20.2.1.1 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 Fudo PAM pod wskazanym adresem IP. Adres zarządzający używany jest również do replikacji danych pomiędzy węzłami klastra oraz *dostępu serwisowego poprzez protokół SSH*.

Informacja: Domyślnym portem dostępu serwisowego poprzez protokół SSH jest port numer 65522.

Wirtualny adres IP, który zostanie automatycznie przejęty przez drugi węzeł klastra w przypadku awarii węzła głównego.

Informacja: Klastrowy adres IP należy dodać na każdym węźle klastra i aktywować dla niego opcję wirtualnego adresu IP  .

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.

20.2.1.2 Ustawianie adresu IP z konsoli

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

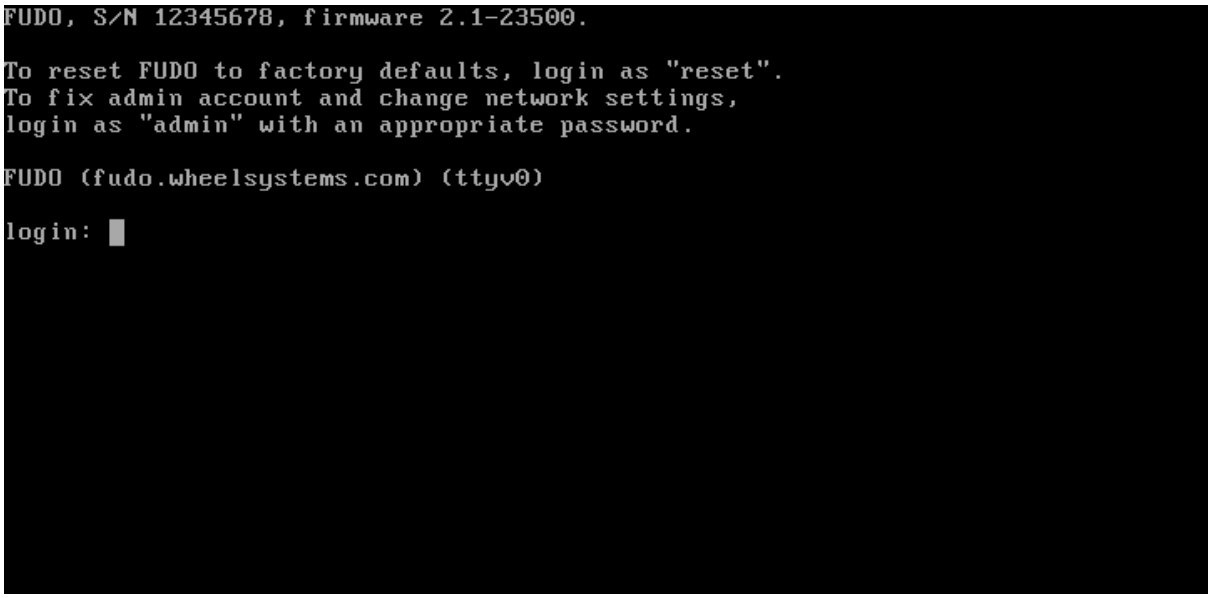
1. Podłącz do urządzenia monitor i klawiaturę.
2. Wprowadź login konta administratora.

Informacja: Domyślne dane logowania:

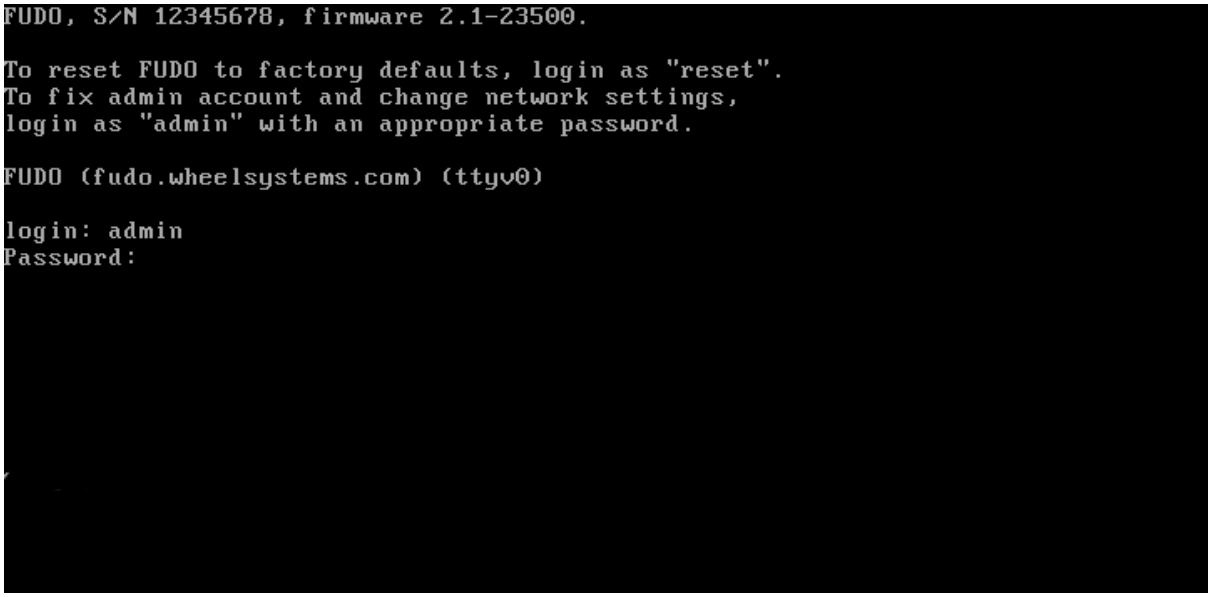
login: admin

hasło: proxycrypto

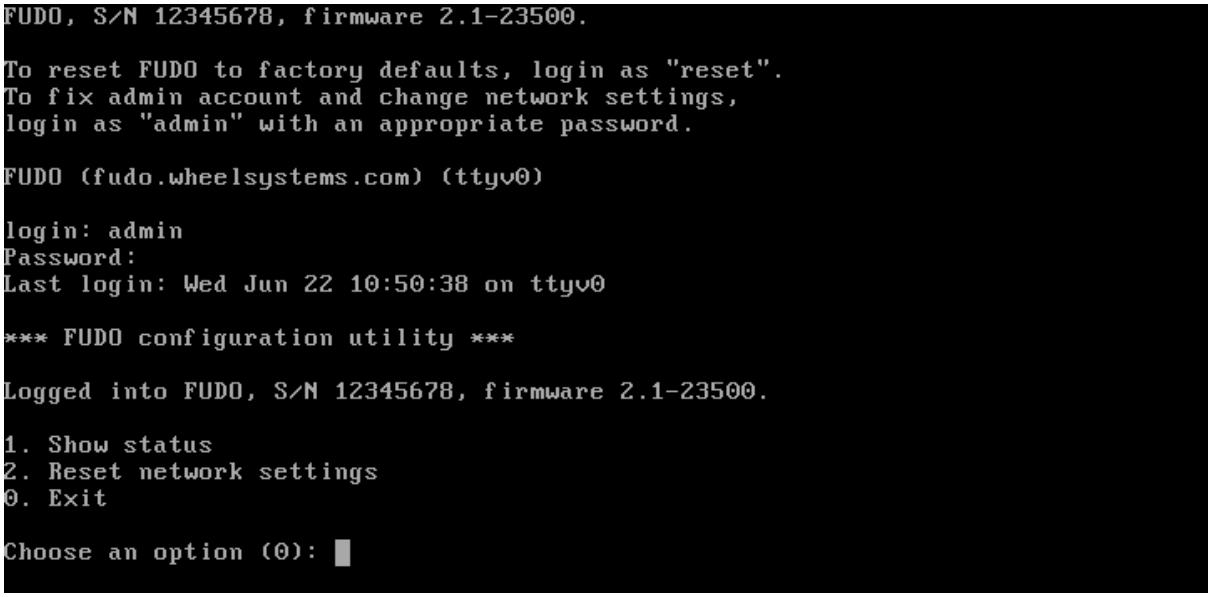
Dla wersji w chmurze domyślnym hasłem jest zazwyczaj identyfikator maszyny wirtualnej dostarczanej z Fudo PAM. Skontaktuj się ze sprzedawcą lub wsparciem technicznym, aby dowiedzieć się więcej.



3. Wprowadź hasło do konta administratora.



4. Wpisz 2 i naciśnij klawisz *Enter*.



5. 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):
```

6. Wprowadź nazwę interfejsu zarządzającego (poprzez interfejs zarządzający udostępniany jest panel administracyjny 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):
```

7. 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
```

8. 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):
```

20.2.1.3 Konfigurowanie mostu sieciowego

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

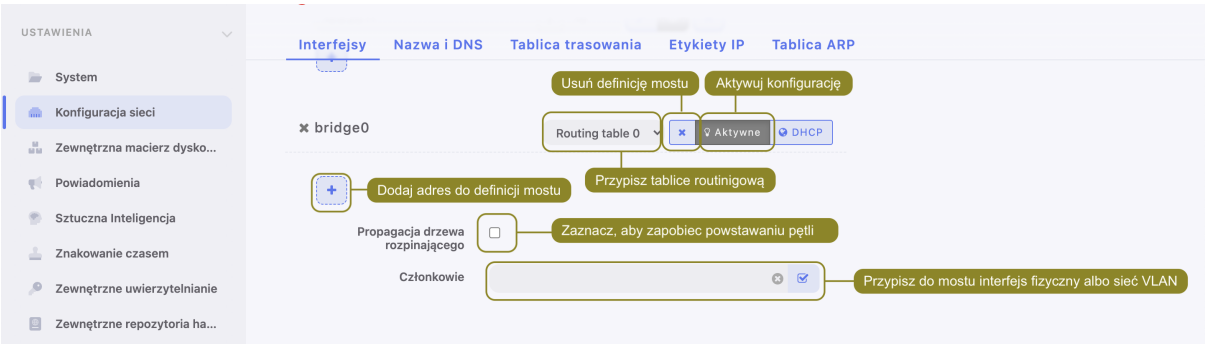
Aby stworzyć most sieciowy, postępuj zgodnie z poniższą instrukcją.

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*.



20.2.1.4 Konfigurowanie sieci wirtualnych (VLAN)

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

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

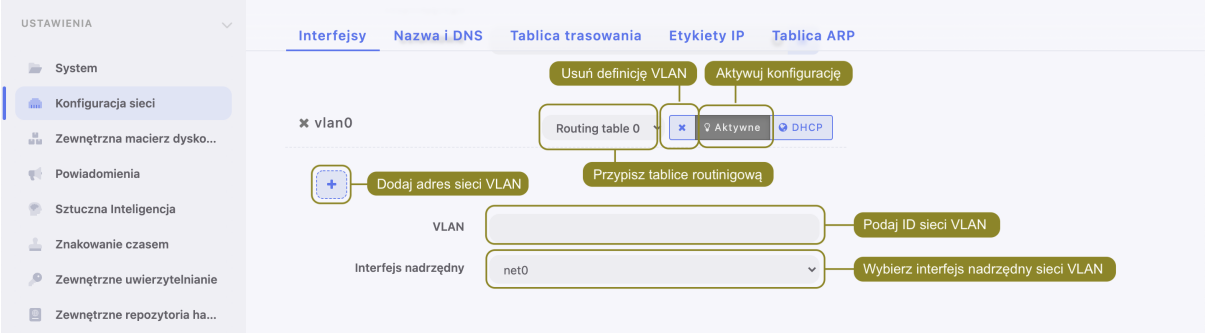
1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij *VLAN*, aby dodać definicję sieci wirtualnej.
3. Wybierz nadrzędny interfejs sieciowy oraz nadaj identyfikator konfigurowanej sieci wirtualnej.

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*.



20.2.1.5 Konfigurowanie agregacji połączeń LACP

Fudo PAM wspiera funkcję agregowania połączeń sieciowych, pozwalając na uzyskanie większej przepustowości transmisji danych lub implementację scenariusza umożliwiającego zapewnienie dostępności usług w przypadku awarii jednego z urządzeń sieciowych.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij *Agregacja połączeń*.
3. Skonfiguruj przypisanie interfejsów fizycznych.

Informacja: Konfiguracja agregacji połączeń wymaga usunięcia wszystkich adresów IP przypisanych bezpośrednio do interfejsów sieciowych będących członkami zagregowanego interfejsu.

---

4. Wprowadź adres IP oraz maskę podsieci, zapisaną w notacji CIDR, dla tworzonej agregacji połączeń.
5. Zaznacz opcje dodatkowe dla definiowanego adresu IP.

	Udostępnij panel administracyjny 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.

6. Kliknij *Zapisz*.

Tematy pokrewne:

- *Zarządzanie serwerami*
- *Gniazda nasłuchiwania*

20.2.2 Etykiety adresów IP

Etykiety adresów IP to parametry globalne konfiguracji. Objęte są procesem replikacji danych w obrębie klastra, ale ich przypisanie do adresów IP jest realizowane lokalnie na każdym z węzłów. Etykiety pozwalają na zachowania ciągłości dostępu do usługi uwierzytelnienia poprzez serwer LDAP w przypadku awarii węzła nadrzędnego a także implementację scenariusza balansowania obciążeniem węzłów klastra.

Definiowanie etykietowanego adresu IP

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Wybierz zakładkę *Etykiety IP*.
3. Kliknij +.
4. Wprowadź adres IP i nazwę etykiety.

Informacja: W nazwach etykiet dopuszczane są tylko małe litery, cyfry oraz znaki _ i -.

5. Kliknij *Zapisz*.
6. Użyj etykietowanego adresu IP w konfiguracji gniazda nasłuchiwania, serwera lub w konfiguracji zewnętrznych źródeł uwierzytelnienia.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

- *Zewnętrzne serwery uwierzytelniania*
- *Serwery*
- *Gniazda nasłuchiwania*

20.2.3 Konfiguracja tras routingu

W konfiguracji domyślnej, 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.

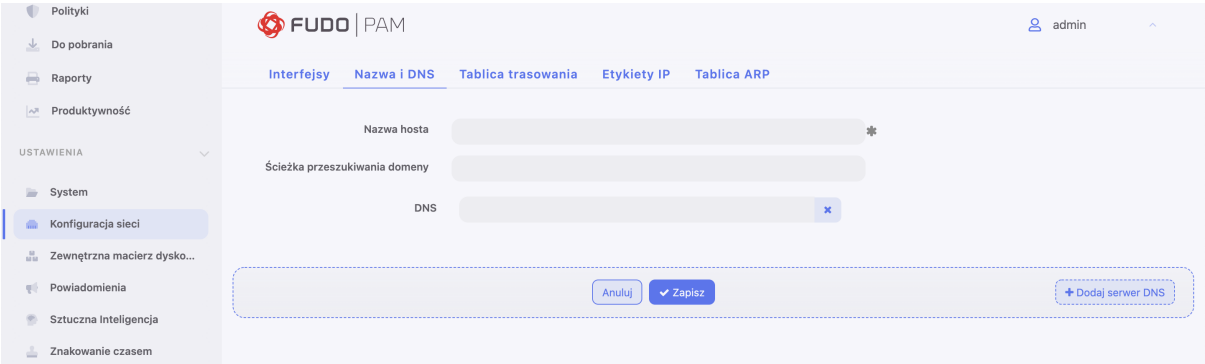
1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Zaznacz opcję usunięcia wybranej trasy routingu i kliknij *Zapisz*.

Tematy pokrewne:

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

20.2.4 Konfiguracja DNS

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



Ścieżka domeny wyszukiwania

Domena wyszukiwania umożliwia identyfikowanie hostów na podstawie nazwy skróconej. Na przykład wskazanie domeny wyszukiwania `tech.whl` pozwala na wskazanie hosta docelowego w postaci `ftp` zamiast `ftp.tech.whl`.

Aby dodać domenę wyszukiwania, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Nazwa i DNS*.
3. W polu *Ścieżka przeszukiwania domeny*, wprowadź domenę domyślną, np. `tech.whl`.

Informacja:

- Aby zdefiniować więcej niż jedną wartość, wprowadź żądane domeny oddzielając je znakiem spacji, na przykład: `tech.whl wheel.com`.
- Implementacja protokołu pozwala na zdefiniowanie do sześciu ścieżek przeszukiwania.

---

4. Kliknij *Zapisz*.

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*

20.2.5 Konfiguracja tablicy ARP

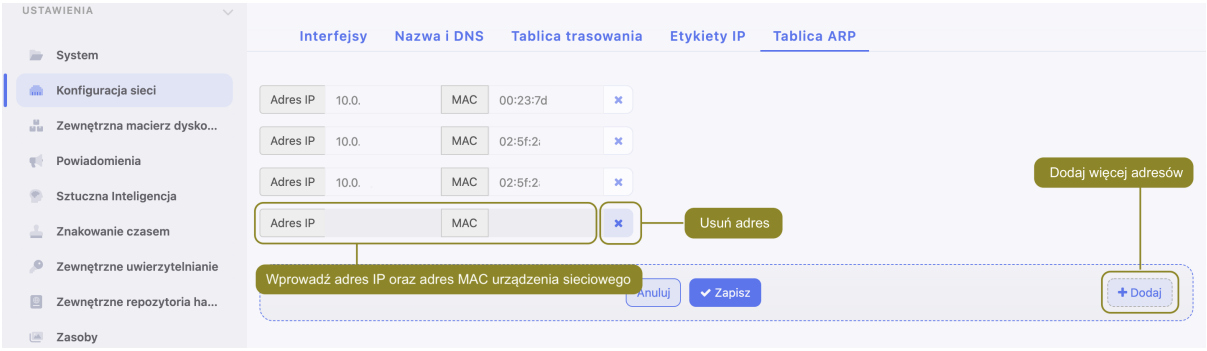
Utworzenie wpisu w tablicy *ARP* pozwala rozwiązać problemy w komunikacji sieciowej.

Dodawanie wpisu ARP

Aby dodać wpis w tablicy ARP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica ARP*.
3. Kliknij *+ Dodaj*.

4. Wprowadź adres IP oraz adres MAC urządzenia sieciowego.
5. Kliknij *Zapisz*.



Modyfikowanie wpisu w tablicy ARP

Aby zmodyfikować wpis ARP, postępuj zgodnie z poniższą instrukcją.

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

Usuwanie wpisu w tablicy ARP

Aby usunąć wpis ARP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica ARP*.
3. Zaznacz ikonę ✖ przy wybranym wpisie i kliknij *Zapisz*.

Tematy pokrewne:

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

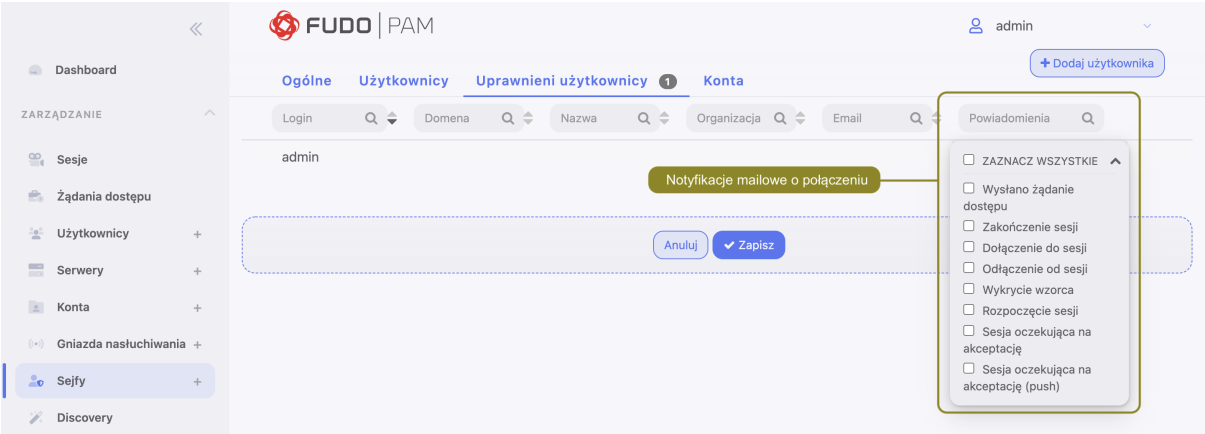
20.3 Powiadomienia

Fudo PAM może wysyłać powiadomienia mailowe o zdarzeniach dotyczących zdefiniowanych połączeń:

- wysłano żądanie dostępu,
- rozpoczęcie sesji,
- zakończenie sesji,
- dołączenie do sesji,
- odłączenie od sesji,
- sesja oczekująca na akceptację,
- sesja oczekująca na akceptację (push),

- wykrycie wzorca.

Usługa powiadomień definiowana jest przy tworzeniu nowego sejfu lub podczas edycji istniejących obiektów.



Informacja:

- Powiadomienia mogą otrzymywać użytkownicy o roli *operator*, *admin* lub *superadmin*.
- Otrzymywanie powiadomień wymaga zalogowania do panelu administracyjnego Fudo PAM i zaznaczenia opcji otrzymywania powiadomień w konfiguracji obiektu sejf pod zakładką *Uprawnieni użytkownicy*. Należy to wykonać dla każdego użytkownika, który ma otrzymywać powiadomienia.

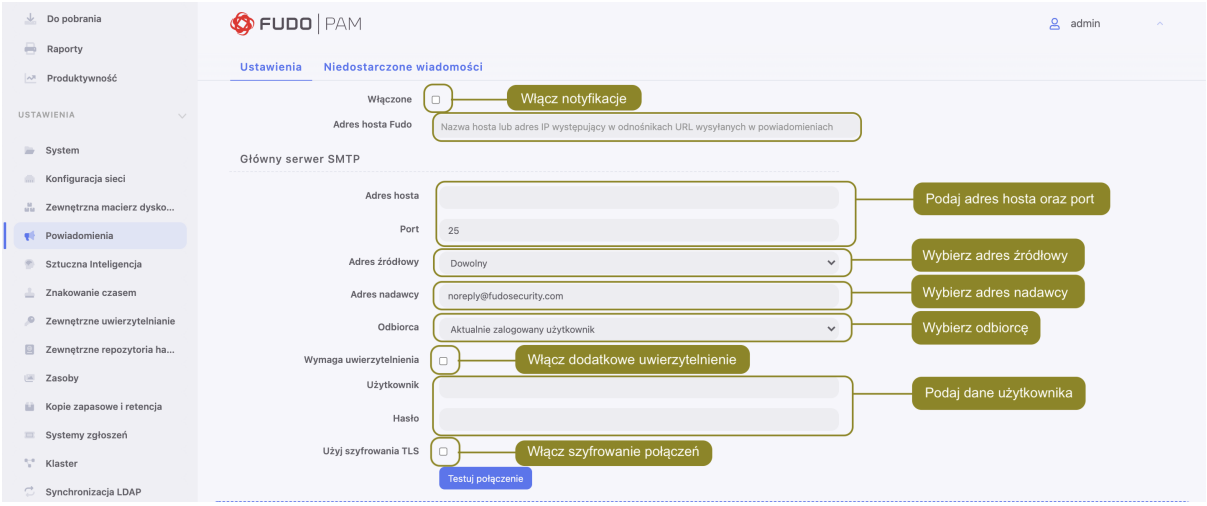
Wysyłanie powiadomień wymaga skonfigurowania serwera poczty SMTP.

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. Wprowadź *Adres hosta Fudo*, czyli nazwę hosta Fudo lub adres IP występujący w odnośnikach URL, wysyłanych w powiadomieniach.

Informacja: Podanie wartości *Adres hosta Fudo* jest konieczne przy konfiguracji notyfikacji o oczekujących sesjach. *Adres hosta Fudo* jest zmienną zarządzającą treścią notyfikacji gdyż służy do wygenerowania linku, który zostanie przesłany do użytkownika drogą mailową. Akceptacja oczekującej sesji będzie możliwa poprzez kliknięcie przesłanego linku.

4. Uzupełnij parametry konfiguracyjne Głównego serwera SMTP, oraz opcjonalnie Zapasowego serwera SMTP.

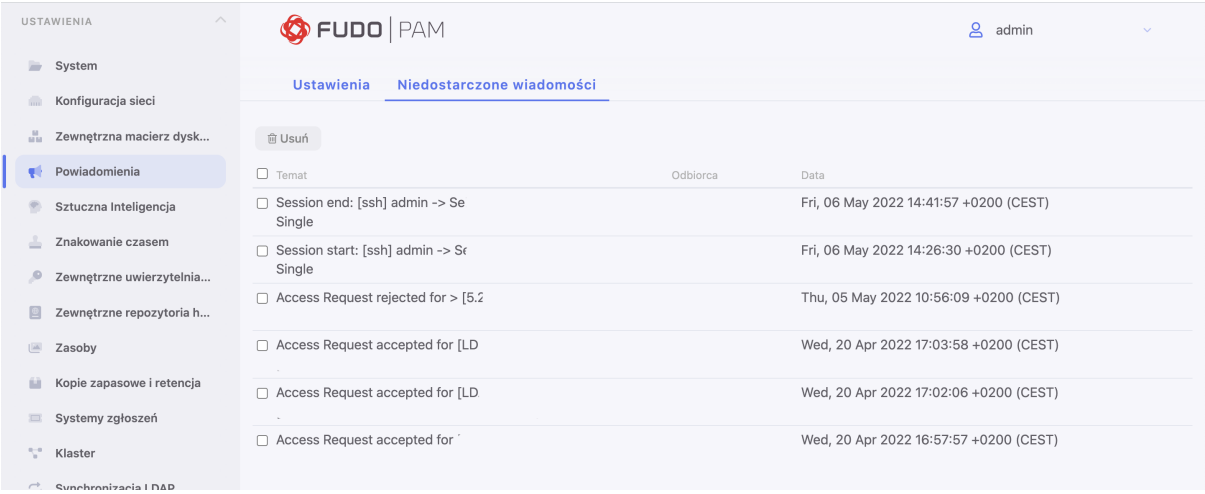


Parametr	Opis
Adres hosta	Adres serwera SMTP, na przykład `smtp.gmail.com`.
Port	Numer portu, na którym działa usługa SMTP.
Adres źródłowy	Adres IP albo adres interfejsu serwera SMTP.
Adres nadawcy	Adres email, z którego wysyłane będą powiadomienia.
Odbiorca	Adresat wiadomości testowej.
Wymaga uwierzytelnienia	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. Dodatkowo zaznacz opcję *Użyj STARTTLS*, jeśli serwer pocztowy ma zapewnić bezpieczne połączenie.

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

5. Kliknij  w celu wgrania certyfikatu urzędu certyfikacji. Wybierz format wyświetlenia wartości SHA1 albo MD5.
6. Kliknij *Zapisz*.

Aby zobaczyć listę wiadomości, które nie zostały dostarczone do odbiorcy z jakiegoś powodu, wybierz pod-zakładkę **Niedostarczone wiadomości**. W ten sposób możesz zareagować na problem oraz go naprawić, by użytkownicy mogli dostawać powiadomienia w przyszłości.



Tematy pokrewne:

- *Konta*

20.4 Sztuczna inteligencja

Fudo PAM buduje indywidualne profile behawioralne użytkowników, na podstawie których jest w stanie wykryć najdrobniejszą zmianę w ich zachowaniu i tym samym zapobiec naruszeniu bezpieczeństwa monitorowanych systemów.

Informacja: *Jest to wersja ewaluacyjna komponentu AI.*

20.4.1 Konfiguracja trenera modeli

Trenowanie modeli wymaga zaangażowania zasobów obliczeniowych. Odpowiednia konfiguracja systemu pozwoli na efektywne przetwarzanie archiwum sesji, przy zachowaniu responsywności systemu w obsłudze bieżących połączeń.

Aby zmienić konfigurację trenera modeli, postępuj zgodnie z poniższą instrukcją.

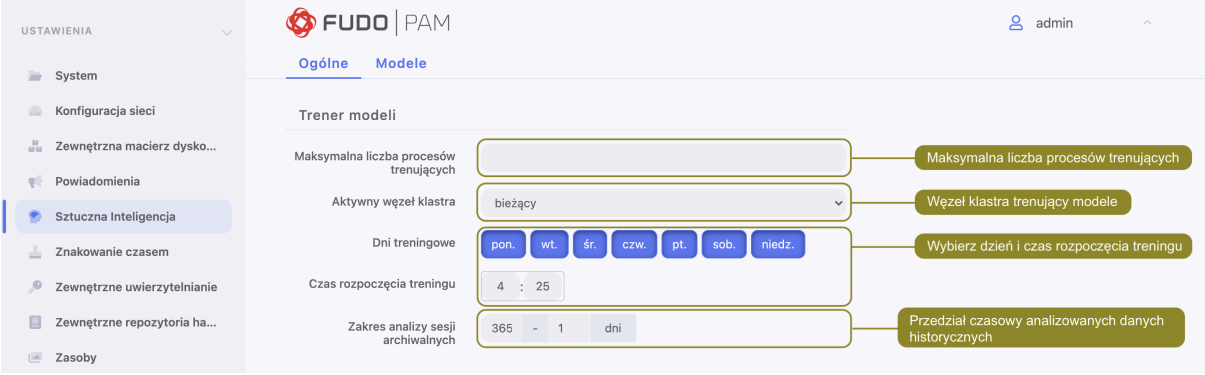
1. Wybierz z lewego menu *Ustawienia* > *Sztuczna Inteligencja*.
2. W sekcji *Trener modeli*, w polu *Maksymalna liczba procesów* określ liczbę procesów odpowiedzialnych za przetwarzanie sesji w celu zbudowania modeli.

Informacja: Wartość domyślna jest wartością optymalną, określoną na podstawie dostępnych zasobów sprzętowych. Faktyczna liczba procesów trenujących modele jest nie większa niż liczba dostępnych rdzeni procesorów.

---

3. Z listy rozwijalnej *Aktywny węzeł klastra*, wybierz węzeł odpowiedzialny za trenowanie modeli.
4. Wybierz dni tygodnia, w które będzie odbywało się trenowanie modeli.
5. Zdefiniuj czas rozpoczęcia procesu trenowania.

6. Określ przedział czasowy analizowania sesji archiwalnych.



7. W sekcji *Parametry modelu ilościowego*, w polu *Tolerancja*, określ dopuszczalne wahania liczby sesji/czasu trwania sesji.

Informacja: Parametr tolerancji wykorzystywany jest przy wyliczaniu ryzyka. Wartość tolerancji jest odejmowana od bieżącej liczby połączeń, a wyrażona w minutach, od czasu trwania pojedynczego połączenia.

---

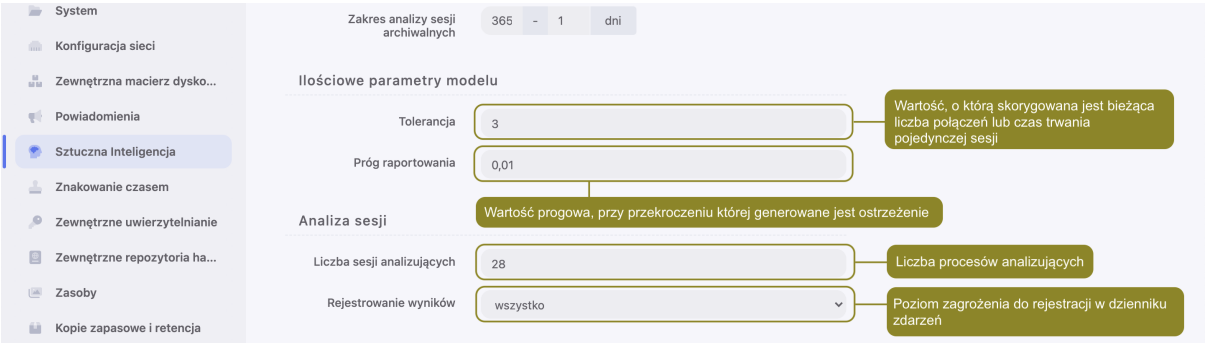
8. W polu *Próg raportowania* zdefiniuj dopuszczalne odchylenie od spodziewanych wartości.

Informacja: Wyrażony w procentach, próg raportowania określa wartość progową przy której wyzwalany jest alarm bezpieczeństwa związany z nadzwyczaj dużą liczbą sesji lub dłuższym niż typowy czasem trwania pojedynczego połączenia.

Np. próg raportowania wyznaczony na 1% spowoduje wyzwolenie alarmu w sytuacji, w której liczba połączeń odbiegająca od wartości spodziewanej została zaobserwowania w 1% przypadków.

---

9. W sekcji *Analiza sesji*, w polu *Liczba procesów analizujących* określ liczbę procesów odpowiedzialnych za bieżącą analizę połączeń. Dodatkowo, z listy rozwijanej *Rejestrowanie wyników* wybierz poziom zagrożenia, który chcesz rejestrować w dzienniku zdarzeń.



Informacja: W sytuacji, w której pula dostępnych procesów analizujących zostaje wyczerpana, bieżąca analiza danych zostaje wstrzymana. Po zakończeniu sesji, dane zostają przekazane do analizy.

---

10. Kliknij *Zapisz*.

20.4.2 Konfigurowanie modeli behawioralnych

Parametryzacja modeli pozwala na odpowiednie dopasowanie charakterystyk do specyfiki środowiska, w którym funkcjonuje Fudo.

SSH

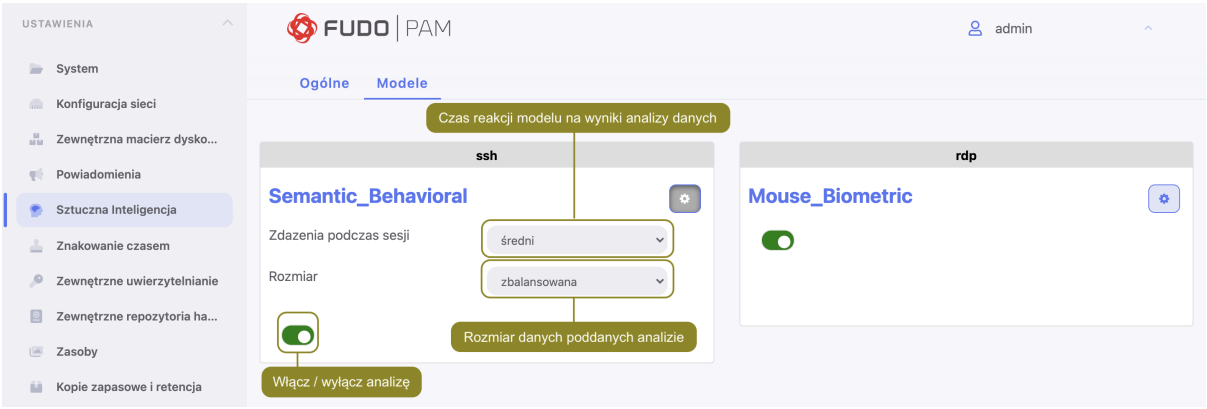
Aby zmienić konfigurację modelu dla protokołu SSH, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Sztuczna Inteligencja*.
2. Kliknij zakładkę *Modele*.
3. Kliknij ikonę dla modelu SSH, aby wyświetlić parametry konfiguracyjne.
4. Z listy rozwijalnej *Czas reakcji*, wybierz jak szybko model ma reagować na wyniki analizy.

Informacja: Szybszy czas reakcji może potencjalnie skutkować błędami w klasyfikacji, z uwagi na mniejszą próbkę danych która została poddana analizie.

---

5. Z listy rozwijalnej *Objętość analizowanych danych*, wybierz ile danych historycznych zostanie użyte do zbudowaniu modelu.



6. Kliknij *Zapisz*.

RDP

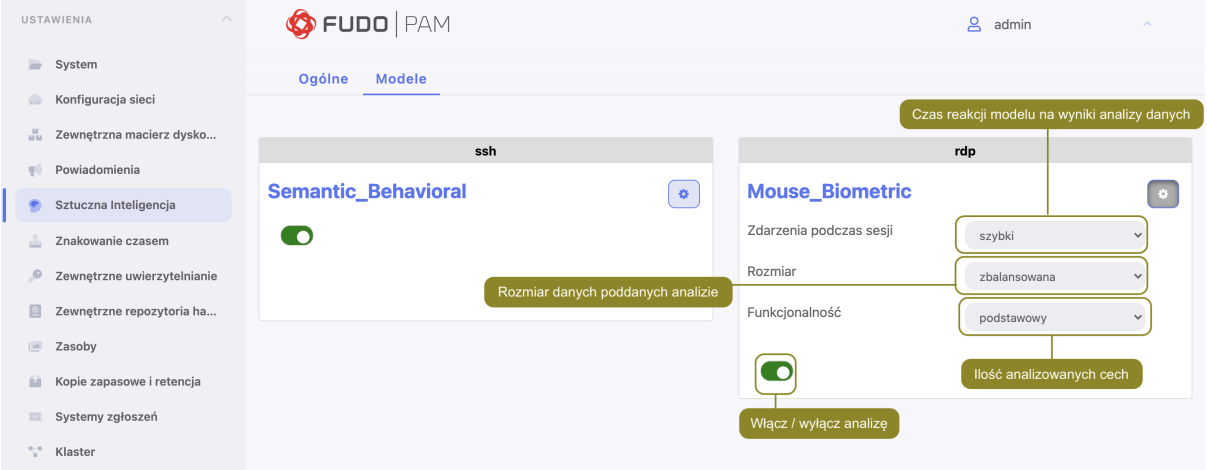
Aby zmienić konfigurację modelu dla protokołu RDP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Sztuczna Inteligencja*.
2. Kliknij zakładkę *Modele*.
3. Kliknij ikonę dla modelu RDP, aby wyświetlić parametry konfiguracyjne.
4. Z listy rozwijalnej *Czas reakcji*, wybierz jak szybko model ma reagować na wyniki analizy.

Informacja: Szybszy czas reakcji może potencjalnie skutkować błędami w klasyfikacji, z uwagi na mniejszą próbkę danych.

---

5. Z listy rozwijalnej *Objętość analizowanych danych*, wybierz ile danych historycznych zostanie użyte do zbudowaniu modelu.
6. Z listy rozwijalnej *Funkcjonalność*, wybierz ilość analizowanych cech.



Informacja: Funkcjonalność determinuje zbiór cech poddawany analizie, który bezpośrednio przekłada się na dokładność i czas budowania modelu. Większy zbiór pozwoli na zbudowanie dokładniejszego modelu kosztem czasu potrzebnego na jego wytrenowanie.

7. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konta*

20.5 Znakowanie czasem

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

Wymagania

- Funkcjonalność znakowania sesji wymaga podpisania odrębnej umowy z instytucją świadczącą usługę znakowania czasem.
- Certyfikat oraz kluczy prywatny usługi znakowania czasem dostarczone przez usługodawcę.
- W przypadku usługi świadczonej przez PWPW, adres IP `193.178.164.5` musi być osiągalny przez Fudo PAM.
- W przypadku usługi świadczonej przez KIR, adres `http://www.ts.kir.com.pl/HttpTspServer` musi być osiągalny przez Fudo PAM.
- Usługa znakowania czasem udostępniana przez KIR, wymaga skonfigurowania serwera DNS. Szczegóły na temat konfigurowania usługi DNS, znajdziesz w rozdziale *Konfiguracja DNS*.

Dane przesyłane do dostawcy usługi znakowania czasem

Podczas znakowania czasem sesji generowany jest hash, który następnie wysyłany jest do dostawcy usługi. Hash ten tworzony jest w oparciu o dane na temat sesji z tabeli `fudo_session` oraz zawartość zrzutu RAW danej sesji. Wysyłany hash jest jednokierunkowy, co zapewnia brak możliwości wyodrębnienia informacji na temat sesji.

Informacja: Aby zrzut RAW był generowany, należy upewnić się, że opcja *Nagrywanie sesji* w konfiguracji konta ustawiona została na `wszystko` lub `raw` (zapoznaj się z przykładem w rozdziale *Dodawanie konta typu regular*).

Konfigurowanie usługi znakowania czasem

Informacja:

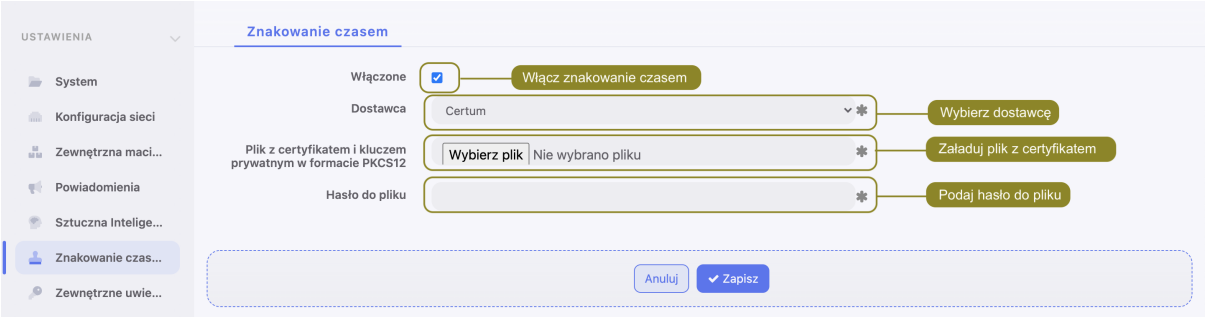
- Znacznikiem czasu zostaną opatrzone jedynie sesje, które zostały zakończone po włączeniu usługi.

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

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*.



Tematy pokrewne:

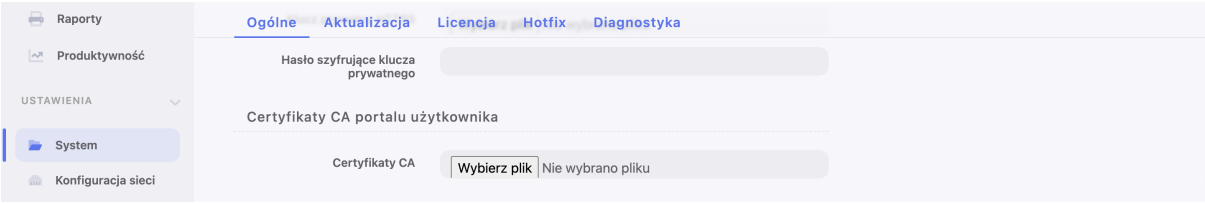
- *Mechanizmy bezpieczeństwa*

20.6 Model uwierzytelniania w oparciu o certyfikaty

Fudo PAM umożliwia logowanie certyfikatem do serwera docelowego.

W celu konfiguracji `certyfikatu` jako metody uwierzytelnienia, postępuj zgodnie z instrukcją:

1. Wybierz *Ustawienia* > *System*
2. W polu *Certyfikaty CA* sekcji *Certyfikaty CA portalu użytkownika* załaduj plik z certyfikat(ami) w formacie PEM.

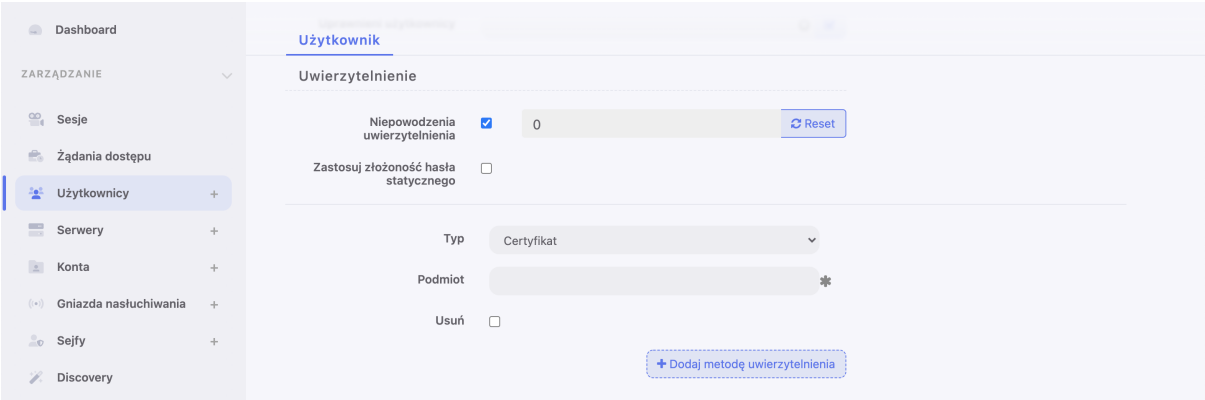


3. Kliknij *Zapisz*.
4. Wybierz *Zarządzanie* > *Użytkownicy* i wybierz użytkownika, dla którego chcesz skonfigurować metodę uwierzytelnienia `certyfikat`, albo

Załóż nowego użytkownika poprzez kliknięcie ikonki + w menu głównym zakładki *Użytkownicy*, albo wybierz *Zarządzanie* > *Użytkownicy* i kliknij + *Dodaj*.

5. W sekcji *Uwierzytelnienie* wybierz Typ: `Certyfikat`.
6. Podaj *Podmiot*.

Informacja: Podmiot powinien być zgodnym z wymaganiami RFC 2253 albo RFC 4514.



7. Kliknij *Zapisz*.

Related Topics:

- *Dodawanie użytkownika*

20.7 Zewnętrzne serwery uwierzytelniania

Uwierzytelnienie użytkowników za pomocą zewnętrznych serwerów uwierzytelniania wymaga skonfigurowania połączeń z serwerami usług danego typu:

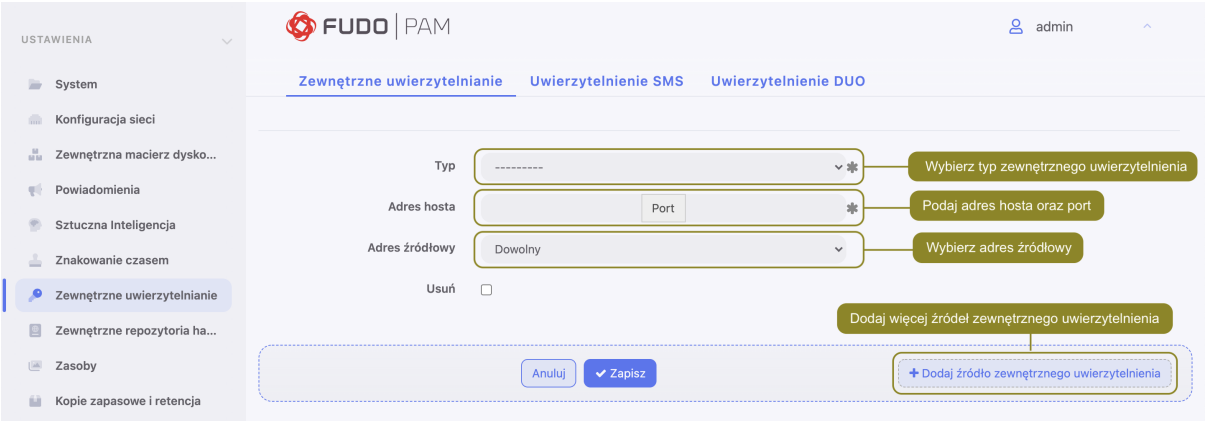
- *CERB*,
- *RADIUS*,
- *LDAP*,
- *Active Directory*,
- *SMS*,
- *DUO*
- *Azure*,

- *Okta*.

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*.



20.7.1 Definicja serwera zewnętrznego uwierzytelniania

Aby dodać serwer uwierzytelniania, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Kliknij *+ Dodaj źródło zewnętrznego 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.
Adres źródłowy	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.
Adres źródłowy	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.
Adres źródłowy	Adres IP, z którego będą wysyłane zapytania do serwera uwierzytelniania.
Bind DN	Miejsce w strukturze katalogowej, w której zawarte są definicje użytkowników uwierzytelnianych w usłudze LDAP. Np. `dc=example,dc=com`
Active Directory	
Adres	Adres IP serwera lub nazwa hosta.
Port	Numer portu, na którym nasłuchuje usługa AD.
Adres źródłowy	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.
Połączenie szyfrowane	Ta opcja jest konieczna do zaznaczenia, aby użytkownicy domenowi mogli zmieniać hasło na Portalu Użytkownika.
Login	Login konta uprzywilejowanego do zmiany hasła użytkownika domenowego na serwerze Active Directory.
Sekret	Sekret do nawiązywania połączeń do zmiany hasła użytkownika domenowego na serwerze Active Directory.
Powtórz sekret	Sekret do nawiązywania połączeń do zmiany hasła użytkownika domenowego na serwerze Active Directory.

Informacja: Etykietowane adresy IP

W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres źródłowy* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

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*.

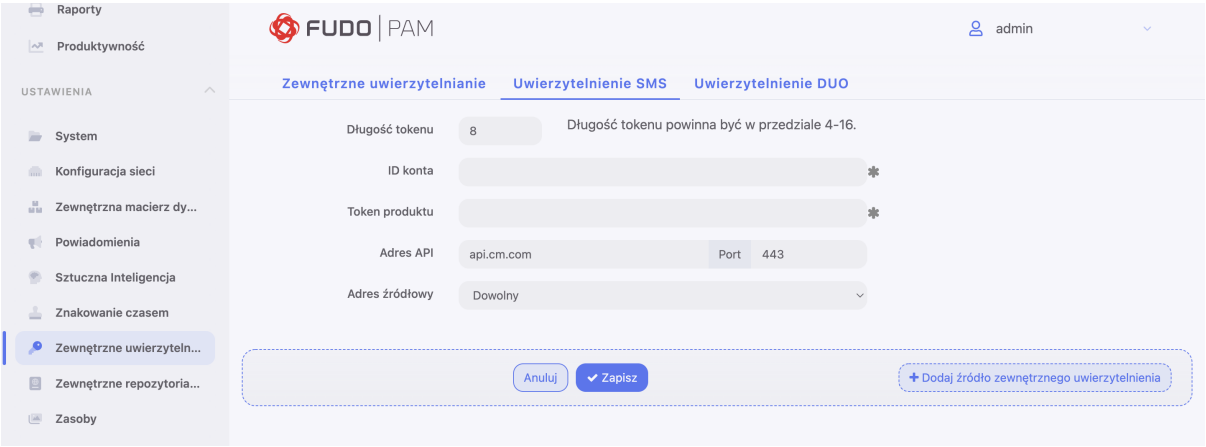
Usuwanie definicji serwera zewnętrznego uwierzytelniania

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.

20.7.2 Definicja uwierzytelniania SMS

1. Wybierz *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Wybierz zakładkę **Uwierzytelnienie SMS**.



- Wprowadź *Długość tokenu*.

Informacja: Długość tokenu powinna być w przedziale 4-16.

- Wprowadź *ID konta*.
- Wprowadź *Token produktu*.
- Wprowadź *Adres API* oraz *port*.

Informacja: Wartości dla *ID konta*, *Token produktu* oraz *Adres API* są generowane po stronie dostawcy usług CM.COM. W tym celu jest wymagana rejestracja konta w tym serwisie.

- Wybierz *Adres źródłowy*.

3. Kliknij *Zapisz*.
4. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
5. Znajdź i wybierz użytkownika, dla którego chcesz uruchomić uwierzytelnianie SMS.

- Wprowadź numer telefonu w polu **Telefon**.
- Pod sekcją **Uwierzytelnienie** wybierz *Typ: SMS*
- Z listy **Pierwszy składnik** wybierz *Hasło statyczne* albo *Zewnętrzne uwierzytelnianie* (AD albo LDAP).

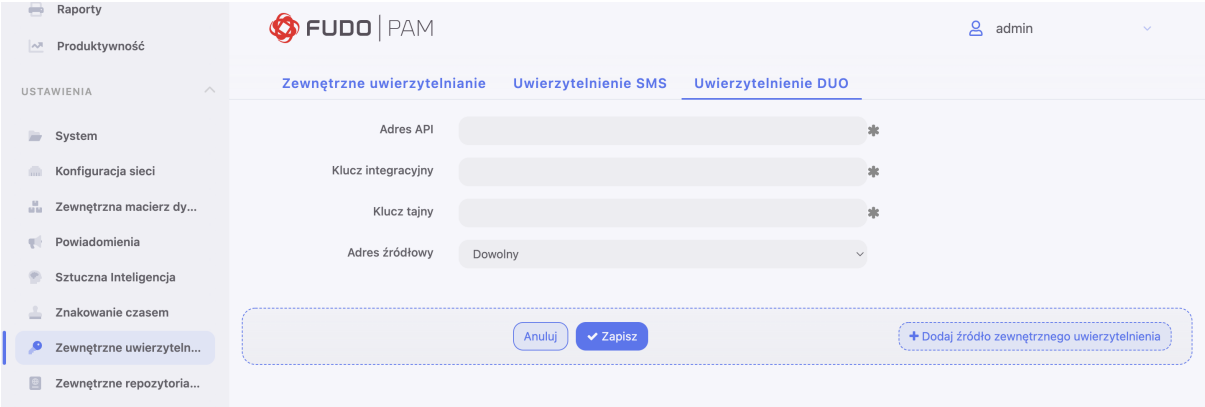
6. Kliknij *Zapisz*.
7. Zaloguj się na User Portal przy pomocy SMS kodu.

20.7.3 Definicja uwierzytelniania DUO

1. Pobierz i zainstaluj aplikację mobilną Duo Mobile.
2. Zarejestruj się na stronie Duo Security w celu stworzenia własnego konta.
3. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
4. Wybierz zakładkę **Uwierzytelnienie DUO**.

- Ze swojego profilu na Duo Security wprowadź: *Adres API*, *Klucz integracyjny* oraz *Klucz tajny*.
- Wybierz *Adres źródłowy*.

5. Kliknij *Zapisz*.



6. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
7. Znajdź i wybierz użytkownika, dla którego chcesz uruchomić uwierzytelnienie DUO.

- Pod sekcją **Uwierzytelnianie** wybierz *Typ: DUO*.

- Z listy **Pierwszy składnik** wybierz *Hasło statyczne* albo *Zewnętrzne uwierzytelnianie* (AD albo LDAP).
- Wprowadź *Użytkownik DUO*.
- Wprowadź *ID użytkownika DUO*.

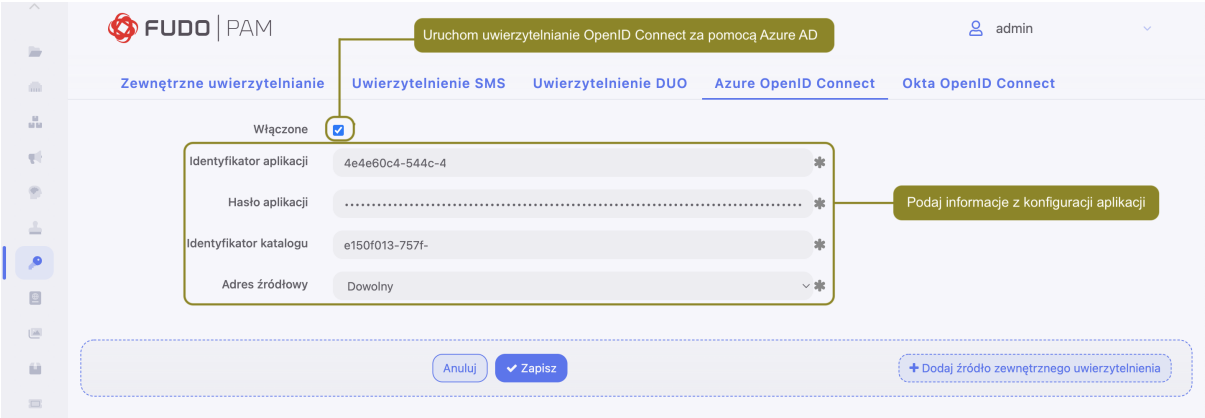
8. Kliknij *Zapisz*.
9. Zaloguj się na portal, akceptując notyfikację typu push z aplikacji Duo Mobile.

20.7.4 Definicja uwierzytelniania Azure

Definicja uwierzytelnienia przez Azure jest globalną metodą uwierzytelniania i nie jest przywiązywana do użytkownika. Zatem jeśli użytkownik nie ma ustawionych żadnych metod uwierzytelniania, to też może się uwierzytelniać korzystając z OpenID Connect w Portalu Użytkownika oraz w Panelu Admina.

Postępuj zgodnie z instrukcją, aby ustawić uwierzytelnienie za pomocą Azure:

1. Wybierz *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Wybierz zakładkę **Azure OpenID Connect** .
3. Zaznacz opcję *Włączone* dla uruchomienia uwierzytelnienia OpenID Connect za pomocą Azure AD.



Ostrzeżenie: W celu poprawnej konfiguracji OIDC, w aplikacji Azure powinien zostać zdefiniowany dozwolony redirect URL. Taki adres URL powinien wskazywać ścieżkę `/oidc` adresów, wykorzystywanych dla hostowania Panelu Admina oraz Portalu Użytkownika. Na przykład,

`https://mgmt.fudo/oidc`

`https://10.10.0.1/oidc`

`https://ag.fudo/oidc`

4. Podaj informację ze swojego profilu aplikacji w Azure:

- Wprowadź *Identyfikator aplikacji* - ID Aplikacji (Klienta) w konfiguracji aplikacji.
- Wprowadź *Hasło aplikacji* - sekret Klienta w konfiguracji aplikacji.
- Wprowadź *Identyfikator katalogu* (tenant) w konfiguracji aplikacji.

> **Informacja:** Wartości do wyżej wymienionych pól są dostępne w profilu aplikacji w Azure.

- Wybierz *Adres źródłowy* do połączenia z Azure AD.

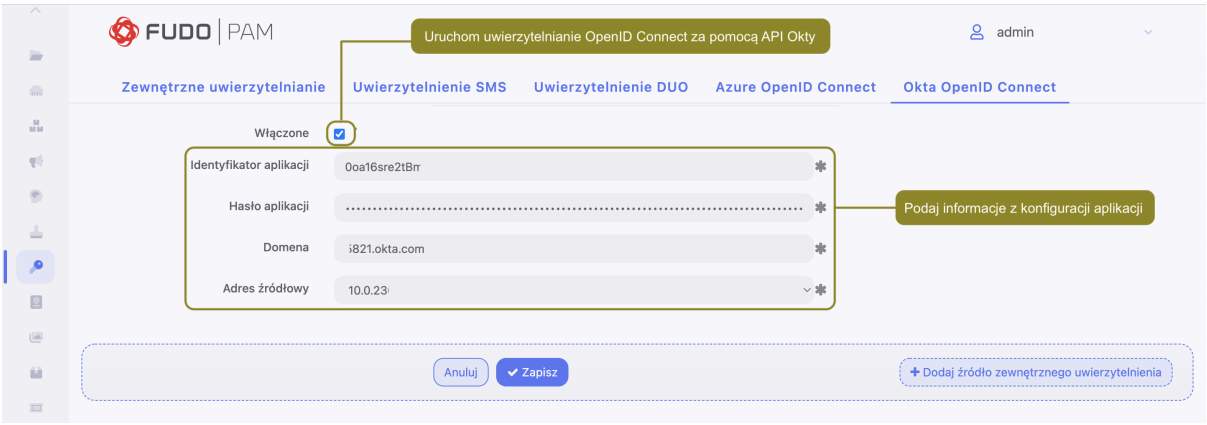
5. Kliknij *Zapisz*.

20.7.5 Definicja uwierzytelniania Oktą

Definicja uwierzytelnienia przez Oktę jest globalną metodą uwierzytelniania i nie jest przywiązywana do użytkownika. Zatem jeśli użytkownik nie ma ustawionych żadnych metod uwierzytelniania, to też może się uwierzytelniać korzystając z OpenID Connect w Portalu Użytkownika oraz w Panelu Admina.

Postępuj zgodnie z instrukcją, aby ustawić uwierzytelnienie za pomocą Okty:

1. Wybierz *Ustawienia* > *Zewnętrzne uwierzytelnianie*.
2. Wybierz zakładkę **Okta OpenID Connect** .
3. Zaznacz opcję *Włączone* dla uruchomienia uwierzytelnienia OpenID Connect za pomocą Okty.



> **Ostrzeżenie:** W celu poprawnej konfiguracji OIDC, w aplikacji Okta powinien zostać zdefiniowany dozwolony redirect URL. Taki adres URL powinien wskazywać ścieżkę `/oidc` adresów, wykorzystywanych dla hostowania Panelu Admina oraz Portalu Użytkownika. Na przykład,
>
> `https://mgmt.fudo/oidc`

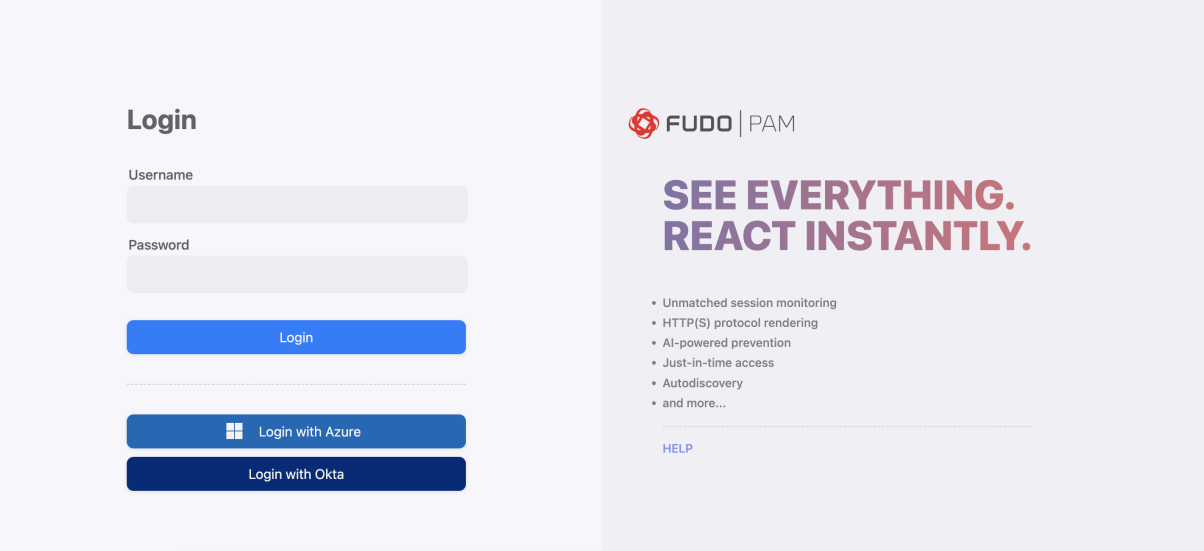
```
https://10.10.0.1/oidc

https://ag.fudo/oidc
```

4. Podaj informację ze swojego profilu aplikacji w Okta:
    - Wprowadź *Identyfikator aplikacji*. ID Aplikacji (Klienta) w konfiguracji aplikacji.
    - Wprowadź *Hasło aplikacji* - sekret Klienta w konfiguracji aplikacji.
    - W polu *Domena* wprowadź nazwę domeny w Okcie (na przykład, `dev-68970590.okta.com`).

    Informacja: Wartości do wyżej wymienionych pól są dostępne w profilu aplikacji w Okcie.

    - Wybierz *Adres źródłowy* do połączenia z API Okty.
5. Kliknij *Zapisz*.

Zaloguj się za pomocą skonfigurowanych metod uwierzytelniania:



Tematy pokrewne:

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

20.8 Zewnętrzne repozytoria haseł

Fudo PAM wspiera zewnętrzne repozytoria haseł do zarządzania hasłami dostępowymi.

20.8.1 CyberArk Enterprise Password Vault

Dodawanie definicji repozytorium haseł

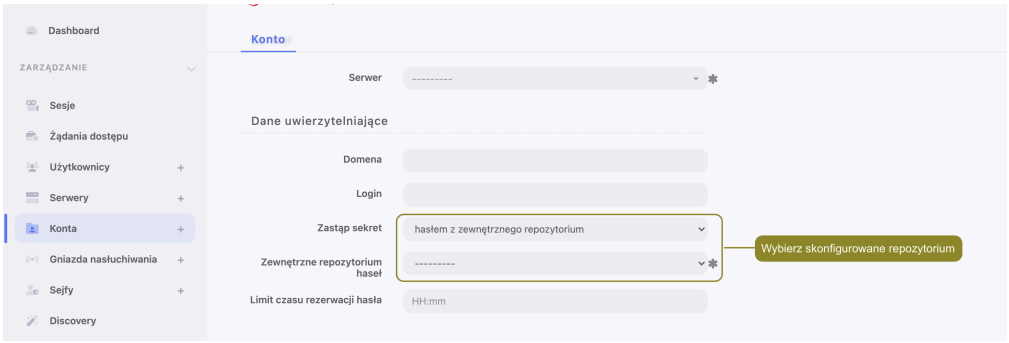
1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Z listy rozwijalnej *Typ* wybierz `CyberArk Enterprise Password Vault`.
4. Wprowadź nazwę obiektu.
5. W polu *URL*, wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

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

Przykład: `https://10.0.0.2/PWCWeb/`

---

6. Wprowadź identyfikator aplikacji.
7. Określ format konta.
8. Kliknij *Zapisz*.
9. Przypisz repozytorium haseł do konta.
    - Wybierz *Zarządzanie* > *Konta*.
    - Wyszukaj i kliknij definicję konta.
    - W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastąp sekret*, wybierz *hasłem z zewnętrznego repozytorium*.
    - Z listy rozwijalnej *Zewnętrzne repozytorium haseł*, wybierz wcześniej zdefiniowane repozytorium.



- 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*

20.8.2 Hitachi ID Privileged Access Manager

Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Uzupełnij parametry konfiguracyjne serwera.
4. Z listy rozwijalnej *Typ* wybierz `Hitachi ID Privileged Access Manager`.
5. Wprowadź nazwę obiektu.
6. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

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

Przykład: `https://10.0.0.2/PWCWeb/`

---

7. W polu *Login* wprowadź nazwę użytkownika uprawionego do pobierania haseł.

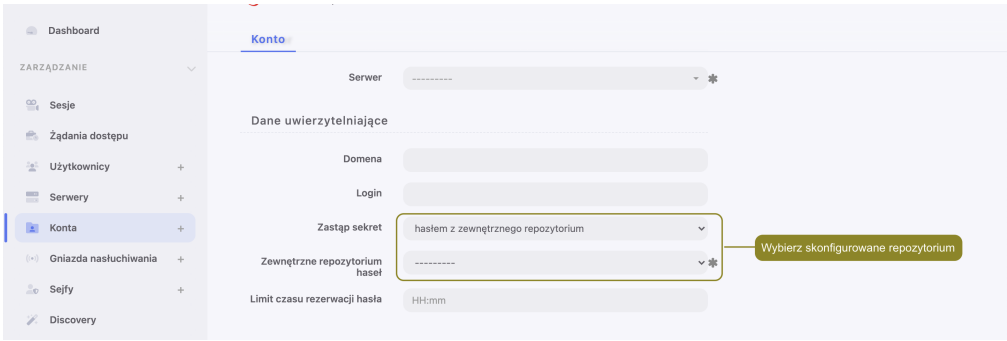
Informacja: Konto użytkownika wskazane w konfiguracji musi być typu OTP (One Time Password).

---

8. W polu *Hasło* i *Powtórz hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
8. Kliknij *Zapisz*.
9. Zdefiniuj nazwę obiektu serwera oraz przestrzeń nazw ERPM w sekcji *Zewnętrzne repozytoria haseł*.
    - Wybierz *Zarządzanie* > *Serwery*.
    - Wyszukaj i kliknij definicję obiektu.
    - W sekcji *Zewnętrzne repozytorium haseł*, wprowadź *Nazwę serwera* i *Przestrzeń nazw ERPM*.

- Kliknij *Zapisz*

10. Przypisz repozytorium haseł do konta.
    - Wybierz *Zarządzanie* > *Konta*.
    - Wyszukaj i kliknij definicję konta.
    - W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastąp sekret*, wybierz *hasłem z zewnętrznego repozytorium*.
    - Z listy rozwijalnej *Zewnętrzne repozytorium haseł*, wybierz wcześniej zdefiniowane repozytorium.



- 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*

20.8.3 Lieberman Enterprise Random Password Manager

Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.

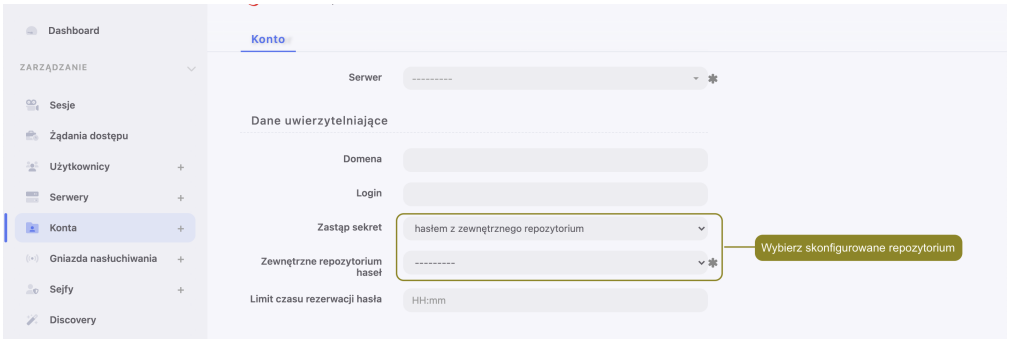
3. Uzupełnij parametry konfiguracyjne serwera.
4. Z listy rozwijalnej *Typ* wybierz `Lieberman Enterprise Random Password Manager`.
5. Wprowadź nazwę obiektu.
6. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

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

Przykład: `https://10.0.0.2/PWCWeb/`

---

7. W polu *Uwierzytelnienie* określ moduł uwierzytelnienia przypisany do użytkownika uprawnionego do przeglądania zawartości repozytorium.
8. W polu *Login* wprowadź nazwę użytkownika uprawionego do pobierania haseł.
9. W polu *Hasło* i *Powtórz hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
8. Kliknij *Zapisz*.
9. Zdefiniuj nazwę obiektu serwera oraz przestrzeń nazw ERPM w sekcji *Zewnętrzne repozytoria haseł*.
    - Wybierz *Zarządzanie* > *Serwery*.
    - Wyszukaj i kliknij definicję obiektu.
    - W sekcji *Zewnętrzne repozytorium haseł*, wprowadź *Nazwę serwera* i *Przestrzeń nazw ERPM*.
    - Kliknij *Zapisz*
10. Przypisz repozytorium haseł do konta.
    - Wybierz *Zarządzanie* > *Konta*.
    - Wyszukaj i kliknij definicję konta.
    - W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastąp sekret*, wybierz *hasłem z zewnętrznego repozytorium*.
    - Z listy rozwijalnej *Zewnętrzne repozytorium haseł*, wybierz wcześniej zdefiniowane repozytorium.



- 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*

20.8.4 Thycotic Secret Server

Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Uzupełnij parametry konfiguracyjne serwera.
4. Z listy rozwijalnej *Typ* wybierz `Thycotic Secret Server`.
5. Wprowadź nazwę obiektu.
6. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

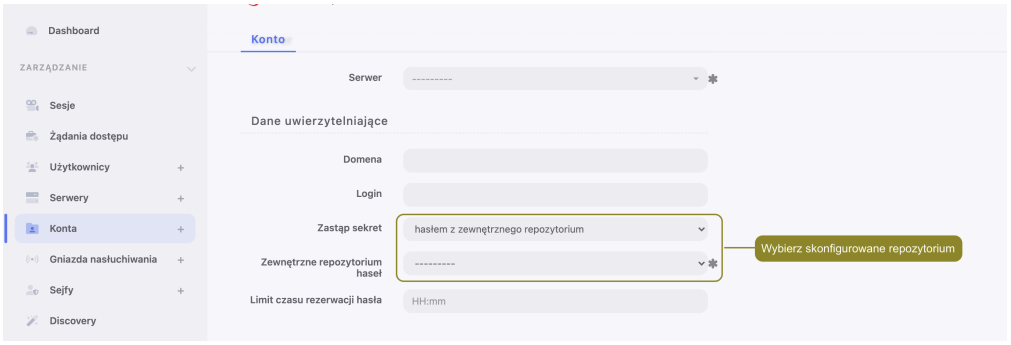
Informacja: Określ w ścieżce URL użycie protokółu HTTPS, aby komunikacja z serwerem podlegała szyfrowaniu.

---

7. W polu *Login* wprowadź nazwę użytkownika uprawionego do pobierania haseł.
8. W polu *Hasło* i *Powtórz hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
9. W polu *Format sekretu* wprowadź ciąg znaków definiujący format identyfikatorów obiektów w systemie Thycotic Secret Server.
8. Kliknij *Zapisz*.
9. Zdefiniuj nazwę obiektu serwera oraz przestrzeń nazw ERPM w sekcji *Zewnętrzne repozytoria haseł*.
    - Wybierz *Zarządzanie* > *Serwery*.

- Wyszukaj i kliknij definicję obiektu.
- W sekcji *Zewnętrzne repozytorium haseł*, wprowadź *Nazwę serwera* i *Przestrzeń nazw ERPM*.
- Kliknij *Zapisz*

10. Przypisz repozytorium haseł do konta.
    - Wybierz *Zarządzanie* > *Konta*.
    - Wyszukaj i kliknij definicję konta.
    - W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastąp sekret*, wybierz *hasłem z zewnętrznego repozytorium*.
    - Z listy rozwijalnej *Zewnętrzne repozytorium haseł*, wybierz wcześniej zdefiniowane repozytorium.



- 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*

Tematy pokrewne:

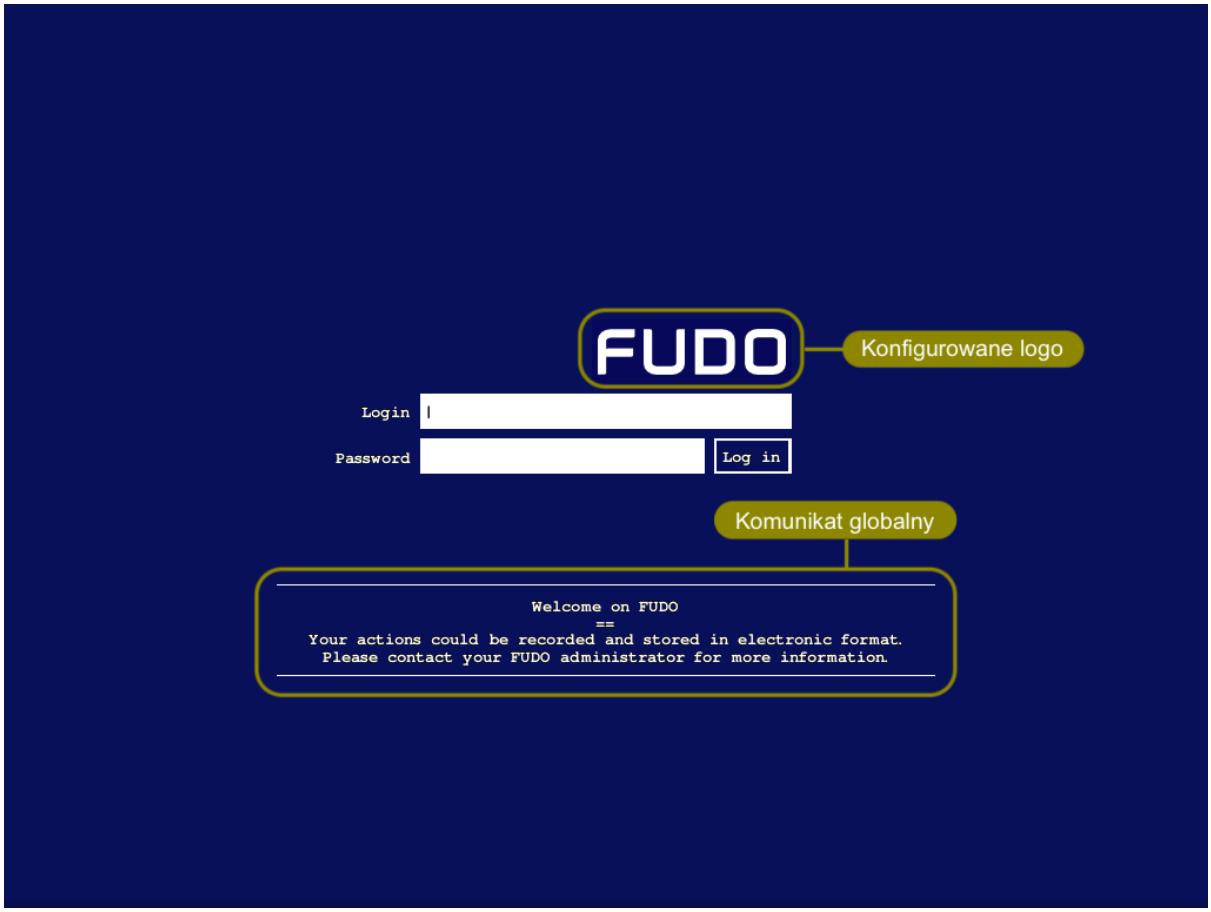
- *Zewnętrzne serwery uwierzytelniania*
- *Opis systemu*

- *Integracja z serwerem CERB*

20.9 Zasoby

20.9.1 Konfiguracja ekranu logowania RDP/VNC

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



Ustawienia dla ekranu logowania RDP

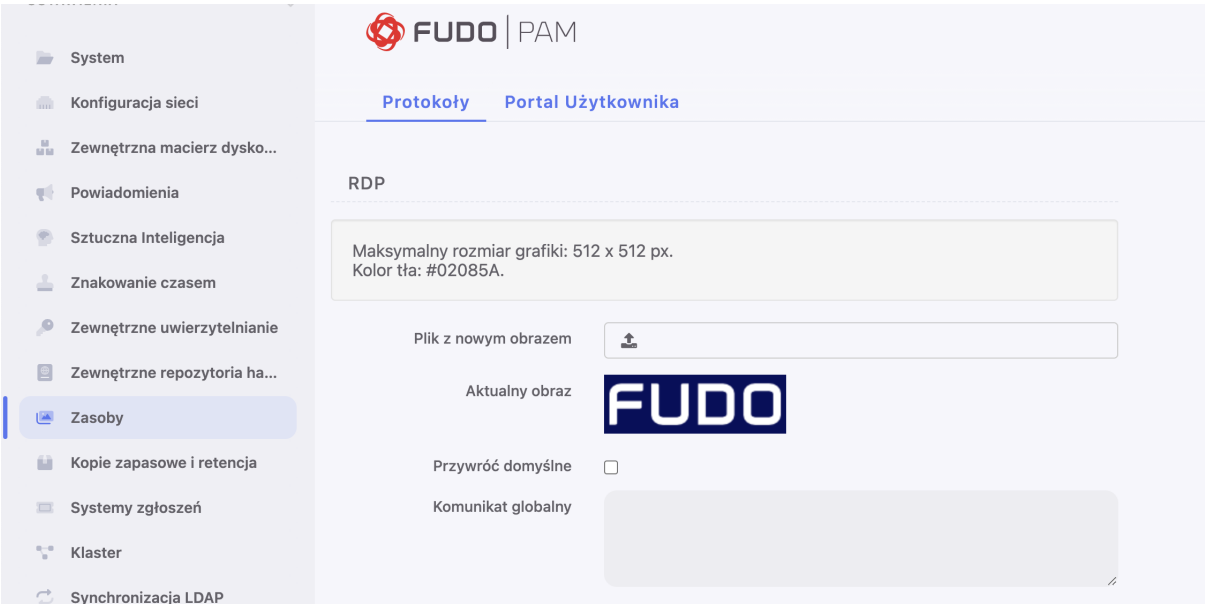
1. Wybierz z lewego menu *Ustawienia* > *Zasoby* > *Protokoły*.
2. W sekcji *RDP* kliknij *Wybierz Plik* i wskaż plik z nowym obrazem dla wybranego ekranu, aby zmienić domyślne logo.

Informacja: Maksymalny rozmiar logo to 512 x 512 px.

---

3. Wprowadź *Komunikat globalny*, aby zmienić komunikat domyślny.

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



4. Kliknij *Zapisz*.

Ustawienia dla ekranu logowania SSH

1. Wybierz z lewego menu *Ustawienia* > *Zasoby* > *Protokoły*.
2. W sekcji *SSH* wprowadź *Komunikat globalny*, aby zmienić komunikat domyślny.

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

---

3. Kliknij *Zapisz*.

Ustawienia dla ekranu logowania VNC

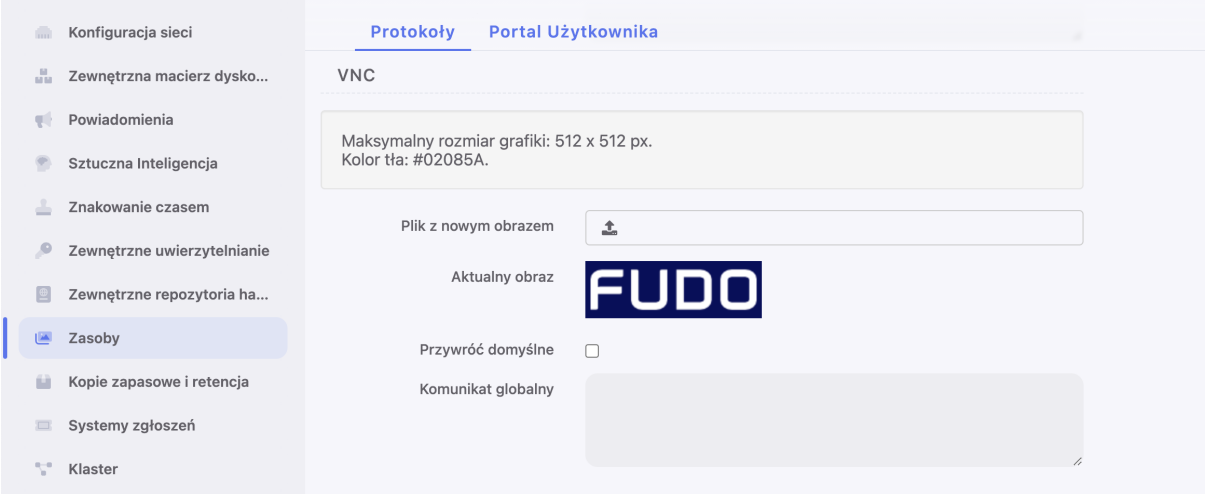
1. Wybierz z lewego menu *Ustawienia* > *Zasoby* > *Protokoły*.
2. W sekcji *VNC* kliknij *Wybierz Plik* i wskaż plik z nowym obrazem dla wybranego ekranu, aby zmienić domyślne logo.

Informacja: Maksymalny rozmiar logo to 512 x 512 px.

---

3. Wprowadź *Komunikat globalny*, aby zmienić komunikat domyślny.

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



4. Kliknij *Zapisz*.

Tematy pokrewne:

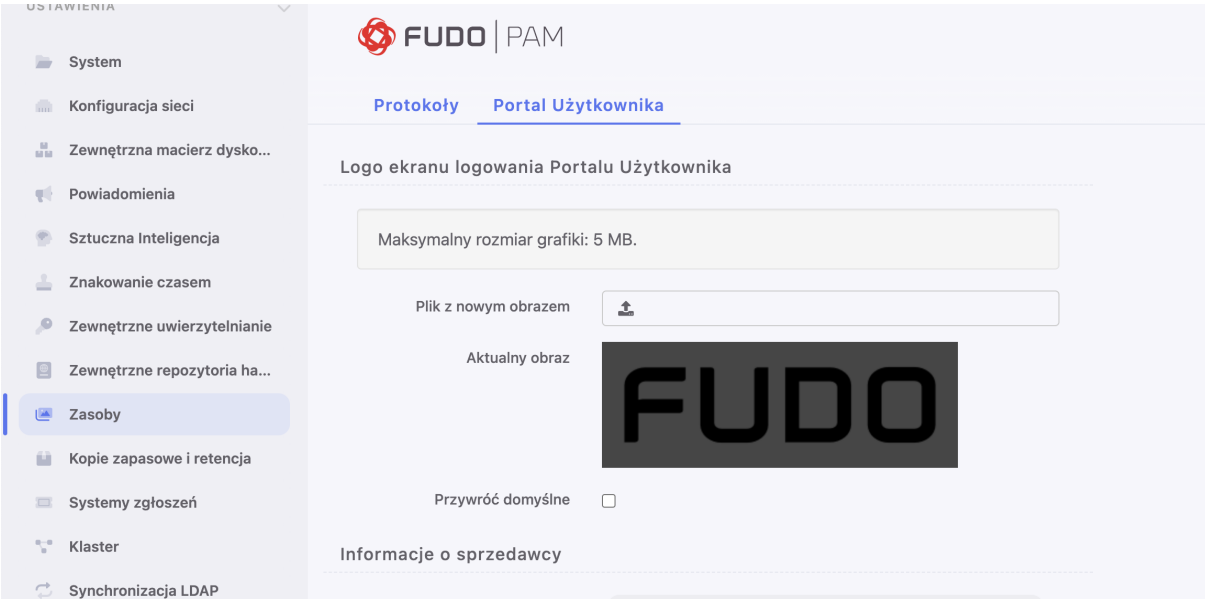
- *Szybki start - RDP*

20.9.2 Ekran logowania *Portalu użytkownika*

Fudo PAM pozwala na zdefiniowanie komunikatu do użytkowników oraz danych kontaktowych prezentowanych na ekranie logowania *Portalu użytkownika*.

1. Wybierz z lewego menu *Ustawienia* > *Zasoby*.
2. Wybierz zakładkę *Portal użytkownika*.
3. W sekcji *Logo ekranu logowania Portalu Użytkownika*, kliknij *Wybierz Plik* i wskaż plik z nowym obrazem dla ekranu logowania.

Informacja: Maksymalny rozmiar logo to 5 MB.



4. Uzupełnij pole *Informacje o sprzedawcy*.

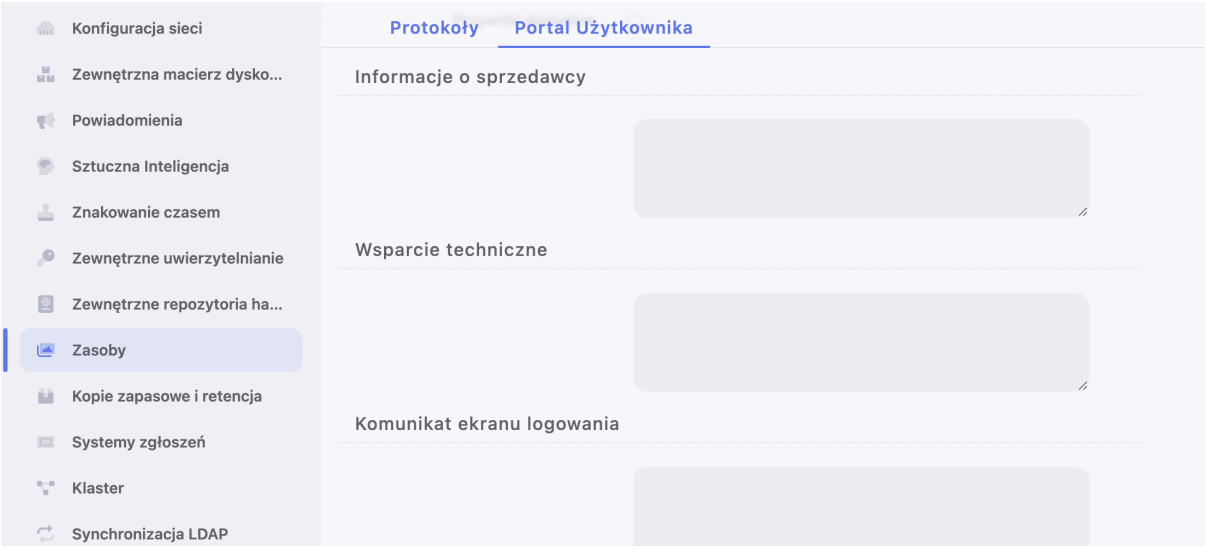
Informacja: Treść może liczyć pięć linii, do 70 znaków w wierszu.

5. Uzupełnij dane kontaktowe do działu wsparcia technicznego.

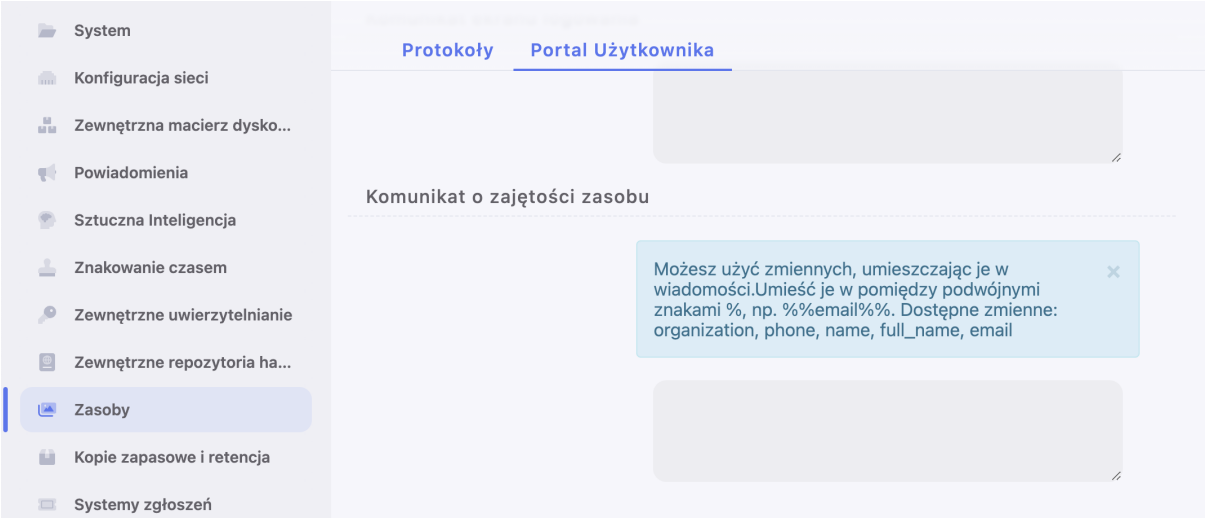
Informacja: Treść może liczyć pięć linii, do 70 znaków w wierszu.

6. Wprowadź treść komunikatu wyświetlanego na ekranie logowania.

Informacja: Treść może liczyć cztery linie, do 120 znaków w wierszu.



7. Podaj tekst wiadomości w polu *Komunikat o zajętości zasobu*, aby dostosować wiadomość, wyświetlaną użytkownikowi w sytuacji, kiedy łącząc się do serwera, inny użytkownik będzie połączony z danym serwerem. Dostosuj komunikat zawierając zmienne `organization`, `phone`, `name`, `full_name`, albo `email` pomiędzy podwójnymi znakami %%. Na przykład, `%%email%%`.



8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Portal użytkownika*

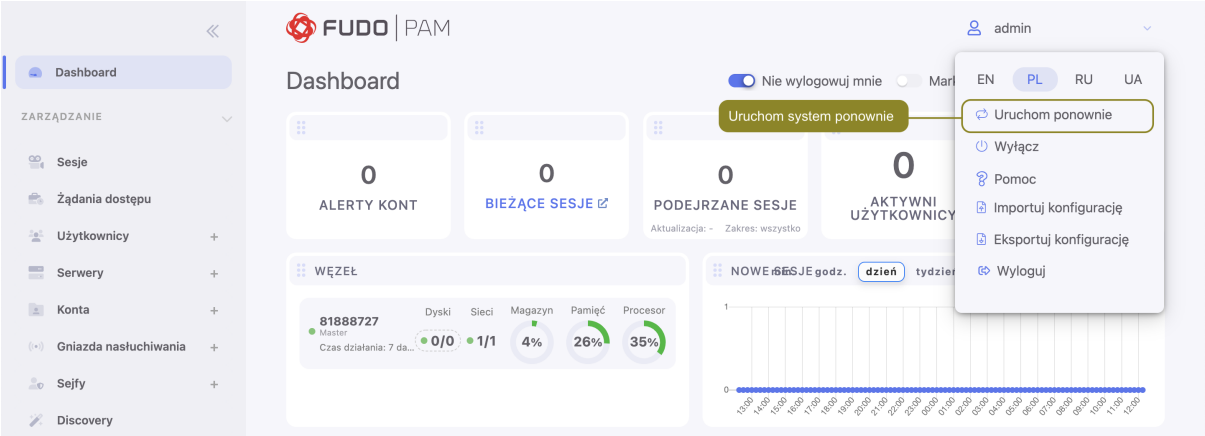
20.10 Przywracanie poprzedniej wersji systemu

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. Obejmuje to także **aktywność modyfikatorów haseł**. Jeśli jakiekolwiek hasła zostały zmienione podczas korzystania z nowszej wersji, przywrócenie poprzedniej wersji spowoduje utratę dostępu do wybranych systemów.

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:

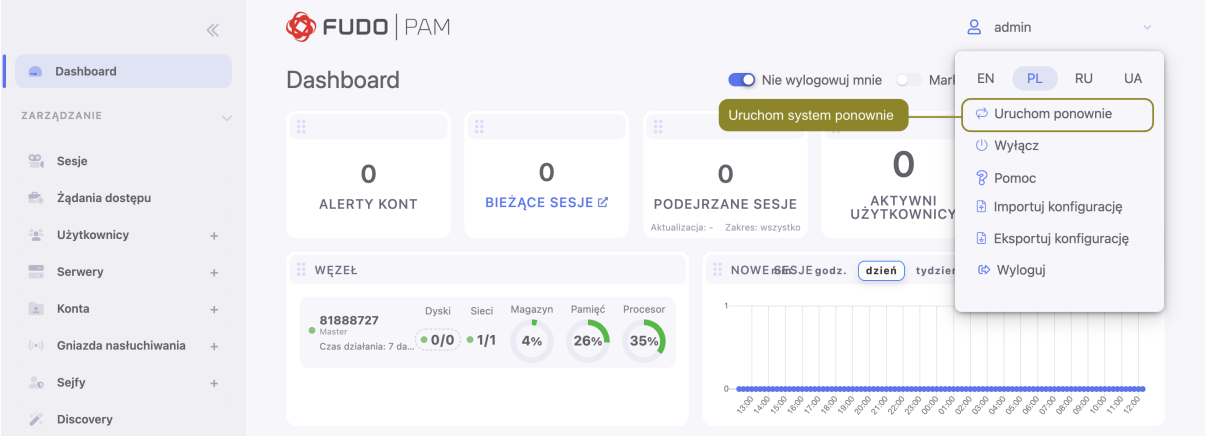
- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

20.11 Ponowne uruchomienie systemu

Ostrzeżenie: Ponowne uruchomienie systemu spowoduje rozłączenie bieżących połączeń użytkowników.

Informacja: Skorzystaj z opcji *Blokowanie nowych połączeń* sekcji *Sesja* ustawień systemowych, aby zablokować możliwość nawiązywania nowych połączeń i ograniczyć liczbę aktywnych użytkowników przed ponownym uruchomieniem 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.

Ostrzeżenie: Przywrócenie poprzedniej wersji spowoduje odtworzenie stanu systemu sprzed jego aktualizacji. **Dane sesji** oraz **zmiany w konfiguracji** dokonane na nowej wersji systemu zostaną utracone. Obejmuje to także **aktywność modyfikatorów haseł**. Jeśli jakiekolwiek hasła zostały zmienione podczas korzystania z nowszej wersji, przywrócenie poprzedniej wersji spowoduje utratę dostępu do wybranych systemów.

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

Tematy pokrewne:

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

20.12 SNMP

Fudo PAM wspiera funkcję monitorowania stanu systemu z wykorzystaniem protokołu SNMP.

Konfigurowanie SNMP

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Serwisowanie i nadzór* zaznacz opcję *SNMPv3*.
3. Z listy rozwijalnej *Adres IP* wybierz adres IP, który będzie używany do komunikacji z innymi systemami poprzez protokół SNMP.
4. Kliknij *Zapisz*.
5. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
6. Kliknij *+ Dodaj*.
7. Z listy rozwijalnej *Rola*, wybierz `service` i uzupełnij pozostałe parametry sekcji *Ogólne*.
8. W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Typ*, wybierz `hasło` i wprowadź ciąg stanowiący hasło uwierzytelniające użytkownika technicznego.

Informacja:

- Ciąg definiujący hasło musi mieć co najmniej osiem znaków.
- Konto użytkownika serwisowego uwierzytelniane jest przez usługę SNMP pierwszym skonfigurowanym hasłem statycznym.

---

9. W sekcji *SNMP*, zaznacz opcję *Włączone*.
10. Z listy rozwijalnej *Metoda uwierzytelnienia*, wybierz metodę uwierzytelnienia.
11. Z listy rozwijalnej *Szyfrowanie*, wybierz algorytm szyfrujący komunikację SNMP.
12. Kliknij *Zapisz*.

SNMP MIBs

MIB wspierane przez Fudo PAM:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - częściowe wsparcie
- UCD-SNMP-MIB

20.12.1 Odczytywanie informacji SNMP poprzez `snmpwalk`

Informacja: Odczyt danych SNMP wymaga zainstalowania pakietu *Net-SNMP 5.7.3*.

Pobieranie wszystkich informacji SNMP

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}"            -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1
```

Pobieranie wybranych informacji SNMP

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}"                -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1.3.6.1.4.1.24410
```

Dane SNMP	Opis
.1.3.6.1.4.1.24410.1.1.1	Status dysków (status ZFS)
.1.3.6.1.4.1.24410.1.1.2	Stan zasilaczy **Informacja:** Ta funkcja nie jest wspierana przez wszystkie urządzenia Fudo PAM. Skontaktuj się z działem wsparcia technicznego, aby uzyskać więcej informacji.
.1.3.6.1.4.1.24410.1.1.3	Temperatury procesora
.1.3.6.1.4.1.24410.1.1.4	Status S.M.A.R.T

20.12.2 Rozszerzenia SNMP Fudo PAM

Informacje ogólne

Rozszerzenia SNMP umożliwiają monitorowanie liczby sesji SNMP, status ZFS, status zasilaczy (jeśli jest dostępny), temperaturę rdzeni procesorów, status S.M.A.R.T dysków twardych (temperatura, realokacja sektorów, stan urządzeń).

Specyfikacja pliku MIB rozszerzeń SNMP

Poniższe pliki MIB mogą zostać wczytane do managera SNMP w celu obsługi rozszerzeń specyficznych dla Fudo PAM.

Ostrzeżenie: W wersji 4.3 zmianie uległy nazwy plików MIB. Zamień dotychczasowe pliki MIB z nową definicją.

FUDO-SECURITY-COMMON-MIB

FUDO-SECURITY-FUDO-MIB

Tematy pokrewne:

- *Bezpieczeństwo*
- *Rozwiązywanie problemów*

20.13 Kopie zapasowe i retencja

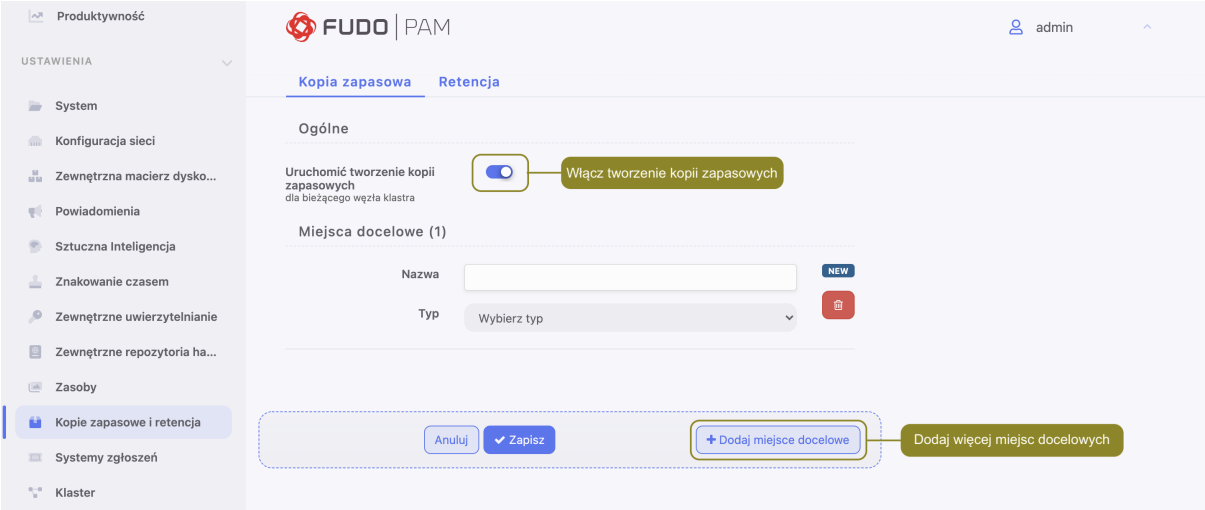
Kopia zapasowa systemu

Ostrzeżenie: Kopia zapasowa systemu zawiera poufne informacje.

Fudo pozwala skonfigurować kilka miejsc, gdzie docelowo się znajdą kopie zapasowe systemu. Mogą to być zewnętrzne repozytoria na S3, Backblaze albo FTP.

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

1. Wybierz z lewego menu *Ustawienia* > *Kopie zapasowe i retencja*.
2. Zaznacz opcję *Włączone* w podzakładce *Kopie zapasowe*.
3. Kliknij przycisk *Dodaj miejsce docelowe*, aby zacząć konfigurację miejsca docelowego.
4. Podaj nazwę dla miejsca docelowego.
5. Wybierz typ: `S3`, `Backblaze` albo `FTP`. Podaj dodatkowe dane w zależności od wybranego typu do połączenia.
6. Kliknij *Zapisz*.



Informacja: Skonfigurowane miejsce docelowe może też zostać dodane do sejfu, aby dane sesji były przechowywane automatycznie.

Retencja danych

Fudo PAM implementuje dwuetapowy mechanizm retencji danych. W pierwszym etapie, dane sesji przenoszone zostają na zewnętrzną macierz dyskową a po upływie zdefiniowanego przedziału czasowego zostają całkowicie usunięte. Więcej na temat konfigurowania zewnętrznej macierzy znajdziesz w rozdziale *Zewnętrzna macierz dyskowa*.

Informacja: Sesje, dla których istnieje *wyeksportowany materiał* nie podlegają retencji. Takie sesje muszą zostać *usunięte ręcznie* lub wyeksportowany materiał musi zostać usunięty w sekcji *Do pobrania*, aby zostały one objęte mechanizmem retencji.

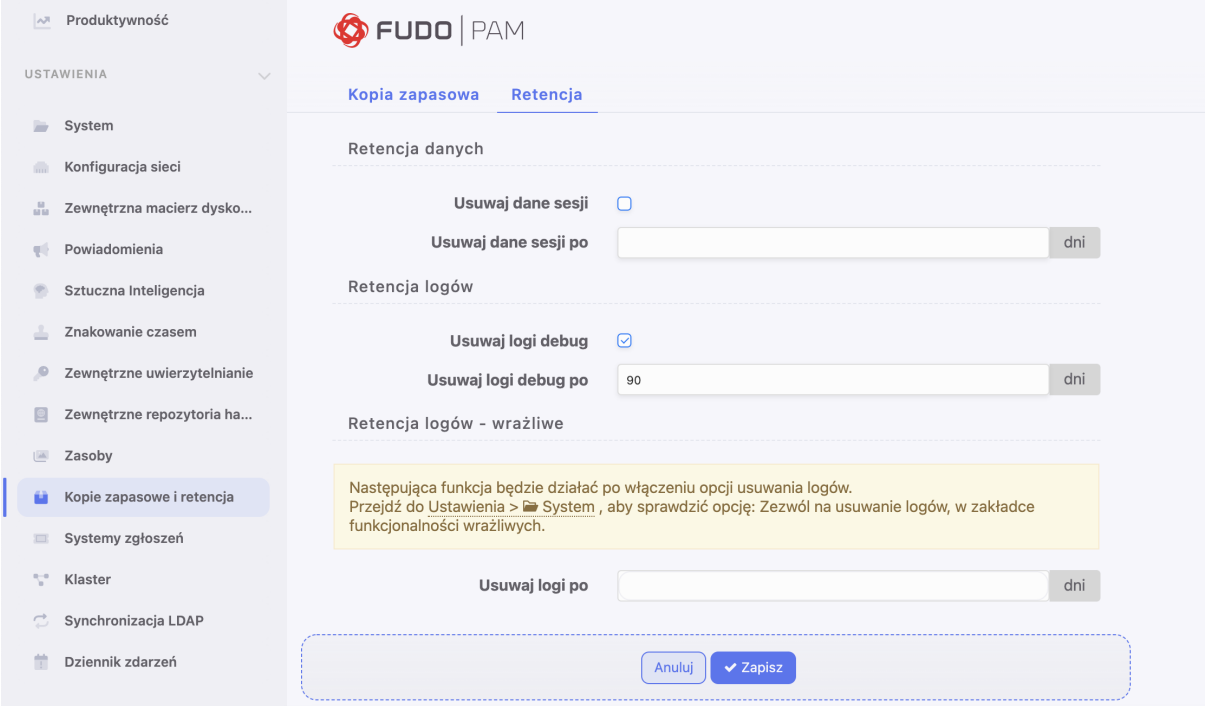
Aby włączyć retencję danych, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Kopie zapasowe i retencja* > Retencja.
2. W sekcji *Retencja danych*, zaznacz opcję *Usuwaj dane sesji* oraz w polu *Usuwaj dane sesji po* podaj liczbę dni, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.

3. W sekcji *Retencja logów*, zaznacz opcję *Usuwaj logi debug* oraz w polu *Usuwaj logi debug po* podaj liczbę dni, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.
4. W sekcji *Retencja logów - wrażliwe* opcja *Usuwaj logi po* jest aktywna wtedy, kiedy opcja *Zezwól na usuwanie logów* w sekcji *Funkcjonalności wrażliwe i bezpieczeństwo systemu* zakładki *Ustawienia* > *System* została zaznaczona oraz potwierdzona przez dwóch administratorów.

Informacja:

- Globalne wartości parametru retencji danych mają niższy priorytet niż wartość retencji zdefiniowana w *koncie*.
- Globalne ustawienia retencji danych są replikowane w ramach *konfiguracji klastrowej*.



5. Kliknij *Zapisz*.

Tematy pokrewne:

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

20.14 Zewnętrzna macierz dyskowa

Fudo PAM umożliwia retencjonowanie danych sesji na zewnętrznej macierzy dyskowej.

Informacja: Zewnętrzna macierz dyskowa w konfiguracji klastrowej

- W konfiguracji klastrowej, każdy z węzłów musi mieć skonfigurowany własny obiekt *WWN*.

- Dane przechowywane na zewnętrznej macierzy dyskowej nie są replikowane pomiędzy węzłami klastra.

20.14.1 Konfigurowanie zewnętrznej macierzy dyskowej

Aby skonfigurować zewnętrzną macierz dyskową, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzna macierz dysków*.

Informacja: Status kart fiber channel przedstawiają ikony:

- - obie karty fiber channel pracują prawidłowo.
- - połączenie z macierzą dyskową jest zdegradowane - jedna z kart fiber channel nie działa prawidłowo.
- - obie karty fiber channel nie funkcjonują prawidłowo.

2. Z listy rozwijalnej «Tryb połączenia», wybierz tryb pracy kart Fiber Channel.
   - Failover - transmisja danych odbywa się przez jedną kartę fiber channel. Gdy ta ulegnie awarii, dane przesyłane są przez drugą kartę, co pozwala zachować ciągłość dostępu do zewnętrznej macierzy.
   - Load balancing - transmisja danych odbywa się z wykorzystaniem obu interfejsów fiber channel.
3. W sekcji *Zewnętrzne urządzenia przechowywania danych* wybierz WWN i kliknij ikonę .

Informacja: Kliknij ikonę , aby odświeżyć listę dostępnych obiektów WWN.

4. Kliknij *Zapisz* i przejdź do konfigurowania *retencji danych*.

20.14.2 Rozszerzanie zewnętrznej macierzy dyskowej

Po zmianie rozmiaru obiektu WWN, należy rozszerzyć dostępną powierzchnię przechowywania w panelu administracyjnym Fudo PAM.

Ostrzeżenie: Po powiększeniu przestrzeni przechowywania na zewnętrznej macierzy dyskowej nie jest możliwe jej pomniejszenie.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzna macierz dysków*.
2. W sekcji opisującej parametry zewnętrznego obiektu WWN, kliknij *Rozszerz*.
3. Potwierdź operację powiększenia przestrzeni przechowywania.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Kopie zapasowe i retencja*

20.15 Eksportowanie/importowanie konfiguracji systemu

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

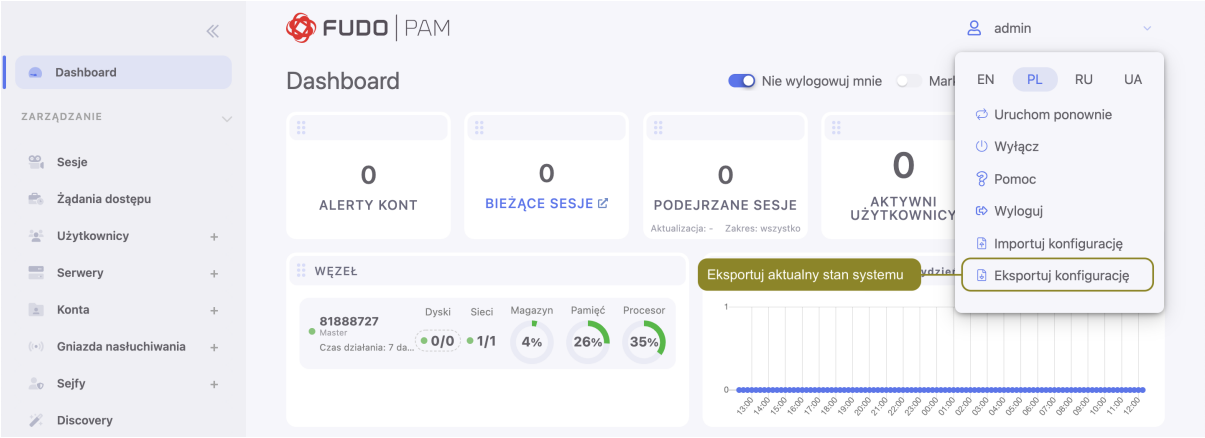
Ostrzeżenie: Wyeksportowana konfiguracja zawiera poufne informacje.

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

20.15.1 Eksportowanie konfiguracji

Aby wyeksportować konfigurację systemu, postępuj zgodnie z poniższą instrukcją.

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



20.15.2 Importowanie konfiguracji

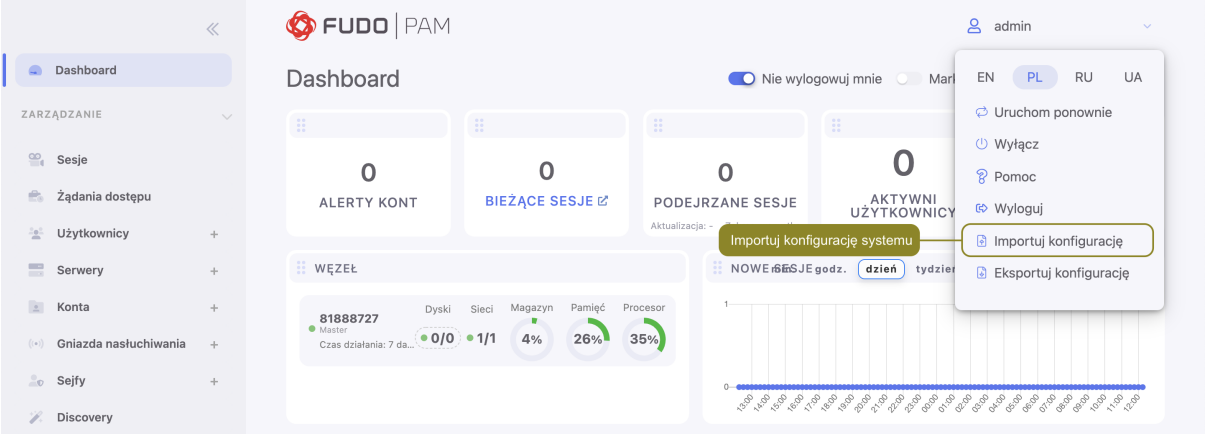
Ostrzeżenie: Zainicjowanie systemu wcześniej zapisaną konfiguracją spowoduje utratę wszystkich danych sesji.

Aby zaimportować konfigurację systemu, postępuj zgodnie z poniższą instrukcją.

1. Odszukaj i odszyfruj *główny klucz szyfrujący* komendą *openssl*:

```
openssl smime -decrypt -in path/to/masterkey.pem -inkey privkey.pem -out
masterkey.tar
```

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



3. Kliknij *Wybierz plik* i wskaż plik z *głównym kluczem szyfrującym*.
4. Kliknij *Wybierz plik* i wskaż plik konfiguracji.
5. Kliknij *Zatwierdź*.
6. Zatwierdź zainicjowanie systemu danymi z pliku.

Tematy pokrewne:

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

20.16 Konfiguracja klastrowa

Klaster 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.
- 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 replikacją danych, skontaktuj się z działem wsparcia technicznego.

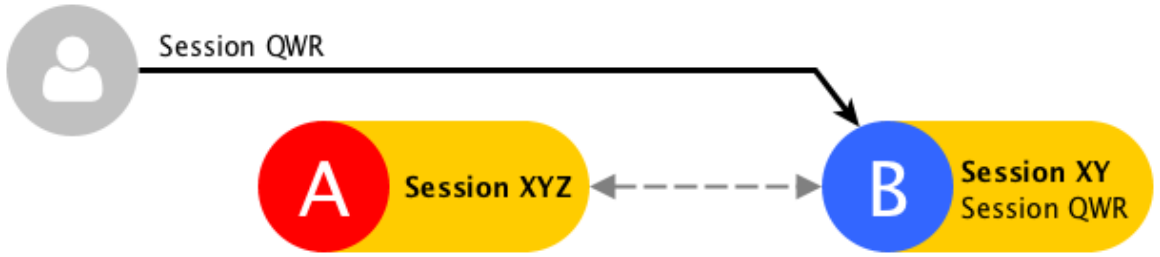
Schemat replikacji danych pomiędzy węzłami klastra jest konfigurowalny. Administrator może wybrać węzły, na które przesyłane są dane a także zdefiniować, które dane podlegają replikacji na wybraną instancję - obiekty modelu danych/sesje.

W przypadku awarii węzła, żądania dostępu do serwerów będą obsługiwane przez inny węzeł, zdeterminowany przez *priorytet grupy redundancji*.

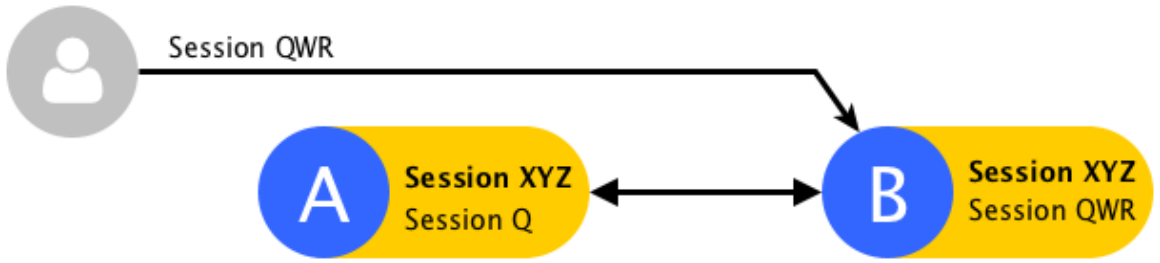
Dane bieżącej sesji są replikowane w trakcie jej trwania.

W przypadku, gdy węzeł ulegnie awarii, bieżące sesje zostaną zerwane...

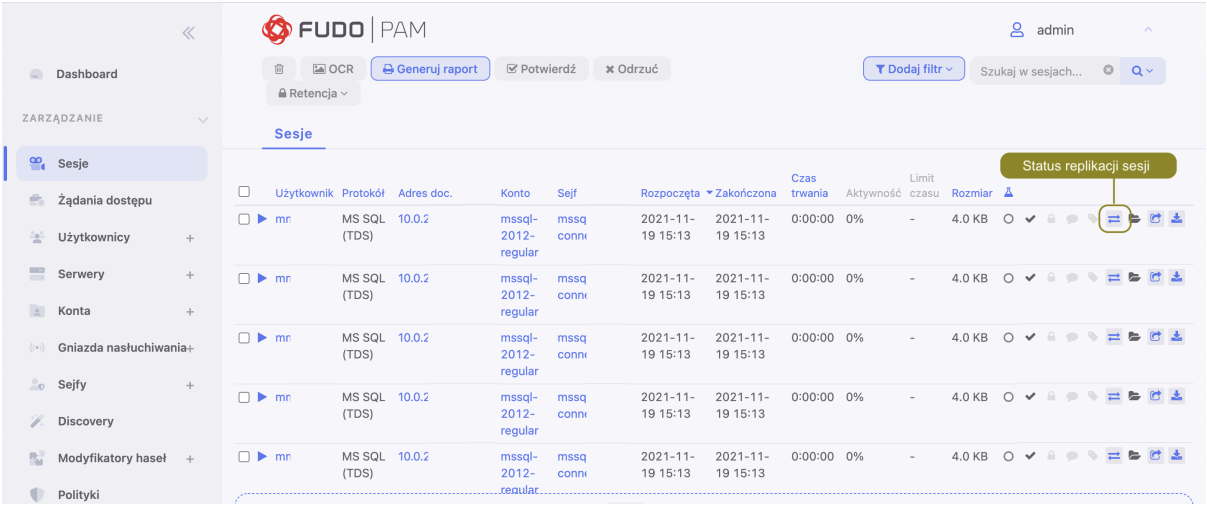
...a użytkownicy będą musieli ponownie nawiązać połączenie.



Część danych sesji, która została zreplikowana zanim miała miejsce awaria, jest dostępna na pozostałych węzłach klastra. Pełen zapis będzie dostępny po przywróceniu działania węzła i zsynchronizawaniu danych.



Stan replikacji danych sesji można zweryfikować klikając ikonę ⇄ na liście sesji.

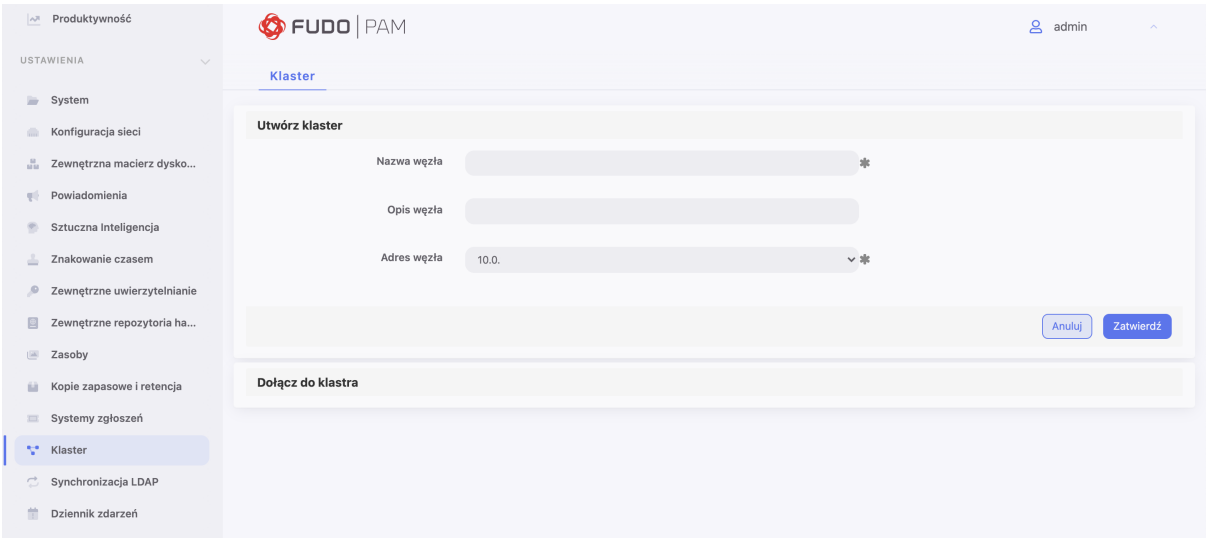


20.16.1 Inicjowanie klastra

Ostrzeżenie: Prawidłowe funkcjonowanie klastra wymaga skonfigurowania *serwera czasu NTP* na wszystkich węzłach klastra.

Aby zainicjować klaster 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.

Informacja: Adres komunikacji klastrowej musi mieć włączoną opcję zarządzania w *ustawieniach sieciowych*.

5. Kliknij *Zatwierdź*, aby zainicjować klaster.

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

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*
- *Grupy redundancji*
- *Konfiguracja klastrowa*

20.16.2 Zarządzanie węzłami klastra

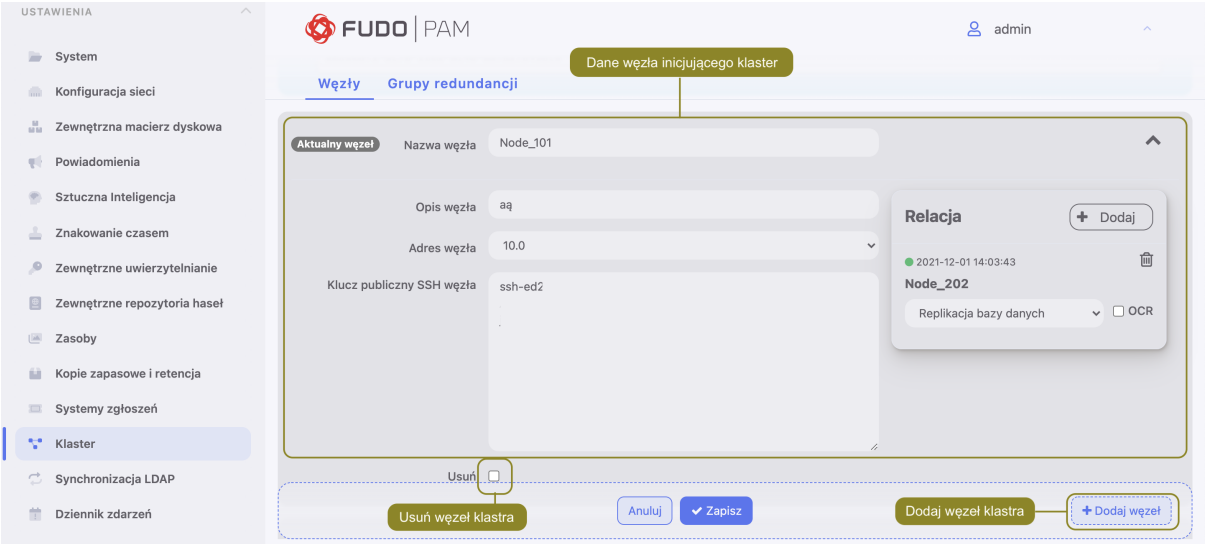
20.16.2.1 Dodawanie węzłów klastra

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 replikacją danych, skontaktuj się z działem wsparcia technicznego.
- Dane sesji oraz parametry konfiguracyjne (*serwery*, *użytkownicy*, *konta*, *sejfy*, *gniazda nasłuchiwania*, *zewnętrzne serwery uwierzytelniania*) węzła dołączanego są usuwane i inicjowane na nowo danymi zreplikowanymi z klastra.

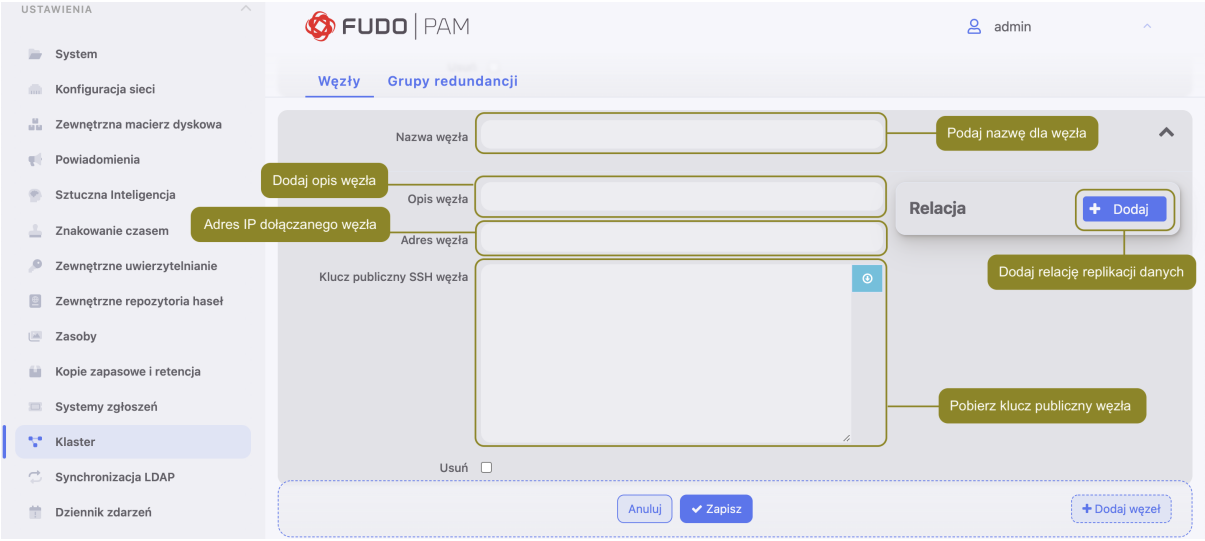
Aby dodać węzeł do klastra Fudo PAM, postępuj zgodnie z poniższą instrukcją.

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

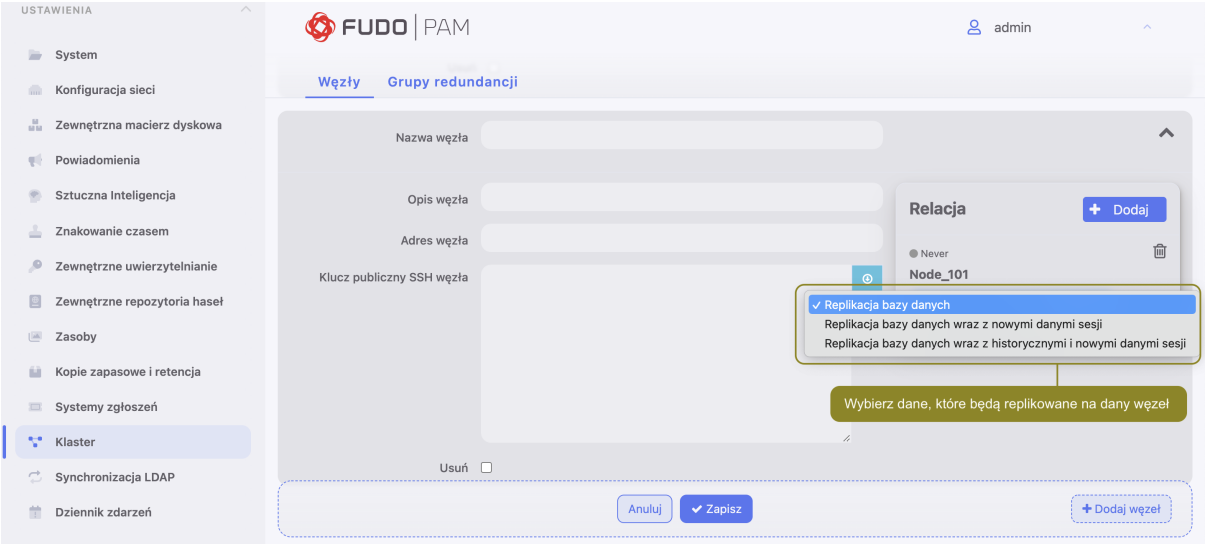


4. Wprowadź nazwę węzła oraz opis, ułatwiający identyfikację obiektu.
5. Podaj adres IP węzła dołączanego.

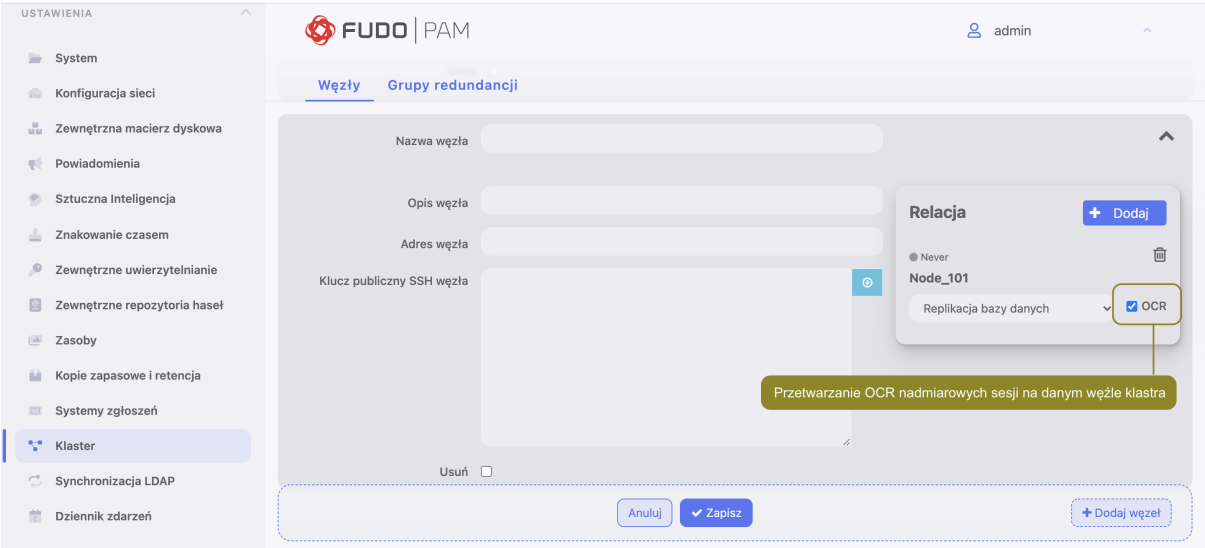
Informacja: Na wskazanym interfejsie sieciowym dołączanego węzła musi być aktywna opcja zarządzania urządzeniem. Informacje na temat konfigurowania ustawień sieciowych znajdziesz w rozdziale *Ustawienia sieci: Konfiguracja interfejsów sieciowych*.



6. Kliknij  aby pobrać klucz publiczny SSH węzła.
7. W sekcji *Relacje* dołączanego węzła, kliknij przycisk *+ Dodaj*.
8. Wybierz z listy węzeł, na który replikowane będą dane.
9. Z listy rozwijalnej, wybierz jakie dane mają podlegać replikacji na wybrany węzeł klastra.

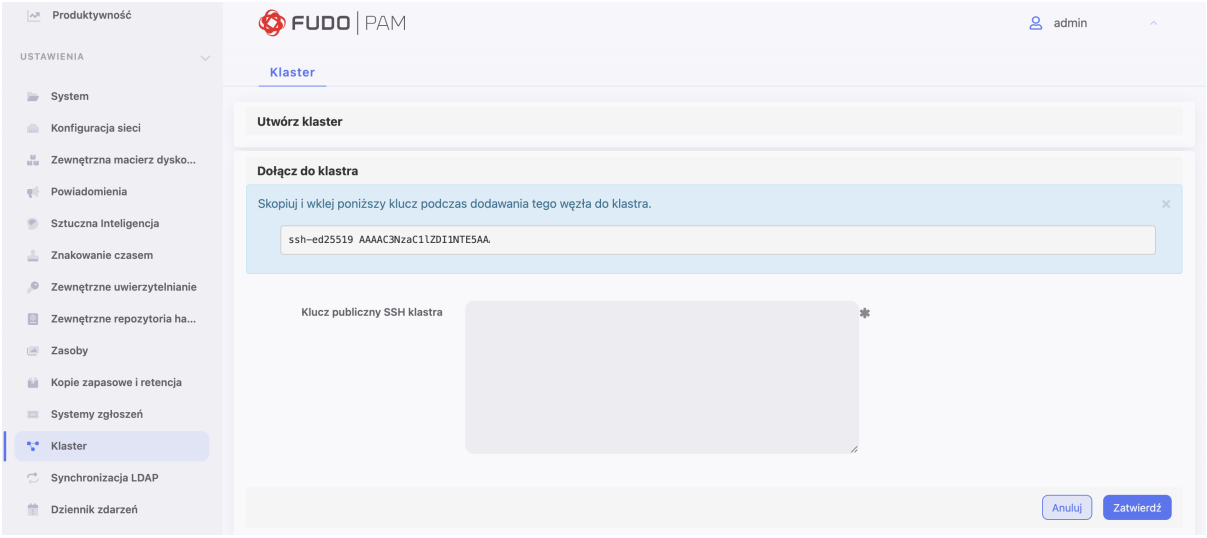


10. Zaznacz opcję *OCR*, aby wybrany węzeł przetwarzał nadwyżkę sesji graficznych.



Informacja: Każda instancja Fudo PAM ma ograniczoną, zdefiniowaną w licencji, liczbę procesów OCR przetwarzających sesje graficzne. Opcja *OCR* umożliwia oddelegowanie przetwarzania nadmiarowych sesji na wskazany węzeł, w sytuacji, w której liczba połączeń przekracza liczbę lokalnych procesów przetwarzających i indeksujących treść.

11. W sekcji *Relacje* węzła, na którym został zainicjowany klaster, kliknij przycisk *+ Dodaj*.
12. Wybierz z listy dołączany węzeł.
13. Z listy rozwijalnej, wybierz jakie dane mają podlegać replikacji na wybrany węzeł klastra.
14. Kliknij *Zapisz*.
15. Skopiuj klucz publiczny klastra.
16. Zaloguj się do panelu administracyjnego węzła dołączanego.
17. Wybierz z lewego menu *Ustawienia* > *Klaster*.
18. Wybierz opcję *Dołącz do klastra*.



19. Wklej wygenerowany wcześniej klucz i kliknij *Zatwierdź*.
20. Kliknij przycisk *Rozumiem konsekwencje, kontynuuj*.

Informacja: Aby sprawdzić status replikacji sesji, odszukaj połączenie na liście sesji i kliknij ikonę ⇄.

Tematy pokrewne:

- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

20.16.2.2 Edytowanie węzłów klastra

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

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

3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

20.16.2.3 Usuwanie węzłów klastra

Ostrzeżenie:

- Odłączenie węzła od klastra i ponowne jego przyłączenie może skutkować utratą danych.
- W przypadku trwałego odłączenia węzła od klastra, zreplikowane dane sesji zarejestrowane na odłączonym węźle nie będą mogły zostać usunięte.

Aby usunąć węzeł klastra 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:

- *Dodawanie węzłów klastra*
- *Edytowanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

20.16.3 Grupy redundancji

Grupy redundancji umożliwiają realizację scenariuszy niezawodnościowych. W przypadku awarii węzła pełniącego dla danej grupy redundancji rolę nadrzędną, przypisane do grupy adresy IP zostaną przejęte przez inny węzeł o najwyższym dla danej grupy priorytecie. 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.

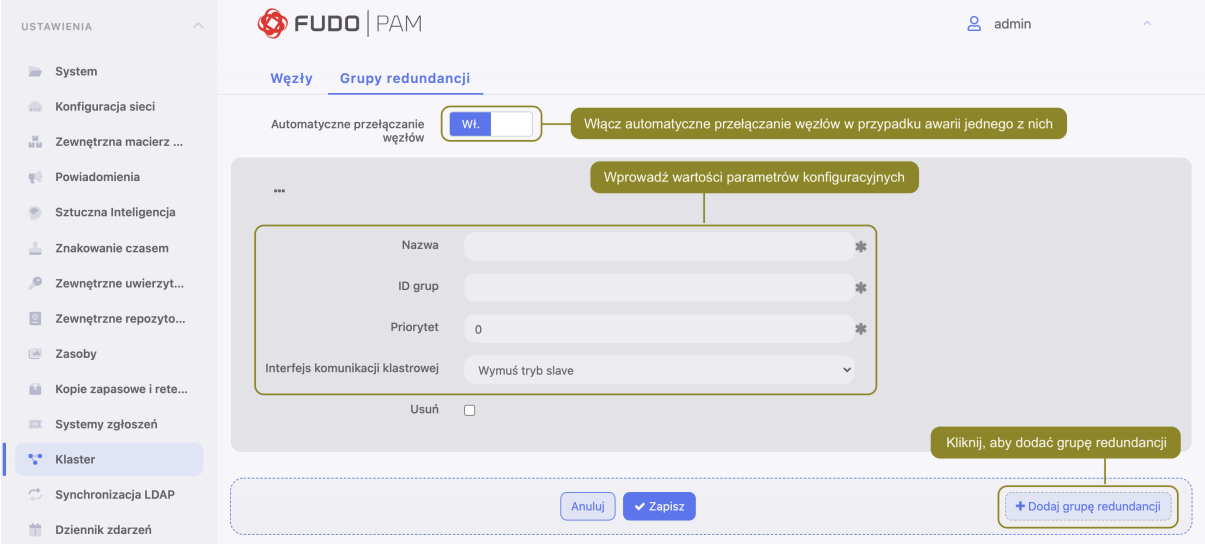
Dodawanie grup redundancji

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.

Informacja: Domyślnie, przypisanie roli *master* do węzła działa na zasadzie czasu nieokreślonego.



5. Kliknij *Zapisz*.
6. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
7. Kliknij [+], aby dodać adres IP.
8. Wprowadź adres IP i kliknij [⚙], aby nadać mu atrybut klastrowy.
9. Z listy rozwijalnej wybierz wcześniej zdefiniowaną grupę redundancji.
10. Kliknij *Zapisz*.

Informacja: Klastrowy adres IP należy zdefiniować na każdym z węzłów klastra.

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.

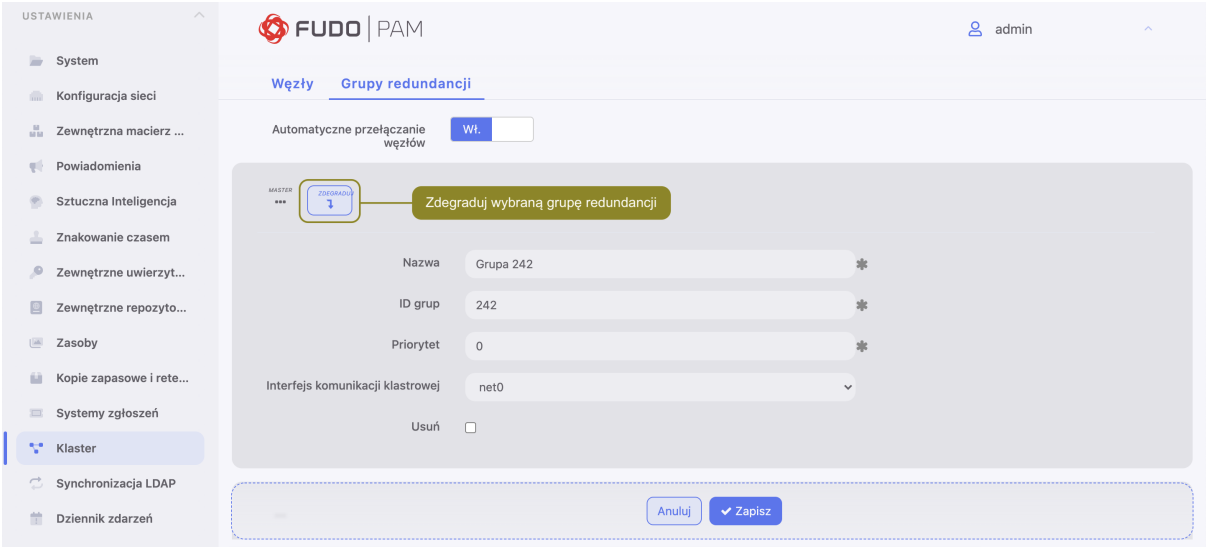
1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Zaznacz opcję *Usuń* przy wybranej grupie redundancji.
4. Kliknij *Zapisz*.

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. Innym przypadkiem użycia jest węzeł klastra, wdrożony w odrębnej lokalizacji, bez możliwości komunikacji z pozostałymi węzłami klastra w warstwie drugiej.

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*.

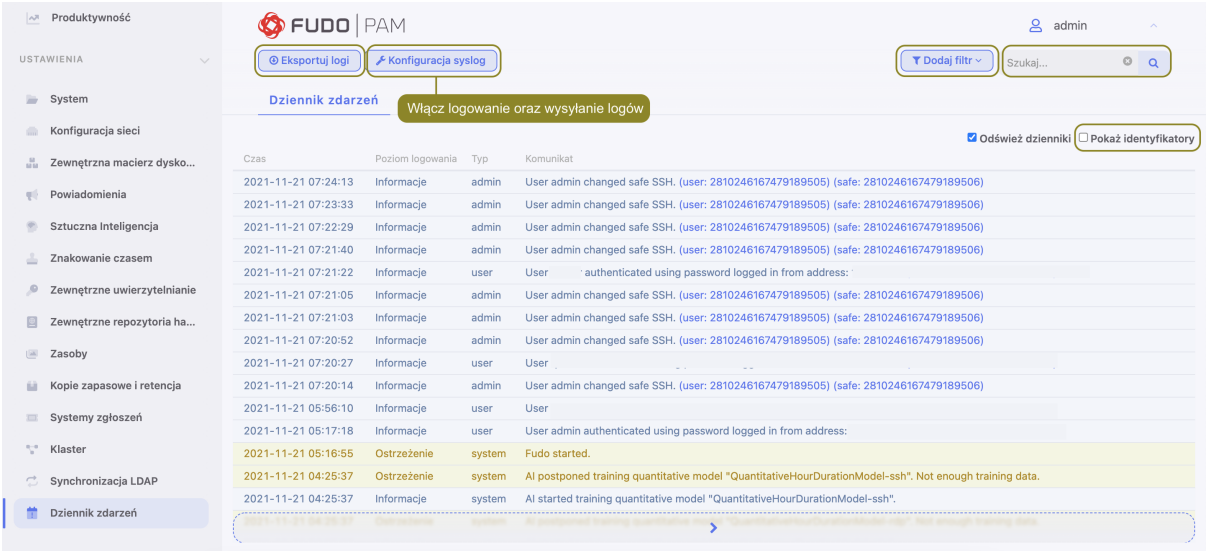
Tematy pokrewne:

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

20.17 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*.



20.17.1 Zewnętrzne serwery syslog

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

Informacja:

- W komunikacji z serwerami syslog, Fudo PAM korzysta z protokołu UDP.
- Do komunikacji z serwerem syslog, wykorzystywany jest interfejs sieciowy z włączoną opcją zarządzania  , z adresem IP pochodzącym z podsieci, w której znajduje się host docelowy lub poprzez bramę domyślną.

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* w celu uruchomienia usługi wysłania komunikatów do serwera zewnętrznego.
4. Zaznacz opcję *Włącz wysyłanie logów debugowych* w celu uruchomienia usługi wysłania komunikatów z treścią logów debugowych do serwera zewnętrznego.
5. Kliknij *+*.
6. Wprowadź adres IP oraz numer portu serwera syslog.
7. 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 komunikatów systemowych znajduje się w rozdziale *Logowane komunikaty*.

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*.

20.17.2 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.

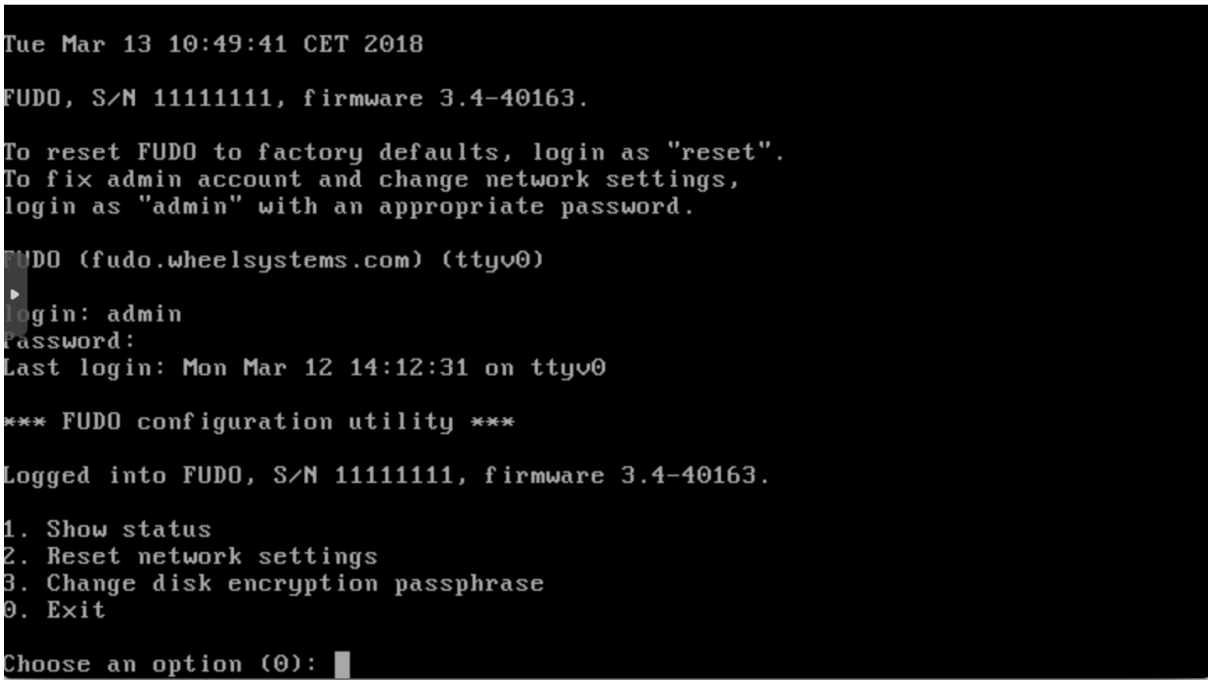
Tematy pokrewne:

- *Logowane komunikaty*
- *Bezpieczeństwo*
- *Zarządzanie serwerami*

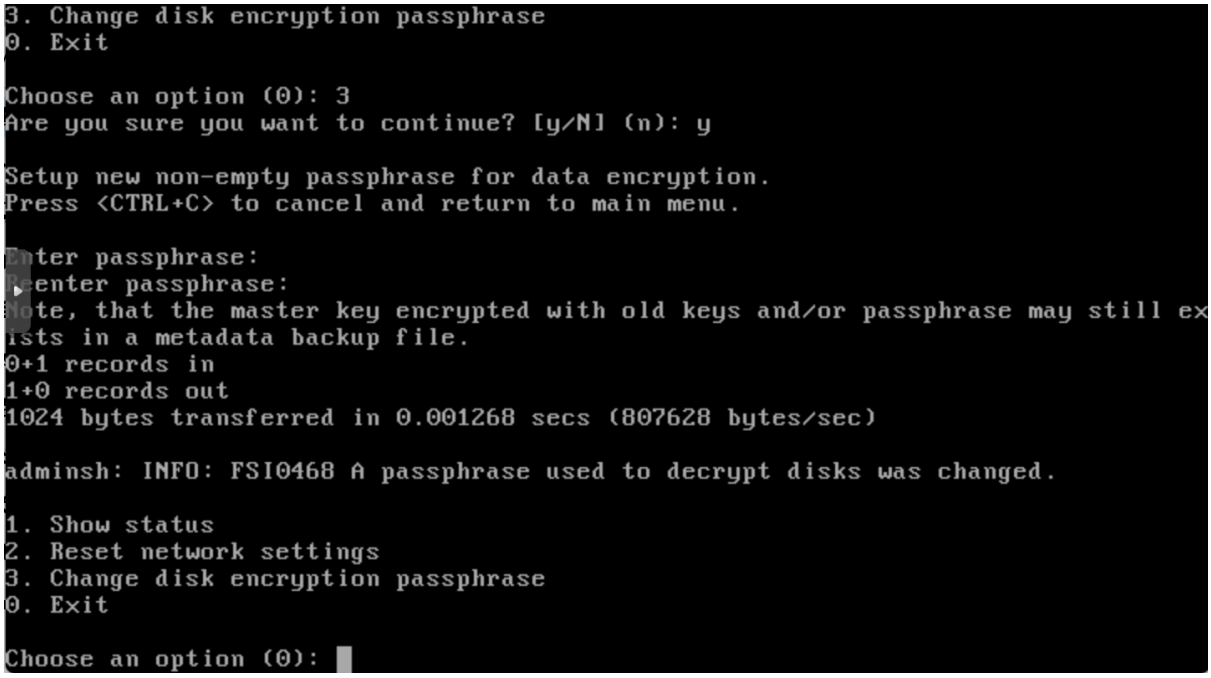
20.18 Zmiana frazy szyfrującej

W środowisku wirtualnym, dane szyfrowane są frazą szyfrującą. Aby zmienić frazę, postępuj zgodnie z poniższą instrukcją.

1. Zaloguj się do konsoli systemowej na konto z uprawnieniami *superadmin*.
2. Wpisz 3 i naciśnij klawisz *Enter*.



3. Wpisz y i naciśnij klawisz *Enter*, aby potwierdzić zmianę frazy szyfrującej.
4. Wprowadź nową frazę i zatwierdź klawiszem *Enter*.
5. Ponownie wprowadź frazę szyfrującą i zatwierdź klawiszem *Enter*.



6. Uruchom ponownie system, aby zastosować zmiany.

Tematy pokrewne:

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

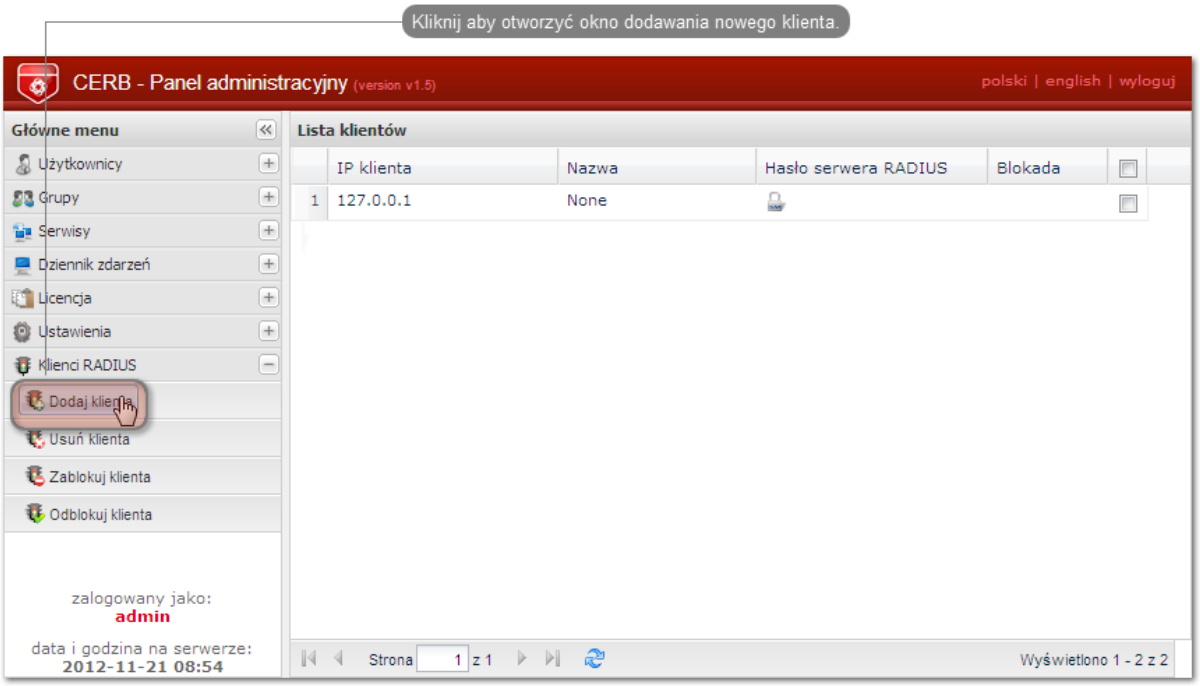
20.19 Integracja z serwerem CERB

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 Fudo PAM, uwierzytelniany byli przez zewnętrzny serwer CERB.

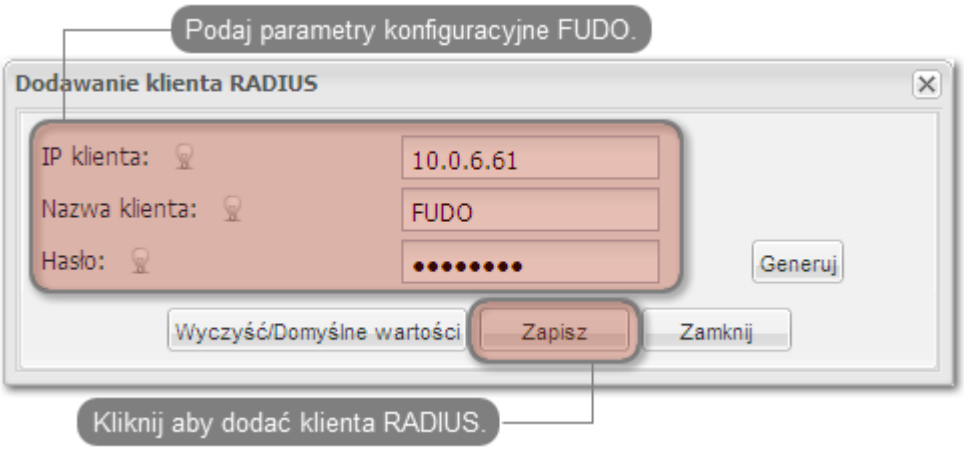
Konfiguracja serwera CERB

1. Dodanie klienta RADIUS.

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



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

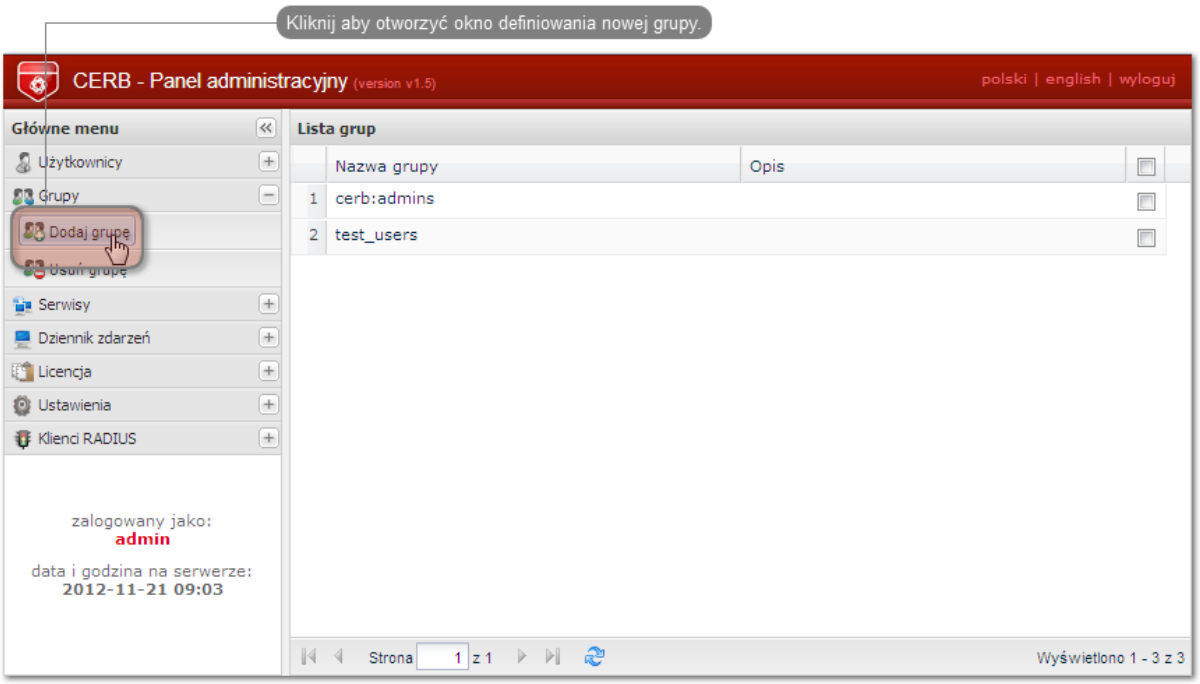


Informacja: Hasło będzie wymagane do skonfigurowania zewnętrznego serwera uwierzytelnia-

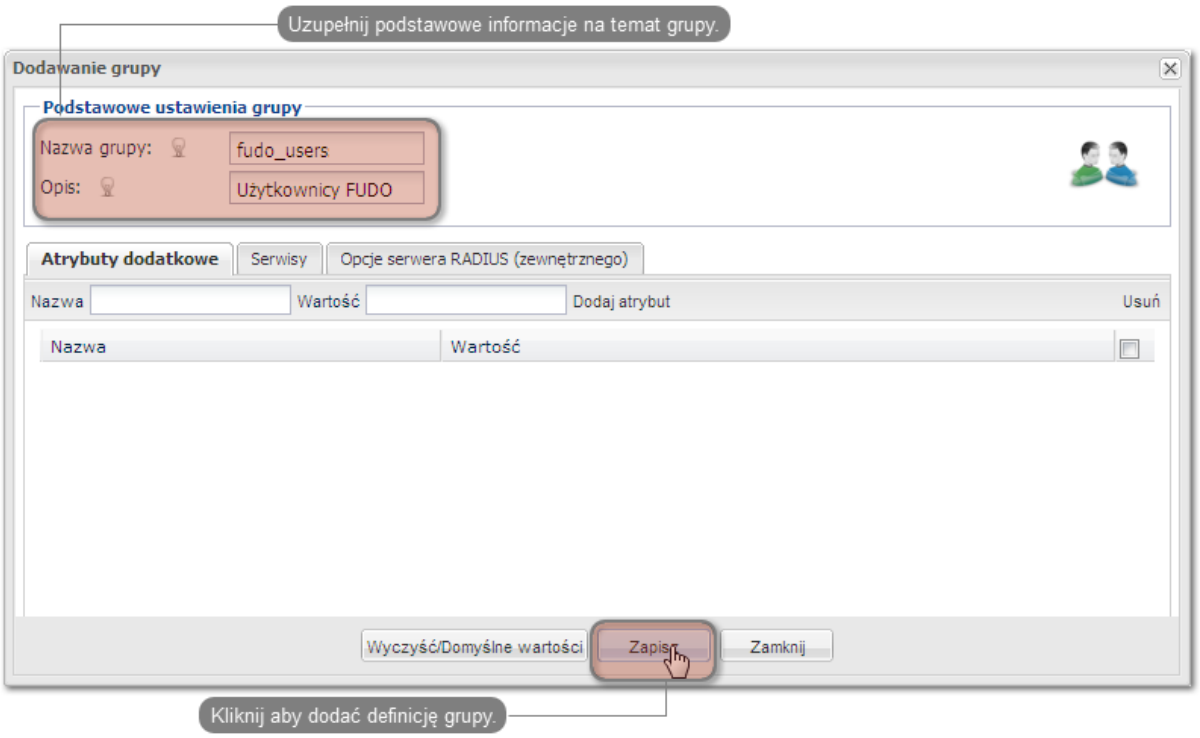
nia w panelu administracyjnym Fudo PAM.

2. Dodanie grupy użytkowników.

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

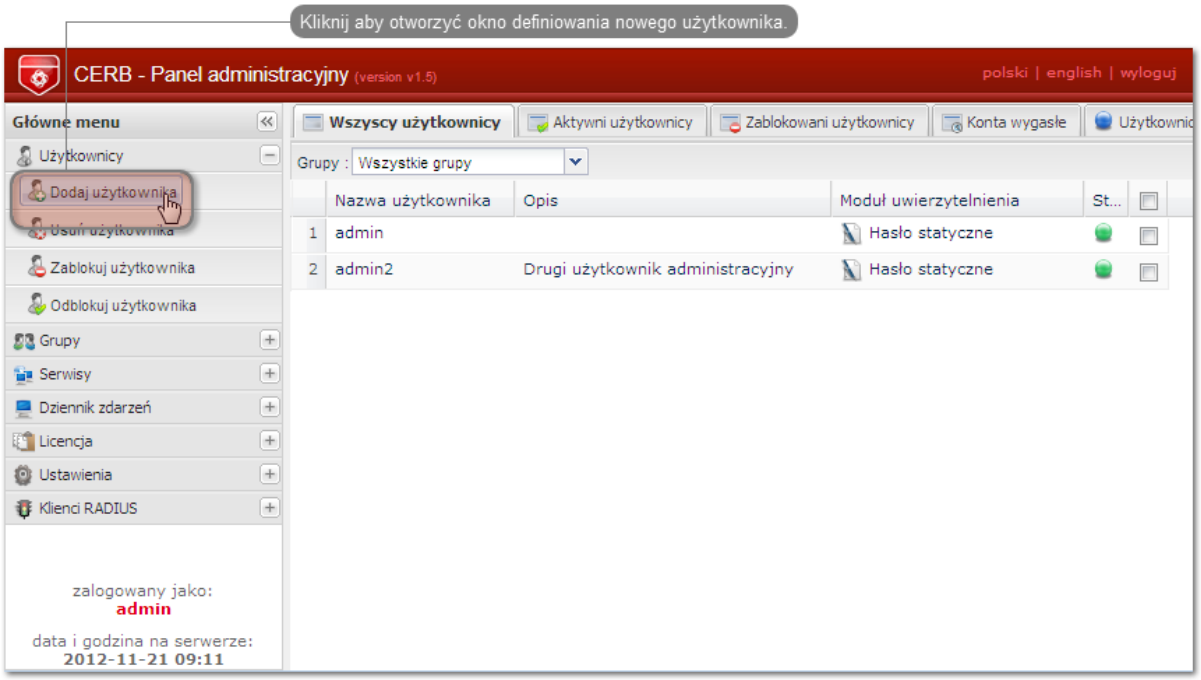


- Podaj nazwę grupy (`fudo_users`) i kliknij *Zapisz*.

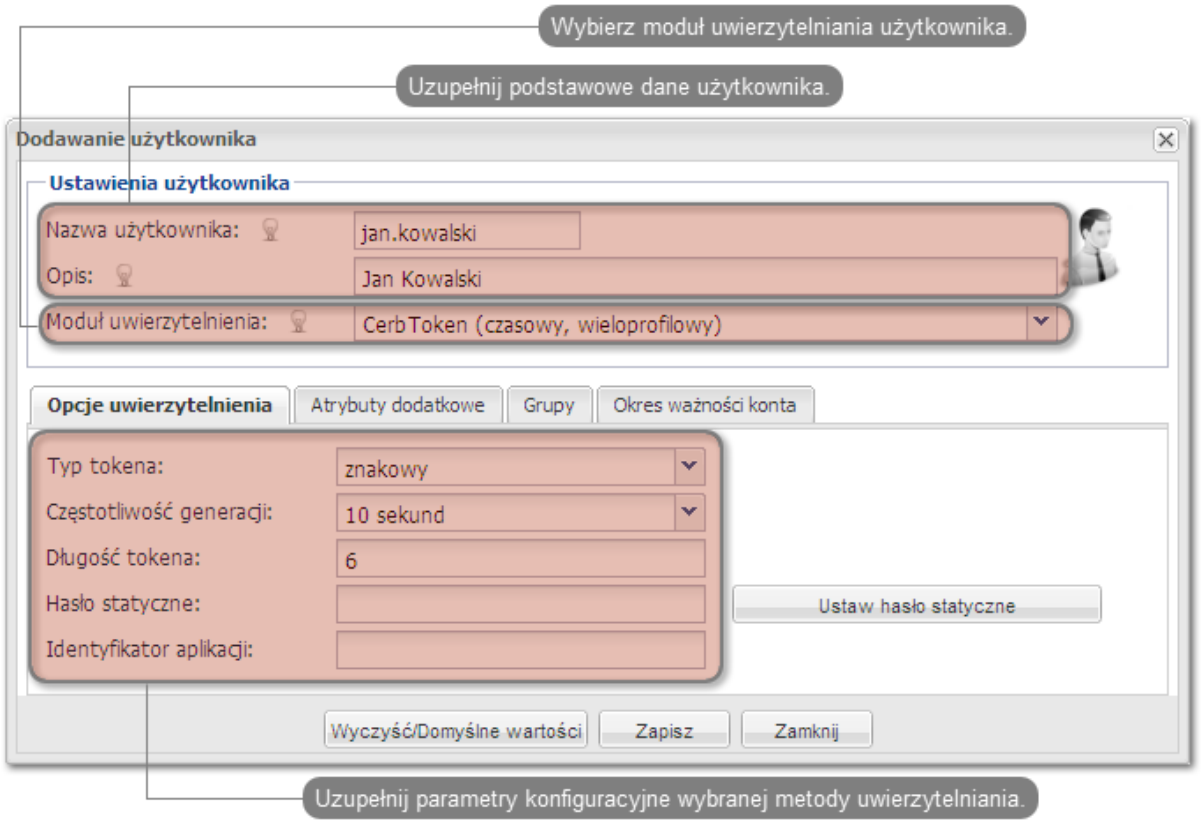


3. Dodanie użytkownika.

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



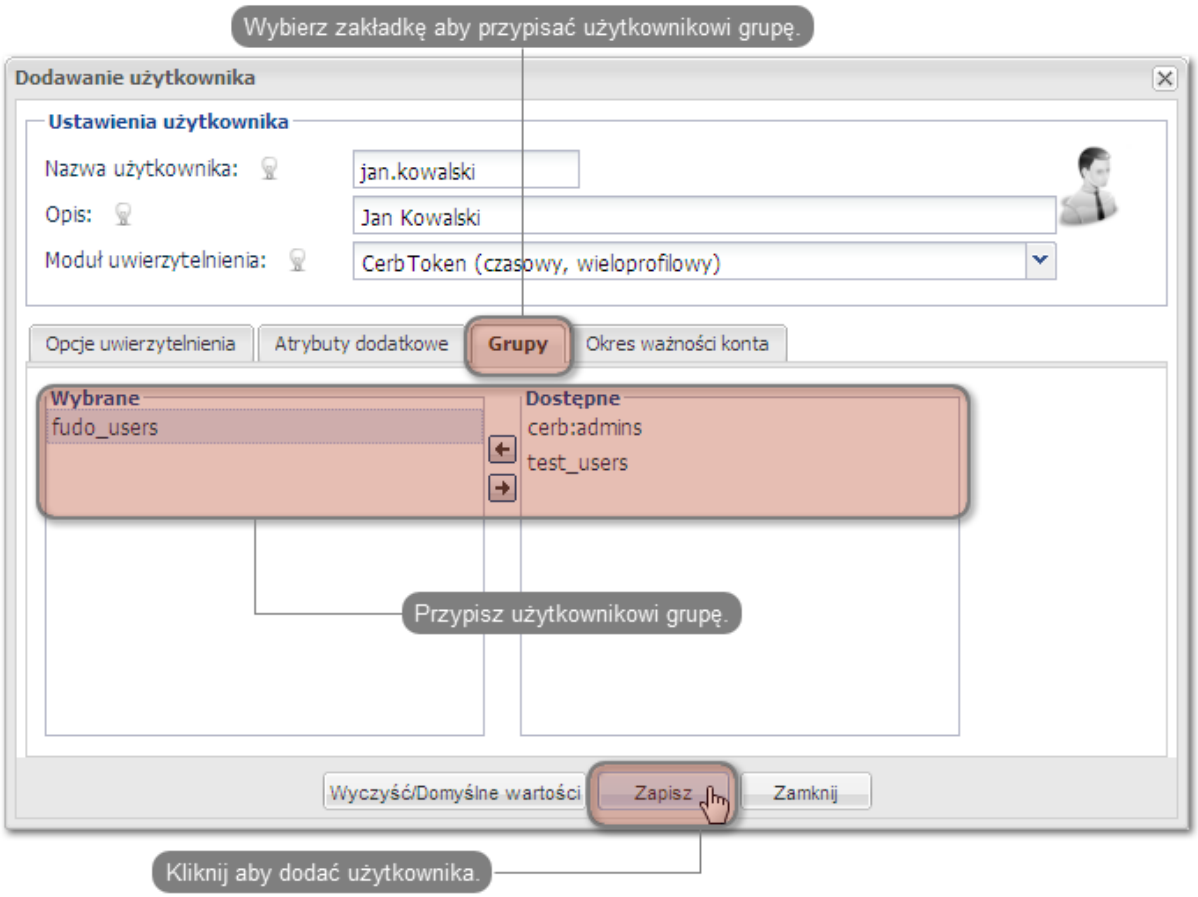
- Podaj nazwę użytkownika, opis oraz wybierz stosowny moduł uwierzytelniania (więcej informacji na temat modułów uwierzytelniania znajdziesz w dokumentacji serwera CERB).



Informacja: Nazwa użytkownika wykorzystywana jest w procesie uwierzytelniania użytkowni-

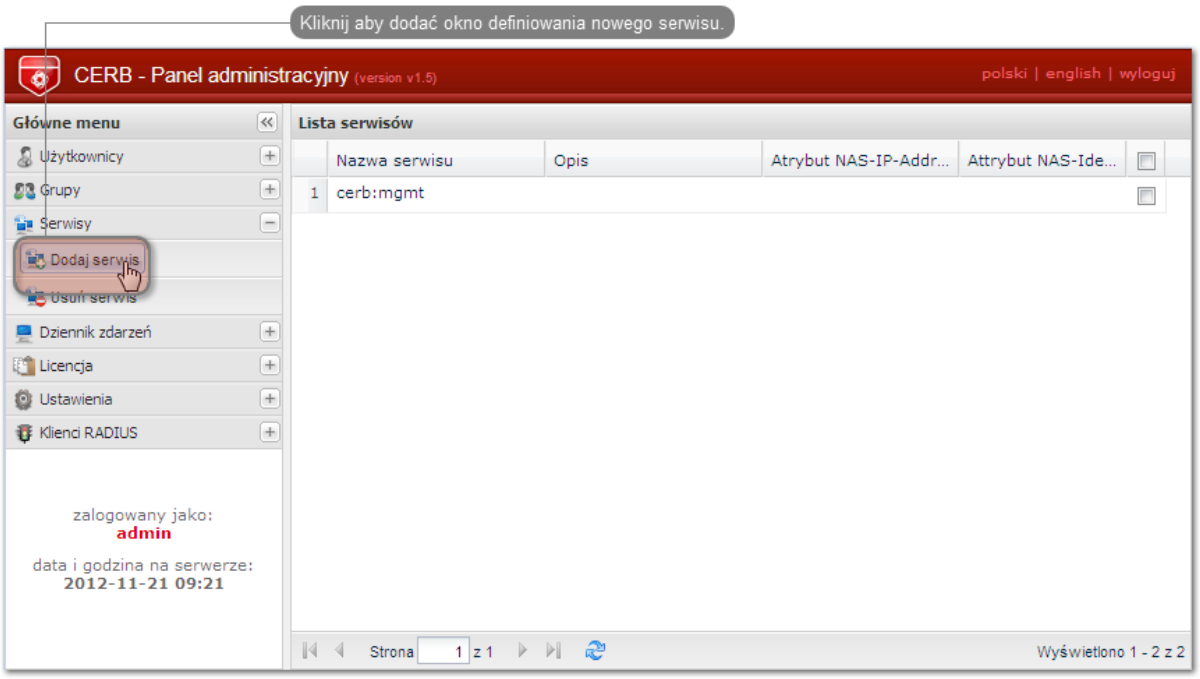
ków łączących się z Fudo PAM.

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

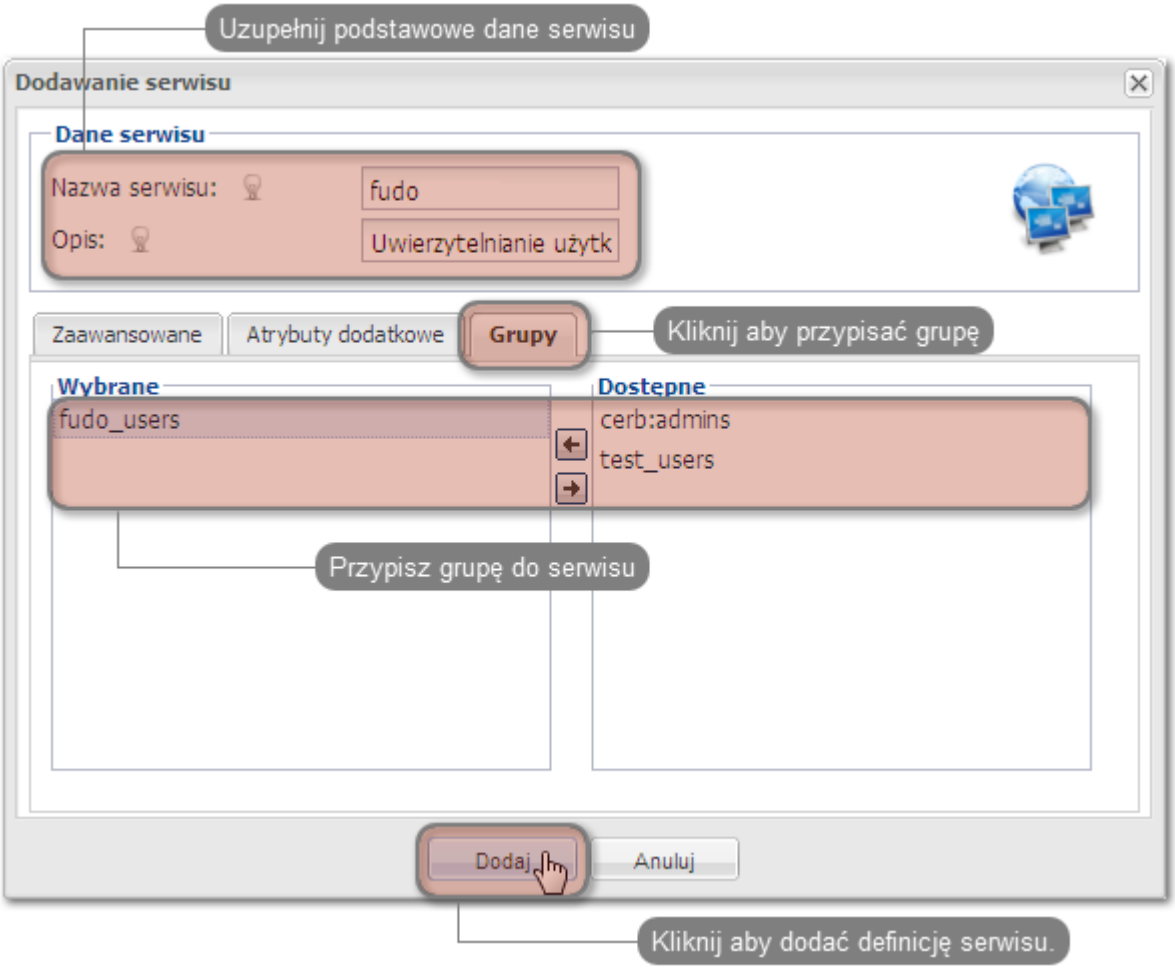


4. Skonfigurowanie serwisu.

- 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*.

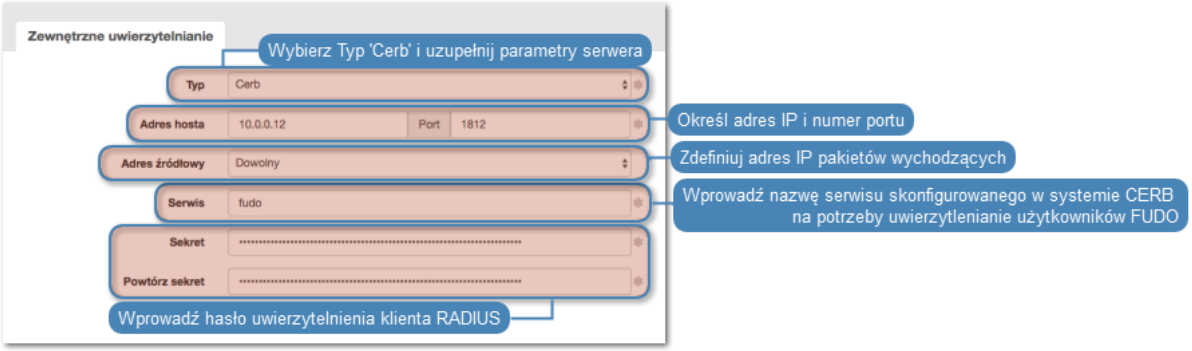


Konfiguracja serwera Fudo PAM

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.

- Przypisz użytkownikowi sejf, za pośrednictwem którego będzie mógł się łączyć do wybranych zasobów.
- W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Typ*, wybierz `Zewnętrzne uwierzytelnienie` i wskaż wcześniej dodany serwer.

- Kliknij *Zapisz*.

Tematy pokrewne:

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

20.20 Czynności serwisowe

Poniższy rozdział zawiera opisy czynności serwisowych.

Fudo PAM umożliwia zmianę pojemności pamięci systemowej poprzez dziedziczenie aktualnych ustawień pojemności maszyny wirtualnej. W celu zastosowania zmian ustawień maszyny wirtualnej po stronie Fudo, *uruchom ponownie* swoją instancję systemową.

20.20.1 Sporządzanie kopii zapasowej kluczy szyfrujących

Klucze szyfrujące wymagane są do zainicjowania systemu plików, na którym przechowywane są dane sesji. Uszkodzenie nośnika z kluczami szyfrującymi uniemożliwia poprawne uruchomienie Fudo PAM.

Microsoft Windows

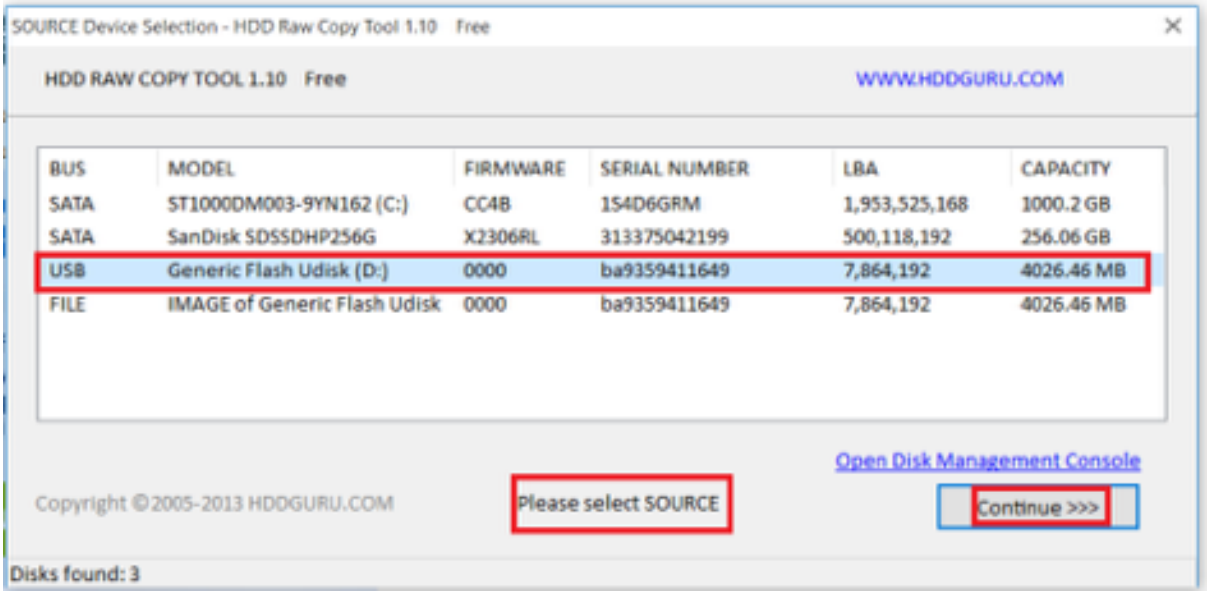
Ostrzeżenie: Po podłączeniu nośnika USB do komputera, pod żadnym pozorem nie należy wykonywać jego inicjowania/formatowania. Komunikat systemowy o braku możliwości odczytu danych należy zignorować i przystąpić do procedury tworzenia kopii zapasowej.

1. Pobierz i zainstaluj program *HDD Raw Copy Tool*.

   `http://hddguru.com/software/HDD-Raw-Copy-Tool/` (dostępna również wersja przenośna)

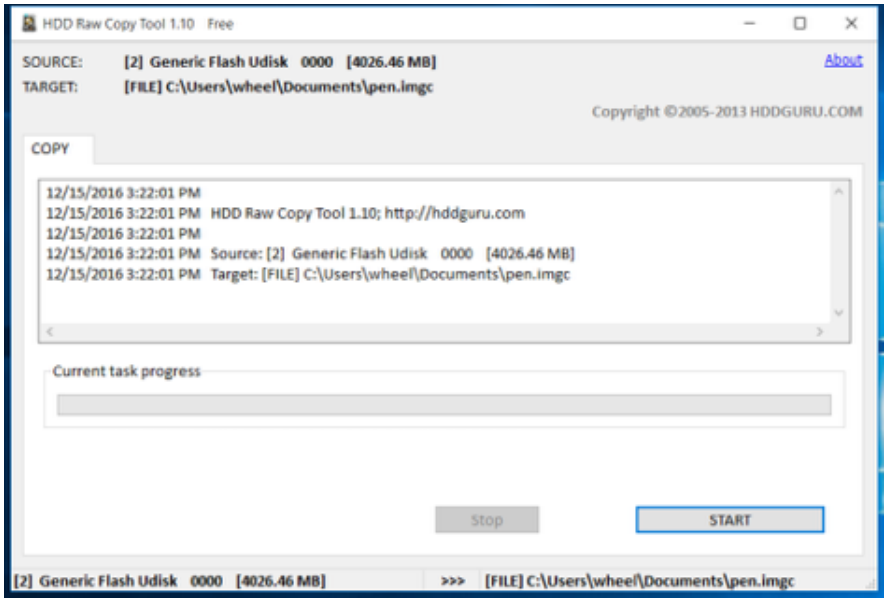
2. Uruchom program.

3. Na ekranie wyboru napędu źródłowego, zaznacz napęd USB z zapisanymi kluczami szyfrującymi i kliknij *Continue*.



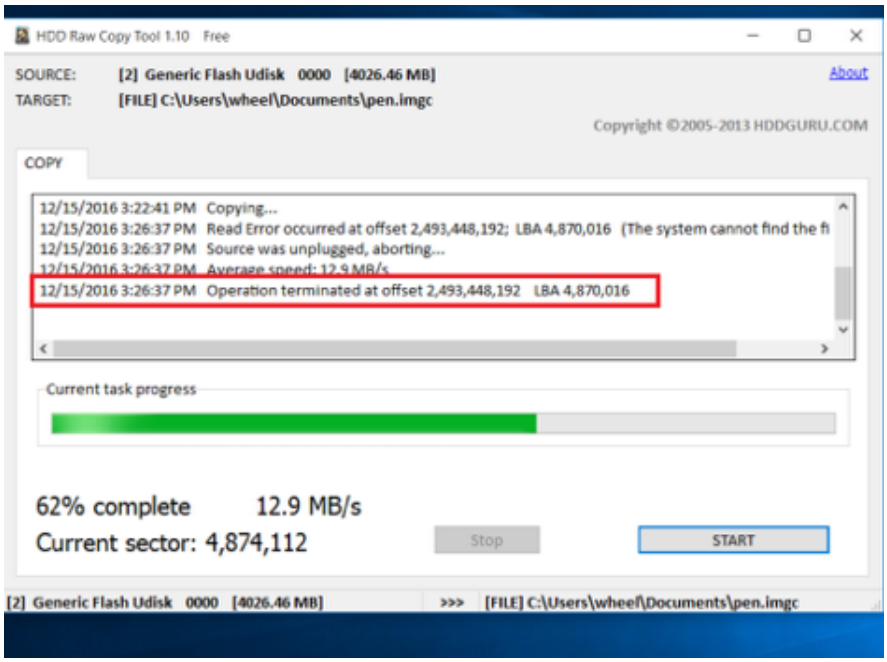
4. Kliknij dwukrotnie *FILE*, wskaż plik docelowy, w którym zapisany zostanie obraz dysku i kliknij *Continue*.

5. Kliknij *START*, aby rozpocząć procedurę kopiowania.

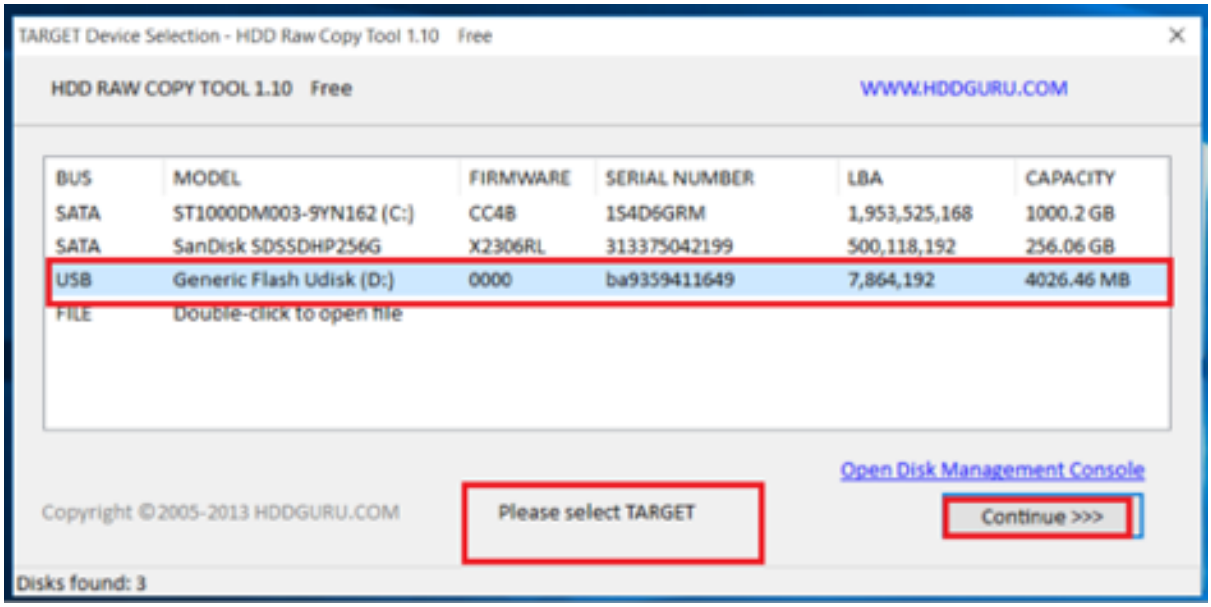


6. Z chwilą wystąpienia komunikatu

   `Operation terminated at offset...`, zamknij okno i odłącz napęd USB.

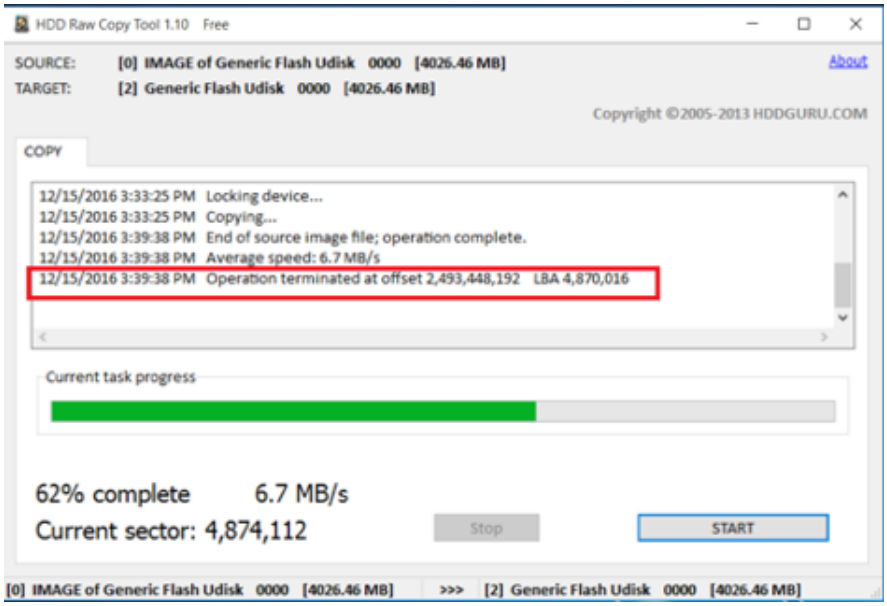


7. Podłącz nośnik pamięci flash i włącz program *HDD Raw Copy Tool*.
8. Na ekranie wyboru napędu źródłowego, zaznacz *FILE* i wskaż plik z obrazem kluczy szyfrujących.
9. Wybierz podłączony nośnik pamięci jako urządzenie docelowe i kliknij *Continue*.



10. Kliknij *Continue*.
11. Kliknij *START*.
12. Proces kopiowania obrazu zakończony jest z chwilą wystąpienia komunikatu:

    ```
    Operation terminated at offset....
    ```



13. Zamknij program i odłącz nośnik flash z zapisanym kluczem szyfrującym.

Mac OS X

1. Uruchom terminal.
2. Wykonaj komendę `sudo -s` i wprowadź hasło użytkownika.
3. Wykonaj komendę `diskutil list`, aby wyświetlić listę urządzeń.
4. Odszukaj napęd o następującym układzie partycji.

```
/dev/disk2 (external, physical):
#: TYPE NAME SIZE IDENTIFIER
0: GUID_partition_scheme *8.0 GB disk2
1: F649773F-1CD6-11E1-9AD2-00262DF29F0D 3.1 KB disk2s1
2: 2B163C2B-1FE5-11E1-8300-00262DF29F0D 1.0 KB disk2s2
```

5. Wykonaj obraz dysku komendą `dd if=/dev/disk2 of=fudo_pen.img bs=1m`, gdzie `if` wskazuje na napęd USB.
6. Odłącz nośnik pamięci flash z kluczem szyfrującym i podłącz nowy.
7. Wykonaj polecenie `dd if=fudo_pen.img of=/dev/disk2 bs=1m`.
8. Wykonaj komendę `sync`.
9. Odłącz nośnik pamięci flash z nowo zapisanym kluczem szyfrującym.

Linux

1. Uruchom terminal.
2. Wykonaj komendę `sudo -s` i wprowadź hasło użytkownika.
3. Wykonaj komendę `dmesg | less`, aby ustalić identyfikator nośnika danych.
4. Wykonaj obraz dysku komendą `dd if=/dev/disk2 of=fudo_pen.img bs=1m`, gdzie `if` wskazuje na napęd USB.
5. Odłącz nośnik pamięci flash z kluczem szyfrującym i podłącz nowy.
6. Wykonaj polecenie `dd if=fudo_pen.img of=/dev/disk2 bs=1m`.
7. Wykonaj komendę `sync`.
8. Odłącz nośnik pamięci flash z nowo zapisanym kluczem szyfrującym.

Tematy pokrewne:

- *Dziennik zdarzeń*
- *Często zadawane pytania*

20.20.2 Monitorowanie stanu systemu

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

Monitorowanie aktywnych sesji

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

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

Monitorowanie przepustowości łącza sieciowego

1. Zaloguj się do panelu administracyjnego Fudo PAM.

2. Wybierz z lewego menu *Zarządzanie* > *Dashboard*.
3. Sprawdź bieżącą aktywność interfejsów sieciowych.

Informacja: 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.

Monitorowanie zajętości macierzy

Ostrzeżenie: Fudo PAM uniemożliwi nawiązywanie nowych połączeń z chwilą, gdy zajętość przestrzeni dyskowej osiągnie wartość 90%.

1. Zaloguj się do panelu administracyjnego Fudo PAM.
2. Wybierz z lewego menu *Zarządzanie* > *Dashboard*.
3. Sprawdź zajętość przestrzeni dyskowej, przejżyj i usuń sesje archiwalne, aby zwolnić miejsce.

Informacja: Więcej informacji o konfigurowaniu widgetów do wygodnego sprawdzania stanu systemu pod linkiem: *Dashboard*.

Tematy pokrewne:

- *Dziennik zdarzeń*
- *Często zadawane pytania*

20.20.3 Kontrola Stanu

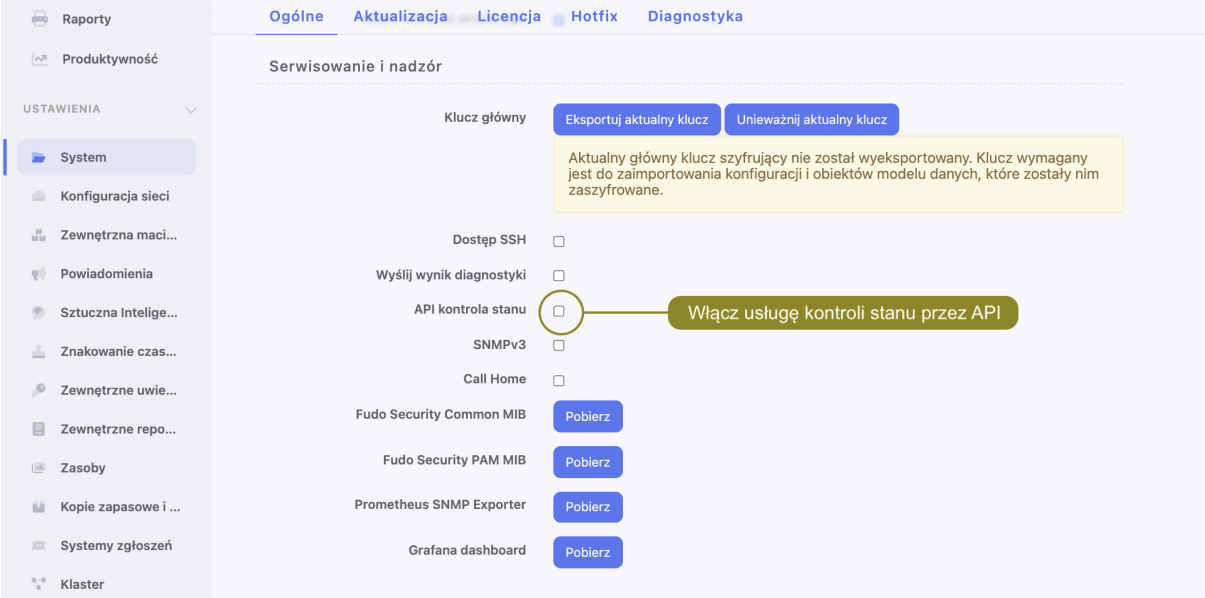
Fudo PAM regularnie przeprowadza kontrolę stanu najważniejszych komponentów systemu. Liczne testy systemu zapewniają stałe sprawdzenie stanu komponentu oraz wysłanie je wyników.

Wyniki są dostępne dla administratora z dwóch poziomów:

1. Korzystając z *SNMP*, dostarczający całość wyników kontroli.
2. Korzystając z funkcji *API kontrola stanu*, dostarczającej podsumowanie wyników kontroli.

20.20.3.1 API kontrola stanu

Funkcja API kontrola stanu jest dostępna w sekcji *Serwisowanie i nadzór* zakładki *Ustawienia* > *System*.



Dostarcza ona krótką informacje o kontroli stanu systemu Fudo PAM. Funkcja może wykorzystywać narzędzia zewnętrzne przy testach stanu systemu.

Wyniki sprawdzenia są dostępne w postaci obiektu JSON:

```
{
"status": "${value}"
}
```

`${value}` może posiadać jedną z dwóch możliwych wartości:

- `ok`: jeśli Fudo PAM działa poprawnie
- `error`: jeśli Fudo PAM nie działa poprawnie, lub któryś z komponentów nie działa właściwie.

Informacja: Ponieważ funkcja kontroli stanu ma na celu dostarczenie klarownych oraz prostych komunikatów, nie przesyła ona szczegółowych informacji, co spowodowało błąd. Szczegółowe informacje dotyczące konkretnego błędu są dostępne po użyciu funkcji *SNMP*.

Włączona opcja *API kontrola stanu* będzie dostępna pod ścieżką:

```
api/healthcheck
```

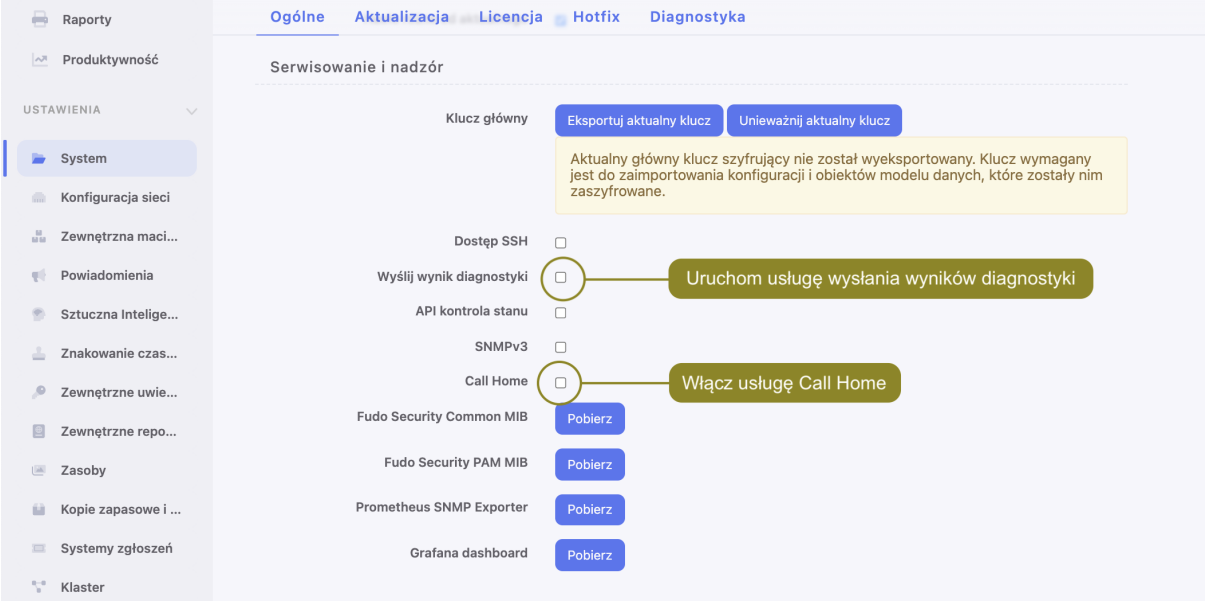
Ostrzeżenie: Opcja *API kontrola stanu* nie wymaga uwierzytelnienia. To oznacza, że każdy kto ma dostęp do TCP jest uprawniony do odczytu wyników stanu kontroli.

20.20.4 Call Home

Call Home jest usługą, pozwalającą Działowi Wsparcia Technicznego Fudo na zdalne łączenie się do systemu klienta i wykonywanie prac naprawczych na klienckiej instancji Fudo PAM.

W celu konfiguracji usługi Call Home, postępuj zgodnie z instrukcją:

1. Przejdź do *Ustawienia* > *System*, dalej do sekcji *Serwisowanie i nadzór*.
2. Zaznacz opcję *Call Home*.
3. Wybierz adres IP swojej instancji Fudo PAM, albo adres `Dowolny`.
4. Dodatkowo, zaznacz opcję *Wyślij wynik diagnostyki* w celu uruchomienia usługi wysłania wyników diagnostyki do Działu Wsparcia Technicznego Fudo.



Informacja:

- Usługa Call Home wymaga utworzenia konta na serwerze Fudo Security. W celu jego założenia, skontaktuj się ze swoim partnerem oraz podaj mu Fudo Unique Identifier (FUID) swojej instancji Fudo PAM. Sprawdź na stronie *Informacja ze stopki dolnej*, gdzie możesz podejrzeć swój FUID.
- Urządzenie Fudo nawiąże wychodzące połączenia SSH z `home.fudosecurity.com`.

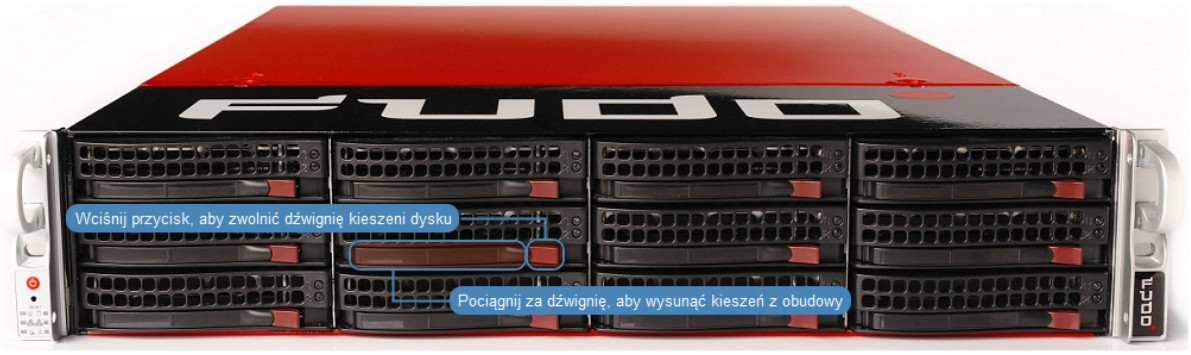
20.20.5 Wymiana dysku macierzy

W domyślnej konfiguracji, macierz dyskowa 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.

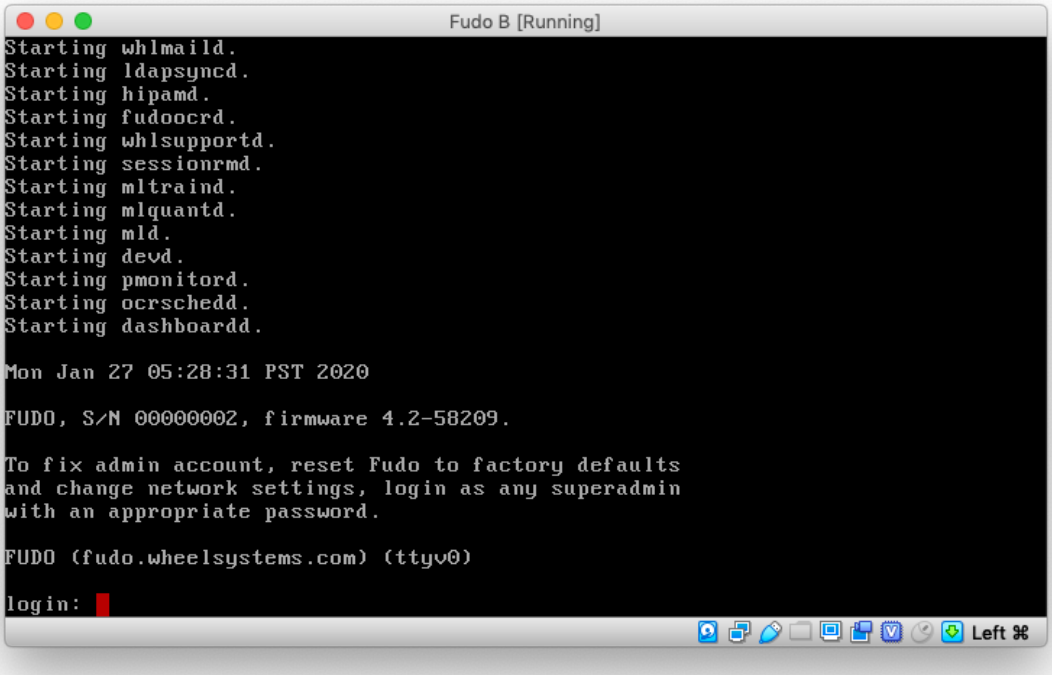
Tematy pokrewne:

- *Urządzenie*
- *Często zadawane pytania*

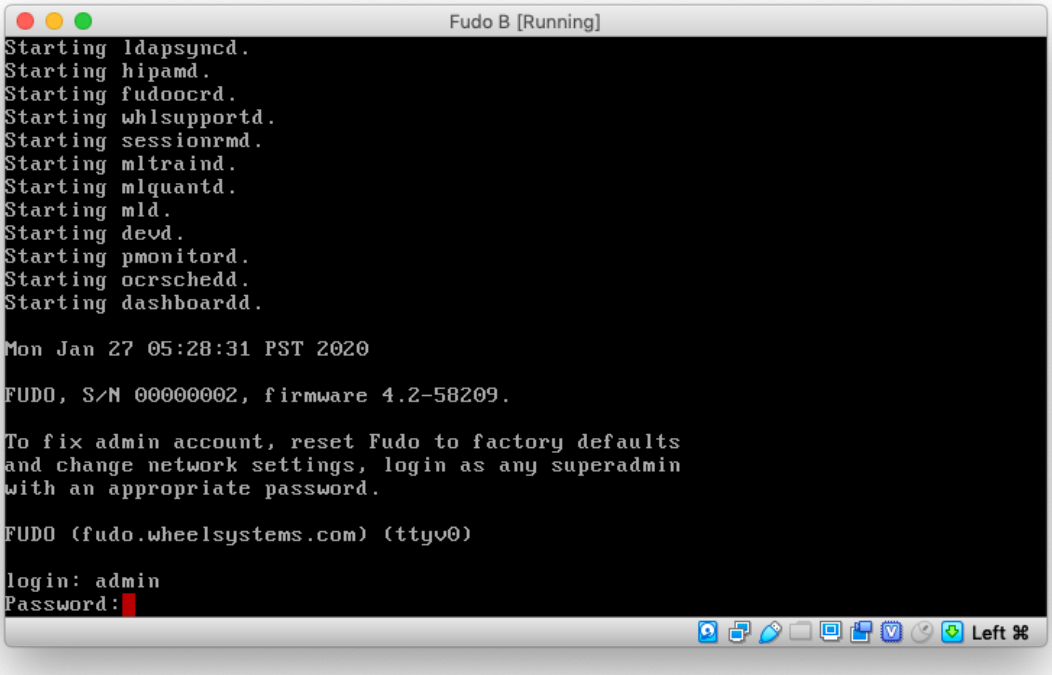
20.20.6 Przywracanie ustawień fabrycznych

Ostrzeżenie: Proces przywracania ustawień fabrycznych jest nieodwracalny i skutkuje usunięciem zarejestrowanych sesji, ustawień systemowych i zdefiniowanych obiektów. 2 pendrive'y muszą być podpięte do urządzenia, żeby proces odbył się poprawnie.

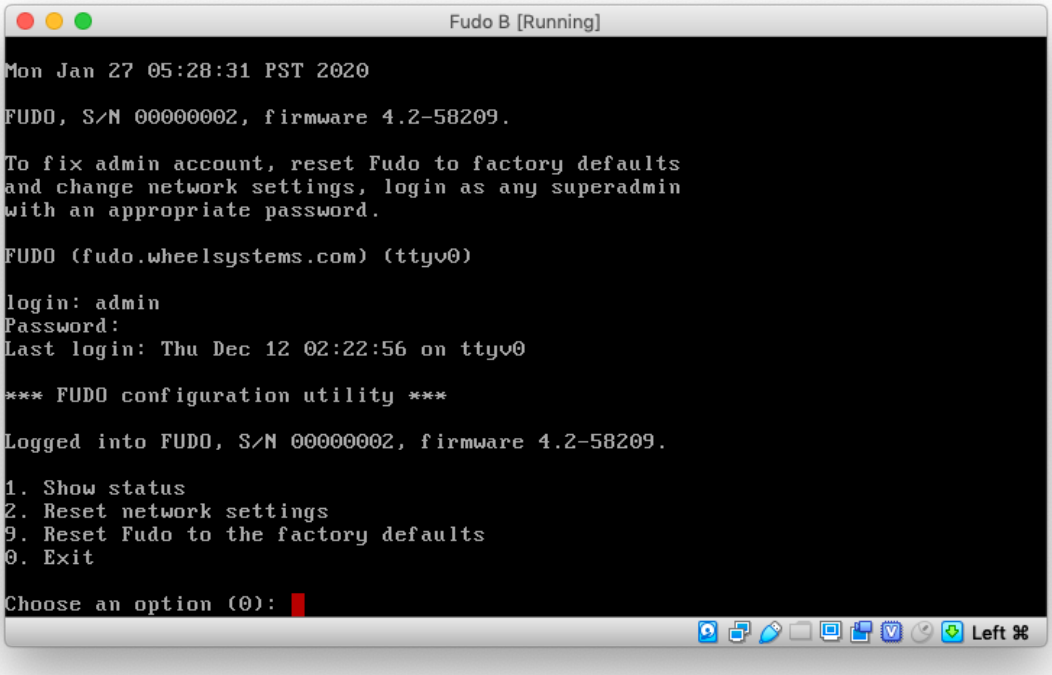
1. Uzyskaj dostęp do konsoli systemowej.
2. Wprowadź nazwę użytkownika z uprawnieniami *superadmin* i naciśnij `Enter`.



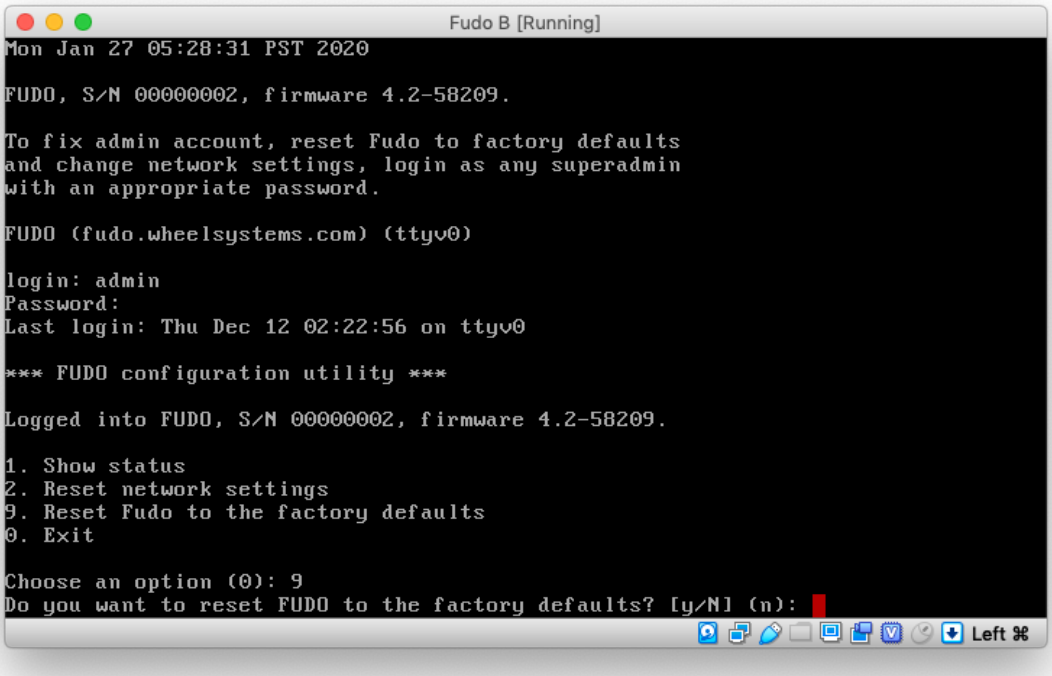
3. Wprowadź hasło i naciśnij klawisz `Enter`.



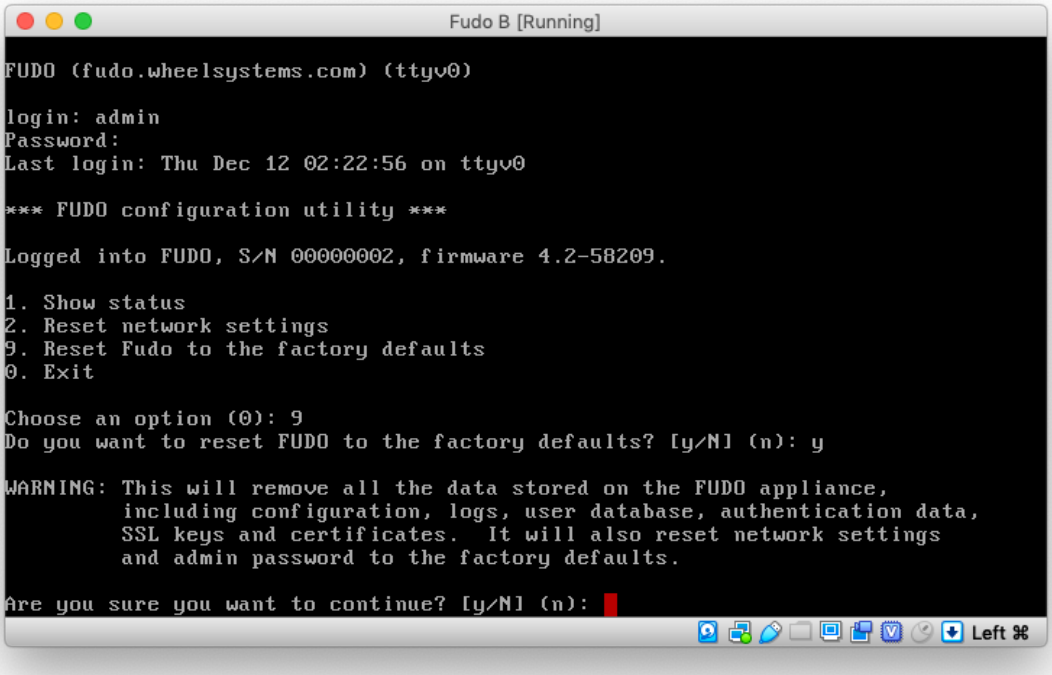
4. Wprowadź `9` i naciśnij klawisz `Enter`.



5. Wprowadź `y` i naciśnij klawisz `Enter`, aby potwierdzić wybór.



6. Wprowadź `y` i naciśnij klawisz `Enter`, aby wykonać procedurę przywrócenia ustawień fabrycznych.



Informacja: W przypadku zdawania urządzenia demonstracyjnego, należy również wyczyścić zawartość nośnika pamięci, na którym zainicjowany został klucz szyfrujący.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*
- *Czynności serwisowe*

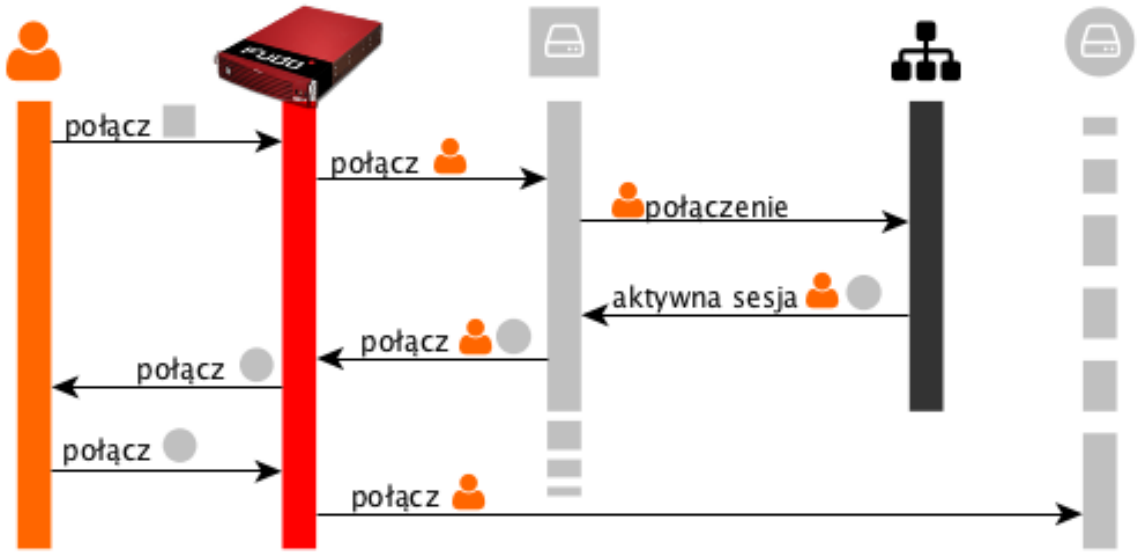
ROZDZIAŁ 21

Informacje uzupełniające

21.1 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.



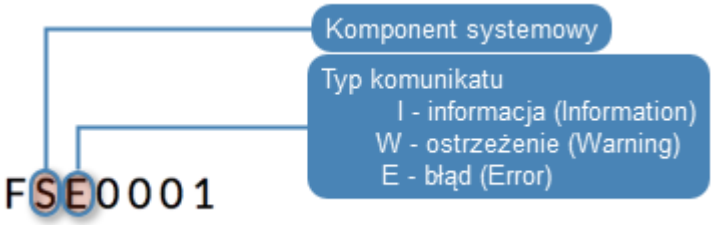
Informacja: Aby proces przekierowania użytkownika się powiódł, wskazany przez broker serwer, musi być zdefiniowany na Fudo i nasłuchiwać na domyślnym porcie RDP (3389) a użytkownik musi być uprawniony do łączenia się z tym zasobem.

Tematy pokrewne:

- *Model danych*
- *RDP*
- *Zarządzanie serwerami*
- *Konta*

21.2 Logowane komunikaty

Informacja: Kod komunikatu zawiera informację o komponencie źródłowym a także o typie wpisu.



Kod komunikatu	Treść komunikatu
FSE0001	Internal system error.
FSE0002	Fudo certificate error.
FSE0003	Unable to change configuration settings.
FSE0004	Configuration import error.
FSE0005	Unable to initialize ${disk}.
FSE0006	Invalid license.
FSE0007	Unable to find license file.
FSE0008	Unable to attach hard drive ${disk}.
FSE0009	Upgrade failed.
FSE0010	License expired.
FSW0011	Retention module was unable to delete session ${sessid} from database.
FSW0012	Retention module error, session ${sessid} skipped.
FSI0013	Session ${sessid} removed according to retention policy.
FSW0014	Retention module was unable to remove session ${sessid}.
FSI0015	Redundancy group ${name} switched to master role.
FSW0016	Unable to send email, SMTP server not configured.
FSI0017	Redundancy group ${name} switched to slave role.
FSI0018	Hard drive ${disk} initialization started.
FSI0019	Hard drive ${disk} initialization completed. Data synchronization may take a moment.
FSE0020	System backup error.
FSI0021	Hard drive ${disk} attached.
FSI0022	Unsupported hard drive hot-swap.
FSI0023	Manual encryption does not support hard drive hot-swap.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FSE0024	Hard drive belongs to another Fudo (${diskserial}) ${disk}.
FSI0025	Cluster node ${name} (${address}) host key set to ${hostkey}.
FSE0026	Cluster communication error.
FSI0027	Cluster node ${name} initialized.
FSE0028	Unable to join node to cluster.
FSI0029	Resumed data synchronization.
FSI0030	Node ${node} initially synchronized.
FSE0031	Timestamping service communication error.
FSE0032	Unable to timestamp session.
FSE0033	Unknown timestamping service provider.
FSI0034	Session ${SESSION} was timestamped.
FSI0035	Email ${mailname} sent to ${admin_email}.
FSW0036	Unable to send email ${mailname} to ${admin_email} through ${account} server.
FSW0037	Output from SMTP client: ${out}.
FSI0038	Saved email ${mailname} sent to ${admin_email}.
FSI0039	System image version ${FULLNEW} uploaded successfully.
FSE0040	Communication error with cluster node %s (%s): Fudo version mismatch (local: %s, remote: %s).
FSI0041	Initial connection from master cluster node.
FSI0042	Cluster node %s (%s) connected from address %s.
FSI0043	Connection from another cluster node.
FSI0044	Connected to cluster node %s (%s) on address %s.
FSI0045	Initial database replication to cluster node %s (%s) completed.
FSE0046	There is no filter called %s.
FSW0047	Error sending notification.
FSE0048	Error authenticating user over RADIUS.
FUI0049	User %s authenticated using password logged in from IP address: %s.
FUI0050	User %s authenticated using password.
FUI0051	User %s authenticated through %s (Host: %s, Port: %d, %s: %s) logged in from IP address: %s.
FUI0052	User %s authenticated through %s (Host: %s, Port: %d, %s: %s).
FUI0053	User %s authenticated through LDAP (Host: %s, Port: %d) logged in from IP address: %s.
FUI0054	User %s authenticated through LDAP (Host: %s, Port: %d).
FUI0055	User %s (domain %s) authenticated through Active Directory (Host: %s, Port: %d) logged in from IP address: %s.
FUI0056	User %s (domain %s) authenticated through Active Directory (Host: %s, Port: %d).
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.
FUW0059	User %s, logging in from IP address %s, has more than one «password» method, using the first password.
FUW0060	User %s has more than one «password» method, using the first password.
FSE0061	Incorrect password repository configuration: login is empty.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
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.
FSI0070	Established proxy connection from %s to %s (%s:%u).
FSI0071	Established gateway connection from %s to %s (%s:%u).
FSI0072	Established transparent connection from %s to %s (%s:%u).
FSI0073	Bastion connection from %s to %s (%s:%u).
FSW0074	Connection terminated because license has expired or was not set.
FSW0075	Connection terminated because number of nodes in cluster exceeded license limit.
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).
FSI0084	Terminating session: %s.
FSI0085	Session finished.
FUI0086	User %s blocked due to connection policy violation.
FUW0087	Session has been terminated due to user %s account expiration.
FUW0088	Session has been terminated due to exceeding the time window defined in the connection %s time policy.
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.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FSE0098	Error fetching password from Thycotic server %s: unable to get password for user %s for the %s server.
FUE0099	Connection terminated.
FUI0100	HTTP connection beetwen client and server initiated.
FUE0101	Unable to find matching HTTP connection.
FUI0102	Session terminated by system administrator.
FUE0103	HTTP connection error.
FUI0104	%s connection terminated.
FUI0105	HTTP session inactive, terminating.
FUE0106	Authentication failed: %s.
FUW0107	Invalid inactivity timeout, falling back to %d seconds.
FUE0108	MySQL connection error.
FUI0109	MySQL connection terminated.
FUE0110	Oracle connection error.
FUI0111	Oracle connection terminated.
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.
FUI0118	Successfully authenticated against the server.
FUI0119	Successfully authenticated against the server as user %s using %s.
FUI0120	Successfully authenticated against the server as user %s within domain %s using %s.
FUI0121	An anonymous user successfully authenticated against the server.
FUI0122	An anonymous user successfully authenticated against the server as user %s.
FUI0123	An anonymous user successfully authenticated against the server as user %s within domain %s.
FUE0124	SSH connection error.
FUE0125	User %s failed to authenticate after %d attempts, disconnecting.
FUI0126	Successfully authenticated against the server as user %s using password.
FUE0127	Invalid authentication method: expected passwordor sshkey, got %s.
FUI0128	User %s authenticated using SSH key.
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).
FUW0131	Functionality %s is not allowed.
FUE0132	Client requested incorrect terminal dimensions (%dx%d).
FUE0133	MSSQL connection error.
FUE0134	TN3270 connection error.
FUE0135	Unknown TN3270 command: %02x.
FUW0136	Functionality %s not allowed.
FUE0136	Telnet connection error.
FSE0137	Unable to read private key.
FSE0138	Server's certificate does not match configured certificate.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
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.
FUI0143	VNC connection closed: %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.
FAI0149	User %s deleted previous system version.
FAI0150	User %s changed backup and retention settings.
FAI0151	User %s %s bastion %s.
FAI0152	User %s deleted bastion %s.
FSE0153	Session indexing failure.
FSE0154	Session conversion failure for session %s.
FSI0155	Starting encoding session video %s.
FSI0156	Completed session video %s encoding.
FAI0157	User %s %s failover configuration.
FAI0158	User %s added node %s.
FAI0159	User %s changed %s in node %s.
FAI0160	User %s deleted node %s.
FAI0161	User %s disconnected node from the cluster.
FAI0162	Cluster has no active nodes. Cluster will be disabled.
FAI0163	User %s created new cluster.
FAI0164	User %s attached current node to cluster.
FAE0165	Error authenticating user %s.
FAI0166	User %s restored original logo for protocol %s.
FAI0167	User %s changed logo for protocol %s.
FAI0168	User %s confirmed sensitive feature %s.
FAI0169	User %s removed confirmation for sensitive feature %s.
FAI0170	User %s changed following notifications settings: %s.
FAI0171	User %s enabled email notifications.
FAI0172	User %s disabled email notifications.
FAI0173	User %(username)s is upgrading Fudo.
FAI0174	User %(username)s upgraded Fudo.
FAI0175	User %(username)s uploaded new upgrade image (version: %(version)s, size: %(size)d).
FAI0176	User %(username)s deleted upgrade files.
FAI0177	User %s uploaded license file.
FAW0178	User %(username)s triggered system restart.
FAW0179	User %(username)s triggered system shutdown.
FAW0180	User %s %s remote SSH access.
FAW0181	User %(username)s changed timestamping settings.
FAW0182	User %(username)s uploaded new PKCS12 file.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FAW0183	User %(username)s changed timestamping provider to %(provider)s.
FAW0184	User %(username)s %(action)s timestamping.
FAI0185	User %s imported system configuration.
FAI0186	User %s exported system configuration.
FAI0187	User %s added NTP server %s.
FAI0188	User %s removed NTP server %s.
FAE0189	Error saving NTP servers: „%s".
FAI0190	User %(username)s changed date & time from %(old_date)s to %(new_date)s.
FAI0191	User %s changed timezone to %s.
FAI0192	User %s changed Fudo HTTPS private key and certificate.
FAI0193	User %s %s SSH access.
FAI0194	User %s requested service data.
FAI0195	User %s added %s to %s for %s %s.
FAI0196	User %s removed %s from %s for %s %s.
FAI0197	User %s changed %s from %s to %s for %s %s.
FAI0198	User %(username)s added IP address %(new_inet)s/%(new_netmask)s to interface %(interface)s with %(new_management)s management and %(new_cluster)s cluster address.
FAI0199	User %(username)s changed subnet mask from %(old_netmask)s to %(new_netmask)s on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0200	User %(username)s %(new_cluster)s cluster address on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0201	User %(username)s %(new_management)s management on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0202	User %(username)s deleted IP address %(old_ip)s from interface %(interface)s.
FAI0203	User %(username)s %(action)s interface %(interface)s.
FAI0204	User %(username)s added member %(member)s to bridge %(interface)s.
FAI0205	User %(username)s removed member %(member)s from bridge %(interface)s.
FAI0206	User %(username)s enabled spanning tree propagation on bridge %(interface)s.
FAI0207	User %(username)s disabled spanning tree propagation on bridge %(interface)s.
FAI0208	User %(username)s changed VLAN %(interface)s parent interface from %(old_parent_interface)s to %(new_parent_interface)s.
FAI0209	User %(username)s changed VLAN %(interface)s ID from %(old_vlan)s to %(new_vlan)s.
FAI0210	User %s deleted interface %s.
FAI0211	User %s changed LDAP synchronization settings.
FAW0213	LDAP error during fetching groups: %s.
FAI0214	User %s enforced full LDAP synchronization.
FAI0215	User %s disabled events logging on syslog servers.
FAI0216	User %s removed syslog server: %s:%s.
FAI0217	User %s added syslog server: %s:%s.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FAI0218	User %s removed syslog server %s.
FAI0219	User %s changed remote log dispatch settings.
FAI0220	User %s changed network interfaces settings.
FAI0221	User %s changed hostname from %s to %s.
FAI0222	User %s added DNS server IP address %s.
FAI0223	User %s removed DNS server IP address %s.
FAI0224	User %s added new route for network %s with gateway %s.
FAI0225	User %s changed gateway for network %s from %s to %s.
FAI0226	User %s deleted network %s with gateway %s.
FAI0227	User %s (%s) terminated session.
FAI0228	Anonymous user from IP address %s with access rights granted by user %s joined session.
FAI0229	User %s from IP address %s joined session.
FAI0230	User %s (%s) suspended session.
FAI0231	User %s (%s) resumed session.
FAE0232	MySQL session playback error.
FAI0233	Anonymous user from IP address %s accessed session %s shared by %s with key %s.
FAI0234	User %s from IP address %s accessed session %s.
FAI0235	User %s %s comment %d for session.
FAI0236	User %s generated key %s with %s access.
FAI0237	User %s is viewing user input for session.
FAI0238	User %s blocked server %s.
FAI0239	User %s unblocked server %s.
FAI0240	User %s blocked connection %s.
FAI0241	User %s unblocked connection %s.
FAI0242	User %s addedd new time policy to connection %s for %s from %s to %s.
FAI0243	User %s changed connection %s %s time policy %s from %s to %s.
FAI0244	User %s deleted time policy for %s %s - %s from connection %s.
FAI0247	User %s deleted server %s.
FAI0248	User %s %s server %s.
FAI0251	User %s deleted connection %s.
FAI0252	User %s %s connection %s.
FAI0253	User %s deleted session.
FAI0254	User %s requested OCR processing for session.
FAW0255	User %s tried to disable a non-exisitent sharing key for session.
FAI0256	User %s disabled anonymous access key %s for session.
FAI0259	User %s deleted download %s.
FAI0260	User %s downloaded file %s for session %s.
FAI0261	Anonymous user from IP address %s terminated session shared by %s with key %s.
FAI0262	User %s terminated session.
FAI0263	User %s blocked user %s.
FAI0264	User %s modified policies settings.
FAI0265	User %s modified regular expressions settings.
FSW0266	Failed to send email.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FSE0267	Error generating report %d: %s.
FAI0268	User %s deleted report „%s”.
FAW0269	User %s cannot delete report „%s”.
FAI0270	Report {} created by user {}.
FAW0271	User %(username)s is blocked.
FAW0272	User %(username)s is not allowed to log in.
FAW0273	User %(username)s logging from IP %(ip)s not found.
FAI0276	User %s unblocked user %s.
FAI0277	User %s deleted user %s.
FAI0278	User %s added user %s to connection %s.
FAI0279	User %s changed user %s.
FAI0281	User %s logged out from Fudo administration panel.
FAI0282	User %s successfully changed his password.
FSE0283	Unable to process pattern: %s
FSW0284	Pattern %s matched on %s with priority %s in session.
FSE0285	Unable to read certificate.
FSE0286	No peer certificate received.
FSW0287	No server key configured, skipping verification.
FSI0288	Server key verification failed.
FUI0289	MSSQL connection terminated.
FSI0290	User %s (%d) was removed. Reason: user wasn't in any of synchronized groups.
FSI0291	System backup initiated, fingerprint: ${fingerprint}.
FSI0292	System backup initiated.
FSI0293	System backup completed, fingerprint: ${fingerprint}.
FSI0294	System backup completed.
FAI0295	User %s blocked bastion %s.
FAI0296	User %s unblocked bastion %s.
FAI0297	User %s created bastion %s.
FAI0298	User %s changed bastion %s.
FAI0299	User %s created server %s.
FAI0300	User %s changed server %s.
FAI0301	User %s changed connection %s.
FAI0302	User %s created connection %s.
FAI0303	User %s created user %s with role %s.
FAI0304	User %s modified %s for %s %s.
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.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FUE0314	Invalid pixel format.
FSE0330	Bad login field configured on LDAP server %s. Error while processing user %s.
FSE0331	Error while processing userAccountControl value of user %s.
FSI0332	User %s will be blocked.
FSI0333	User %s will be unblocked.
FSW0334	User %s has incorrect principal name.
FSI0335	User %s synchronized from LDAP server %s.
FSI0336	Remove pair connection %s user %s.
FSI0337	Add conection %s to user %s.
FSW0338	User %s paired with connection %s, server conflict.
FSI0339	User %s (%s) was removed. Reason: user was not in any of synchronized groups.
FSI0340	Full synchronization from LDAP server %s started.
FSI0341	User %s connections cleared.
FSI0342	User %s will be resynchronized from server %s.
FSI0343	Resynchronized user %s will be removed.
FSW0344	Connection to LDAP server error: %s.
FSI0345	Successfully fetched password from %s.
FUE0346	Client sent a packet bigger than %d bytes.
FSE0348	Unable to get configuration settings.
FAI0349	Anonymous user from IP address %s with access rights granted by user %s left session.
FAI0350	User %s from IP address %s left session.
FUE0351	Client sent unsupported NTLM v1 response.
FSE0352	Bastion requires login and server delimited with one of «%s» (%s).
FAI0353	User %(username)s is deleting upgrade snapshost.
FAI0354	User %(username)s deleted upgrade snapshot.
FSE0355	Inconsistent data, starting recovery replication to cluster node %s (%s).
FUW0356	Unsupported X11 extension: %s.
FUW0357	Server uses higher resolution than the current limit: %dx%d.
FUW0358	Server uses higher color depth than the current limit: %d bpp.
FUE0359	Server rejected X11 connection: %.*s.
FUE0360	Server requires unsupported X11 authentication: %.*s.
FSW0361	Fudo started.
FSE0362	Unable to propagate ARP.
FUE0363	User %s has no access to host %s:%u.
FUI0364	RDP server sent a redirection packet.
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.
FUI0370	User %s authenticated using OTP logged in from IP address: %s.
FUI0371	User %s authenticated using OTP.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FSE0372	Unable to invalidate OTP password %jd.
FUW0373	Session has been terminated due to exceeding the time window defined in a time policy for the user %s and the safe %s.
FSI0374	Established %s connection from %s to %s:%u.
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 to be delimited with one of the «%s» characters (listener: %s, login: %s).
FSE0378	Unable to establish connection: server not found, user not found or user has no access to the server (listener: %s, login: %s).
FSE0379	Unable to establish connection: transparent server (tcp://%s:%u) not found or cannot be reached through listener (listener: %s, login: %s).
FSE0380	Unable to authenticate user %s: server is blocked.
FSE0381	Unable to authenticate user %s: account not found.
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.
FSI0387	Password for account %s verified successfully.
FSI0389	Password for account %s changed successfully.
FAI0393	User %s displayed password history for account %s.
FAI0394	User %s displayed password to account %s changed at %s.
FAI0395	User %s displayed current password for account %s.
FAI0396	User %s blocked safe %s.
FAI0397	User %s unblocked safe %s.
FAI0398	User %s deleted safe %s.
FAI0399	User %s changed safe %s.
FAI0400	User %s created safe %s.
FAI0401	User %s blocked account %s.
FAI0402	User %s unblocked account %s.
FAI0403	User %s deleted account %s.
FAI0404	User %s changed account %s.
FAI0405	User %s created account %s.
FAI0406	User %s blocked listener %s.
FAI0407	User %s unblocked listener %s.
FAI0408	User %s deleted listener %s.
FAI0409	User %s changed listener %s.
FAI0410	User %s created listener %s.
FAI0411	User %s blocked password change policy %s.
FAI0412	User %s unblocked password change policy %s.
FAI0413	User %s deleted password change policy %s.
FAI0414	User %s changed password change policy %s.
FAI0415	User %s created password change policy %s.
FSI0416	Connection between safe %s and user %s has been removed.
FSI0417	Connection between safe %s and user %s has been added.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FSI0418	User %s was removed from safes %s.
FSE0420	Unable to authenticate user %s against server %s.
FAI0421	User %s assigned listener %s to safe %s.
FAI0422	User %s unassigned listener %s from safe %s.
FAI0423	User %s assigned account %s to safe %s.
FAI0424	User %s unassigned account %s from safe %s.
FAI0425	User %s assigned authentication method %s to user %s.
FAI0426	User %s unassigned authentication mathod %s from user %s.
FAI0427	User %s changed authentication mathod %s assigned to user %s.
FAI0428	User %s assigned user %s to safe %s.
FAI0429	User %s unassigned user %s from safe %s.
FAI0430	User %s blocked password changer %s.
FAI0431	User %s unblocked password changer %s.
FAI0432	User %s deleted password changer %s.
FAI0433	User %s changed password changer %s.
FAI0434	User %s created password changer %s.
FSW0435	Password changer timed out for acccount %s.
FUI0436	User %s authenticated using token logged in from IP address: %s.
FUI0437	User %s authenticated using token.
FAW0438	User %s authenticated using new token while the old one still exists.
FAW0439	User %s authenticated using old token.
FAI0440	User %s granted access for account %s to user %s.
FAI0441	User %s revoked access for account %s from user %s.
FAI0442	User %s granted access for listener %s to user %s.
FAI0443	User %s revoked access for listener %s from user %s.
FAI0444	User %s created policy %s.
FAI0445	User %s deleted policy %s.
FAI0446	User %s changed policy %s.
FAI0447	User %s assigned regexp %s to policy %s .
FAI0448	User %s unassigned regexp %s from policy %s.
FAI0449	User %s created regexp %s.
FAI0450	User %s deleted regexp %s.
FAI0451	User %s changed regexp %s.
FAI0452	User %s granted access for safe %s to user %s.
FAI0453	User %s revoked access for safe %s from user %s.
FAI0454	User %s granted access for server %s to user %s.
FAI0455	User %s revoked access for server %s from user %s.
FAI0456	User %s granted access for user %s to user %s.
FAI0457	User %s revoked access for user %s from user %s.
FAI0458	User %s displayed password history for account %s. Reason: %s.
FAI0459	User %s displayed password to account %s changed at %s. Reason: %s.
FAI0460	User %s displayed current password for account %s. Reason: %s
FSE0461	Invalid data from %s LDAP server.
FAI0462	User {} created redundancy group {}.
FAI0463	User {} deleted redundancy group {}.
FAE0464	User %s is not allowed to login from address %s.
FUW0465	Establishing new connections has been disabled.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FSE0466	Fudo versions do not conform.
FUE0467	Client tried to authenticate using an invalid UTF-8 login.
FSI0468	A passphrase used to decrypt disks was changed.
FSE0469	Unexpected number of bastions (%s).
FSE0470	Unexpected number of servers (%s).
FSE0471	Unexpected number of users (%s).
FSE0472	RDP servers %s must all use TLS (NLA) or Standard RDP Security.
FSE0473	Fudo cannot be upgraded to PAM.
FSI0474	Fudo can be upgraded to PAM.
FSE0475	Connection %s replaces a login and forwards a secret for servers %s which is not allowed.
FSE0476	ZVOL with encryption key does not exist.
FSE0477	Replication of encryption key to cluster node %s (%s) failed.
FSE0478	Unable to join cluster's node ${name}. Fudo versions do not conform (local: ${VERSION}, remote: ${rversion}).
FSE0479	Servers %s must all use the same %s settings.
FSE0480	Servers %s must all use the same protocol.
FAI0481	New OTP for user %s has been generated.
FSW0482	Unable to verify password for account %s.
FUI0483	User %s authenticated using Citrix logon ticket logged in from IP address: %s.
FUI0484	User %s authenticated using Citrix logon ticket.
FUE0485	ICA connection error.
FUI0486	ICA server closed connection.
FAI0487	User %s requested timestamping for session.
FAI0488	User %s requested timestamping for account.
FSI0489	Label %s not defined on this node, skipping listener %s.
FAI0490	User %s created external authentication %s.
FAI0491	User %s changed external authentication %s: %s.
FAI0492	User %s deleted external authentication %s.
FSE0493	Unable to establish connection to server %s (%s): label %s not defined on this node.
FSI0494	Label %s not defined on this node, skipping external authentication %s.
FSE0495	Communication error with cluster node %s (%s): connection failure.
FSE0496	Communication error with cluster node %s (%s): unable to replicate a batch with object %jd to table %s.
FSE0497	Communication error with cluster node %s (%s): unable to replicate a batch with object %jd (name: %s) to table %s.
FSE0498	Communication error with cluster node %s (%s): unable to store object %jd in table %s.
FSE0499	Communication error with cluster node %s (%s): unable to store object %jd (name: %s) in table %s.
FSE0500	Communication error with cluster node %s (%s): unable to connect to %s.
FSE0501	Communication error with cluster node %s (%s): failure during handshake.
FSE0502	Database error.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FSE0503	Communication error with a cluster node: Fudo version mismatch (local: %s, remote: %s).
FSE0504	Communication error with cluster node %s (%s): %s.
FSE0505	Communication error with a cluster node: failure during handshake.
FSI0508	Successfully replicated encryption key to node %s (%s).
FSE0509	Communication error with cluster node %s (%s): unable to replicate session data.
FSE0510	Communication error with cluster node %s (%s): intial replication failed.
FSW0511	There has been an attempt to reset Fudo to factory defaults. Resetting Fudo to factory defaults has been administratively disabled.
FAI0512	User %s enabled reset account.
FAI0513	User %s disabled reset account.
FAW0514	User %s of role %s tried to view %s, but has insufficient privileges for this action.
FSE0515	Unable to upload backup #${currno} at ${datetime}.
FSI0516	Backup #${currno} at ${datetime} successfully uploaded.
FSE0517	Backup configuration error: %s.
FSE0518	Backup internal error.
FSI0519	${type} backup snapshot ${snapname} successfully taken.
FUE0520	User %s tried to access ICA server %s:%u using Citrix StoreFront which is not permitted.
FUE0521	Citrix StoreFront sent an ICA file without a destination address.
FSW0522	Roolback to ${oldversion} failed.
FSW0523	Upgrade to ${oldversion} failed.
FSW0524	Roolback to ${version} succeeded.
FSW0525	Upgrade to ${version} succeeded.
FSE0526	Error communicating with bypass card. Error setting nextboot mode.
FSE0527	Error communicating with bypass card. Error setting bpe mode.
FSE0528	Error communicating with bypass card. Error switching card mode.
FSE0529	Error communicating with bypass card.
FAI0530	User %s enabled snmp.
FAI0531	User %s disabled snmp.
FSW0532	External storage is unavailable.
FSE0533	Unable to attach external storage.
FSI0534	External storage attached.
FSE0535	External storage is unavailable in this configuration.
FSW0536	External storage detached.
FSI0537	External storage attached successfully.
FAI0538	Set external storage connection mode to %s
FAI0539	Set configured WWN to %s, external storage connection mode to %s
FAI0540	Interface discovery while configuring external storage: %s
FSW0540	Found ${cdisk} paths to fiber channel ${wwn} from ${cscbus} devices.
FSW0541	Retention module was unable to move session ${sessid}.
FAI0542	User %s assigned account %s, listener %s to safe %s.
FAI0543	User %s unassigned account %s, listener %s from safe %s.
FSE0544	Failed to list snapshots.
FSW0545	Unable to change password for account %s.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
FUI0546	ICA client closed connection.
FAE0547	User %s could not create a ticket requesting an access to safe %s.
FAI0548	User %s created ticket %s requesting an access to safe %s.
FAI0549	User %s approved ticket %s requesting an access for user %s to safe %s.
FAI0550	User %s rejected ticket %s requesting an access for user %s to safe %s.
FAI0551	User %(username)s added member %(member)s to lagg %(interface)s.
FAI0552	User %(username)s removed member %(member)s from lagg %(interface)s.
FSE0553	Unable to extract public key from CA.
FUE0554	SFTP server uses an unsupported version %u.
FAI0555	User %s added address %s to server %s.
FAI0556	User %s removed address %s from server %s.
FAI0557	User %s changed address %s assigned to server %s.
FSI0558	Starting encoding file for session %s.
FSI0559	Completed encoding file for session %s.
FSE0560	Session has not been approved nor rejected.
FSE0561	Unexpected number of connections (%s).
FAI0562	User %s rejected session %s. Reason: %s.
FAI0563	User %s rejected session %s.
FAI0564	User: {} tried to accept session: {} but it was accepted by:
FAI0565	User: {} rejected session: {}
FAI0566	User: {} tried to reject session: {} but it was accepted by:
FAI0567	User: {} tried to reject session: {} but it was rejected by:
FAI0568	User: {} accepted session: {}
FAI0569	User: {} tried to accept session: {} but it was rejected by:
FAI0570	User %s approved session %s.
FSI0571	Proxy connection closed.
FSE0572	Proxy connection error.
FSI0573	Client sent an invalid token.
FSE0574	Unable to resolve ${ip} domain to address.
FSE0575	Unable to convert raw file to pcap.
FSI0578	User %s (%s) was removed. Reason: user's external server dosen't exists any more.
FSE0580	Cluster %s has an invalid token: %s.
FAI0581	User %s changed domain search path from %s to %s.
FSW0582	Disk $cdev was removed.

21.3 Plik konfiguracyjny połączenia ICA

Plik konfiguracyjny `.ica` definiuje parametry konfiguracyjne umożliwiające nawiązanie połączenia z monitorowanym serwerem za pomocą klienta protokołu ICA.

21.3.1 Plik ICA do połączeń bez TLS

```
[ApplicationServers]
<nazwa połączenia>=

[<nazwa połączenia>]
ProxyType=SOCKSV5
ProxyHost=<host>:<port>
ProxyUsername=*
ProxyPassword=*
Address=<login użytkownika>
Username=<login użytkownika>
ClearPassword=<hasło>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

Informacja: `<nazwa połączenia>` służy do celów informacyjnych i może być dowolnym ciągiem znaków.

21.3.2 Plik ICA do połączeń TLS

```
[ApplicationServers]
<nazwa połączenia>=

[<nazwa połączenia>]
SSLEnable=On
SSLProxyHost=<FQDN>:<port>
Address=<login użytkownika>
Username=<login użytkownika>
ClearPassword=<hasło>
TransportDriver=TCP/IP
EncryptionLevelSession=Basic
Compress=Off
```

Informacja: `<nazwa połączenia>` służy do celów informacyjnych i może być dowolnym ciągiem znaków.

Tematy pokrewne:

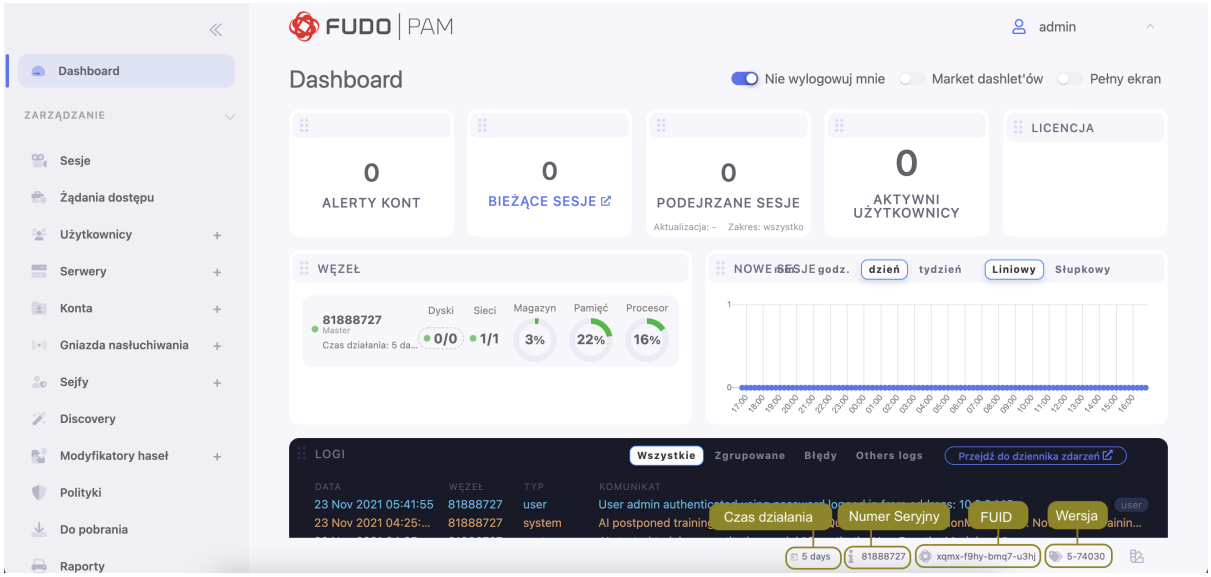
- *Szybki start - ICA*
- *Protokół ICA*
- *Model danych*

21.4 Informacja ze stopki dolnej

Dolna stopka menu zawiera informacje systemowe obecnej instancji Fudo PAM.

1. **Czas działania** - czas, kiedy system został aktywowany ostatnio.
2. **Numer Seryjny** - ID węzła klastra. Jest unikatowy dla pojedynczego klastra.

3. **FUID (Fudo Unique Identifier)** - Unikatowy ID obecnej instancji Fudo PAM.
4. **Wersja** - Obecna wersja systemu.



ROZDZIAŁ 22

Fudo Officer 1.0

Fudo Officer 1.0 jest aplikacją mobilną, pozwalająca administratorom Fudo PAM zarządzać żądaniami użytkowników o dostęp do serwera. Żądania mogą być akceptowane bądź odrzucane przez administratorów w aplikacji Fudo Officer albo w panelu admina Fudo PAM w zakładce *Zarządzanie* > *Sesje*.

Informacja: Więcej informacji na temat obsługi żądań w Panelu Admina: *Akceptowanie żądań użytkowników* oraz *Odrzucanie żądań użytkowników*.

Aplikacja Fudo Officer jest dostępna w językach: angielski, polski, rosyjski oraz ukraiński. Język aplikacji ustawia się automatycznie zgodnie z ustawieniami telefonu.

Ostrzeżenie: Aplikacja Fudo Officer działa tylko z włączoną usługą *Call Home*, dostępną w sekcji *Serwisowanie i nadzór* zakładki *Ustawienia* > *System*.

Dodatkowo, w Sejfie powinna być zaznaczona opcja *Wymagaj potwierdzenia* oraz opcja notyfikacji push *Session awaiting approval (push)* dla użytkownika.

22.1 Konfiguracja

Ostrzeżenie: Powiązanie urządzenia jest konfigurowane dla obecnie zalogowanego użytkownika.

W celu konfiguracji aplikacji Fudo Officer, postępuj zgodnie z instrukcją:

1. Zezwól aplikacji na wysłanie notyfikacji.
2. Ustaw PIN (4-6 cyfrowy numer). Ten PIN jest niezależny od PINa, którym odblokowujesz telefon.

3. Dodaj swój pierwszy profil.

3.1. Otwórz panel Admina Fudo PAM.

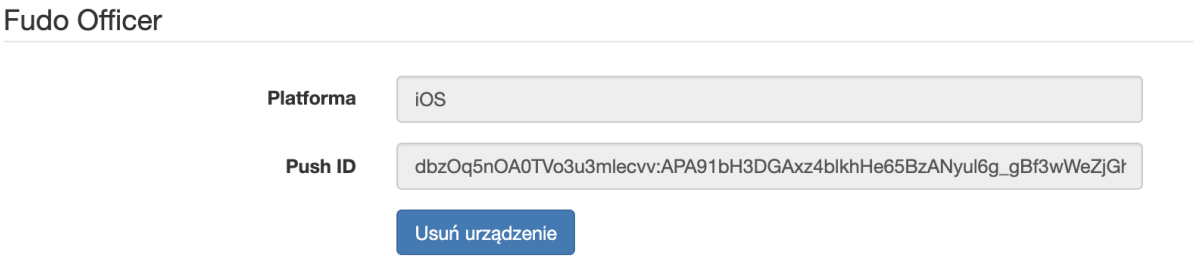
3.2. Przejdź do *Zarządzanie* > *Użytkownicy*. Wybierz użytkownika, dla którego chcesz założyć profil.

3.3. Przewiń w dół do sekcji *Fudo Mobile* i kliknij przycisk *Dodaj urządzenie*.

3.4. Wyświetlony QR kod ma być zeskanowany telefonem, więc wróć do aplikacji i kliknij *Dodaj profil*. Następnie, kliknij *Skanuj kod QR*. Zeskanuj QR kod, wyświetlony w panelu Admina Fudo PAM.

3.5. Ustaw nazwę profilu i kliknij *Utwórz profil*. Nazwa profilu jest edytowalna.

3.6. Wróć do panelu Admin Fudo PAM i kliknij *OK* w okienku z QR kodem. Sekcja *Fudo Mobile* powinna pokazywać *Platformę* powiązanego urządzenia oraz *Push ID*.



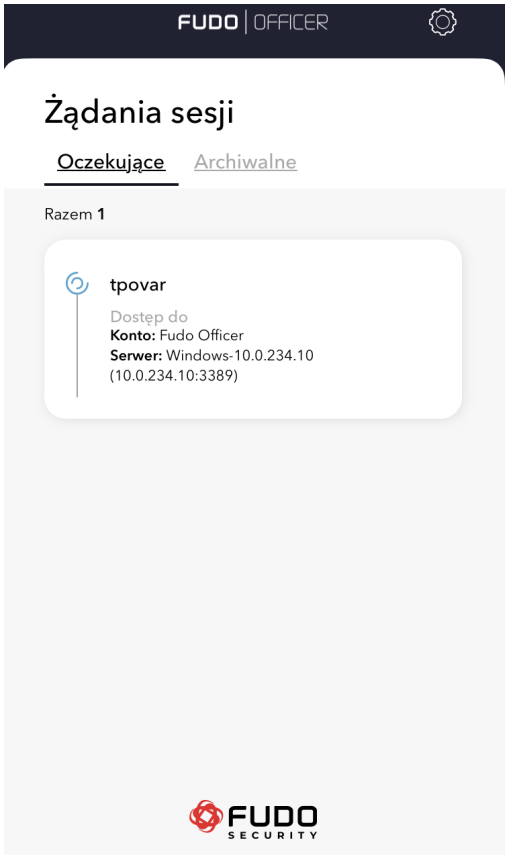
3.7. Kliknij *Zapisz*.

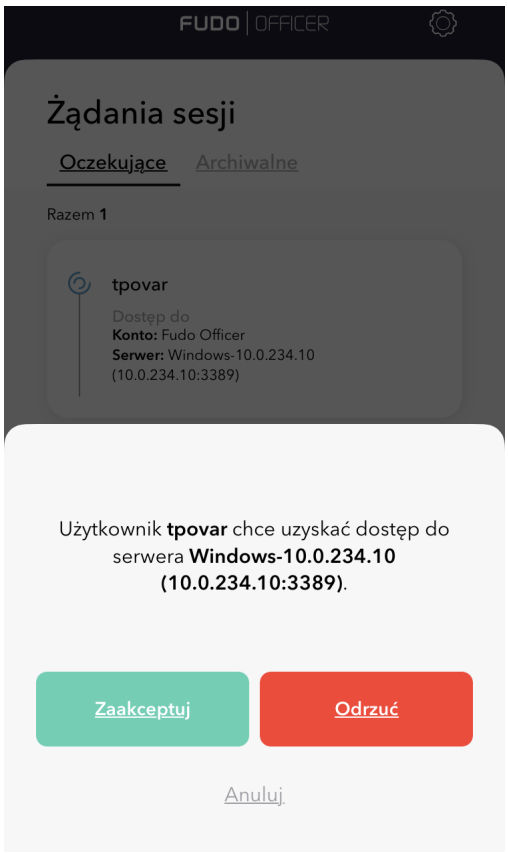
Teraz możesz zarządzać żądaniami użytkowników z poziomu stworzonego profilu.

Informacja: Profil jest unikalny dla jednego użytkownika jednej instancji Fudo PAM.

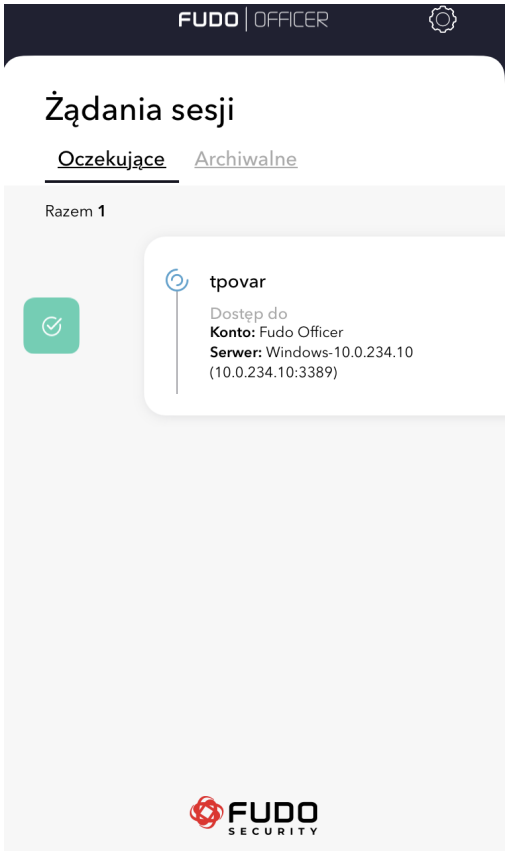
22.2 Zarządzanie żądaniami sesji

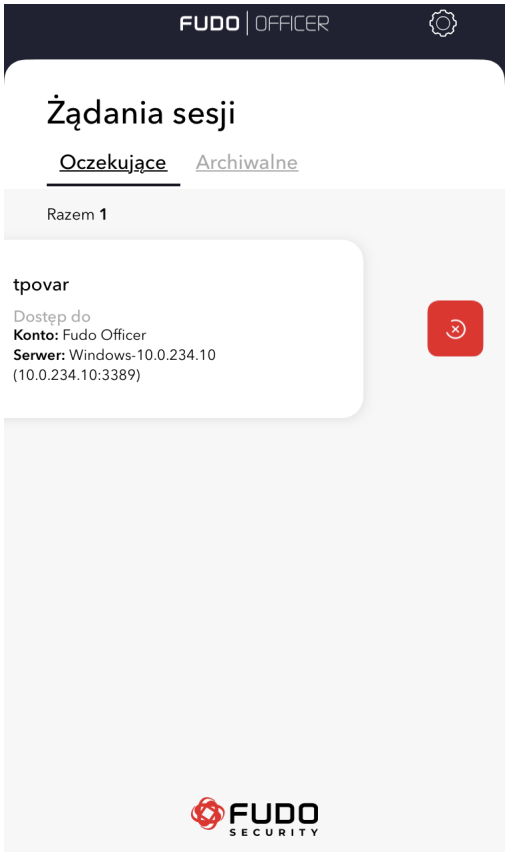
Żądania oczekujące odpowiedzi są dostępne w zakładce *Oczekujące*. Kliknij na pozycję żądania, żeby zaakceptować bądź odrzucić go.





Alternatywnie, przewin `w prawo` na pozycji żądania, żeby zaakceptować żądanię, albo przewiń `w lewo`, żeby go odrzucić.





Przeprocesowane żądania (zaakceptowane oraz odrzucone) są dostępne w zakladce *Archiwalne*. Można je sortować według `Daty`, `Nazwy serwera` albo `Użytkownika`.

22.3 Ustawienia

Edytuj profil

1. Wybierz ikonkę z zębatką w prawym górnym rogu.
2. Przewiń w lewo na wybranym profilu.
3. Kliknij ikonkę z ołówkiem, żeby edytować nazwę profilu, albo Kliknij ikonkę z krzyżykiem, jeśli chcesz usunąć profil.

Dodaj profil

1. Otwórz panel Admina Fudo PAM.
2. Przejdź do *Zarządzanie* > *Użytkownicy*. Wybierz użytkownika, dla którego chcesz założyć profil.
3. Przewiń w dół do sekcji *Fudo Mobile* i kliknij przycisk *Dodaj urządzenie*.
4. Wyświetlony QR kod ma być zeskanowany telefonem, więc wróć do aplikacji i kliknij *Dodaj profil*. Następnie, kliknij *Skanuj kod QR*. Zeskanuj QR kod, wyświetlony w panelu Admina Fudo PAM.
5. Ustaw nazwę profilu i kliknij *Utwórz profil*. Nazwa profilu jest edytowalna.
6. Wróć do panelu Admin Fudo PAM i kliknij *OK* w okienku z QR kodem. Sekcja *Fudo Mobile* powinna pokazywać *Platformę* powiązanego urządzenia oraz *Push ID*.
7. Kliknij *Zapisz*.

Zmień PIN kod

1. Wybierz ikonkę z zębatką w prawym górnym rogu.
2. Kliknij *Zmień PIN kod*.
3. Wprowadź aktualny PIN kod.
4. Wprowadź nowy PIN kod 4-6 cyfrowy.
5. Potwierdź nowy PIN kod.

Przełącznik *Bezpieczny dostęp do aplikacji* jest domyślnie włączony. Włacza on metodę uwierzytelnienia do logowania do aplikacji.

ROZDZIAŁ 23

AAPM (Application to Application Password Manager)

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

Moduł AAPM wspiera systemy operacyjne Microsoft Windows oraz rodziny systemów BSD i Linux.

23.1 Kompilowanie narzędzia *fudopv*

W wyniku poniższych kroków zostanie stworzona aplikacja *fudopv* z załączonym interpreterem języka Python.

Informacja: Procedurę uruchomienia *fudopv* na systemie docelowym, bez kompilowania plików źródłowych, znajdziesz w rozdziale *Wdrożenie fudopv bez kompilacji kodu źródłowego*.

23.1.1 Python

Informacja: *fudopv* wymaga środowiska języka Python 3.x.

Windows

Pobierz i zainstaluj środowisko Python: https://www.python.org/downloads/

Informacja: Podczas instalacji, zaznacz opcję dodania `python.exe` do ścieżki (path).

Linux

Zainstaluj środowisko Python zgodnie z zaleceniami producenta.

Przykładowa konfiguracja:

```
./configure \
  --prefix=/opt/python-3.6 \
  --with-ensurepip=install \
  --disable-optimizations \
  --enable-shared
```

Informacja:

- `--disable-optimizations` - opcje optymalizacji mogą skutkować problemami z budowaniem środowiska,
- `--with-ensurepip=install` - instalacja narzędzi do zarządzania pakietami Pythona,
- `--enable-shared` - jedna z zależności *fudopv* wymaga biblioteki `.so` interpretera Pythona.

23.1.2 Środowisko wirtualne

Informacja: Do utworzenia paczki niezbędny jest moduł `virtualenv`.

1. Wykonaj polecenie `pip install virtualenv requests` lub `easy_install virtualenv requests`.
2. W katalogu `fudopv/` wykonaj komendę: `virtualenv deps`.

W podkatalogu `deps/` zostanie utworzone środowisko wirtualne, niezbędne do zbudowania aplikacji *fudopv*.

Windows

Wykonaj komendę `deps\Scripts\Activate`, aby aktywować środowisko.

Linux

Jeśli korzystamy z interpretera zbudowanego ze źródeł można wykorzystać znajdujące się tam narzędzia `pip` oraz `easy_install`. Należy dodatkowo

Jeśli korzystasz z interpretera zbudowanego ze źródeł, możesza wykorzystać znajdujące się w nim narzędzia *pip* oraz *easy_ install*. W takim przypadku, należy dodatkowo ustawić ścieżkę do bibliotek współdzielonych i uruchomić `virtualenv` wskazując interpreter w parametrze `-p`:

```
    LD_LIBRARY_PATH=/opt/python-3.6/lib
/opt/python-3.6/bin/pip install virtualenv requests
/opt/python-3.6/bin/virtualenv -p /opt/python-3.6/bin/python deps
```

W celu aktywacji środowiska, wykonaj komendę

```
source deps/bin/activate
```

23.1.3 Pobranie zależności

W aktywnym środowisku wirtualnym, wykonaj komendę `pip install -r requirements.txt`, aby w katalogu `deps/`, zainstalować wymagane zależności.

Informacja: Jeśli wystąpi problem `ImportError: No module named _markerlib`, wykonaj komendę `pip install --upgrade distribute` i ponownie zainstaluj zależności.

Windows

Pobierz i zainstaluj *pywin32*: https://sourceforge.net/projects/pywin32/files/

Informacja: Wybierając instalator pamiętaj o wybraniu wersji dla języka Python 3.x.

Po aktywowaniu środowiska `virtualenv`, uruchom poniższe polecenie ze ścieżką do instalatora pywin32:

```
easy_install path\to\pywin32
```

Linux

System operacyjny Linux nie wymaga dodatkowych kroków.

23.1.4 Zbudowanie narzędzia *fudopv*

1. Pobierz i rozpakuj archiwum źródłowe *fudopv*.
2. Wykonaj komendę `python setup.py`, która utworzy paczkę w katalogu *fudopv*.

Informacja: PyInstaller nie wspiera tworzenia paczek z poziomu konta uprzywilejowanego. Jeśli wystąpi problem `ERROR: You are running PyInstaller as user root. This is not supported.`, zmień funkcję `check_not_running_as_root()` w `./deps/lib/python3.6/site-packages/PyInstaller/utils/misc.py`, tak żeby nie zwracała wyniku sprawdzenia.

Tematy pokrewne:

- *Uruchamianie fudopv*
- *Wdrożenie fudopv bez kompilacji kodu źródłowego*
- *Interfejs API*

23.2 Wdrożenie *fudopv* bez kompilacji kodu źródłowego

Aby korzystać z narzędzia *fudopv* bez kompilacji plików źródłowych, postępuj zgodnie z poniższą procedurą.

1. Pobierz i zainstaluj środowisko języka Python 3.x.

Informacja: Zaleca się, aby *fudopv* uruchamiane było w środowisku wirtualnym.

2. Wykonaj polecenie `pip install virtualenv requests` lub `easy_install virtualenv requests`, aby zainstalować środowisko wirtualne.
3. W katalogu `fudopv/` wykonaj polecenie `virtualenv deps`.
4. Dodaj *fudopv* do ścieżki wyszukiwania. Wykonaj polecenie `export PYTHONPATH=~/fudopv` gdzie `"~/fudopv"` będzie ścieżką do katalogu, w którym rozpakowałeś program narzędziowy i wykonałeś `virtualenv/easy_install`.
5. Wykonaj polecenie `python -m fudopv`, aby uruchomić *fudopv*.

Tematy pokrewne:

- *Uruchamianie fudopv*
- *Kompilowanie narzędzia fudopv*
- *Interfejs API*

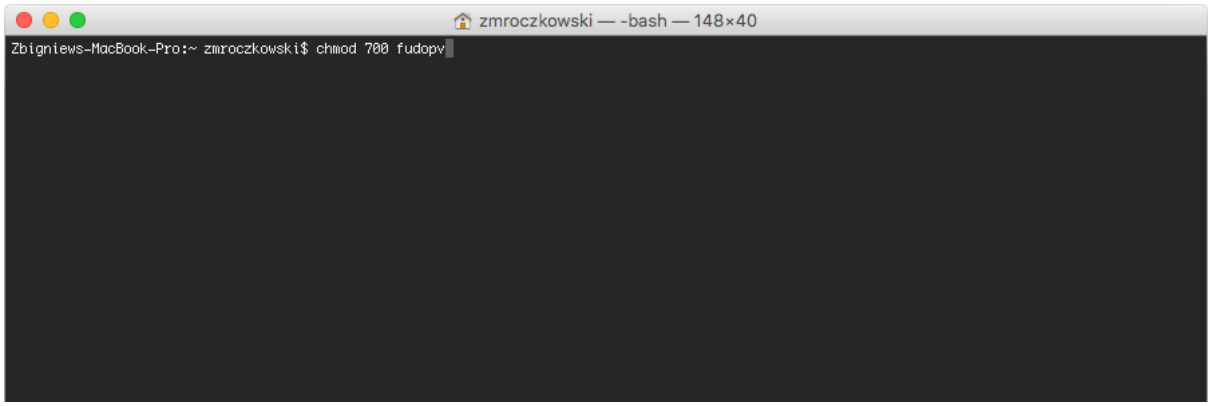
23.3 Uruchamianie *fudopv*

Parametry wywołania

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

Komenda/opcja/parametr	Opis
Komendy	
`getcert`	Pobierz certyfikat SSL *Portalu Użytkownika*.
`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.

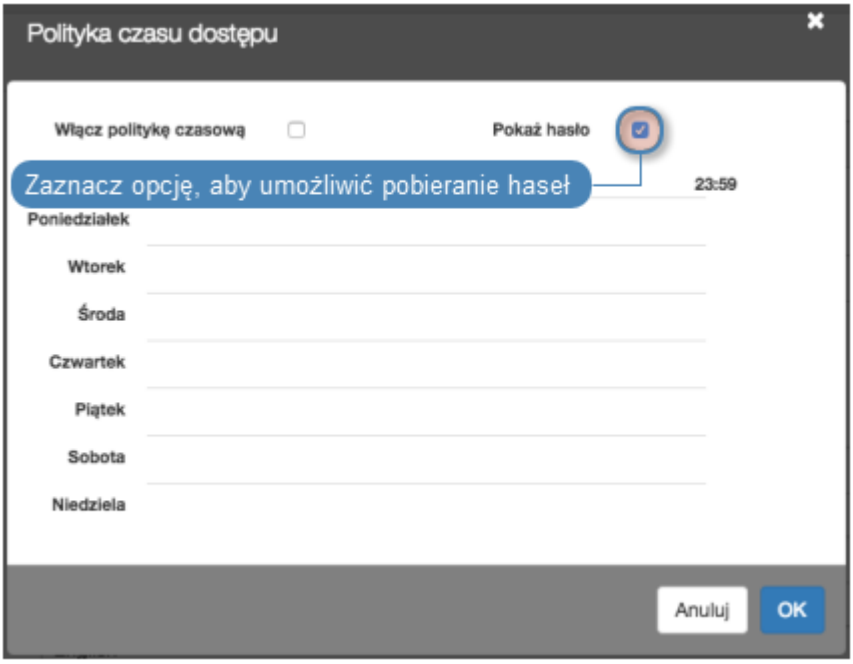
1. Skrypt `fudopv` umieść na serwerze i nadaj mu prawa wykonywalności.



2. Zaloguj się do panelu administracyjnego Fudo PAM.
3. Stwórz konto użytkownika o roli `user`, uwierzytelnianego hasłem statycznym lub jednorazowym.

Informacja:

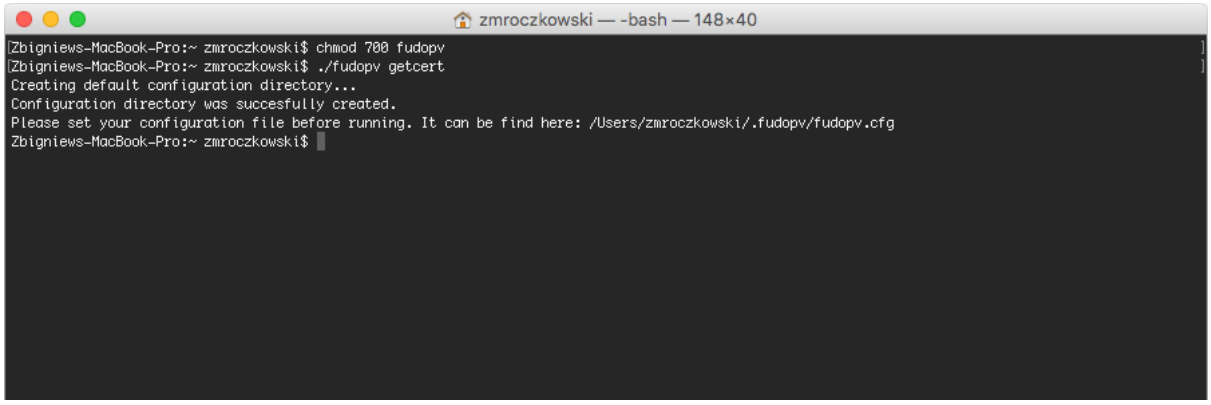
- Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
- Kliknij *+Dodaj*.
- Wprowadź nazwę użytkownika.
- Określ termin ważności konta.
- Z listy rozwijalnej *Rola*, wybierz `user`.
- Przypisz użytkownikowi sejf i kliknij obiekt, aby wywołać jego właściwości.
- Zaznacz opcję *Pokaż hasło*.



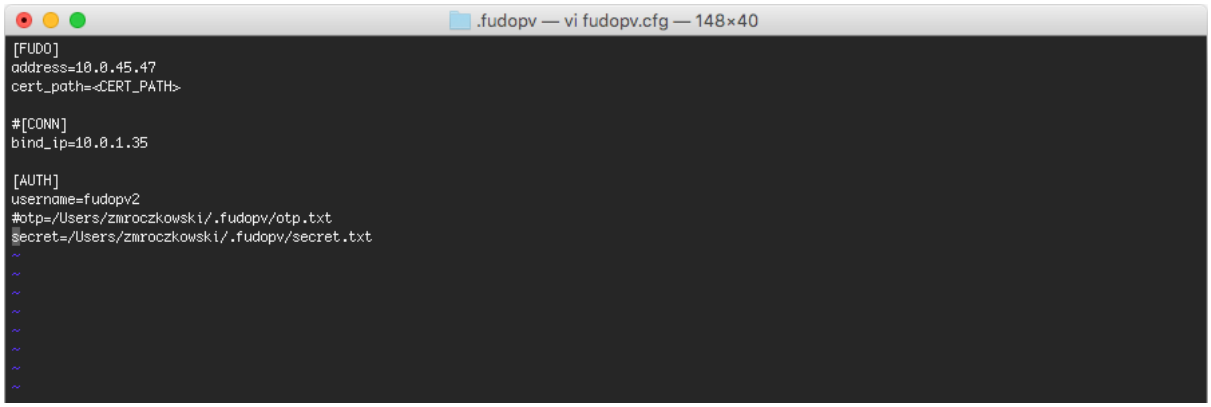
- W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Typ*, wybierz `Hasło` lub `Hasło jednorazowe`.
- Dla uwierzytelnienia hasłem, wprowadź hasło w polach *Hasło* i *Powtórz hasło*.

- Jeśli chcesz żeby zapytania API mogły być wysyłane tylko z określonego adresu IP, w sekcji *API*, kliknij ikonę + i wprowadź 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 *Portalu Użytkownika*.
`cert_path`	Ścieżka pliku z certyfikatem SSL Portalu Użytkownika.

`[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. Parametr opcjonalny.

`[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.

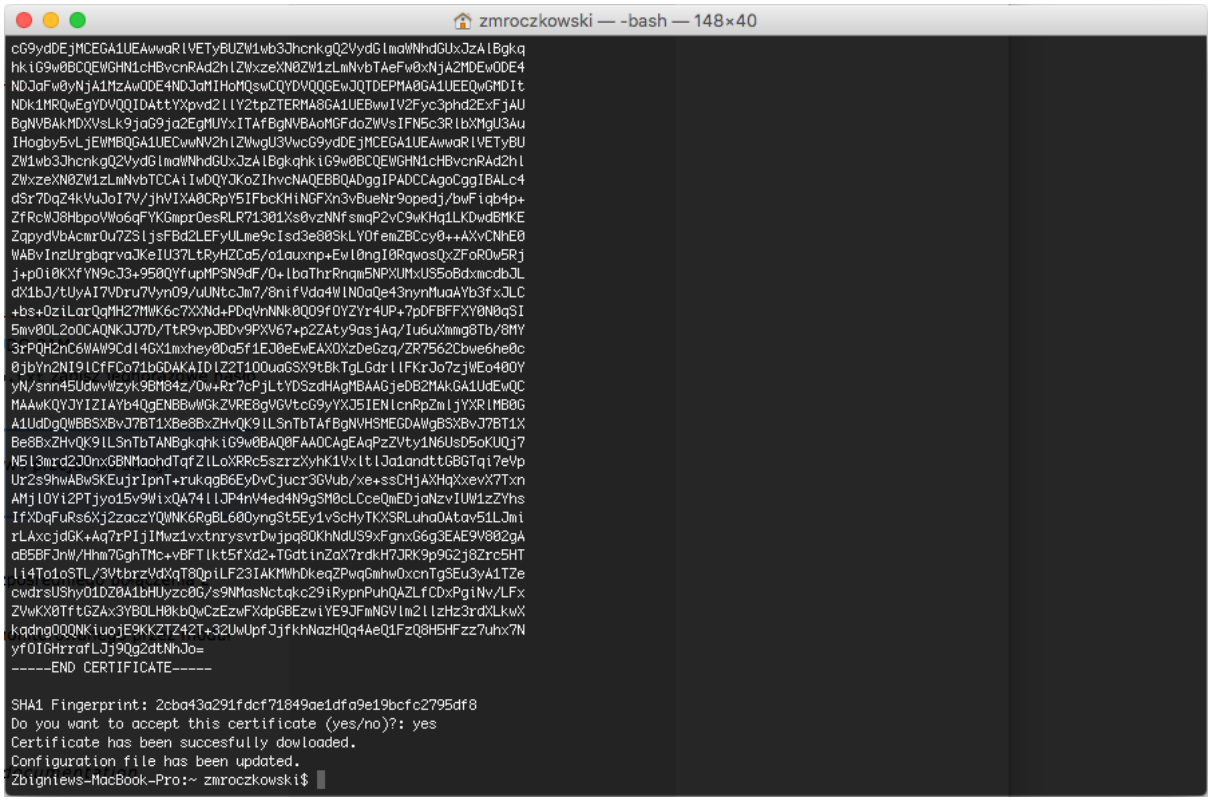
Informacja:

- W sekcji `[FUDO]`, w linii `address`, wprowadź adres IP Portalu Użytkownika.
- Linię `cert_path` pozostaw bez zmian, zostanie ona uzupełniona automatycznie przy okazji poprawnego wykonania komendy `fudopv getcert`.
- Jeśli dla użytkownika skonfigurowana została możliwość wysyłania zapytań do API z określonego adresu IP, 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.

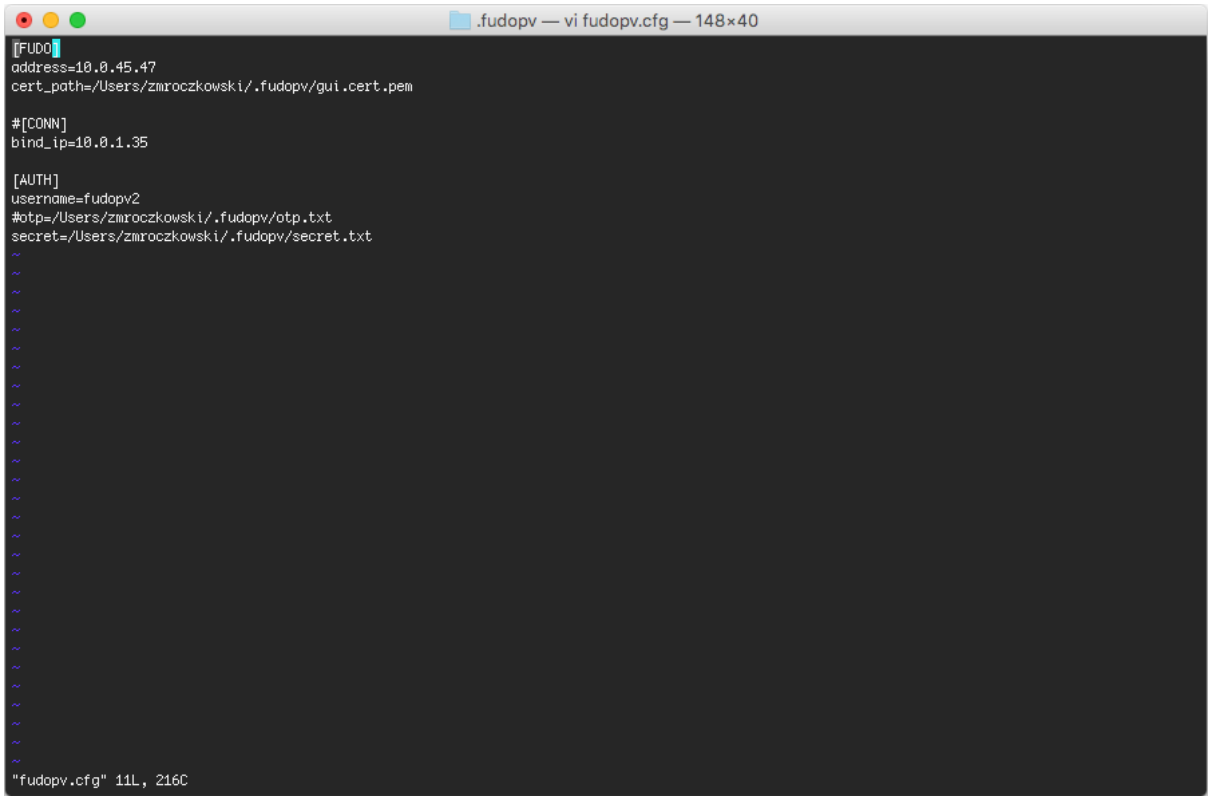
Na przykład:

```
[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 Portalu Użytkownika.

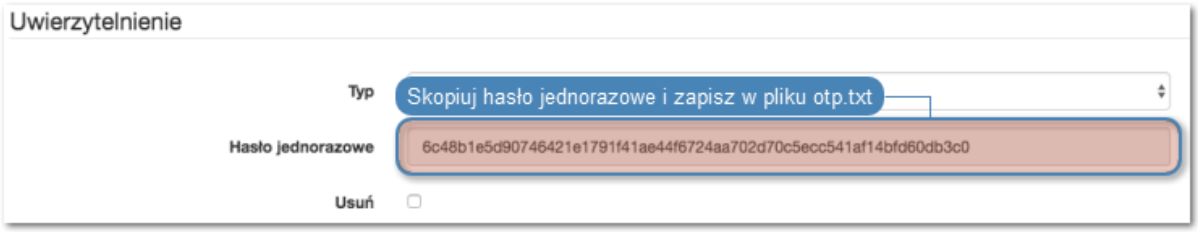


Informacja: Po prawidłowym wykonaniu komendy, ścieżka certyfikatu w pliku konfiguracyjnym zostanie automatycznie uzupełniona.



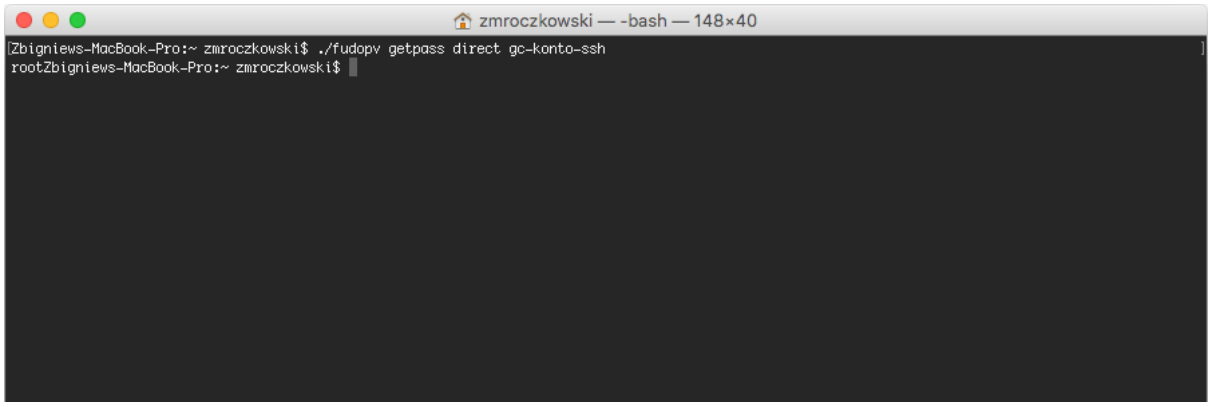
7. W pliku `secret.txt`, zapisz hasło konta użytkownika; lub w pliku `otp.txt` zapisz jednorazowe hasło dostępu.

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

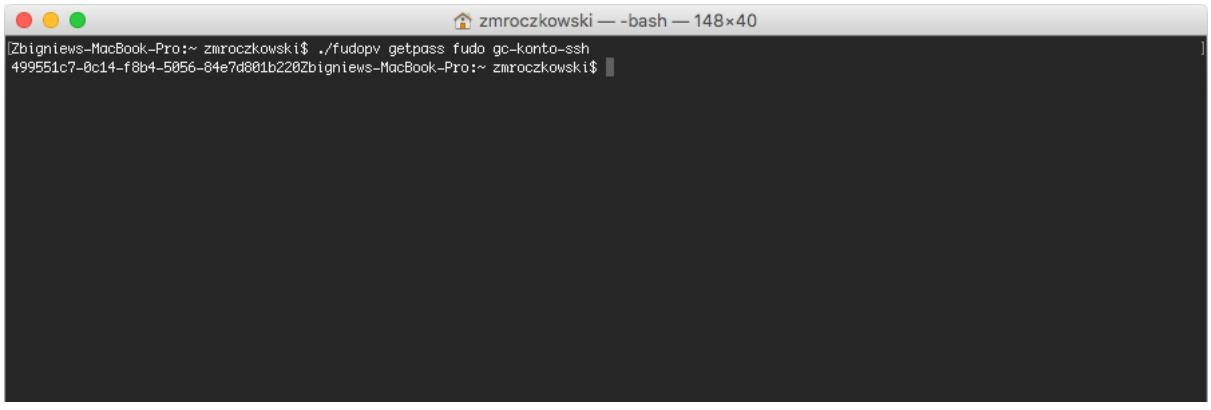


8. Wykonaj komendę:

- `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.

Tematy pokrewne:

- *Kompilowanie narzędzia fudopv*
- *Model danych*

- *Opis systemu*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

23.4 Interfejs API

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

Tematy pokrewne:

- *Kompilowanie narzędzia fudopv*
- *Uruchamianie fudopv*

23.5 Sposoby uwierzytelnienia

Legenda:

- **url**: adres wykonywanego przez `fudopv` połączenia,
- **->**: żądanie wysyłane przez `fudopv`,
- **<-**: odpowiedź otrzymywany od Fudo,
- **status**: status odpowiedzi,
- **FUDO**: adres Fudo,
- **USER**: nazwa użytkownika,
- **SECRET**: hasło (static/OTP),
- **SESSIONID**: token sesji,
- **method**: metoda protokołu HTTP: GET/POST/PUT,
- **{„key”: „value”}**: JSON przekazywany w zapytaniu/odpowiedzi.

23.5.1 Hasło statyczne

Statyczne hasło użytkownika, przechowywane w pliku `secret.txt`.

- -> url: https://FUDO/api/portal/login
- -> method: POST
- -> `{"username": "USER", "password": "SECRET"}`
- <- status:
  - 200, OK
    - <- `{"sessionid": "SESSIONID"}`
  - 401, UNAUTHORIZED
  - <- *Nie dotyczy.*

23.5.2 Token

Jednorazowe hasło użytkownika, przechowywane w pliku `otp.txt`.

- -> url: https://FUDO/api/portal/login
- -> method: POST
- -> `{"username": "USER", "otp": "SECRET"}`
- <- status:
  - 200, OK
    - <- `{"otp": NEW_SECRET, "sessionid": "SESSIONID"}`
  - 401, UNAUTHORIZED
  - <- *Nie dotyczy.*

Po zapisaniu nowego hasła w pliku `otp.txt`, `fudopv` wysyła potwierdzenie jego otrzymania.

- -> url: https://FUDO/api/portal/confirm
- -> method: POST
- -> `{"otp": "NEW_SECRET"}`
- <- status: 204, NO CONTENT

Tematy pokrewne:

- *Uruchamianie fudopv*
- *Kompilowanie narzędzia fudopv*
- *Interfejs API*

ROZDZIAŁ 24

Systemy zgłoszeń

Zakładka *Systemy zgłoszeń* jest dedykowana do usługi **Service now**, która jest niedostępna.

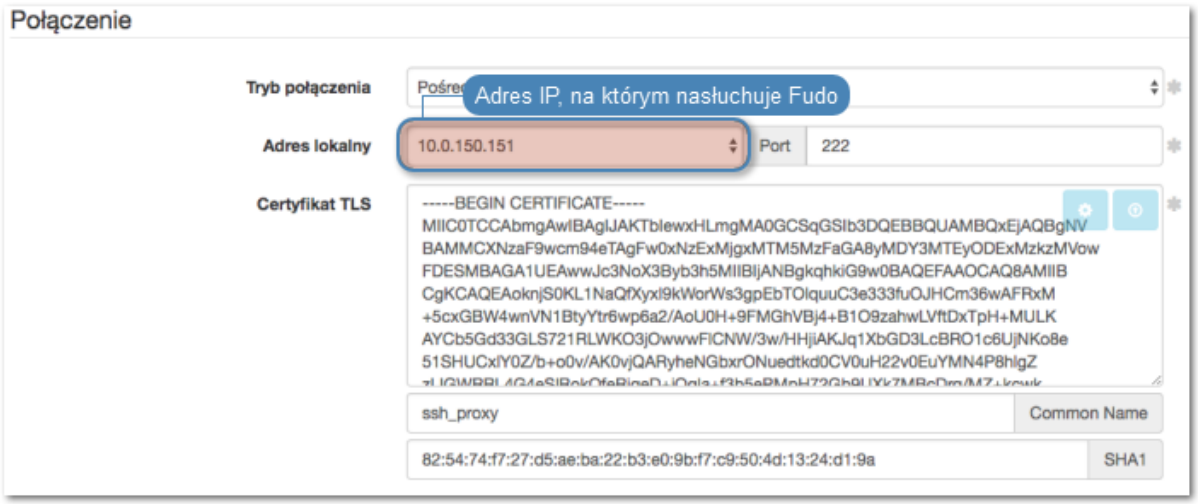
ROZDZIAŁ 25

Aplikacje klienckie

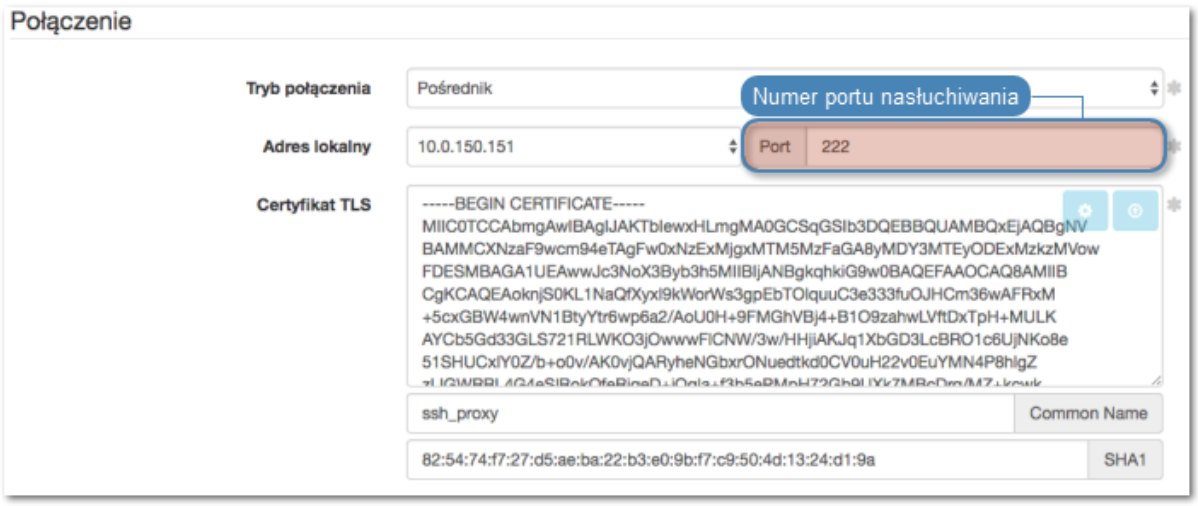
25.1 PuTTY

Połączenie *SSH* z serwerem monitorowanym poprzez gniazdo nasłuchiwania w trybie *proxy*.

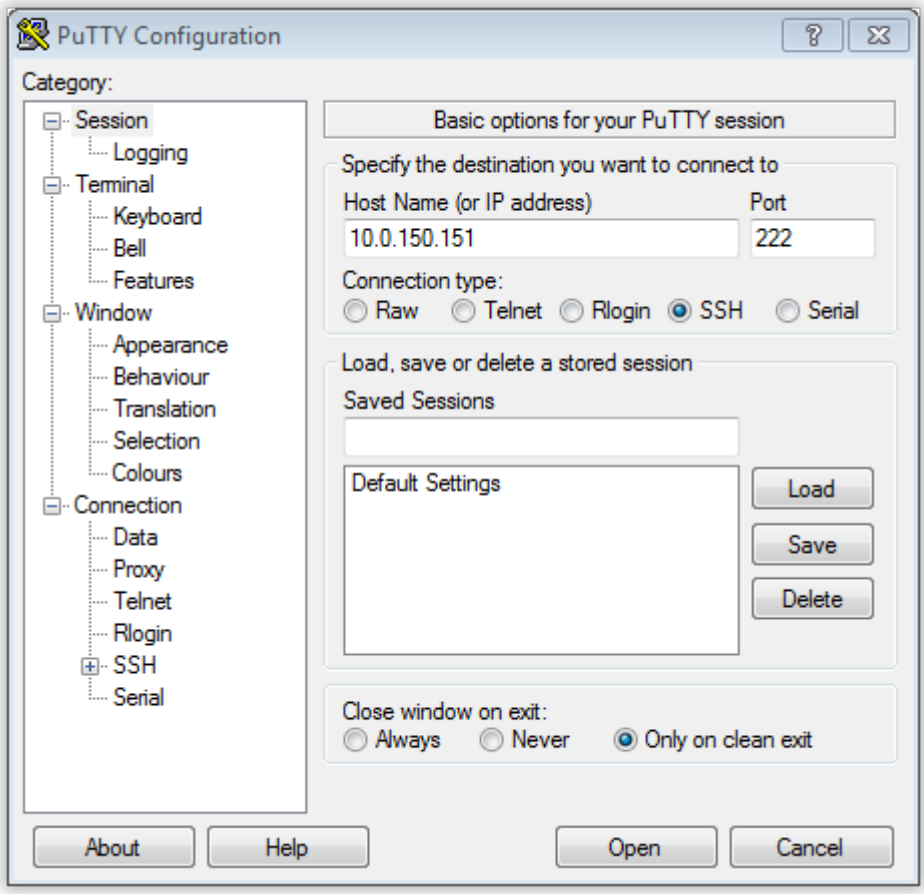
1. Pobierz i uruchom PuTTY.
2. W polu *Host Name (or IP address)* wprowadź adres IP zdefiniowany w sekcji *Połączenie*, w parametrze *Adres lokalny* gniazda nasłuchiwania.



3. Wprowadź numer portu zgodnie z definicją w obiekcie.

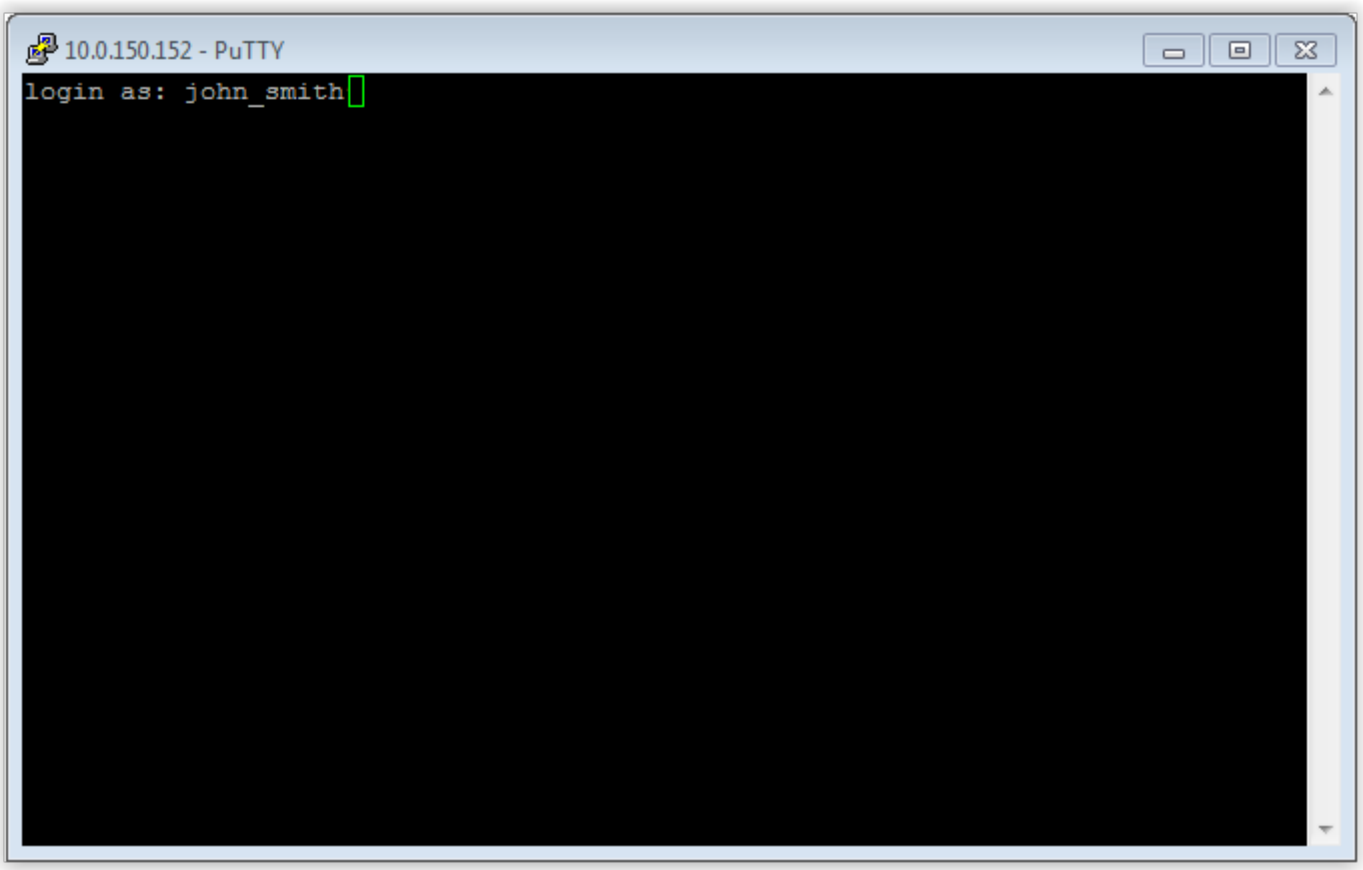


4. W polu wyboru typu połączenia (*Connection type*), wybierz `SSH`.



5. Kliknij *Open*.

6. Wprowadź nazwę użytkownika wraz z nazwą konta, na serwerze docelowym.



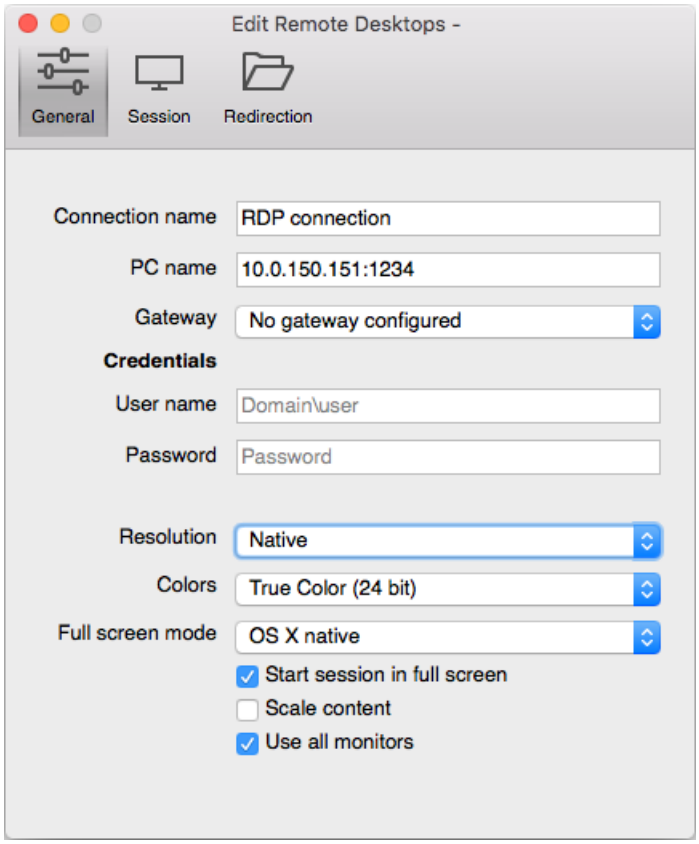
6. Wprowadź hasło użytkownika.

Tematy pokrewne:

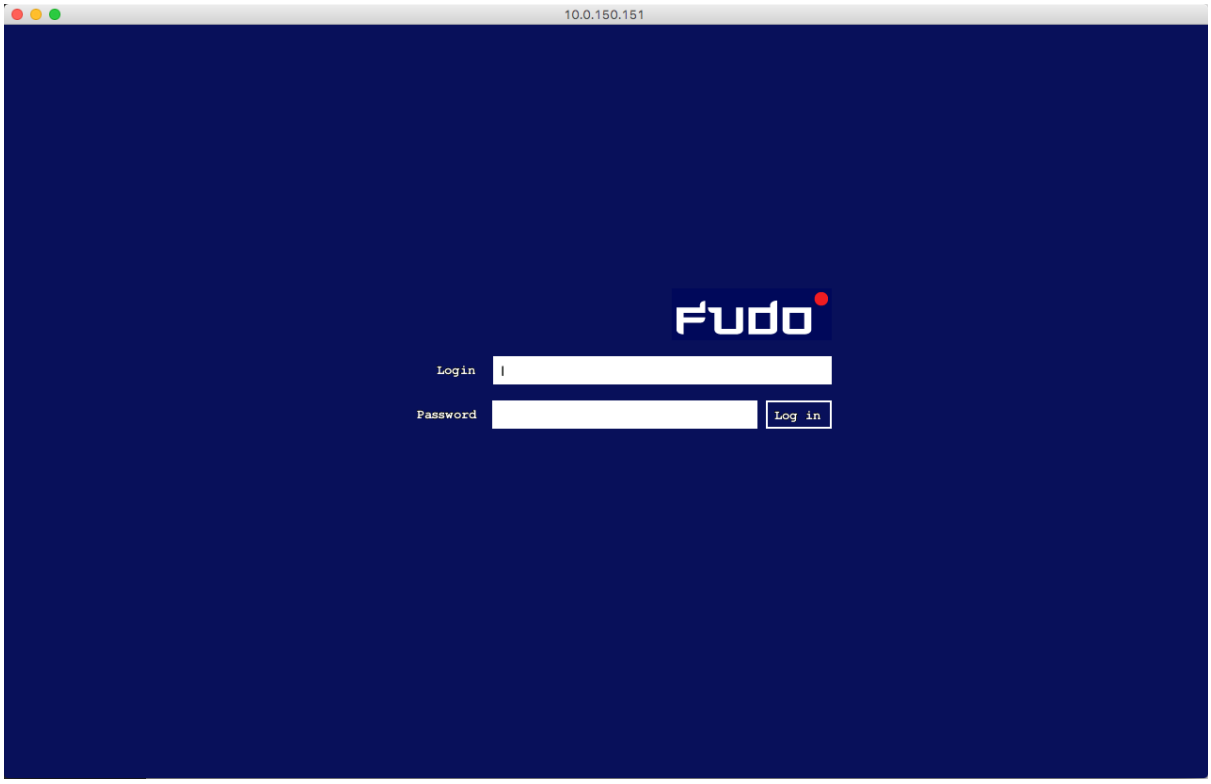
- *SSH*

25.2 Microsoft Remote Desktop

1. Uruchom klienta połączeń RDP.
2. W polu *PC name*, wprowadź adres IP oraz numer portu zdefiniowany w gnieździe nasłuchiwania.

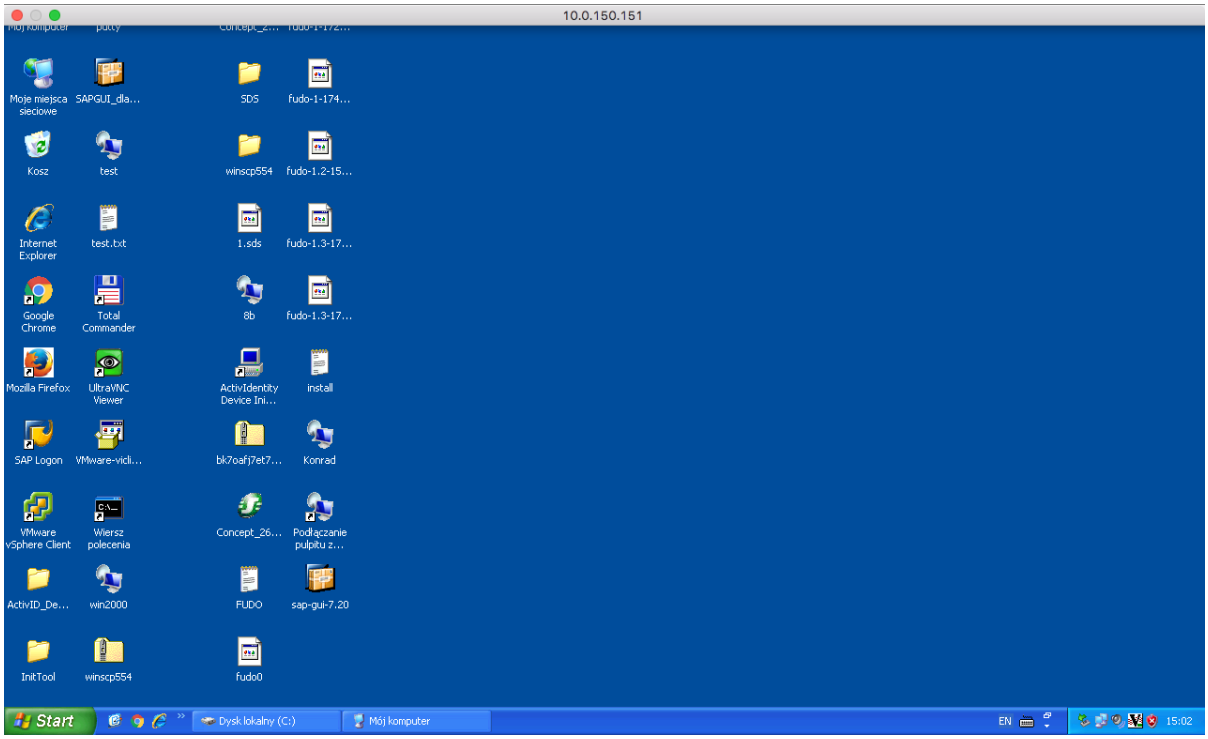


3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter].



Informacja: 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*.

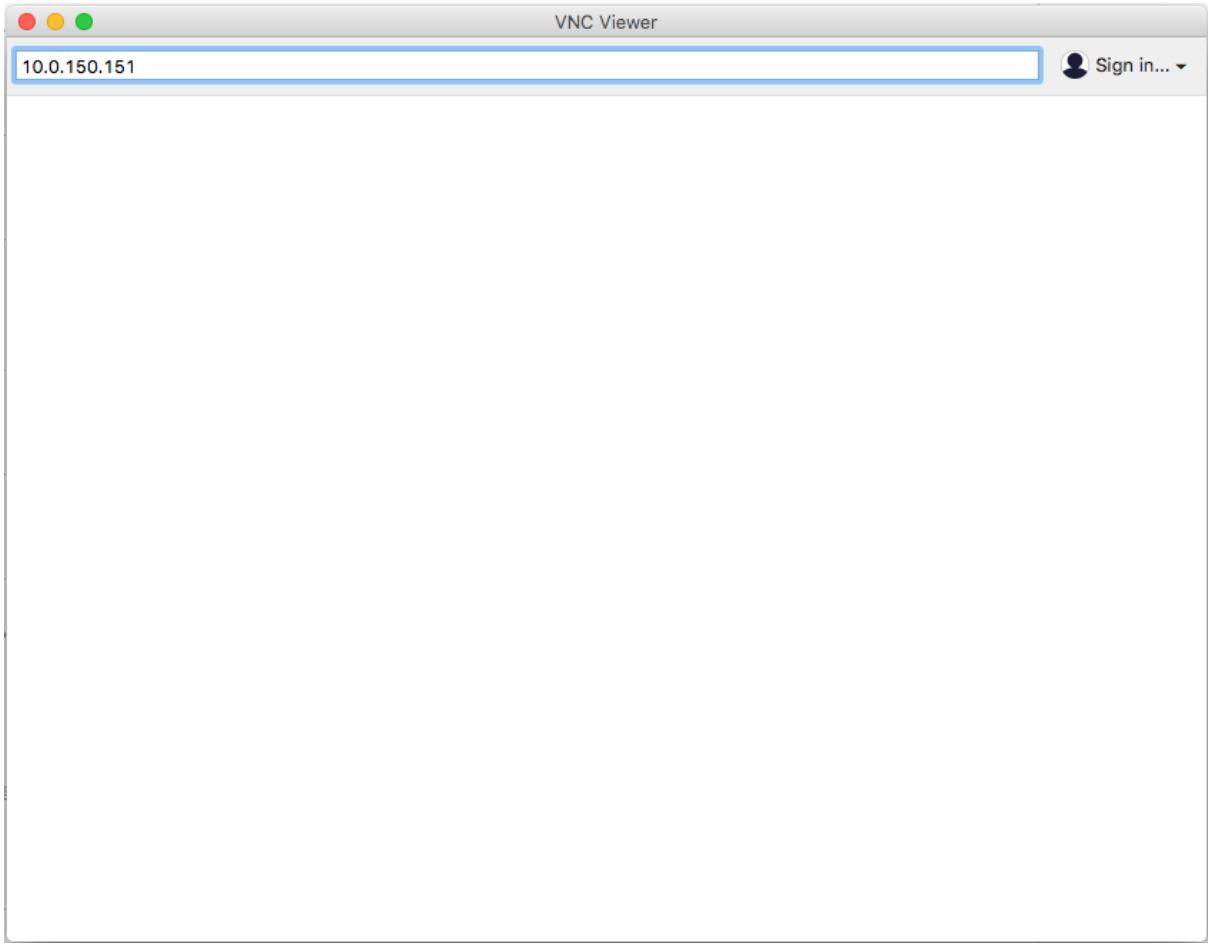


Tematy pokrewne:

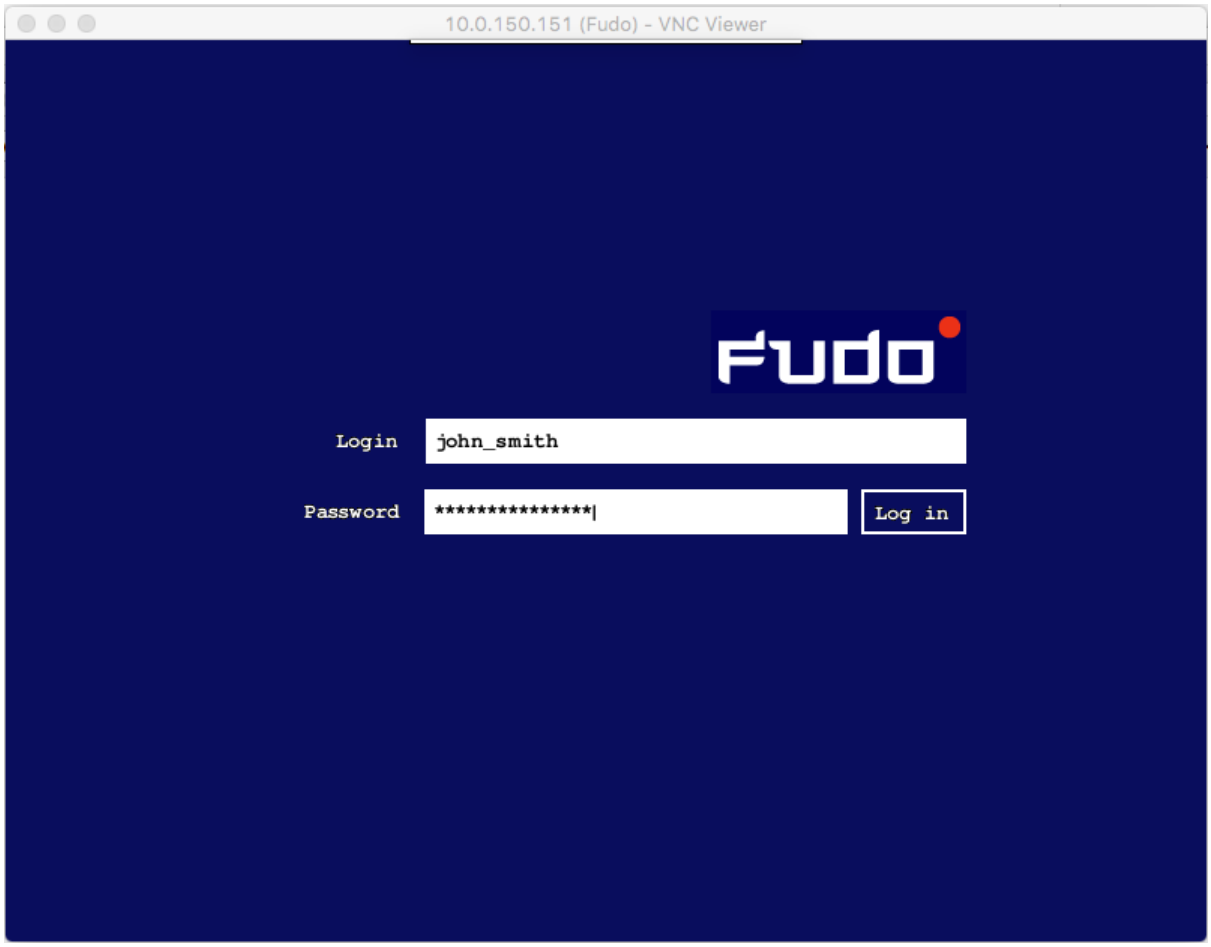
- *RDP*

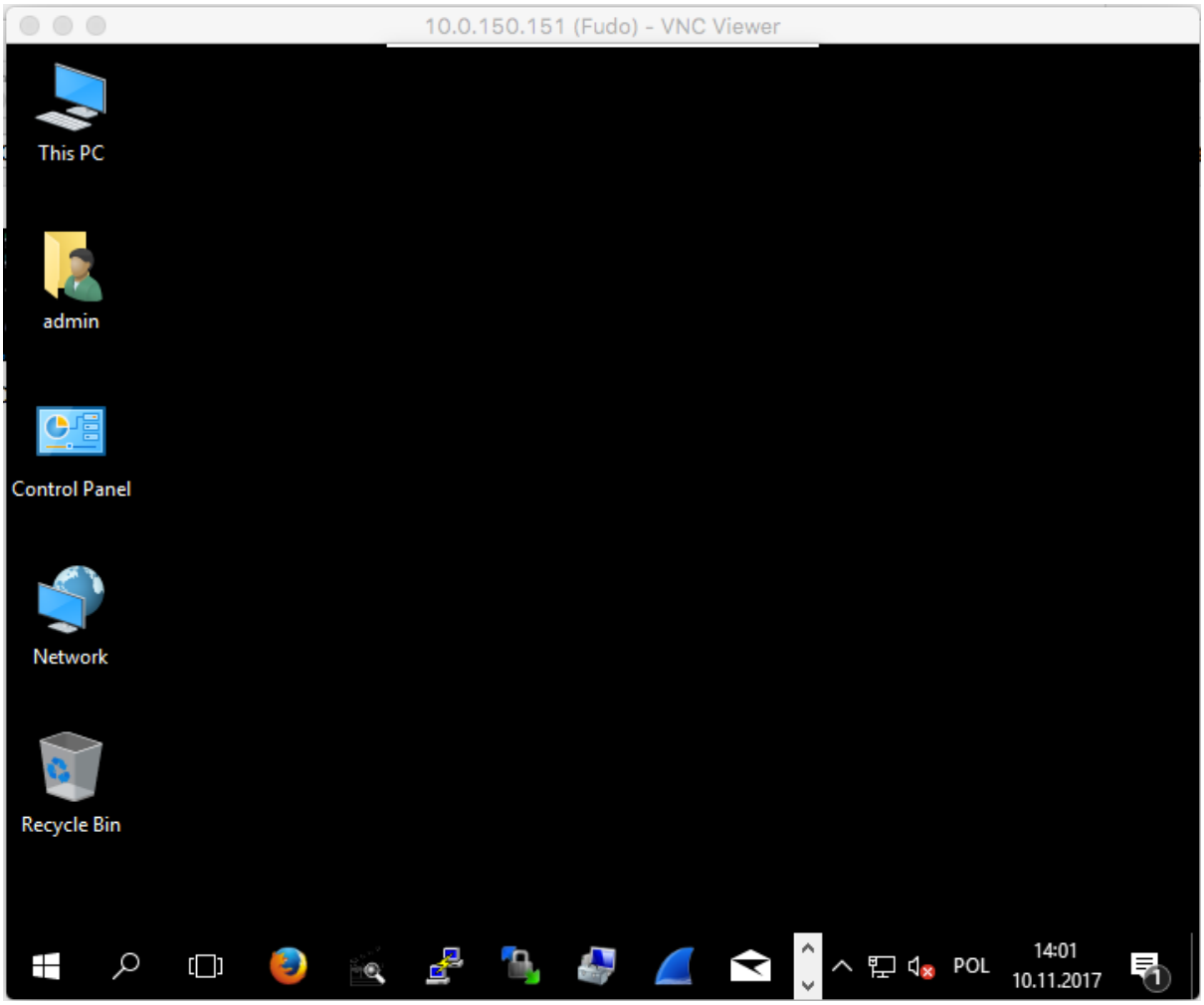
25.3 VNC Viewer

1. Uruchom aplikację kliencką *VNC Viewer* i w polu adresu wprowadź `10.0.150.151`.



2. Wprowadź nazwę użytkownika, hasło i zatwierdź klawiszem enter.


10.0.150.151 (Fudo) - VNC Viewer
Login
john_smith
Password
Log in

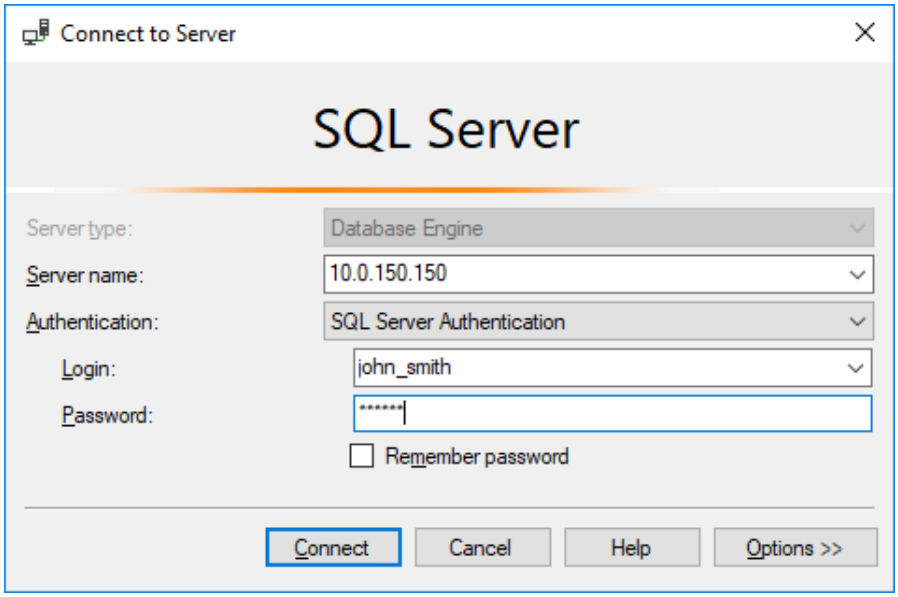


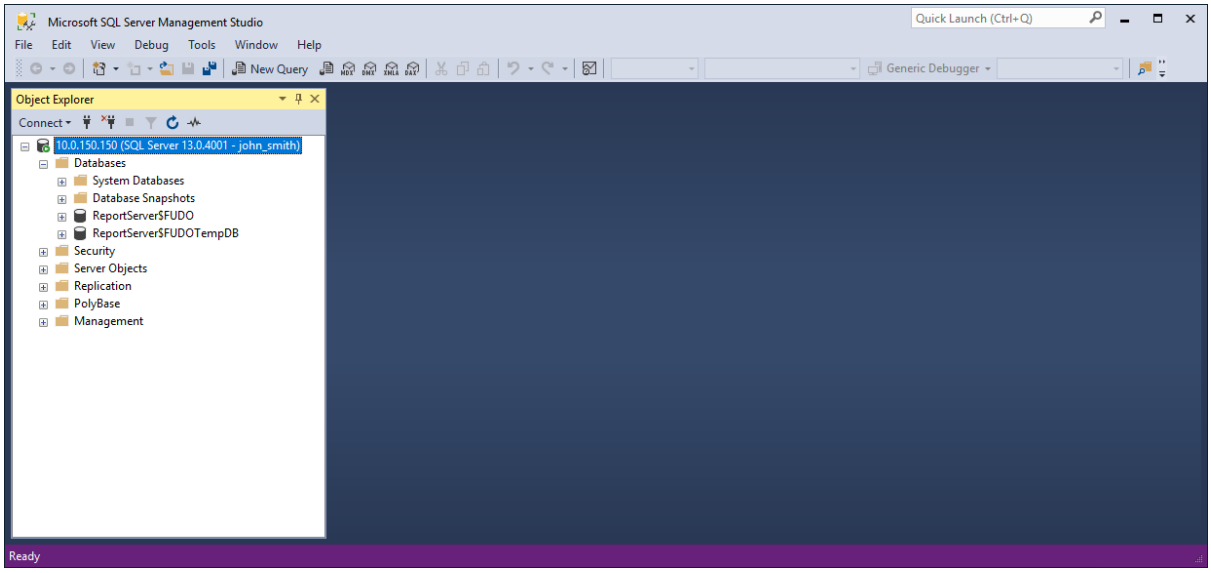
Tematy pokrewne:

- *Szybki start*

25.4 SQL Server Management Studio

1. Uruchom *SQL Server Management Studio*.
2. Wprowadź wcześniej skonfigurowany adres proxy, na którym Fudo oczekuje na połączenia z serwerem MS SQL (10.0.150.150).
3. Z listy rozwijalnej *Authentication*, wybierz *SQL Server Authentication*.
4. Wprowadź nazwę użytkownika oraz hasło.
5. Kliknij *Connect*.





Tematy pokrewne:

- *MS SQL*

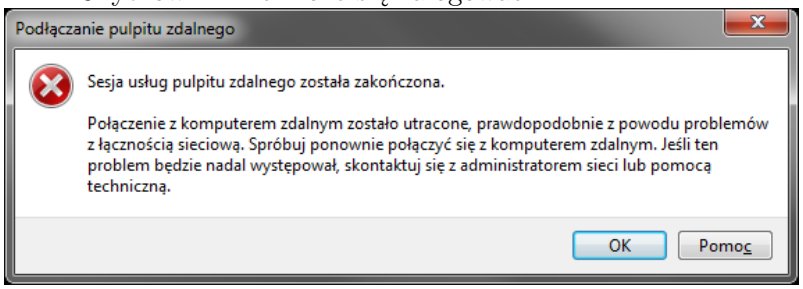
ROZDZIAŁ 26

Rozwiązywanie problemów

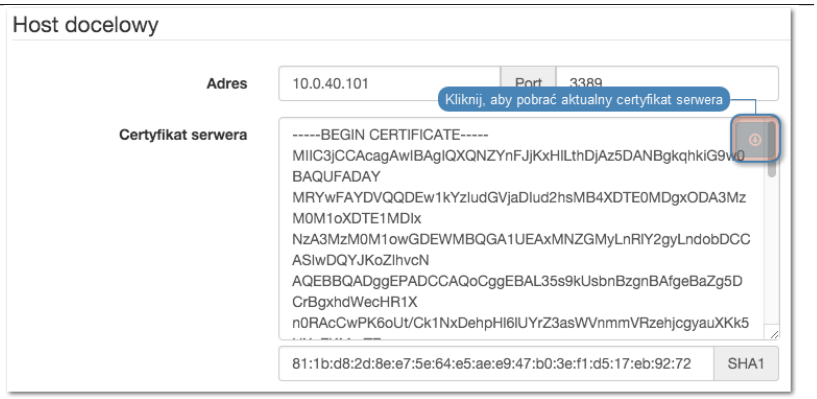
26.1 Uruchamianie Fudo PAM

Problem	Objawy i opis rozwiązania
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.

26.2 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 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. • Sprawdź czy użytkownik ma zdefiniowaną domenę i upewnij się, że podaje ją przy próbie logowania. • Fudo PAM nie jest w stanie prawidłowo obsłużyć przypadków, w których istnieją dwaj użytkownicy o tym samym loginie, z których jeden ma zdefiniowaną domenę taką samą jak *domena domyślna* a drugi nie ma określonej domeny. Sprawdź, czy nie istnieje inny użytkownik o tym samym loginie, ze zdefiniowaną domeną taką samą jak domena domyślna.
	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 Fudo PAM: 1. Zaloguj się do panelu administracyjnego Fudo PAM. 2. Wybierz *Ustawienia* > *System*, zakładka *Diagnostyka*. 3. Wprowadź adres serwera w sekcji *Ping* i wykonaj polecenie, żeby sprawdzić osiągalność hosta. • Sprawdź, czy serwer jest osiągalny pod wybranym numerem portu: 1. Zaloguj się do panelu administracyjnego Fudo PAM. 2. Wybierz *Ustawienia* > *System*, zakładka *Diagnostyka*. 3. w sekcji *Netcat*, wprowadź adres IP serwera wraz z numerem portu wybranej usługi i wykonaj polecenie.
	Objawy: Komunikat klienta: *Cannot establish new connection because the capacity of the filesystem has been reached.*

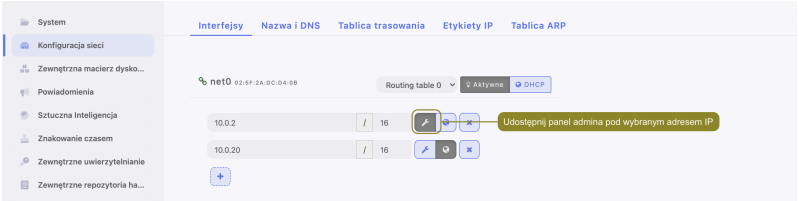
Problem	Objawy i opis rozwiązania
Przy próbie logowania nie wszyscy użytkownicy widzą ekran logowania Fudo PAM (standardowy, z szarym tłem).	**Przyczyna:** • Zapisane poświadczenia w skrócie RDP skutkują ukryciem ekranu Fudo PAM i bezpośrednim zalogowaniem do serwera docelowego. • Zapisane poświadczenia w skrócie RDP, użytkownik używa poświadczeń lokalnych na Fudo PAM tak więc przed Fudo PAM jest poprawnie uwierzytelniany i nie pokazuje mu się ekran logowania. Następnie gdy 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 Fudo PAM.

Problem	Objawy i opis rozwiązania
Połączenie jest zrywane	**Objawy:** • Użytkownik próbuje się połączyć z serwerem przez 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=8483885321111147010) is blocked.*
	Przyczyna: użytkownik jest zablokowany w 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 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 *sejfu*.

Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem Telnet5250 poprzez aplikację PC5250 w wersji 20091005 S oraz 20111019 S	**Objawy:** próba nawiązania połączenia kończy się niepowodzeniem.
	Przyczyna: w przypadku wymienionych wersji aplikacji klienckiej, konieczne jest skonfigurowanie ruchu TCP na portach 449, 8470 i 8476, celem poprawnego zestawienia połączenia.
	Rozwiązanie: • Dodaj serwer Telnet TN5250, z domyślnym numerem portu, tj. 23. • Dodaj trzy obiekty typu serwer o protokole *TCP* i numerach portów odpowiednio 449, 8470 i 8476. • Dodaj gniazdo nasłuchiwania *TN5250*, w trybie *Pośrednik*, z domyślnym numerem portu. • Dodaj trzy gniazda nasłuchiwania *TCP*, w trybie *Pośrednik*, z numerami portów odpowiednio 449, 8470 i 8476. • Dodaj konto typu *regular*, określ parametry uwierzytelnienia i przypisz do głównej definicji serwera TN5250. • Dodaj trzy konta typu *anonymous* przypisując do kolejnych serwerów pomocniczych. • Dodaj sejf i przypisz konta wraz z odpowiadającymi gniazdami nasłuchiwania.

26.3 Logowanie do panelu administracyjnego

Problem	Objawi i opis rozwiązania
Nie można zalogować się do panelu administracyjnego	• Zweryfikuj czy wprowadzony adres Fudo PAM jest poprawny. • Ustaw adres IP Fudo PAM z poziomu konsoli, postępując zgodnie z instrukcją w rozdziale *Konfiguracja interfejsów sieciowych* w dokumentacji systemu Fudo PAM. • Upewnij się, że adres IP ma włączoną funkcję zarządzania Fudo PAM. 

26.4 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.

26.5 Konfiguracja klastrowa

Problem	Objawy i opis rozwiązania
Obiekty nie replikują się na drugi węzeł	**Objawy:** Obiekty utworzone na jednym węźle, nie pojawiają się automatycznie na pozostałych węzłach klastra. **Rozwiązanie:** Skontaktuj się z działem wspracia technicznego.

26.6 Znakowanie czasem

Problem	Objawy i opis rozwiązania
Sesje nie są znakowane znacznikiem czasu	**Objawy:** • Komunikat w dzienniku zdarzeń: *Timestamping service communication error.*
	Przyczyna: brak komunikacji z serwerem usługi znakowania czasem.
	Rozwiązanie: Upewnij się, że serwer usługi znakowania czasem jest osiągalny przez system Fudo. • adres IP serwera znakowania czasem PWPW: 193.178.164.5 • adres serwera znakowania czasem KIR: http://www.ts.kir.com.pl/HttpTspServer
	Objawy: • Komunikat w dzienniku zdarzeń: *Unable to timestamp session.* • Brak ikony przy wybranej sesji.
	Przyczyna: Problem z funkcjonowaniem usługi znakowania czasem.
	Rozwiązanie: Zweryfikuj poprawność *konfiguracji usługi znakowania czasem*.

26.7 Tryb serwisowy

Tryb serwisowy umożliwia diagnozowanie Fudo PAM w przypadku gdy system nie uruchamia się poprawnie.

Włączenie trybu serwisowego

1. Uzyskaj dostęp do terminala systemowego.
2. Podczas uruchamiania Fudo, wprowadź `1` i zatwierdź klawiszem *Enter*.

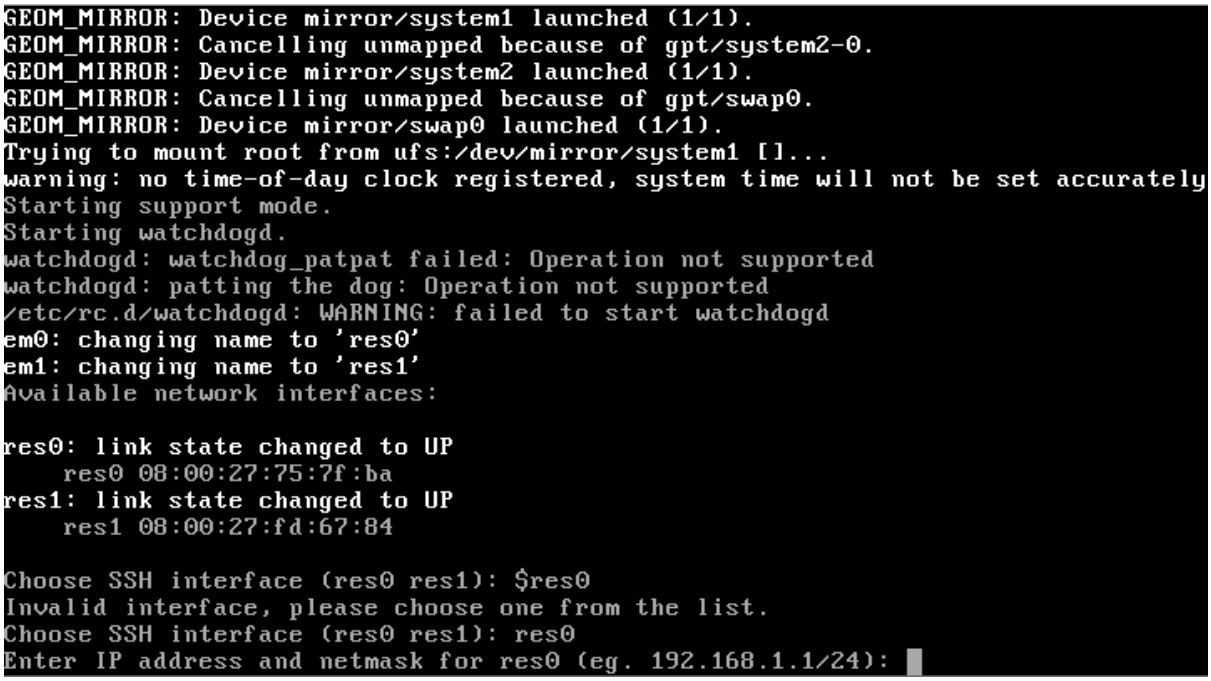
3. Wprowadź nazwę interfejsu sieciowego.

Informacja: W trybie serwisowym, nazwy interfejsów sieciowych przyjmują nazwę `res*`.

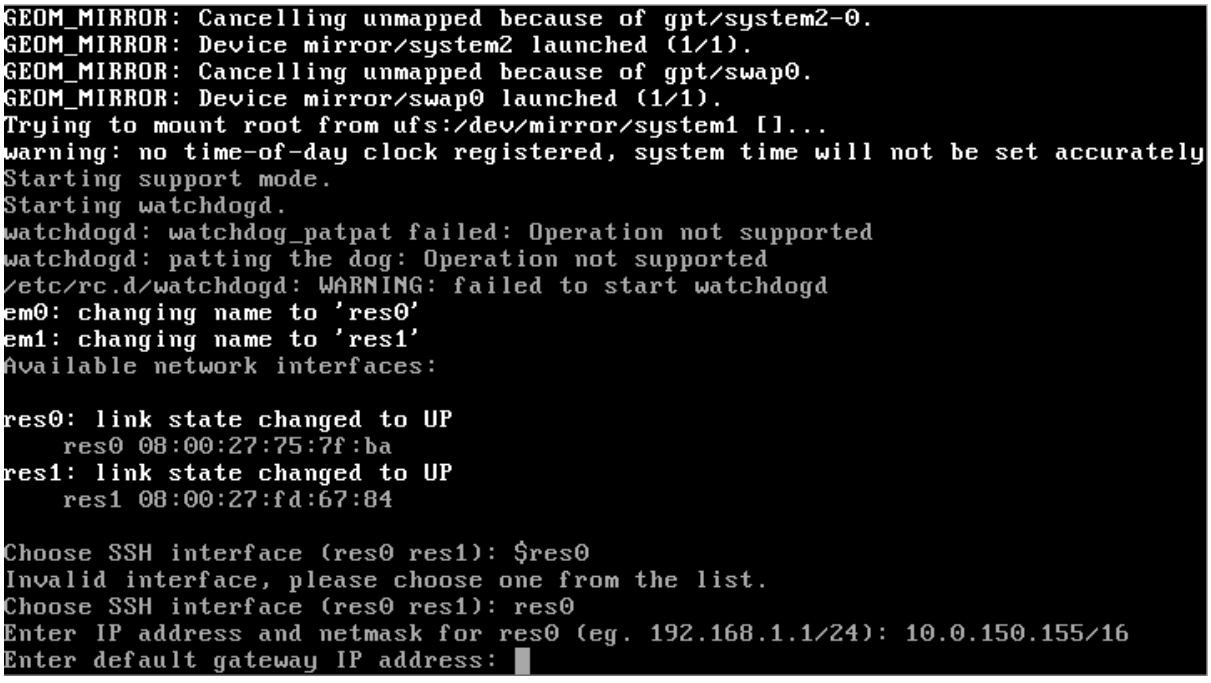
```
GEOM_MIRROR: Cancelling unmapped because of gpt/system0-0.
GEOM_MIRROR: Device mirror/system0 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system1-0.
GEOM_MIRROR: Device mirror/system1 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device mirror/system2 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/swap0.
GEOM_MIRROR: Device mirror/swap0 launched (1/1).
Trying to mount root from ufs:/dev/mirror/system1 []...
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $
```

4. Wprowadź adres IP wraz z maską podsieci, np. `10.0.0.8/16`.

Informacja: Adres IP służy do nawiązania zdalnego połączenia SSH z Fudo PAM i musi być osiągalny przez inżyniera wsparcia technicznego. W miarę możliwości, interfejs należy zaadresować tak samo jak przed wystąpieniem awarii.



5. Wprowadź adres IP bramy i zatwierdź klawiszem `[Enter]`, aby umożliwić nawiązanie zdalnego połączenia z Fudo PAM.



Informacja:

- Odcisk palca pozwala na weryfikację, że połączenie zostało nawiązane z właściwym systemem.

```
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address: 10.0.0.1
res0: link state changed to DOWN
add net default: gateway 10.0.0.1
SSH Fingerprint: SHA256:dgu2Ec8deFWPZkIxJk6EV9loggwm+OKXERsW+2PQBSY
res0: link state changed to UP
```

6. Po zakończeniu prac serwisowych, użyj kombinacji klawiszy `[Ctrl]` + `C`, aby zerwać połączenie i zresetować interfejs sieciowy.

```
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address: 10.0.0.1
res0: link state changed to DOWN
add net default: gateway 10.0.0.1
SSH Fingerprint: SHA256:dgu2Ec8deFWPZkIxJk6EV9loggwm+OKXERsW+2PQBSY
res0: link state changed to UP
^CDec 21 13:31:56 init: single user shell terminated, restarting
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
ifconfig: ioctl SIOCSIFNAME (set name): File exists
ifconfig: ioctl SIOCSIFNAME (set name): File exists
Available network interfaces:

    res0 08:00:27:75:7f:ba
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1):
```

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*
- *Czynności serwisowe*

ROZDZIAŁ 27

Często zadawane pytania

1. Jaka jest maksymalna ilość nagranych sesji na Fudo PAM dostępna z poziomu systemu?

2. W jaki sposób 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 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 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?

12. Co należy zrobić przed zdaniem maszyny demonstracyjnej?

Przetwarzanie sesji - uczenie maszynowe

13. Ile czasu zajmuje wytrenowanie modeli? Ile sesji muszę nagrać, aby zobaczyć wyniki?

14. Mamy 20 kont i 20 użytkowników w firmie - ile czasu zajmie zauważenie różnic w zachowaniu użytkowników?

15. Jeśli łączę się do różnych serwerów, czy Fudo tworzy osobny model dla każdego z nich?

16. Jeśli przekażę swoje dane logowania innej osobie, czy sztuczna inteligencja stwierdzi, że zalogował się ktoś inny i przerwie połączenie?

17. Ikonka statusu sesji jest stale żółta - co to oznacza?

18. Pięciu użytkowników korzysta z tego samego konta do nawiązywania połączeń - czy system będzie w stanie stwierdzić kto i kiedy łączył się z serwerem?

19. W jaki sposób system będzie w stanie stwierdzić, że to ktoś inny zalogował się do systemu, skoro wszyscy wykonujemy te same komendy?

20. Dlaczego moje sesje nie są analizowane?

1. Jaka jest maksymalna ilość nagranych sesji na Fudo PAM dostępna z poziomu systemu?

Urządzenia serii F1000 dysponują 24 TB przestrzeni dyskowej (15,9 TB przestrzeni użytkowej), a serii F3000 mają do dyspozycji macierz wewnętrzną o pojemności 96 TB (59,5 TB przestrzeni użytkowej) przeznaczoną do przechowywania danych sesji.

Rozmiar sesji determinowany jest aktywnością użytkownika. Średnie wartości dla jednej godziny zarejestrowanego połączenia wynoszą:

RDP	218 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	41,5 MB aktywnej sesji.

Przy takich założeniach, wewnętrzna przestrzeń dyskowa pozwala na zarejestrowanie:

	RDP	SSH
F1000	28,6 lat	150,2 lat
F3000	112,8 lat	592,5 lat

Informacja:

- Informacja o zajętości przestrzeni dyskowej bierze pod uwagę obszar zarezerwowany przez mechanizm redundancji danych. Stąd wynika raportowana zajętość macierzy dyskowej po zainicjowaniu systemu.
- 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 Fudo PAM obsługuje archiwizację sesji?

Wszystkie sesje archiwizowane są na wewnętrznej macierzy dyskowej urządzenia, przeznaczonej na rejestrowanie zdalnych połączeń. Fudo PAM wspiera zewnętrzne macierze a także umożliwia eksport 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 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 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 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*.

12. Co należy zrobić przed zdaniem maszyny demonstracyjnej?

Przed zdaniem maszyny demonstracyjnej należy usunąć dane oraz konfigurację poprzez *przywrócenie ustawień fabrycznych* oraz wyczyścić nośnik z kluczem szyfrującym.

13. Ile czasu zajmuje wytrenowanie modeli? Ile sesji muszę nagrać, aby zobaczyć wyniki?

Modele są trenowane zgodnie z ustawieniami terminarza w konfiguracji *Sztucznej inteligencji*.

- W przypadku modelu SSH, wytrenowanie modelu wymaga minimum 65 sesji (każda musi zawierać co najmniej 25 unikatowych komend) oraz 5 unikatowych predyktorów (np. użytkowników). Uzyskanie optymalnych wyników wymaga 300 sesji dla każdego predyktora i 10 unikatowych predyktorów.
- Dla modelu RDP, minimum konieczne do wytrenowania modelu, to 5 godzin nagrań dla pojedynczego predyktora. Optymalne wyniki uzyskuje się przy 30 godzinach nagrań i 10 unikatowych predyktorach.

14. Mamy 20 kont i 20 użytkowników w firmie - ile czasu zajmie zauważenie różnic w zachowaniu użytkowników?

Czas jest ściśle uzależniony od dostępności zarejestrowanych sesji. Jeśli jest wystarczająca ilość danych do zbudowania modelu, system będzie w stanie wykryć zmiany w zachowaniu użytkowników w jeden dzień po nagraniu pierwszej sesji dla danego predyktora (użytkownika).

- W przypadku modelu SSH, wytrenowanie modelu wymaga minimum 65 sesji (każda musi zawierać co najmniej 25 unikatowych komend) oraz 5 unikatowych predyktorów (np. użytkowników). Uzyskanie optymalnych wyników wymaga 300 sesji dla każdego predyktora i 10 unikatowych predyktorów.
- Dla modelu RDP, minimum konieczne do wytrenowania modelu, to 5 godzin nagrań dla pojedynczego predyktora. Opymalne wyniki uzyskuje się przy 30 godzinach nagrań i 10 unikatowych predyktorach.

15. Jeśli łączę się do różnych serwerów, czy Fudo tworzy osobny model dla każdego z nich?

Fudo PAM tworzy i utrzymuje jeden model RDP oraz jeden model SSH dla pojedynczego użytkownika.

16. Jeśli przekażę swoje dane logowania innej osobie, czy sztuczna inteligencja stwierdzi, że zalogował się ktoś inny i przerwie połączenie?

Fudo PAM będzie w stanie wykryć taki przypadek i odpowiednio ustawić poziom zagrożenia sesji, ale nie przerwie automatycznie połączenia.

17. Ikonka statusu sesji jest stale żółta - co to oznacza?

Żółty kolor oznacza, że model nie był w stanie jednoznacznie ustalić poziom zagrożenia dla sesji. W sytuacji, gdy nie mamy podejrzenia, że doszło do nieuprawnionego dostępu, te sesje można uznać za prawidłowe. Jeśli jednak doszło do nadużycia uprawnień, sesje te należy poddać audytowi.

18. Pięciu użytkowników korzysta z tego samego konta do nawiązywania połączeń - czy system będzie w stanie stwierdzić kto i kiedy łączył się z serwerem?

Użytkownicy muszą mieć indywidualne konta na Fudo PAM, aby system był w stanie zidentyfikować zagrożone sesje.

19. W jaki sposób system będzie w stanie stwierdzić, że to ktoś inny zalogował się do systemu, skoro wszyscy wykonujemy te same komendy?

Każdy użytkownik wykonuje te same komendy w odmienny sposób. Np. jeden użytkownik wykona `ls -la` a drugi `ls -al`. Kombinacja takich niewielkich różnic pozwala stwierdzić zgodność zachowania użytkownika z wytrenowanym dla niego modelem.

20. Dlaczego moje sesje nie są analizowane?

Aby sesja została poddana analizie, musi istnieć odpowiadający jej model. Ponadto, sesja musi spełniać pewne wymagania ilościowe: musi być dostatecznie długa i zawierać minimalną ilość informacji. Więcej informacji na ten temat znajdziesz w rozdziale *Przetwarzanie sesji - uczenie maszynowe*.

ROZDZIAŁ 28

Słownik pojęć

AAPM Moduł AAPM (Application to Application Password Manager) umożliwiający bezpieczną wymianę haseł pomiędzy aplikacjami.

Active Directory Usługa uwierzytelniania i autoryzacji użytkowników w domenie Windows.

AD Active Directory - usługa uwierzytelnienia i autoryzacji użytkowników w domenie Windows.

ARP Address Resolution Protocol - protokół mapujący adresy warstwy trzeciej (adresy IP) na fizyczne adresy warstwy łącza danych (adresy MAC).

Azure Microsoft Azure - platforma chmurowa firmy Microsoft, udostępniająca mechanizmy pozwalające przetwarzać oraz składować dane.

broker połączeń RDP Mechanizm zarządzania sesjami dostępowymi do maszyn będących częścią farmy serwerów.

CERB Kompleksowe rozwiązanie uwierzytelniania i autoryzacji użytkowników, wspierające metody uwierzytelniania tj. token mobilny (aplikacja na telefon komórkowy), hasło statyczne, hasła jednorazowe SMS.

certyfikat CA Certyfikat urzędu certyfikacji.

DHCP Mechanizm dynamicznego zarządzania adresacją w sieciach LAN.

DNS Domain Name Server - serwer nazw, tłumaczy mnemoniczne nazwy hostów na adresy IP.

DoS (Denial of Service) Próba ataku na system polegająca na wysłaniu znacznej ilości zapytań do serwera, tak aby zaprzestał przetwarzać kolejne żądania użytkowników.

dostęp SSH Dostęp serwisowy do Fudo PAM poprzez protokół SSH.

DUO jest aplikacją mobilną, która działa na podstawie dwuetapowej autoryzacji Duo Security. Aplikacja generuje kod dostępu do logowania oraz umożliwia wysłanie notyfikacji typu push w celu uwierzytelniania.

Efficiency Analyzer/Productivity Analyzer Moduł analizy produktywności dostarczający danych statystycznych na temat aktywności użytkowników.

fudopv Skrypt modułu AAPM, rezydujący na serwerze, umożliwiający wymianę haseł pomiędzy aplikacjami.

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

grupa redundancji Zdefiniowana grupa adresów IP, które w przypadku awarii jednego z węzłów, zostaną przypisane do drugiego serwera, dla zachowania ciągłości świadczenia usług.

Hasło statyczne Podstawowa metoda uwierzytelniania użytkowników, w której do potwierdzenia tożsamości używana jest kombinacja ciągów znakowych w postaci loginu i hasła.

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.

hot-swap Mechanizm umożliwiający wymianę komponentu bez wyłączania urządzenia.

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).

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.

LDAP Lightweight Directory Access Protocol - protokół dostępu i zarządzania rozproszonymi usługami katalogowymi w sieciach IP.

modyfikator haseł Narzędzie służące do zmiany hasła do konta na monitorowanym serwerze.

notacja CIDR Skrócona notacja adresów sieciowych, w której adres IP zapisywany jest zgodnie z notacją IPv4, a maska podawana jest w postaci liczby wiodących cyfr «1» w zapisie bitowym (192.168.1.1 - 255.255.255.0; 192.168.1.1/24).

OATH Open Authentication - otwarty standard bezpiecznego, dwuskładnikowego uwierzytlenienia użytkowników i urządzeń.

OCR Optical Character Recognition - przetwarzanie obrazów pod kątem identyfikacji i indeksacji tekstów.

Odcisk Palca Fingerprint - ciąg znaków będący działaniem funkcji skrótu na danych wejściowych, pozwalający jednoznacznie stwierdzić, czy dane nie zostały zmienione.

Okta Okta - to narzędzie klasy enterprise do zarządzania dostępami oraz tożsamościami cyfrowymi pracowników.

polityka Mechanizm pozwalający definiować wzorce i automatyczne akcje, które podejmie system w przypadku wykrycia danego wzorca.

polityka czasowa Mechanizm definiowania przedziałów czasu, w których użytkownicy mają dostęp do serwerów.

PSM (Privileged Session Management) Moduł Fudo PAM służący rejestracji zdalnych sesji dostępowych.

RADIUS Remote Authentication Dial In User Service - protokół sieciowy służący regulowaniu dostępu do określonych usług udostępnianych w sieci informatycznej.

RDP Remote Desktop Protocol - protokół zdalnego dostępu do graficznych interfejsów użytkownika w systemach operacyjnych firmy Microsoft.

repozytorium haseł Repozytorium haseł zarządza hasłami do serwerów docelowych, w dostępie do których, pośredniczy Fudo PAM.

retencja Retencja danych to mechanizm, który usuwa dane sesji po upływie zdefiniowanego czasu.

SMS jest usługą przesyłania wiadomości tekstowych w cyfrowych urządzeniach mobilnych.

SSH Secure Shell - protokół sieciowy do bezpiecznej komunikacji ze zdalnymi urządzeniami.

serwer dynamiczny Serwer dodawany automatycznie z chwilą nawiązywania połączenia, jeśli wcześniej zdefiniowany został obiekt opisujący zbiór serwerów w formie podsieci.

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

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.

serwer

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

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.

użytkownik Użytkownik definiuje podmiot uprawniony do nawiązywania połączeń z monitorowanymi serwerami. Szczegółowa definicja obiektu (unikatowa kombinacja loginu i domeny, pełna nazwa, adres email) pozwalają na jednoznaczne wskazanie osoby odpowiedzialnej za działania, w przypadku współdzielenia konta uprzywilejowanego.

VLAN Mechanizm sieci wirtualnych, umożliwiający separację domen rozgłoszeniowych.

VNC Protokół graficznego dostępu do zdalnych zasobów komputerowych.

WWN World Wide Name - unikatowy identyfikator obiektów w rozwiązaniach macierzy dyskowych.

zewnętrzny serwer uwierzytelnienia Serwer przechowujący dane użytkowników, używany do weryfikacji tożsamości w procesie logowania do Fudo PAM lub nawiązywania połączenia z serwerami docelowymi.

znacznik czasu Znacznik będący skrótem danych, pozwalający zweryfikować czy dane nie zostały zmienione.

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

V

W

X

Z