



Fudo Enterprise 5.4 - Dokumentacja Systemu

Fudo Security

29.04.2024

1	O dokumentacji	1
2	Motywy kolorystyczne Panelu Administracyjnego	4
3	Wstęp	6
3.1	Opis systemu	6
3.2	Wspierane protokoły	8
3.2.1	HTTP	8
3.2.2	Modbus	9
3.2.3	MS SQL (TDS)	9
3.2.4	MySQL	10
3.2.5	RDP	10
3.2.6	SSH	14
3.2.7	Telnet 3270	18
3.2.8	Telnet 5250	18
3.2.9	Telnet	19
3.2.10	VNC	19
3.2.11	X11	20
3.2.12	TCP	21
3.2.13	Pobranie hasła	21
3.3	Scenariusze wdrożenia	22
3.4	Tryby połączenia	23
3.5	Metody i tryby uwierzytelniania użytkowników	26
3.6	Mechanizmy bezpieczeństwa	29
3.6.1	Szyfrowanie danych	29
3.6.2	Kopie zapasowe	29
3.6.3	Uprawnienia użytkowników	30
3.6.4	Sandboxing	30
3.6.5	Niezawodność	30
3.6.6	Konfiguracja klastrowa	30
3.7	Model danych	31
3.8	Dashboard	32
3.8.1	Widgety	33
3.8.2	Zarządzanie widgetami	34
3.8.3	Status dysków	34
3.9	Portal użytkownika	35

3.10	Licencje produktów stron trzecich	36
4	Instalacja i pierwsze uruchomienie	37
4.1	Wymagania	37
4.2	Urządzenie	38
4.3	Pierwsze uruchomienie	40
4.3.1	Środowisko wirtualne	45
5	Szybki start	51
5.1	SSH	51
5.1.1	Założenia	51
5.1.2	Konfiguracja	51
5.1.3	Nawiązanie połączenia	56
5.1.4	Podgląd sesji połączeniowej	57
5.2	SSH w trybie bastionu	57
5.2.1	Założenia	58
5.2.2	Konfiguracja	58
5.2.3	Nawiązanie połączenia	62
5.2.4	Podgląd sesji połączeniowej	64
5.3	RDP	65
5.3.1	Założenia	65
5.3.2	Konfiguracja	65
5.3.3	Nawiązanie połączenia	70
5.3.4	Podgląd sesji połączeniowej	72
5.4	RDP w trybie bastionu	73
5.4.1	Założenia	74
5.4.2	Konfiguracja	74
5.4.3	Nawiązanie połączenia	79
5.4.4	Podgląd sesji połączeniowej	81
5.5	Telnet	82
5.5.1	Założenia	83
5.5.2	Konfiguracja	83
5.5.3	Nawiązanie połączenia	86
5.5.4	Podgląd sesji połączeniowej	87
5.6	Telnet 5250	87
5.6.1	Założenia	88
5.6.2	Konfiguracja	88
5.6.3	Nawiązanie połączenia	92
5.6.4	Podgląd sesji połączeniowej	94
5.7	MySQL	95
5.7.1	Założenia	96
5.7.2	Konfiguracja	96
5.7.3	Nawiązanie połączenia	99
5.7.4	Podgląd sesji połączeniowej	100
5.8	MS SQL	101
5.8.1	Założenia	102
5.8.2	Konfiguracja	103
5.8.3	Nawiązanie połączenia	106
5.8.4	Podgląd sesji połączeniowej	107
5.9	HTTP	108
5.9.1	Założenia	109
5.9.2	Konfiguracja	109

5.9.3	Nawiązanie połączenia	114
5.9.4	Podgląd sesji połączeniowej	115
5.10	VNC	116
5.10.1	Założenia	117
5.10.2	Konfiguracja	117
5.10.3	Nawiązanie połączenia	121
5.10.4	Podgląd sesji połączeniowej	121
5.11	Uwierzytelnienie użytkowników w katalogu LDAP	122
5.11.1	Założenia	122
5.11.2	Konfiguracja	122
6	Użytkownicy	125
6.1	Dodawanie użytkownika	126
6.2	Kopiowanie uprawnień użytkownika	134
6.3	Modyfikowanie użytkownika	135
6.4	Blokowanie użytkownika	136
6.5	Odblokowanie użytkownika	138
6.6	Usuwanie użytkownika	139
6.7	Zliczanie niepowodzeń uwierzytelnienia	140
6.8	Role użytkownika	141
6.9	Synchronizacja użytkowników z LDAP	143
7	Serwery	149
7.1	Dodawanie serwera	149
7.1.1	Dodawanie serwera HTTP	149
7.1.2	Dodawanie serwera Modbus	151
7.1.3	Dodawanie serwera MS SQL	152
7.1.4	Dodawanie serwera MySQL	154
7.1.5	Dodawanie serwera RDP	155
7.1.6	Dodawanie serwera SSH	156
7.1.7	Dodawanie serwera Telnet	158
7.1.8	Dodawanie serwera Telnet 3270	159
7.1.9	Dodawanie serwera Telnet 5250	161
7.1.10	Dodawanie serwera VNC	162
7.1.11	Dodawanie serwera TCP	163
7.2	Importowanie listy serwerów z pliku CSV	164
7.3	Modyfikowanie serwera	166
7.4	Blokowanie serwera	166
7.5	Odblokowanie serwera	167
7.6	Usuwanie serwera	167
8	Pule	169
8.1	Dodawanie puli	169
8.2	Usuwanie puli	170
9	Zdalne aplikacje	171
9.1	Dodanie zdalnej aplikacji	171
9.2	Połączenie do zdalnej aplikacji przez Portal Użytkownika	172
9.3	Usuwanie zdalnej aplikacji	172
10	Konta	173
10.1	Dodawanie konta	173

10.1.1	Dodawanie konta typu <i>anonymous</i>	173
10.1.2	Dodawanie konta typu <i>forward</i>	175
10.1.3	Dodawanie konta typu <i>regular</i>	178
10.2	Edytowanie konta	183
10.3	Blokowanie konta	183
10.4	Odblokowanie konta	184
10.5	Usuwanie konta	185
10.6	Zarządzanie ostrzeżeniami bezpieczeństwa	185
10.6.1	Zmiana hasła konta	185
10.6.2	Zignorowanie ostrzeżenia	187
11	Gniazda nasłuchiwania	188
11.1	Dodawanie gniazda nasłuchiwania	188
11.1.1	Konfigurowanie gniazda nasłuchiwania SSH	190
11.1.2	Konfigurowanie gniazda nasłuchiwania RDP	193
11.1.3	Konfigurowanie gniazda nasłuchiwania VNC	197
11.1.4	Konfigurowanie gniazda nasłuchiwania HTTP	200
11.1.5	Konfigurowanie gniazda nasłuchiwania Modbus	205
11.1.6	Konfigurowanie gniazda nasłuchiwania MySQL	207
11.1.7	Konfigurowanie gniazda nasłuchiwania TCP	209
11.1.8	Konfigurowanie gniazda nasłuchiwania MS SQL	211
11.1.9	Konfigurowanie gniazda nasłuchiwania Telnet	213
11.1.10	Konfigurowanie gniazda nasłuchiwania Telnet 3270	216
11.1.11	Konfigurowanie gniazda nasłuchiwania Telnet 5250	219
11.2	Modyfikowanie gniazda nasłuchiwania	221
11.3	Blokowanie gniazda nasłuchiwania	222
11.4	Odblokowanie gniazda nasłuchiwania	223
11.5	Usuwanie gniazda nasłuchiwania	224
12	Sejfy	226
12.1	Dodawanie sejfu	227
12.2	Modyfikowanie sejfu	230
12.3	Blokowanie sejfu	230
12.4	Odblokowanie sejfu	231
12.5	Usuwanie sejfu	232
13	Żądania dostępu	234
13.1	Żądania oczekujące	236
13.2	Żądania aktywne	237
13.3	Archiwum żądań	237
14	Wykrywanie (Discovery)	239
14.1	Tworzenie reguły	240
14.1.1	Tworzenie reguły dla kont	240
14.1.2	Tworzenie reguły dla serwerów	241
14.2	Zarządzanie regułami	242
14.3	Tworzenie skanera	243
14.3.1	Tworzenie skanera dla kont kontrolera domeny	243
14.3.2	Tworzenie skanera dla serwerów kontrolera domeny	245
14.3.3	Tworzenie skanera dla kont lokalnych	247
14.4	Zarządzanie skanerami	248
14.5	Zarządzanie wykrytymi kontami	249

14.6	Zarządzanie wykrytymi serwerami	250
15	Modyfikatory haseł	252
15.1	Polityki haseł	252
15.1.1	Dodawanie polityki zmiany haseł	252
15.1.2	Edytowanie polityki zmiany haseł	253
15.1.3	Usuwanie polityki zmiany haseł	253
15.2	Uniwersalne modyfikatory haseł	254
15.2.1	Definiowanie modyfikatora haseł	254
15.2.2	Edytowanie uniwersalnego modyfikatora haseł	257
15.2.3	Usuwanie modyfikatora haseł	258
15.3	Tryby połączenia	258
15.3.1	SSH	258
15.3.2	LDAP	259
15.3.3	Telnet	260
15.3.4	WinRM	261
15.4	Konfigurowanie modyfikatora haseł Unix poprzez SSH	262
16	Polityki	265
16.1	Definiowanie polityki na podstawie modułu AI	265
16.2	Definiowanie polityki na podstawie wzorca	269
17	Do pobrania	273
17.1	Sesje	273
17.2	Pliki	273
18	Aktywność konta w Portalu Użytkownika	276
19	Sesje	278
19.1	Filtrowanie sesji	280
19.1.1	Definiowanie filtrów	280
19.1.2	Zarządzanie definicjami filtrowania	281
19.1.3	Przeszukiwanie pełnotekstowe	281
19.2	Odtwarzanie sesji	282
19.3	Wstrzymywanie połączenia	288
19.4	Przerywanie połączenia	289
19.5	Dołączanie do sesji	290
19.6	Udostępnianie sesji	291
19.7	Komentowanie sesji	293
19.8	Zarządzanie retencją sesji	295
19.9	Eksportowanie sesji	296
19.9.1	Dostępne formaty plików eksportu sesji	298
19.10	Usuwanie sesji	299
19.11	Przetwarzanie OCR sesji	299
19.12	Replikacja sesji w konfiguracji klastrowej	301
19.13	Znakowanie czasem wybranych sesji	302
19.14	Anulowanie znakowania czasem	303
19.15	Akceptowanie żądań użytkowników	304
19.16	Odrzucanie żądań użytkowników	304
19.17	Przetwarzanie sesji - uczenie maszynowe	305
19.17.1	Model zawartości	305
19.17.2	Ocena sesji	306

19.17.3	Modele ilościowe	308
20	Raporty	309
20.1	Subskrybowanie raportu cyklicznego	310
20.2	Rezygnacja z subskrypcji raportu cyklicznego	311
20.3	Generowanie raportu na żądanie	311
20.4	Wyświetlanie i zapisywanie raportów	312
20.5	Usuwanie raportów	312
21	Produktywność	313
21.1	Zestawienie	313
21.2	Analiza sesji	314
21.3	Porównanie aktywności	315
22	Administracja	316
22.1	System	316
22.1.1	Data i czas	316
22.1.2	Certyfikaty HTTPS	318
22.1.3	Blokowanie nowych połączeń	319
22.1.4	Dostęp SSH	319
22.1.5	Funkcjonalności wrażliwe	320
22.1.6	Aktualizacja systemu	321
22.1.6.1	Aktualizowanie systemu	321
22.1.6.2	Przywrócenie poprzedniej wersji systemu	323
22.1.6.3	Usuwanie migawki aktualizacji	324
22.1.7	Licencja	325
22.1.8	Hotfix	325
22.1.9	Diagnostyka	326
22.1.10	Szyfrowanie konfiguracji	328
22.1.11	Domyślna domena	330
22.1.12	Złożoność haseł	332
22.1.13	Single Sign On	333
22.1.13.1	Konfiguracja Fudo Enterprise	333
22.1.13.2	Single Sign On do Panelu Administracyjnego	334
22.1.13.3	Single Sign On do Portalu Użytkownika	334
22.1.13.4	Konfiguracja kontrolera domeny	335
22.1.13.5	Konfiguracja stacji roboczej	335
22.1.14	Modyfikatory haseł - aktywny węzeł klastra	336
22.1.14.1	Manager haseł w klastrze	336
22.2	Konfiguracja sieci	337
22.2.1	Konfiguracja ustawień sieciowych	337
22.2.1.1	Zarządzanie interfejsami fizycznymi	338
22.2.1.2	Ustawianie adresu IP z konsoli	340
22.2.1.3	Konfigurowanie mostu sieciowego	343
22.2.1.4	Konfigurowanie sieci wirtualnych (VLAN)	344
22.2.1.5	Konfigurowanie agregacji połączeń LACP	345
22.2.2	Etykiety adresów IP	346
22.2.3	Konfiguracja tras routingu	347
22.2.4	Konfiguracja DNS	348
22.2.5	Konfiguracja tablicy ARP	349
22.3	Powiadomienia	350
22.4	Sztuczna inteligencja	353

22.4.1	Konfiguracja trenera modeli	354
22.4.2	Modele behawioralne	355
22.5	Znakowanie czasem	357
22.6	Model uwierzytelniania w oparciu o certyfikaty	358
22.7	Uwierzytelnienie	359
22.7.1	Widok zarządzania serwerami uwierzytelnienia	360
22.7.2	Definicja serwera zewnętrznego uwierzytelniania	360
22.7.3	Definicja uwierzytelniania OATH	362
22.7.4	Definicja uwierzytelniania SMS	362
22.7.5	Definicja uwierzytelniania DUO	363
22.7.6	Definicja uwierzytelniania OpenID Connect	364
22.8	Zewnętrzne repozytoria haseł	366
22.8.1	CyberArk Enterprise Password Vault	366
22.8.2	CyberArk Credential Provider	368
22.8.3	Thycotic Secret Server	370
22.8.4	Local Administrator Password Solutions (LAPS)	371
22.9	Zasoby	374
22.9.1	Konfiguracja ekranu logowania RDP/VNC	374
22.9.2	Ekran logowania <i>Portalu użytkownika</i>	376
22.10	Przywracanie poprzedniej wersji systemu	378
22.11	Ponowne uruchomienie systemu	379
22.12	SNMP	380
22.12.1	Odczytywanie informacji SNMP poprzez <code>snmpwalk</code>	382
22.12.2	Rozszerzenia SNMP Fudo Enterprise	382
22.13	Kopia zapasowa i retencja	383
22.13.1	Kopia zapasowa systemu	383
22.13.2	Retencja danych	385
22.14	Zewnętrzna macierz dyskowa	387
22.14.1	Konfigurowanie zewnętrznej macierzy dyskowej	387
22.14.2	Rozszerzanie zewnętrznej macierzy dyskowej	388
22.15	Eksportowanie/importowanie konfiguracji systemu	388
22.15.1	Eksportowanie konfiguracji	389
22.15.2	Importowanie konfiguracji	389
22.16	Konfiguracja klastrowa	390
22.16.1	Inicjowanie klastra	391
22.16.2	Zarządzanie węzłami klastra	392
22.16.2.1	Dodawanie węzłów klastra	392
22.16.2.2	Edytowanie węzłów klastra	396
22.16.2.3	Usuwanie węzłów klastra	396
22.16.3	Grupy redundancji	397
22.17	Dziennik zdarzeń	400
22.17.1	Zewnętrzne serwery syslog	400
22.17.2	Eksportowanie dziennika zdarzeń	402
22.18	Zmiana frazy szyfrującej	402
22.19	Integracja z serwerem CERB	404
22.20	Czynności serwisowe	410
22.20.1	Sporządzanie kopii zapasowej kluczy szyfrujących	411
22.20.2	Monitorowanie stanu systemu	414
22.20.3	Kontrola Stanu	415
22.20.3.1	API kontrola stanu	415
22.20.4	Call Home	416

22.20.5	Wymiana dysku macierzy	417
22.20.6	Przywracanie ustawień fabrycznych	418
23	Informacje uzupełniające	422
23.1	Broker połączeń RDP	422
23.2	Logowane komunikaty	423
23.3	Informacja ze stopki dolnej	436
24	Fudo Officer 1.0	438
24.1	Konfiguracja	438
24.2	Zarządzanie żadaniami sesji	439
24.3	Ustawienia	442
25	AAPM (Application to Application Password Manager)	443
25.1	Kompilowanie narzędzia <i>fudopv</i>	443
25.1.1	Python	444
25.1.2	Środowisko wirtualne	444
25.1.3	Pobranie zależności	445
25.1.4	Zbudowanie narzędzia <i>fudopv</i>	445
25.2	Wdrożenie <i>fudopv</i> bez kompilacji kodu źródłowego	446
25.3	Uruchamianie <i>fudopv</i>	446
25.4	Sposoby uwierzytelnienia	451
25.4.1	Hasło statyczne	452
26	Systemy zgłoszeń	453
27	Aplikacje klienckie	454
27.1	PuTTY	454
27.2	Microsoft Remote Desktop	456
27.3	TightVNC Viewer	458
27.4	SQL Server Management Studio	459
28	Rozwiązywanie problemów	460
28.1	Uruchamianie Fudo Enterprise	460
28.2	Połączenia z serwerami	460
28.3	Logowanie do panelu administracyjnego	465
28.4	Odtwarzanie sesji	466
28.5	Konfiguracja klastrowa	466
28.6	Znakowanie czasem	467
28.7	Tryb serwisowy	467
29	Przypadki użycia	471
29.1	Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator	471
29.1.1	Protokoły obsługujące OATH	471
29.1.2	Konfiguracja domyślnych wartości OATH	472
29.1.3	Konfiguracja metody OATH użytkownikowi	472
29.2	Konfiguracja uwierzytelnienia OpenID Connect w Azure	477
29.3	Konfiguracja usługi Remote Desktop Services na serwerze Windows dla Fudo Enterprise	484
29.3.1	Konfiguracja usługi Remote Desktop Services (RDS)	485
29.3.2	Konfiguracja Fudo Enterprise	496
29.4	Zarządzanie certyfikatami na potrzeby połączeń RDP	502
29.4.1	Lokalizacja certyfikatu dla protokołu RDP w Windows Server	502

29.4.2 Dostarczanie certyfikatu CA	505
30 Często zadawane pytania	521
31 Słownik pojęć	526
Indeks	529

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 Enterprise.

3. Wstęp

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

4. Instalacja i pierwsze uruchomienie

Rozdział opisuje procedurę wdrożenia Fudo Enterprise 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. Pule

Rozdział zawiera tematy związane z zarządzaniem pulami.

9. Zdalne aplikacje

Rozdział zawiera tematy związane z zarządzaniem aplikacjami zdalnymi.

10. Konta

Rozdział zawiera tematy związane z zarządzaniem kontami.

11. Gniazda nasłuchiwania

Rozdział zawiera tematy związane z zarządzaniem gniazdami nasłuchiwania.

12. Sejfy

Rozdział zawiera tematy związane z zarządzaniem sejfami.

13. Żądania dostępu

Rozdział zawiera opis funkcjonalności wysyłania żądań dostępu do zasobów.

14. Wykrywanie (Discovery)

Rozdział zawiera opis funkcjonalności automatycznego wykrywania kont oraz serwerów.

15. Modyfikatory haseł

Rozdział opisuje zagadnienia automatycznej zmiany haseł w systemach docelowych.

16. Polityki

Rozdział opisuje zagadnienia związane z proaktywnym monitoringiem.

17. Aktywność konta w Portalu Użytkownika

Rozdział zawiera informacje dotyczące funkcjonalności informowania o zajętości zasobów.

18. Sesje

Rozdział zawiera informacje dotyczące rejestrowanych sesji dostępowych.

19. Raporty

Rozdział zawiera informacje na temat generowania raportów.

20. Analiza produktywności

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

21. Administracja

Rozdział zawiera opisy procedur administracyjnych.

22. Informacje uzupełniające

Rozdział zawiera informacje uzupełniające bezpośrednio związane z procedurami zarządzania.

23. Fudo Officer 1.0

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

24. AAPM (Application to Application Password Manager)

Rozdział zawiera opis modułu zmiany haseł w aplikacjach trzecich.

25. Systemy zgłoszeń

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

26. Aplikacje klienckie

Rozdział zawiera opisy konfigurowania aplikacji klienckich dla wybranych protokołów.

27. Rozwiązywanie problemów

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

28. Często zadawane pytania

Rozdział zawiera odpowiedzi na często zadawane pytania.

29. 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.

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

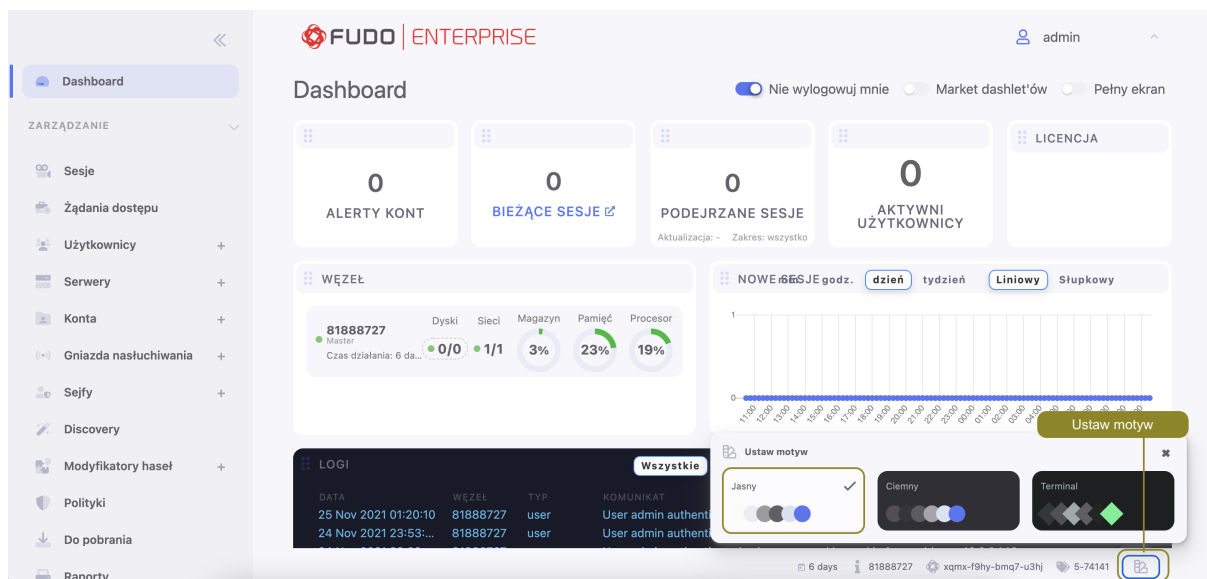
Nota prawna

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

Motywy kolorystyczne Panelu Administracyjnego

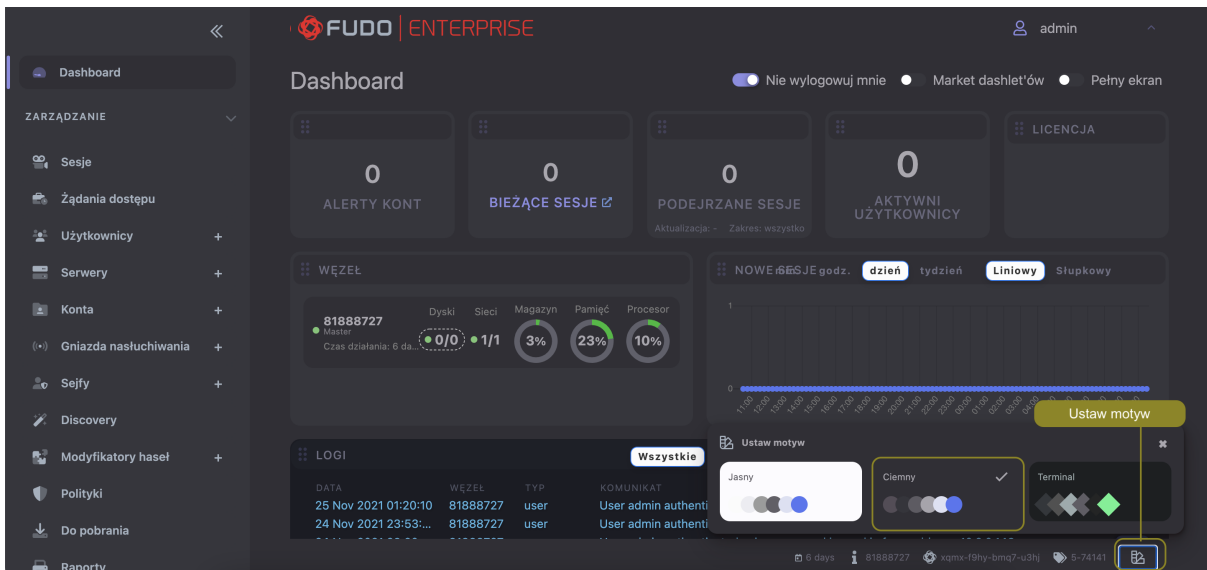
Fudo Enterprise udostępnia trzy motywy kolorystyczne Panelu Administracyjnego. Kliknij ikonę w prawym dolnym rogu ekranu w celu wywołania listy dostępnych wariantów.

Jasny:

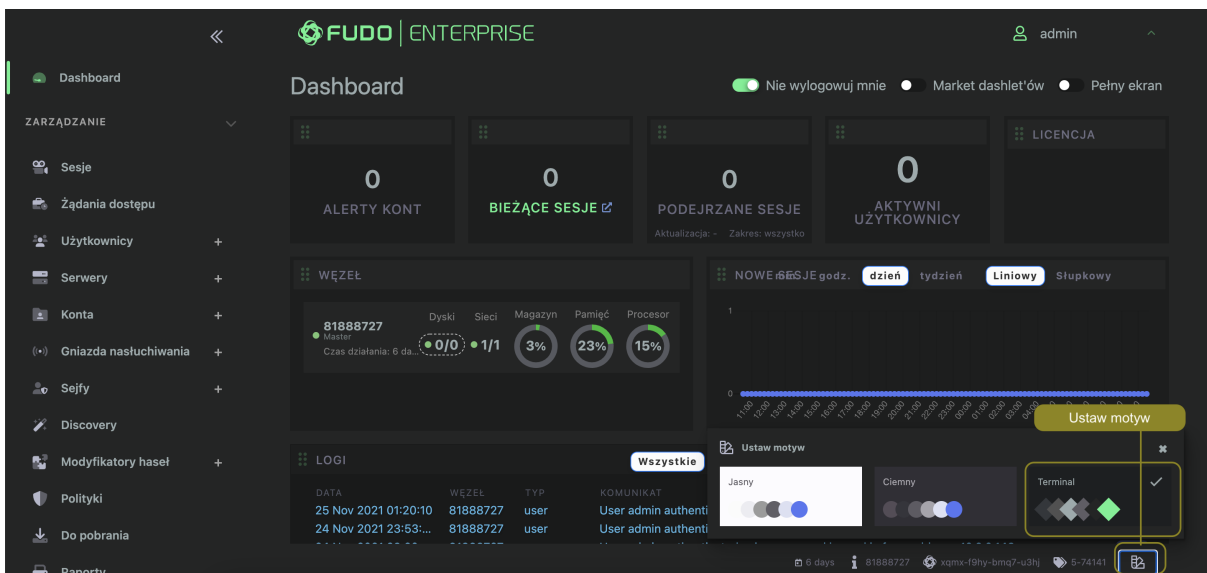


The screenshot shows the Fudo Enterprise Admin Panel interface. The top navigation bar includes the logo 'FUDO | ENTERPRISE', the user 'admin', and settings for 'Nie wylogowuj mnie', 'Market dashlet'ów', and 'Pełny ekran'. The main dashboard area displays several widgets: 'ALERTY KONT' (0), 'BIEŻĄCE SESJE' (0), 'PODEJRZANE SESJE' (0), and 'AKTYWNI UŻYTKOWNICY' (0). Below these are widgets for 'WĘZEL' (Node) and 'NOWE SESJE' (New Sessions). The 'WĘZEL' widget shows metrics for '81888727' including 'Dyski', 'Sieci', 'Magazyn', 'Pamięć', and 'Processor'. The 'NOWE SESJE' widget shows a line chart for 'godz.' (hour) with tabs for 'dzień', 'tydzień', 'Liniowy', and 'Stupkowy'. In the bottom right corner, a 'Ustaw motyw' (Set Theme) button is visible, which has been clicked to open a theme selection menu. This menu shows three options: 'Jasny' (Light) with a checkmark, 'Ciemny' (Dark), and 'Terminal'. A yellow box highlights the 'Ustaw motyw' button, and a yellow circle highlights the 'Ciemny' option.

Ciemny:



Terminal:



Tematy pokrewne:

- *Wstęp*

3.1 Opis systemu

Fudo Enterprise jest kompletnym rozwiązaniem do zarządzania zdalnym dostępem uprzywilejowanym. Fudo Enterprise 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 Enterprise 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 Enterprise pozwala również na podgląd aktualnie trwających połączeń i ingerencję administratora w monitorowaną sesję w przypadku stwierdzenia nadużycia praw dostępu.

Fudo Enterprise 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 beczynności.

Wiecej 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 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 *Starszy szyfr* 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 renderowanych 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 instancji Fudo Enterprise.

- 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 Enterprise dla renderowanych sesji HTTP](#).

3.2.2 Modbus

Wspierane tryby połączenia:

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

Uwagi:

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

3.2.3 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 Enterprise.

Fudo Enterprise działa według algorytmu, weryfikującego, czy obiekty nowej sesji (**gniazdo nasłuchiwania**, **konto**, **adres serwera (serwer)**, **użytkownik**, oraz **sejf**) są takie same, jak obiekty którejs 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.

3.2.4 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.

3.2.5 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.

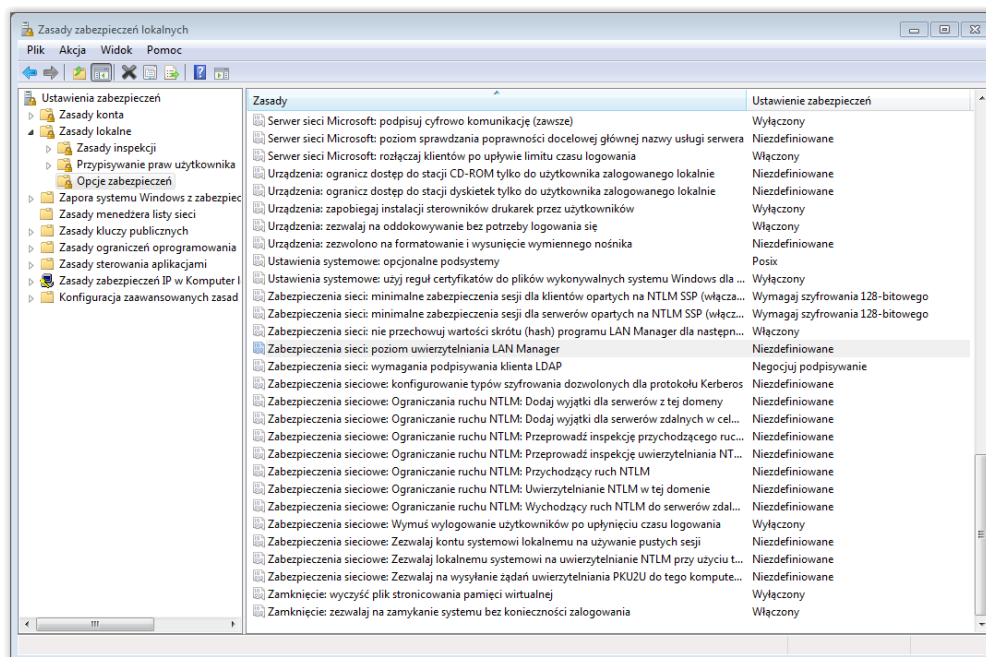
Wspierane algorytmy

- kiedy jest wybrany poziom bezpieczeństwa TLS, a opcja *Starszy szyfr* wyłączona:
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
 - TLS_AES_128_GCM_SHA256
 - 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
- kiedy jest wybrany poziom bezpieczeństwa TLS, a opcja *Starszy szyfr* włączona:
 - TLS_AES_256_GCM_SHA384
 - TLS_CHACHA20_POLY1305_SHA256
 - TLS_AES_128_GCM_SHA256
 - ECDHE-ECDSA-AES256-GCM-SHA384
 - ECDHE-RSA-AES256-GCM-SHA384
 - DHE-RSA-AES256-GCM-SHA384
 - ECDHE-ECDSA-CHACHA20-POLY1305
 - ECDHE-RSA-CHACHA20-POLY1305
 - DHE-RSA-CHACHA20-POLY1305
 - ECDHE-ECDSA-AES128-GCM-SHA256
 - ECDHE-RSA-AES128-GCM-SHA256
 - DHE-RSA-AES128-GCM-SHA256
 - ECDHE-ECDSA-AES256-SHA384
 - ECDHE-RSA-AES256-SHA384

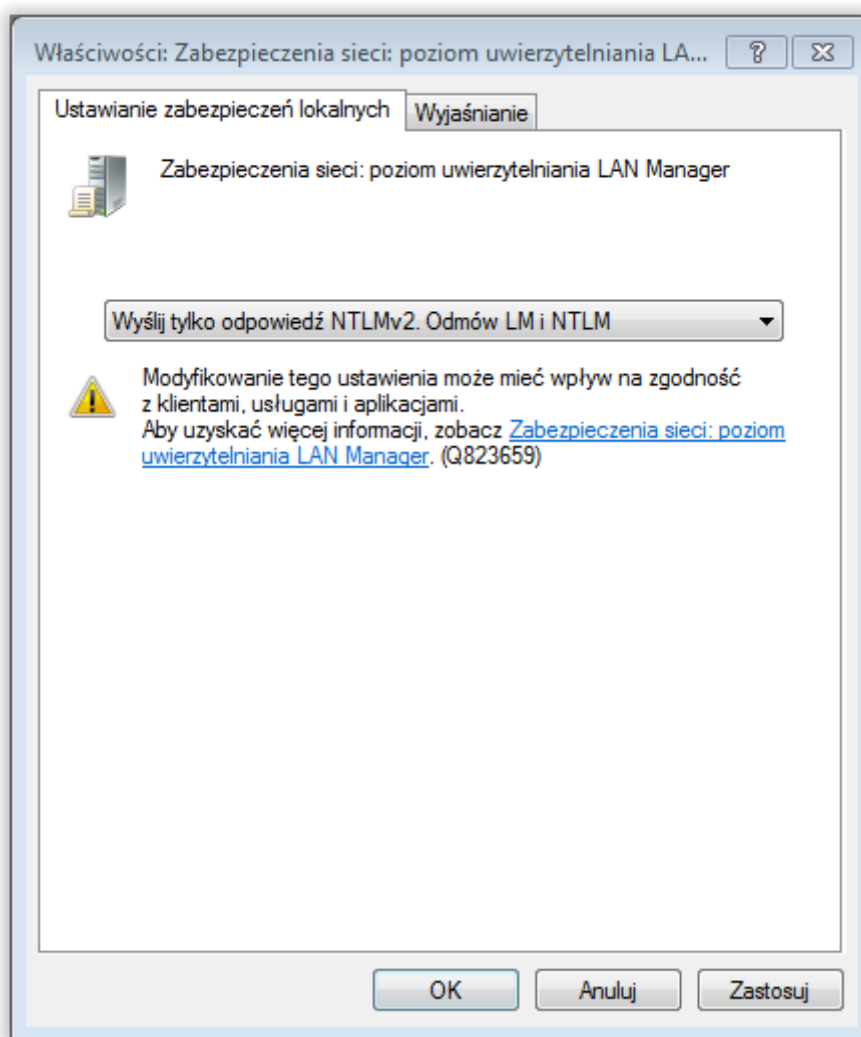
- DHE-RSA-AES256-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA
- ECDHE-RSA-AES256-SHA
- DHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA
- DHE-RSA-AES128-SHA
- AES256-GCM-SHA384
- AES128-GCM-SHA256
- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA

Uwagi:

- Implementacja wsparcia dla protokołu RDP umożliwia uwierzytelnienie poprzez protokół RADIUS, w trybie *challenge-response*.
- Dla serwerów RDP są wspierane opcje NLA oraz TLS.
- Dla gniazd nasłuchiwania RDP, poza standardową opcją bezpieczeństwa jest wspierana opcja *Enhanced RDP Security (TLS)*.
- W przypadku uwierzytelnienia z opcją *NLA* Fudo Enterprise 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 Enterprise sprawdza i ustawia język wprowadzania danych w chwili zestawienia połączenia i nie wspiera dynamicznej zmiany języka na ekranie logowania.

RemoteApp

Fudo Enterprise 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 Enterprise. Połączenia inicjowane poprzez *Remote Desktop Web Access* mogą być monitorowane jedynie w trybie transparentnym/bramy.

3.2.6 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 (przezroczysty, 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 *Starszy szyfr*)

Wspierane kodowanie: UTF-8

Wspierane algorytmy kryptograficzne:

Ostrzeżenie: Protokół *OpenSSH* został zaktualizowany do wersji 9.6 w Fudo Enterprise 5.4.8. Poniższe listy są aktualne dla tej wersji oraz wyższych.

- Jeśli korzystasz ze starszej wersji Fudo Enterprise, zapoznaj się z dokumentacją w wersji 5.3 lub wcześniejszą.
- Jeśli korzystasz z wersji 5.4.7, przeczytaj uwagę dotyczącą algorytmów *MAC* niżej.

- Wspierane algorytmy *key exchange*:
 - curve25519-sha256
 - curve25519-sha256@libssh.org
 - diffie-hellman-group-exchange-sha256
 - diffie-hellman-group16-sha512
 - diffie-hellman-group18-sha512
 - diffie-hellman-group14-sha256
 - ecdh-sha2-nistp256
 - ecdh-sha2-nistp384
 - ecdh-sha2-nistp521
 - sntrup761x25519-sha512@openssh.com
- dodatkowo dochodzą 3 algorytmy *key exchange*, kiedy opcja *Starszy szyfr* zostaje włączona:
 - diffie-hellman-group14-sha1
 - 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
 - ecdsa-sha2-nistp256
 - ecdsa-sha2-nistp384
 - ecdsa-sha2-nistp521

- ssh-ed25519
- rsa-sha2-512
- rsa-sha2-256
- sk-ecdsa-sha2-nistp256-cert-v01@openssh.com
- sk-ecdsa-sha2-nistp256@openssh.com
- sk-ssh-ed25519-cert-v01@openssh.com
- sk-ssh-ed25519@openssh.com
- dodatkowo dochodzą 4 algorytmy *host key*, kiedy opcja *Starszy szyfr* zostaje włączona:
 - ssh-rsa
 - ssh-rsa-cert-v01@openssh.com
 - 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 *Starszy szyfr* 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
 - umac-64@openssh.com
 - umac-128@openssh.com
 - hmac-sha2-256
 - hmac-sha2-512
- dodatkowo dochodzą 11 algorytmów *MAC*, kiedy opcja *Starszy szyfr* zostaje włączona:
 - hmac-sha1
 - 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
 - hmac-md5-96-etm@openssh.com

Ostrzeżenie: Wersja Fudo Enterprise 5.4.7 wspiera ograniczoną listę algorytmów *MAC*:

- hmac-sha2-256
- hmac-sha2-512
- umac-128@openssh.com
- umac-64@openssh.com

dotąd 6 algorytmów *MAC* przy włączonej opcji *Starszy szyfr*:

- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- hmac-ripemd160@openssh.com
- hmac-sha1
- hmac-sha1-96

Uwagi:

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

3.2.7 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 nawiązania 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.

3.2.8 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 nawiązania 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.

3.2.9 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 nawiązania 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 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);

3.2.11 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 Enterprise dla aplikacji korzystających z podstawowego protokołu X11 do rysowania tekstu.

3.2.12 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.

3.2.13 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 uwiaryzelniające*.

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:

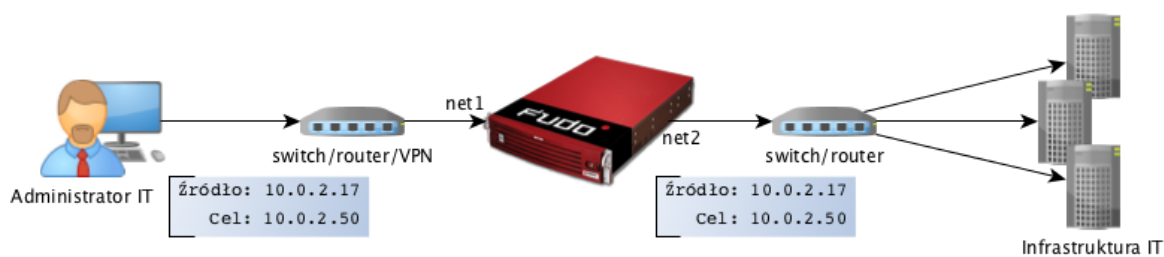
- Brak wsparcia mechanizmu dołączania do sesji.
- Brak wsparcia odtwarzacza.

3.3 Scenariusze wdrożenia

Informacja: Zaleca się umiejscowienie Fudo Enterprise 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 Enterprise 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.



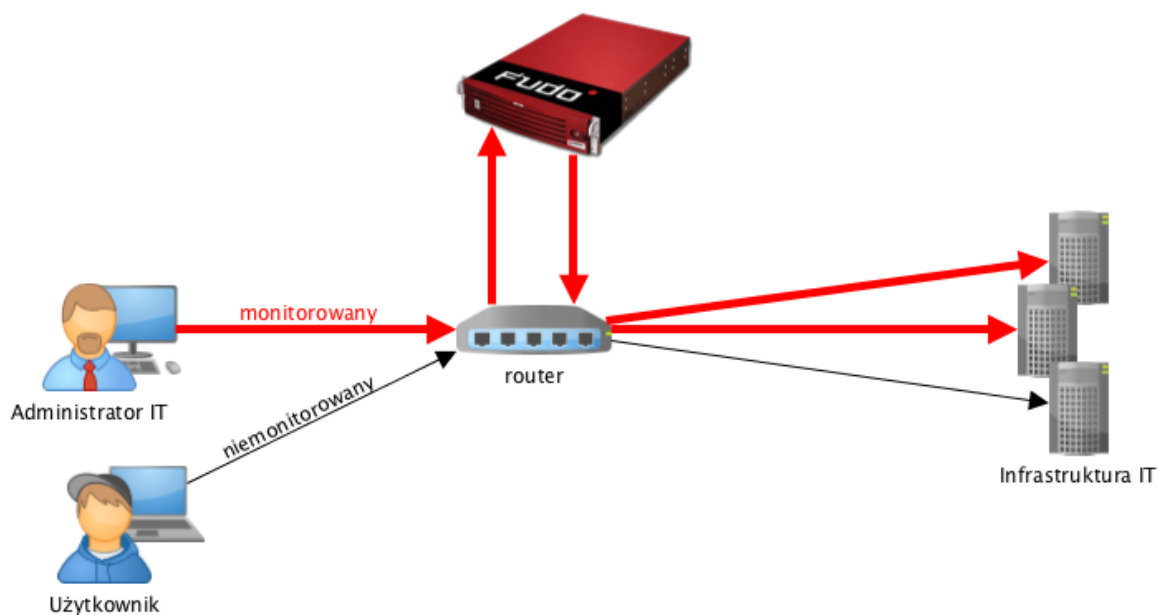
Fudo Enterprise pośrednicząc w przekazywaniu ruchu, zachowuje źródłowy adres IP klienta wysyłającego zapytania do serwerów.

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 Enterprise 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

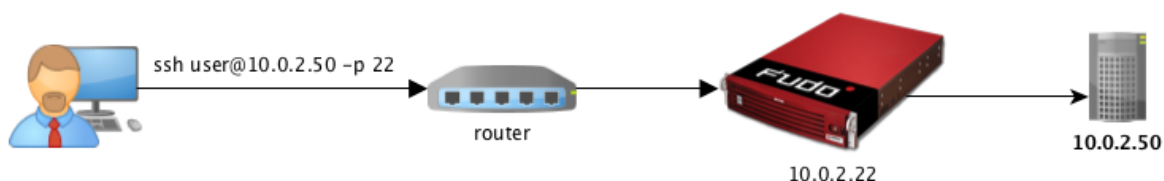
Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryby **transparent** i **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tych trybów muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

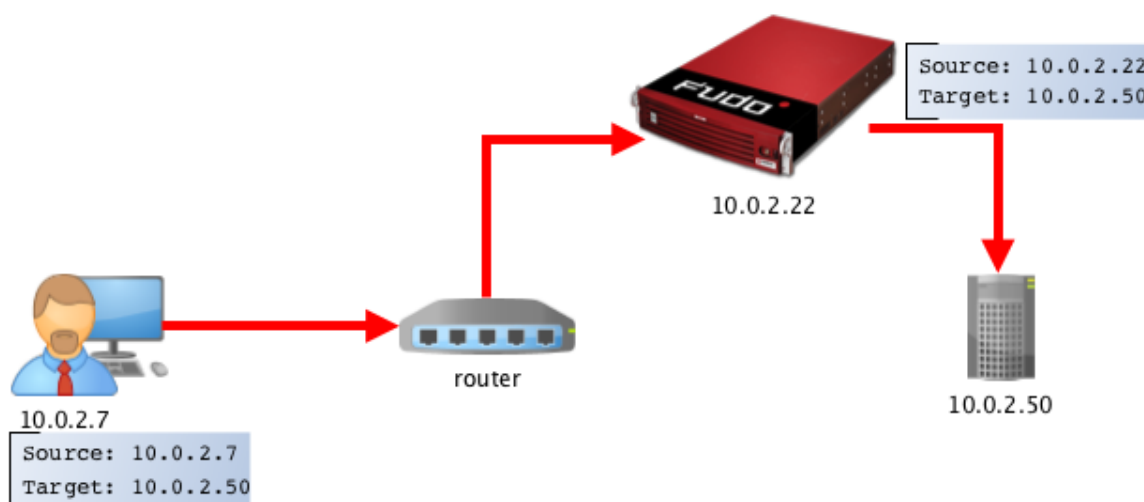
Przezroczysty

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



Brama

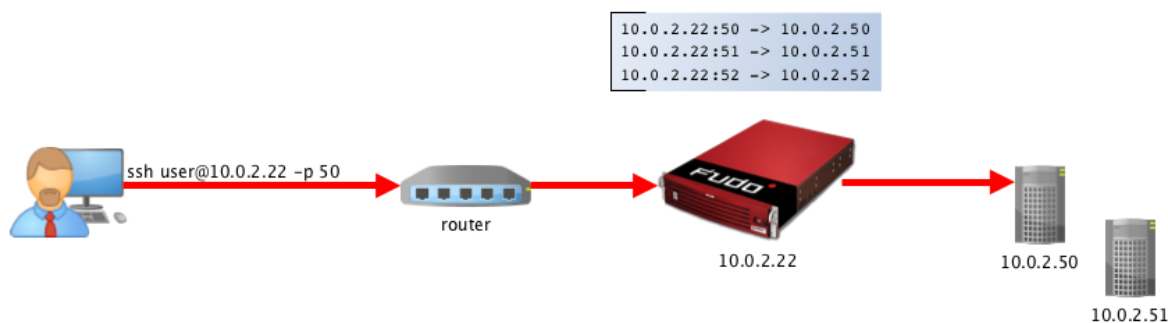
W trybie bramy, klient łączy się z serwerem docelowym wskazując bezpośrednio jego adres IP. Fudo Enterprise zestawiając połączenie z monitorowanym zasobem używa własnego adresu IP. Tryb pracy bramy pozwala na sterowanie ruchem sieciowym, by ten stale przechodził przez Fudo Enterprise, w przypadku gdy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



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

Pośrednik

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

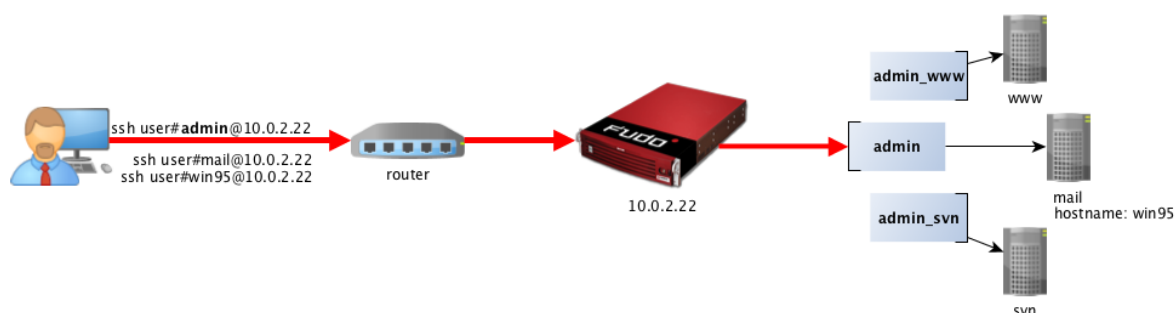


Takie rozwiązanie ukrywa faktyczną adresację serwerów, a odpowiednie ich skonfigurowanie pozwala na odrzucanie zapytań ze źródłowym adresem IP innym niż adres IP Fudo Enterprise.

Bastion

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

W trybie bastionu, konto na serwerze docelowym (lub sam serwer) zdefiniowane jest w ciągu identyfikującym użytkownika, np. `ssh user#admin@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.



Podczas połączenia, Fudo Enterprise oczekuje:

`<username>[@domain] [#<serverlogin>#<address>[:<port>]]`, gdzie:

- `<username>`: login użytkownika na Fudo Enterprise,
- `[@domain]` jest opcjonalne,
- `<serverlogin>`: login użytkownika na serwerze docelowym,
- `<address>`: adres serwera docelowego (`<port>` może być pominięty, jeśli jest natywny dla protokołu).

Ostrzeżenie: Symbol # pomiędzy jest wymagany.

Sekwencja dopasowania obiektu docelowego:

1. Dokładna nazwa użytkownika - Fudo Enterprise dokonuje próby dopasowania podanego ciągu znaków do obiektu, istniejącego w lokalnej bazie danych.
2. Dokładna адреса serwera - Fudo Enterprise dokonuje próby dopasowania podanego ciągu znaków adresu IP serwera do adresu, istniejącego w lokalnej bazie danych.
3. Adres IP zwrócony przez usługę DNS - Fudo Enterprise odpytuje usługę DNS o nazwę hosta i dokonuje próby dopasowania zwróconego adresu IP z adresem IP lokalnie zdefiniowanego serwera.
4. Nazwa hosta zwrócona przez usługę DNS - Fudo Enterprise odpytuje usługę odwrotnego DNS i dokonuje próby dopasowania zwróconej nazwy hosta z lokalnie zdefiniowanym obiektem.

Informacja: Jeśli konto nie ma zdefiniowanego *loginu*, Fudo Enterprise zapyta o niego podczas połączenia z serwerem docelowym.

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 Enterprise pośrednicząc w nawiązywaniu połączeń z serwerami dokonuje uwierzytelnienia użytkowników.

Wspierane metody uwierzytelnienia:

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

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. *challenge-response*).

Tryby uwierzytelnienia

Po uwierzytelnieniu użytkownika, Fudo Enterprise 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 Enterprise 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 Enterprise, drugi raz w celu zalogowania się do systemu docelowego.

Uwierzytelnianie z podmianą hasła

W tym trybie, podczas zestawiania połączenia, Fudo Enterprise 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 użytkownika jest ignorowany przy zestawianiu połączenia.
-

Uwierzytelnienie przez serwer docelowy

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

Autoryzacja dostępu przez administratora

Fudo Enterprise 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 Enterprise 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 Enterprise 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 Enterprise, 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 Enterprise, 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 „zapiecztowania” zaszyfrowanych danych. Klucz główny (Master Key) może zostać wyeksportowany przez super-administradora, 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 Enterprise 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 Enterprise wykorzystuje mechanizm sandboxowania CAPSICUM, który separuje poszczególne połączenia na poziomie systemu operacyjnego Fudo Enterprise. 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

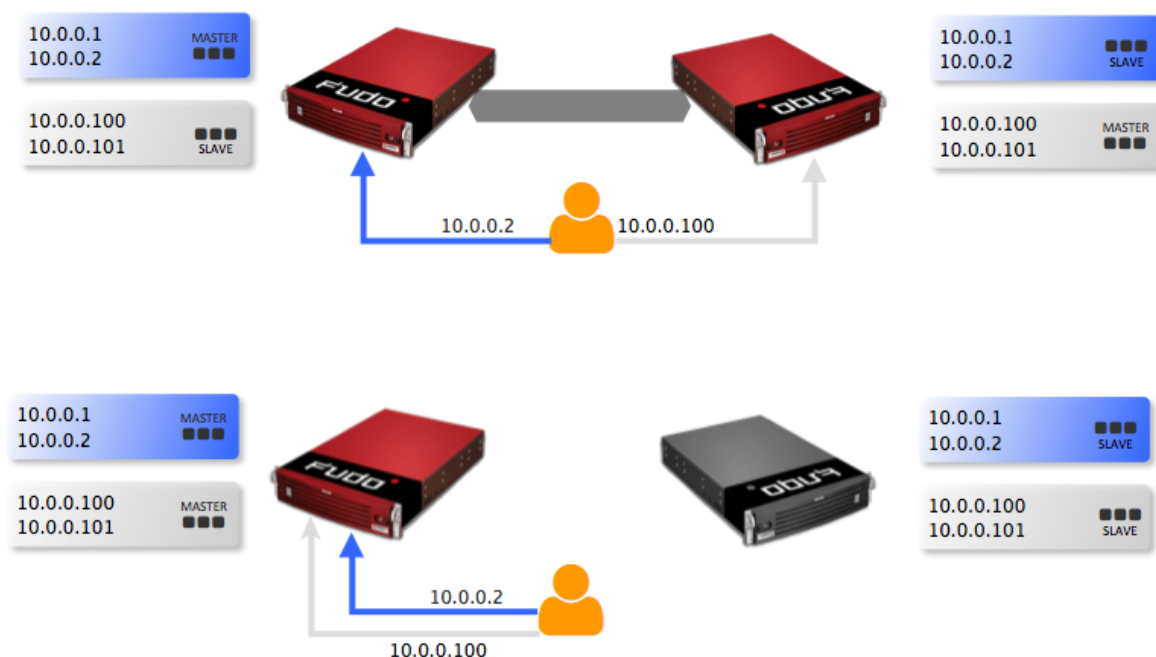
Fudo Enterprise dostarczane jest w konfiguracji sprzętowej zapewniającej optymalną wydajność i wysoką niezawodność systemu.

3.6.6 Konfiguracja klastrowa

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

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

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



Tematy pokrewne:

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

3.7 Model danych

Fudo Enterprise operuje na pięciu podstawowych typach obiektów: użytkownik, serwer, konto, sejf oraz gniazdo nasłuchiwanie.

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.

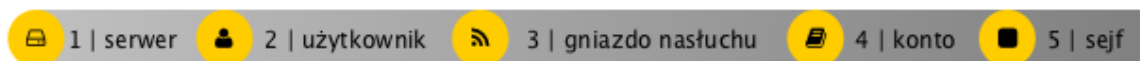
Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

Konto stanowi definicję konta uprzywilejowanego na monitorowanym serwerze. Obiekt określa tryb uwierzytelnienia użytkowników: anonimowe (bez uwierzytelnienia), zwykle (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.

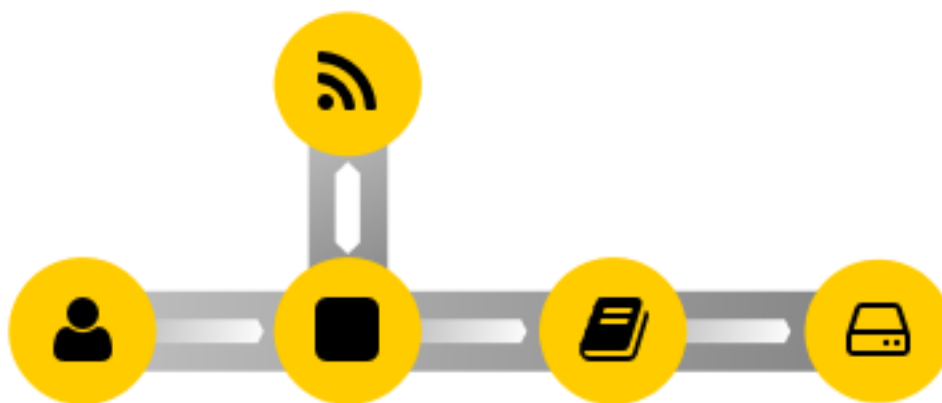
Gniazdo nasłuchiwanie determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

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



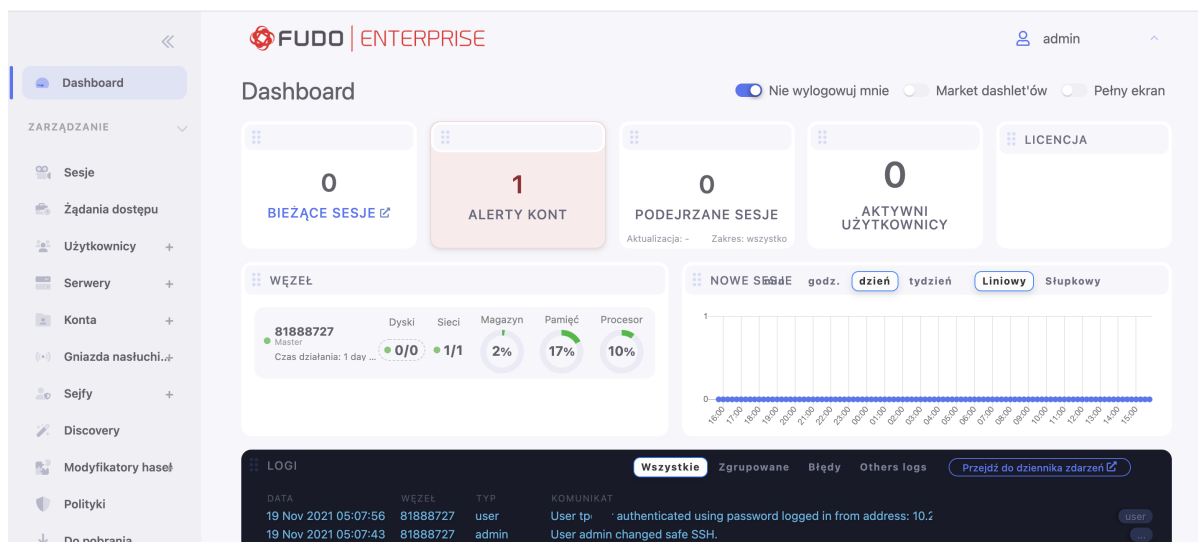
Sejf jest centralnym obiektem modelu danych, który reguluje dostęp do monitorowanych serwerów. Wskazuje konta uprzywilejowane na systemach docelowych, wraz z gniazdami nasłuchiwania określającymi właściwe dla *wybranego trybu* parametry połączenia (np. adres IP, numer portu). Taki model danych pozwala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

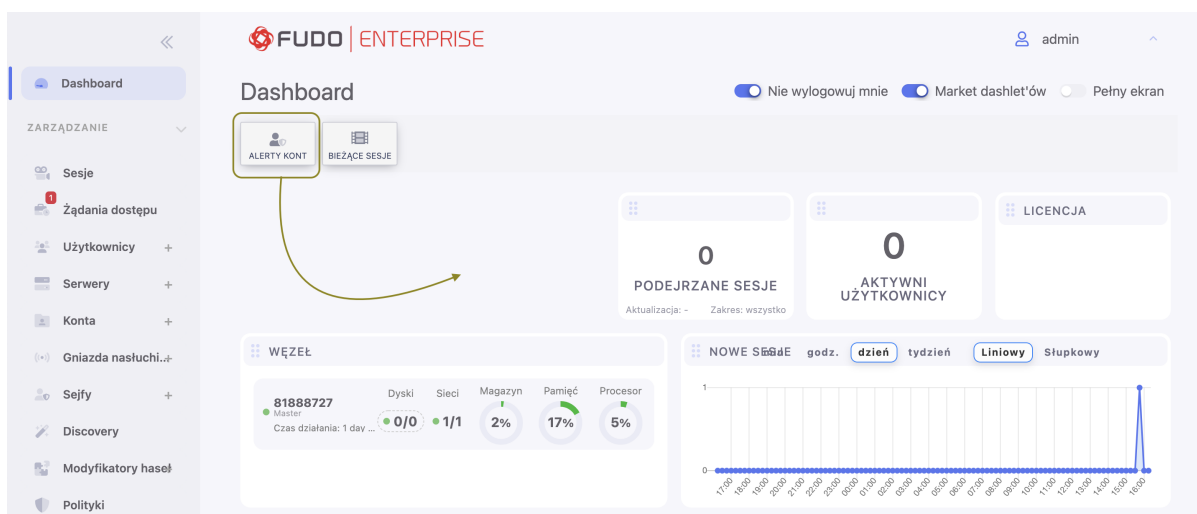
3.8.1 Widżety

Nowe sesje	Wykres obrazujący liczbę nowo nawiązanych połączeń w jednostce czasu.
Aktualne sesje	Liczba aktualnie zestawionych połączeń.
Sesje podejrzone	Liczba sesji o wysokim stopniu zagrożenia. Widżet pozwala wyświetlać podejrzone sesje według następujących konfiguracji czasowych: z ostatnich 12 godzin, ostatniego dnia, ostatniego tygodnia, lub z ostatniego miesiąca. Na widżecie jest też link, prowadzący do odfiltrowanej listy wszystkich takich sesji z określonego przedziału czasowego.
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 Enterprise oraz pozostałych węzłów klastra.
Logi systemowe	Ostatnie wpisy systemowego dziennika zdarzeń.

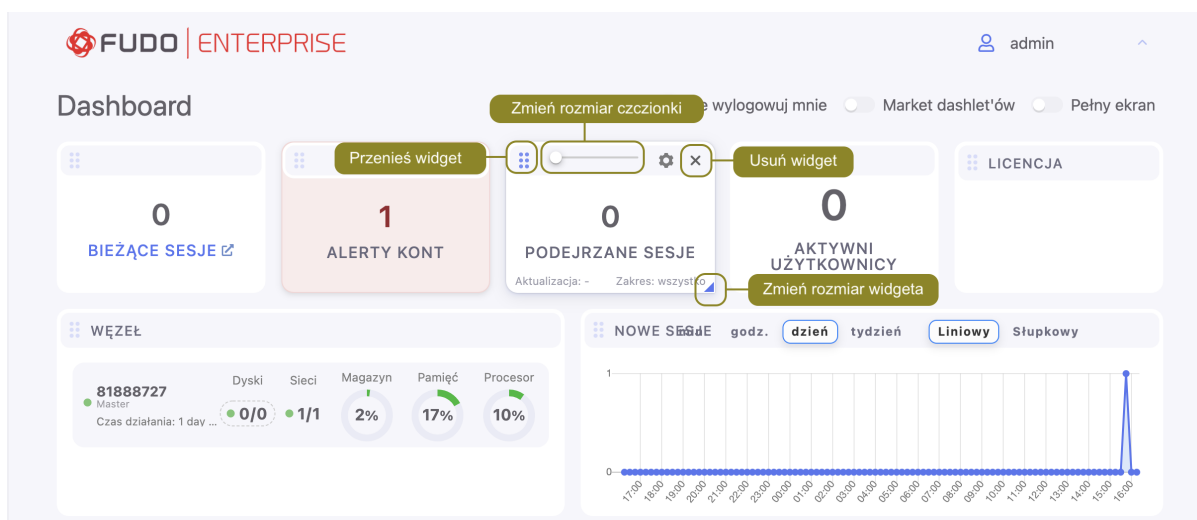
Informacja: Dostępność widżetów zależy od *roli przypisanej użytkownikowi*.

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 przeciągnij lewy górny róg widgetu, aby zmienić jego pozycję.
5. Kliknij suwak pod wartością liczbową, aby zmienić rozmiar czcionki.
6. Kliknij ✕ w prawym górnym rogu elementu, który chcesz usunąć.

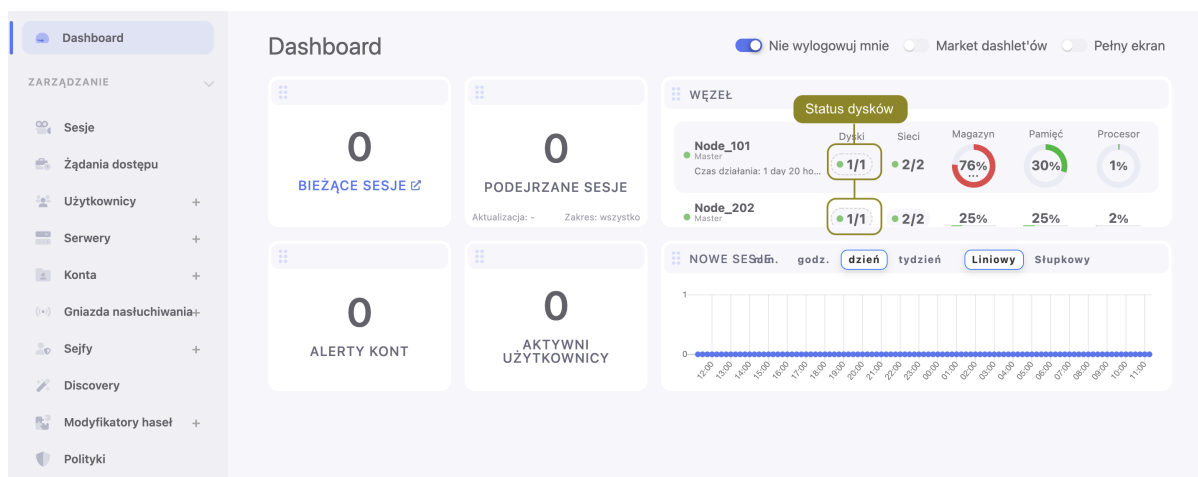


- Kliknij *Usuń*, aby potwierdzić usunięcie widgetu.

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 widżecie *WĘZEL*.



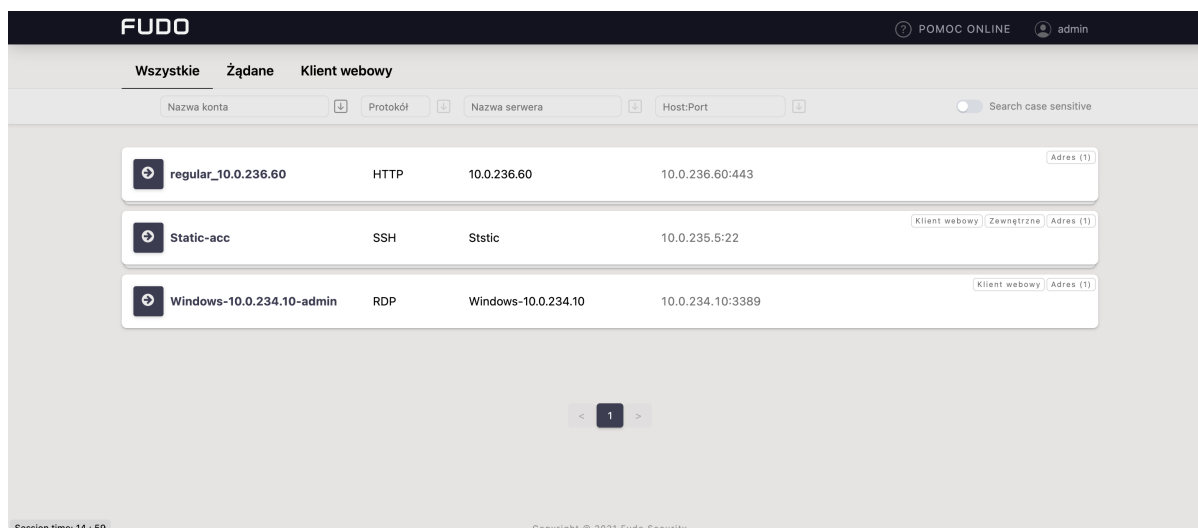
- Dysk pracuje prawidłowo.
- Dysk w trakcie synchronizacji danych.
- Błędy odczytu/zapisu danych - dysk nie działa prawidłowo i może wkrótce ulec awarii - skontaktuj się z działem wsparcia technicznego w celu omówienia dalszych kroków mających na celu przywrócenie urządzenia do pełnej sprawności.
- Awaria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

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.

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 Enterprise wymaga:

- Możliwości wykonywania połączeń dla sesji administracyjnych na port 443/TCP urządzenia.
- Możliwości nawiązania połączenia wychodzącego z Fudo Enterprise do serwera `home.fudosecurity.com` na port 22/TCP dla funkcji *Call Home*.
- Możliwości wykonywania połączeń do Fudo Enterprise przez klientów oraz z Fudo Enterprise do maszyn docelowych.
- Prawidłowo skonfigurowanego *serwera czasu*.

Domyślne porty wykorzystywane przy pierwszym uruchomieniu

Port	Opis
443/TCP	Wymagany do celów administracyjnych.
65522/TCP	Konieczny do połączeń administracyjnych opartych na SSH.
22/TCP	Wykorzystywany przez dodane domyślnie gniazdo nasłuchiwania SSH oraz aplikację mobilną Fudo Officer i usługę <i>Call Home</i> .
3389/TCP	Wykorzystywany przez dodane domyślnie gniazdo nasłuchiwania RDP.

Wymagania sprzętowe

Fudo Enterprise 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

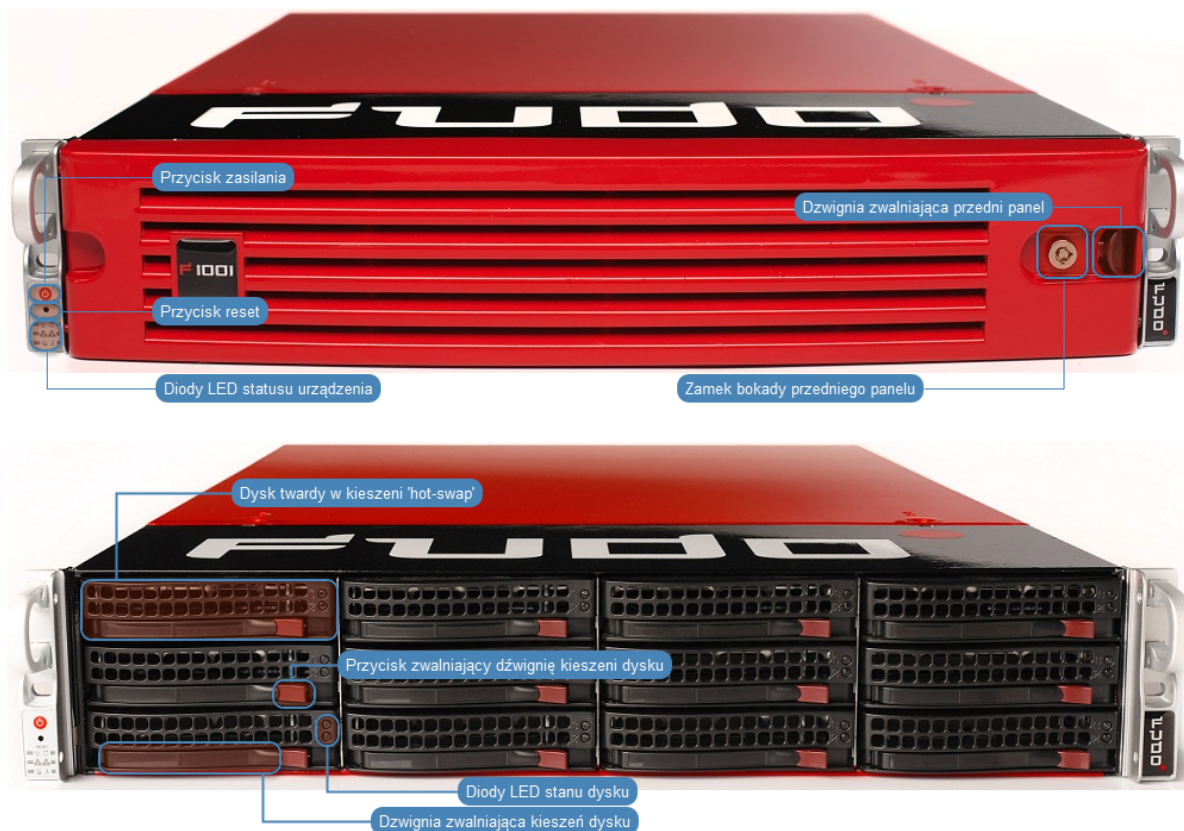
Fudo Enterprise dostarczane jest w obudowie do montażu w standardowej szafie serwerowej 19", w rozmiarze 2U (model F100x), 3U (model F300x) lub 4U (model F500x).

Fudo Enterprise 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

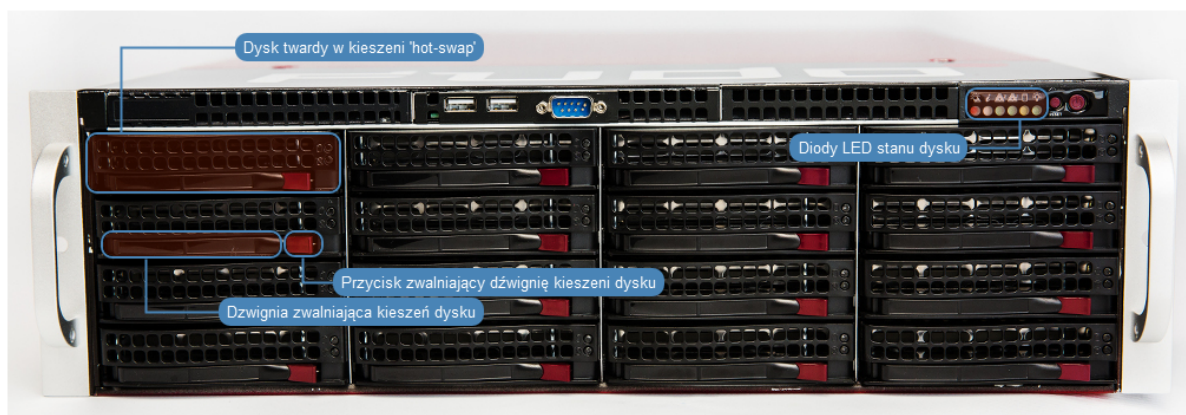
Sytuacja może różnić się w zależności od zastosowania kart rozszerzeń.



Fudo Enterprise 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 Enterprise 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 Enterprise 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 Enterprise. Skontaktuj się ze sprzedawcą lub wsparciem technicznym, aby dowiedzieć się więcej.

```
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: █
```

3. Wprowadź hasło do konta administratora.

```
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:
```

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 potwierdzić 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 Enterprise) 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

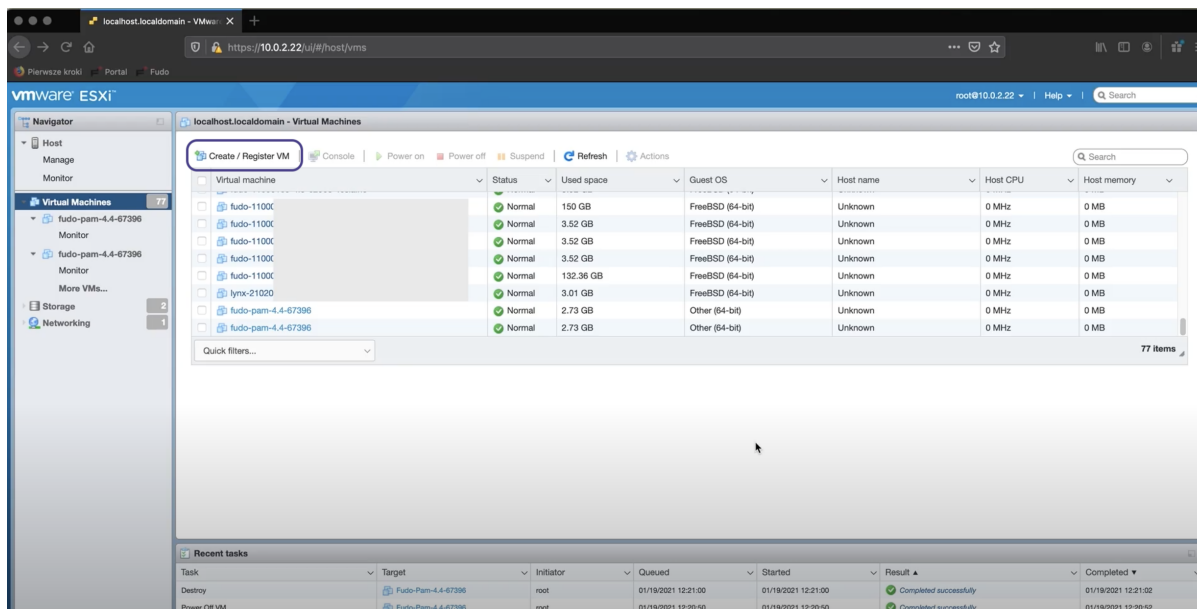
Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
Enter new default gateway IP address (10.0.0.1):
```

4.3.1 Środowisko wirtualne

Lokalne wdrożenie Fudo Enterprise polega na załadowaniu pliku OVA / OVF do maszyny wirtualnej i uruchomieniu panelu Fudo Enterprise w przeglądarce. Poniższa instrukcja opisuje wdrożenie Fudo Enterprise przy pomocy narzędzi VMware lub Proxmox.

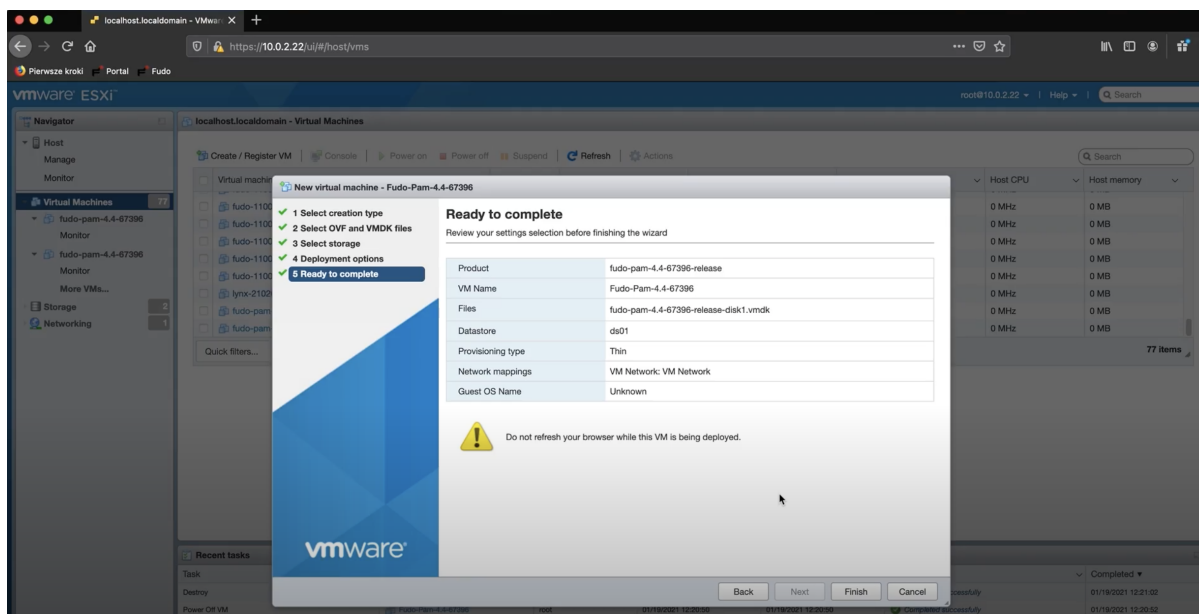
Inicjacja w VMware przy użyciu pliku OVA

1. Kliknij przycisk *Create / Register VM*.



2. W oknie dialogowym wybierz opcję *Deploy a virtual machine from an OVF or OVA file*.
3. Wprowadź nazwę dla maszyny wirtualnej.
4. Wskaż pobrany wcześniej plik OVA lub przeciągnij i upuść go w przeznaczonym do tego obszarze okna dialogowego.

5. Wskaż miejsce przechowywania dysków i plików konfiguracyjnych maszyny wirtualnej.
6. Skonfiguruj opcje wdrożenia tworzonej maszyny według potrzeb.



7. Kliknij *Finish* i poczekaj na załadowanie pliku konfiguracyjnego.
8. Uruchom utworzoną maszynę wirtualną.
9. Kliknij przycisk *Console* i wybierz opcję *Launch remote console*. Wybierz swoją aplikację i zweryfikuj certyfikat.
10. W konsoli podaj hasło.

Informacja: Hasło jest opcjonalne i może pozostać puste. Jeśli hasło zostanie utworzone, system Fudo zaszyfruje je i będzie pytać o nie przy każdym ponownym uruchomieniu maszyny wirtualnej.

11. Wybierz region oraz miasto podając odpowiednie kody z listy i potwierdź swój wybór.
12. Wprowadź datę i godzinę w formacie DD.MM.RRRR GG:MM.


```

43. Sarajevo
44. Saratov
45. Simferopol
46. Skopje
47. Sofia
48. Stockholm
49. Tallinn
50. Tirane
51. Tiraspol
52. Ulyanovsk
53. Uzhgorod
54. Vaduz
55. Vatican
56. Vienna
57. Vilnius
58. Volgograd
59. Warsaw
60. Zagreb
61. Zaporozhye
62. Zurich
Please enter a city number: 59
Are you sure to continue with Warsaw (59)? (Y/n): Y
Timezone has been changed.
Enter a date and time [format: DD.MM.YYYY HH:MM]: 22.11.2022 15:40
Are you sure to continue with introduced date and time (Y/n): Y

```

13. Ustaw konfigurację sieci:

a. Zaloguj się jako administrator:

login: admin

hasło: proxycrypto

b. Z listy *Fudo configuration utility* wybierz opcję 3 - *Reset network settings*.

c. Wybierz nowy interfejs zarządzania i wprowadź adres IP.

```

Retype new password:

*** FUDO configuration utility ***

Logged into FUDO, S/N 82960413, firmware FUDO-5-81225, fuid (mjfu-rkfg-t5jw-dcn5
).

1. Show status
2. Disks status and identification
3. Reset network settings
X. Reset Fudo to the factory defaults
0. Exit

Choose an option (^C anytime to abort) (0): 3

Available network interfaces:

net0 ()
  ether: 9e:e8:31:5c:5b:c2
  media: Ethernet 10Gbase-T <full-duplex>

Choose new management interface (net0): net0
Enter new net0 IP address and netmask (eg. 192.168.1.1/24) (192.168.1.1/24): 172
.16.30.10/24
Enter new default gateway IP address: 172.16.30.1

```

Informacja: Twoja instancja Fudo Enterprise została pomyślnie zainicjowana! Teraz możesz wprowadzić zarejestrowany adres IP w przeglądarce i rozpocząć pierwszą konfigurację Fudo

Enterprise.

Inicjacja w Proxmox przy użyciu pliku OVF

1. Utwórz nową maszynę wirtualną używając parametrów z manifestu pliku OVF, a następnie zaimportuj dyski do lokalizacji `local-zfs`:
 - a. Zaloguj się do komputera zdalnego, np. za pomocą `ssh 10.0.2.33` i podaj hasło.
 - b. W katalogu `fudo.install` wywołaj komendę: `qm importovf <vmid> <manifest> <storage> [OPTIONS]`

Np:

```
qm importovf 109 ./fudo-one-36271-release.ovf local-zfs
```

```

2213.fudo-74-24[14:21:33 0.01] raf@ubuntu18-rw:~$ ssh 10.0.2.33
Linux presales-prox33 5.4.73-1-pve #1 SMP PVE 5.4.73-1 (Mon, 16 Nov 2020 10:52:16 +0100) x86_64

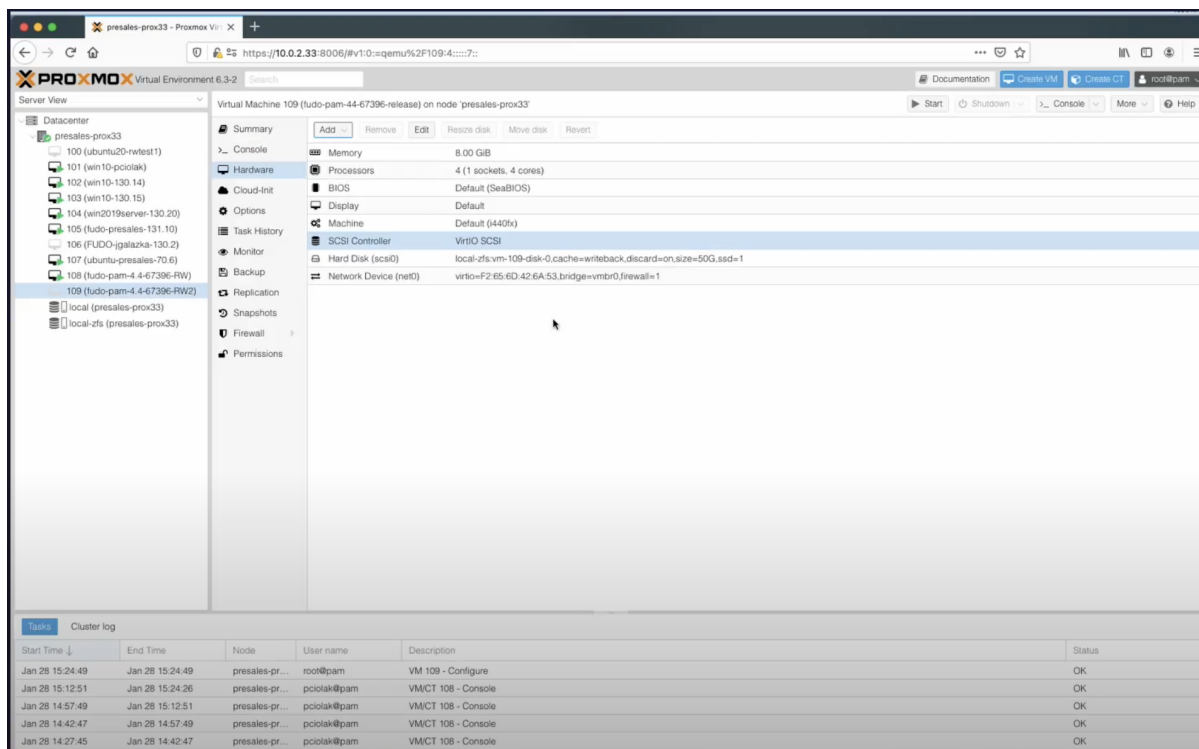
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jan 27 18:55:03 2021 from 10.2.0.120
Filesystem      Size  Used Avail Use% Mounted on
udev            126G  3.6G  122G   3% /dev
tmpfs           26G   179M   25G   1% /run
rpool/ROOT/pve-1 1.4T   38G   1.3T   3% /
tmpfs           126G   49M   126G   1% /dev/shm
tmpfs           5.0M    0   5.0M   0% /run/lock
tmpfs           126G    0   126G   0% /sys/fs/cgroup
rpool           1.3T  128K   1.3T   1% /rpool
rpool/data      1.3T  128K   1.3T   1% /rpool/data
rpool/ROOT      1.3T  128K   1.3T   1% /rpool/ROOT
/dev/fuse       30M   20K   30M   1% /etc/pve
tmpfs           26G    0   26G   0% /run/user/1000

[15:22:20 0.95] raf@presales-prox33:~$ sudo -i
[sudo] password for raf:
root@presales-prox33:~# ls
fudo.install
root@presales-prox33:~# cd fudo.install/
root@presales-prox33:~/fudo.install# ls
fudo-pam-4.4-67396-release-disk1.vmdk  fudo-pam-4.4-67396-release.mf  fudo-pam-4.4-67396-release.ova  fudo-pam-4.4-67396-release.ovf
root@presales-prox33:~/fudo.install# ls -la
total 2137139
drwxr-xr-x 2 root root          6 Jan 27 17:44 .
drwx----- 8 root root         15 Jan 27 17:48 ..
-rw-r--r-- 1 64 64 1094333440 Jan 16 12:42 fudo-pam-4.4-67396-release-disk1.vmdk
-rw-r--r-- 1 64 64          217 Jan 16 12:40 fudo-pam-4.4-67396-release.mf
-rw----- 1 root root 1094346752 Jan 16 12:42 fudo-pam-4.4-67396-release.ova
-rw-r--r-- 1 64 64          9910 Jan 16 12:40 fudo-pam-4.4-67396-release.ovf
root@presales-prox33:~/fudo.install# qm importovf
400 not enough arguments
qm importovf <vmid> <manifest> <storage> [OPTIONS]
root@presales-prox33:~/fudo.install# qm importovf 109 ./fudo-pam-4.4-67396-release.ovf local-zfs

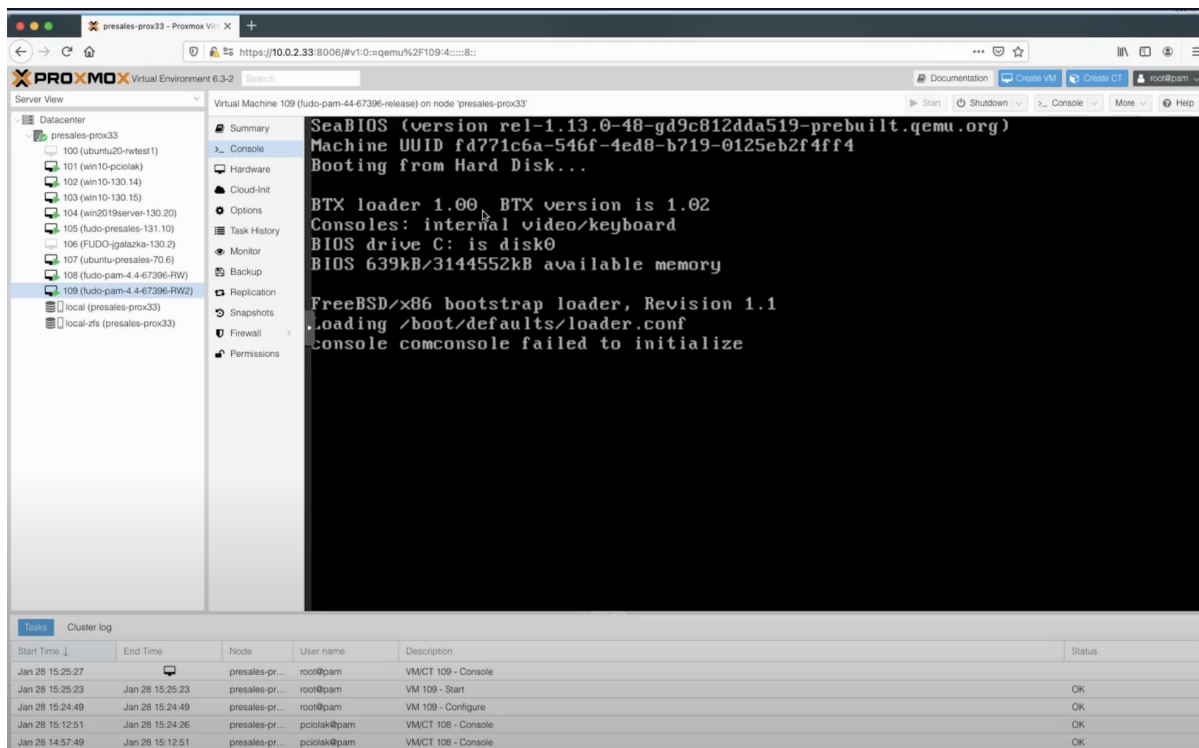
```

2. Poczekać na zaimportowanie danych manifestu.
3. W kliencie Proxmox znaleźć swój serwer i otworzyć ustawienia dla swojej maszyny wirtualnej 109 (`fudo-one-36271-release`).
4. W sekcji *Hardware* zmienić opcję *Hard Disk* na *Write back*, a w sekcji *Advanced* zaznaczyć opcję *SSD emulation* oraz opcję *Discard*. Kliknij *OK*.
5. W sekcji *SCSI Controller* wybrać opcję *VirtIO SCSI* jako typ kontrolera SCSI.
6. Dodaj nowe urządzenie sieciowe i w polu *Model* wybrać opcję *VirtIO (paravirtualized)*.



7. Kliknij opcję *Start*.

8. Przejdź do *Konsoli*.



9. Wybierz region oraz miasto podając odpowiednie kody z listy i potwierdź swój wybór.

10. Wprowadź datę i godzinę w formacie DD.MM.RRRR GG:MM.

11. Ustaw konfigurację sieci:

a. Zaloguj się jako administrator:

login: admin

hasło: proxycrypto

- b. Z listy *Fudo configuration utility* wybierz opcję 3 - *Reset network settings*.
- c. Wybierz nowy interfejs zarządzania i wprowadź adres IP z maską podsieci.
- d. Wprowadź nowy adres IP bramy domyślnej.

Informacja: Twoja instancja Fudo Enterprise została pomyślnie zainicjowana!

12. Wprowadź zarejestrowany adres IP w pasku przeglądarki i zaloguj się jako administrator.
13. W zakładce *Network configuration settings* wprowadź nazwę dla adresu bramy. Kliknij *Save*.
14. Dodaj adres nowego serwera DNS w zakładce *Name & DNS*. Kliknij *Save*.
15. W zakładce *System settings* dodaj adres nowego serwera NTP. Kliknij *Save*.
16. Z menu kontekstowego w prawym górnym rogu wybierz opcję *Restart*.
17. Poczekaj na ponowne uruchomienie systemu i zaloguj się ponownie.

Informacja: Teraz możesz rozpocząć swoją pierwszą konfigurację Fudo Enterprise.

Tematy pokrewne:

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

5.1 SSH

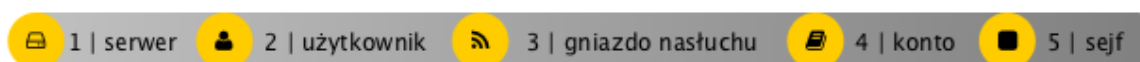
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie połączeń SSH ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *SSH* uwierzytelnia się na Fudo Enterprise używając własnego loginu i hasła (*john_smith/john*). Fudo Enterprise 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
Starszy szyfr	✘
Adres źródłowy	Dowolny
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Adresy serwerów</i>	
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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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
Starszy szyfr	✘
Nierozróżnianie wielkości liter	✘
<i>Uprawnienia</i>	
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
<i>Ogólne</i>	
Nazwa	admin_ssh_server
Zablokowane	✘
Typ	regular
Nagrywanie sesji	wszystko
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	ssh_server
<i>Dane uwierzytelniające</i>	
Domena	✘
Login	admin
Zastąp sekret	hasłem
Hasło	password
Powtórz hasło	password
Polityka modyfikatora hasel	✘


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:

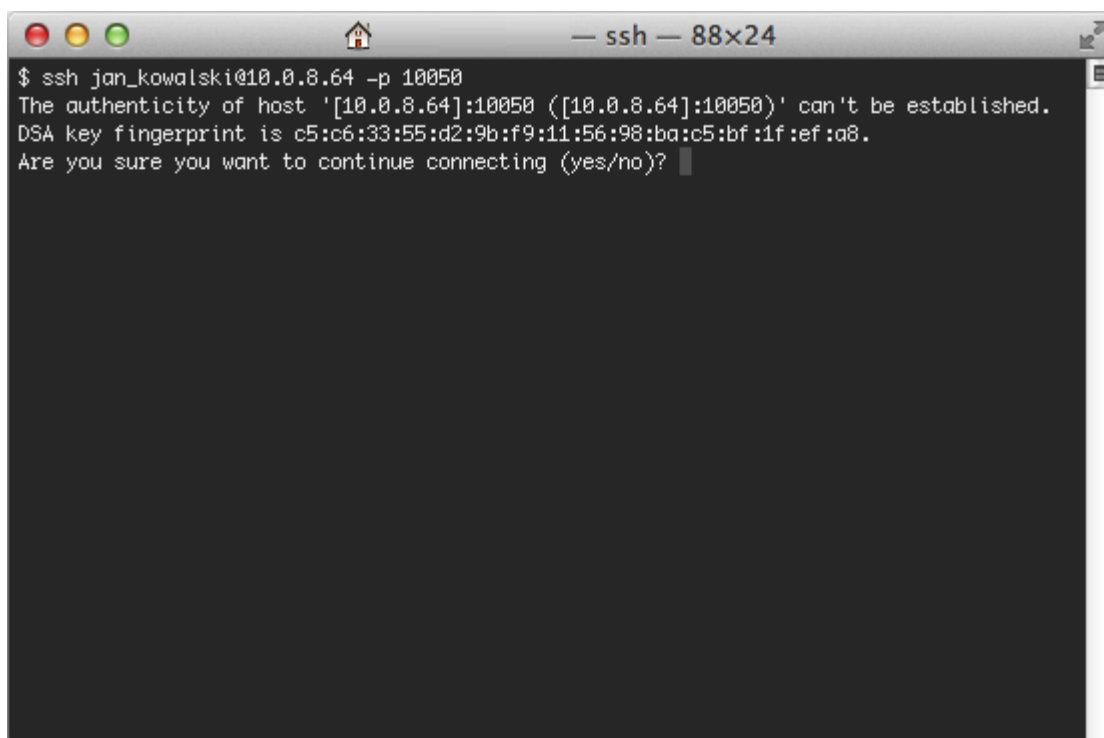
Parametr	Wartość
Nazwa	ssh_safe
Zablokowane	✘
Powiadomienia	✘
Powód logowania	✘
Wymagaj potwierdzenia	✘
Polityki	✘
Note access	No access
<i>Funkcjonalność protokołów</i>	
RDP	✘
SSH	✔
VNC	✘

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:



```
$ ssh jan_kowalski@10.0.8.64 -p 10050
The authenticity of host '[10.0.8.64]:10050 ([10.0.8.64]:10050)' can't be established.
DSA key fingerprint is c5:c6:33:55:d2:9b:f9:11:56:98:ba:c5:bf:1f:ef:a8.
Are you sure you want to continue connecting (yes/no)?
```

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 Enterprise.
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*
- *Zasoby*

5.2 SSH w trybie bastionu

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, 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 Enterprise używając własnego loginu i hasła (*john_smith/john*). Nawiązując połączenie, użytkownik wskazuje w treści loginu nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego. Połączenie realizowane jest za pośrednictwem portu numer 22, domyślnego dla protokołu SSH.

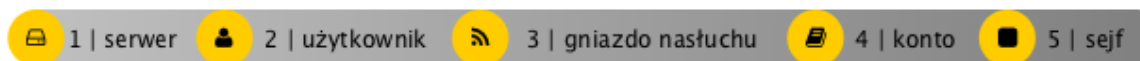
Fudo Enterprise zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na *root/password* (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).



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
<i>Ogólne</i>	
Nazwa	ssh_server
Opis	✘
Zablokowane	✘
Protokół	SSH
Starszy szyfr	✘
Adres źródłowy	Dowolny
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Adresy serwerów</i>	
Adres IP	192.168.0.100
Port	22

4. W sekcji *Weryfikacja serwera* wybierz *Klucz publiczny serwera* i kliknij *Pobierz klucz*, aby pobrać klucz lub wprowadź go w polu tekstowym.
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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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	X
Protokół	SSH
Starszy szyfr	X
Nierozróżnianie wielkości liter	X
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	X
Tryb połączenia	Bastion
Adres lokalny	10.0.150.151
Port	22
Adres zewnętrzny	X
Port zewnętrzny	X

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
<i>Ogólne</i>	
Nazwa	admin_ssh_server
Zablokowane	✘
Typ	regular
Nagrywanie sesji	wszystko
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	ssh_server
<i>Dane uwierzytelniające</i>	
Domena	✘
Login	root
Zastąp sekret	hasłem
Hasło	password
Powtórz hasło	password
Polityka modyfikatora ha- seł	Statyczne, bez ograniczeń

4. Kliknij ikonę wygenerowania klucza SSH lub wgraj klucz prywatny serwera.
5. 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:

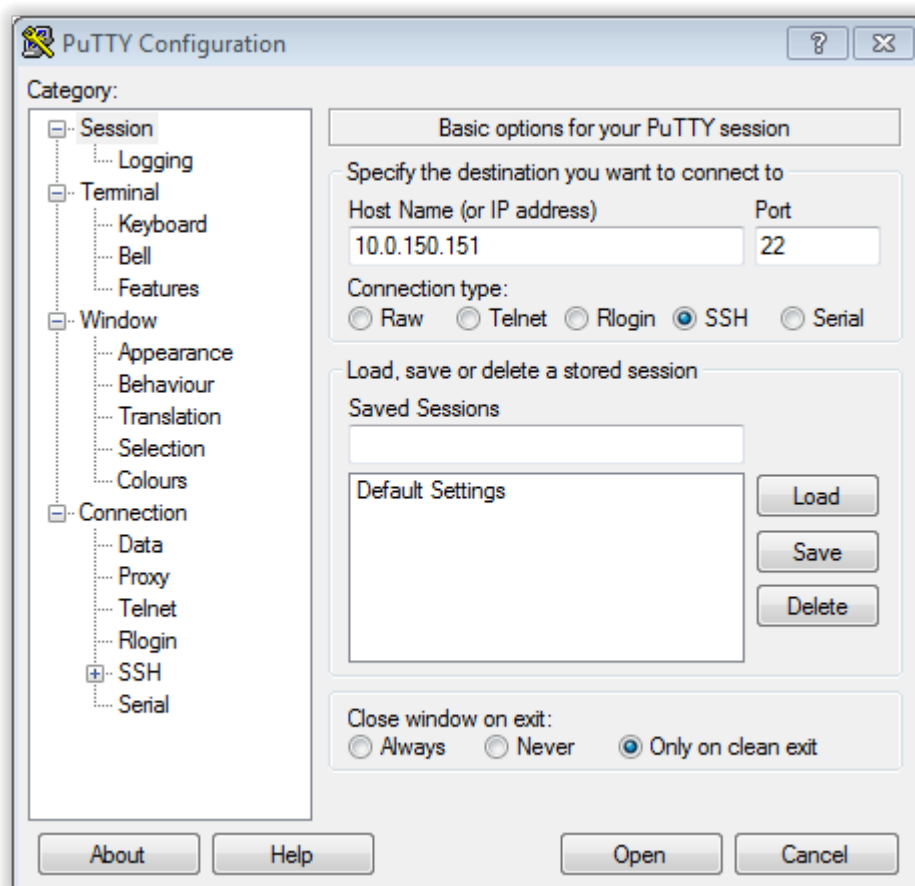
Parametr	Wartość
<i>Ogólne</i>	
Nazwa	ssh_safe
Zablokowane	
Powiadomienia	
Powód logowania	
Wymagaj potwierdzenia	
Polityki	
Note access	No access
<i>Funkcjonalność protokołów</i>	
RDP	
SSH	
VNC	

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*.

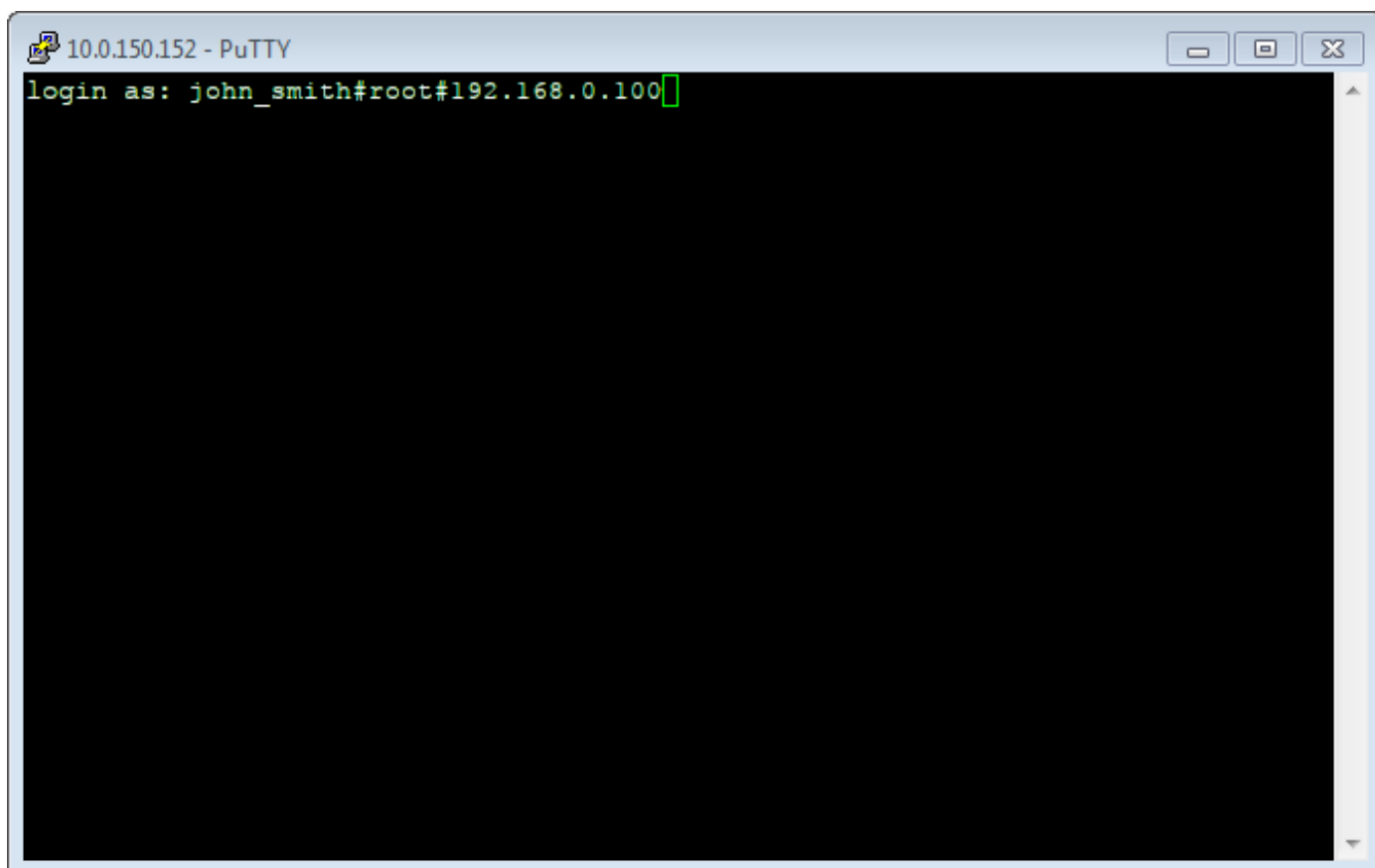
5.2.3 Nawiązanie połączenia

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, login konta na serwerze docelowym oraz adres serwera docelowego.



6. Wprowadź hasło użytkownika.

Interfejs Wiersza polecenia

Uruchom terminal i wykonaj komendę używając podanego formatu:

```
ssh -l <fudo-user>#<server-user>#<server-address> <fudo-address>
```

Example:

```
ssh -l john_smith#root#192.168.0.110 10.0.150.151
```

5.2.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Fudo Enterprise.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Fudo Enterprise.
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*
- *Zasoby*

5.3 RDP

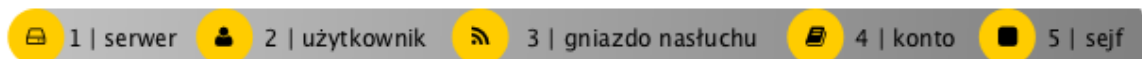
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie połączeń RDP ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta *RDP* używając indywidualnego loginu i hasła. Fudo Enterprise uwierzytelnia 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
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Adresy serwerów</i>	
Adres IP	10.0.35.10
Port	3389

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

Host docelowy

Adres: 10.0.35.54 Port: 3389

Adres źródłowy: 10.0.150

Certyfikat serwera:

```
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANApps6+1WF1s7FE7y
Var/CNulwboAtX
f5ZW3Z6Rab7CpV
VFUCAwEAAQ==
-----END PUBLIC KEY-----
```

c0:4c:1b:4c:a6:2a:c5:f3:31:6d:12:4e:14:ba:0a:0a:0d:58:38:00 SHA1

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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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	✘
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Połączenie</i>	
Tryb połączenia	proxy
Adres lokalny	10.0.150.151
Port	3389
Adres zewnętrzny	✘
Port zewnętrzny	✘

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



- Kliknij *Zapisz*.

Dodanie konta

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

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

Parametr	Wartość
<i>Ogólne</i>	
Nazwa	admin_rdp_server
Zablokowane	✘
Typ	regular
Nagrywanie sesji	wszystko
OCR sesji	✔
Język OCR	Angielski
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	rdp_server
<i>Dane uwierzytelniające</i>	
Domena	✘
Login	admin
Zastęp sekret	hasłem
Hasło	password
Powtórz hasło	password
Polityka modyfikatora hasła	✘

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.

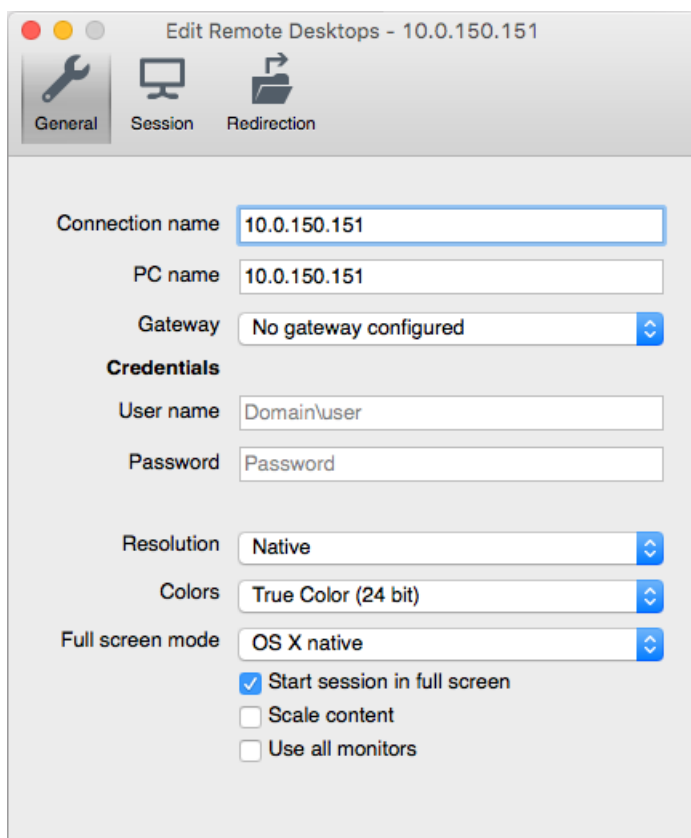
1. Wybierz z lewego menu *Zarządzanie > Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
<i>Ogólne</i>	
Zablokowane	
Powiadomienia	
Powód logowania	
Wymagaj potwierdzenia	
Polityki	
Note access	No access
<i>Funkcjonalność protokołów</i>	
RDP	
SSH	
VNC	
<i>Uprawnienia</i>	
Uprawniani użytkownicy	
<i>Konta</i>	
admin_rdp_server	rdp_listener

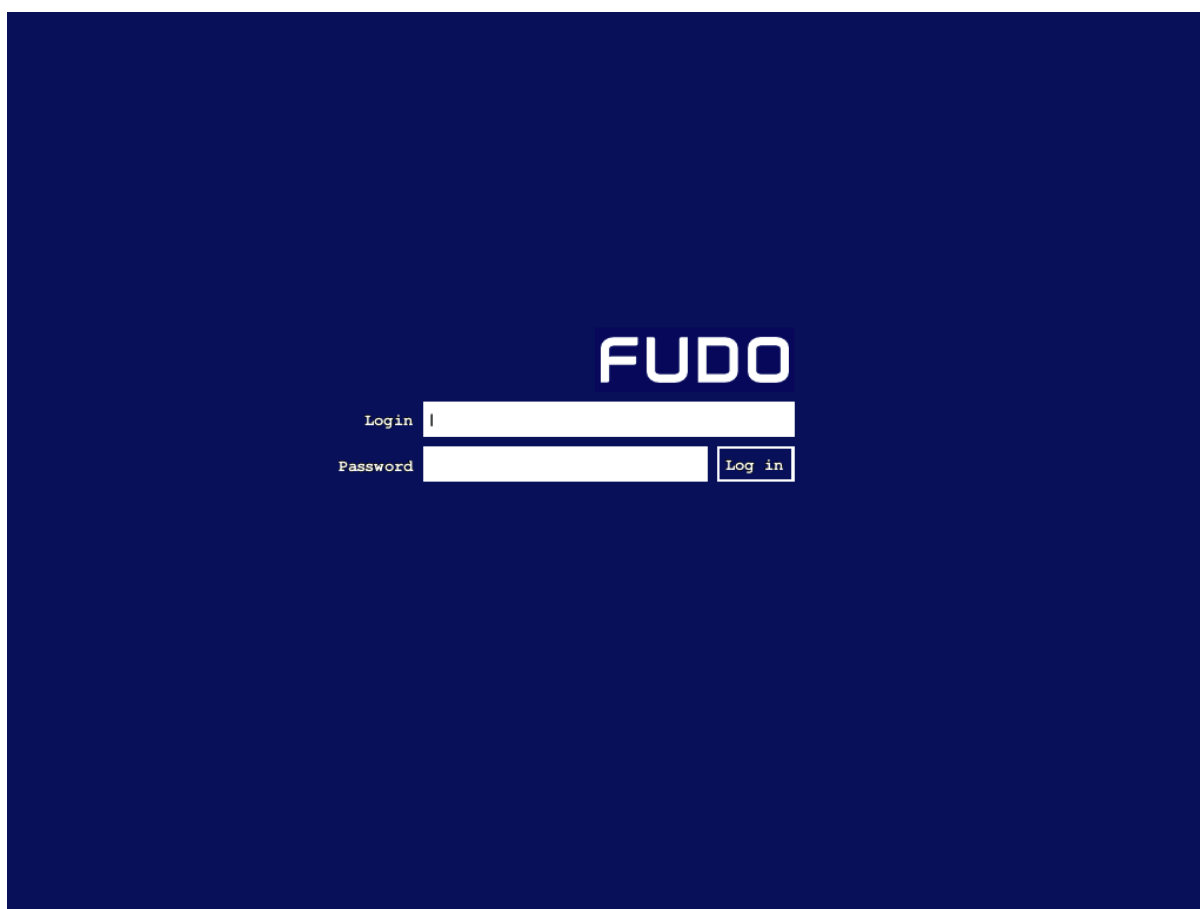
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto *admin_rdp_server* i kliknij
11. Kliknij *OK*.
12. Kliknij w kolumnie *Gniazda nasłuchiwania*.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

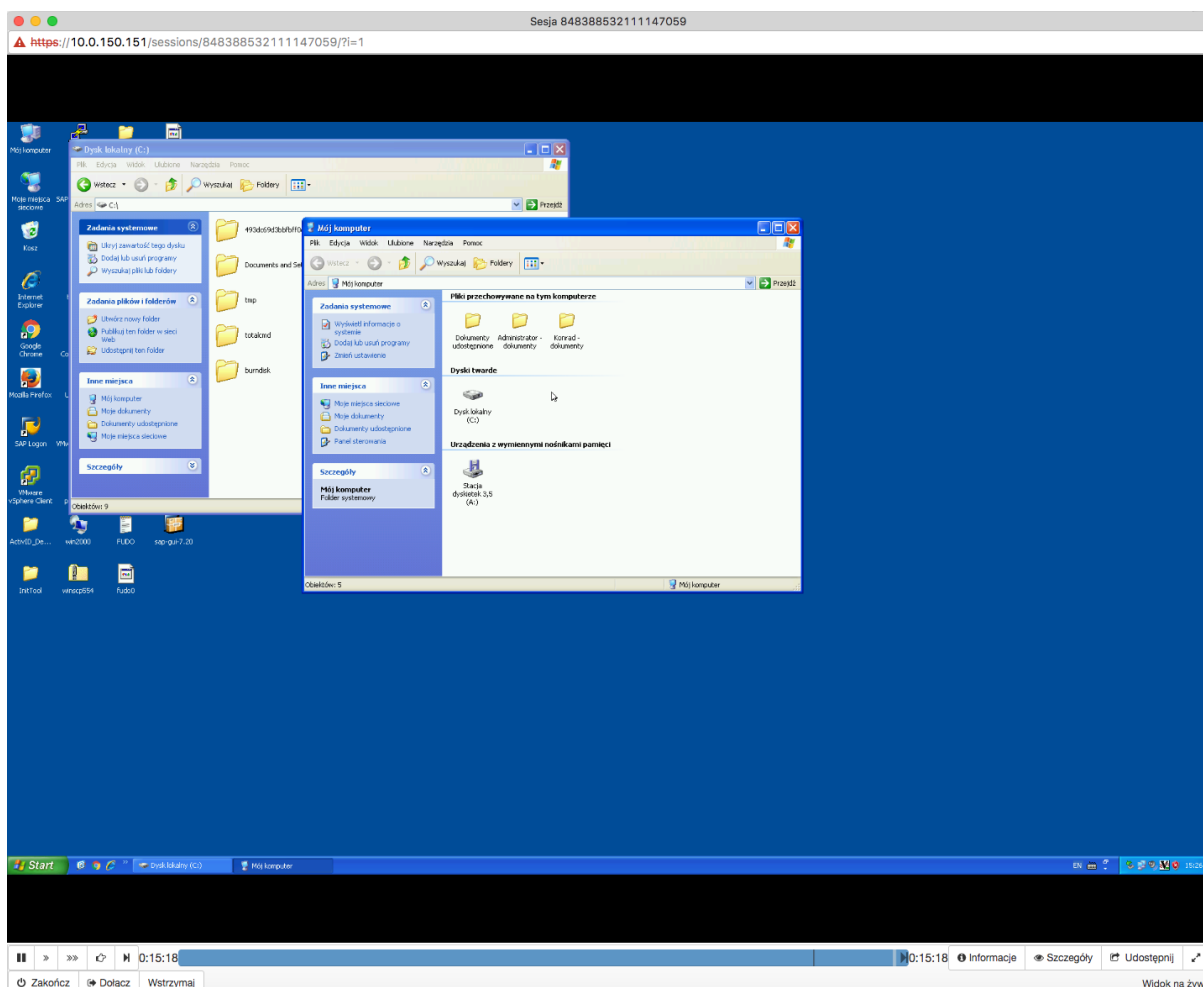
5.3.3 Nawiązanie połączenia

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



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





Tematy pokrewne:

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

5.4 RDP w trybie bastionu

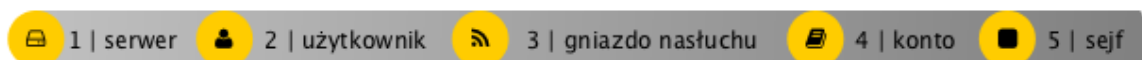
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie połączeń RDP ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem w trybie bastionu, wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego. Fudo Enterprise 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 serwer*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parameter	Value
Nazwa	rdp_server
Opis	✘
Zablokowane	✘
Protokół	RDP
TLS włączony	✔
NLA włączony	✘
Starszy szyfr	✘
Informuj o istniejącym połączeniu	✘
Adres źródłowy	10.0.150.151
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Miejsce przeznaczenia</i>	
Adres	10.0.35.54
Maska	32
Port	3389
Werifikacja serwera	None

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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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
<i>Ogólne</i>	
Nazwa	rdp_listener_bastion
Zablokowane	X
Protokół	RDP
Bezpieczeństwo	Standard RDP Security
Komunikat	X
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	X
<i>Połączenie</i>	
Tryb połączenia	bastion
Adres lokalny	10.0.150.151
Port	3389
Adres zewnętrzny	X
Port zewnętrzny	X

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
<i>Ogólne</i>	
Nazwa	admin_rdp_server
Zablokowane	✘
Typ	regular
Nagrywanie sesji	wszystko
OCR sesji	✔
Język OCR	Angielski
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	rdp_server
<i>Dane uwierzytelniające</i>	
Domena	✘
Login	admin
Zastęp 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
<i>Ogólne</i>	
Nazwa:	rdp_safe
Zablokowane	
Powiadomienia	
Powód logowania	
Wymagaj potwierdzenia	
Polityki	
Note access	No access
<i>Funkcjonalność protokołów</i>	
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. Wprowadź nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego (*john_smith#admin#10.0.35.54*) oraz hasło użytkownika.

Enter your user account

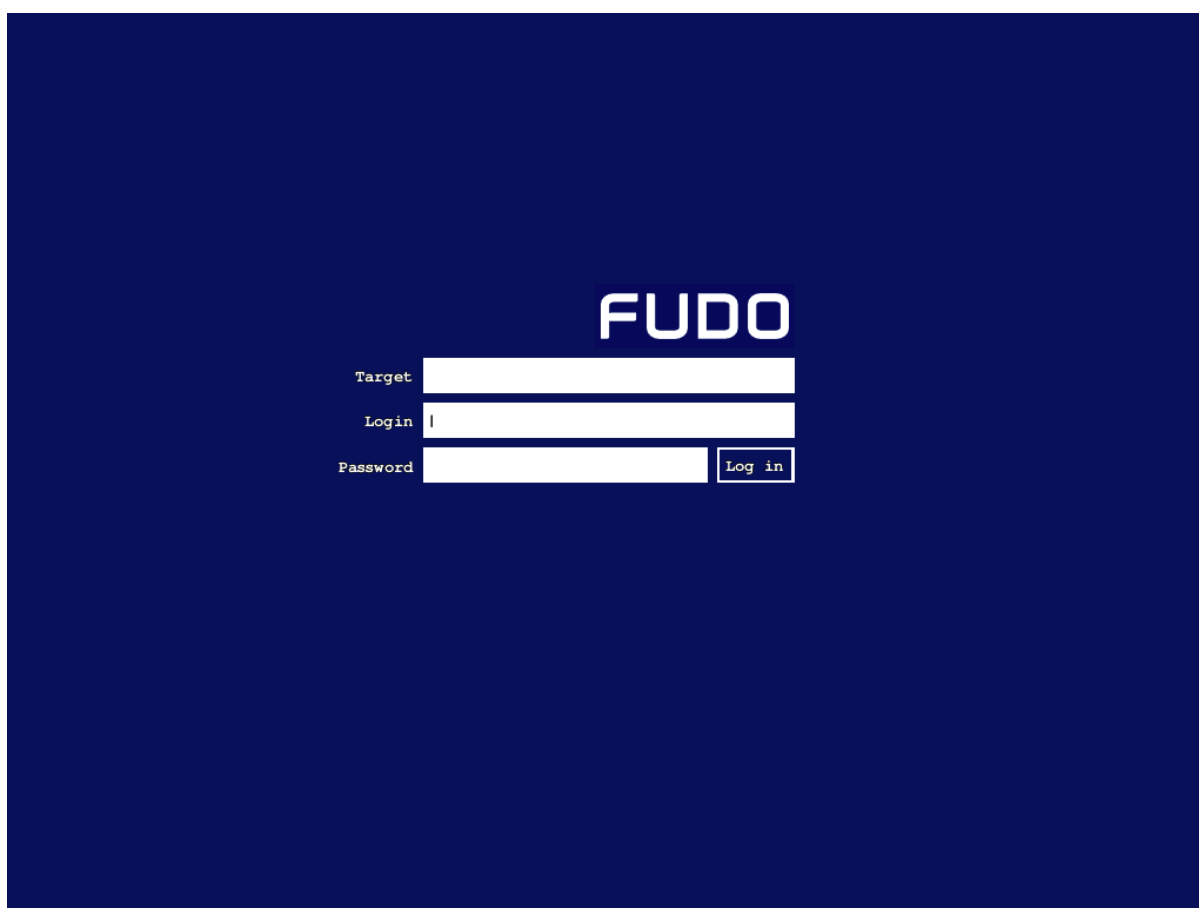
This user account will be used to connect to 10.0.150.151 (remote PC).

User Name:

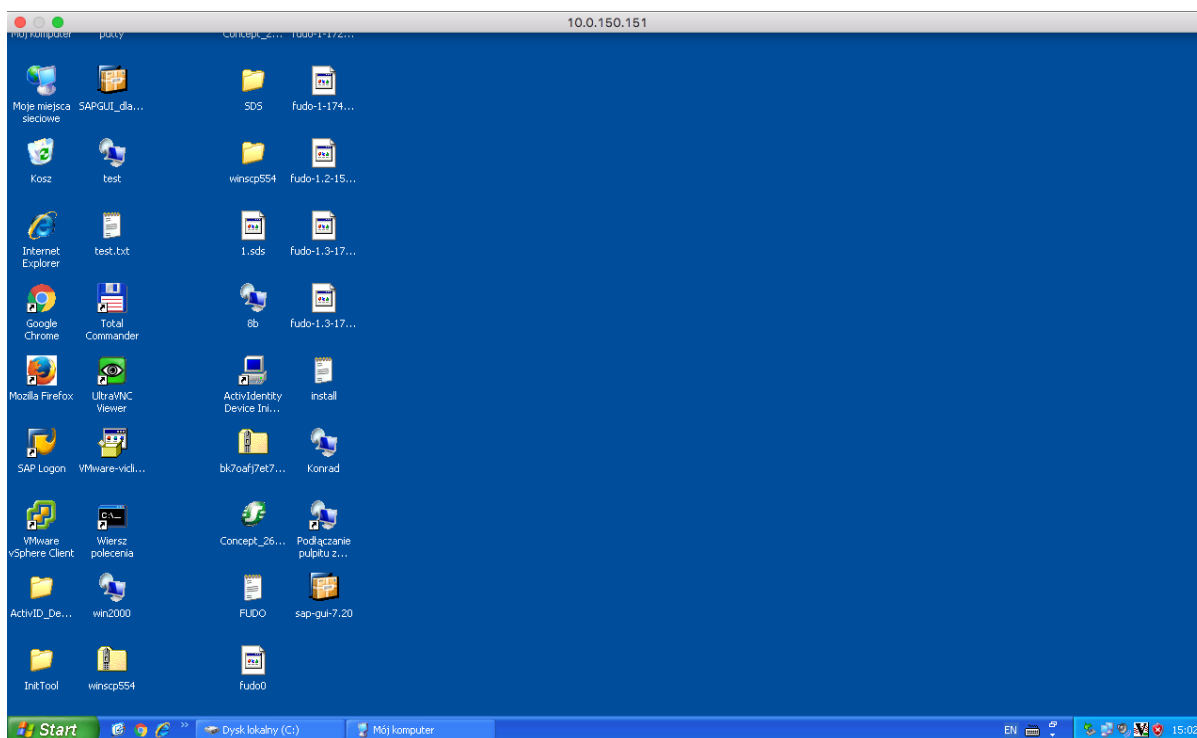
Password:

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.



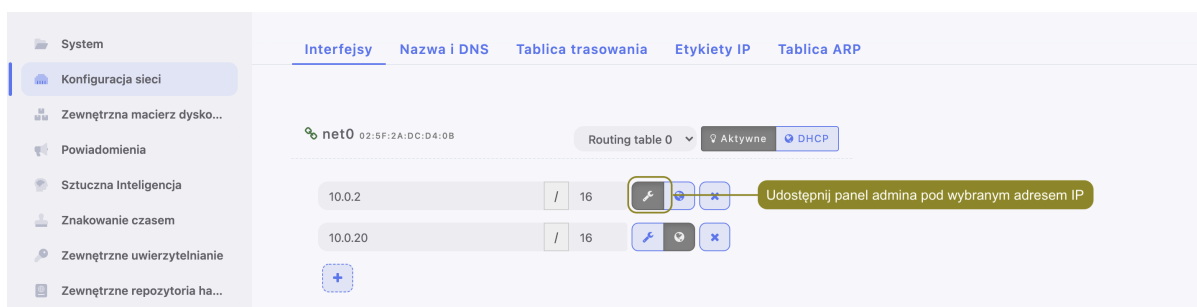
- W przypadku gdy wskazane konto nie istnieje, Fudo Enterprise dokona próby dopasowania podanego ciągu znaków do nazwy serwera. Jeśli system nie stwierdzi istnienia obiektu serwera o takiej nazwie, spróbuje dokonać dopasowania na podstawie nazwy DNS hosta.
- Fudo Enterprise pozwala na zastosowanie własnego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



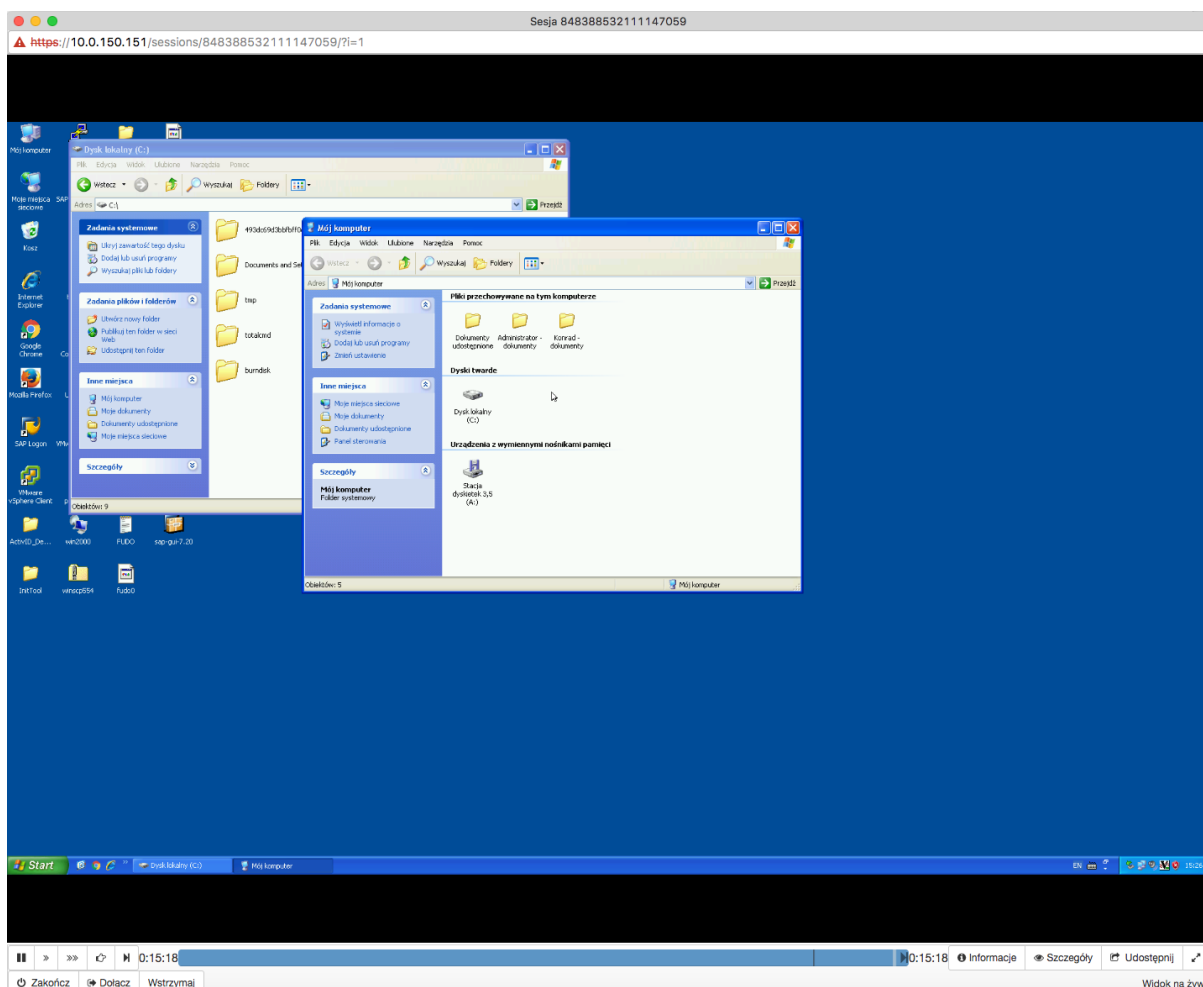
5.4.4 Podgląd sesji połączeniowej

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

Informacja: Upewnij się, że wprowadzony 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 Enterprise.
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 Enterprise, 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 Enterprise 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 Enterprise nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu przez

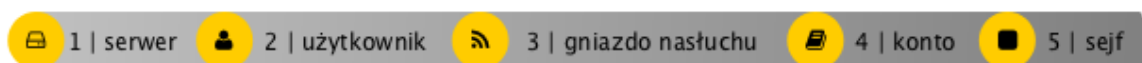
Fudo Enterprise musi uwierzytelnić się na serwerze docelowym po zestawieniu połączenia.



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	X
Zablokowane	X
Protokół	Telnet
Adres źródłowy	Dowolny
Użyj szyfrowania TLS	X
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	X
<i>Adresy serwerów</i>	
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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Połączenie</i>	
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
<i>Ogólne</i>	
Nazwa	admin_telnet_server
Zablokowane	✘
Typ	forward
Nagrywanie sesji	wszystko
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	telnet_server
<i>Dane uwierzytelniające</i>	
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
<i>Ogólne</i>	
Nazwa	telnet_safe
Zablokowane	
Powiadomienia	
Powód logowania	
Wymagaj potwierdzenia	
Polityki	
Note access	No access
<i>Funkcjonalność protokołów</i>	
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 Enterprise:

```
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 Enterprise.

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 Enterprise.
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 Enterprise, której celem jest monitorowanie połączeń Telnet 5250 ze zdalnym serwerem. Scenariusz zakłada, że

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

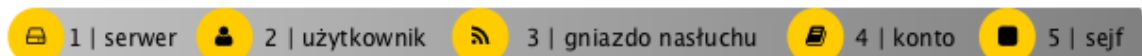
Informacja: Połączenia telnet realizowane za pośrednictwem Fudo Enterprise nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu przez Fudo Enterprise musi uwierzytelnić się na serwerze docelowym po zestawieniu połączenia.



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	X
Zablokowane	X
Protokół	Telnet 5250
Adres źródłowy	Dowolny
Użyj szyfrowania TLS	X
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	X
<i>Adresy serwerów</i>	
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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Połączenie</i>	
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), zwykle (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
<i>Ogólne</i>	
Nazwa	admin_telnet_server
Zablokowane	✘
Typ	forward
Nagrywanie sesji	wszystko
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	telnet_server
<i>Dane uwierzytelniające</i>	
Zastęp 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
<i>Ogólne</i>	
Nazwa	telnet_safe
Zablokowane	
Powiadomienia	
Powód logowania	
Wymagaj potwierdzenia	
Polityki	
Note access	No access
<i>Funkcjonalność protokołów</i>	
RDP	
SSH	
VNC	

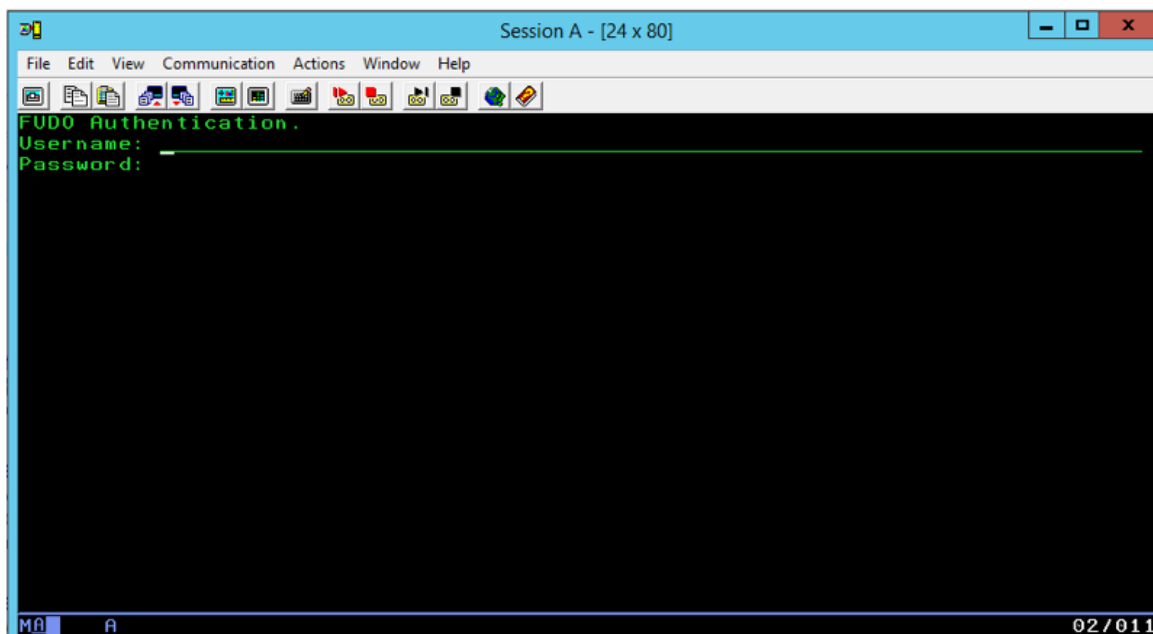
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto *admin_telnet_server* i kliknij
11. Kliknij *OK*.
12. Kliknij w kolumnie *Gniazda nasłuchiwania*.
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 '^]'.
```

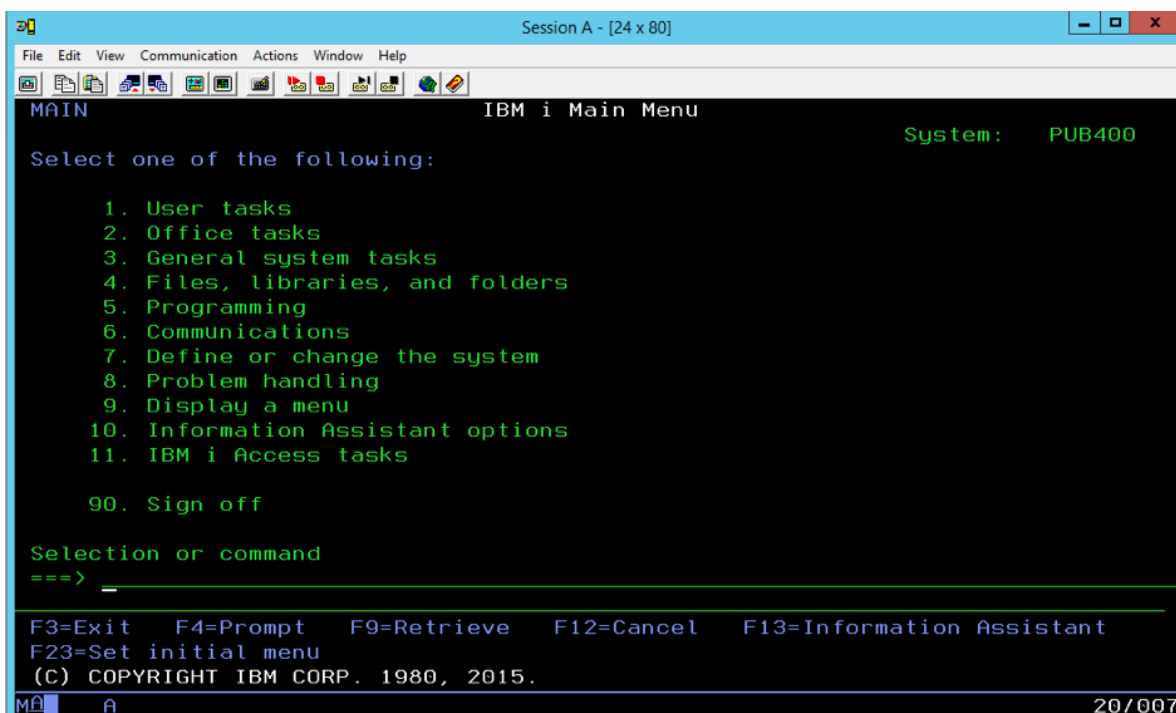
3. Wprowadź dane uwierzytelniające użytkownika na Fudo Enterprise.



4. Wprowadź dane uwierzytelniające użytkownika na serwerze:

```
FreeBSD/amd64 (fbsd83-cerb.wh1) (pts/0)
login:
password:
```

Informacja: Połączenia telnet nie wspierają mechanizmów podmiiany danych logowania.



5.6.4 Podgląd sesji połączeniowej

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

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


```

MAIN                               IBM i Main Menu                               System:  PUB400
Select one of the following:
  1. User tasks
  2. Office tasks
  3. General system tasks
  4. Files, libraries, and folders
  5. Programming
  6. Communications
  7. Define or change the system
  8. Problem handling
  9. Display a menu
 10. Information Assistant options
 11. IBM i Access tasks
 90. Sign off

Selection or command
==>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2015.

```

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 Enterprise, 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 Enterprise 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*).

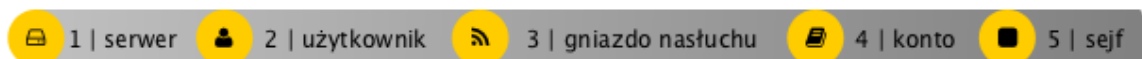


Ostrzeżenie: Domyślny plugin serwera MySQL `caching_sha2_password` nie jest obecnie wspierany przez Fudo Enterprise. Wspierane plugin'y dla połączeń MySQL przez Fudo Enterprise - to są `mysql_native_password` oraz `mysql_old_password`. Plugin Serwera powinien być ustawiony do `mysql_native_password` 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
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Adresy serwerów</i>	
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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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
<i>Ogólne</i>	
Nazwa	mysql_listener
Zablokowane	✘
Protokół	MySQL
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Połączenie</i>	
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 podmianną 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
<i>Ogólne</i>	
Nazwa	admin_mysql_server
Zablokowane	✘
Typ	regular
Nagrywanie sesji	wszystko
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	mysql_server
<i>Dane uwierzytelniające</i>	
Domena	✘
Login	admin
Zastęp 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:

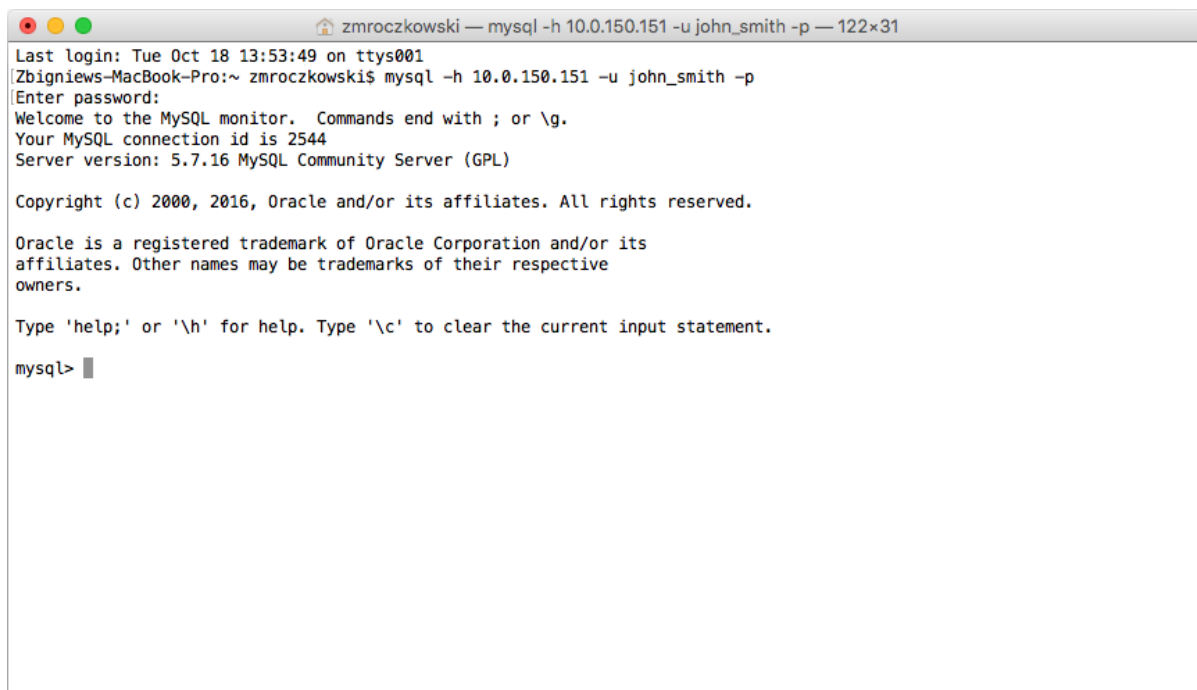
Parametr	Wartość
<i>Ogólne</i>	
Nazwa	mysql_safe
Zablokowane	
Powiadomienia	
Powód logowania	
Wymagaj potwierdzenia	
Polityki	
Note access	No access
<i>Funkcjonalność protokołów</i>	
RDP	
SSH	
VNC	

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.



```
zmroczkowski — mysql -h 10.0.150.151 -u john_smith -p — 122x31
Last login: Tue Oct 18 13:53:49 on ttys001
Zbigniew-MacBook-Pro:~ zmroczkowski$ mysql -h 10.0.150.151 -u john_smith -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2544
Server version: 5.7.16 MySQL Community Server (GPL)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> █
```

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 Enterprise.

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

Sesja 84838853211147061
<https://10.0.150.151/sessions/84838853211147061/?i=1&qj=on&qc=on&live=2016-10-18+03%3A17%3A59&qo=on>

Sesja: 84838853211147061, użytkownik: john_smith, serwer: mysql_server Zakończ

INIT 2016-10-18 03:17:33.035478

Wersja protokołu: 10 Wersja serwera: 5.7.16 Identyfikator połączenia: 2544 Nazwa wtyczki uwierzytelnienia: mysql_native_password
 Funkcjonalności: CLIENT_IGNORE_SPACE, CLIENT_RESERVED, CLIENT_PLUGIN_AUTH, CLIENT_INTERACTIVE, CLIENT_SECURE_CONNECTION, CLIENT_MULTI_RESULTS, CLIENT_CONNECT_ATTRS, CLIENT_NO_SCHEMA, CLIENT_TRANSACTIONS, CLIENT_IGNORE_SIGPIPE, CLIENT_LONG_FLAG, CLIENT_CONNECT_WITH_DB, CLIENT_FOUND_ROWS, CLIENT_PLUGIN_AUTH_LENENC_CLIENT_DATA, CLIENT_LOCAL_FILES, CLIENT_COMPRESS, CLIENT_MULTI_STATEMENTS, CLIENT_LONG_PASSWORD, CLIENT_ODBC, CLIENT_PS_MULTI_RESULTS, CLIENT_PROTOCOL_41

OK 2016-10-18 03:17:33.035478

Zmienione wiersze: 0 Ostatnio wstawione ID: 0 Stan: 2 Ostrzeżenie: 0 Informacja:

COM_QUERY 2016-10-18 03:17:33.037478

Zapytanie:

```
select @@version_comment limit 1
```

00:00:00 00:01:18 Informacje Udostępnij
Zakończ Wstrzymaj

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*
- *Zasoby*

5.8 MS SQL

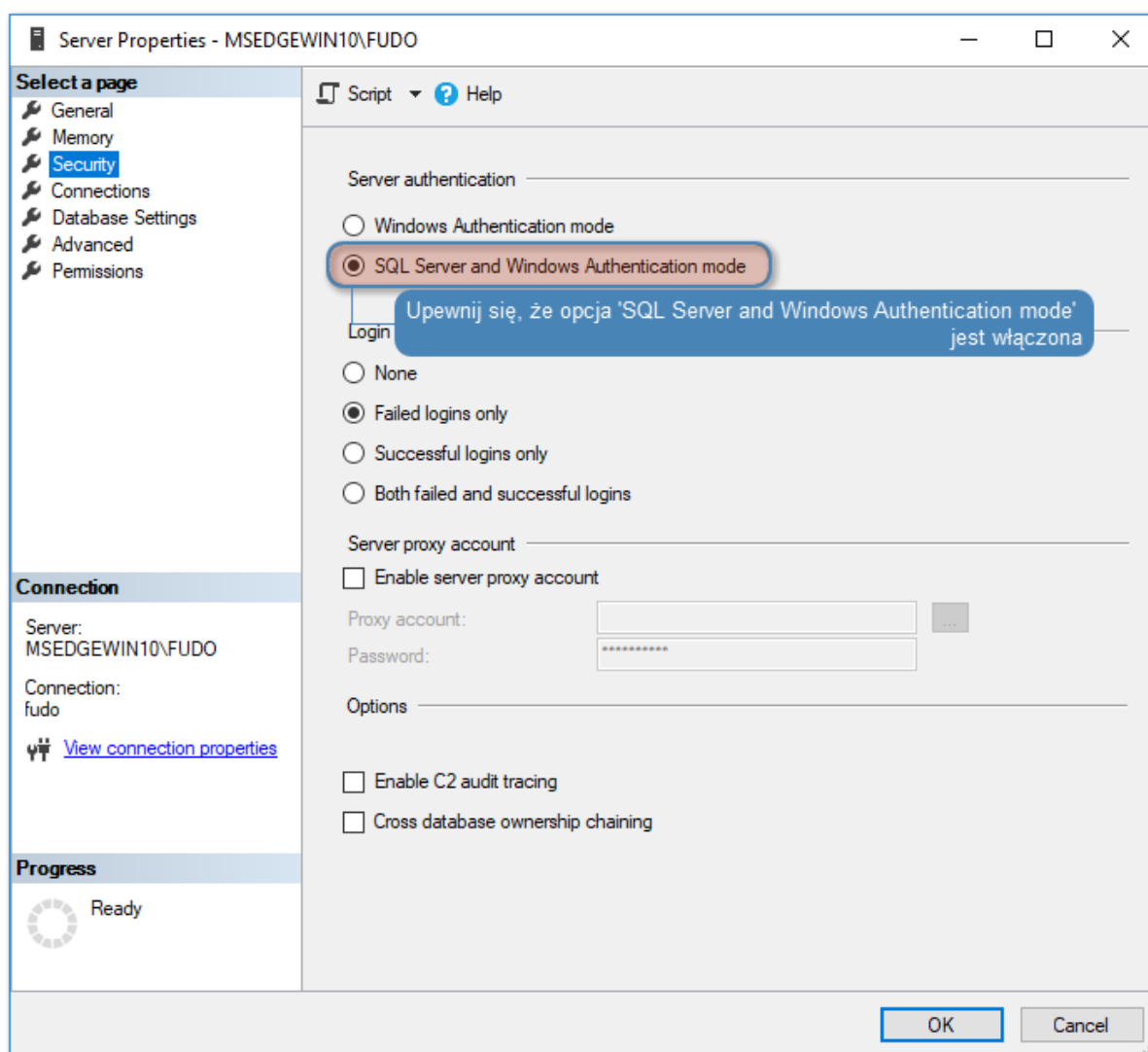
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie połączeń ze zdalnym serwerem baz danych MS SQL. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta *SQL Server Management Studio*, używając indywidualnego loginu i hasła. Fudo Enterprise 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*).



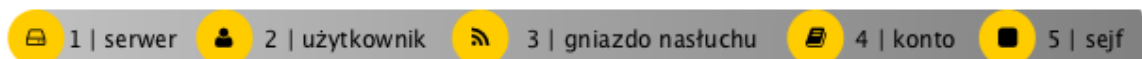
5.8.1 Założenia

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	X
Zablokowane	X
Protokół	MS SQL (TDS)
Adres źródłowy	Dowolny
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	X
<i>Adresy serwerów</i>	
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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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
<i>Ogólne</i>	
Nazwa	MSSQL_proxy
Zablokowane	✘
Protokół	MS SQL (TDS)
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Połączenie</i>	
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 podmianną 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
<i>Ogólne</i>	
Nazwa	admin_mssql_server
Zablokowane	✘
Typ	regular
Nagrywanie sesji	wszystko
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	mssql_server
<i>Dane uwierzytelniające</i>	
Domena	✘
Login	fudo
Zastęp 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:

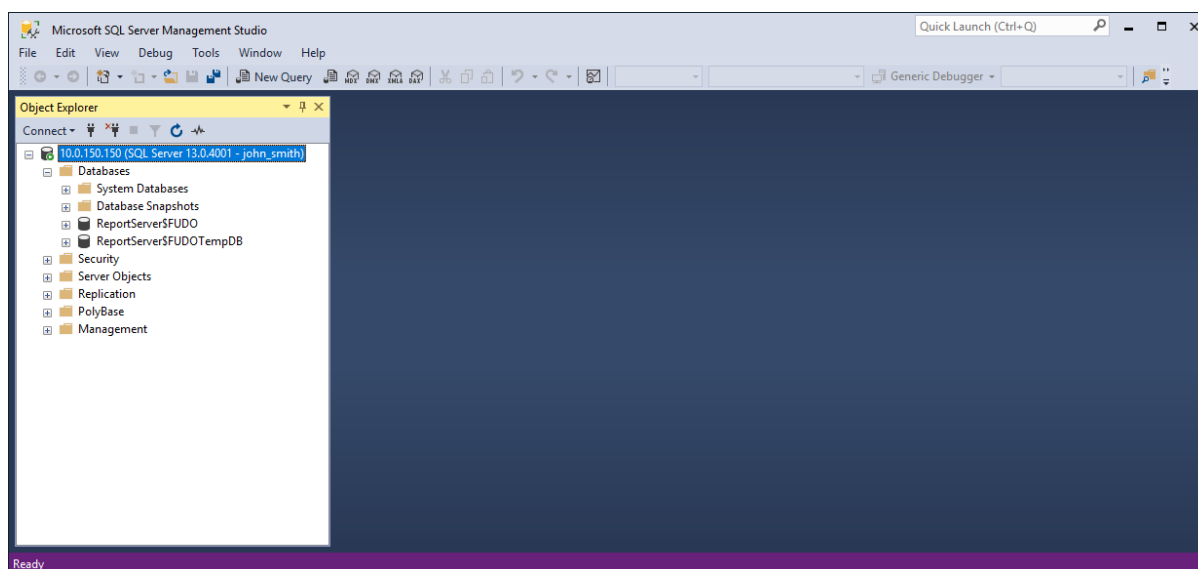
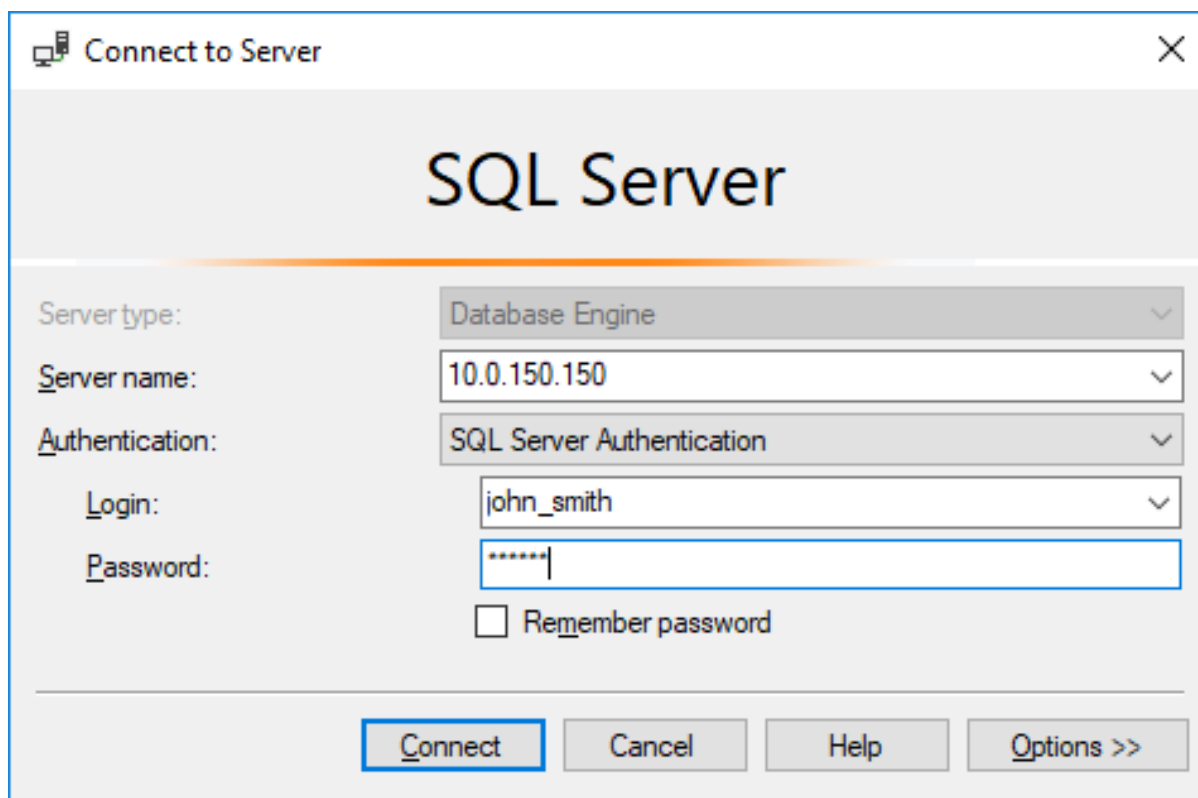
Parametr	Wartość
<i>Ogólne</i>	
Nazwa	mssql_safe
Zablokowane	
Powiadomienia	
Powód logowania	
Wymagaj potwierdzenia	
Polityki	
Note access	No access
<i>Funkcjonalność protokołów</i>	
RDP	
SSH	
VNC	

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 Enterprise.

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 Enterprise.
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 Enterprise.

Fudo Enterprise działa według algorytmu, weryfikującego, czy obiekty nowej sesji (**gniazdo nasłuchiwania**, **konto**, **adres serwera (serwer)**, **użytkownik**, oraz **sejf**) są takie same, jak obiekty któreś 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*
- *Zasoby*

5.9 HTTP

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, 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.

<p>Ostrzeżenie: Renderowanie sesji HTTP jest wymagającym procesem i może mieć negatywny wpływ na ogólną wydajność systemu. Monitorowanie rednerowanych połączeń HTTP</p>

zaleca się na maszynach fizycznych, z uwzględnieniem następujących limitów dla jednoczesnych połączeń HTTP.

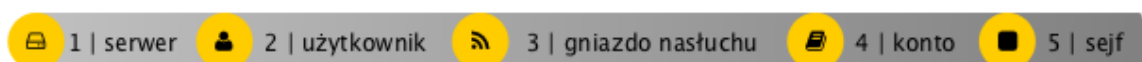
Model	Maksymalna zalecana liczba jednoczesnych połączeń HTTP*
F100x	2
F300x	5
F500x	10

*Rzeczywista maksymalna liczba obsługiwanych sesji HTTP uwarunkowana jest konfiguracją danej instancji Fudo Enterprise.

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 serwer*.
3. Uzupełnij parametry konfiguracyjne serwera:

Parametr	Wartość
Nazwa	twitter
Opis	✘
Zablokowane	✘
Protokół	HTTP
TLS włączony	✔
Starszy szyfr	✘
HTTP host	✘
Czas oczekiwania HTTP	900
Uwierzytelnienie HTTP	Twitter
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Adresy serwerów</i>	
Adres	twitter.com
Maska	32
Port	443
Weryfikacja serwera	Brak

4. Kliknij *Zapisz* albo *Zapisz i wyjdź*

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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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
<i>Ogólne</i>	
Nazwa	twitter_listener
Zablokowane	
Protokół	HTTP
Renderuj sesje	
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	
<i>Połączenie</i>	
Tryb połączenia	Pośrednik
Adres lokalny	10.0.236.70
Port	997
Użyj szyfrowania TLS	
Starszy szyfr	
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 podmianną 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
<i>Ogólne</i>	
Nazwa	twitter_admin
Zablokowane	✘
Typ	regular
Nagrywanie sesji	wszystko
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji	✘
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	twitter
<i>Dane uwierzytelniające</i>	
Domena	✘
Login	Tweety
Zastęp 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*.

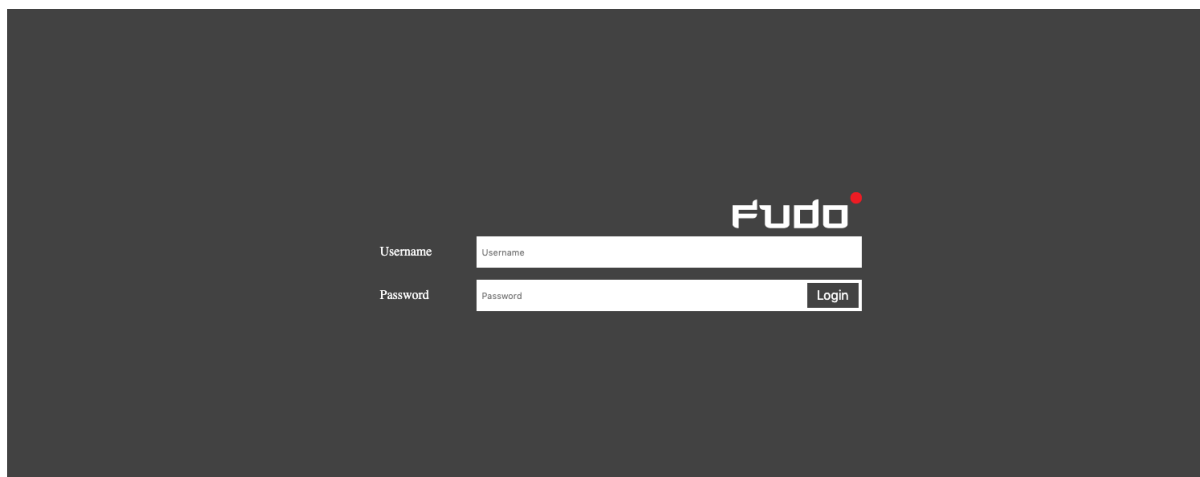
Parametr	Wartość
<i>Ogólne</i>	
Nazwa	http_safe
Zablokowane	X
Powiadomienia	X
Powód logowania	X
Wymagaj potwierdzenia	X
Polityki	X
Note access	No access
<i>Funkcjonalność protokołów</i>	
RDP	X
SSH	X
VNC	X

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*.

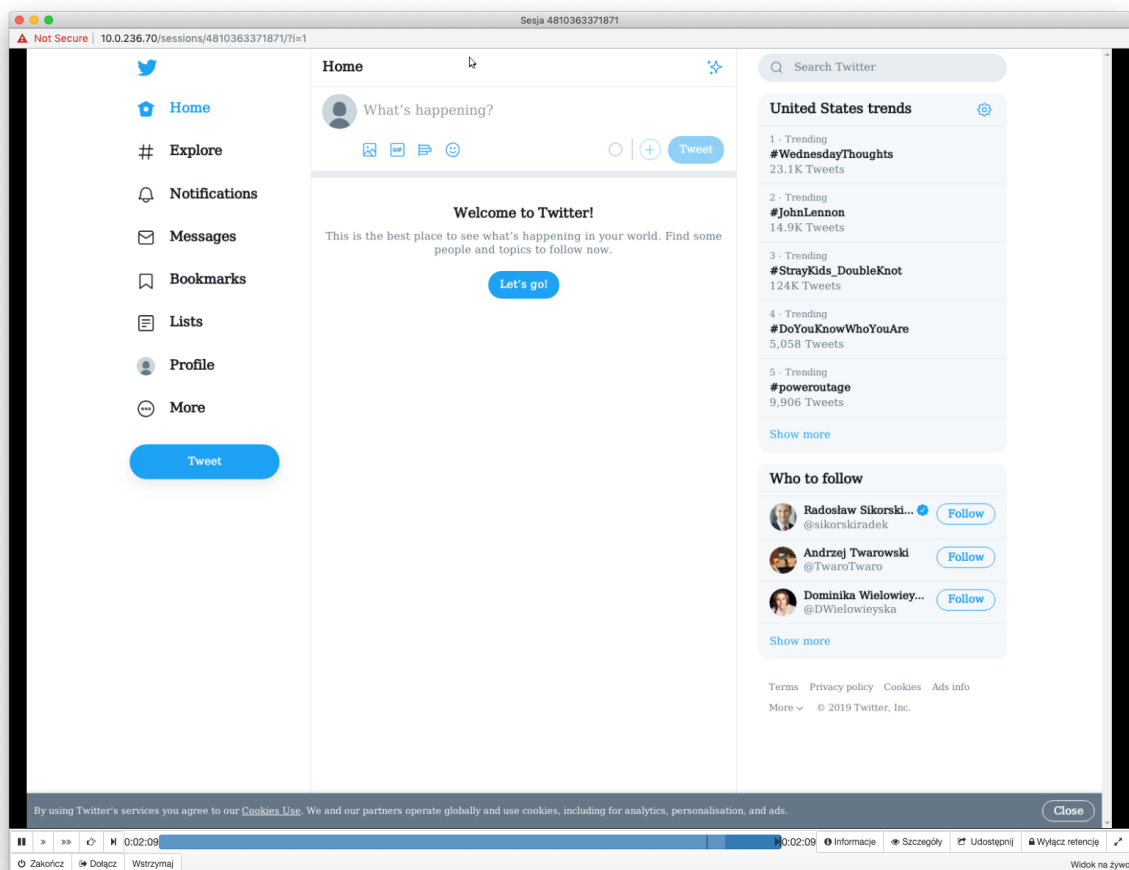
Informacja: W przypadku uwierzytelniania dwuskładnikowego, wprowadź hasło statyczne wraz ze składnikiem dynamicznym (wskazanie tokena) jako jeden ciąg znaków.



4. Kontynuuj przeglądanie serwisu.

5.9.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Fudo Enterprise.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Fudo Enterprise.
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 VNC

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, 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 Enterprise używając własnego loginu i hasła (*john_smith/john*). Fudo Enterprise zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła.

Informacja: Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedy-

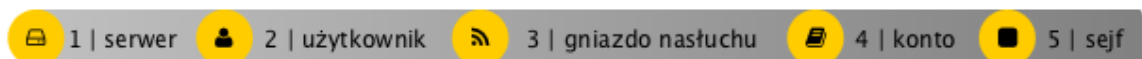
nie hasła, login zdefiniowany w koncie typu *regular* jest ignorowany przy zestawianiu połączenia.



5.10.1 Założenia

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

5.10.2 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
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Adresy serwerów</i>	
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
<i>Ogólne</i>	
Login	john_smith
Rola	user
Zablokowane	X
Ważność konta	Bezterminowe
<i>Zakładka Ustawienia</i>	
Sejfy	X
<i>Zakładka Dane Użytkownika</i>	
Domena Fudo	X
Domena AD	X
Baza LDAP	X
Imię i nazwisko	John Smith
Email	X
Organizacja	X
Telefon	X
<i>Sekcja Uwierzytelnienie</i>	
Niepowodzenia uwierzytelnienia	X
Zastosuj złożoność hasła	X
Dodaj metodę uwierzytelnienia	Hasło statyczne
Hasło	john
<i>Zakładka Uprawnienia</i>	
Uprawnieni użytkownicy	X

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	X
Protokół	VNC
Komunikat	X
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	X
<i>Połączenie</i>	
Tryb połączenia	proxy
Adres lokalny	10.0.150.151
Port	5900
Adres zewnętrzny	X
Port zewnętrzny	X

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
<i>Ogólne</i>	
Nazwa	admin_vnc_server
Zablokowane	✘
Typ	regular
Nagrywanie sesji	wszystko
OCR sesji	✔
Język OCR	Angielski
Notatki	✘
<i>Retencja danych</i>	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	61 dni
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Serwer</i>	
Serwer	vnc_server
<i>Dane uwierzytelniające</i>	
Domena	✘
Login	✘
Zastęp sekret	hasłem
Hasło	root
Powtórz hasło	root
Polityka modyfikatora hasła	✘

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.

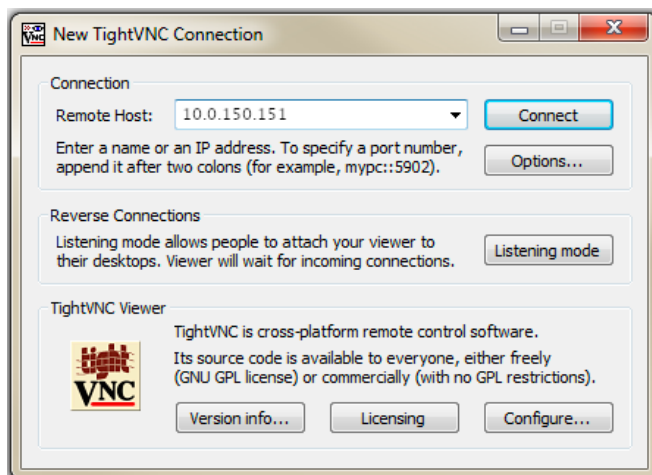
1. Wybierz z lewego menu *Zarządzanie > Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	vnc_safe
Zablokowane	✘
Powiadomienia	✘
Powód logowania	✘
Wymagaj potwierdzenia	✘
Polityki	✘
Note access	No access
<i>Funkcjonalność protokołów</i>	
RDP	✘
SSH	✘
VNC	✔
<i>Uprawnienia</i>	
Uprawnieni użytkownicy	✘
<i>Powiązania obiektu</i>	
admin_vnc_server	vnc_listener

4. Kliknij *Zapisz*.

5.10.3 Nawiązanie połączenia

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



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

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

Tematy pokrewne:

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

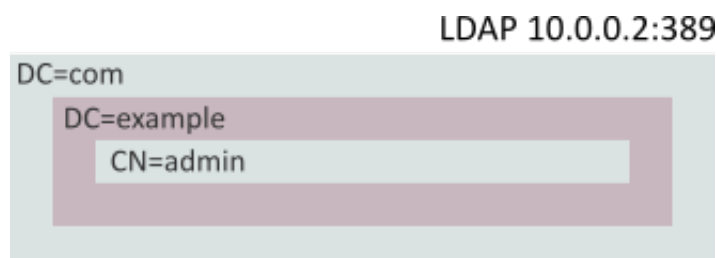
5.11 Uwierzytelnienie użytkowników w katalogu LDAP

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 Enterprise.

5.11.1 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`.





5.11.2 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	

Typ *

Adres hosta **Port** *

Wysyłaj żądania z

Bind DN *

Połączenie szyfrowane

Usuń

4. Kliknij *Zapisz*.

Dodanie metody uwierzytelnienia użytkownika

- Wybierz z lewego menu *Zarządzanie > Użytkownicy*.
- Odszukaj na liście i kliknij użytkownika *admin*.
- W polu *Baza LDAP* wprowadź ciąg definiujący obiekt *admin* w strukturze 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`).

- Kliknij *+ Dodaj metodę uwierzytelnienia*.
- Z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz *Zewnętrzne uwierzytelnienie*.
- Wybierz metodę „LDAP 10.0.0.2:389 bind dn:dc=example,dc=com” i kliknij *Zapisz*.
- Kliknij *Zapisz*, aby zapisać zmiany w definicji użytkownika.

Tematy pokrewne:

- *Uwierzytelnienie*
- *Dodawanie użytkownika*
- *Konfigurowanie monitorowania połączeń SSH*

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.

The screenshot displays the FUDO Enterprise user management interface. On the left is a sidebar with navigation options. The main content area is titled 'Użytkownicy' and includes a search bar, a filter dropdown menu, and a table of users. The filter menu is open, showing options like 'Nazwa', 'Rola', 'Organizacja', 'Email', 'Imię i nazwisko', 'Zablokowany', 'Zsynchronizowany z LDAP', and 'Przypisany sejf'. The table lists users: 'Test_User_4', 'Test_User_5', and 'Test_User_6'. Annotations highlight various UI elements: 'Odblokuj / Zablokuj wybranego Użytkownika', 'Odblokuj (1) / Zablokuj (1)', 'Usuń zaznaczone (2)', 'Dodaj użytkownika', 'Usuń wybranego Użytkownika', 'Dodaj Użytkownika', 'Filtruj Użytkowników', 'Zastosuj', 'Zablokowany Użytkownik', and 'Powód zablokowania'.

Informacja: Fudo Enterprise umożliwia importowanie definicji użytkowników z usług, takich jak Active Directory lub innych zgodnych z protokołem LDAP. Aby uzyskać więcej informacji na ten temat, przejdź do rozdziału *Synchronizacja użytkowników z LDAP*.

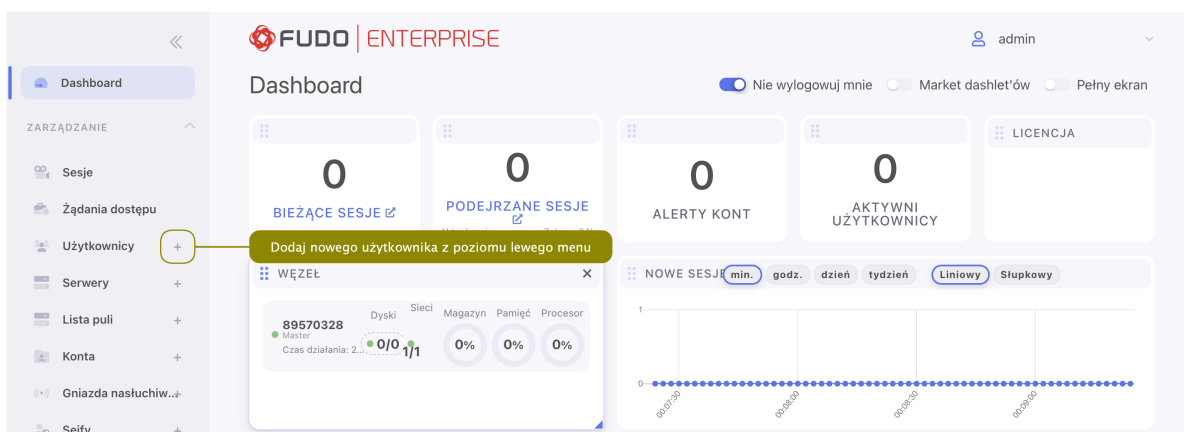
6.1 Dodawanie użytkownika

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.

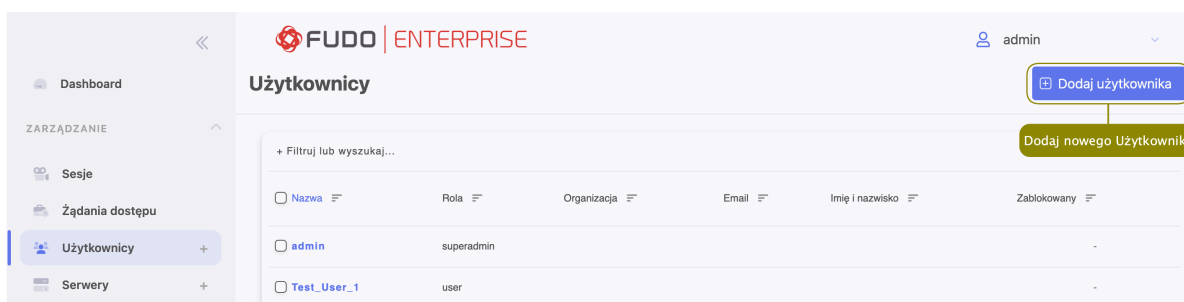
Ostrzeżenie: Tworząc obiekt Użytkownik dla połączeń MySQL, miej na uwadze, że domyślny plugin MySQL `mysql_caching_sha2_password` nie jest obecnie wspierany przez Fudo Enterprise. Wspierane plugin'y dla połączeń MySQL to: `mysql_native_password` oraz `mysql_old_password`. W celu zapewnienia kompatybilności plugin Serwera powinien być ustawiony na `mysql_native_password` w `/etc/mysql/mysql.conf.d/mysqld.cnf`, natomiast Użytkownik powinien być stworzony z plugin'em `mysql_native_password`.

Aby dodać definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

1. Kliknij **+** obok zakładki *Użytkownicy*, lub



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



3. Wprowadź nazwę użytkownika.

Ostrzeżenie: Symbole `%` oraz `#` nie są akceptowane w nazwie użytkownika.

Informacja:

- Model danych dopuszcza istnienie więcej niż jednego obiektu o tej samej nazwie, z zachowaniem unikalności kombinacji nazwy i domeny.
- Pole *Nazwa* nie rozróżnia wielkości liter.

4. Z rozwijanej listy *Rola* wybierz rolę użytkownika, która będzie determinować prawa dostępu.

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

Rola	Prawa dostępu
user	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • monitorowanie stanu systemu poprzez protokół SNMP.
operator	<ul style="list-style-type: none"> • 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 widżety widoku głównego: sesje równoległe, sesje podejrzone, 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 widżety widoku głównego: sesje równoległe, sesje podejrzone, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych.

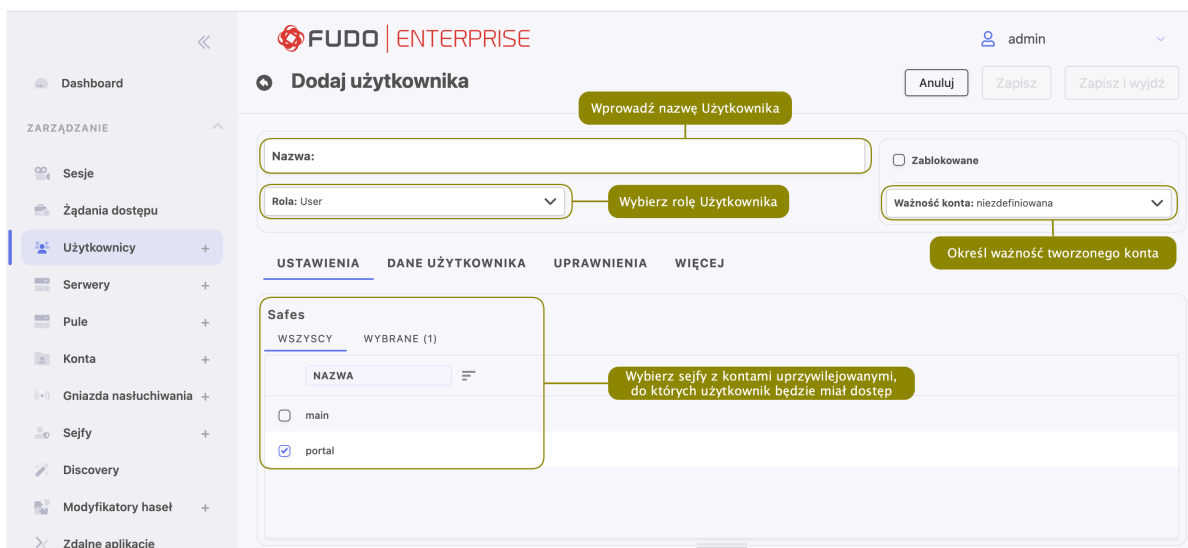
superadmin

- 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 widżety widoku głównego: sesje równoległe, sesje podejrzone, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych, licencja, dziennik zdarzeń systemowych.

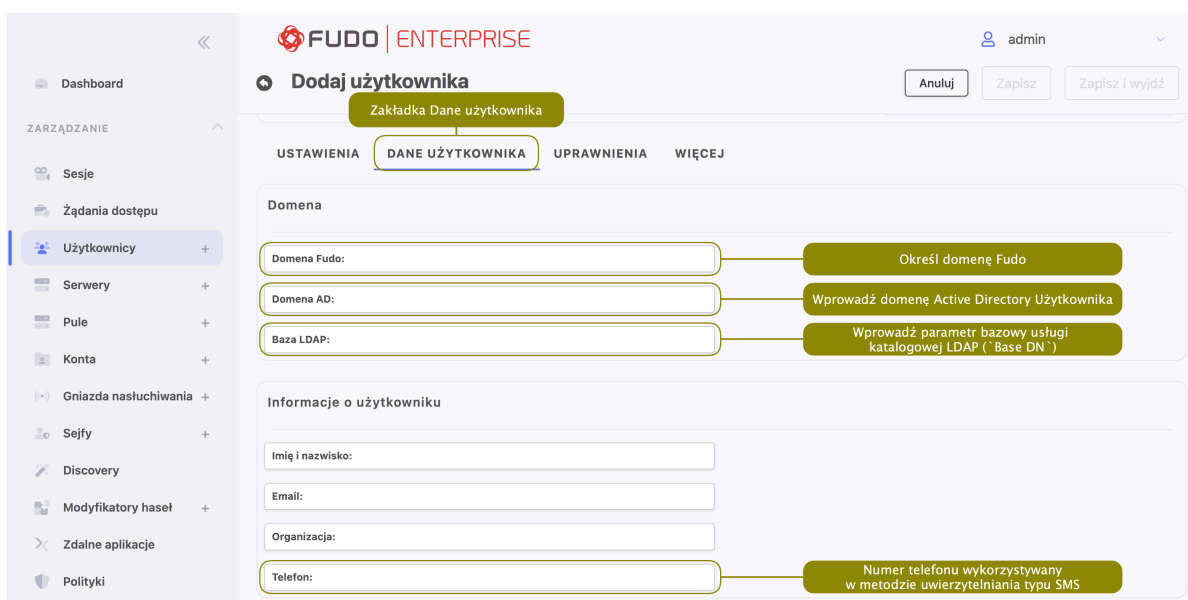
-
5. Zaznacz opcję *Zablokowane*, aby uniemożliwić użytkownikowi zalogowanie zaraz po utworzeniu konta.
 6. Określ ważność tworzonego konta.
 7. W zakładce *Ustawienia*, w polu *Sejfy* wybierz sejfy z kontami uprzywilejowanymi, do których użytkownik będzie miał dostęp.

Informacja:

- Definiowanie polityki czasu dostępu użytkownika do sejfu odbywa się z poziomu menu *Zarządzanie > Sejfy* - w tym celu zapoznaj się z rozdziałem *Dodawanie sejfu*.
-



8. W zakładce *Dane użytkownika*, w polu *Domena* określ *Domene Fudo*.



Informacja:

- *Domena Fudo* wykorzystywana jest do uwierzytelnienia użytkownika w systemie Fudo Enterprise.
- W przypadku zdefiniowania *Domeny Fudo* użytkownik będzie musiał podać ją przy logowaniu do panelu administracyjnego lub portalu użytkownika oraz podczas nawiązywania połączeń z monitorowanymi serwerami.
- Istnieje również możliwość skonfigurowania *Domeny domyślnej*, która dopuszcza dowolność. Jeśli *Domena domyślna* została podana, użytkownik ze skonfigurowaną *Domene Fudo* może ją wskazać podczas logowania ale nie jest to konieczne. Przejdź do rozdziału *Domyślna domena* w celu zapoznania się z zasadami działania tej opcji.

9. Wprowadź domene *Active Directory* użytkownika.

Informacja: Podczas gdy *domena Fudo* jest wykorzystywana do uwierzytelnienia użytkownika w systemie Fudo Enterprise, *domena AD* jest brana pod uwagę przy uwierzytelnianiu użytkownika przed serwerem, z którym nawiązuje sesję.

10. Wprowadź parametr bazowy usługi katalogowej LDAP (*Baza 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`.
-

11. W polu *Informacje o użytkowniku* wprowadź:

- pełne imię i nazwisko użytkownika,
- adres e-mail użytkownika,
- jednostkę organizacyjną użytkownika,
- numer telefonu użytkownika.

12. W zakładce *Uprawnienia* wciśnij przycisk *Zarządzaj* aby dodać użytkowników uprawnionych do zarządzania tworzonym obiektem, a w przypadku użytkowników o roli *Admin* i *Operator*, zdefiniuj prawo do zarządzania pozostałymi obiektami modelu danych, jak serwery, pule, konta, sejfy czy gniazda nasłuchiwania.
-

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

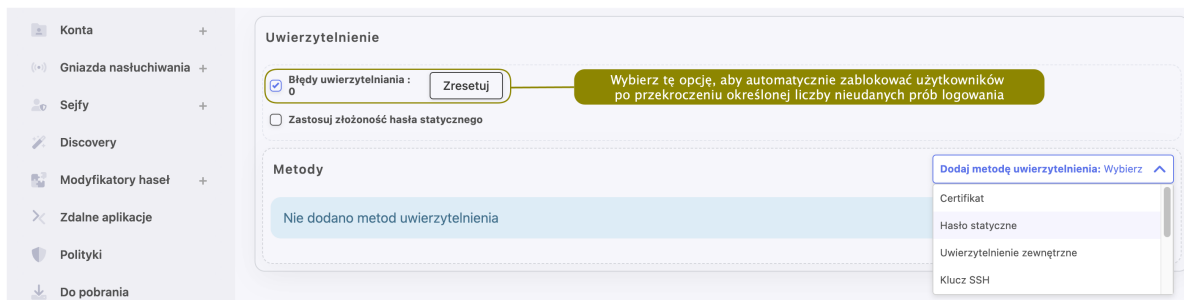
13. Jeśli użytkownik ma korzystać z funkcjonalności *Application to Application Password Manager*, w zakładce *Więcej*, w polu *AAPM* dodaj adres IP wykorzystywany przez *Access Gateway* oraz *AAPM* do komunikacji z Fudo Enterprise.
 14. Jeśli chcesz skonfigurować aplikację *Fudo Officer*, w polu *Fudo Officer* wciśnij przycisk *Dodaj urządzenie*. Następnie pobierz aplikację *Fudo Officer* ze sklepu *App Store* i zeskanuj wyświetlony kod QR, aby zakończyć powiązanie urządzenia mobilnego. Więcej informacji na ten temat znajdziesz w rozdziale *Fudo Officer 1.0*.
-

Informacja: W celu dodania urządzenia mobilnego, należy włączyć funkcję *Call Home*. Aby ją włączyć przejdź do *Settings > System*, do zakładki *General*, do sekcji *Serwisowanie i nadzór*.

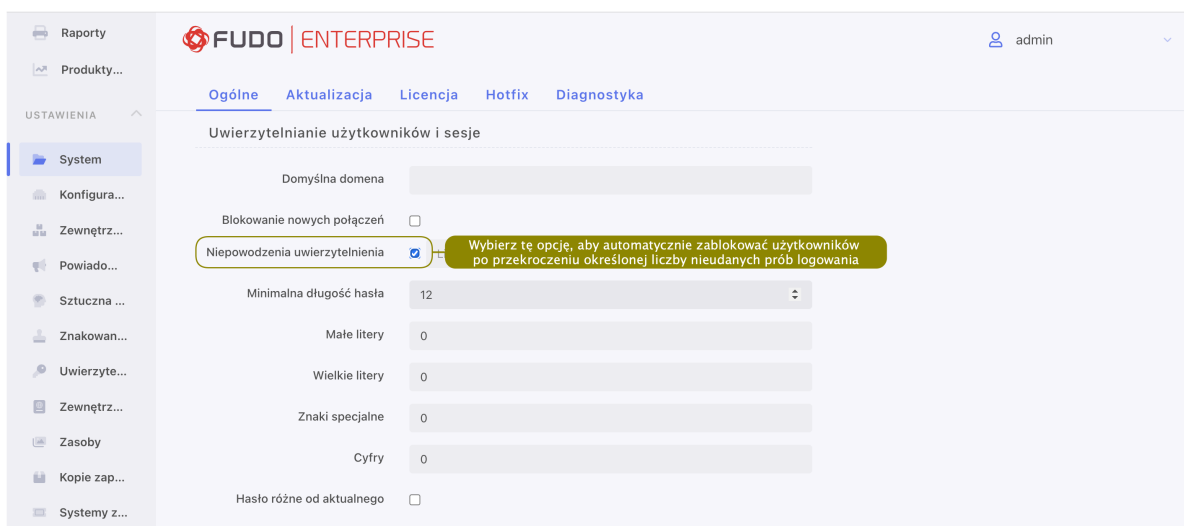
15. W polu *SNMP* kliknij opcję *Włączone* aby używać SNMP i wybierz metody uwierzytelnienia oraz szyfrowania z dostępnych list rozwijanych.
-

Informacja: Konfiguracja SNMP jest dostępna tylko dla użytkownika o roli *Service*.

16. Wróć do karty *Ustawienia* i w sekcji *Uwierzytelnienie* zaznacz opcję *Niepowodzenia uwierzytelnienia*, aby konto zostało automatycznie zablokowane w przypadku przekroczenia limitu nieudanych prób logowania.

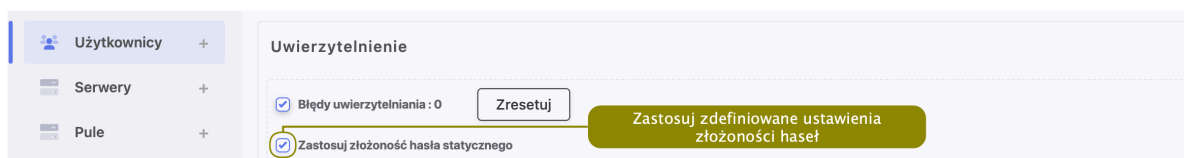


Informacja: Nieudane próby logowania są rejestrowane, jeśli włączona jest opcja *Niepowodzenia uwierzytelnienia* dla konkretnego użytkownika oraz w zakładce *Ustawienia > System*, w sekcji *Uwierzytelnianie użytkowników i sesje*.



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*.

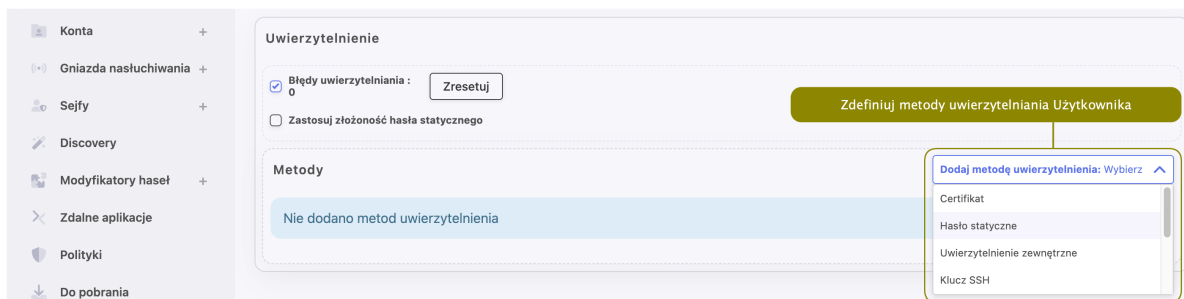


18. Określ sposób uwierzytelnienia użytkownika.

Informacja: Aby włączyć możliwość konfiguracji metod uwierzytelnienia, należy najpierw za-

pisać tworzony obiekt.

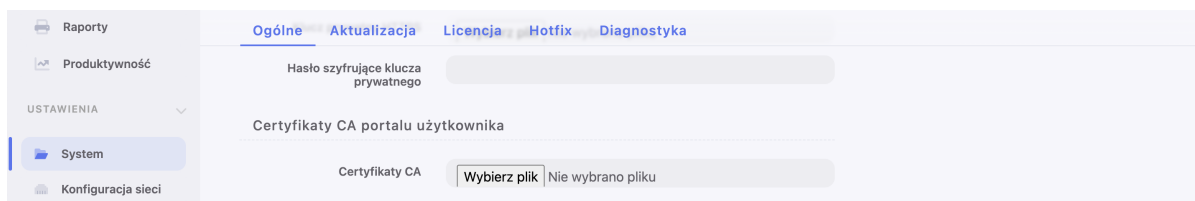
- Aby dodać metodę uwierzytelnienia, wybierz żądany typ z listy rozwijanej *Dodaj metodę uwierzytelnienia*. Poniżej znajduje się opis procedur specyfikacji dostępnych metod uwierzytelnienia.



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 w rozdziale: *Model uwierzytelniania w oparciu o certyfikaty*.

Hasło

- Wprowadź hasło w polu *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 bezpośrednio (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 *Zewnętrzne źródło uwierzytelnienia* wybierz źródło, które zostanie użyte do uwierzytelnienia użytkownika.

Informacja: Procedura definiowania zewnętrznych źródeł uwierzytelnienia opisana jest w roz-

dziale *Uwierzytelnienie*.

Klucz SSH

- W polu „Klucz publiczny” podaj klucz publiczny SSH używany do weryfikacji tożsamości użytkownika.

SMS

- W sekcji **Pierwszy składnik** wybierz i skonfiguruj *Hasło statyczne* lub *Uwierzytelnienie zewnętrzne* (AD lub LDAP).
- Wprowadź numer telefonu służący do procedury uwierzytelnienia w polu **Telefon**.

Informacja: Więcej informacji na temat konfiguracji SMS jako metody uwierzytelnienia znajdziesz w rozdziale: *Definicja uwierzytelnienia SMS*.

DUO

- W polu **Pierwszy składnik** wybierz i skonfiguruj *Hasło statyczne* lub *Uwierzytelnienie zewnętrzne* (AD albo LDAP).
- W polu **Drugi składnik**:
 - Wprowadź *Użytkownik DUO*.
 - Wprowadź *ID użytkownika DUO*.

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

OATH

- W polu **Pierwszy składnik** wybierz *Hasło statyczne* lub *Uwierzytelnienie zewnętrzne* (AD albo LDAP).
- W polu **Drugi składnik**:
 - Wybierz *Typ tokenu*.
 - Wprowadź sekret, który będzie użyty do generowania części dynamicznej hasła przez aplikację *Google Authenticator*. Sekret musi być zgodny z formatem **Base32**. Alternatywnie, kliknij przycisk *Generuj*, aby wygenerować go automatycznie lub *QRCode*, aby wyświetlić kod QR.
 - Określ *Długość tokenu*.
 - Określ wartość *Kroku czasowego*.
 - Jeśli wymagane, wybierz opcję *Zainicjowany*.

Przeczytaj więcej w rozdziale *Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator*.

API key

- Wpisz lub wygeneruj *Klucz API*.

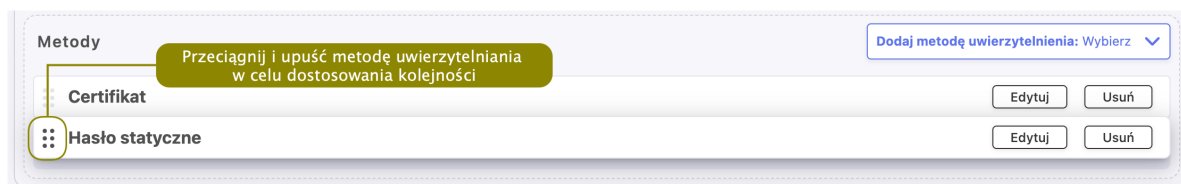
- Skopiuj wygenerowany klucz API w celu wykorzystania go w systemach, które wymagają uwierzytelnienia z użytkownikiem Fudo.

Informacja: Po zapisaniu klucza API nie ma możliwości jego podglądu.

20. W celu zdefiniowania kolejnych metod uwierzytelnienia wybierz nowy typ z listy rozwijanej *Dodaj metodę uwierzytelnienia*.

Informacja:

- W procesie uwierzytelnienia Fudo Enterprise 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 Enterprise próbuje uwierzytelnić użytkownika za pomocą kolejnych.
- W celu dostosowania kolejności metod uwierzytelnienia użyj funkcjonalności *przeciągnij i upuść*.



21. Kliknij *Zapisz* lub *Zapisz i wyjdź*

Tematy pokrewne:

- *Zliczanie niepowodzeń uwierzytelnienia*
- *Synchronizacja użytkowników z LDAP*
- *Domyślna domena*
- *Model danych*
- *Złożoność haseł*

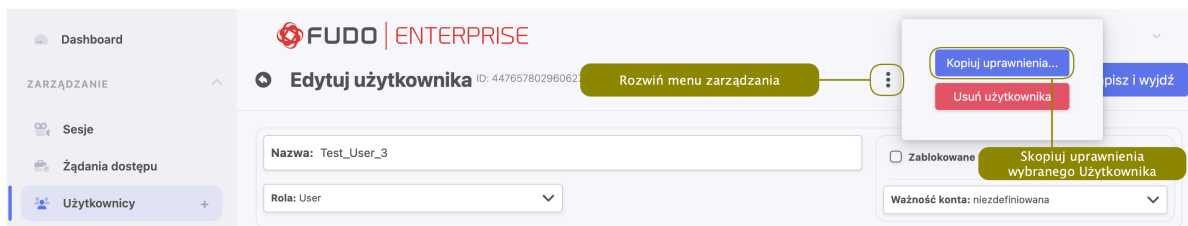
6.2 Kopiowanie uprawnień użytkownika

Funkcja „Kopiuj uprawnienia” umożliwia skopiowanie uprawnień od użytkownika o roli *Admin* lub *Operator* do użytkownika, który jest obecnie edytowany. Proces kopiowania polega na pobraniu uprawnień od wybranego użytkownika i zastosowaniu wszystkich różnic do użytkownika edytowanego.

Informacja: Aby skopiować uprawnienia od skonfigurowanego użytkownika, musisz najpierw zapisać definicję tworzonego użytkownika.

W celu kopiowania uprawnień z innej definicji użytkownika, postępuj zgodnie z poniższymi krokami:

1. Podczas edycji lub tworzenia nowej definicji użytkownika wybierz symbol trzech kropek obok przycisku „Anuluj”.
2. Wybierz przycisk *Kopiuj uprawnienia...*



3. Z listy rozwijanej *Kopiuj* z wybierz użytkownika, od którego zamierzasz skopiować uprawnienia.
4. Kliknij *Zapisz*.

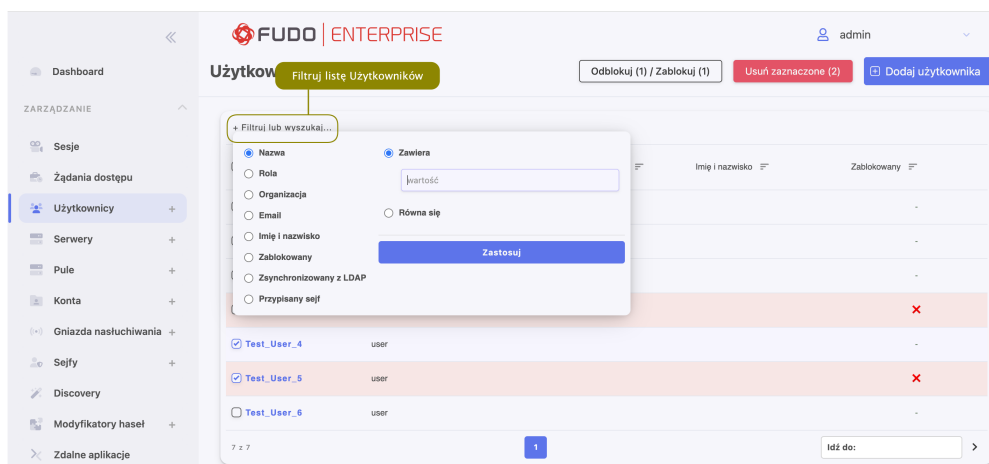
Related topics:

- *Synchronizacja użytkowników z LDAP*
- *Model danych*
- *Pierwsze uruchomienie*

6.3 Modyfikowanie użytkownika

Aby zmodyfikować definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

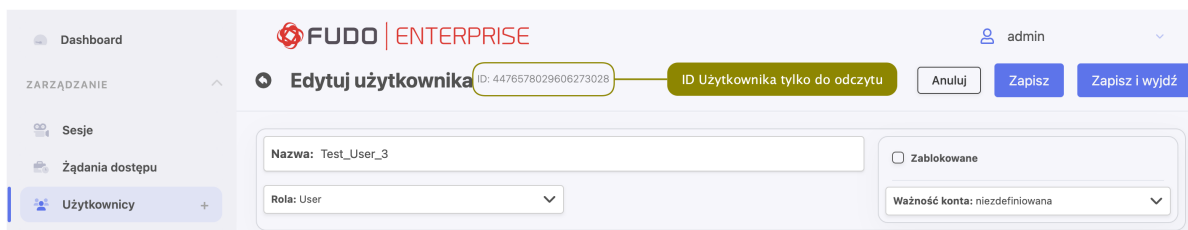
1. Wybierz z lewego menu *Zarządzanie > Użytkownicy*.
2. Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



3. Odszukaj na liście definicję użytkownika, którą chcesz edytować.
4. Kliknij nazwę użytkownika, aby edytować jego parametry konfiguracyjne.
5. Zmień parametry konfiguracyjne zgodnie z potrzebami.

Informacja:

- ID użytkownika jest identyfikatorem obiektu nadawanym automatycznie przez Fudo Enterprise i jest parametrem tylko do odczytu.



6. Kliknij *Zapisz* lub *Zapisz i wyjdź*.

Tematy pokrewne:

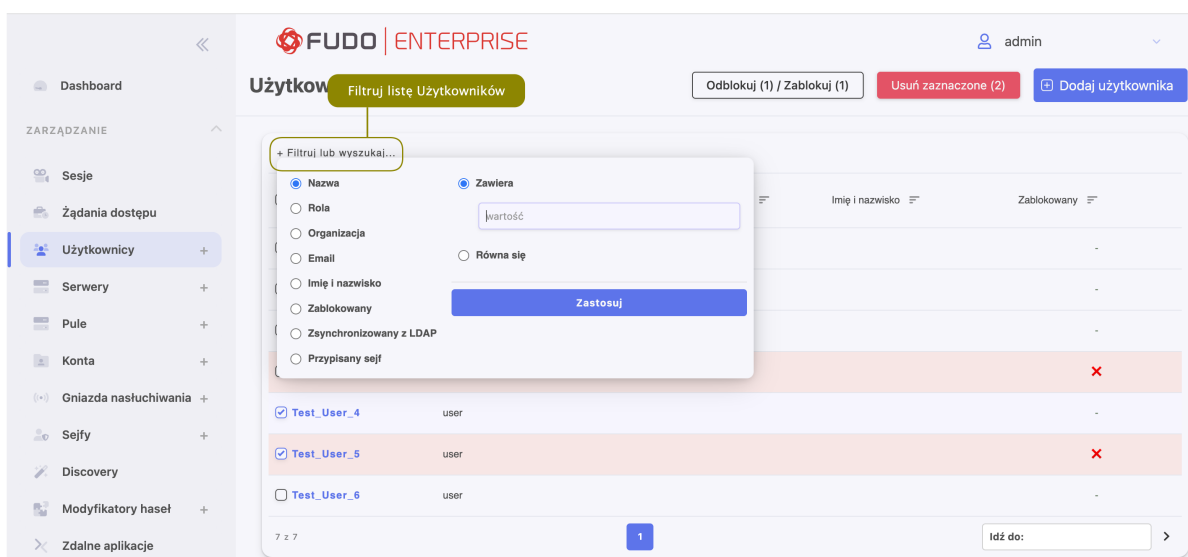
- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*

6.4 Blokowanie użytkownika

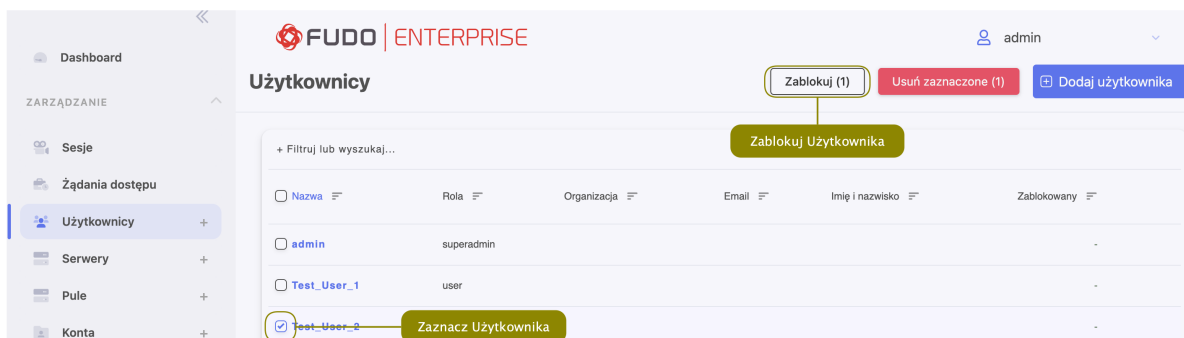
Aby zablokować użytkownikowi możliwość nawiązywania połączeń ze zdefiniowanymi zasobami, postępuj zgodnie z poniższą instrukcją.

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

1. Wybierz z lewego menu *Zarządzanie > Użytkownicy*.
2. Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



2. Odszukaj na liście i zaznacz użytkownika, którego chcesz zablokować.
3. Kliknij *Zablokuj*, aby zablokować użytkownikowi możliwość nawiązywania połączeń.

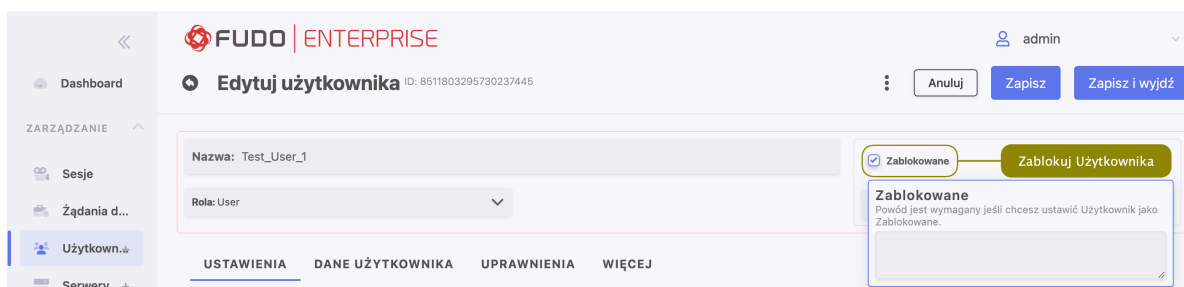


4. Wprowadź wymagany powód zablokowania zasobu i kliknij *Zablokuj*.

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

Konto użytkownika może zostać również zablokowane z poziomu formularza edycji obiektu. W tym celu:

- Edytuj wybraną definicję użytkownika.
- Zaznacz opcję *Zablokowane*.



- Wprowadź wymagany powód zablokowania zasobu.
- Kliknij *Zapisz* lub *Zapisz i wyjdź*

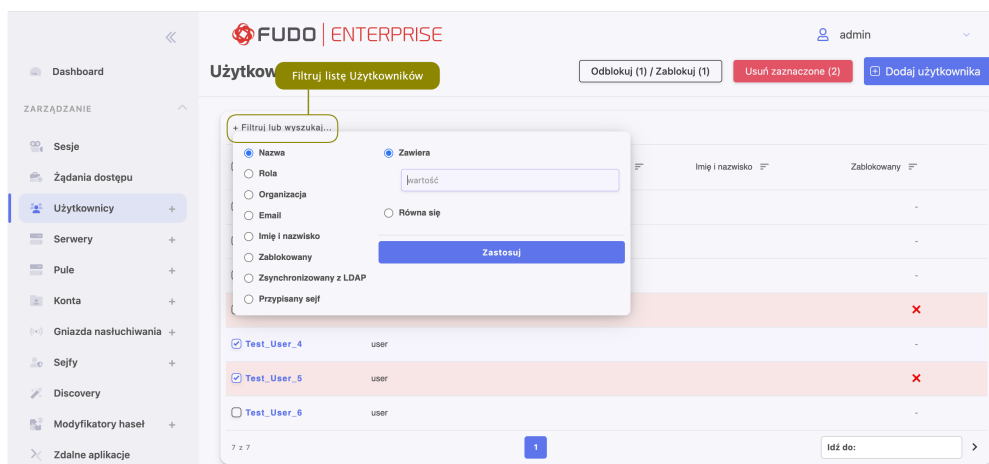
Tematy pokrewne:

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

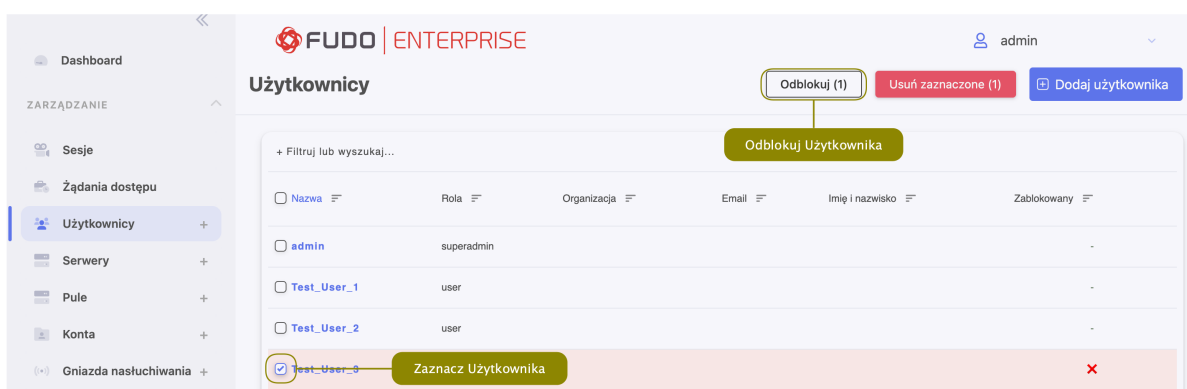
6.5 Odblokowanie użytkownika

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

1. Wybierz z lewego menu *Zarządzanie > Użytkownicy*.
2. Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



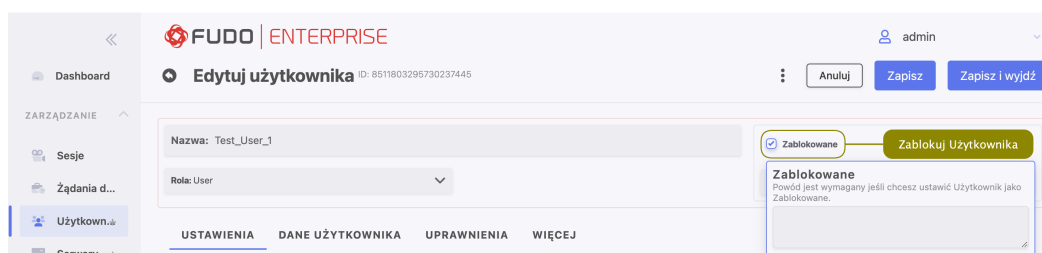
3. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.
4. Kliknij *Odblokuj*, aby umożliwić użytkownikowi nawiązywanie połączeń.



5. Kliknij *Odblokuj*, aby potwierdzić odblokowanie obiektu.

Konto użytkownika może zostać również odblokowane z poziomu formularza edycji obiektu. W tym celu:

- Edytuj wybraną definicję użytkownika.
- Odznacz opcję *Zablokowane*.



- Kliknij *Zapisz* lub *Zapisz i wyjdź*

Tematy pokrewne:

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

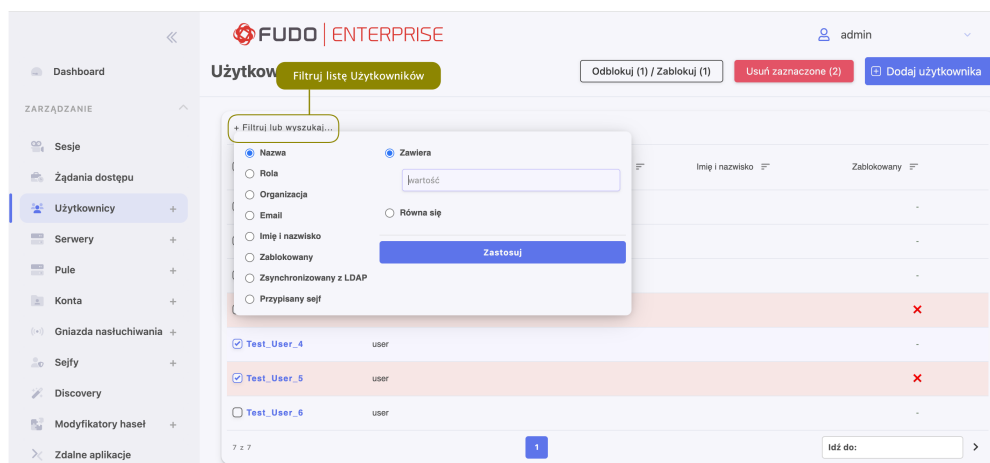
6.6 Usuwanie użytkownika

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. Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



3. Odszukaj na liście i zaznacz konta, które chcesz usunąć.
4. Kliknij *Usuń zaznaczone*.



5. Potwierdź operację usunięcia zaznaczonych obiektów.

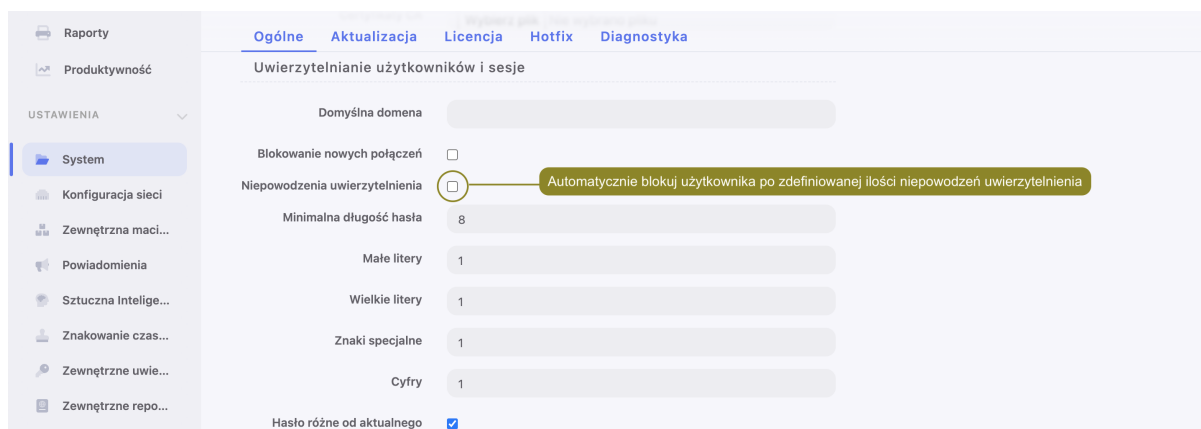
Tematy pokrewne:

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

6.7 Zliczanie niepowodzeń uwierzytelnienia

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

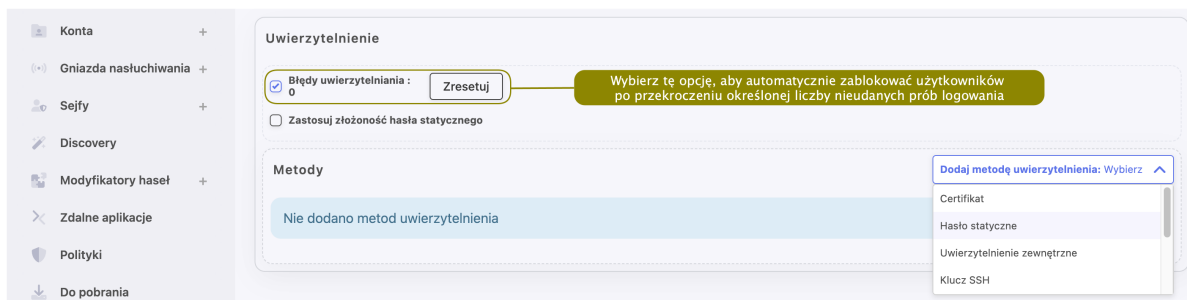
1. Wybierz z lewego menu *Ustawienia > System*.
2. W sekcji *Uwierzytelnianie użytkowników i sesje*, zaznacz opcję *Niepowodzenia uwierzytelnienia*.
3. Określ liczbę niepowodzeń uwierzytelnienia, po której konto użytkownika zostanie zablokowane.



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 Enterprise.

Rola	Prawa dostępu
user	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• monitorowanie stanu systemu poprzez protokół SNMP.
operator	<ul style="list-style-type: none">• 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 widżety widoku głównego: sesje równoległe, sesje podejrzone, 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 widżety widoku głównego: sesje równoległe, sesje podejrzone, 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 Enterprise pozwala

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

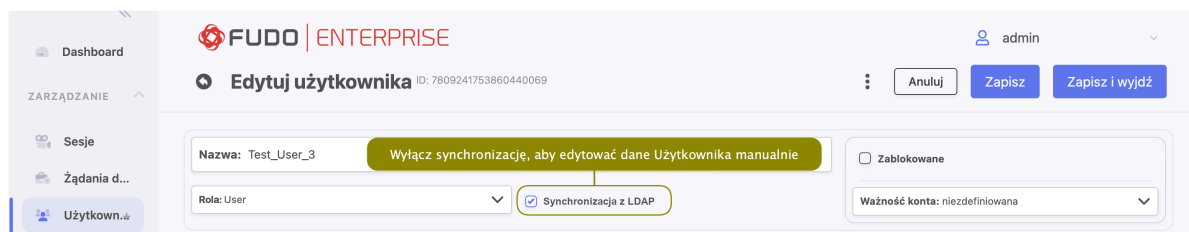
Ostrzeżenie: Dla skutecznej konfiguracji synchronizacji opartej o protokół LDAP jest konieczne wsparcie parametru `memberOf` na serwerze LDAP. Atrybut ten służy do wskazania grup, do których należy użytkownik.

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 Enterprise 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=wh1`).

Informacja: Synchronizacja użytkowników przechowywanych w strukturze LDAP wymaga:

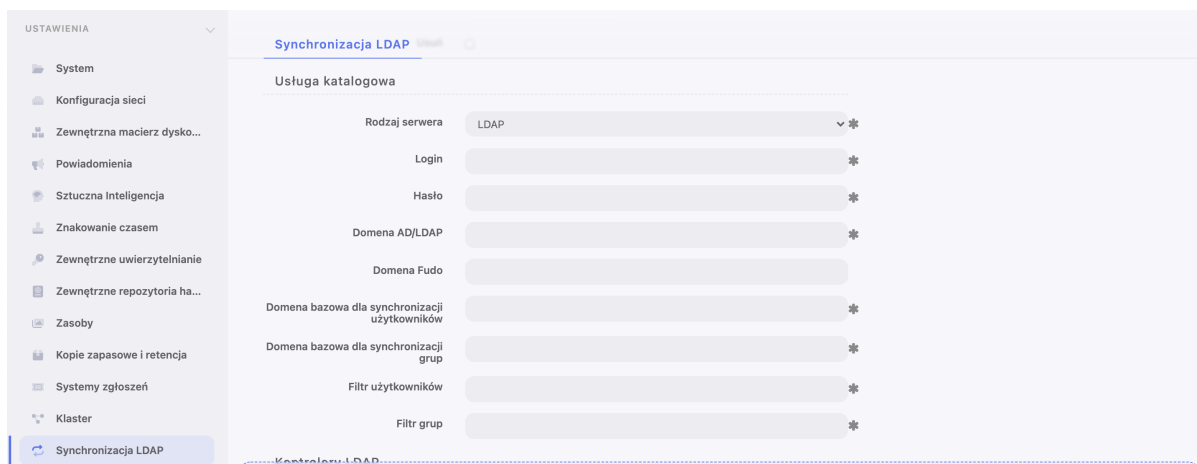
- użycia nakładki *memberOf*


- 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.

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



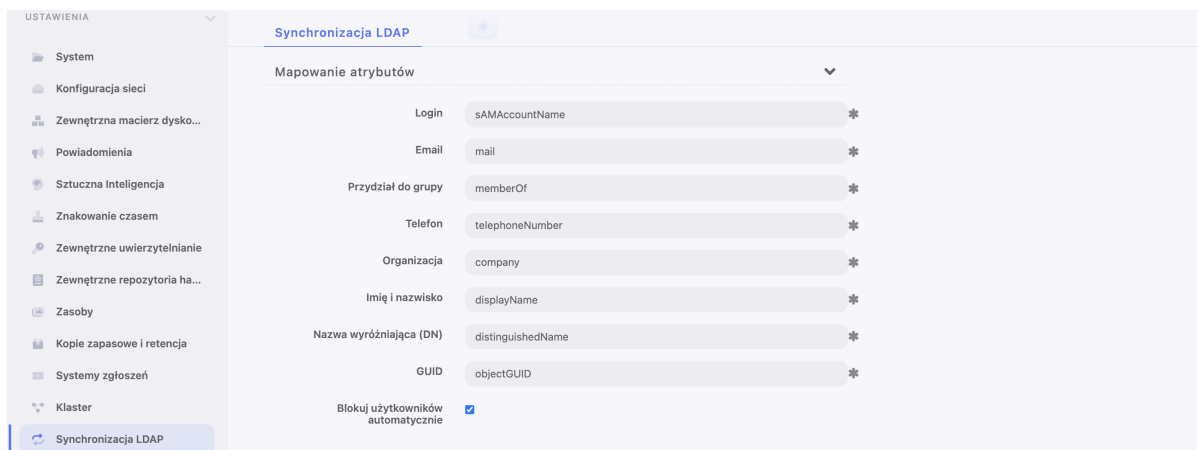
- Zaznacz opcję *Zablokuj automatycznie*, aby Fudo automatycznie zablokowało lokalne konta użytkowników, zablokowanych w usłudze katalogowej.
- Kliknij  w sekcji *Kontrolery LDAP*, aby zdefiniować host usługi katalogowej.
- Wprowadź adres IP serwera oraz numer portu, na którym dostępna jest usługa katalogowa.

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.


- Zaznacz opcję *Stronicuj wyniki LDAP*, aby włączyć stronicowanie danych zwracanych przez serwer LDAP.
- Zaznacz opcję *Połączenie szyfrowane* i wgraj certyfikat 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 uwierzytelnienia 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 Enterprise uwierzytelniając użytkownika będzie wysyłać zapytania do zewnętrznych źródeł uwierzytelniania w następującej kolejności:

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

24. W sekcji *Metody uwierzytelnienia użytkowników*, zaznacz opcję *Dodaj certyfikat X.509*, aby pobrać certyfikat użytkownika i przypisać go jako jedną z metod jego uwierzytelniania.
25. Zaznacz opcję „Dodaj klucz SSH wyodrębniony z certyfikatu X.509”, aby pobrać klucz SSH użytkownika z certyfikatu i przypisać go jako jedną z metod jego uwierzytelniania.
26. Kliknij *Zapisz*.

Tematy pokrewne:

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

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

- Fudo Enterprise pozwala skonfigurować serwer z unikalnym adresem oraz serwer z grupą adresów, aby nawiązywać połączenia z wybraną siecią.
- Serwery o tym samym protokole mogą być dodane do Puli Serwerów, które w ramach innych obiektów (na przykład, kont), będą zarządzalne jako jeden serwer.

7.1 Dodawanie serwera

7.1.1 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 instancji Fudo Enterprise.

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

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

2. Wpisz unikalną nazwę serwera.

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

4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.

5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.

6. Przejdź do sekcji *Ustawienia*.

7. W polu *Protokół* wybierz HTTP.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

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

9. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).

10. W polu *Host HTTP*, wprowadź nagłówek HTTP. Nagłówek HTTP wskazuje zasób na serwerze, na którym hostowanych jest wiele stron internetowych.

11. Wprowadź *Czas oczekiwania HTTP* wyrażony w sekundach czas bezczynności, po upływie którego, połączenie będzie wymagało ponownego uwierzytelnienia.

12. Zaznacz opcję *Uwierzytelnienie HTTP*, aby uruchomić dodatkową weryfikację.

Wybierz jedną z dostępnych platform, lub zdefiniuj wartości własne, które będą wykorzystane podczas weryfikacji:

- podaj *URL strony logowania*, *login* oraz *hasło*,
- zaznacz *Naciśnij klawisz Enter przed hasłem*.

Informacja: *Uwierzytelnienie HTTP* będzie aktywne tylko wtedy, gdy w ustawieniach gniazda nasłuchiwanie HTTP zostanie włączona opcja *Renderuj sesje*. Aby włączyć opcję *Renderuj sesje*, zapoznaj się z tematem *Konfigurowanie gniazda nasłuchiwanie HTTP*.

13. 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*.
-

14. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, *IPv4* albo *IPv6*,
 - Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.
-

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, *IPv4* albo *IPv6*. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsięci, podaj własną wartość dla pól *Adres* oraz *Maska*.

- Jeśli opcja wyżej *TLS włączony* została zaznaczona, dodatkowo wybierz sposób szyfrowania: *Certyfikat serwera*, albo *Certyfikat CA`* i podaj dane certyfikatu, albo *Brak* aby wyłączyć szyfrowanie.

15. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.2 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 serwer*.

2. Wpisz unikalną nazwę serwera.
 3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
 4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
 5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
 6. Przejdź do sekcji *Ustawienia*.
-

7. W polu *Protokół* wybierz Modbus.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

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. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, IPv4 albo IPv6,
- Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, IPv4 albo IPv6. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsieci, podaj własną wartość dla pól *Adres* oraz *Maska*.

10. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.3 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 serwer*.

2. Wpisz unikalną nazwę serwera.
3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz MSSQL(TDS).

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

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. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, *IPv4* albo *IPv6*,
- Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, *IPv4* albo *IPv6*. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsieci, podaj własną wartość dla pól *Adres* oraz *Maska*.

10. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.4 Dodawanie serwera MySQL

Ostrzeżenie: Domyślny plugin serwera MySQL `caching_sha2_password` nie jest obecnie wspierany przez Fudo Enterprise. Wspierane plugin'y dla połączeń MySQL przez Fudo Enterprise - 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 serwer*.

2. Wpisz unikalną nazwę serwera.
3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz MySQL.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

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. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:
 - Wybierz *Host*, IPv4 albo IPv6,
 - Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, IPv4 albo IPv6. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsieci, podaj własną wartość dla pól *Adres* oraz *Maska*.

10. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.5 Dodawanie serwera RDP

Informacja:

- Serwer może posiadać tylko jedno konto typu *anonymous*.
 - Serwer może posiadać tylko jedno konto typu *forward*.
 - Fudo Enterprise pozwala na uwierzytelnienie Kerberos'em przed serwerem RDP.
-

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

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

2. Wpisz unikalną nazwę serwera.
3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz RDP.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

8. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
 - Zaznacz opcję *NLA włączony*, aby dodać warstwę bezpieczeństwa.

Informacja: Tryb bezpieczeństwa serwera RDP musi być zgodny z trybem bezpieczeństwa *gniazda nasłuchiwanie RDP*. Opcja *NLA enabled* dla serwera RDP jest równoznaczna z opcją *Enhanced RDP Security (TLS)* dla gniazda nasłuchiwanie RDP.

- Zaznacz dodatkowo opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
9. Zaznacz *Informuj o istniejącym połączeniu*, aby użytkownik, łączący się do serwera, był informowany o tym, że inny użytkownik jest obecnie połączony z danym serwerem.
 10. 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*.

-
11. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, IPv4 albo IPv6,
- Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, IPv4 albo IPv6. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsieci, podaj własną wartość dla pól *Adres* oraz *Maska*.

- Jeśli opcja wyżej *TLS włączony* została zaznaczona, dodatkowo wybierz sposób szyfrowania: *Certyfikat serwera*, albo *Certyfikat CA* i podaj dane certyfikatu, albo *Brak* aby wyłączyć szyfrowanie.

12. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.6 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 serwer*.

2. Wpisz unikalną nazwę serwera.
3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz SSH.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

8. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
9. 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*.
-

10. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, IPv4 albo IPv6,
 - Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.
-

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, IPv4 albo IPv6. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsiaci, podaj własną wartość dla pól *Adres* oraz *Maska*.

11. W sekcji *Weryfikacja serwera* wybierz **Klucz publiczny serwera** i pobierz certyfikat, albo wybierz **Brak**, aby wyłączyć weryfikację serwera SSH.
12. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.7 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 Enterprise, 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 serwer*.

2. Wpisz unikalną nazwę serwera.
3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz *Telnet*.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

8. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
 - Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
9. 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*.
-

10. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, *IPv4* albo *IPv6*,
 - Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.
-

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, *IPv4* albo *IPv6*. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsięci, podaj własną wartość dla pól *Adres* oraz *Maska*.

- Jeśli opcja wyżej *TLS włączony* została zaznaczona, dodatkowo wybierz sposób szyfrowania: *Certyfikat serwera*, albo *Certyfikat CA* i podaj dane certyfikatu, albo *Brak* aby wyłączyć szyfrowanie.

11. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.8 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 Enterprise, 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 serwer*.

2. Wpisz unikalną nazwę serwera.
 3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
 4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
-

5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz **Telnet 3270**.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

8. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
 - Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
9. 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*.

10. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:
 - Wybierz **Host**, IPv4 albo IPv6,
 - Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji **Host**, IPv4 albo IPv6. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsięci, podaj własną wartość dla pól *Adres* oraz *Maska*.

- Jeśli opcja wyżej *TLS włączony* została zaznaczona, dodatkowo wybierz sposób szyfrowania: **Certyfikat serwera**, albo **Certyfikat CA** i podaj dane certyfikatu, albo **Brak** aby wyłączyć szyfrowanie.

11. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.9 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 Enterprise, 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 serwer*.

2. Wpisz unikalną nazwę serwera.
3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz **Telnet 5250**.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

8. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
 - Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
9. 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*.

10. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, IPv4 albo IPv6,
- Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, IPv4 albo IPv6. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsieci, podaj własną wartość dla pól *Adres* oraz *Maska*.

- Jeśli opcja wyżej *TLS włączony* została zaznaczona, dodatkowo wybierz sposób szyfrowania: *Certyfikat serwera*, albo *Certyfikat CA* i podaj dane certyfikatu, albo *Brak* aby wyłączyć szyfrowanie.

11. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.1.10 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 serwer*.

2. Wpisz unikalną nazwę serwera.
3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz *VNC*.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

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. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, IPv4 albo IPv6,
 - Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.
-

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, IPv4 albo IPv6. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsieci, podaj własną wartość dla pól *Adres* oraz *Maska*.

10. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

- *Pule*
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Gniazda nastuchiwania*
- *Sejfy*
- *Konta*

7.1.11 Dodawanie serwera TCP

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

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

2. Wpisz unikalną nazwę serwera.
3. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu.
4. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację zasobu infrastruktury.
5. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do obiektu.
6. Przejdź do sekcji *Ustawienia*.
7. W polu *Protokół* wybierz TCP.

Ostrzeżenie: Po zapisaniu definicji serwera protokół jest nieedytowalny.

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. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz *Host*, IPv4 albo IPv6,
- Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Informacja: Domyślna wartość dla pola *Maska* jest podawana automatycznie po wybraniu opcji *Host*, IPv4 albo IPv6. W ten sposób system Fudo Enterprise identyfikuje serwer jako posiadający jeden unikalny adres. Aby zdefiniować dla serwera adres całej podsieci, podaj własną wartość dla pól *Adres* oraz *Maska*.

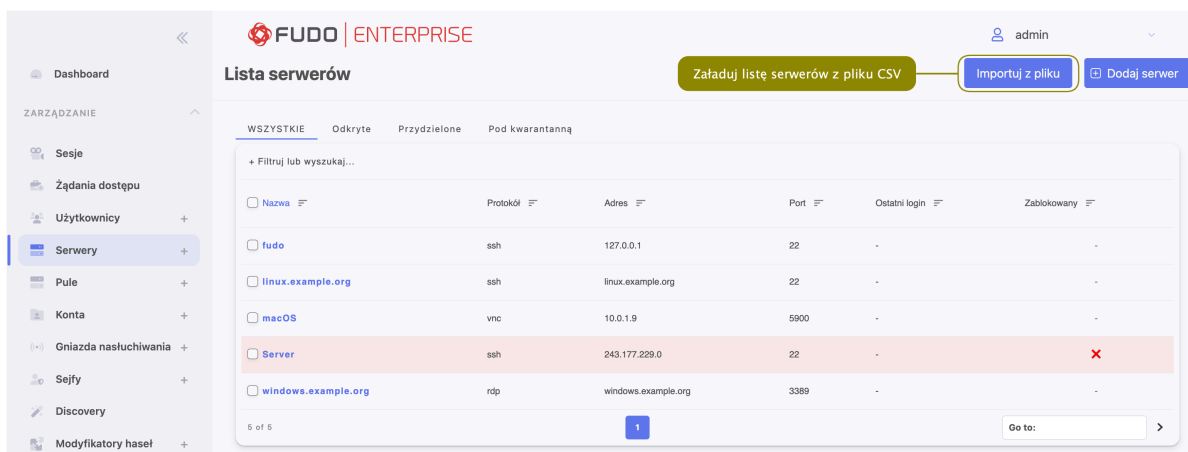
10. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

- *Pule*
- *TCP*
- *Konfigurowanie gniazda nasłuchiwania TCP*
- *Model danych*

7.2 Importowanie listy serwerów z pliku CSV

1. Wybierz z lewego menu *Zarządzanie > Serwery* i kliknij *Importuj z pliku*.



2. Przeciągnij i upuść plik w obszarze okna dialogowego lub kliknij przycisk *Przełóżaj pliki*, aby zaimportować go z lokalnego dysku.
3. Wyświetlone okno dialogowe przedstawia listę serwerów, które mają zostać zaimportowane do konfiguracji Fudo Enterprise.
4. Kliknij *Prześlij dane*, aby zaimportować listę serwerów lub *Wyczyść dane* w celu przerwania procedury.

Informacja: Jeśli którykolwiek z serwerów skonfigurowanych w pliku CSV posiada nieprawidłowe wartości, zostanie pominięty w procesie importowania. Na przykład, serwer o takiej samej nazwie jak serwer już istniejący w konfiguracji nie zostanie zaimportowany.

Format pliku CSV

Plik CSV powinien być zbudowany według poniższych zasad:

- Pierwszy wiersz jest wierszem nagłówka zawierającym nazwy odpowiadające nazwom pól z API (patrz *Dokumentacja API: API v2: Servers*).
- Wiersz nagłówka musi zawierać wszystkie pola, które są wymagane w trakcie ręcznego tworzenia serwera dla danego protokołu. Pozostałe pola są opcjonalne i mogą pozostać puste.
- Separatorem może być przecinek (,), średnik (;) lub kreska pionowa, czyli tzw. *pipe* (|).
- Tekst ujęty w cudzysłów („”) jest traktowany jako *string*, więc separatory pól w nim zawarte są ignorowane.

Przykład:

```
name,protocol,address,port,mask,bind_ip
Server1,ssh,243.177.229.0,22,,10.0.144.193
Server2,rdp,243.177.228.0,22,32,fudo:label:labelname
```

Tematy pokrewne:

- *Model danych*
- *Dodawanie serwera*
- *Blokowanie serwera*

- *Odblokowanie serwera*
- *Usuwanie serwera*

7.3 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*

7.4 Blokowanie serwera

Fudo Enterprise 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 wybierz serwer, który chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Zablokowane*, aby zablokować możliwość nawiązywania połączeń z wybranymi zasobami.
4. Wprowadź powód zablokowania zasobu i kliknij *Ustaw powód*.
5. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.5 Odblokowanie serwera

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

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Zablokowane*, aby przywrócić możliwość nawiązywania połączeń z serwerami.
4. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

Tematy pokrewne:

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

7.6 Usuwanie serwera

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

1. Wybierz z lewego menu *Zarządzanie > Serwery*.
2. Zdefiniuj filtry, aby zawęzić listę serwerów.
3. Zaznacz serwery do usunięcia i kliknij *Usuń zaznaczone*.

Servers list

Filter or search...

Name	Protocol	Host	Port	Last login	Blocked
<input type="checkbox"/> 10.0.2	ssh	10.0.2	22	17-10-2022, 18:37:03	-
<input type="checkbox"/> s123456	ssh	1.22.3	22	-	-
<input type="checkbox"/> telnet_server_1	telnet	10.0.2	23	17-10-2022, 09:37:51	-
<input type="checkbox"/> 10.0.2	rdp	10.0.2	3389	15-10-2022, 15:25:32	-
<input type="checkbox"/> 10.0.2	rdp	10.0.2	3389	17-10-2022, 14:01:21	-
<input checked="" type="checkbox"/> telnet_server_4	telnet	10.0.2	23	-	-
<input checked="" type="checkbox"/> telnet_server_3	telnet	10.0.0	23	-	-
<input type="checkbox"/> telnet_server_2	telnet	10.0.2	23	-	-
<input type="checkbox"/> Debian SSH Dynamic	ssh	10.0.0	22	-	-
<input type="checkbox"/> Disco D	rdp	10.0.0	3389	-	-
<input type="checkbox"/> windyn	rdp	10.0.0	245	-	-
<input type="checkbox"/> test2	ssh	10.10.	22	-	-
<input type="checkbox"/> megan62	ssh	99.0.0	46246	-	-
<input type="checkbox"/> reginald49	ssh	99.0.0	10106	-	-
<input type="checkbox"/> aray	rdp	99.0.0	20766	-	-
<input type="checkbox"/> dmiller	rdp	99.0.0	58803	-	-

Alternatywnie, wybierz serwer do usunięcia i kliknij ikonkę z wertykalną linią trzech kropek.

4. Potwierdź operację usunięcia zaznaczonych obiektów.

Tematy pokrewne:

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

Fudo Enterprise pozwala dodawać istniejące konfiguracje serwerów do puli serwerów, które w ramach innych obiektów (na przykład, kont), będą zarządzalne jako jeden serwer.

Informacja: Serwery są grupowane na podstawie protokołu.

8.1 Dodawanie puli

Aby dodać pulę, postępuj zgodnie z instrukcją:

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

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

2. Wpisz nazwę puli.
3. Opcjonalnie, kliknij opcję *Opis* i podaj tekst, ułatwiający identyfikację obiektu.
4. W sekcji *Uprawnienia* dodaj użytkowników, uprawnionych do danego obiektu.
5. W sekcji *Ustawienia* zaznacz serwery, które będą dodane do puli.

Informacja: Protokół dodawanych serwerów powinien być unikalny w ramach puli.

6. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

8.2 Usuwanie puli

Ostrzeżenie: Pula nie może zostać usunięta, jeśli jest przypisana do konta.

Aby usunąć pulę, postępuj zgodnie z instrukcją:

1. Wybierz z lewego menu *Zarządzanie > Pule*
2. Zdefiniuj filtry, aby zawęzić listę pul.
3. Zaznacz pule do usunięcia i kliknij *Usuń zaznaczone*.

Alternatywnie, wybierz pulę do usunięcia i kliknij ikonkę z wertykalną linią z trzech kropek.

4. Potwierdź usunięcie pul(i).

Tematy pokrewne:

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

Fudo Enterprise pozwala bezpośrednio się połączyć z aplikacją zdalną poprzez protokół RDP, korzystając z funkcji Zdalne aplikacje.

Administrator może skonfigurować dane wejściowe dla konkretnego zasobu, aby użytkownicy mogli się połączyć z nim przez Portal Użytkownika oraz klienta Remote Desktop Protocol.

9.1 Dodanie zdalnej aplikacji

Aby skonfigurować zdalną aplikację, postępuj zgodnie z instrukcją:

1. Wybierz *Zarządzanie > Zdalne aplikacje*.
2. Kliknij przycisk *Dodaj zdalną aplikację* button.
3. Podaj dane zdalnej aplikacji:
 - 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*.
4. Kliknij *Zapisz* albo *Zapisz i zamknij*.
5. Dodaj zdefiniowaną zdalną aplikację do konta z dostępem do serwera RDP:
 - Wybierz *Zarządzanie > Konta*,
 - wybierz konto z dostępem do serwera RDP, albo stwórz nowe,
 - w sekcji *Zdalne aplikacje* kliknij *Dodaj zdalną aplikację* i wybierz z listy skonfigurowaną aplikację zdalną.
 - kliknij *Zapisz*.

9.2 Połączenie do zdalnej aplikacji przez Portal Użytkownika

Aby nawiązać połączenie, zaloguj się do Portalu Użytkownika, wybierz konto oraz gniazdo nasłuchiwania, aby się połączyć z aplikacją zdalną. Wybierz opcję Klient natywny.

Informacja: Kiedy połączenie zostaje nawiązane użytkownikiem, jego zdalna sesja jest połączona tylko z aplikacją. Zatem, jeśli użytkownik nie ma dostępu do całego pulpitu, zamknięcie aplikacji przerywa połączenie.

9.3 Usuwanie zdalnej aplikacji

Usuwanie definicji zdalnej aplikacji

Aby usunąć konfigurację zdalnej aplikacji, postępuj zgodnie z instrukcją:

1. Wybierz *Zarządzanie > Zdalne aplikacje*.
2. Wybierz konfigurację zdalnej aplikacji, którą chcesz usunąć.
3. W trybie edycji zdalnej aplikacji znajdź ikonkę z linią trzech kropek.
4. Kliknij przycisk *Usuń aplikację*.
5. Potwierdź usunięcie zdalnej aplikacji.

Usuwanie zdalnej aplikacji z definicji konta

Aby usunąć zdefiniowaną zdalną aplikację z definicji konta, postępuj zgodnie z instrukcją:

1. Wybierz *Zarządzanie > Konta*.
2. Wybierz konto, posiadające skonfigurowaną zdalną aplikację.
3. W sekcji *Zdalne aplikacje* wybierz opcję *Usuń*.
4. Kliknij *Zapisz*.

Related topics:

- *Data model*
- *System initiation*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*
- *Konta*
- *Dodawanie 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.

10.1 Dodawanie konta

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nastu-chiwania* 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.

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

Informacja: Podczas ręcznego tworzenia konta, przypisanie kategorii *uprzywilejowane* lub *nieuprzywilejowane* ma charakter wyłącznie informacyjny, jednak w procesie *Wykrywania (Discovery)* jest ona automatycznie przypisywana na podstawie parametrów konta w systemie źródłowym.

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.

Informacja: Retencja danych dla sesji nawiązanych za pośrednictwem tego konta będzie aktywna tylko w sytuacji, kiedy włączona jest opcja retencji na poziomie globalnym. W celu sprawdzenia globalnych ustawień retencji przejdź do rozdziału *Retencja danych*.

9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Serwer*, z listy rozwijalnej *Serwer*, wybierz serwer docelowy albo grupę serwerów, 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*

10.1.2 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 Enterprise 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 Enterprise 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 Enterprise nagrywa sesję w formacie, dostępnym do odtworzenia w playerze.
 - **brak** - Fudo Enterprise 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** lub **nieuprzywilejowany**.

Informacja: Podczas ręcznego tworzenia konta, przypisanie kategorii *uprzywilejowane* lub *nieuprzywilejowane* ma charakter wyłącznie informacyjny, jednak w procesie *Wykrywania (Discovery)* jest ona automatycznie przypisywana na podstawie parametrów konta w systemie źródłowym.

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.

Informacja: Retencja danych dla sesji nawiązanych za pośrednictwem tego konta będzie aktywna tylko w sytuacji, kiedy włączona jest opcja retencji na poziomie globalnym. W celu sprawdzenia globalnych ustawień retencji przejdź do rozdziału *Retencja danych*.

9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
 10. W sekcji *Serwer*, z listy rozwijalnej *Serwer*, wybierz serwer docelowy albo grupę serwerów, z którym skojarzone będzie definiowane konto.
 11. W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastąp sekret*, wybierz żadaną 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 Enterprise, 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*).

Dane uwierzytelniające

Zastąp sekret

Przekazuj domenę

Uwierzytelnienie przez serwer

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.

Informacja:

Włączona opcja *Przekazuj domenę* wykorzystuje *ustawienia domen konta użytkownika* w następnym rozdziale.

- jeśli użytkownik ma skonfigurowaną *Domenę AD*, Fudo Enterprise użyje jej do uwierzytelnienia przed serwerem.
- jeśli użytkownik nie ma skonfigurowanej *Domeny AD*, natomiast ma skonfigurowaną *Domenę Fudo*, Fudo Enterprise użyje *Domeny Fudo* do uwierzytelnienia przed serwerem.

-
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*

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

Informacja: Podczas ręcznego tworzenia konta, przypisanie kategorii *uprzywilejowane* lub *nieuprzywilejowane* ma charakter wyłącznie informacyjny, jednak w procesie *Wykrywania (Discovery)* jest ona automatycznie przypisywana na podstawie parametrów konta w systemie źródłowym.

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.

Informacja: Retencja danych dla sesji nawiązanych za pośrednictwem tego konta będzie aktywna tylko w sytuacji, kiedy włączona jest opcja retencji na poziomie globalnym. W celu sprawdzenia globalnych ustawień retencji przejdź do rozdziału [Retencja danych](#).

9. W sekcji *Uprawnienia*, dodaj użytkowników uprawnionych do zarządzania obiektem.
10. W sekcji *Serwer*, z listy rozwijalnej *Serwer*, wybierz serwer docelowy albo grupę serwerów, 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.



Informacja: Jeśli domena zostanie wpisana w polu *Domena*, Fudo Enterprise zawsze wykorzysta ją do uwierzytelniania przed serwerem. Domena zostanie automatycznie dodana do loginu użytkownika.

13. W polu *Login*, wprowadź login użytkownika uprzywilejowanego na serwerze docelowym.
14. Z listy rozwijalnej *Zastąp sekret*, wybierz żadaną 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 Enterprise, 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.

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

Informacja: Zdefiniowanie 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.

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

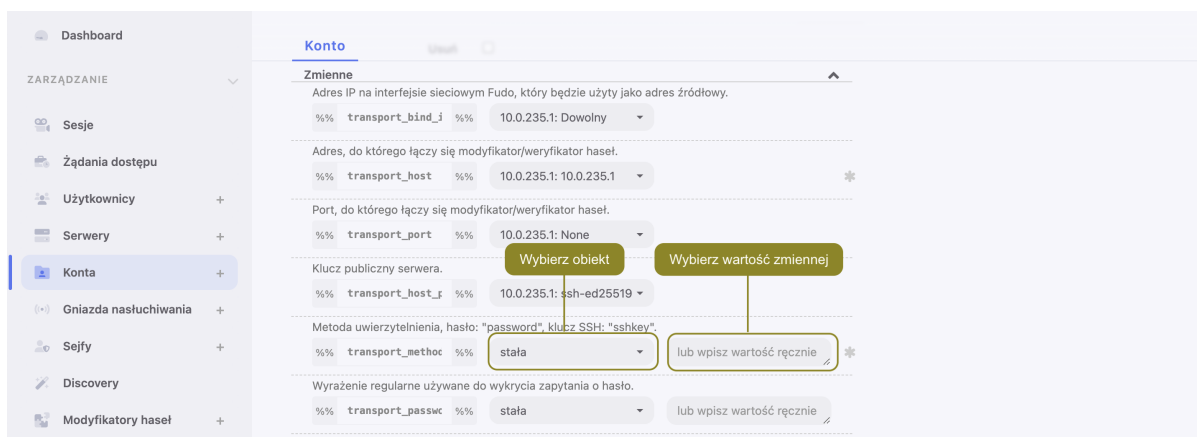
Informacja: Kiedy ta opcja jest włączona, Weryfikator Hasła uruchamia Modyfikator Hasła. Kiedy jest wyłączona, Weryfikator Hasła wysyła komunikat: „Nie udało się zweryfikować hasła dla konta <nazwa_konta>”.

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

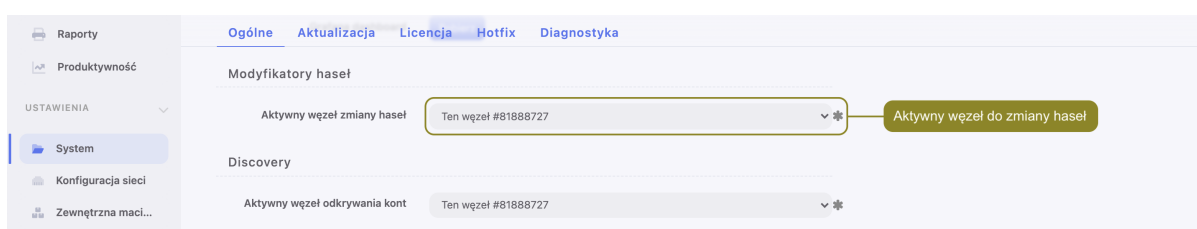
Informacja: Opcja dodania modyfikatora dostępna jest po wybraniu opcji zastąpienia sekretu hasłem.

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

- W sekcji *Zmienne*, sparametryzuj zmienne skryptu.

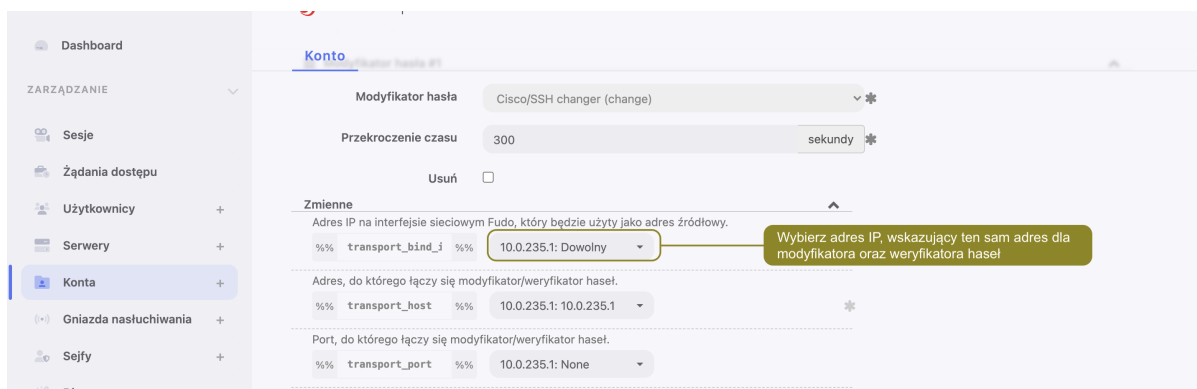


Fudo Enterprise umożliwia zmianę hasła na innym węzle klastra, niż ten, który jest wskazany jako aktywny węzeł klastra dla Modyfikatorów hasel.



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 węzle, wskazanym jako *aktywny węzeł klastra dla Modyfikatorów hasel*.

Więcej informacji na temat pracy węzłów klastra w ramach zmiany hasel znajdziesz pod linkiem: [Modyfikatory hasel - aktywny węzeł klastra](#)

Tematy pokrewne:

- [Edytowanie konta](#)

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

10.2 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*

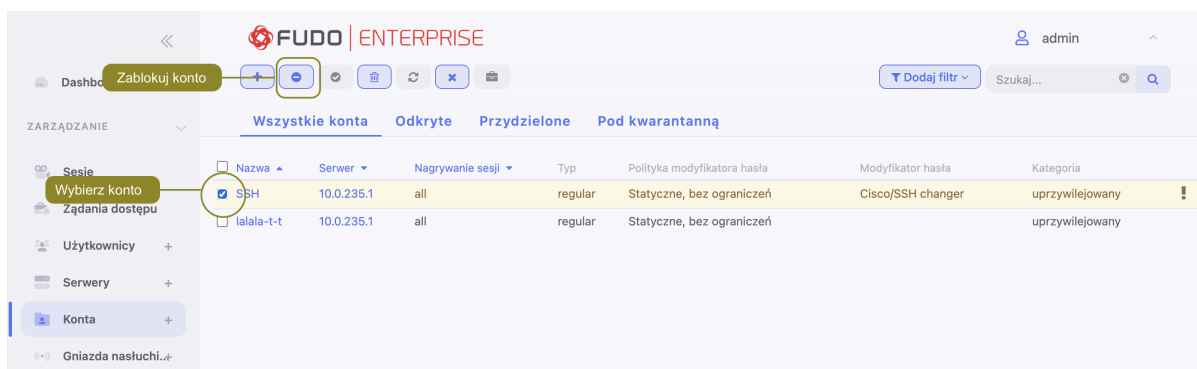
10.3 Blokowanie konta

Ostrzeżenie: Zablokowanie konta spowoduje zerwanie aktualnie trwających sesji połączeniowych z powiązonym 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*

10.4 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*

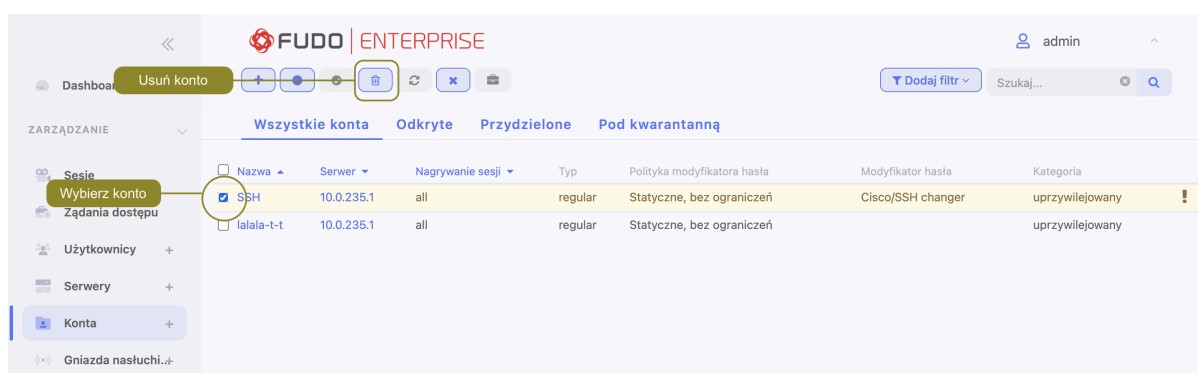
10.5 Usuwanie konta

Ostrzeżenie: Usunięcie konta spowoduje zerwanie aktualnie trwających sesji połączeniowych z powiązaniem 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*

10.6 Zarządzanie ostrzeżeniami bezpieczeństwa

Fudo Enterprise 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 Enterprise identyfikuje takie zdarzenia i komunikuje administratorom systemu.

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

10.6.1 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*.

Nazwa	Serwer	Nagrywanie sesji	Typ	Polityka modyfikatora hasła	Modyfikator hasła	Kategoria
SSH	10.0.235.1	all	regular	Stacyczne, bez ograniczeń	Cisco/SSH changer	uprzywilejowany
lalala-t-t	10.0.235.1	all	regular	Stacyczne, bez ograniczeń		uprzywilejowany

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*.

Modyfikatory haseł

Modyfikator hasła #1

Modyfikator hasła: Cisco/SSH changer (change) *

Przekroczenie czasu: 300 sekundy *

Usuń:

Zmienne: Adres IP na interfejsie sieciowym Fudo, który będzie użyty jako adres źródłowy.

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

Konto

Użytkownik, który został zablokowany, usunięty lub stracił dostęp do hasła konta, widział obecne hasło do konta. Zresetuj hasło, aby zredukować ryzyko potencjalnego włamania. Zagrożający użytkownicy, którzy widzieli hasło:

- **user** dostęp do podglądu hasła został usunięty lub stracił ważność, widział hasło o 2021-07-14 06:59:08.

Bieżące hasło do tego konta było widziane przez użytkownika, który wciąż ma do niego dostęp. Użytkownicy którzy widzieli hasło:

- **tpo** widział hasło o 2021-11-10 02:44:33

Ogólne

10.6.2 Zignorowanie ostrzeżenia

Zignorowanie ostrzeżenia z poziomu listy kont

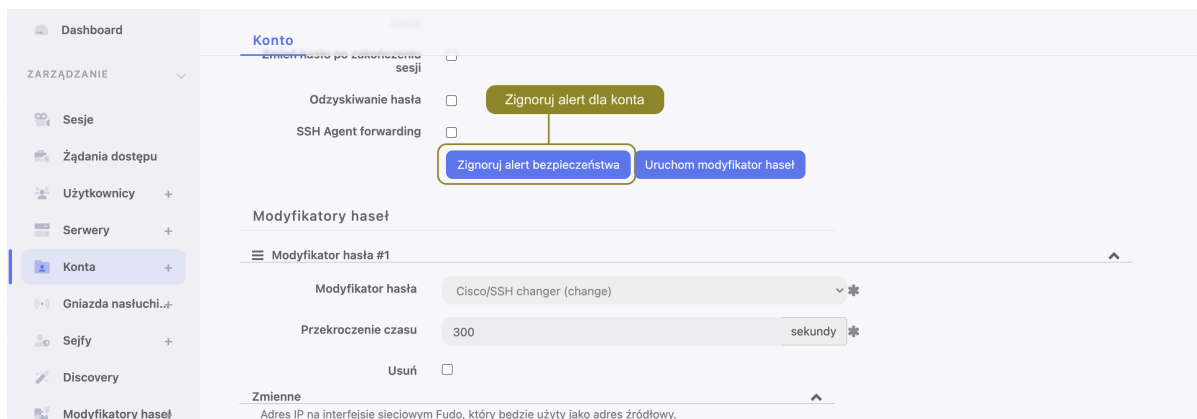
1. Wybierz z lewego menu *Zarządzanie > Konta*.
2. Odszukaj na liście i zaznacz konta, dla których chcesz zignorować ostrzeżenie.
3. Kliknij *Ignoruj alert*.



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*

Gniazda nasłuchiwania

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryby **transparent** i **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tych trybów muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

Funkcjonalność ta zostanie usunięta w kolejnym wydaniu.

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

11.1 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.

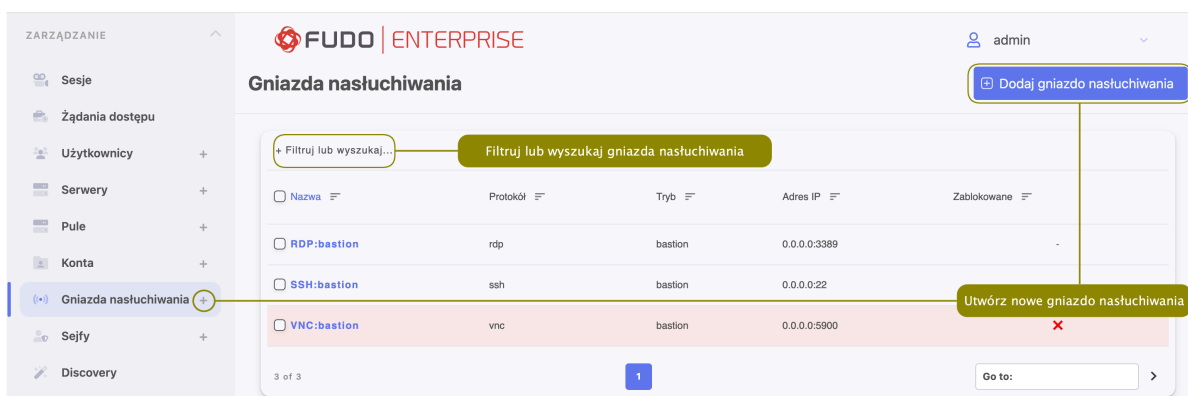
Informacja:

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

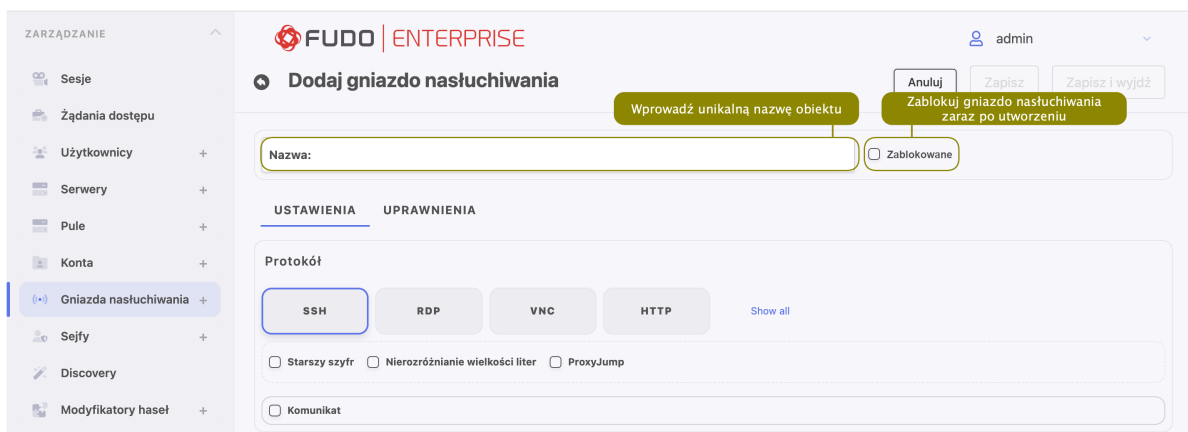
W celu utworzenia gniazda nasłuchiwania, postępuj zgodnie z poniższą instrukcją:

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



2. Wprowadź unikalną nazwę obiektu.

3. Zaznacz opcję *Zablokowane*, aby gniazdo było niedostępne po utworzeniu.



4. Przejdź do zakładki *Uprawnienia* i dodaj użytkowników uprawnionych do zarządzania tworzonym gniazdem nasłuchiwania. Użyj filtrowania po nazwie lub roli w celu ograniczenia listy wyświetlanych obiektów.



5. Wróć do zakładki *Ustawienia*, a następnie przejdź do rozdziału opisującego dalszą konfigurację gniazda nasłuchiwania zgodnie z wybranym protokołem:

- *Konfigurowanie gniazda nasłuchiwania SSH*
- *Konfigurowanie gniazda nasłuchiwania RDP*
- *Konfigurowanie gniazda nasłuchiwania VNC*
- *Konfigurowanie gniazda nasłuchiwania HTTP*
- *Konfigurowanie gniazda nasłuchiwania Modbus*
- *Konfigurowanie gniazda nasłuchiwania MySQL*
- *Konfigurowanie gniazda nasłuchiwania TCP*
- *Konfigurowanie gniazda nasłuchiwania MS SQL*
- *Konfigurowanie gniazda nasłuchiwania Telnet*
- *Konfigurowanie gniazda nasłuchiwania Telnet 3270*
- *Konfigurowanie gniazda nasłuchiwania Telnet 5250*

11.1.1 Konfigurowanie gniazda nasłuchiwania SSH

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem SSH. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i w polu *Protokół* wciśnij przycisk *SSH*.
2. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
3. Zaznacz opcję *Nierozróżnianie wielkości liter*, aby proces uwierzytelnienia nie rozróżniał wielkości liter w nazwie użytkownika.

4. Zaznacz opcję *ProxyJump* pozwalającą na wskazanie systemu pośredniczącego, przez który można będzie łączyć się do docelowego serwera.
5. Zaznacz opcję *Komunikat* w celu wyświetlenia okna służącego do wprowadzenia wiadomości, która będzie wyświetlana użytkownikom na ekranie logowania.
6. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

bastion

Informacja:

- Użytkownik łączy się z serwerem docelowym wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego, np. `john_smith#root#192.168.0.110`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Wciśnij przycisk `bastion` w polu *Tryb połączenia*.
- 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 nasłuchiowaniem 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*.
-

- Zaznacz opcję *Adres zewnętrzny*, aby aktywować pole i wprowadź adres IP (lub nazwę domenową FQDN) oraz 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.

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk **proxy** w polu *Tryb połączenia*.
 - 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 nasłuchiowaniem 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*.
-

- Zaznacz opcję *Adres zewnętrzny*, aby aktywować pole i wprowadź adres IP (lub nazwę domenową FQDN) oraz numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą

zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
 - Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.
7. W polu *Klucz publiczny Fudo* wciśnij *Generuj parę kluczy* aby wygenerować klucze lub wybierz *Wczytaj* aby wskazać plik zawierający klucze z dysku lokalnego (opcjonalnie, wprowadź hasło deszyfrujące).
 8. Kliknij *Zapisz*.

Tematy pokrewne:

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

11.1.2 Konfigurowanie gniazda nasłuchiwania RDP

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem RDP. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie*

gniazda nasłuchiwania.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i w polu *Protokół* wciśnij przycisk RDP.
2. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
3. Zaznacz *NLA włączony*, aby dodać warstwę bezpieczeństwa.

4. Zaznacz opcję *Komunikat* w celu wyświetlenia okna służącego do wprowadzenia wiadomości, która będzie wyświetlana użytkownikom na ekranie logowania.
5. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

bastion

Informacja:

- Użytkownik łączy się z serwerem docelowym wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego, np. `john_smith#root#192.168.0.110`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Wciśnij przycisk `bastion` w polu *Tryb połączenia*.
- 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 nasłuchiowaniem 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*.

-
- Zaznacz opcję *Adres zewnętrzny*, aby aktywować pole i wprowadź adres IP (lub nazwę domenową FQDN) oraz 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.

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk *proxy* w polu *Tryb połączenia*.
- 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 nasłuchiowaniem 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*.

-
- Zaznacz opcję *Adres zewnętrzny*, aby aktywować pole i wprowadź adres IP (lub nazwę domenową FQDN) oraz numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
 - Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.
6. W polu *Certyfikat CA*, kliknij *Generuj certyfikat*, aby wygenerować certyfikat TLS, albo kliknij *Wczytaj*, aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwolonym formatem pliku z certyfikatem serwera jest PEM, jednak poza rozszerzeniem *.pem* akceptowane są również *.txt* oraz *.cert*.

7. Kliknij *Zapisz*.

Tematy pokrewne:

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

11.1.3 Konfigurowanie gniazda nasłuchiwania VNC

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem VNC. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i w polu *Protokół* wciśnij przycisk *VNC*.
2. Zaznacz opcję *Nierozróżnianie wielkości liter*, aby proces uwierzytelnienia nie rozróżniał wielkości liter w nazwie użytkownika.

3. Zaznacz opcję *Komunikat* w celu wyświetlenia okna służącego do wprowadzenia wiadomości, która będzie wyświetlana użytkownikom na ekranie logowania.
4. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

bastion

Informacja:

- Użytkownik łączy się z serwerem docelowym wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego, np. `john_smith#root#192.168.0.110`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Wciśnij przycisk `bastion` w polu *Tryb połączenia*.
- 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 nasłuchiwaniami 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*.

- Zaznacz opcję *Adres zewnętrzny*, aby aktywować pole i wprowadź adres IP (lub nazwę domenową FQDN) oraz 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.

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk **proxy** w polu *Tryb połączenia*.
 - 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 nasłuchiowaniem 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*.
-

- Zaznacz opcję *Adres zewnętrzny*, aby aktywować pole i wprowadź adres IP (lub nazwę domenową FQDN) oraz numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwanie korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

5. Kliknij *Zapisz*.

Tematy pokrewne:

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

11.1.4 Konfigurowanie gniazda nasłuchiwania HTTP

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem SSH. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i w polu *Protokół* wciśnij przycisk **HTTP**.
2. Zaznacz opcję *TLS włączony* w celu uruchomienia trybu szyfrowania.
3. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).

4. 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 instancji Fudo Enterprise.

Informacja:

- W przypadku renderowanych sesji HTTP, surowy ruch nie jest rejestrowany.
- Opcja *Renderuj sesje* musi być włączona, aby aktywować uwierzytelnianie na serwerze HTTP (patrz temat *Dodawanie serwera HTTP*).

5. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

bastion

Informacja:

- Użytkownik łączy się z serwerem docelowym wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego, np. `john_smith#root#192.168.0.110`.
 - Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.
-

- Wciśnij przycisk **bastion** w polu *Tryb połączenia*.
 - 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 nasłuchiowaniem 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*.
-

Informacja:

- Tryb Bastion jest dostępny tylko przy zaznaczonej opcji *Renderuj sesje*.
 - Zaznacz opcję *Adres zewnętrzny*, aby aktywować pole i wprowadź adres IP (lub nazwę domenową FQDN) oraz numer portu, pod którym Fudo jest osiągalne spoza sieci lokalnej.
-

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk **proxy** w polu *Tryb połączenia*.
 - 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 nasłuchiowaniem 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*.
-

- Zaznacz opcję *Adres zewnętrzny*, aby aktywować pole i wprowadź adres IP (lub nazwę domenową FQDN) oraz 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.

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

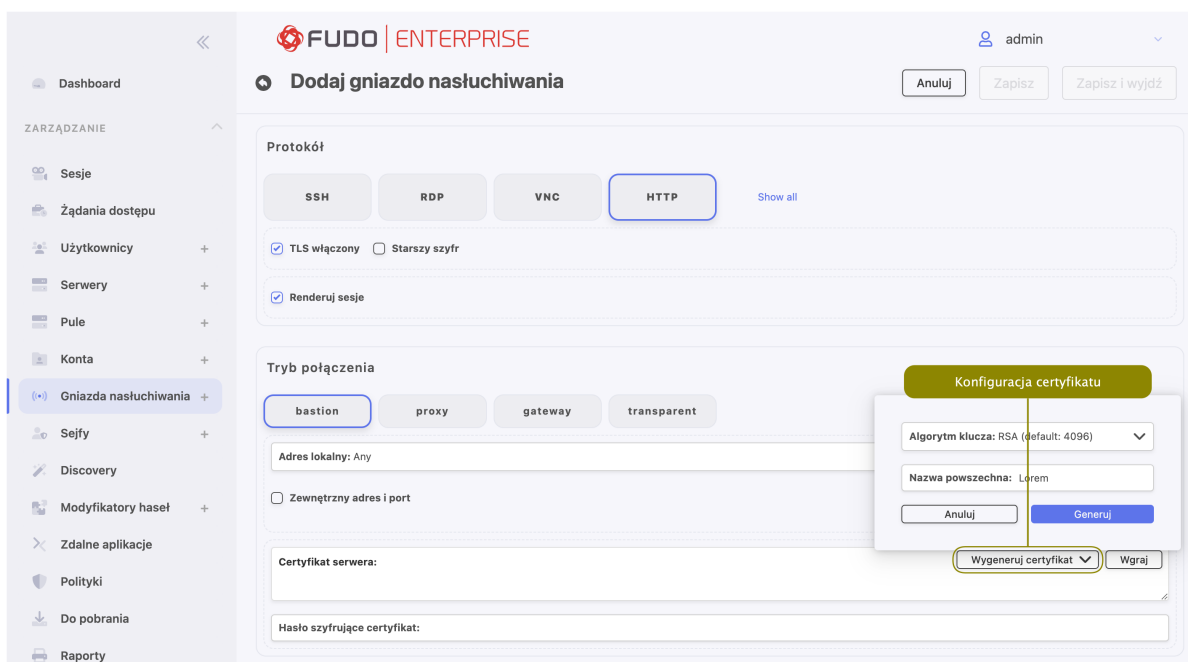
Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

Informacja: Użytkownik łączy się z serwerem docelowym podając jego adres IP.

Fudo Enterprise pośredniczy w połączeniu wykorzystując źródłowy adres IP użytkownika. Taki tryb pracy wymaga wdrożenia Fudo Enterprise w *trybie mostu*.

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
 - Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.
6. W polu *Certyfikat CA*, kliknij *Generuj certyfikat*, aby wygenerować certyfikat TLS, albo kliknij *Wczytaj*, aby wgrać plik z certyfikatem TLS na początku i kluczem prywatnym, wklejonym na końcu pliku. Reszta pól konfiguracyjnych będzie wypełniona automatycznie. Dozwołonym formatem pliku z certyfikatem serwera jest PEM, jednak poza rozszerzeniem `.pem` akceptowane są również `.txt` oraz `.cert`.



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

7. Kliknij *Zapisz*.

Tematy pokrewne:

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

11.1.5 Konfigurowanie gniazda nasłuchiwania Modbus

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem Modbus. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale [Dodawanie gniazda nasłuchiwania](#).

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i wciśnij przycisk **Pokaż wszystkie**.
2. Wciśnij przycisk **Modbus** w polu *Protokół*.

5. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w rozdziale [Wstęp > Tryby połączenia](#).

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk **proxy** w polu *Tryb połączenia*.
- 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 nasłuchiowaniem 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*.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

6. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*

- *Sejfy*
- *Konta*

11.1.6 Konfigurowanie gniazda nasłuchiwania MySQL

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem MySQL. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i wciśnij przycisk *Pokaż wszystkie*.
2. Wciśnij przycisk MySQL w polu *Protokół*.

3. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk **proxy** w polu *Tryb połączenia*.
- 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 nasłuchiowaniem 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*.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*

- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

11.1.7 Konfigurowanie gniazda nasłuchiwania TCP

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem TCP. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i wciśnij przycisk *Pokaż wszystkie*.
2. Wciśnij przycisk TCP w polu *Protokół*.

3. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk *proxy* w polu *Tryb połączenia*.
- 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 nasłuchiowaniem 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*.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Protokół TCP*
- *Dodawanie serwera TCP*
- *Model danych*

11.1.8 Konfigurowanie gniazda nasłuchiwania MS SQL

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem MS SQL. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i wciśnij przycisk *Pokaż wszystkie*.
2. Wciśnij przycisk **MS SQL(TDS)** w polu *Protokół*.

3. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

bastion**Informacja:**

- Użytkownik łączy się z serwerem docelowym wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego, np. `john_smith#root#192.168.0.110`.
 - Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.
-

- Wciśnij przycisk **bastion** w polu *Tryb połączenia*.

- 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 nasłuchiowaniem 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*.
-

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk **proxy** w polu *Tryb połączenia*.
 - 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 nasłuchiowaniem 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*.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

4. Kliknij *Zapisz*.

Tematy pokrewne:

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

11.1.9 Konfigurowanie gniazda nasłuchiwania Telnet

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem Telnet. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i wciśnij przycisk *Pokaż wszystkie*.
2. Wciśnij przycisk **Telnet** w polu *Protokół*.

3. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

bastion

Informacja:

- Użytkownik łączy się z serwerem docelowym wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego, np. `john_smith#root#192.168.0.110`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Wciśnij przycisk `bastion` w polu *Tryb połączenia*.
- 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 nasłuchiowaniem 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*.

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk **proxy** w polu *Tryb połączenia*.
 - 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 nasłuchiowaniem 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*.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
 - Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.
-

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu

muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

4. Kliknij *Zapisz*.

Tematy pokrewne:

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

11.1.10 Konfigurowanie gniazda nasłuchiwania Telnet 3270

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem Telnet 3270. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i wciśnij przycisk *Pokaż wszystkie*.
2. Wciśnij przycisk **Telnet 3270** w polu *Protokół*.

3. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

bastion

Informacja:

- Użytkownik łączy się z serwerem docelowym wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego, np. `john_smith#root#192.168.0.110`.
 - Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.
-

- Wciśnij przycisk `bastion` w polu *Tryb połączenia*.
 - 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 nasłuchiowaniem 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*.
-

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk `proxy` w polu *Tryb połączenia*.
 - 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 nasłuchiwaniami 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*.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*

- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

11.1.11 Konfigurowanie gniazda nasłuchiwania Telnet 5250

Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem Telnet 5250. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

1. Przejdź do zakładki *Ustawienia* dodawanego gniazda nasłuchiwania i wciśnij przycisk *Pokaż wszystkie*.
2. Wciśnij przycisk **Telnet 5250** w polu *Protokół*.

3. W polu *Tryb połączenia*, wybierz jeden z dostępnych sposobów obsługi połączeń.

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

bastion

Informacja:

- Użytkownik łączy się z serwerem docelowym wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym oraz adres serwera docelowego, np. `john_smith#root#192.168.0.110`.
- Więcej informacji na temat trybu połączenia bastion znajdziesz w rozdziale *Tryby połączenia*.

- Wciśnij przycisk **bastion** w polu *Tryb połączenia*.

- 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 nasłuchiowaniem 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*.
-

proxy

Informacja: Użytkownik nawiązuje połączenie z serwerem podając adres IP Fudo Enterprise i numer portu, który jednoznacznie wskazuje docelową maszynę.

- Wciśnij przycisk **proxy** w polu *Tryb połączenia*.
 - 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 nasłuchiowaniem 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*.
-

gateway

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **gateway** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

transparent

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą tryb **transparent** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tego trybu muszą zostać przekonfigurowane na tryby proxy i bastion przed przeprowadzeniem aktualizacji do następnej wersji.

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

- Wciśnij przycisk **transparent** w polu *Tryb połączenia*.
- Z listy rozwijalnej *Interfejs*, wybierz interfejs sieciowy, który będzie obsługiwał ruch sieciowy dla tworzonego gniazda nasłuchiwania.

4. Kliknij *Zapisz*.

Tematy pokrewne:

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

11.2 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 wybranego gniazda nasłuchiwania w celu edycji jego ustawień.
4. Zmień parametry konfiguracyjne zgodnie z potrzebami.
5. Kliknij *Zapisz*.

Tematy pokrewne:

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

11.3 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. Zaznacz okienko wyboru towarzyszące nazwie obiektu lub obiektów, które chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj / Zablokuj*, aby zablokować możliwość nawiązywania połączeń z serwerami, z którymi połączenia realizowane są za pośrednictwem wskazanego gniazda nasłuchiwania.
4. Wprowadź powód zablokowania zasobu (wymagany) i kliknij *Zablokuj*.

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

Tematy pokrewne:

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

11.4 Odblokowanie gniazda nasłuchiwania

1. Wybierz z lewego menu *Zarządzanie > Gniazda nasłuchiwania*.
2. Zaznacz okienko wyboru towarzyszące nazwie obiektu lub obiektów, które chcesz zablokować.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Odblokuj / Zablokuj*, aby odblokować możliwość nawiązywania połączeń z serwerami, z którymi połączenia realizowane są za pośrednictwem wskazanego gniazda nasłuchiwania.

4. Kliknij *Odblokuj*, aby potwierdzić odblokowanie obiektu.

Tematy pokrewne:

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

11.5 Usuwanie gniazda nasłuchiwania

Ostrzeżenie: Usunięcie gniazda nasłuchiwania spowoduje przerwanie aktualnie trwających sesji połączeniowych korzystających z usuwanego obiektu.

1. Wybierz z lewego menu *Zarządzanie > Gniazda nasłuchiwania*.
2. Zaznacz okienko wyboru towarzyszące nazwie obiektu lub obiektów, które chcesz usunąć.

Informacja: Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

The screenshot shows the 'Gniazda nasłuchiwania' (Listening Ports) management interface in Fudo Enterprise. The interface includes a sidebar with navigation options like 'Dashboard', 'Sesje', 'Ządania dostępu', 'Użytkownicy', 'Serwery', 'Pule', 'Konta', 'Gniazda nasłuchiwania', 'Sejfy', and 'Discovery'. The main content area displays a table of listening ports with columns for 'Nazwa', 'Protokół', 'Tryb', 'Adres IP', and 'Zablokowane'. A table row for 'SSH:bastion' is highlighted, and a 'Wybierz obiekt' button is shown next to it. At the top, there are buttons for 'Odblokuj (1) / Zablokuj (1)', 'Usuń zaznaczone (2)', and 'Dodaj gniazdo nasłuchiwania'. A search bar and filter buttons are also visible.

3. Kliknij *Usuń zaznaczone*.

4. Kliknij *Potwierdź*, aby zatwierdzić usunięcie zaznaczonych obiektów.

Tematy pokrewne:

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

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.

The screenshot shows the FUDO ENTERPRISE interface. The main content area is titled 'Sejfy' and contains a table with the following data:

Nazwa	Użytkownicy	Konta	Gniazda nasłuchiwania
>>> Web Client	admin		
LDAP_Ubuntu_10.0.:			
portal	tpo	SSH	new-ssh-listener
portal		portal	portal

The left sidebar shows a navigation menu with 'Sejfy' selected and a '+' icon next to it. A callout box labeled 'Dodaj nowy sejf' points to this icon. At the top of the main area, there are buttons for '+ Dodaj', 'Blokuj', 'Odblokuj', and 'Usuń'. A search bar with 'Szukaj...' and a filter dropdown 'Dodaj filtr' are also visible.

12.1 Dodawanie sejfu

Ostrzeżenie: Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nastęchiwania* 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 protokoły RDP, VNC oraz SSH, 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.

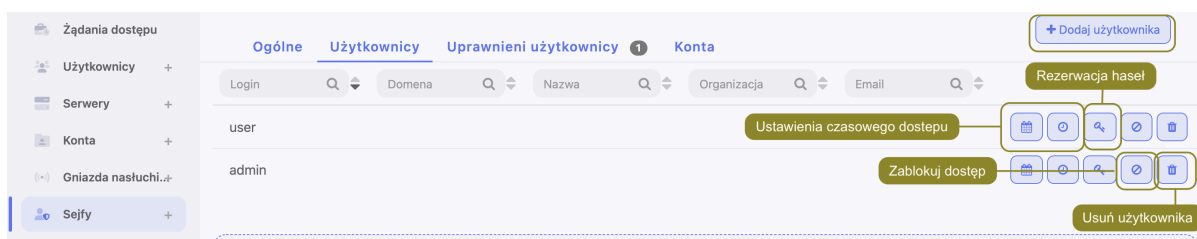
13. Z listy rozwijanej *Miejsce docelowe kopii zapasowej* wybierz skonfigurowane miejsce docelowe dla przechowania kopii zapasowych. Konfiguracja jest dostępna pod linkiem *Kopie zapasowe i retencja*.
14. W sekcji *Funkcjonalność protokołów*, zaznacz funkcje dozwolone w połączeniach.

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.

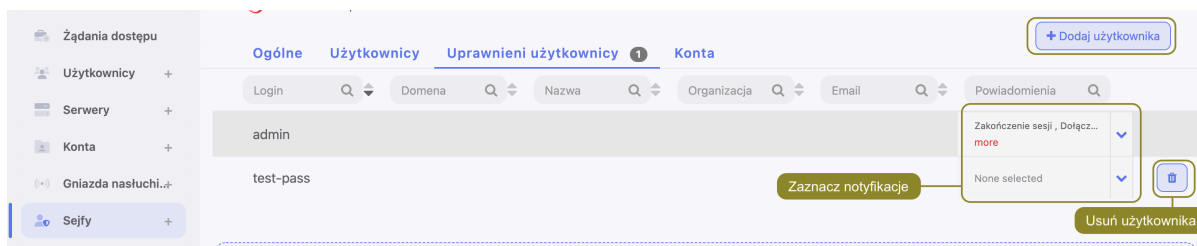
15. Wybierz zakładkę *Użytkownicy*, aby nadać użytkownikom uprawnienia dostępu do sejfów.
 - Kliknij *+ Dodaj użytkownika*.
 - Kliknij przy użytkowniku, któremu chcesz przyznać dostęp do sejfów.




- Kliknij *ok*, aby zamknąć okno modalu.
- Zdefiniuj opcje dostępu do sejfów.
 - Kliknij , aby wypełnić pola *Od* and *Do* interwałem czasu, w którym użytkownik będzie mógł nawiązywać połączenia za pośrednictwem wybranego sejfów. Kiedy podany czas nadejdzie, dostęp do sejfów zostanie przyznany użytkownikowi automatycznie. Opcja *Zablokowane* z poprzedniego kroku powinna być odznaczona. Opcja *okresu dostępu* jest nieaktywna, kiedy opcja *głosowania do uzyskania dostępu* jest włączona.
 - Kliknij , aby zdefiniować wyznaczone godzinachy, w których użytkownik będzie mógł nawiązywać połączenia. 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 uniemożliwić użytkownikowi nawiązywanie połączeń poprzez wybrany sejf. Użytkownik będzie miał zablokowany dostęp, dopóki administrator nie wyłączy opcji *Zablokowane*, albo nie kliknie *Odblokuj dostęp* w konfiguracji sejfów.

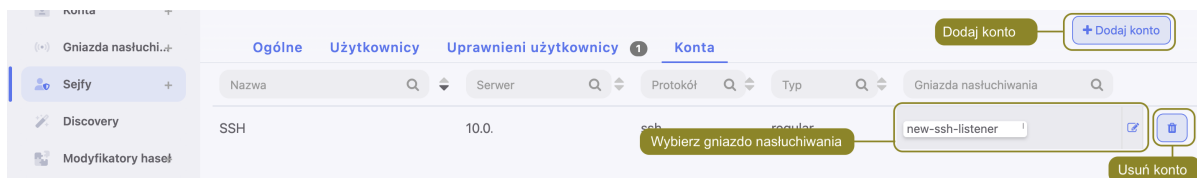
– Kliknij , aby usunąć użytkownika z sejfu.




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 skonfigurowanego sejfu.
- Kliknij *ok*, aby zamknąć okno modalu.

18. Kliknij *Zapisz*.

Tematy pokrewne:

- *Model danych*
- *Modyfikowanie sejfu*
- *Blokowanie sejfu*
- *Usuwanie sejfu*
- *Żądania dostępu*

12.2 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*

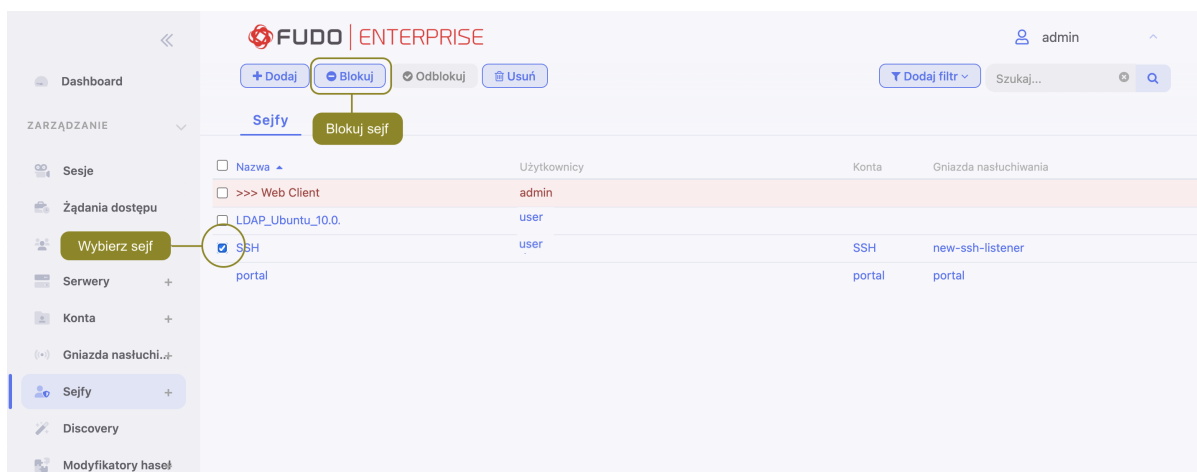
12.3 Blokowanie sejfu

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:

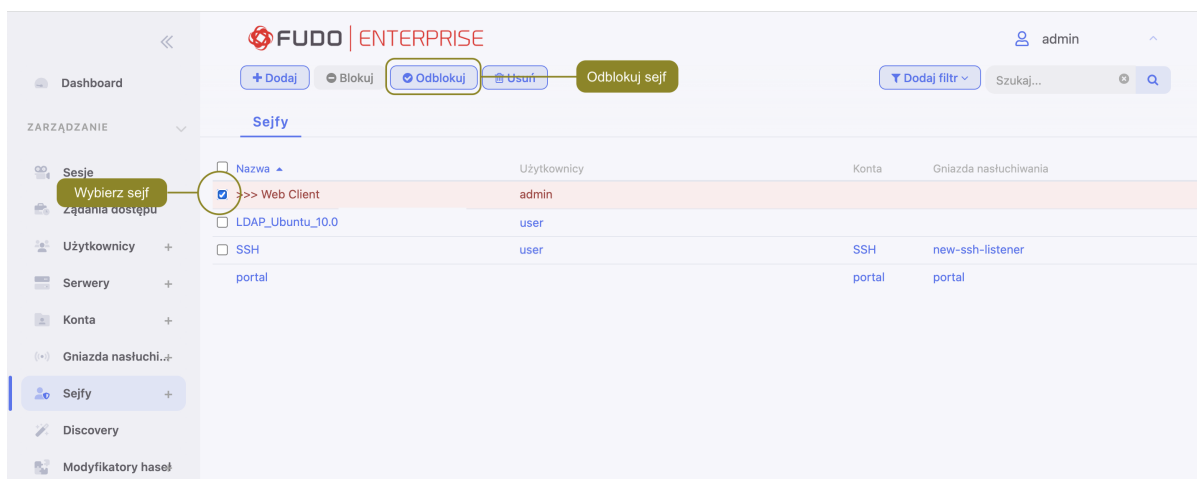
- *Odblokowanie sejfu*
- *Model danych*
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*

12.4 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 sejfów*
- *Dodawanie sejfów*
- *Modyfikowanie sejfów*
- *Usuwanie sejfów*

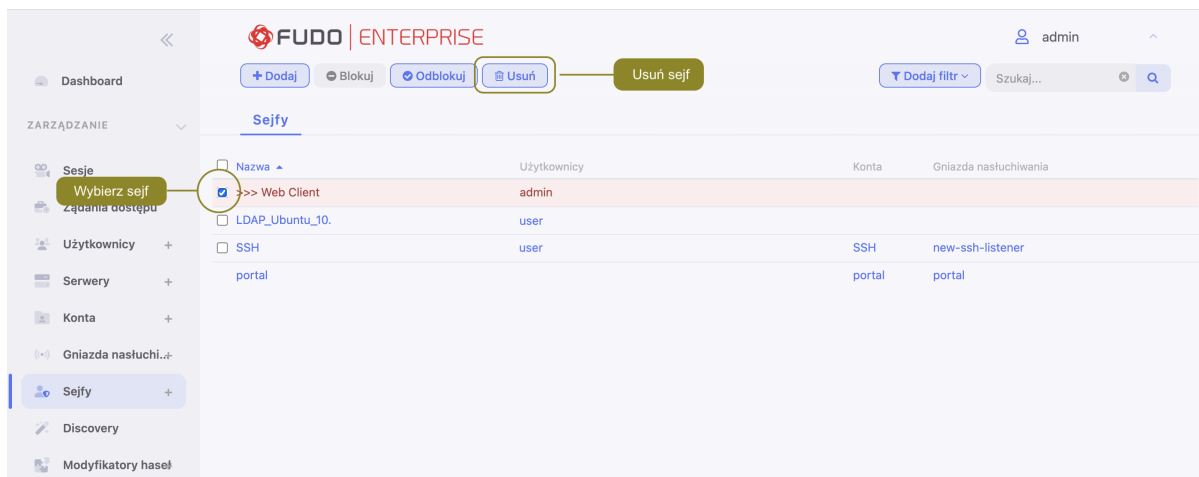
12.5 Usuwanie sejfów

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

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*

Żądania dostępu

Wysłanie żądania na potrzeby dostępu do zasobów jest podstawą funkcjonalności **Just In Time**. Użytkownik wysyłający ma do wyboru dwa typy żądania: **natychmiastowy** lub **zaplanowany**.

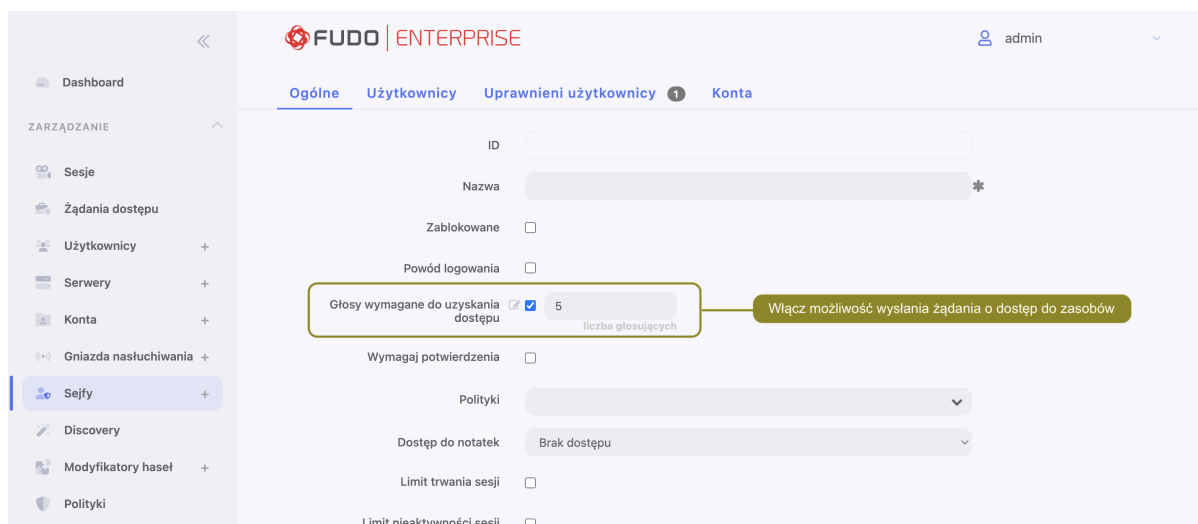
W przypadku wybrania **natychmiastowego** typu żądania, użytkownik może ustalić okres dostępu od zaraz do maksymalnie 24 godzin. Okres dostępu użytkownika zaczyna się w momencie zatwierdzenia żądania przez administratora - wtedy ma on 24 godziny na rozpoczęcie sesji. Kiedy użytkownik rozpoczyna sesję, 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 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.



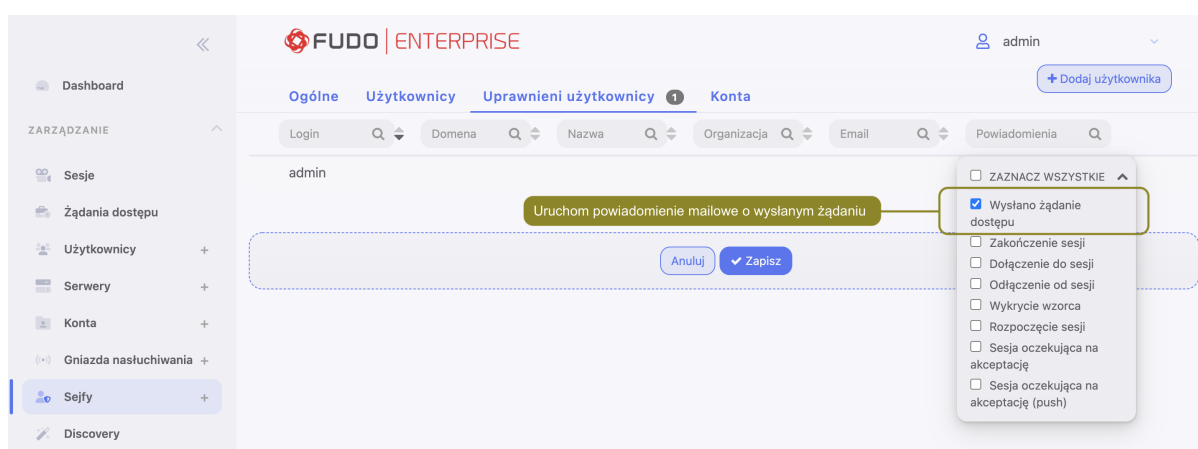
Informacja: Użytkownicy o rolach *Admin* oraz użytkownicy dodani do sejfu jako *Uprawnieni użytkownicy* mogą głosować o udzielenie dostępu.

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*.

13.1 Żądania oczekujące

Żądania oczekujące decyzji uprawnionych osób są widoczne w zakładce *Żądania dostępu* pod sekcją *Zarządzanie*.

Uż...	Data ↓	Wa...	Powód	P..	Konto	G...	Sejf	S..	Klie...	Glosy	Akcja
tp...	2021-11-19 06:49:04	zapla...	2021-1...	For test 2	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.23...		ODPOWIEDZ
tpi...	2021-11-19 06:48:41	natyc...	2h	For test 2	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.23...		ODPOWIEDZ

Żeby zgłosić, wciśnij przycisk *Odpowiedz*. W modalu będzie widoczna szczegółowa informacja o wysłanym żądaniu. Wprowadź *Powód odpowiedzi* oraz wybierz opcję akceptacji albo odrzucenia.

Odpowiedz na prośbę

Konto SSH **Serwer** 10.0 **Gniazda nasłuchiwania** checkout, new-ssh-listener, **Protokół** ssh **Użytkownik** tpo **Data** 2021-11-19 06:49:04

For test 2

Typ prośby **zaplanowany** Wartość prośby **2021-11-20 00:01:00 - 2021-12-19 23:59:00**

Powód odpowiedzi (wymagane tylko w przypadku odrzucenia prośby):

0/250

Anuluj Odrzuć Zaakceptuj

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.`

13.2 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.

Uż...	Data ↓	W...	Pow...	F...	K...	G...	Sejf	€	Kl...	Głosy	Akcja	
tpovar	2021-11-22 23:27:55	sche...	2021...	For w...	ssh	SSH	SSH	SSH	10.0...	100%	udziel	ANULUJ

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.

13.3 Archiwum żądań

Historia skompletowanych żądań jest widoczna w zakładce *Archiwum*.

Uż...	Data ↓	T...	Value	Powód	P...	Konto	G...	Sejf	S...	Klie...	Głosy	S...
tpovar	2021-11-19 06:49:04	schedul...	2021-1...	For test 2	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	100%	1/1	anulowa
tpovar	2021-11-19 06:48:41	immedi...	2h	For test 2	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	100%	0/1	wygasły
tpovar	2021-11-18 01:17:40	immedi...	2h	kkk	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	100%	0/1	odrzuco
tpovar	2021-11-12 12:23:14	immedi...	2h	ijkjill	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	100%	1/1	udzielon
tpovar	2021-11-10 11:45:38	schedul...	2021-1...	For wor...	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	100%	1/1	udzielon
tpovar	2021-11-10 11:45:02	immedi...	4h	For work	ssh	SSH	checkout, new-ssh-listener	SSH	10.0.235.1	100%	0/1	wygasły

Informacja o dokonanych głosach na konkretne żądanie jest dostępna po najechaniu na rekord kolumny *Głosy*.

Głosy 1/1	
✓ zaakceptowany przez admin	2021-09-21 05:44:19
✗ anulowany przez admin	2021-09-21 05:47:25
stop	

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*

Wykrywanie (Discovery)

Funkcja *Discovery* umożliwia wyszukiwanie:

- kont o różnych poziomach uprawnień na serwerze kontrolera domeny,
- serwerów na serwerze kontrolera domeny,
- kont lokalnych na serwerach Windows.

Dodatkowe nazewnictwo, które zostało wprowadzone w ramach tej funkcjonalności do zakładki *Discovery*, zakładki *Konta* oraz zakładki *Serwery*:

- *Skaner* - główny komponent, służący do wykrywania kont i serwerów na serwerze docelowym. Może, ale nie musi posiadać reguły, definiujące akcje stosowane do wykrytych obiektów. Skaner może być uruchamiany manualnie lub automatycznie według ustawionego harmonogramu.
- *Reguła* pozwala ustalić kryteria do spełnienia dla obiektów, które mają zostać wykryte oraz akcje do nich zastosowane.
- *Kategoria konta* - poziom uprzywilejowania konta.
- *Konta Odkryte* - konta, które zostały wykryte na serwerze docelowym przez skaner.
- *Serwery Odkryte* - serwery, które zostały wykryte na serwerze docelowym przez skaner.
- *Konta Przydzielone* - konta, które zostały przydzielone do sejfu oraz / lub gniazda nasłuchiwania.
- *Serwery Przydzielone* - serwery, które zostały dodane do puli.
- *Konta / Serwery na kwarantannie* - konta lub serwery, które zostały zablokowane na serwerze docelowym.

Informacja:

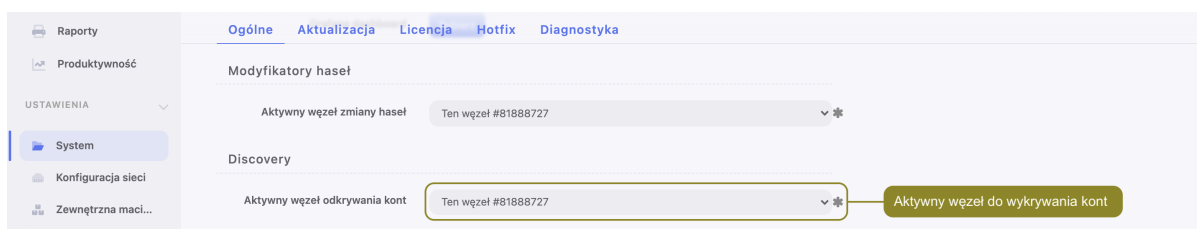
- Funkcja *Discovery* wykonuje skanowanie serwera Active Directory łącząc się przy pomocy protokołu LDAP.

- Do łączenia się z serwerem i skanowania w poszukiwaniu kont lokalnych wykorzystywany jest protokół WinRM.

Funkcja *Discovery* działa najskuteczniej ze skonfigurowanym skanerem oraz regułą. Reguła ma na celu zidentyfikowanie konta oraz wykonanie odpowiednich akcji. Skaner z kolei przeszukuje serwer docelowy pod kątem kont lub serwerów do wykrycia oraz przy dodanej regule wykonuje automatyczne przydzielenie.

Dla szybszej 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 lub serwery będą musiały być przydzielone przez administratora manualnie.

Informacja: Aktywny węzeł odkrywania kont jest ustawiony w sekcji *Discovery* zakładki *Ustawienia > System*.



14.1 Tworzenie reguły

Każda reguła może być włączona albo wyłączona. Kiedy reguła jest włączona, system automatycznie przydziela bądź wysyła na kwarantannę konta lub serwery, które spełniają zadane kryteria. Reguły działają na elementach **odkrytych**, lecz nie na elementach, które już zostały przydzielone albo wysłane na kwarantannę. W praktyce oznacza to, że jeśli działająca reguła została zmieniona, jej zmiany wejdą “w życie” już dla nowo odkrytych kont lub serwerów.

14.1.1 Tworzenie reguły dla kont

W celu stworzenia reguły postępuj zgodnie z poniższą instrukcją:

1. Wybierz *Zarządzanie > Discovery > Reguły*.
2. Kliknij *+ Dodaj*.



3. Wprowadź nazwę reguły.

4. Z rozwijanej listy *Typ skanera* wybierz *Konta*.
5. Opcjonalnie, wprowadź opis reguły.
6. W sekcji *Konfiguracja*:
 - 6.1. Wybierz *Kategorię konta* (*uprzywilejowany*, *nieuprzywilejowany* lub *wszystko*).
 - 6.2. W polu *Nazwa konta* wybierz *zawiera*, *zaczyna się od* lub *kończy się*, aby doprecyzować nazwę kont do wykrycia.
7. Ustaw *Akcje*:
 - 7.1. **Wyślij na kwarantannę**, lub
 - 7.2. **Przydziel** dodając konta do konkretnych sejfów oraz / lub gniazd nasłuchiwania. **Tylko gniazda nasłuchiwania o trybie połączenia bastion są wspierane.**

8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tworzenie skanera*
- *Zarządzanie wykrytymi kontami*

14.1.2 Tworzenie reguły dla serwerów

W celu stworzenia reguły postępuj zgodnie z poniższą instrukcją:

1. Wybierz *Zarządzanie* > *Discovery* > *Reguły*.
2. Kliknij *+* *Dodaj*.

	Nazwa	Typ	Sejfy	Gniazda naslu...	Stworzony	Opis	Skaner	Włączony/Wył...
<input checked="" type="checkbox"/>	Onboard_Domain...	Konta	marcin-DISCOVE...	RDP:bastion	2023-06-29 09:27	test-user1 => acc...	Domain_Accounts	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Onboard_Domain...	Serwery			2023-06-29 09:11	WIN7 => server o...	Domain_Servers	<input type="checkbox"/>
<input type="checkbox"/>	Onboard_Local A...	Konta	marcin-DISCOVE...	RDP:bastion	2023-06-29 13:09		Local Accounts	<input type="checkbox"/>

3. Wprowadź nazwę reguły.
4. Z rozwijanej listy *Typ skanera* wybierz *Serwery*.
5. Opcjonalnie, wprowadź opis reguły.
6. W sekcji *Konfiguracja*, w polu *Adres serwera* wybierz *zaczyna się od* lub *kończy się*, aby doprecyzować adres serwera do wykrycia.
7. Ustaw *Akcje*:
 - 7.1. **Wyślij na kwarantannę**, lub
 - 7.2. **Przydziel** dodając serwery do konkretnych puli.

8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tworzenie skanera*
- *Zarządzanie wykrytymi kontami*

14.2 Zarządzanie regułami

Każda reguła może być włączona albo wyłączona. Kiedy reguła jest włączona, system automatycznie przydziela bądź wysyła na kwarantannę konta lub serwery, które spełniają zadane kryteria. Reguły działają na elementach **odkrytych**, lecz nie na elementach, które już zostały

przydzielone albo wysłane na kwarantannę. W praktyce oznacza to, że jeśli działająca reguła została zmieniona, jej zmiany wejdą “w życie” już dla nowo odkrytych kont lub serwerów.

<input type="checkbox"/>	Nazwa	Typ	Sejfy	Gniazda naslu...	Stworzony	Opis	Skaner	Włączony/Wył...
<input checked="" type="checkbox"/>	Onboard_Domain...	Konta	marcin-DISCOVE...	RDP:bastion	2023-06-29 09:27	test-user1 => acc...	Domain_Accounts	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Onboard_Domain...	Serwery			2023-06-29 09:11	WIN7 => server o...	Domain_Servers	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Onboard_Local A...	Konta	marcin-DISCOVE...	RDP:bastion	2023-06-29 13:09		Local Accounts	<input checked="" type="checkbox"/>

Tematy pokrewne:

- *Tworzenie skanera*
- *Zarządzanie wykrytymi serwerami*
- *Zarządzanie wykrytymi kontami*

14.3 Tworzenie skanera

14.3.1 Tworzenie skanera dla kont kontrolera domeny

Funkcjonalność skanera polega na przeszukiwaniu serwera kontrolera domeny pod kątem kont o różnym stopniu uprzywilejowania i przyznaniu im dostępu poprzez dodanie do odpowiednich gniazd nasłuchiwania oraz / lub sejfów. Alternatywnie, wysłania kont na kwarantannę. Proces przyznania wykrytym kontom dostępu nazywa się *przydzieleniem*.

Informacja: Przed przystąpieniem do utworzenia skanera musisz skonfigurować:

- serwer, który ma zostać przeskanowany - zapoznaj się z rozdziałem *Serwery*,
- konto uprzywilejowane na tym serwerze (*Konta*) oraz
- pulę, do której chcesz przypisywać wykryte konta (*Pule*).

Polityka modyfikatora hasła oraz modyfikator i weryfikator hasła może zostać dodany w późniejszych krokach, już po zapisaniu skanera.

W celu stworzenia skanera postępuj zgodnie z poniższą instrukcją:

1. Wybierz *Zarządzanie > Discovery > Skanery*.
2. Kliknij *+ Dodaj*.
3. Wprowadź nazwę skanera.
4. Z listy *Typ skanera* Wybierz *Konta Kontrolera Domeny*.
5. Opcjonalnie, wprowadź opis skanera.
6. W sekcji *Harmonogram* wybierz dzień oraz czas, kiedy co tydzień skaner będzie uruchamiany przez system. Ten krok może zostać pominięty, jeśli administrator chce uruchamiać skaner manualnie.

7. W sekcji *Konfiguracja*:

7.1. Wybierz *Serwer docelowy*.

7.2. Wprowadź numer portu do serwera docelowego.

7.3. Wprowadź *Certyfikat CA*.

7.4. Opcjonalnie podaj wartość *Base DN* uszczegóławiającą lokalizację w domenie. Użyj następującego formatu: `cn=##username##,dc=example,dc=com`.

7.5. Opcjonalnie podaj wartość *Group DN* wskazującą konkretną grupę w domenie. Użyj następującego formatu: `cn=##username##,dc=example,dc=com`.

Informacja: Jeśli nie określono *Base DN* lub *Group DN*, skaner przeszuka całą domenę.

7.6. Wybierz *Konto* do połączenia z serwerem docelowym.

7.7. Wybierz *Kategorię konta* (*uprzywilejowany*, *nieuprzywilejowany* lub *wszystko*).

Informacja: Funkcja Discovery identyfikuje konta *uprzywilejowane* w Active Directory (AD) na podstawie przynależności do określonych grup, które oznaczają wysoki poziom praw i uprawnień. Aby zostać rozpoznanymi jako *uprzywilejowane* przez skaner Discovery, konta muszą należeć do jednej z czterech grup o wysokich uprawnieniach w AD:

- Enterprise Admins (EA),
 - Domain Admins (DA),
 - Built-in Administrators (BA),
 - Schema Admins (SA).
-

7.8. Wybierz pule, do których zostaną przypisane wykryte konta.

7.9. 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. W sekcji *Modyfikatory Haseł* wybierz *Polityka modyfikatora hasła*, *Modyfikator hasła* i/lub *Weryfikator haseł*, które będą automatycznie przypisane do odkrytych kont.

Informacja:

- Administrator może wstępnie zdefiniować wartości zmiennych w konfiguracji modyfikatorów haseł (patrz sekcja *Uniwersalne modyfikatory haseł*).
- Wstępne definiowanie wartości jest opcjonalne. Jeśli zmienna nie zostanie wstępnie zdefiniowana, przyjmie wartość z konta, do którego przypisany jest modyfikator hasła.
- Domyślne modyfikatory haseł nie mają predefiniowanych wartości zmiennych.

9. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tworzenie reguły*
- *Zarządzanie wykrytymi kontami*

14.3.2 Tworzenie skanera dla serwerów kontrolera domeny

Funkcjonalność skanera polega na przeszukiwaniu serwera kontrolera domeny pod kątem serwerów i przydzieleniu ich do odpowiednich pul. Alternatywnie, wysłania serwerów na kwarantannę. Proces przyznania wykrytym serwerom dostępu nazywa się *przydzieleniem*.

Informacja: Przed przystąpieniem do utworzenia skanera musisz skonfigurować:

- serwer, który ma zostać przeskanowany - zapoznaj się z rozdziałem *Serwery*,
- konto uprzywilejowane na tym serwerze - zapoznaj się z rozdziałem *Konta*.

W celu stworzenia skanera postępuj zgodnie z poniższą instrukcją:

1. Wybierz *Zarządzanie* > *Discovery* > *Skanery*.
2. Kliknij *+* *Dodaj*.
3. Wprowadź nazwę skanera.
4. Z listy *Typ skanera* Wybierz **Serwery Kontrolera Domeny**.
5. Opcjonalnie, wprowadź opis skanera.
6. W sekcji *Harmonogram* wybierz dzień oraz czas, kiedy co tydzień skaner będzie uruchamiany przez system. Ten krok może zostać pominięty, jeśli administrator chce uruchamiać skaner manualnie.
7. W sekcji *Konfiguracja*:
 - 7.1. Wybierz *Serwer docelowy*.
 - 7.2. Wprowadź numer portu do serwera docelowego.
 - 7.3. Wprowadź *Certyfikat CA*.
 - 7.4. Opcjonalnie podaj wartość *Base DN* uszczegóławiającą lokalizację w domenie. Użyj następującego formatu: `cn=##username##,dc=example,dc=com`.
 - 7.5. Opcjonalnie podaj wartość *Group DN* wskazującą konkretną grupę w domenie. Użyj następującego formatu: `cn=##username##,dc=example,dc=com`.

Informacja: Jeśli nie określono *Base DN* lub *Group DN*, skaner przeszuka całą domenę.

- 7.6. Wybierz *Konto* do połączenia z serwerem docelowym.
- 7.7. Podaj Certyfikat CA serwera, który zostanie przydzielony odkrytym serwerom.
- 7.8. 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*.

Tematy pokrewne:

- *Tworzenie reguły*
- *Zarządzanie wykrytymi kontami*

14.3.3 Tworzenie skanera dla kont lokalnych

Funkcjonalność skanera polega na przeszukiwaniu serwerów z puli w ścelu wykrycia kont lokalnych 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*.

Informacja: Przed przystąpieniem do utworzenia skanera musisz skonfigurować:

- pulę serwerów, która ma zostać przeskanowana - zapoznaj się z rozdziałem *Pule*,
- konto z uprzywilejowanym dostępem do serwerów w skanowanej puli - zapoznaj się z rozdziałem *Konta*.

Polityka modyfikatora hasła oraz modyfikator i weryfikator hasła może zostać dodany w późniejszych krokach, już po zapisaniu skanera.

W celu stworzenia skanera postępuj zgodnie z poniższą instrukcją:

1. Wybierz *Zarządzanie > Discovery > Skanery*.
2. Kliknij *+* *Dodaj*.
3. Wprowadź nazwę skanera.
4. Z listy *Typ skanera* Wybierz *Konta Lokalne Windows*.
5. Opcjonalnie, wprowadź opis skanera.
6. W sekcji *Harmonogram* wybierz dzień oraz czas, kiedy co tydzień skaner będzie uruchamiany przez system. Ten krok może zostać pominięty, jeśli administrator chce uruchamiać skaner manualnie.
7. W sekcji *Konfiguracja*:
 - 7.1. Wybierz pulę serwerów, w której ma zostać wykonane skanowanie.
 - 7.2. Wprowadź numer portu.
 - 7.3. Wprowadź *Certyfikat CA*.
 - 7.4. Wybierz *Konto* do połączenia z serwerem docelowym.

Informacja: Do utworzenia jednego skanera do skanowania kont lokalnych na wielu serwerach, wymagane jest posiadanie na każdym ze skanowanych serwerów konta administratora z dokładnie tą samą metodą uwierzytelniania.

7.5. 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. W sekcji *Modyfikatory Haseł* wybierz *Polityka modyfikatora hasła*, *Modyfikator hasła* i/lub *Weryfikator hasel*, które będą automatycznie przypisane do odkrytych kont.

Informacja:

- Administrator może wstępnie zdefiniować wartości zmiennych w konfiguracji modyfikatorów haseł (patrz sekcja *Uniwersalne modyfikatory haseł*).
- Wstępne definiowanie wartości jest opcjonalne. Jeśli zmienna nie zostanie wstępnie zdefiniowana, przyjmie wartość z konta, do którego przypisany jest modyfikator hasła.
- Domyślne modyfikatory haseł nie mają predefiniowanych wartości zmiennych.

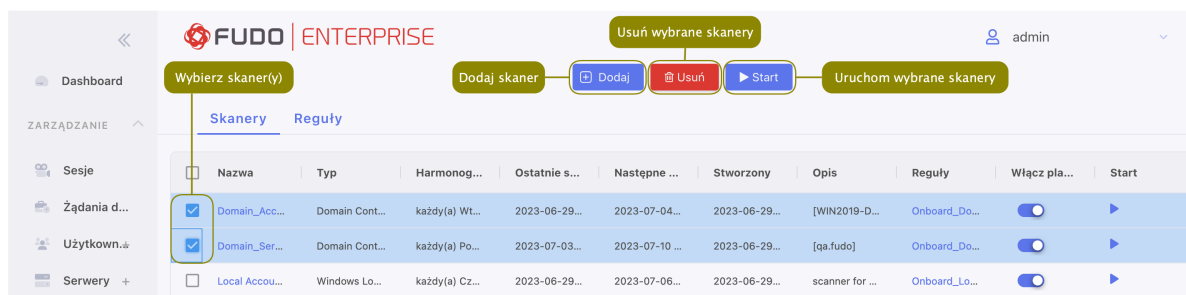
9. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tworzenie reguły*
- *Zarządzanie wykrytymi kontami*

14.4 Zarządzanie skanerami

Skanery ze zdefiniowanym harmonogramem mogą być włączone lub wyłączone. Jeśli harmonogram skanera jest włączony, system automatycznie wykona zadaną konfigurację. Jeśli natomiast harmonogram skanera jest wyłączony, system będzie czekać na decyzję administratora przed tym, jak wykonać zdefiniowaną akcję.



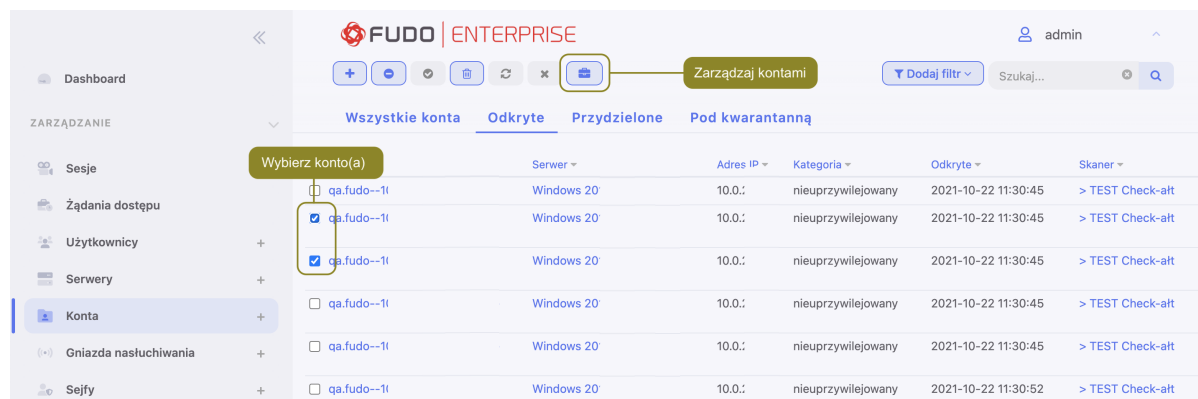
Można jednocześnie uruchomić lub usunąć kilka skanerów poprzez ich zaznaczenie i wybranie *Start* lub *Usuń*.

Tematy pokrewne:

- *Tworzenie reguły*
- *Zarządzanie wykrytymi serwerami*
- *Zarządzanie wykrytymi kontami*

14.5 Zarządzanie wykrytymi kontami

Konta *odkryte*, *przydzielone* oraz konta *pod kwarantanną* dostępne są w głównym widoku zakładki *Konta*.



Informacja: Konta, które znajdują się w zakładce *Odkryte* zostały wykryte przez skaner, lecz nie zostały ani przydzielone, ani wysłane na kwarantannę. Jest to zazwyczaj spowodowane brakiem ustawienia automatycznej reguły. Administrator może je przydzielić lub wysłać na kwarantannę manualnie, korzystając z opcji *Zarządzaj kontami* zlokalizowanej w górnym menu zakładki.

1. Wybierz *Zarządzanie > Konta > Odkryte*
2. Zaznacz konto(a), które chcesz *przydzielić* albo wysłać na kwarantannę.
3. Wybierz opcję *Zarządzaj kontami*.
4. Wybierz akcję:
 - 4.1 **Wyślij na kwarantannę** (opcjonalnie podaj powód) lub
 - 4.2 **Przydziel** dodając konta do konkretnych sejfów oraz / lub gniazd nasłuchiwania. **Tylko gniazda nasłuchiwania o trybie połączenia bastion są wspierane.**

5. Kliknij *Utwórz regułę*, jeśli chcesz uruchomić powtarzanie zdefiniowanej czynności.

6. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tworzenie reguły*
- *Tworzenie skanera*

14.6 Zarządzanie wykrytymi serwerami

Serwery *odkryte*, *przydzielone* oraz *pod kwarantanną* dostępne są w głównym widoku zakładki *Serwery*.

Informacja: Serwery, które znajdują się w zakładce *Odkryte* zostały wykryte przez skaner, lecz nie zostały ani przydzielone, ani wysłane na kwarantannę. Jest to zazwyczaj spowodowane brakiem ustawienia automatycznej reguły. Administrator może je przydzielić lub wysłać na kwarantannę manualnie, korzystając z opcji *Zarządzaj serwerami* zlokalizowanej w górnym menu zakładki.

1. Wybierz *Zarządzanie > Serwery > Odkryte*
2. Zaznacz serwery, które chcesz przydzielić albo wysłać na kwarantannę.
3. Wybierz opcję *Zarządzaj serwerami*.

4. Wybierz akcję:

4.1 **Przydziel** dodając konta do konkretnej puli lub

4.2 **Wyślij na kwarantannę** i podaj powód (wymagane).

5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tworzenie reguły*
- *Tworzenie skanera*

Fudo Enterprise 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*.

Wbudowane 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

15.1 Polityki haseł

Polityka zmiany haseł określa częstotliwość zmiany hasła oraz jego złożoność.

15.1.1 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 nieuprawniony.

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*.

15.1.2 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*.

15.1.3 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*

15.2 Uniwersalne modyfikatory haseł

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

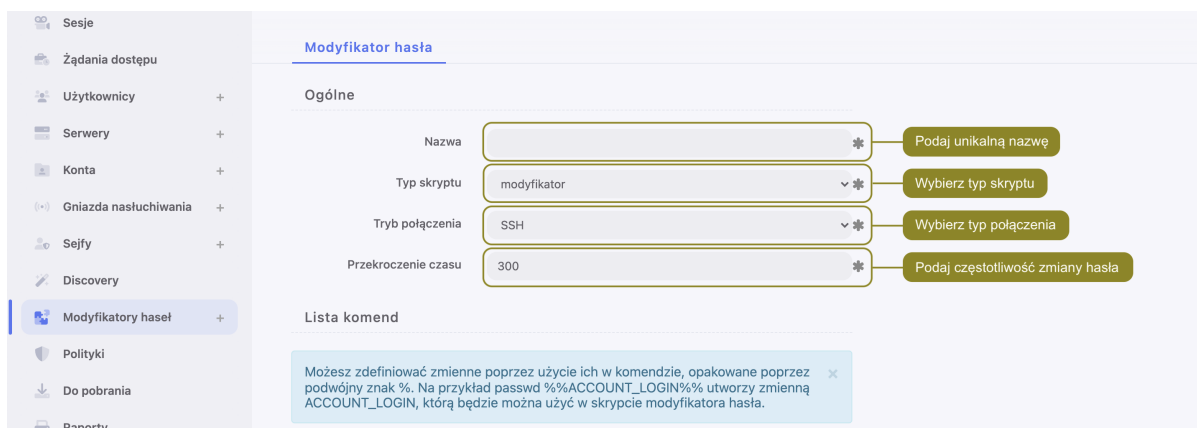
Informacja: W konfiguracji klastrowej, zmiana haseł realizowana jest przez wybrany węzeł, wskazany w ustawieniach systemowych. Więcej informacji na temat zmiany aktywnego węzła klastra, znajdziesz w rozdziale *Modyfikatory haseł - aktywny węzeł klastra*.

15.2.1 Definiowanie modyfikatora haseł

Informacja: Fudo Enterprise umożliwia tworzenie modyfikatorów haseł na podstawie istniejących definicji. Otwórz formularz edycji istniejącego skryptu i kliknij *Kopiuj*, aby stworzyć nowy obiekt na podstawie wybranej definicji.



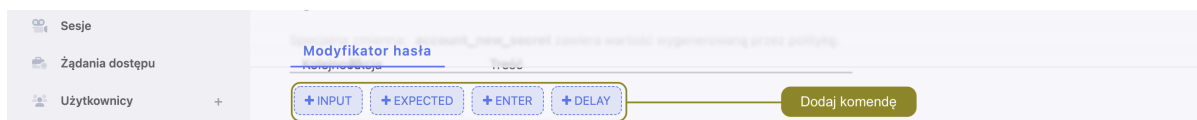
1. Wybierz z lewego menu *Zarządzanie > Modyfikatory haseł*.
2. Wybierz zakładkę *Własne modyfikatory*.
3. Kliknij *+ Dodaj*.
4. W sekcji *Ogólne*, wprowadź nazwę modyfikatora haseł.
5. Z listy rozwijalnej *Typ skryptu*, wybierz czy definiowany obiekt jest modyfikatorem czy weryfikatorem hasła.
6. Z 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 Enterprise 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.

The screenshot displays the 'Modyfikator' configuration screen. On the left is a sidebar with navigation options like 'Sejfy', 'Discovery', 'Modyfikatory haseł', etc. The main area is titled 'Modyfikator' and 'Zmienne'. It features a table with the following columns: 'Nazwa zmiennej', 'Rodzaj obiektów', 'Atrybut', 'Predefiniowana wartość', and 'Zaszyfruj'. Annotations include:

- 'Wybierz rodzaj obiektu' pointing to the 'Rodzaj obiektów' dropdown.
- 'Przypisz wartość' pointing to the 'Atrybut' dropdown.
- 'Predefiniuj wartości dla funkcji Discovery' pointing to the 'Predefiniowana wartość' field.
- 'Zszyfruj wartość zmiennej' pointing to the 'Zaszyfruj' checkbox.

 The table contains several rows, with the last row having the 'Zaszyfruj' checkbox checked. At the bottom are 'Anuluj' and 'Zapisz' buttons.

Informacja: Dzięki predefiniowanym wartościom modyfikator haseł przypisany do konta podczas procesu *Wykrywanie (Discovery)* nie wymaga żadnej dodatkowej konfiguracji.

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 <code>transport_secret</code> 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 <code>account_login</code> reprezentuje login użytkownika, któremu jest zmieniane hasło.
5	EXPECTED	Password	Spodziewany wyraz «Password» w treści konsoli.
6	INPUT	%%transport_secret%%	Zmienna <code>transport_secret</code> 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
<code>transport_method</code>	constant		
<code>transport_bind_to</code>	server_property	<code>bind_ip</code>	
<code>transport_user</code>	account	<code>login</code>	
<code>transport_host</code>	server_address_property	<code>host</code>	
<code>transport_port</code>	server_property	<code>port</code>	
<code>transport_secret</code>	account	<code>secret</code>	
<code>transport_host_public_key</code>	constant		
<code>account_login</code>	account	<code>login</code>	

15.2.2 Edytowanie uniwersalnego modyfikatora haseł

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

3. Znajdź i kliknij wybrany modyfikator.
4. Zmień wybrane komendy.
5. Kliknij *X*, aby usunąć komendę.
6. Kliknij *Zapisz*.

15.2.3 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*

15.3 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.

15.3.1 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, skutkuje 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.

15.3.2 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 zdefiniowaną tylko jedną komendę.

Zmienne

Zmienna	Opis
transport_base	Parametr <i>base DN</i> 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.

15.3.3 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 wykonanymi 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.

15.3.4 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 wykonywanymi 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 Enterprise nie może obsłużyć. **Upewnij się, że zmienne `account_login` i `transport_login` mają różne wartości.**

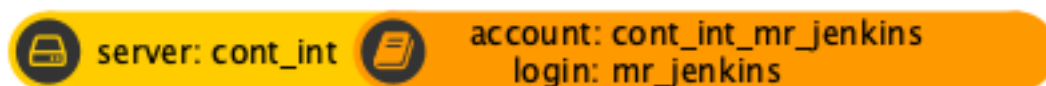
Zmienna	Opis
<code>transport_bind_ip</code>	Adres IP używany przez Fudo przy komunikacji ze zdalnym systemem.
<code>transport_ca_certificate</code>	Certyfikat CA systemu docelowego.
<code>transport_encoding</code>	Kodowanie tekstu na systemie docelowym.
<code>transport_host</code>	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
<code>transport_login</code>	Nazwa konta na systemie docelowym, służącego do zmiany hasła. Wskazane konto musi być różne od konta, na którym jest zmieniane hasło (zmienna <code>account_login</code>).
<code>transport_port</code>	Numer portu, służący do nawiązania połączenia z systemem docelowym.
<code>transport_secret</code>	Sekret służący do uwierzytelnienia konta wykorzystywanego w procesie zmiany hasła.
<code>account_login</code>	Login użytkownika, któremu jest zmieniane hasło.
<code>account_new_secret</code>	Zmienna systemowa, inicjowana wartością automatycznie wygenerowaną przez Fudo.

Tematy pokrewne:

- *Uniwersalne modyfikatory haseł*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

15.4 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*.

The screenshot shows the 'Polityka' configuration page. On the left is a sidebar menu with 'Modyfikatory haseł' selected. The main area has a 'Name' field with a tooltip 'Podaj unikalną nazwę'. Below it are two rows: 'Zmiana hasła włączona' with a checked checkbox and '10' minutes, and 'Weryfikacja hasła włączona' with a checked checkbox and '5' minutes. A tooltip 'Włącz częstotliwość zmiany / weryfikacji haseł' points to these rows. Under 'Specyfikacja hasła', there are fields for 'Długość' (with a tooltip 'Ustaw jak złożone ma być hasło'), 'Małe litery' (0), 'Wielkie litery' (2), 'Znaki specjalne' (2), and 'Cyfry' (2). At the bottom are 'Anuluj' and 'Zapisz' buttons.

3. Wprowadź nazwę polityki zmiany haseł.

Informacja: Opisowa nazwa pozwoli osobom administrującym Fudo Enterprise, 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*

Polityki to grupy definicji scenariuszy pozwalające na proaktywny monitoring przebiegu sesji. W przypadku wykrycia scenariusza, Fudo Enterprise może automatycznie wykonać stosowne akcje oraz powiadomić administratora.

Fudo Enterprise umożliwia budowanie mechanizmu na podstawie **modułu AI** lub **Wzorca** (Wyrażenia regularnego):

- przy wyborze **modułu AI** jako podstawy polityki, polityka będzie uruchamiana, kiedy pewien próg *Prawdopodobieństwa Zagrożenia* zostanie przekroczony;
- kiedy się wybierze **wzorzec** jako podstawę polityki, system będzie się spodziewał podania scenariusza dla wykrycia konkretnych danych wejściowych / wyjściowych.

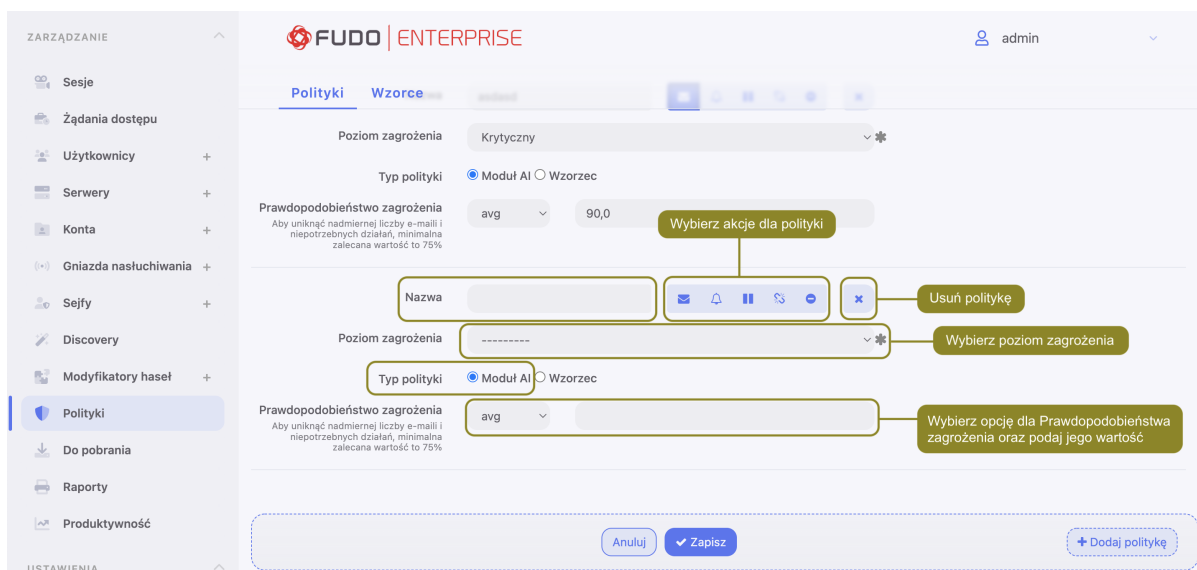
Obydwa rodzaje polityk reagują konkretną sekwencją działań, kiedy scenariusz polityki wykonuje się użytkownikiem podczas sesji:

- wysłanie wiadomości mailowej,
- wysłanie powiadomienia SNMP TRAP,
- wstrzymanie sesji,
- przerwanie sesji,
- blokowanie użytkownika.

16.1 Definiowanie polityki na podstawie modułu AI

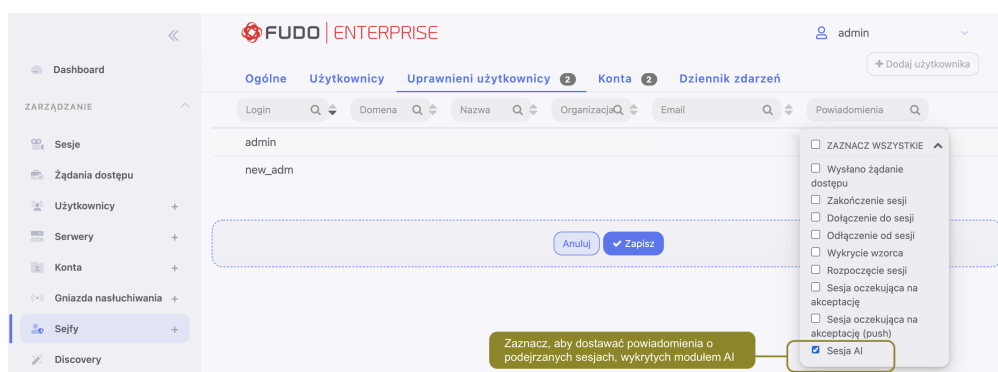
Aby skonfigurować politykę na podstawie modułu AI, postępuj zgodnie z instrukcją:

1. Wybierz *Zarządzanie > Polityki*.
2. Kliknij *Dodaj politykę*.
3. Podaj nazwę dla polityki.



4. Wybierz czynności do wykonania, kiedy scenariusz polityki będzie wykryty podczas sesji:
- Wyślij email.

Informacja: Wysłanie wiadomości mailowej wymaga konfiguracji oraz uruchomienia *usługi notyfikacji*, a także ustawienia notyfikacji typu *Sesja AI* w Sejfie.



- Wyślij notyfikację SNMP TRAP.

Informacja: Wysłanie powiadomień SNMP TRAP wymaga konfiguracji SNMPv3 TRAP w zakładce Ustawienia > System. Wejdź do strony *SNMPv3 TRAP* po więcej informacji.

- wstrzymaj sesję.
- zakończ sesję.
- zablokuj użytkownika.

Ostrzeżenie: Jeśli usługa SNMP TRAP nie została skonfigurowana, powiadomienia o naruszeniu polityki nie będą dostarczane, ale reszta opcji będzie wykonywana.

- Wybierz *Poziom zagrożenia*. Ten parametr jest wykorzystywany przy wysłaniu wiadomości mailowej oraz dodawany do Dziennika zdarzeń z kodem FSW0284.
- Zaznacz Moduł AI w polu *Typ polityki*.
- Wybierz opcję *min*, *średni* albo *maks* w polu *Prawdopodobieństwo zagrożenia*, podaj wartość.

Informacja: Wartości dla *Prawdopodobieństwa zagrożenia* są kalkulowane *modelem behawioralnym* dla każdego segmentu sesji. Oceny segmentów są uśredniane per model (Mouse Biometric, Keyboard Biometric), tworząc *Prawdopodobieństwo zagrożenia Modelu*, co powoduje, że moduł AI dostarcza jedną wartość dla Prawdopodobieństwa zagrożenia dla całej sesji. Te wartości są wykorzystywane w polityce, a jej działania przeprowadzane na podstawie minimum, średniej bądź maksimum wartości Prawdopodobieństwo zagrożenia Modelu.

W praktyce, jeśli administrator chce zmniejszyć czułość polityki w taki sposób, by ona reagowała na przekroczenie progu przez **wszystkie modele**, *Prawdopodobieństwo zagrożenia* ustawia się na **minimum**. Jeśli sytuacja wymaga, by polityka była bardziej czuła i wykonywała akcje po przekroczeniu progu przez **co najmniej jeden model**, wtedy *Prawdopodobieństwo zagrożenia* ustawia się na **maximum**.

Domyślnie wybrana opcja dla *Prawdopodobieństwa zagrożenia* jest **średni**.

- Aby uniknąć nadmiernej liczby e-maili i niepotrzebnych działań, minimalna zalecana wartość dla *Prawdopodobieństwa zagrożenia* to 75%.
- Dla drastycznych akcji, na przykład przerwanie połączenia bądź blokowania użytkownika, jest polecane korzystanie z maksymalnych progów, aby zminimalizować konsekwencje fałszywie dodatnich wyników.

- Kliknij *Zapisz*.

Informacja: Dodaj stworzoną politykę do *sejfu*, wykorzystywanego do połączeń.

Przykłady definiowania polityki na podstawie modułu AI

Przykład 1. Wysyłanie notyfikacji SNMP TRAP o podejrzanych sesjach.

Aby skonfigurować politykę, wysyłającą notyfikacje SNMP TRAP o podejrzanych sesjach, postępuj zgodnie z instrukcją:

1. Stwórz użytkownika o roli **service** dla usługi SNMPv3:
 - Wybierz *Zarządzanie > Użytkownicy*.
 - Stwórz nowego użytkownika.
 - Wprowadź Login.
 - Wybierz **service** w polu *Rola*.
 - Wybierz **Hasło** w polu *Typ uwierzytelniania* i podaj hasło.
 - W sekcji *SNMP* podaj ustawienia:
 - Włącz SNMP.
 - Wybierz **SHA** albo **MD5** w polu *Metoda uwierzytelniania*.
 - Wybierz **AES** albo **DES** w polu *Szyfrowanie* .
 - Kliknij *Zapisz*.
2. Skonfiguruj SNMPv3 TRAP:
 - Wybierz *Ustawienia > System*.
 - Przewiń do sekcji *Serwisowanie i nadzór*.
 - Podaj *adres* serwera SNMPv3 TRAP oraz *port*.
 - Wybierz użytkownika o roli **service**, stworzonego na kroku 1.
 - Kliknij *Zapisz*.
3. Stwórz politykę:
 - Wybierz *Zarządzanie > Polityki*.
 - Kliknij *Dodaj politykę*.
 - Podaj nazwę dla polityki.
 - Wybierz opcję *SNMP TRAP*.
 - Wybierz moduł **AI** w polu *Typ polityki*.
 - W polu *Prawdopodobieństwo zagrożenia* wybierz opcję (na przykład, **średni**) i podaj jej wartość (na przykład, **90%**).
 - Kliknij *Zapisz*.
4. Dodaj stworzoną politykę do *sejfu*, wykorzystywanego do połączeń.

Przykład 2. Przerwanie podejrzanych sesji, kiedy próg Prawdopodobieństwa zagrożenia zostanie przekroczony.

Aby skonfigurować politykę, przerywającą podejrzane sesje, kiedy próg Prawdopodobieństwa zagrożenia zostanie przekroczony, postępuj zgodnie z instrukcją:

1. Stwórz politykę:
 - Wybierz *Zarządzanie > Polityki*.

- Kliknij *Dodaj politykę*.
- Podaj nazwę dla polityki.
- Wybierz opcję *Zakończ sesję*.
- Wybierz moduł AI w polu *Typ polityki*.
- W polu *Prawdopodobieństwo zagrożenia* wybierz opcję (na przykład, *średni*) i podaj jej wartość (na przykład, *90%*).
- Kliknij *Zapisz*.

2. Dodaj stworzoną politykę do *sejfu*, wykorzystywanego do połączeń.

16.2 Definiowanie polityki na podstawie wzorca

Informacja: Fudo Enterprise wspiera wyrażenia regularne opisane standardem *POSIX Extended*.

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

The screenshot shows the 'Polityki' (Policies) management interface. The left sidebar contains a menu with items like 'Sesje', 'Ządania dostępu', 'Użytkownicy', 'Serwery', 'Konta', 'Gniazda nastuchi', 'Sejfy', 'Discovery', 'Modyfikatory haseł', and 'Polityki'. The main area is titled 'Polityki' and 'Wzorce'. It features three input fields: 'Nazwa', 'Wzorzec', and 'Usuń' with a checkbox. At the bottom, there is a dashed box containing three buttons: 'Anuluj', 'Zapisz', and '+ Dodaj wzorzec'.

4. Zdefiniuj nazwę i ciąg znaków stanowiący wzorzec.

Informacja: Fudo Enterprise 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 wyrażen 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:]+.*justfilename
```

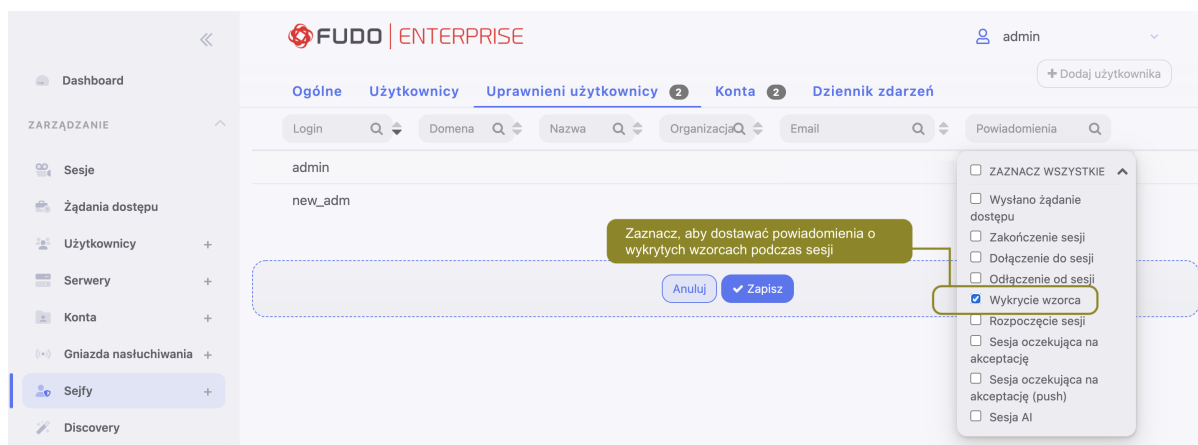
Definiowanie polityk

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

3. Wprowadź nazwę dla definiowanej polityki.
4. Określ akcje, które Fudo Enterprise podejmie z chwilą stwierdzenia wystąpienia któregoś ze wzorców.
 - Wyślij powiadomienie email do administratora systemu.
 - Wyślij notyfikację SNMP TRAP.
 - Wstrzymaj połączenie.
 - Przerwij połączenie.
 - Zablokuj konto użytkownika.

Informacja:

- Wysyłanie powiadomień wymaga skonfigurowania *usługi powiadomień* oraz zaznaczonej opcji *Wykrycie wzorca* w *ustawieniach sejfu*.



- Wysłanie powiadomień SNMP TRAP wymaga konfiguracji SNMPv3 TRAP w zakładce Ustawienia > System. Wejdź do strony *SNMPv3 TRAP* po więcej informacji.
- Zablokowanie użytkownika powoduje automatyczne przerwanie połączenia.

5. Wybierz wzorce śledzone w ramach danej polityki.
6. Określ poziom zagrożenia dla dodawanej polityki.

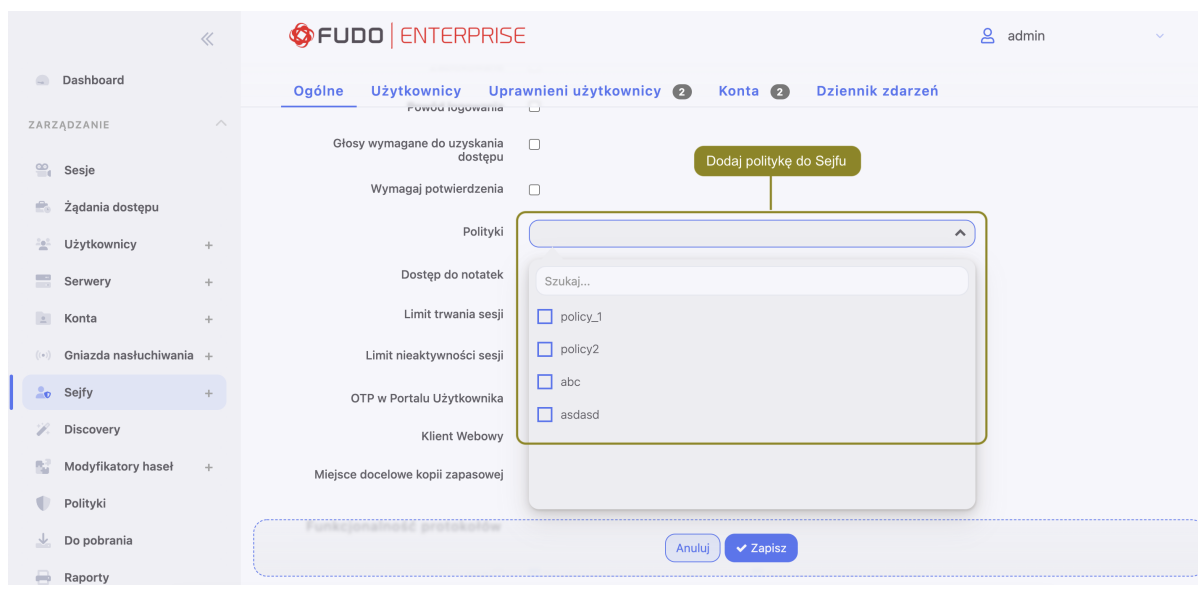
Informacja: Informacja o poziomie zagrożenia zawarta jest w treści powiadomienia.

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*.



Tematy pokrewne:

- *Sejfy*
- *Sztuczna inteligencja*
- *Przetwarzanie sesji - uczenie maszynowe*
- *Przerywanie połączenia*
- *Powiadomienia*
- *Bezpieczeństwo*

Do pobrania

Zakładka **Do pobrania** umożliwia śledzenie postępu konwersji wskazanych wcześniej do pobrania nagrań sesji oraz plików przesyłanych podczas sesji SFTP.

17.1 Sesje

Fudo Enterprise 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 dotycząca eksportowania sesji oraz dostępnych formatów zapisu znajduje się w rozdziale *Eksportowanie sesji*.

ID sesji	Użytkownik sesji	Serwer	Początek sesji	Rozmiar	Format	Rozdzielczość	Załadane w	Wzrost
2945354156300304445	OATH_User	TELNET_KI_mach	2024-02-27 00:48:47	1.3 KB	Dziennik zdarzeń	Automatyczna	2024-03-07 03:25:57	81059814
2945354156300304432	OATH_User	FACE	2024-02-26 01:46:29	641.9 KB	Spakowany katalog sesji (TGZ)	Automatyczna	2024-03-07 03:25:29	81059814
2945354156300304444	OATH_User	TELNET_KI_mach	2024-02-27 00:40:03	304.0 MB	MPEG-2 (popularny format)	Automatyczna	2024-03-07 03:25:01	81059814
2945354156300304466	OATH_User	TEL_5250_mach	2024-02-28 02:07:11	5.0 MB	DivX5 (AVI)	Automatyczna	2024-03-07 03:24:45	81059814
2945354156300304412	OATH_User	SSH_serwer	2024-02-26 00:56:15	11.3 KB	DivX5 (AVI)	Automatyczna	2024-02-27 04:34:12	81059814

17.2 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**.

The screenshot displays the SFTP session player interface. It shows a list of sessions with columns for time, ID, and name. The selected session is '2024-03-07 04:34:00 ID żądania: 6 Zapis'. The file details shown are: File name: /home/milo/Downloads/transfer.zip, Flags: ZAPIS, UTWÓRZ, OBETNIJ, Permissions: Owner rw, Grupa r, Inni r. The playback controls include a 'Pobierz transferowany plik' button and a 'File' button (highlighted with a red box) for downloading the file. Other buttons like 'Delta' are also visible.

4. Wybierz *Zarządzanie* > *Do pobrania*.
5. Przejdź do zakładki **Pliki**.
6. Kliknij i, aby pobrać wybrany materiał.

The screenshot shows the Fudo Enterprise management interface. The left sidebar has 'Do pobrania' highlighted with a red box. The main area shows the 'Pliki' tab selected. A table lists files with columns: ID, ID sesji, ID pliku, Rozmiar, Użytkownik sesji, Serwer, and Początek sesji. The 'Pobierz pliki' button is highlighted with a red box, and a red box around the download icon in the table indicates the action to be taken.

ID	ID sesji	ID pliku	Rozmiar	Użytkownik sesji	Serwer	Początek sesji
3	2945354156300304472	2945354156300304472_240307_043145_1728	304.0 MB	OATH_User	SSH_serwer	2024-03-07 04:31:45
2	2945354156300304472	2945354156300304472_240307_043145_1	304.0 MB	OATH_User	SSH_serwer	2024-03-07 04:31:45
1	2945354156300304470	2945354156300304470_240307_040255_5	304.0 MB	OATH_User	SSH_serwer	2024-03-07 04:02:55

Tematy pokrewne:

- *Eksportowanie sesji*

- *Sesje*

Aktywność konta w Portalu Użytkownika

Fudo Enterprise 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 bycia informowanym o zajętości zasobów, postępuj zgodnie z instrukcją:

1. Przejdź do *Zarządzanie > Serwery*.
 - Odszukaj na liście i wybierz serwer, który chcesz edytować.
 - Zaznacz opcję *Informuj o istniejącym połączeniu* w sekcji *Ustawienia*.
 - Kliknij *Zapisz* albo *Zapisz i wyjdź*
2. Przejdź do *Zarządzanie > Konta*.
 - Odszukaj na liście i wybierz konto 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).

- Kliknij *Zapisz*

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%%`.

1. Wybierz *Ustawienia > Zasoby > zakładkę User portal*.
2. Podaj tekst wiadomości w polu *Komunikat o zajętości zasobu*.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie serwera RDP*
- *Ekran logowania Portalu użytkownika*

Sesje

Fudo Enterprise 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 (<i>dotyczy sesji nagranych z opcją rejestrowania pełnego ruchu</i>).
	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 (<i>dotyczy sesji nagranych z opcją rejestrowania pełnego lub surowego ruchu</i>).
	Monitor aktywności użytkownika (<i>dotyczy sesji aktualnie trwających</i>).
	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 <i>niepodlegająca retencji</i> .
	Status analizy behawioralnej sesji. <i>Jest to wersja ewaluacyjna komponentu AI.</i> - 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 Enterprise przechowuje materiał sesji w formie skompresowanej, z czego wynikać mogą różnice pomiędzy podawanym a faktycznym rozmiarem sesji.

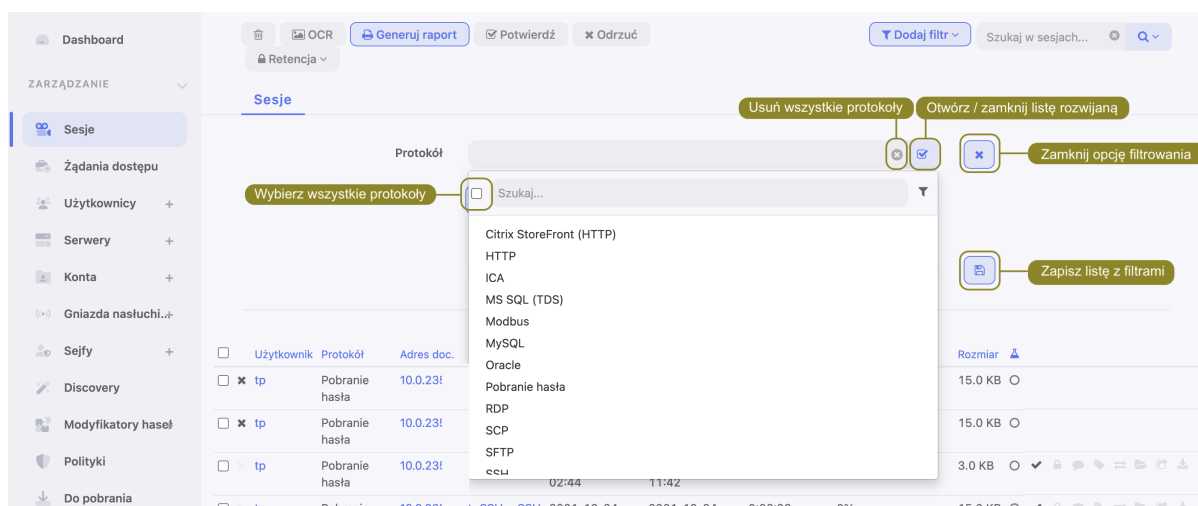


19.1 Filtrowanie sesji

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.

19.1.1 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.

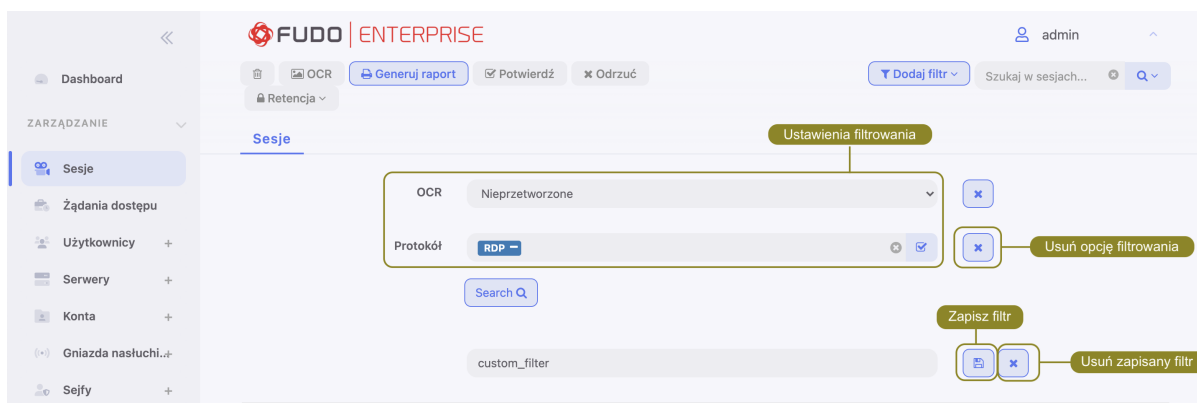
4. Kliknij *Dodaj filtr* i wybierz ponownie wcześniej zaznaczony parametr filtrowania, aby wyłączyć filtrowanie według zadanego parametru.

19.1.2 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 żadaną 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 żadaną definicję filtrowania.
2. Kliknij ikonę usunięcia definicji filtrowania.
3. Potwierdź usunięcie wybranej definicji filtrowania.

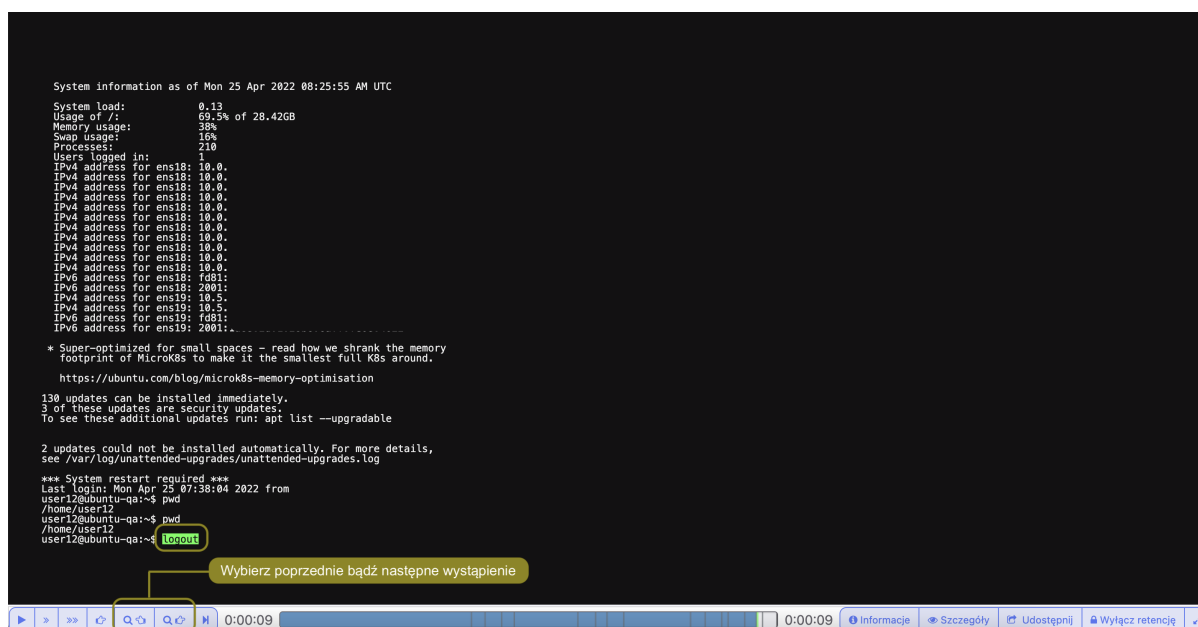
19.1.3 Przeszukiwanie pełnotekstowe

Fudo Enterprise 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*

19.2 Odtwarzanie sesji

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

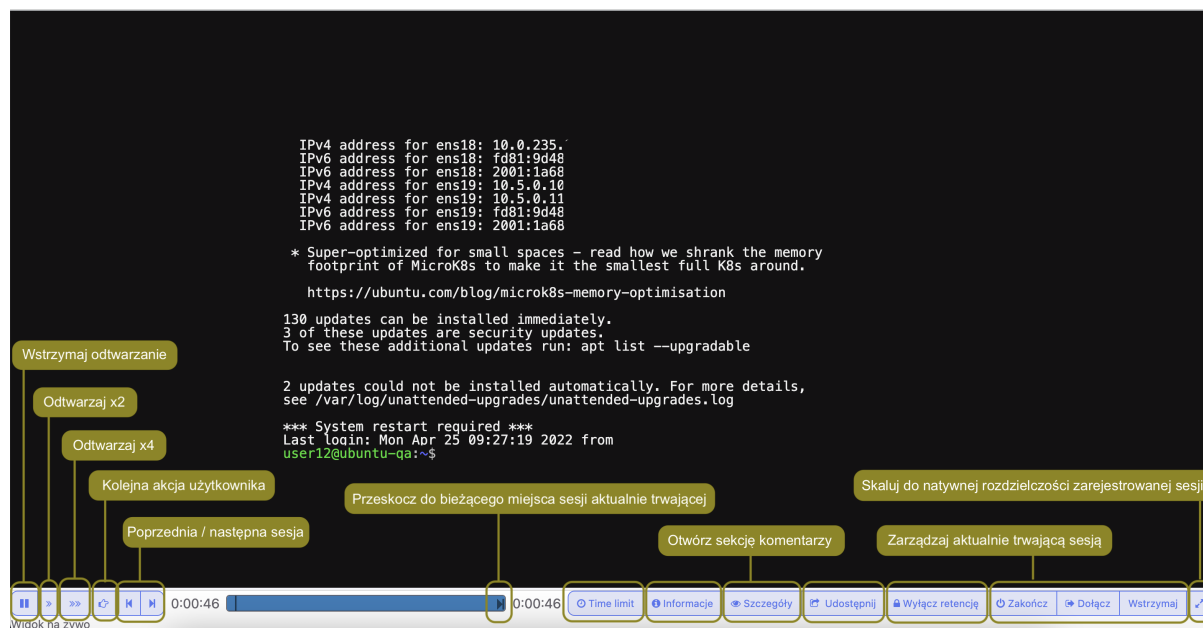
1. Wybierz z lewego menu *Zarządzanie > Sesje*.
2. Wyszukaj na liście żadaną sesję i kliknij ikonę rozpoczęcia odtwarzania.

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.

The screenshot shows the Fudo Enterprise dashboard with the 'Sesje' (Sessions) section active. The table displays the following data:

	Użytkownik	Protokół	Adres doc.	Konto	Sejf	Rozpoczęta	Zakończona	Czas trwania	Aktywność	Limit czasu	Rozmiar	
<input type="checkbox"/>	user	SSH	10.0.235.1:22	SSH_user12	main	2022-04-25 01:25	2022-04-25 01:26	0:00:09	100%	-	44.0 KB	🔄 📄 📁 📧 📧 📧 📧 📧
<input type="checkbox"/>	user	SSH	10.0.235.1:22	SSH_user12	main	2022-04-25 00:38	2022-04-25 00:38	0:00:42	100%	-	52.0 KB	🔄 📄 📁 📧 📧 📧 📧 📧

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/
/assets/components/Query.mmenu/dist/css/qj	GET	text/css	6.9 KB		http://10.0.150.150/
/assets/components/fancybox/jquery.fancybox	GET	text/css	4.8 KB		http://10.0.150.150/
/assets/css/style.css	GET	text/css	224.5 KB		http://10.0.150.150/
/assets/components/modernizr/modernizr.js	GET	application/javascript	50.2 KB		http://10.0.150.150/
/assets/js/build.js	GET	application/javascript	391.7 KB		http://10.0.150.150/
/assets/js/social.js	GET	application/javascript	865 bytes		http://10.0.150.150/
/assets/img/logo.svg	GET	image/svg+xml	8.3 KB		http://10.0.150.150/
/files/infosecurity_1920_en_r02.png	GET	image/png	747.1 KB		http://10.0.150.150/
Podgląd szczegółów żądania HTTP	GET	image/png	172.2 KB		http://10.0.150.150/
files/Banner_Fudo_1920_ENG.png	GET	image/png	773.7 KB		http://10.0.150.150/
/assets/fonts/Roboto-Regular_gdi.woff	GET	application/font-woff	26.0 KB		http://10.0.150.150/assets/css/style.css
/assets/fonts/Roboto-Light_gdi.woff	GET	application/font-woff	33.1 KB		http://10.0.150.150/assets/css/style.css
/assets/fonts/Roboto-Black_gdi.woff	GET	application/font-woff	33.0 KB		http://10.0.150.150/assets/css/style.css
/assets/img/bg-products.png	GET	image/png	371.5 KB		http://10.0.150.150/assets/css/style.css
/assets/img/img-top.png	GET	image/png	122 bytes		http://10.0.150.150/assets/css/style.css
/assets/img/btn-arrow-red.png	GET	image/png	249 bytes		http://10.0.150.150/assets/css/style.css
/files/Produkty/CERB%20Banking/ikony_cerb_	GET	image/png	35.6 KB		http://10.0.150.150/
/files/Produkty/LYNX/ikony_lynx_small_2.png	GET	image/png	29.5 KB		http://10.0.150.150/
/files/Produkty/FUDO/ikony_fudo_small_2.png	GET	image/png	26.6 KB		http://10.0.150.150/
/files/Loga%20klientow/mtel-imate-prijatelje.png	GET	image/png	3.1 KB		http://10.0.150.150/
/assets/img/product-shadow.png	GET	image/png	609 bytes		http://10.0.150.150/assets/css/style.css
/files/Produkty/CERB%20AS/ikony_cerb_small	GET	image/png	32.6 KB		http://10.0.150.150/
files/FUDO	GET	image/peg	108.9 KB		http://10.0.150.150/

Szczegóły żądania

Request	Response
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 referer: http://10.0.150.150/	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

SSH

Session 5746593124524813164

Not Secure https://10.0.180.1/sessions/5746593124524813164/?i=1

Session: 5746593124524813164, user: mmietusiewicz, server: dwt-centos

Time	Source	Destination	Size
2023-11-06 14:09:55	10.0.180.150:22	10.2.0.150:49889	5 bytes
2023-11-06 14:09:55	10.2.0.150:49889	10.0.180.150:22	1.2 KB
2023-11-06 14:09:55	10.0.180.150:22	10.2.0.150:49889	2.2 KB
2023-11-06 14:09:58	10.2.0.150:49889	10.0.180.150:22	1.0 KB

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	
Długość	32768
Pobierz plik od początku transmisji do bieżącego miejsca w sesji	
Dane	Podgląd danych

SCP

Sesja: 688817234205737383, użytkownik: user1, serwer: ssh1		
Nazwa pliku	Utworzony	Rozmiar pliku
fudo-3-37462.upg	2018-11-21 21:14:20	114.6 MB
Pobierz plik		

MySQL, MSSQL

The screenshot displays a web browser window with the URL `https://10.0.150.150/sessions/84838853211147120/?i=1`. The page title is "Sesja: 84838853211147120, użytkownik: john_smith, serwer: mssql_server".

Pakiet SQL

```
DECLARE @edition sysname; SET @edition = cast(SERVERPROPERTY(N'EDITION') as sysname); select case when @edition = N'SQL Azure' then 2 else 1 end as 'DatabaseEngineTy  
SELECT SERVERPROPERTY('EngineEdition') AS DatabaseEngineEdition  
select N'Windows' as host_platform
```

Wynik tabularyczny

host_platform
1
04000000
Windows

Pakiet SQL

```
IF ((SELECT HAS_PERMS_BY_NAME(null, null, 'VIEW SERVER STATE')) = 1) BEGIN IF EXISTS(SELECT * FROM sys.system_views WHERE name = N'dm_server_registry') SELECT value_d  
SERVERPROPERTY('ProductBuildType') AS [ProductBuildType],  
SERVERPROPERTY('ProductLevel') AS [ProductLevel],  
SERVERPROPERTY('ProductUpdateLevel') AS [ProductUpdateLevel],  
SERVERPROPERTY('ProductVersion') AS [ProductVersion]
```

At the bottom of the interface, there is a timer showing "00:00:00" and a "Przerwij połączenie" button. On the right side, there are several interactive buttons: "Zakończ", "Przerwij połączenie", "Wstrzymaj sesję", "Udostępnij zapis sesji", "Szczegóły połączenia", "Informacje", and "Udostępnij".

Modbus

Id	Time	Status	Data (Hex)	Delay
43	2015-04-30 15:17:42	0x7E (Nieznany komunikat)	05 03 10 00 00 30	+20 ms
44	2015-04-30 15:17:42	0x7E (Nieznany komunikat)	05 03 01 0F FF 51	+30 ms
45	2015-04-30 15:17:42	0x7E (Nieznany komunikat)	05 03 08 00 01 51	+25 ms
46	2015-04-30 15:17:42	0x7E (Nieznany komunikat)	05 03 10 00 00 40	+20 ms
47	2015-04-30 15:17:42	0x7E (Nieznany komunikat)	05 03 10 00 00 50	+30 ms
48	2015-04-30 15:17:42	0x7E (Nieznany komunikat)	05 03 10 00 00 60	+30 ms
49	2015-04-30 15:17:42	0x7E (Nieznany komunikat)	05 03 10 00 00 90	+20 ms
50	2015-04-30 15:17:42	0x7E (Nieznany komunikat)	05 03 10 00 00 A0	+11 ms

Tematy pokrewne:

- *Funkcjonalności wrażliwe*

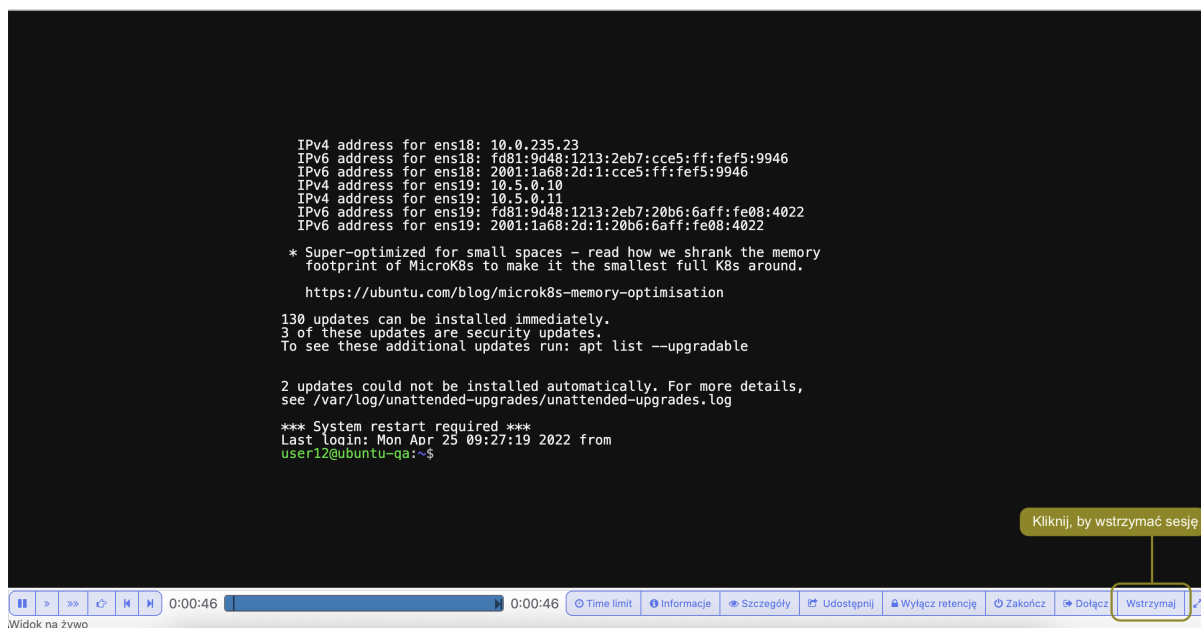
19.3 Wstrzymywanie połączenia

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 żadaną sesję i kliknij ikonę rozpoczęcia odtwarzania.
5. Kliknij *Wstrzymaj*.



Tematy pokrewne:

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

19.4 Przerwanie połączenia

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

Informacja: Fudo Enterprise 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.

```

IPv4 address for ens18: 10.0.235.23
IPv6 address for ens18: fd81:9d48:1213:2eb7:cce5:ff:fef5:9946
IPv6 address for ens18: 2001:1a68:2d:1:cce5:ff:fef5:9946
IPv4 address for ens19: 10.5.0.10
IPv4 address for ens19: 10.5.0.11
IPv6 address for ens19: fd81:9d48:1213:2eb7:20b6:6aff:fe08:4022
IPv6 address for ens19: 2001:1a68:2d:1:20b6:6aff:fe08:4022

* Super-optimized for small spaces – read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

  https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable

2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 09:27:19 2022 from
user12@ubuntu-qa:~$

```

Kliknij, by zakończyć sesję

Widok na żywo

6. Zdecyduj czy użytkownik powinien pozostać zablokowany.

Tematy pokrewne:

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

19.5 Dołączanie do sesji

Fudo Enterprise pozwala administratorowi na dołączenie do aktualnie trwającej sesji i jednocześnie pracę z użytkownikiem.

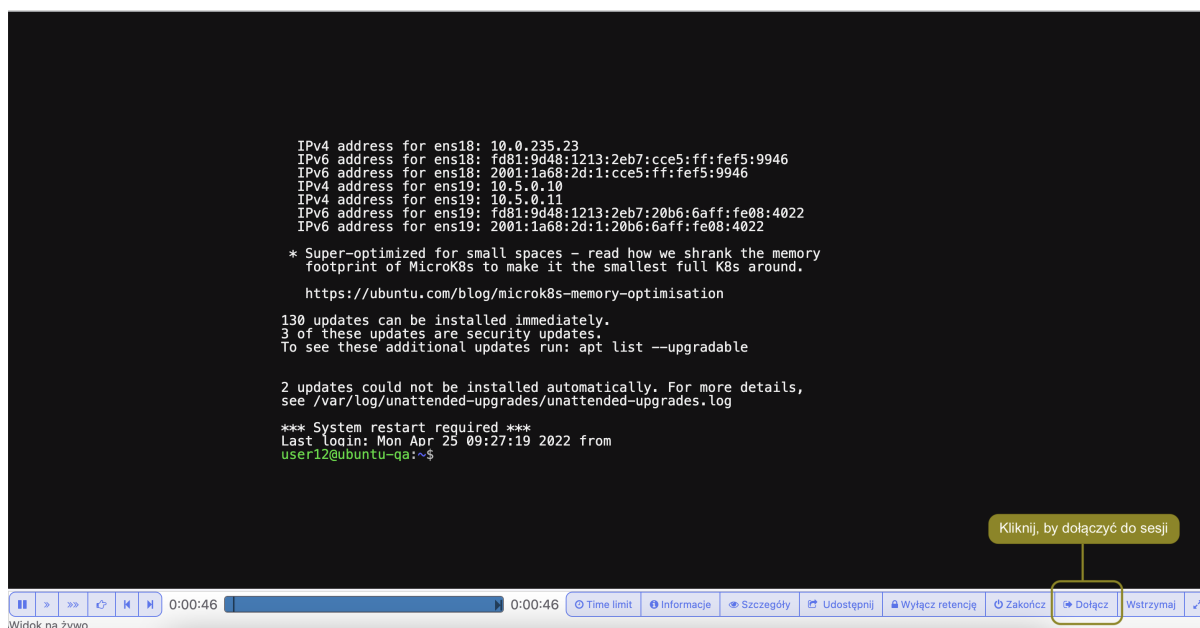
Informacja:

- 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 węzle, 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*

19.6 Udostępnianie sesji

Fudo Enterprise 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 *Udostępni*.

```

IPv4 address for ens18: 10.0.235.23
IPv6 address for ens18: fd81:9d48:1213:2eb7:cce5:ff:fe5:9946
IPv6 address for ens18: 2001:1a68:2d:1:cce5:ff:fe5:9946
IPv4 address for ens19: 10.5.0.10
IPv4 address for ens19: 10.5.0.11
IPv6 address for ens19: fd81:9d48:1213:2eb7:20b6:6aff:fe08:4022
IPv6 address for ens19: 2001:1a68:2d:1:20b6:6aff:fe08:4022

* Super-optimized for small spaces - read how we shrank the memory
  footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

130 updates can be installed immediately.
3 of these updates are security updates.
To see these additional updates run: apt list --upgradable

2 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Mon Apr 25 09:27:19 2022 from
user12@ubuntu-qa:~$

```

Kliknij, by udostępnić sesję

Widok na żywo

0:00:46 | 0:00:46 | Time limit | Informacje | Szczegóły | Udostępnij | Wyłącz retencję | Zakończ | Dołącz | Wstrzymaj

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

Udostępnij sesję

Zdefiniuj ramy czasowe dostępności sesji

Dostępne od
2014-03-07 16:02:02

Dostępne do
2014-03-08 00:02:02

Tylko do odczytu

Kliknij, aby wygenerować adres url dla sesji

Określ możliwość ingerencji w sesję - dotyczy sesji na żywo

Zamknij Udostępnij

- Skopiuj odnośnik i kliknij *Zamknij*.

Udostępnij sesję

Udostępnij ten adres

Skopiuj adres url, aby udostępnić zapis sesji

https://10.0.35.10/sessions/848388532111147457/?key=MdvjVmaS:848388532111147457:84

Zamknij

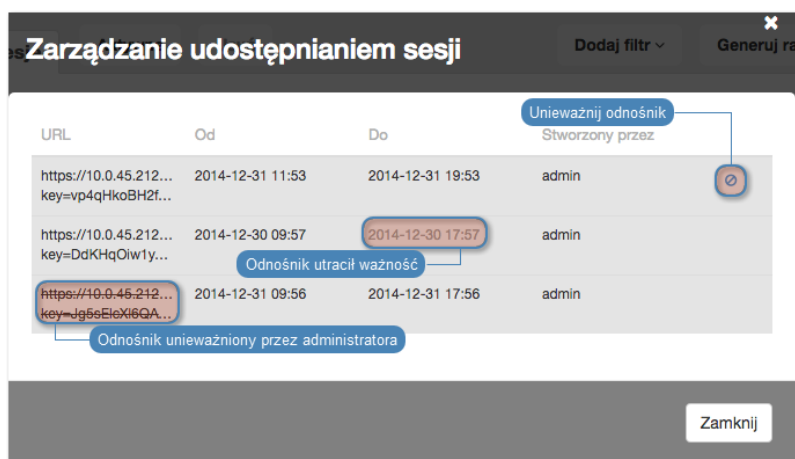
Zamknij okno udostępniania sesji

Unieważnienie odnośnika

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



- Kliknij ikonę unieważnienia odnośnika.



Tematy pokrewne:

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

19.7 Komentowanie sesji

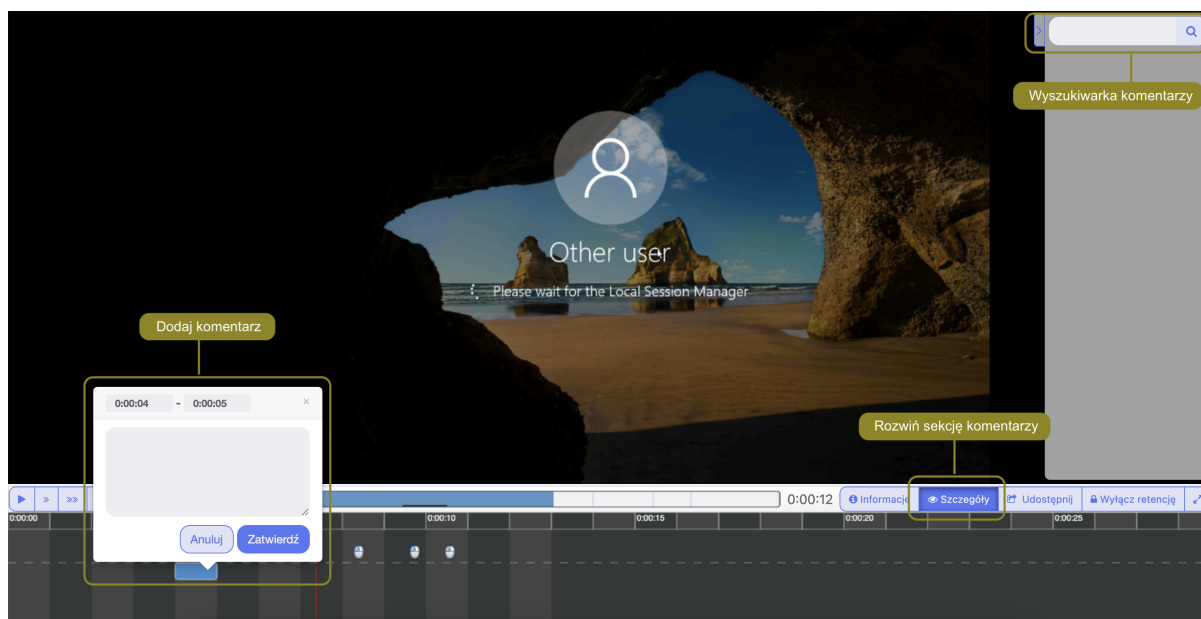
Fudo Enterprise pozwala na dodawanie komentarzy i znaczników do zarejestrowanych sesji.

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:

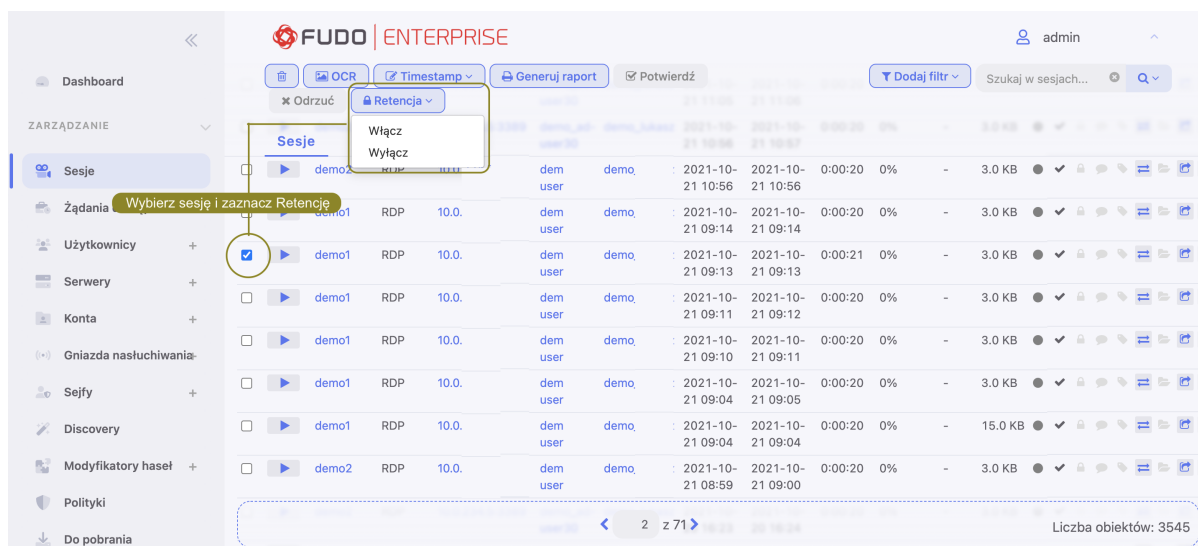
- *Funkcjonalności wrażliwe*

19.8 Zarządzanie retencją sesji

Mechanizm retencji danych automatycznie usuwa sesje po upływie zdefiniowanego interwału czasu. Fudo Enterprise umożliwia wykluczenie wybranych sesji z procesu retencji, aby nie zostały automatycznie usunięte.

Wyłączenie 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:

- *Kopia zapasowa systemu*
- *Filtrowanie sesji*
- *Konta*
- *Gniazda nastuchiwania*

19.9 Eksportowanie sesji

Fudo Enterprise 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 żadaną sesję i kliknij ikonę eksportu zarejestrowanego materiału.

The screenshot shows the 'Sesje' page in the Fudo Enterprise interface. The left sidebar contains navigation options like 'Dashboard', 'ZARZĄDZANIE', 'Sesje', 'Żądania dostępu', 'Użytkownicy', 'Serwery', 'Konta', 'Gniazda nastuchiwania+', 'Sejfy', 'Discovery', 'Modyfikatory haseł', and 'Polityki'. The main area shows a table of sessions with columns: 'Użytkownik', 'Protokół', 'Adres doc.', 'Konto', 'Sejf', 'Rozpoczęta', 'Zakończona', 'Czas trwania', 'Aktywność', 'Limit czasu', and 'Rozmiar'. A 'Pobierz sesję' button is highlighted in the top right corner of the table.

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* umożliwi monitorowanie postępu konwersji.

6. Kliknij ikonę pobrania sesji.

The screenshot shows the 'Do pobrania' page in the Fudo Enterprise interface. The left sidebar contains navigation options like 'ZARZĄDZANIE', 'Sesje', 'Żądania dostępu', 'Użytkownicy', 'Serwery', 'Konta', 'Gniazda nastuchiwania+', 'Sejfy', 'Discovery', 'Modyfikatory haseł', 'Polityki', 'Do pobrania', 'Raporty', and 'Produktywność'. The main area shows a table of converted sessions with columns: 'ID sesji', 'Użytkownik sesji', 'Serwer', 'Początek sesji', 'Rozmiar', 'Format', 'Rozdzielczość', 'Zażądane przez', 'Węzeł', and 'Węzeł'. A 'Pobierz skonwertowany materiał' button is highlighted in the top right corner of the table.

19.9.1 Dostępne formaty plików eksportu sesji

Poniższa tabela przedstawia zestawienie formatów plików dostępnych podczas eksportu sesji dla różnych protokołów.

	WebM	DivX5 (AVI)	Xvid (AVI)	MPEG-2	MJPEG	Flash Video (FLV)	Text log	TGZ	PCAP * **
SSH	x	x	x	x	x	x	x	x	x
RDP	x	x	x	x	x	x		x	
VNC	x	x	x	x	x	x		x	
HTTP	x	x	x	x	x	x		x	x
MySQL								x	
TCP								x	
MS SQL (TDS)								x	
Telnet	x	x	x	x	x	x	x	x	
Telnet 3270	x	x	x	x	x	x	x	x	
Telnet 5250	x	x	x	x	x	x	x	x	
SCP								x	
SFTP								x	

Informacja: * Eksport do pliku PCAP jest dostępny tylko dla sesji SSH z tunelowaniem oraz sesji HTTP bez renderowania.

** Eksport do pliku PCAP jest dostępny tylko, jeśli sesja została nagrana w formacie RAW. Aby dowiedzieć się więcej na temat opcji „all” lub „raw”, przejdź do [konfiguracji konta](#).

Podczas zapisywania sesji w formacie plików wideo (AVI, MPEG-2, MJPEG, FLV) dostępna jest możliwość wyboru jednej z poniższych rozdzielczości:

- 480p (852x480),
- 720p (1280x720),
- 1080p (1920x1080).

Tematy pokrewne:

- [Filtrowanie sesji](#)
- [Udostępnianie sesji](#)
- [Odtwarzanie sesji](#)
- [Dołączanie do sesji](#)

19.10 Usuwanie sesji

Informacja: Fudo Enterprise przechowuje powiązane z sesją pliki oraz nagrane wideo w zakładce *Zarządzanie > Do pobrania*. Zatem podczas usuwania sesji system usuwa też pliki, przechowywane w zakładce *Do pobrania > Pliki*. Natomiast nagrane wideo z sesją pod zakładką *Do pobrania > Sesje* zostają i mogą być pobrane w dowolnym momencie.

Aby usunąć zarejestrowaną sesję, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie > Sesje*.
2. Znajdź i zaznacz żądaną sesję.

	Użytkownik	Protokół	Adres doc.	Konto	Sejf	Rozpoczęta	Zakończona	Czas trwania	Aktywność	Limit czasu	Rozmiar
<input type="checkbox"/>	tpo	Pobranie hasła	10.0.1	SSH	SSH	2021-11-12 12:24	2021-11-12 12:30	0:05:15	0%	-	15.0 KB
<input checked="" type="checkbox"/>	tpo	Pobranie hasła	10.0.1	SSH	SSH	2021-11-10 02:44	2021-11-10 11:42	8:58:15	0%	-	3.0 KB
<input type="checkbox"/>	tpo	Pobranie hasła	10.0.1	SSH	SSH	2021-10-24 23:46	2021-10-24 23:52	0:06:00	0%	-	15.0 KB
<input type="checkbox"/>	tpo	Pobranie hasła	10.0.1	SSH	SSH	2021-10-11 01:24	2021-10-12 08:09	1 day, 4:45:18	0%	-	3.0 KB
<input type="checkbox"/>	tpo	Pobranie hasła	10.0.1	SSH	SSH	2021-10-11 01:16	2021-10-11 01:20	0:04:05	0%	-	3.0 KB
<input type="checkbox"/>	tpo	Pobranie hasła	10.0.1	SSH	SSH	2021-10-11 01:15	2021-10-11 01:15	0:00:53	0%	-	15.0 KB

3. Kliknij *Usuń*.
4. Potwierdź usunięcie sesji.

Informacja: Fudo Enterprise 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*

19.11 Przetwarzanie OCR sesji

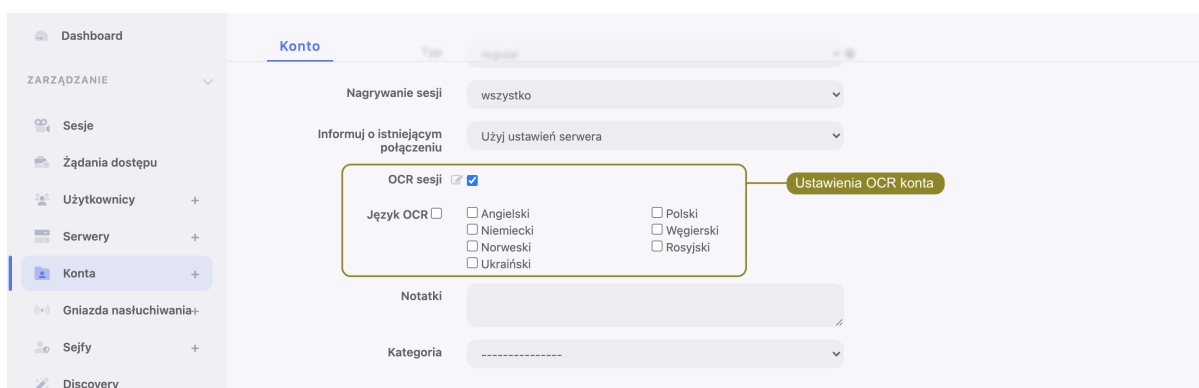
Zarejestrowany materiał sesji RDP i VNC oraz renderowanej sesji HTTP może być indeksowany na potrzeby przeszukiwania pełnotekstowego.

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.

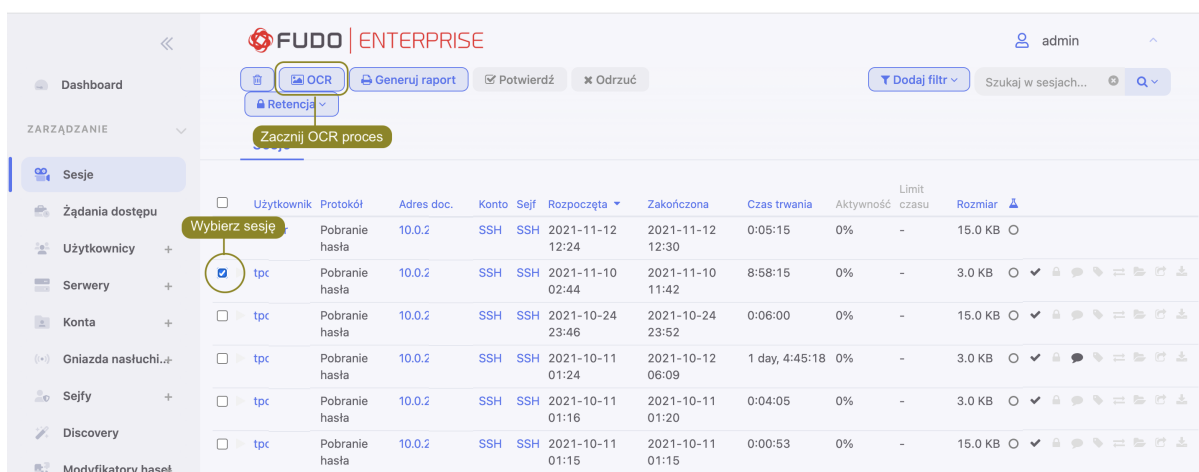


5. Kliknij *Zapisz*.

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 nie-

przetworzonych.


3. Zatwierdź przetwarzanie wybranych sesji.

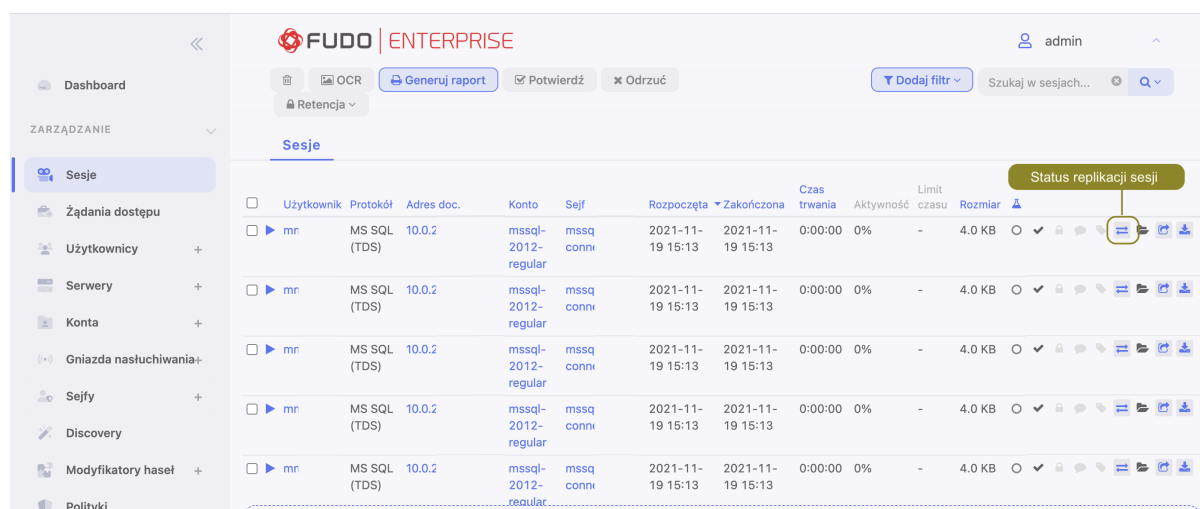
Tematy pokrewne:






- [Filtrowanie sesji](#)
- [Konta](#)
- [Gniazda nastuchiwania](#)

19.12 Replikacja sesji w konfiguracji klastrowej

Poza automatyczną replikacją danych w ramach konfiguracji klastrowej, Fudo Enterprise 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.



	Użytkownik	Protokół	Adres doc.	Konto	Sejf	Rozpoczęta	Zakończona	Czas trwania	Aktywność	Limit czasu	Rozmiar	Status replikacji sesji
<input type="checkbox"/>	mn	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
<input type="checkbox"/>	mn	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
<input type="checkbox"/>	mn	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
<input type="checkbox"/>	mn	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
<input type="checkbox"/>	mn	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	

Informacja: Opcja wysłania sesji do wybranych instancji Fudo Enterprise dotyczy węzłów, na które dane wybranej sesji nie są replikowane automatycznie.

3. Kliknij *Wyślij sesję* przy wybranym węźle, aby zreplikować dane na wskazany węzeł

Session replication info

user	protocol	server	account	safe	started_at	finished_at	duration	activity	size
Administrator	rdp	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32:11	2019-12-05 15:15:33	0:43:21	601	52.9 MB

Nazwa węzła	Status replikacji	Akcja
node-A	replicated	
node-B	not replicated	Send Session
node-C	replicated	
node-D	not replicated	Send Session
node-OCR	replicated	

Wyślij do wszystkich węzłów

lub *Wyślij do wszystkich węzłów*, aby dane sesji zostały zreplikowane na wszystkie węzły klastra.

Session replication info

user	protocol	server	account	safe	started_at	finished_at	duration	activity	size
Administrator	rdp	win2016-BL-DC-RDP	win2016-BL-DC-RDP	RDP-safe	2019-12-05 14:32:11	2019-12-05 15:15:33	0:43:21	601	52.9 MB

Nazwa węzła	Status replikacji	Akcja
node-A	replicated	
node-B	not replicated	Send Session
node-C	replicated	
node-D	not replicated	Send Session
node-OCR	replicated	

Wyślij do wszystkich węzłów

Tematy pokrewne:

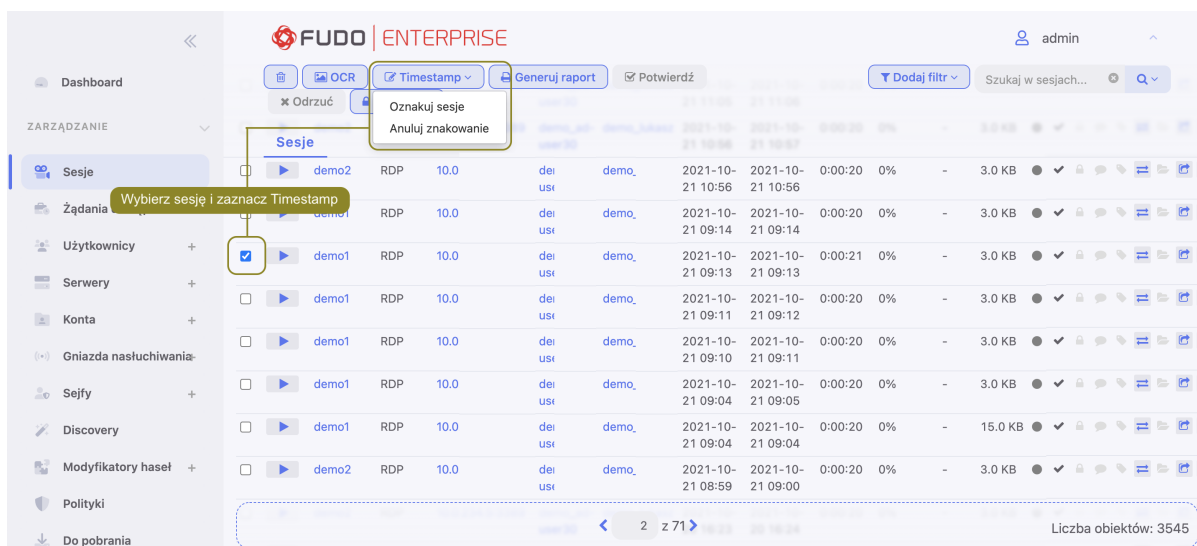
- *Konfiguracja klastrowa*
- *Sesje*

19.13 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 opatrzeć 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.

19.14 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*

19.15 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*.

Użytkownik	Protokół	Adres doc.	Konto	Sejf	Rozpoczęta	Zakończona	Czas trwania	Aktywność	Limit czasu	Rozmiar	Akcje
tpc	Pobranie hasła	10.0.2	SSH	SSH	2021-11-19 06:47			0%	-	3.0 KB	✓ ✕
tpc	Pobranie hasła	10.0.2	SSH	SSH	2021-11-12 12:24	2021-11-12 12:30	0:05:15	0%	-	15.0 KB	○
tpc	Pobranie hasła	10.0.2	SSH	SSH	2021-11-10 02:44	2021-11-10 11:42	8:58:15	0%	-	3.0 KB	○ ✓ ✕
tpc	Pobranie hasła	10.0.2	SSH	SSH	2021-10-24 23:46	2021-10-24 23:52	0:06:00	0%	-	15.0 KB	○ ✓ ✕
tpc	Pobranie hasła	10.0.2	SSH	SSH	2021-10-11 01:24	2021-10-12 06:09	1 day, 4:45:18	0%	-	3.0 KB	○ ✓ ✕

Tematy pokrewne:

- *Filtrowanie sesji*
- *Konta*
- *Gniazda nastuchiwania*

19.16 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*.

The screenshot shows the 'Sesje' (Sessions) management page in Fudo Enterprise. The interface includes a sidebar with navigation options like 'Dashboard', 'ZARZĄDZANIE', 'Sesje', 'Żądania dostępu', 'Użytkownicy', 'Serwery', 'Konta', 'Gniazda nasłuchi...', and 'Sejfy'. The main area displays a table of sessions with columns: Użytkownik, Protokół, Adres doc., Konto, Sejf, Rozpoczęta, Zakończona, Czas trwania, Aktywność, Limit czasu, and Rozmiar. A callout box labeled 'Odrzuć żądanie' points to a button in the top right. Another callout box labeled 'Wybierz sesję i odrzuć żądanie' points to a button above the table. A third callout box labeled 'Odrzuć' points to a button in the top right of the table.

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*

19.17 Przetwarzanie sesji - uczenie maszynowe

Fudo Enterprise 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 Enterprise śledzi także parametry ilościowe sesji i informuje administratora o nadmiernie dużej liczbie połączeń lub podejrzenie długo trwającej sesji.

19.17.1 Model zawartości

Model zawartości analizuje sesje RDP oraz SSH w celu zbudowania indywidualnych profili behawioralnych użytkowników. Na podstawie zebranych danych, Fudo Enterprise 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.

19.17.2 Ocena sesji

Fudo Enterprise analizuje sesję 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 udostępnił dane logowania innym, powstały na tej podstawie model może nie być w stanie stwierdzić różnicy w zachowaniach użytkowników.

Informacja (popup) o poziomie zagrożenia sesji zawiera wartość indywidualną Prawdopodobieństwa Zagrożenia dla każdego modelu, oceniającego sesję. **Prawdopodobieństwo zagrożenia** jest wartością procentową, wskazującą poziom zagrożenia sesji. Poziom prawdopodobieństwa zagrożenia jest kolorowany na podstawie logiki, opisanej poniżej:

Ikona o kolorze zielonym wskazuje wartość Prawdopodobieństwa Zagrożenia poniżej 50%.

Ikona nabywa koloru pomarańczowym kiedy Prawdopodobieństwo Zagrożenia jest powyżej 50%, z tym że zasadnicze statystyki modelu wskazują, że może to powodować powstanie też wartości False Positive Rate (*FPR*) powyżej 5%. W tym wypadku w wyniku trenowania modelu powstaje wyższy, indywidualny dla każdej pary Użytkownik-model ML próg procentowy dla uzyskania najbardziej optymalnego rezultatu.

Ikona jest o kolorze czerwonym kiedy Prawdopodobieństwo Zagrożenia jest powyżej 50%, a wartość False Positive Rate poniżej 5%. Jeśli wymagania False Positive Rate nie zostają osiągnięte, jest wybierany wyższy próg, zgodnie z definicją False Positive Rate (*FPR*).

Wykres *Prawdopodobieństwa Zagrożenia Sesji* pokazuje wyniki prawdopodobieństwa zagrożenia dla konkretnych odcinków sesji (nazywane segmentami), obliczone na podstawie trenowania modeli AI. Segment - to zbiór akcji/działania użytkownika, na podstawie których model może wykonać pojedynczą predykcję.

Informacja: Sesja powinna być wystarczająco długa, by algorytmy predykcji zostały uruchomione. Minimalna długość sesji, wymagana by analiza została wykonana - to 3 segmenty (około

1 minuty).

Dodatkowo, wykres *Prawdopodobieństwa Zagrożenia Sesji* zawiera przekierowanie do konkretnego segmentu sesji w playerze, co pozwala na szybką reakcję po stronie administratora. Administrator może przeanalizować wyniki, dostarczone przez wytrenowane modele AI oraz poprawić ustawienia dla przyszłych sesji. Na przykład, poprzez dodanie *Polityki*, wysyłającej powiadomienie, kiedy podany próg prawdopodobieństwa zagrożenia zostanie przekroczony.

Informacja: Proces aktualizacyjny do wersji Fudo Enterprise 5.3 usuwa wyniki obliczania poziomu zagrożenia sesji, wyrachowane przed aktualizacją systemu i wprowadza nowy algorytm. Dla „starych” sesji informacja szczegółowa nie jest dostępna.

19.17.3 Modele ilościowe

Fudo Enterprise monitoruje liczbę połączeń oraz ich czas trwania i może zaalarmować administratora jeśli stwierdzi nadzwyczaj dużą liczbę połączeń jednoczesnych lub podejrzenie 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*
- *Polityki*

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.

ID	Utworzony	Tytuł	Stworzony przez
2810246167479189633	2021-11-21 00:00:24	Daily (2021-11-20) - System report	system
2810246167479189632	2021-11-20 00:00:13	Daily (2021-11-19) - System report	system
2810246167479189631	2021-11-19 00:00:14	Daily (2021-11-18) - System report	system
2810246167479189630	2021-11-18 00:00:28	Daily (2021-11-17) - System report	system
2810246167479189629	2021-11-17 00:00:31	Daily (2021-11-16) - System report	system
2810246167479189628	2021-11-16 00:00:31	Daily (2021-11-15) - System report	system
2810246167479189627	2021-11-15 03:13:20	Report generated by admin	admin
2810246167479189626	2021-11-15 03:08:37	Report generated by admin	admin
2810246167479189625	2021-11-15 03:08:24	Report generated by admin	admin
2810246167479189624	2021-11-15 00:00:03	Weekly (2021-11-14) - System report	system
2810246167479189623	2021-11-15 00:00:03	Daily (2021-11-14) - System report	system
2810246167479189622	2021-11-14 00:00:07	Daily (2021-11-13) - System report	system

Raporty predefiniowane

Raport do kont	dostępu	Raport zawiera konta, wraz ze skojarzonymi serwerami docelowymi oraz sejfami, do których dostęp miał miejsce w określonym przedziale czasu.
Raport do sejfów	dostępu	Raport zawiera sejfy, wraz ze skojarzonymi serwerami, do których dostęp miał miejsce w określonym przedziale czasu.
Raport do serwerów	dostępu	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 użytkownika	dostępu	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 dostępu użytkownika	praw	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.

20.1 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*.

ID	Utworzony	Tytuł	Stworzony przez
<input type="checkbox"/> 2810246167479189633	2021-11-21 00:00:24	Daily (2021-11-20) - System report	system
<input type="checkbox"/> 2810246167479189632	2021-11-20 00:00:13	Daily (2021-11-19) - System report	system
<input type="checkbox"/> 2810246167479189631	2021-11-19 00:00:14	Daily (2021-11-18) - System report	system
<input type="checkbox"/> 2810246167479189630	2021-11-18 00:00:28	Daily (2021-11-17) - System report	system

20.2 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*.

20.3 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*.

Użytkownik	Protokół	Adres doc.	Konto	Sejf	Rozpoczęta	Zakończona	Czas trwania	Aktywność	Limit czasu	Rozmiar
<input type="checkbox"/> tpc	Pobranie hasła	10.0.1	SSH	SSH	2021-11-12 12:24	2021-11-12 12:30	0:05:15	0%	-	15.0 KB
<input checked="" type="checkbox"/> tpc	Pobranie hasła	10.0.1	SSH	SSH	2021-11-10 02:44	2021-11-10 11:42	8:58:15	0%	-	3.0 KB
<input type="checkbox"/> tpc	Pobranie hasła	10.0.1	SSH	SSH	2021-10-24 23:46	2021-10-24 23:52	0:06:00	0%	-	15.0 KB
<input type="checkbox"/> tpc	Pobranie hasła	10.0.1	SSH	SSH	2021-10-11 01:24	2021-10-12 06:09	1 day, 4:45:18	0%	-	3.0 KB
<input type="checkbox"/> tpc	Pobranie hasła	10.0.1	SSH	SSH	2021-10-11 01:16	2021-10-11 01:20	0:04:05	0%	-	3.0 KB
<input type="checkbox"/> tpc	Pobranie hasła	10.0.1	SSH	SSH	2021-10-11 01:15	2021-10-11 01:15	0:00:53	0%	-	15.0 KB

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.

20.4 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.

20.5 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*

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

21.1 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 Enterprise 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*.

Zestawienie

Sortuj po wybranym kryterium

Organizacja/Użytkownik	Sumaryczny czas trwania sesji	Czas aktywności	Czas nieaktywności	Produktywność	Sesje	Serwery
Wszyscy	45:45	1:19	44:26	2%		14
5_1_test			-1:58	100%	2	1
user14	0:01	0:03	-1:58	100%	2	1
Fudo Security	1:53	0:05	1:48	4%	29	2
of	0:00	0:00	0:00	0%	15	1
of	1:52	0:02	1:50	1%	10	1
si	0:00	0:03	-1:57	100%	4	1
Nieprzydzielony	10:24	0:53	9:31	8%	226	13

Tematy pokrewne:

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

21.2 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*

21.3 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*

Poniższy rozdział zawiera opisy czynności administracyjnych.

22.1 System

22.1.1 Data i czas

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

Ostrzeżenie:

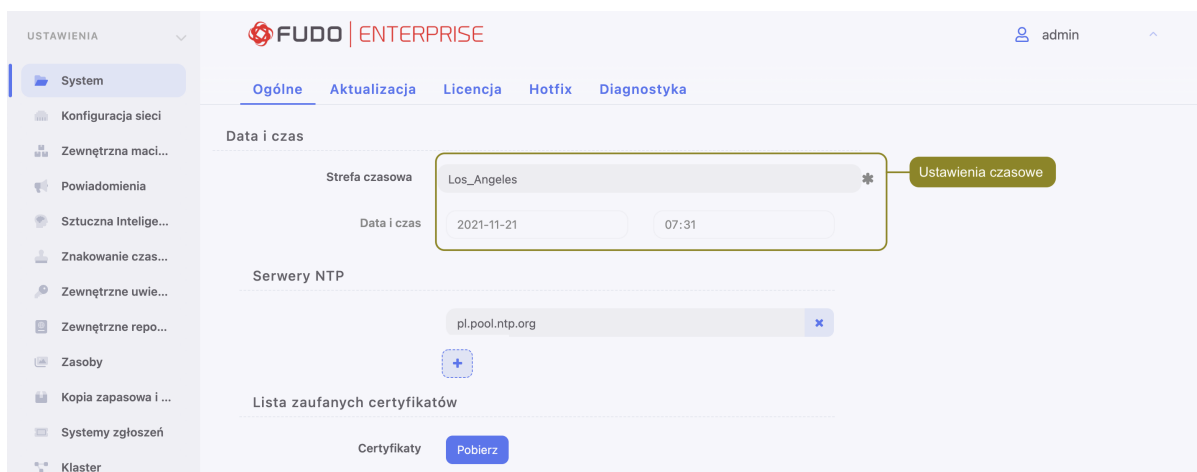
- Zaleca się, aby data i czas pobierane były z serwera NTP, będącego pewnym źródłem danych referencyjnych. Ręczna zmiana ustawień daty i czasu może spowodować nieprawidłowości w funkcjonowaniu urządzenia.
- Pobieranie czasu z serwera NTP jest wymagane w przypadku *konfiguracji klastrowych*.

Zmiana daty i czasu

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

Aby zmienić datę i czas serwera Fudo Enterprise, 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*.

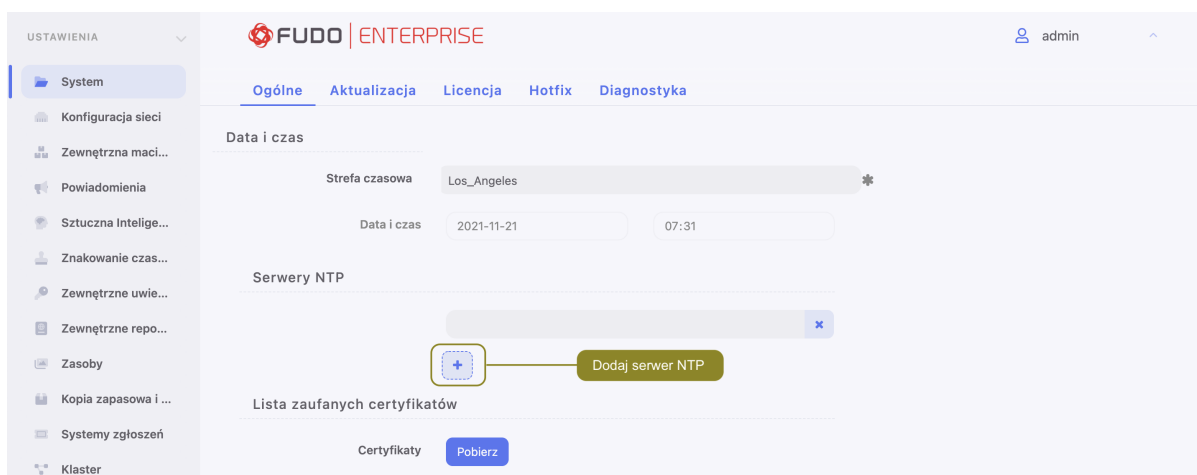
Konfiguracja serwerów czasu

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 użytkownika 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 użytkownika 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*

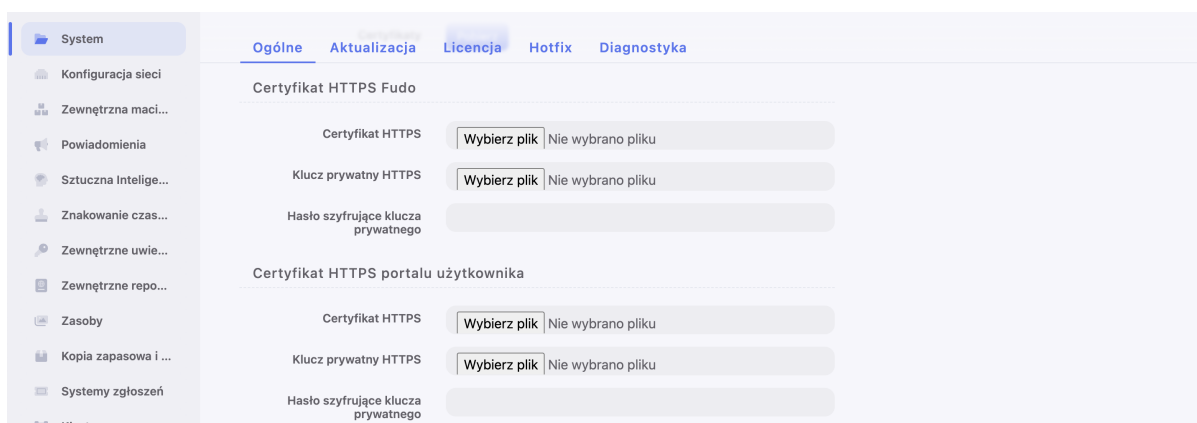
22.1.2 Certyfikaty HTTPS

Certyfikat HTTPS pozwala administratorowi upewnić się, że nawiązał połączenie z panelem administracyjnym Fudo Enterprise 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 *Przełączaj* w polu *Klucz prywatny HTTPS* i wskaż w systemie plików definicję klucza prywatnego SSL.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Bezpieczeństwo*
- *Zarządzanie serwerami*

22.1.3 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*.

The screenshot shows the 'Ustawienia' (Settings) menu on the left, with 'System' selected. The main content area is titled 'Uwierzytelnianie użytkowników i sesje' (User authentication and sessions). It contains several configuration options:

- Domyślna domena: [text input field]
- Blokowanie nowych połączeń: (highlighted with a green circle and a callout box: 'Włącz opcję blokowania nowych połączeń')
- Niepowodzenia uwierzytelnienia:
- Minimalna długość hasła: 8
- Małe litery: 1
- Wielkie litery: 1
- Znaki specjalne: 1
- Cyfry: 1

3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

22.1.4 Dostęp SSH

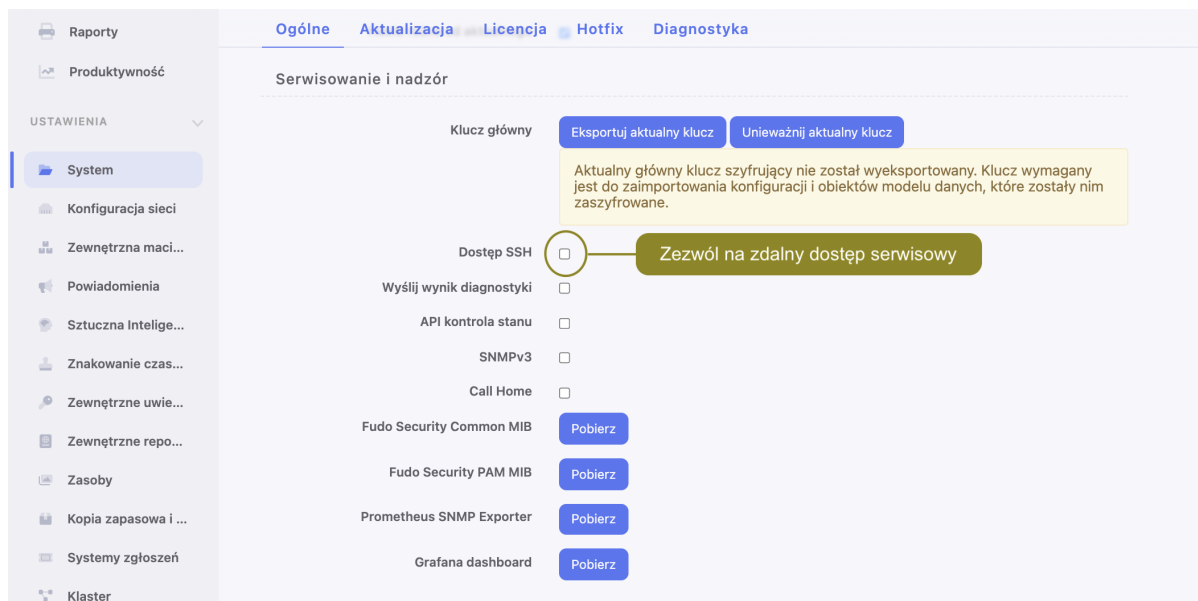
Opcja umożliwia zdalny dostęp serwisowy do Fudo Enterprise za pośrednictwem protokołu SSH.

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*

22.1.5 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: Kopia zapasowa systemu*.
5. Powiadom innego użytkownika **superadmin** o zainicjowaniu funkcjonalności, która wymaga potwierdzenia.

Tematy pokrewne:

- *Odtwarzanie sesji*

22.1.6 Aktualizacja systemu

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 węzle podrzędnym.

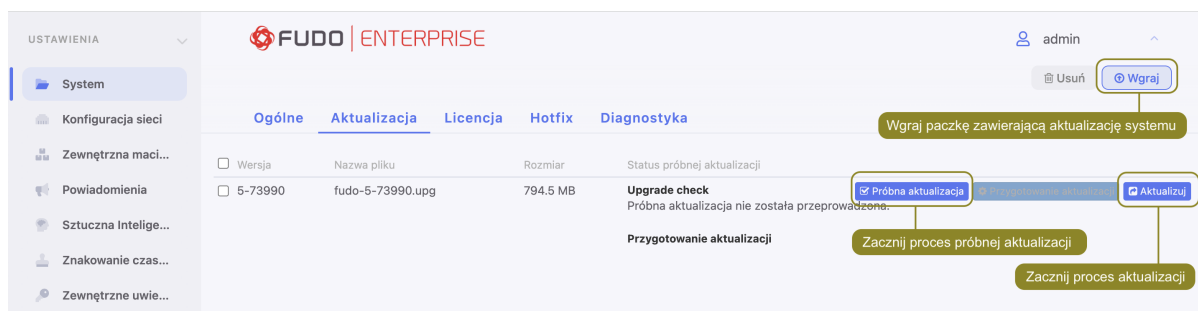
22.1.6.1 Aktualizowanie systemu

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 Enterprise 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 Enterprise 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*.

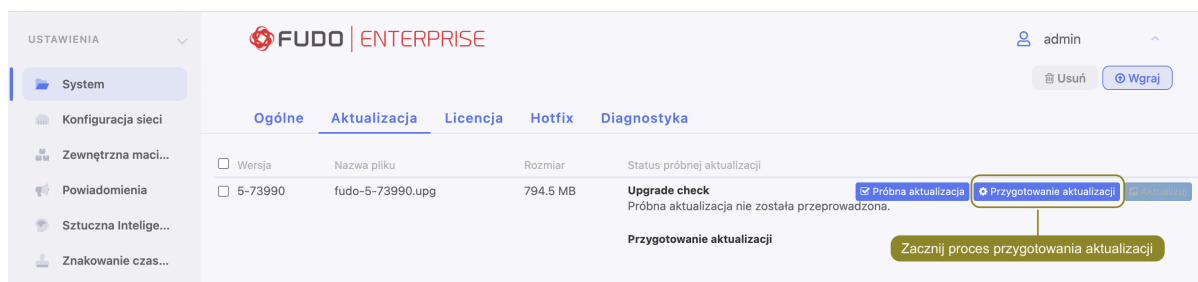
1. Wybierz z lewego menu *Ustawienia > System*.
2. Wybierz zakładkę *Aktualizacja*.
3. Kliknij *Wgraj*.
4. Wskaż plik zawierający aktualizację systemu (.upg).
5. Opcjonalnie, kliknij *Próbna aktualizacja* przy wybranym pliku obrazu, aby stwierdzić, czy obiekty modelu danych i bieżąca konfiguracja są kompatybilne z nową wersją systemu.



Informacja:

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

6. Jeśli aktualizacja wymaga przygotowania, kliknij *Przygotowanie aktualizacji*.



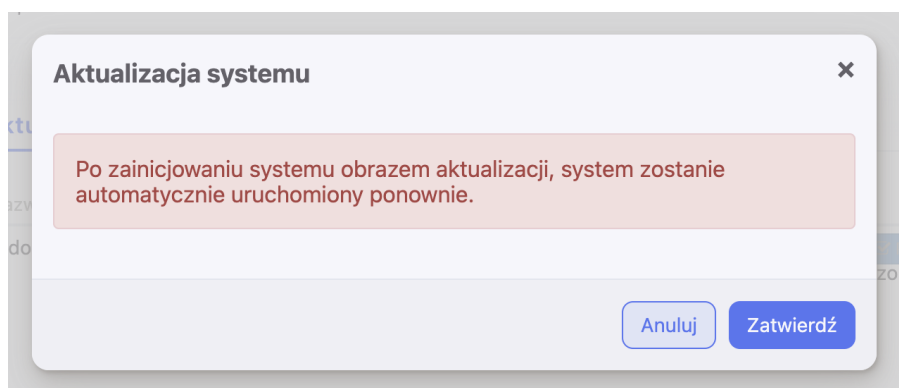
Informacja:

- 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.

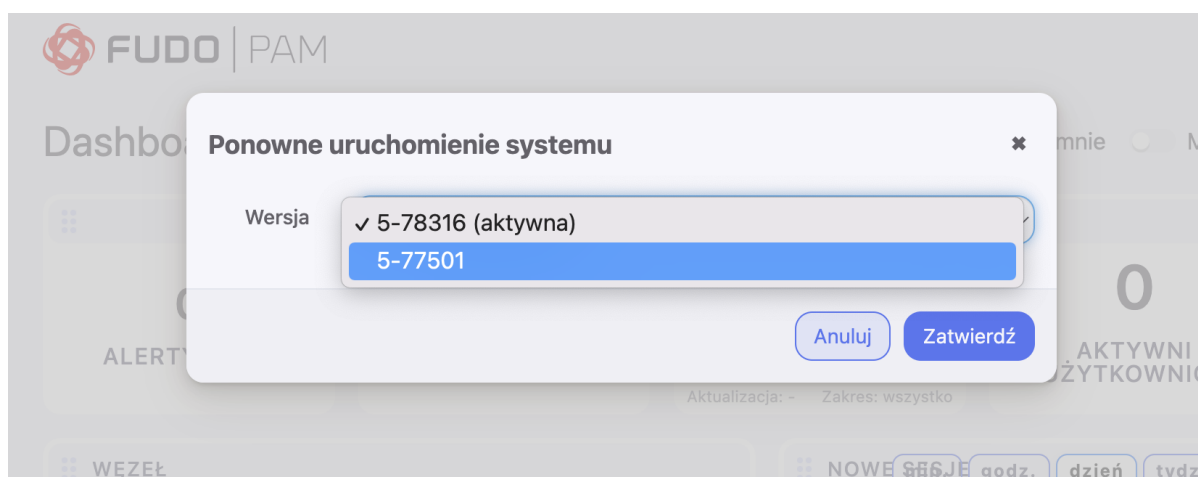
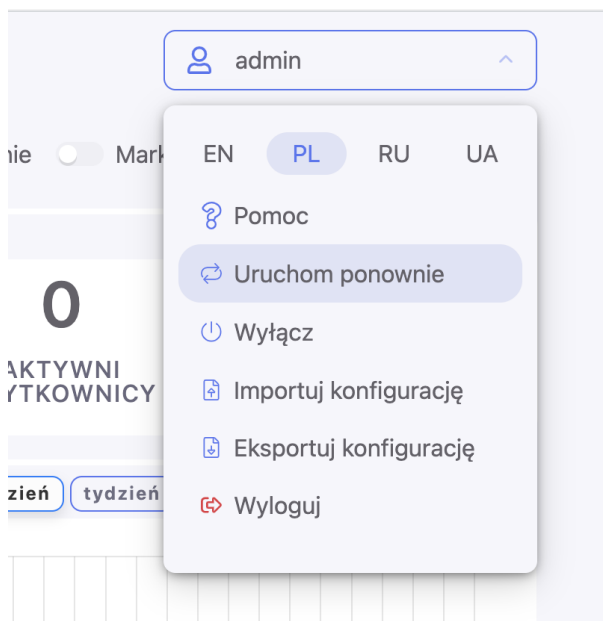
8. Kliknij *Zatwierdź*, aby wykonać aktualizację.



Informacja: Jeśli przed aktualizacją została włączona opcja systemowa *Blokowanie nowych połączeń*, pamiętaj żeby wyłączyć ją po ponownym uruchomieniu systemu.

22.1.6.2 Przywrócenie poprzedniej wersji systemu

Fudo Enterprise oprócz bieżącej wersji systemu, przechowuje jego poprzednią wersję, pozwalając na jej przywrócenie. W przypadku gdy uruchomienie systemu w nowej wersji nie powiedzie się, Fudo Enterprise wykryje problem i uruchomi system w poprzedniej wersji. Fudo Enterprise 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 jakiegokolwiek 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](#).

22.1.6.3 Usuwanie migawki aktualizacji

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

Ostrzeżenie: Usunięcie migawki aktualizacji uniemożliwi przywrócenie poprzedniej wersji systemu.

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

Tematy pokrewne:

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

22.1.7 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.

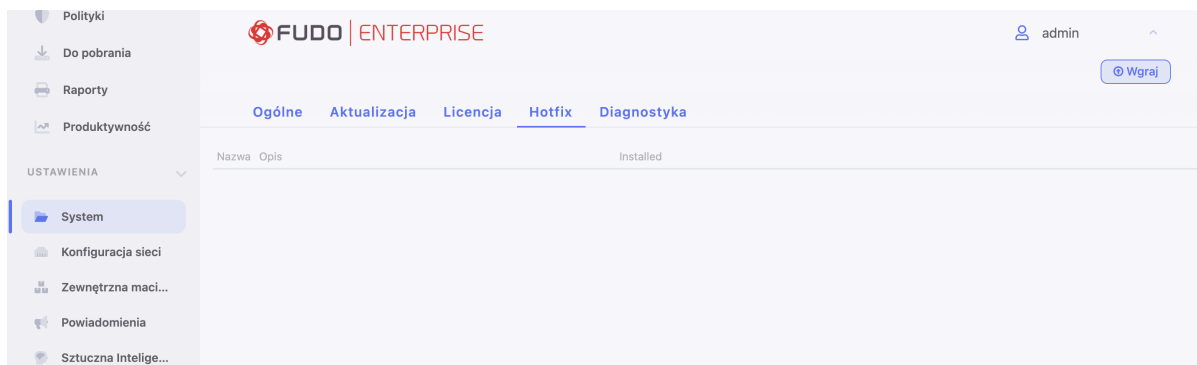
Tematy pokrewne:

- *Opis systemu*
- *Wymagania*

22.1.8 Hotfix

Funkcjonalność Hotfix pozwala administratorowi naprawić błędy systemowe poprzez wgranie paczki naprawczej w Panelu Administracyjnym. Paczka jest dostarczana przez Dział Wsparcia Technicznego Fudo Enterprise 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:

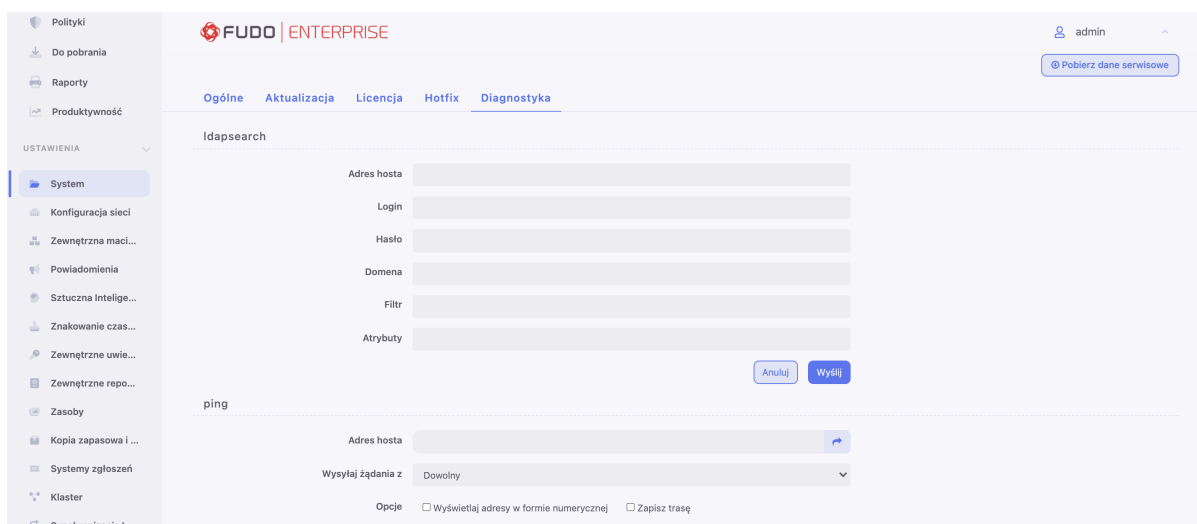
- [Aktualizacja systemu](#)
- [System](#)

22.1.9 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 żadaną komendę, wprowadź parametry wykonania i kliknij przycisk wykonania komendy.



The screenshot displays the 'Diagnostyka' (Diagnostics) section of the Fudo Enterprise 5.4 interface. The left sidebar contains navigation options: 'Do pobrania', 'Raporty', 'Produktywność', and 'USTAWIENIA' (Settings) with a dropdown arrow. Under 'USTAWIENIA', the 'System' menu is selected, showing sub-items like 'Konfiguracja sieci', 'Zewnętrzna maci...', 'Powiadomienia', 'Sztuczna Intelige...', 'Znakowanie czas...', 'Zewnętrzne uwie...', 'Zewnętrzne repo...', 'Zasoby', 'Kopia zapasowa i ...', 'Systemy zgłoszeń', and 'Klaster'. The main content area has a top navigation bar with 'Ogólne', 'Aktualizacja', 'Licencja', 'Hotfix', and 'Diagnostyka' (active). A 'Pobierz dane serwisowe' button is in the top right. The diagnostic tools are organized into three sections: 'netcat', 'host', and 'traceroute'. Each section has an 'Adres hosta' field with a refresh icon. The 'netcat' section includes a 'Port' field, a 'Wysyłaj żądania z' dropdown set to 'Dowolny', and 'Flags' with radio buttons for 'Wylącznie IPv4' and 'Wylącznie IPv6'. The 'host' section is currently empty. The 'traceroute' section includes a 'Wysyłaj żądania z' dropdown set to 'Dowolny' and 'Opcje' (Options) with checkboxes for 'Nie rozwiązuj nazw skoków', 'Tryb omijania firewall-a', 'Użyj protokołu ICMP zamiast UDP', and 'Ustaw flagę "Nie fragmentuj"'. A 'Zapisz zmiany' button is visible in the top right of the main content area.

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 mnemonicicznej.
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 Enterprise i hostem docelowym.
Nie rozwiązuje nazw skoków	Adresy kolejnych punktów przeskoku nie będą rozwiązywane do nazw mnemonicicznych.
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*

22.1.10 Szyfrowanie konfiguracji

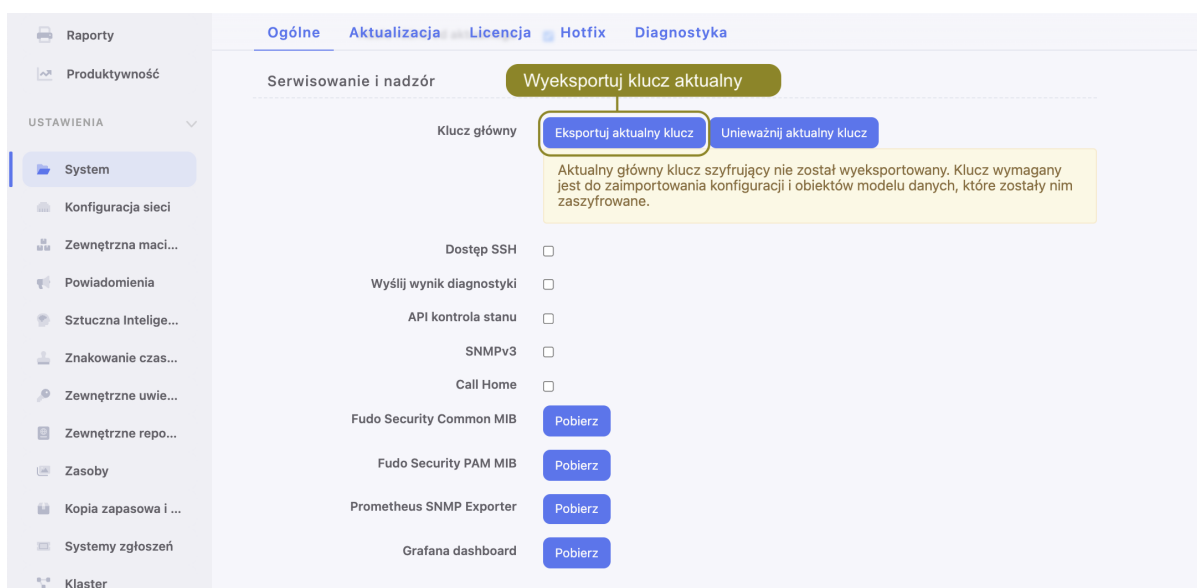
Główny klucz szyfrujący zapewnia bezpieczeństwo i poufność danych konfiguracyjnych, kopii zapasowych systemu i zewnętrznych wolumenów przechowywania danych. Klucz umożliwia również odzyskanie klucza szyfrującego wewnętrznego wolumenu danych w przypadku zaginięcia lub uszkodzenia kluczy zapisanych na 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 skutkuje 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 skutkuje 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*.

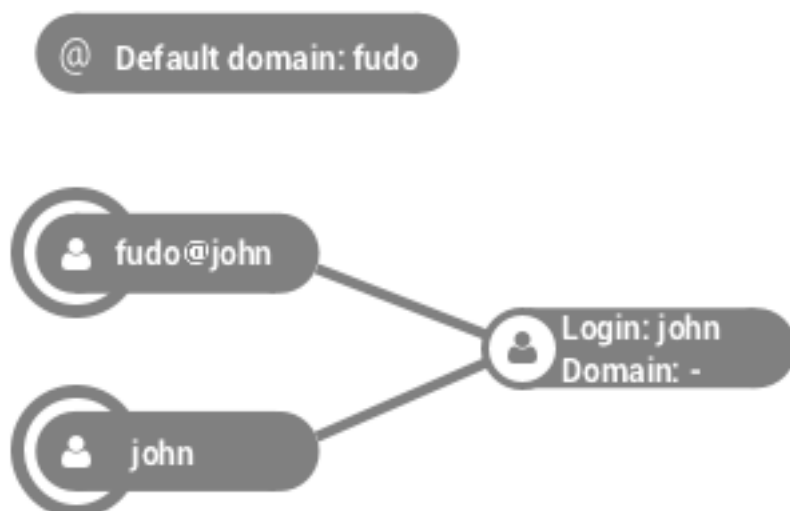
Tematy pokrewne:

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

22.1.11 Domyślna domena

Informacja: Pamiętaj, że działanie opcji *Domena domyślna* jest ściśle powiązane z ustawieniami *Domeny Fudo* w *specyfikacji użytkownika*.

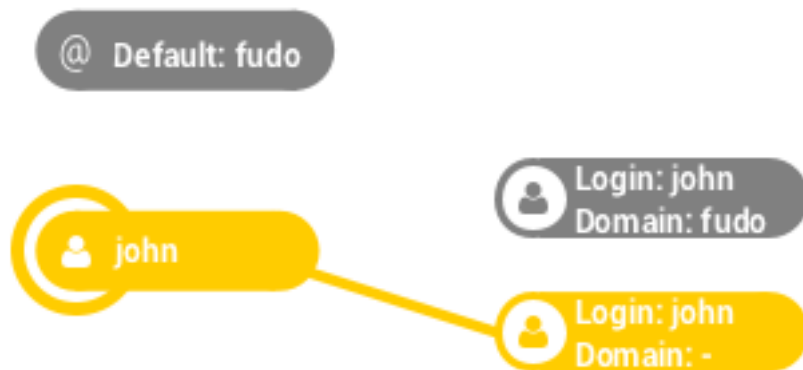
- W przypadku gdy została zdefiniowana *Domena domyślna*, a użytkownik nie ma przypisanej *Domeny Fudo*, może uwierzytelniać się podając domenę domyślną (przykład: john@domain) lub jej nie wskazywać (przykład: john).



- W sytuacji, w której istnieją dwaj użytkownicy o tym samym loginie, z których jeden ma zdefiniowaną *Domene Fudo* taką samą jak *Domena domyślna*, a drugi nie ma określonej *Domeny Fudo*:
 - W przypadku, kiedy użytkownik poda domenę przy logowaniu, nastąpi dopasowanie użytkownika ze zdefiniowaną domeną,



- W przypadku, kiedy użytkownik nie poda domeny przy logowaniu, nastąpi dopasowanie użytkownika, który nie miał określonej domeny.



- Jeśli użytkownik, który ma zdefiniowaną *Domenę Fudo* taką samą jak *Domena domyślna*, spróbuje się zalogować swoją metodą uwierzytelnienia bez podania domeny, Fudo Enterprise zgłosi błąd logowania.

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*

22.1.12 Złożoność haseł

Fudo Enterprise 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 określ minimalną liczbę małych liter.
5. Zaznacz *Wielkie litery* i określ minimalną liczbę wielkich liter.
6. Zaznacz *Znaki specjalne* i określ minimalną liczbę znaków specjalnych.
7. Zaznacz *Cyfry* i określ 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, przejdź do *Zarządzanie > Użytkownicy*, edytuj wybranego użytkownika i zaznacz opcję *Zastosuj złożoność hasła statycznego* w sekcji *Uwierzytelnienie*.

Tematy pokrewne:

- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

22.1.13 Single Sign On

Opcja Single Sign On umożliwia automatyczne zalogowanie do systemu. Fudo Enterprise pozwala uruchomić usługę Single Sign On dla Panelu Administracyjnego oraz Portalu Użytkownika.

22.1.13.1 Konfiguracja Fudo Enterprise

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.

22.1.13.2 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:

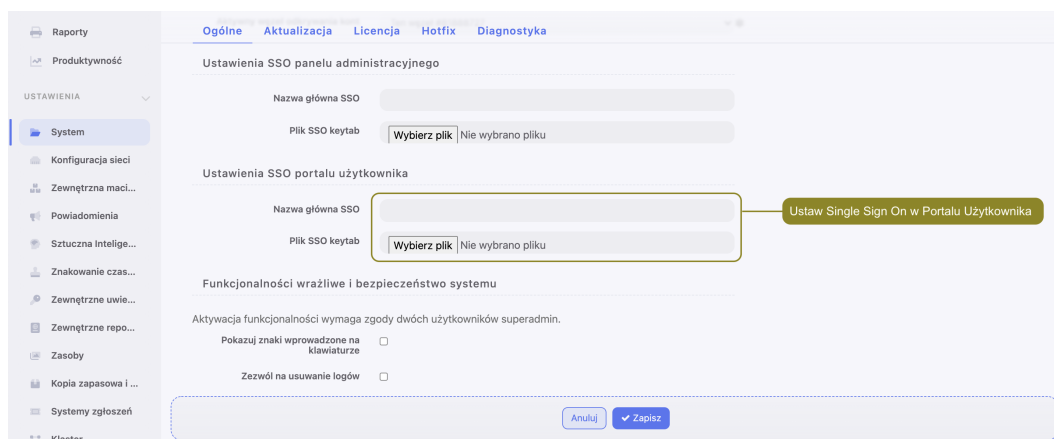
- Wybierz z lewego menu *Ustawienia > System*.
- W sekcji *Ustawienia SSO panelu administracyjnego*, w polu *Nazwa główna SSO*, wprowadź identyfikator: `HTTP/hostname.yourdomain.local@yourdomain.local`.
- Wgraj plik `hostname.yourdomain.local.keytab` z identyfikatorem konta użytkownika w Active Directory oraz kluczami do szyfrowania i deszyfrowania żądań Kerberos.

- Kliknij *Zapisz*.

22.1.13.3 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*.

22.1.13.4 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 Enterprise wykonując komendę w konsoli CMD lub PowerShell:

```
ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.local -mapuser
sso\nazwa_uzytkownika -pass haslo_uzytkownika. -ptype KRB5_NT_PRINCIPAL -out
hostname.yourdomain.local.keytab
```

22.1.13.5 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.

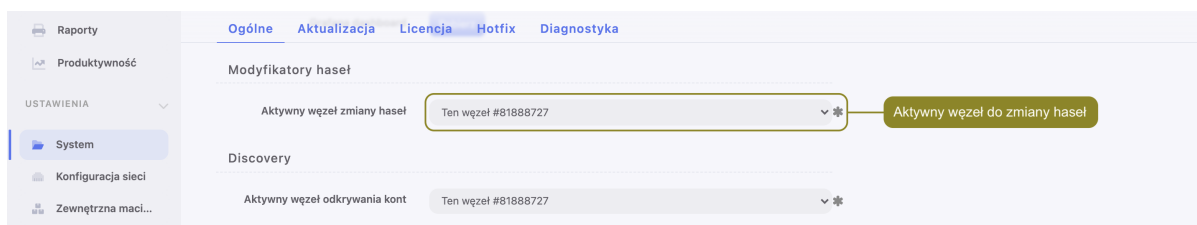
Tematy pokrewne:

- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

22.1.14 Modyfikatory haseł - aktywny węzeł klastra

Opcja wyboru aktywnego węzła klastra wskazuje instancję Fudo Enterprise, 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*.

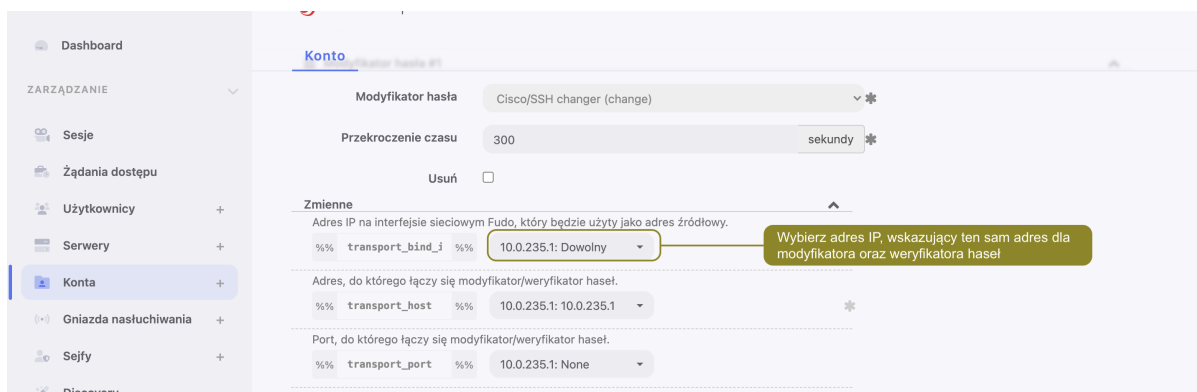
Informacja: W sytuacji, w której wskazany węzeł ulegnie awarii, zadanie zmiany haseł nie zostanie automatycznie podjęte przez inną instancję Fudo Enterprise. Automatyczna zmiana haseł wymaga zmiany przypisania aktywnego węzła lub przywrócenie działania uszkodzonej jednostki.

22.1.14.1 Manager haseł w klastrze

Fudo Enterprise 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.



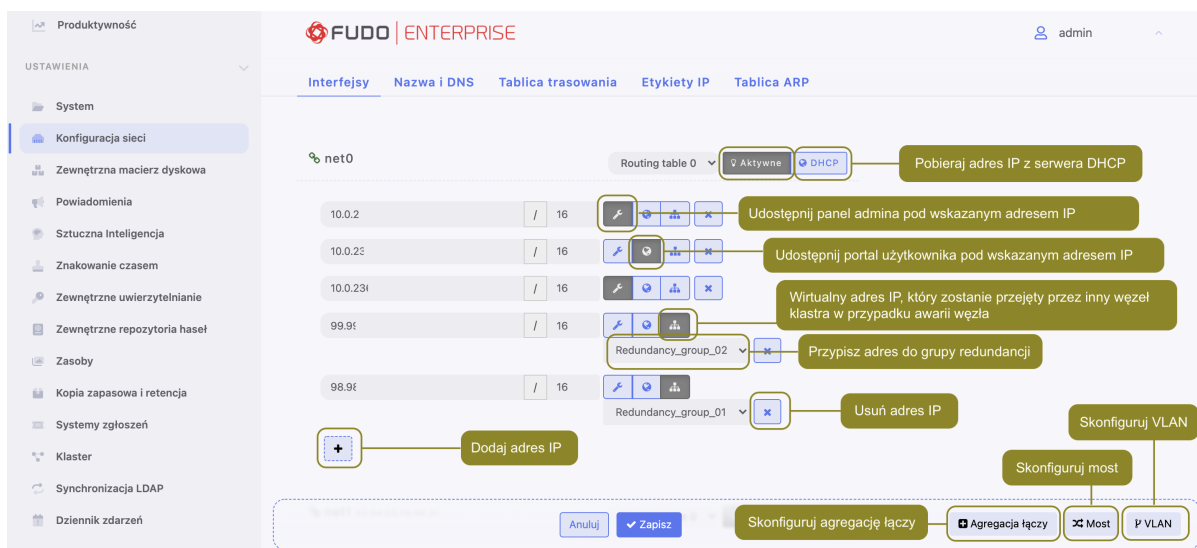
Jeśli wartości zmiennej `transport_bind_ip` będą wskazywać różne węzły klastra, Modyfikator / Weryfikator hasła będą działać na węzle, wskazanym jako *aktywny węzeł klastra dla Modyfikatorów hasel*.

Tematy pokrewne:

- *Modyfikatory hasel*
- *Uniwersalne modyfikatory hasel*

22.2 Konfiguracja sieci

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



22.2.1 Konfiguracja ustawień sieciowych

W specyfikacji domyślnej, Fudo Enterprise 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.

22.2.1.1 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 Enterprise 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 .

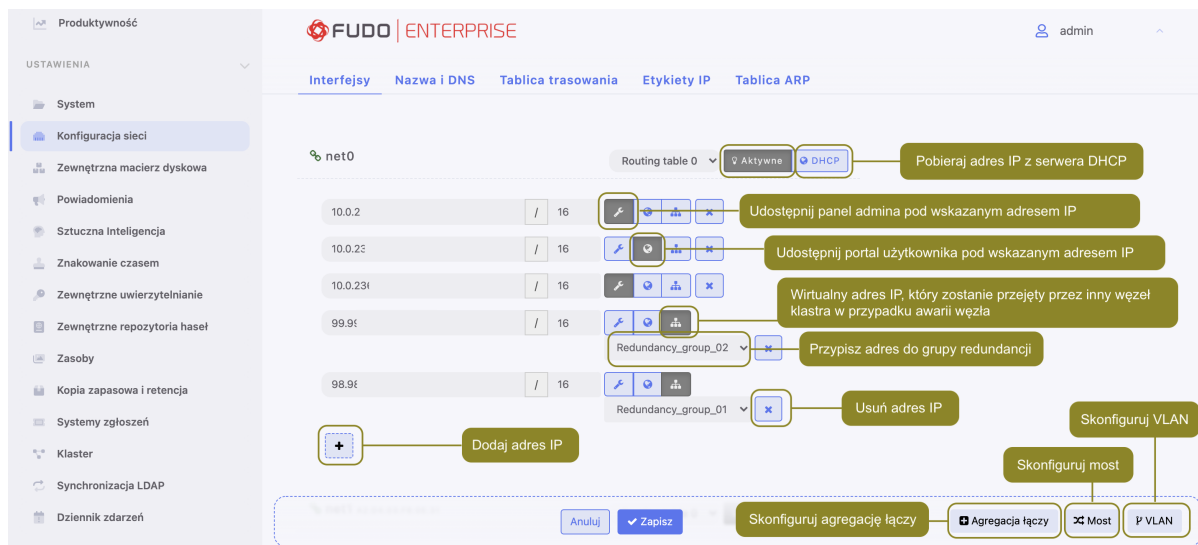


Udostępnij *Portal użytkownika* pod wskazanym adresem IP.

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.

22.2.1.2 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 Enterprise. Skontaktuj się ze sprzedawcą lub wsparciem technicznym, aby dowiedzieć się więcej.

```
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: █
```

3. Wprowadź hasło do konta administratora.

```
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:
```

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 potwierdzić 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 Enterprise) 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):

```

22.2.1.3 Konfigurowanie mostu sieciowego

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

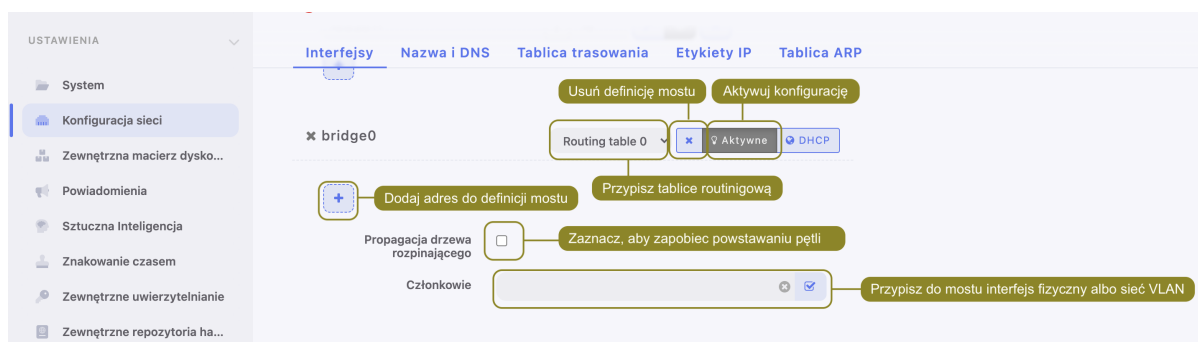


Aby stworzyć most sieciowy, postępuj zgodnie z poniższą instrukcją.

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



22.2.1.4 Konfigurowanie sieci wirtualnych (VLAN)

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

Aby skonfigurować Fudo Enterprise 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*.



22.2.1.5 Konfigurowanie agregacji połączeń LACP

Fudo Enterprise 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 Enterprise 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*

22.2.2 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.

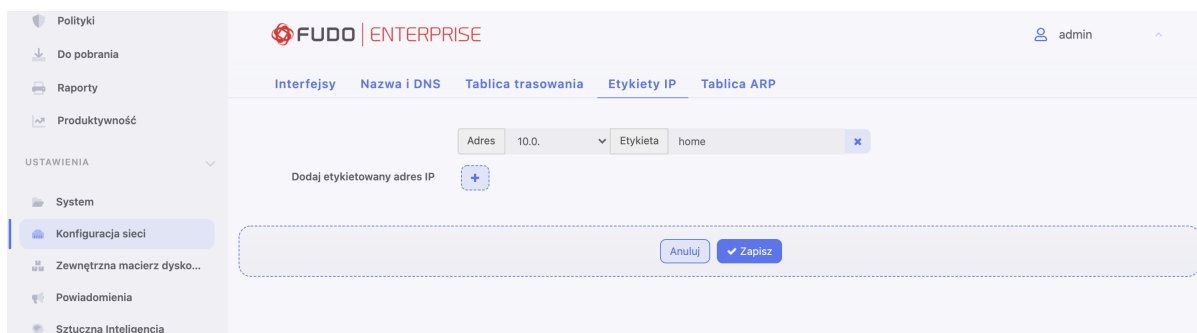
Definiowanie etykietowanego adresu IP

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*

- *Uwierzytelnienie*
- *Serwery*
- *Gniazda nastuchiwania*

22.2.3 Konfiguracja tras routingu

W konfiguracji domyślnej, Fudo Enterprise 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.

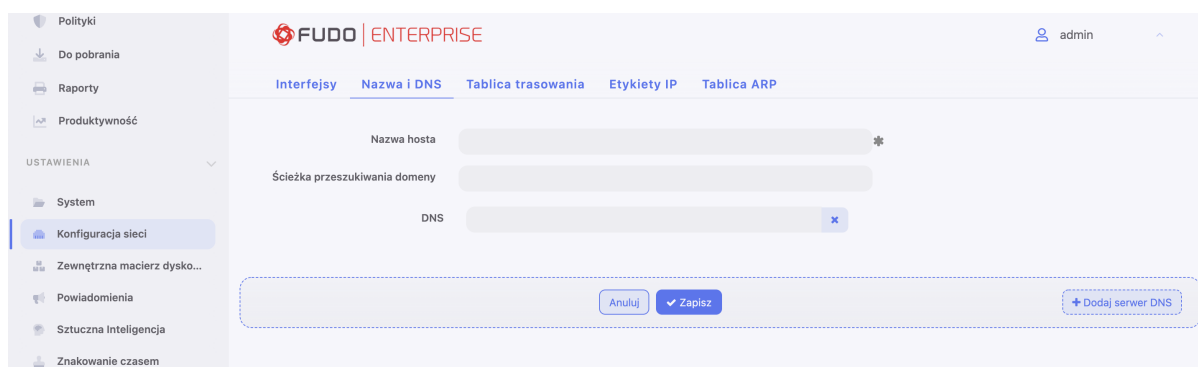
1. Wybierz z lewego menu *Ustawienia > Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Zaznacz opcję usunięcia wybranej trasy routingu i kliknij *Zapisz*.

Tematy pokrewne:

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

22.2.4 Konfiguracja DNS

Informacja: Serwer DNS pozwala na używanie mnemoniczych 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*

22.2.5 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*

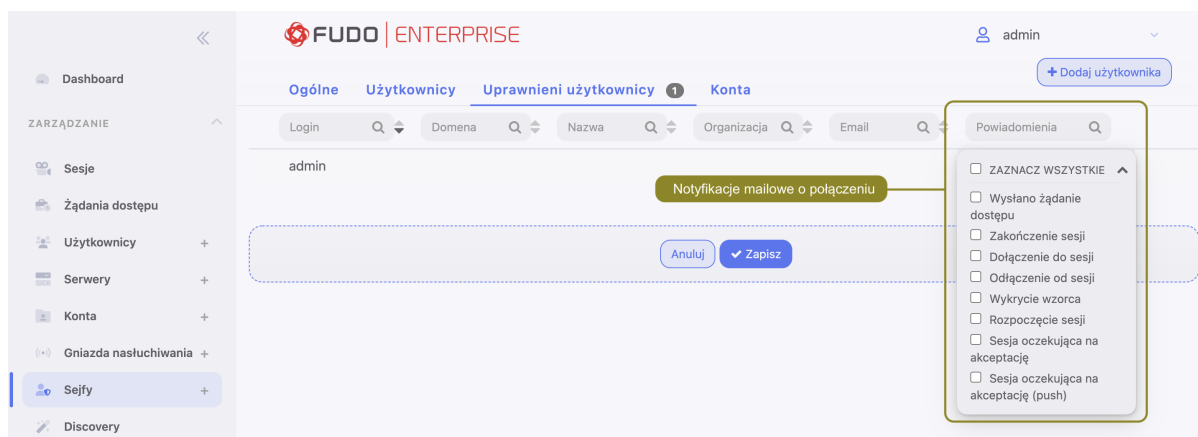
22.3 Powiadomienia

Fudo Enterprise 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 Enterprise 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 <code>smtp.gmail.com</code> .
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 <i>Użyj STARTTLS</i> , jeśli serwer pocztowy ma zapewnić bezpieczne połączenie.

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

- Kliknij  w celu wgrania certyfikatu urzędu certyfikacji. Wybierz format wyświetlenia wartości SHA1 albo MD5.
- 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.

Temat	Odbiorca	Data
Session end: [ssh] admin -> Se Single		Fri, 06 May 2022 14:41:57 +0200 (CEST)
Session start: [ssh] admin -> Sr Single		Fri, 06 May 2022 14:26:30 +0200 (CEST)
Access Request rejected for > [5.2		Thu, 05 May 2022 10:56:09 +0200 (CEST)
Access Request accepted for [LD		Wed, 20 Apr 2022 17:03:58 +0200 (CEST)
Access Request accepted for [LD		Wed, 20 Apr 2022 17:02:06 +0200 (CEST)
Access Request accepted for		Wed, 20 Apr 2022 16:57:57 +0200 (CEST)

Tematy pokrewne:

- [Konta](#)

22.4 Sztuczna inteligencja

Fudo Enterprise 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. Fudo Enterprise oznacza sesje jako podejrzane i wysyła wiadomości oraz/lub notyfikacje SNMP TRAP, aby administrator był świadomy zaistniałej sytuacji. Fudo Enterprise też automatycznie może wstrzymać podejrzaną sesję, bądź całkowicie ją przerwać i zablokować użytkownika.

Moduł AI Fudo Enterprise jest wieloskładnikowym systemem, wymagającym konfiguracji przed początkiem pracy, aby działać najbardziej wydajnie i dostarczać najlepsze statystyki. Aby skonfigurować swój moduł AI wykonaj 3 kroki:

1. Skonfiguruj trenera modeli, zgodnie z opisem poniżej.
2. Włącz *modele behawioralne*, aby uruchomić analizę behawioralną w oparciu o wybrane protokoły (SSH oraz/lub RDP) oraz zebranie indywidualnych statystyk per model.
3. Ustaw *Polityki* dla przyszłych sesji, aby moduł AI mógł wykrywać niepożądane zachowania użytkowników podczas sesji i reagować automatycznie, m.in wysyłać wiadomości mailowe, notyfikacje SNMP TRAP, wstrzymywać lub przerywać sesję, blokować użytkownika.

Po wykonaniu wspomnianych trzech czynności, obserwuj działanie modułu AI poprzez monitorowanie:

- skrzynki odbiorczej, jeśli zostały wybrane opcje wysyłania powiadomień w polityce;
- aktualnej liczby podejrzanych sesji na widżecie Podejrzane sesje na Dashboard'zie. Widżet wyświetla liczbę sesji, które są zakwalifikowane jako sesje z **Wysokim Poziomem Zagrożenia** oraz zawiera też link, prowadzący do odfiltrowanej listy wszystkich takich sesji z określonego przedziału czasowego;
- poziomu zagrożenia oraz *Prawdopodobieństwa zagrożenia* trwającej *sesji* na wykresie, skierowanym do podejrzanego segmentu sesji w playerze.

22.4.1 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 zaobserwowana 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*.

22.4.2 Modele behawioralne

Parametryzacja modeli pozwala na odpowiednie dopasowanie charakterystyk do specyfiki środowiska, w którym funkcjonuje Fudo.

Informacja: Od wersji Fudo Enterprise 5.3 modele AI zostały zmodyfikowane.

Ostrzeżenie:

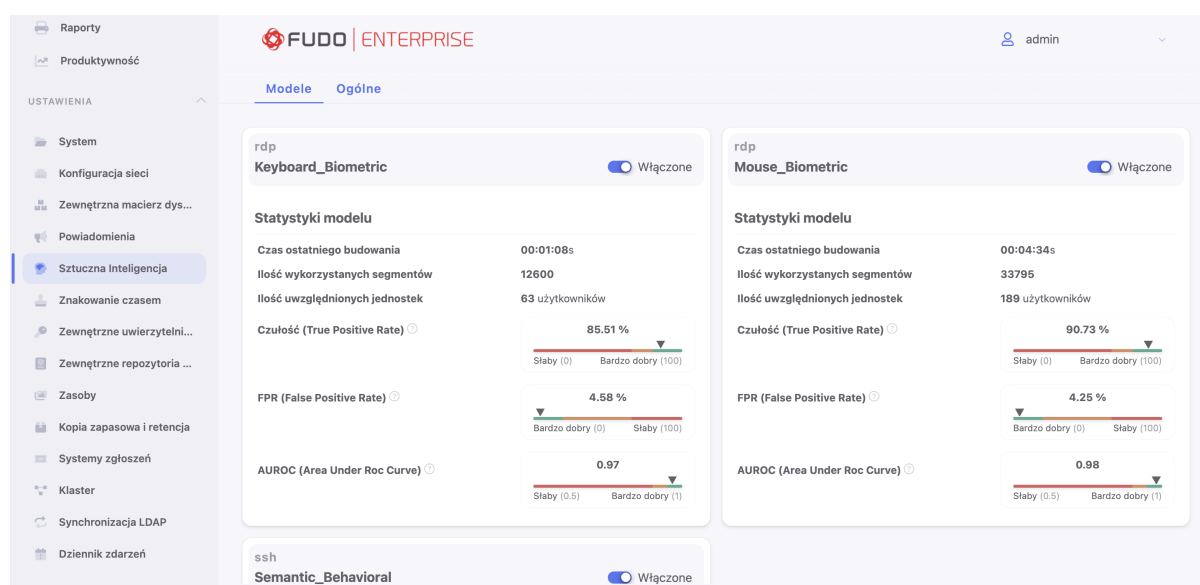
- Skrypt aktualizacyjny do wersji Fudo Enterprise 5.3 lub nowszej wyłącza wszystkie *modele AI* i dodaje nowe. Po zakończeniu procesu aktualizacyjnego, wszystkie modele należy włączyć w zakładce *Ustawienia > Sztuczna Inteligencja* manualnie.
- W przypadku klastrowej konfiguracji systemu, jest wymagana w pierwszej kolejności aktualizacja aktywnych modeli na węźle o roli master.

Ponieważ modele AI są oparte o protokoły (RDP oraz/lub SSH), aktywność użytkownika podczas sesji jest analizowana na podstawie funkcjonalności, które konkretny protokół umożliwia:

Model Mouse Biometric (RDP) - model predykcji, działający w oparciu o ruchy myszką oraz klikanie. Model funkcjonuje na podstawie 700 różnych właściwości, które są powiązane ze sposobem użytkownika na kierowanie urządzeniem wskazującym. Wspomniane właściwości są wykorzystywane podczas trenowania modeli, są indywidualnie kalibrowane, aby uzyskać najlepszą możliwą wartość predykcji oraz zminimalizować wartość *FPR*.

Model Keyboard Biometric (RDP) - model predykcji, działający w oparciu o dynamikę wprowadzania znaków z klawiatury. Model dostarcza wyniki, zebrane na podstawie 100 unikatowych właściwości, możliwych do wykonania przez użytkownika podczas pracy na klawiaturze. Wspomniane właściwości są wykorzystywane podczas trenowania modeli, są indywidualnie kalibrowane, aby uzyskać najlepszą możliwą wartość predykcji oraz zminimalizować wartość *FPR*.

Model Semantic Behavioral (SSH) - model, funkcjonujący na podstawie wprowadzanych z klawiatury komend. Model działa poprzez wykrycie indywidualnych preferencji osób do uzyskania tego samego wyniku na różne sposoby. Na przykład, jedna osoba preferuje skorzystać z `wget`, niż `curl` albo `vim` raczej, niż `emacs`. Jeden użytkownik preferuje komendę `reset`, aby wyczyścić okno terminala, a drugi korzysta ze skrótu klawiaturowego `CTRL+L`. Te wartości nie są statyczne, tylko zdobyte na podstawie trenowania na podstawie danych. Dodatkowo, jest dobierany zestaw z ponad 600 różnych właściwości, którymi użytkownicy są cechowane. Model używa mieszanki preferencji oraz wspomnianych właściwości, indywidualnie kalibruje je, aby uzyskać najlepszą możliwą wartość predykcji oraz zminimalizować wartość *FPR*.



Fudo dostarcza statystyki dla każdego modelu z ostatnio przeprowadzonego trenowania, a mianowicie:

Czas ostatniego budowania - czas trwania ostatnio przeprowadzonego trenowania.

Ilość wykorzystanych segmentów - ilu odcinków sesji wykorzystano do ostatnio przeprowadzonego trenowania.

Ilość uwzględnionych jednostek - ilu użytkowników wykorzystano do ostatnio przeprowadzonego trenowania.

Czułość (ang. True Positive Rate) - to procent wszystkich złośliwych (malicious) sesji rozpoznanych przez model jako podejrzane (im wyższa wartość, tym lepsza).

FPR (ang. False Positive Rate) - to procent wszystkich prawidłowych sesji niepoprawnie rozpoznanych przez model jako podejrzane (im niższy wartość, tym lepszy).

AUROC (ang. Area Under ROC curve) - jest to jednolita metryka podsumowująca jakość modelu (im wyższa wartość, tym lepsza).

Statystyki dla wartości Czułości, FPR oraz AUROC są wizualizowane na kolorowanej skali dla każdego modelu.

Informacja: Statystyki modelu są wyświetlane zaraz po zakończeniu pierwszego trenowania i będą uaktualniane po każdym kolejnym.

Tematy pokrewne:

- *Konta*
- *Sesje*
- *Przetwarzanie sesji - uczenie maszynowe*
- *Polityki*

22.5 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 Enterprise.
- W przypadku usługi świadczonej przez KIR, adres <http://www.ts.kir.com.pl/HttpTspServer> musi być osiągalny przez Fudo Enterprise.
- 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*

22.6 Model uwierzytelniania w oparciu o certyfikaty

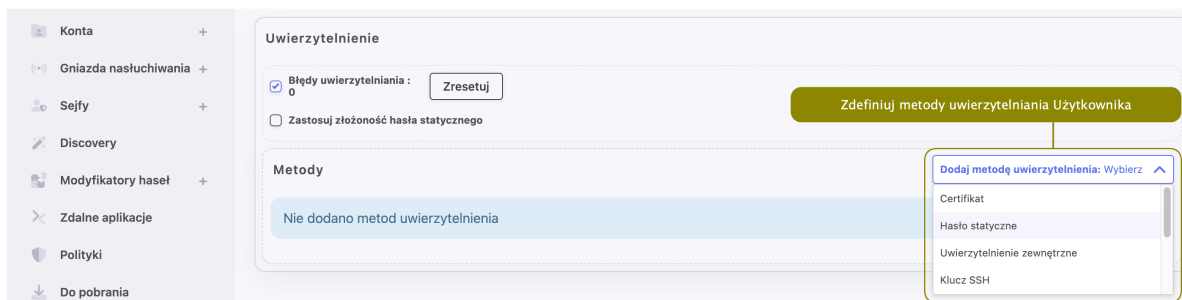
Fudo Enterprise umożliwia logowanie certyfikatem do serwera docelowego. Certyfikat powinien być zgodny ze standardami PIV.

W celu konfiguracji certyfikatu jako metody uwierzytelnienia, postępuj zgodnie z instrukcją:

1. Wybierz *Ustawienia* > *System*
2. W zakładce *Ogólne*, w polu *Certyfikaty CA* sekcji *Certyfikaty CA użytkownika* załaduj plik z certyfikatami w formacie PEM.

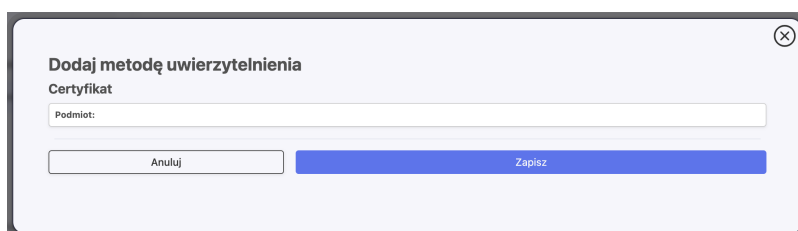
Informacja: Fudo Enterprise obsługuje wielo-domenowość. Dla wielo-domenowej konfiguracji wystarczy wgrać plik PEM z certyfikatami root/intermediate ze wszystkich CA. Dla takiej konfiguracji jest wymagane unikalny *Subject* dla każdego użytkownika.

3. Kliknij *Zapisz*.
4. Wybierz *Zarządzanie > Użytkownicy* i edytuj użytkownika, dla którego chcesz skonfigurować metodę uwierzytelnienia *certyfiakat*, lub utwórz nowego użytkownika przechodząc do menu *Zarządzanie > Użytkownicy* i klikając *+ Dodaj użytkownika*.
5. W sekcji *Uwierzytelnienie* z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz typ *Certyfiakat*.



6. Podaj *Podmiot* i kliknij *Zapisz*.

Informacja: *Podmiot* powinien być zgodny z wymaganiami RFC 2253 albo RFC 4514.



7. Kliknij *Zapisz* w celu zapisania zmian w definicji użytkownika.

Related Topics:

- [Dodawanie użytkownika](#)

22.7 Uwierzytelnienie

Fudo Enterprise ma szeroki spektrum metod uwierzytelnienia użytkownika przed serwerem docelowym. Są to:

- uwierzytelnienie zewnętrzne:
 - *CERB*,
 - *RADIUS*,
 - *LDAP*,
 - *Active Directory*,
- *OATH*,
- *SMS*,
- *DUO*,

- *OpenID Connect.*

Uwierzytelnienie użytkowników za pomocą zewnętrznych serwerów uwierzytelnienia wymaga skonfigurowania połączeń z serwerami usług danego typu.

22.7.1 Widok zarządzania serwerami uwierzytelnienia

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

Aby przejść do widoku zarządzania serwerami uwierzytelnienia, wybierz z lewego menu *Ustawienia > Uwierzytelnienie*.

22.7.2 Definicja serwera zewnętrznego uwierzytelniania

Aby dodać serwer uwierzytelnienia, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia > Uwierzytelnienie*.
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.
5. Kliknij *Zapisz*.

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.
Drugi czynnik	Dodatkowa weryfikacja metodą uwierzytelnienia OATH, SMS albo DUO.
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.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Parametr	Opis
Drugi czynnik	Dodatkowa weryfikacja metodą uwierzytelnienia OATH, SMS albo DUO.
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. <code>dc=example,dc=com</code>
Drugi czynnik	Dodatkowa weryfikacja metodą uwierzytelnienia OATH, SMS albo DUO.
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 uwierzytelniania.
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.
Drugi czynnik	Dodatkowa weryfikacja metodą uwierzytelnienia OATH, SMS albo DUO.

Ostrzeżenie: Kiedy została wybrana dodatkowa metoda uwierzytelnienia (OATH, SMS or DUO) jako drugi czynnik dla synchronizacji z zewnętrznym serwerem uwierzytelnienia (AD / LDAP / CERB / RADIUS), nie będzie wystarczające wybranie samego Zewnętrznego uwierzytelnienia w definicji Użytkownika. Dodatkowo wybrana metoda uwierzytelnienia powinna zostać skonfigurowana dla Użytkownika jako główna metoda uwierzytelnienia. Wtedy Użytkownik będzie automatycznie synchronizowany, zgodnie z ustawieniami źródła zewnętrznego uwierzytelnienia.

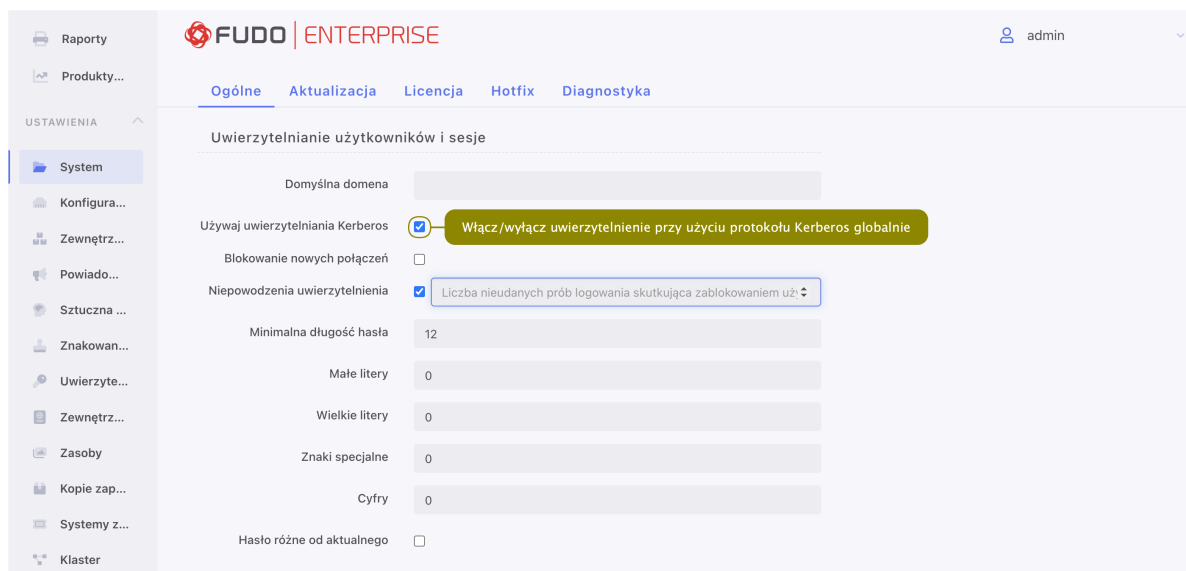
Informacja: Przy konfiguracji uwierzytelnienia **Radius** Fudo Enterprise wspiera tylko **Password Authentication Protocol (PAP)**. Aby zagwarantować kompatybilność i skuteczne uwierzytelnienie, upewnij się, że serwer Radius jest skonfigurowany do akceptowania żądań PAP.

Informacja:

- Uwierzytelnienie przy użyciu Kerberosa jest pierwszym krokiem w przypadku korzystania

z metody zewnętrznego uwierzytelnienia Active Directory.

- Funkcjonalność ta jest domyślnie włączona, a Kerberos jest używany do uwierzytelnienia na serwerze podczas sesji RDP oraz przy metodzie zewnętrznego uwierzytelnienia Active Directory.
- W celu wyłączenia obsługi protokołu Kerberos wybierz *Ustawienia > System*, przejdź do sekcji *Uwierzytelnianie użytkowników i sesje* i zaznacz opcję *Używaj uwierzytelniania Kerberos*.



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*.

22.7.3 Definicja uwierzytelniania OATH

Sprawdź szczegóły na stronie *Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator*.

22.7.4 Definicja uwierzytelniania SMS

1. Wybierz *Ustawienia > Uwierzytelnienie*.
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*.

Skonfiguruj metodę uwierzytelnienia SMS dla użytkownika:

4. Wybierz z lewego menu *Zarządzanie > Użytkownicy*.
5. Znajdź i wybierz użytkownika, dla którego chcesz uruchomić uwierzytelnianie SMS.
6. Przejdź do sekcji *Uwierzytelnienie* i z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz *SMS*.
 - W sekcji **Pierwszy składnik** wybierz *Hasło statyczne* lub *Uwierzytelnienie zewnętrzne* (AD lub LDAP).
 - Wprowadź numer telefonu w polu **Telefon**.
7. Kliknij *Zapisz*.
8. Zaloguj się do Access Gateway przy pomocy SMS kodu.

22.7.5 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 > Uwierzytelnienie*.
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*.

Skonfiguruj metodę uwierzytelnienia DUO dla użytkownika:

6. Wybierz z lewego menu *Zarządzanie > Użytkownicy*.
7. Znajdź i wybierz użytkownika, dla którego chcesz uruchomić uwierzytelnienie DUO.
8. Przejdź do sekcji *Uwierzytelnienie* i z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz *DUO*.
 - Z listy **Pierwszy składnik** wybierz *Hasło statyczne* lub *Zewnętrzne uwierzytelnianie* (AD lub LDAP).
 - Wprowadź *Użytkownik DUO*.
 - Wprowadź *ID użytkownika DUO*.
9. Kliknij *Zapisz*.
10. Zaloguj się do Access Gateway, akceptując notyfikację typu push z aplikacji Duo Mobile.

22.7.6 Definicja uwierzytelniania OpenID Connect

Definicja uwierzytelnienia przez OpenID Connect 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 Access Gateway oraz w Panelu Admina.

Postępuj zgodnie z instrukcją, aby ustawić uwierzytelnienie za pomocą OpenID Connect:

1. Wybierz *Ustawienia > Uwierzytelnienie*.
2. Wybierz zakładkę **Uwierzytelnienie OpenID Connect**.
3. Kliknij *Dodaj źródło zewnętrznego uwierzytelnienia*.
4. Zaznacz opcję *Włączone* dla uruchomienia uwierzytelnienia OpenID Connect za pomocą tego konkretnego dostawcy.
5. Podaj nazwę (na przykład, *Azure*, *Okta*).
6. Podaj *Configuration URL*.

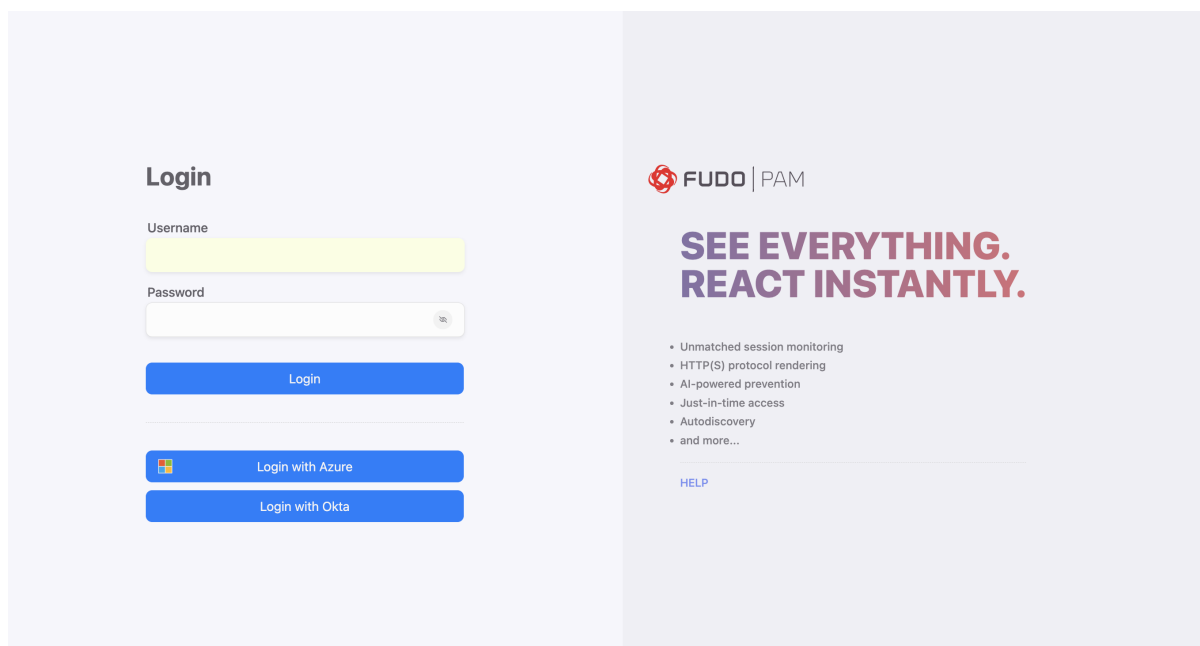
Informacja: Ten URL jest specyficzny dla każdego dostawcy OpenID Connect, więc służy do jego identyfikacji w celu prawidłowej konfiguracji. Przykład *Configuration URL* dla Google: <https://accounts.google.com/.well-known/openid-configuration>.

7. Podaj *Client ID*, *Client secret*. Te dane są dostępne po rejestracji na stronie wybranego dostawcy.
8. Dodaj *Username mapping* oraz *Email mapping*. Te pola są przydatne w przypadku innej konwencji nazewnictwa użytkownika.
9. Podaj *Bind address*.
10. Kliknij *Zapisz*.

Informacja: Algorytm ustalania tożsamości użytkownika jest następujący:

1. Użytkownik jest początkowo identyfikowany za pomocą pola `sub` od dostawcy OpenID Connect (OIDC).
2. Jeśli użytkownik nie został zidentyfikowany za pomocą pola `sub`, następnym krokiem jest sprawdzenie ustawienia *autolink* dla dostawcy OIDC. Jeśli to ustawienie jest niepoprawne, proces kończy się bez odnalezienia użytkownika. Jeśli ustawienie *autolink* jest poprawne, proces wyszukiwania jest kontynuowany.
3. Jeśli zdefiniowano *Mapowanie nazwy użytkownika*, przeprowadzane jest wyszukiwanie odpowiadającego pola w danych JSON. Po zlokalizowaniu pola w danych, system następnie szuka użytkownika o tej nazwie.
4. Jeśli *Mapowanie nazwy użytkownika* nie zostało zdefiniowane, pole nie zostało odalone w danych lub użytkownik nie został odnaleziony po nazwie, kolejnym krokiem jest sprawdzenie, czy zdefiniowano *Mapowanie email*. Jeśli zostało zdefiniowane i istnieje w danych JSON, następnym krokiem jest próba zidentyfikowania użytkownika na podstawie tego adresu email.
5. Jeśli ani *Mapowanie nazwy użytkownika*, ani *Mapowanie email* nie są zdefiniowane, system będzie starał się zidentyfikować użytkownika po jego nazwie lub adresie email. Jest to realizowane przez wyszukiwanie w danych pól `upn` lub `unique_name` w tej określonej kolejności.
6. Gdy do identyfikacji użytkownika używane jest pole `email`, wymagane jest, aby w danych znajdowało się pole `email_verified` o wartości `true`.
7. Ostatnim krokiem jest sprawdzenie, czy odnaleziony użytkownik ma już przechowywane pole `sub`, inne niż to otrzymane od dostawcy OIDC. Jeśli się nie zgadzają, proces kończy się niepowodzeniem.
8. Otrzymane pole `sub` użytkownika jest przechowywane w bazie danych do przyszłego użytku.

-
11. Zaloguj się przy użyciu skonfigurowanej metody uwierzytelnienia:



Tematy pokrewne:

- *Metody uwierzytelniania*
- *Konfiguracja uwierzytelnienia OpenID Connect w Azure*
- *Opis systemu*
- *Integracja z serwerem CERB*

22.8 Zewnętrzne repozytoria haseł

Fudo Enterprise wspiera zewnętrzne repozytoria haseł do zarządzania hasłami dostępowymi.

22.8.1 CyberArk Enterprise Password Vault

Funkcja zdeprecjonowana od wersji 5.4

- Fudo Enterprise 5.4 jest ostatnią wersją obsługującą *CyberArk Enterprise Password Vault*. Funkcjonalność ta zostanie usunięta w kolejnym wydaniu.
 - Użytkownicy korzystający z *CyberArk Enterprise Password Vault* muszą dokonać migracji do *CyberArk Credential Provider*.
-

Dodawanie definicji repozytorium haseł

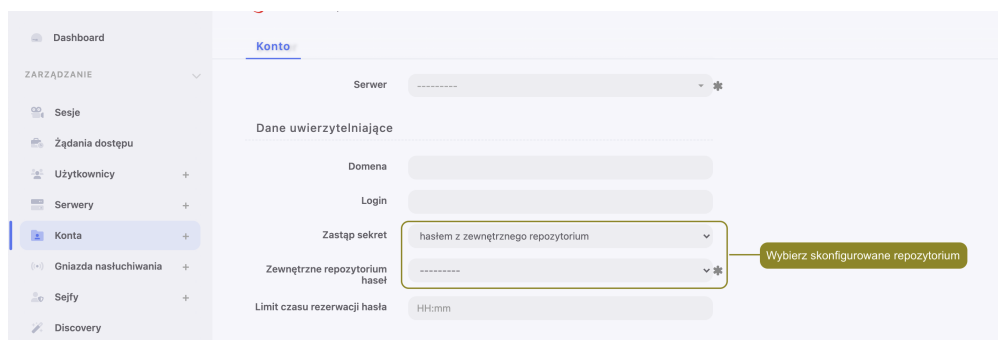
1. Wybierz z lewego menu *Ustawienia > Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Z listy rozwijalnej *Typ* wybierz *CyberArk Enterprise Password Vault*.
4. Wprowadź nazwę obiektu.

5. W polu *URL*, wprowadź ścieżkę do interfejsu API wybranego rozwiązania (HTTP lub HTTPS).

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

Przykład: `https://10.0.0.2/PWCWeb/`

6. W polu *Login* wprowadź nazwę użytkownika uprawnionego do pobierania haseł.
7. W polu *Hasło* i *Powtórz hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
8. Wprowadź identyfikator aplikacji.
9. 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*.

Informacja: Nie można usunąć definicji repozytorium haseł, jeśli jest ona przypisana do jakiegokolwiek konta.

Tematy pokrewne:

- *Uwierzytelnienie*
- *Opis systemu*
- *Integracja z serwerem CERB*

22.8.2 CyberArk Credential Provider

Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia > Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. Z listy rozwijalnej *Typ* wybierz *CyberArk Credential Provider*.
4. Wprowadź nazwę obiektu.
5. W polu *URL*, wprowadź ścieżkę do interfejsu API wybranego rozwiązania (HTTP lub HTTPS).

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

Przykład: `https://10.0.0.2/PWCWeb/`

6. Wprowadź identyfikator aplikacji.
7. Podaj *Sejf* (opcjonalnie). Jeśli *Sejf* nie jest zdefiniowany, wyszukiwanie zostanie przeprowadzone we wszystkich sejfach CyberArk.

Informacja: Wyszukiwanie danego serwera/konta odbywa się w oparciu o następujące atrybuty *CyberArk Credential Provider*, które należy zdefiniować zgodnie z poniższymi zasadami:

- **Address** - musi zgadzać się z adresem IP serwera Fudo (pole wymagane),
 - **UserName** - musi zgadzać się z wartością pola *Login* podaną podczas tworzenia konta Fudo (pole wymagane) - patrz rozdział *Dodawanie konta typu regular*,
 - **Safe** - musi zgadzać się z polem *Sejf* w utworzonym w Fudo zewnętrznym repozytorium haseł (pole opcjonalne).
-

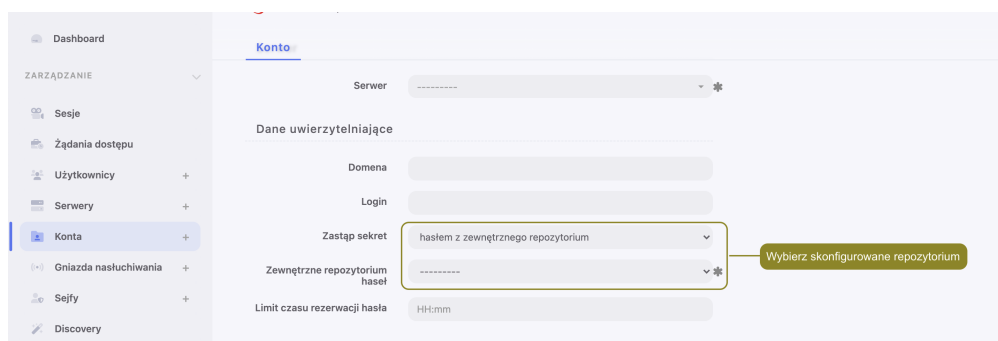
8. W przypadku uwierzytelniania za pomocą certyfikatu klienta, należy zdefiniować pola *Certyfikat tożsamości* i *Klucz tożsamości*.

Informacja: Pola *Certyfikat tożsamości* i *Klucz tożsamości* należy wypełnić w formacie PKCS #8. Aby dowiedzieć się, jak wygenerować *Certyfikat tożsamości* i *Klucz tożsamości*, przejdź do następnej sekcji.

- Jeżeli użyto adresu HTTPS do API serwera haseł, w polu *Certyfikat SSL* podaj certyfikat serwera HTTPS.

Ostrzeżenie: W przypadku zastosowania protokołu LDAPS bez dostarczenia Certyfikatu SSL połączenie SSL zostanie zaakceptowane bez weryfikacji.

- Kliknij *Zapisz*.
- Przypisz repozytorium haseł do konta.
 - Wybierz *Zarządzanie > Konta*.
 - Wyszukaj i kliknij definicję konta.
 - W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastęp sekret*, wybierz *hasłem z zewnętrznego repozytorium*.
 - Z listy rozwijalnej *Zewnętrzne repozytorium haseł*, wybierz wcześniej zdefiniowane repozytorium.



- Kliknij *Zapisz*.

Generowanie klucza i certyfikatu ‘CyberArk Credential Provider’

- Wygeneruj losowy numer seryjny (np. 11223344556677), który posłuży CyberArk do weryfikacji klienta.
- Wygeneruj pliki *client.key* i *client.crt* za pomocą *openssl*. Przykład:

```
openssl req -new -newkey rsa:2048 -days 365 -nodes -x509 -subj "/C=PL/ST=Mazowieckie/
↵L=Warsaw/OU=MyApp/CN=client" -set_serial "11223344556677" -keyout client.key -out
↵client.crt
```

- Wklej zawartość pliku *client.crt* w polu *Certyfikat tożsamości*.
- Wklej zawartość pliku *client.key* w polu *Klucz tożsamości*.
- Dodaj wygenerowany wcześniej numer seryjny do konfiguracji uwierzytelniania serwera w CyberArk.

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*.

Informacja: Nie można usunąć definicji repozytorium haseł, jeśli jest ona przypisana do jakiegokolwiek konta.

Tematy pokrewne:

- *Uwierzytelnienie*
- *Opis systemu*
- *Integracja z serwerem CERB*

22.8.3 Thycotic Secret Server

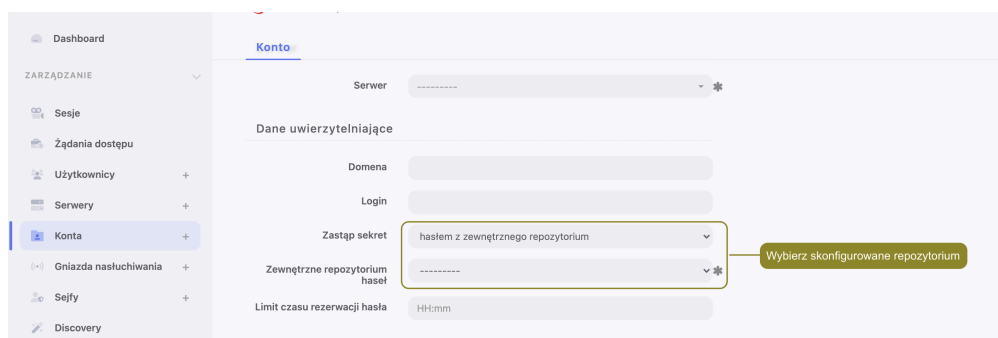
Dodawanie definicji repozytorium haseł

1. Wybierz z lewego menu *Ustawienia > Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj serwer*.
3. 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 protokołu HTTPS, aby komunikacja z serwerem podlegała szyfrowaniu.

7. W polu *Login* wprowadź nazwę użytkownika uprawnionego 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.
10. Kliknij *Zapisz*.
11. Przypisz repozytorium haseł do konta.
 - Wybierz *Zarządzanie > Konta*.
 - Wyszukaj i kliknij definicję konta.

- W sekcji *Dane uwierzytelniające*, z listy rozwijalnej *Zastęp 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*.

Informacja: Nie można usunąć definicji repozytorium haseł, jeśli jest ona przypisana do jakiegokolwiek konta.

Tematy pokrewne:

- *Uwierzytelnienie*
- *Opis systemu*
- *Integracja z serwerem CERB*

22.8.4 Local Administrator Password Solutions (LAPS)

Konfiguracja Active Directory/LDAP

Serwer LDAP powinien mieć określone atrybuty w klasie obiektu `computer`:

- `dNSHostName` - nazwa serwera - musi być identyczna z unikalną nazwą serwera podaną podczas jego tworzenia w Fudo Enterprise (patrz np. rozdział *Dodawanie serwera TCP*),

- `sAMAccountName` - login do powyższego serwera - musi być identyczny z *Loginem* konta z sekcji *Dane uwierzytelniające* (patrz rozdział *Dodawanie konta typu regular*),
- `ms-Mcs-AdmPwd` - hasło w postaci *plaintext*,
- `ms-Mcs-AdmPwdExpirationTime` - data wygaśnięcia hasła (opcjonalnie).

Dodawanie definicji repozytorium haseł

Informacja: Aby dodać repozytorium haseł LAPS w Fudo Enterprise musisz podać następujące parametry AD/LDAP:

- URL do serwera AD/LDAP, np. `ldaps://10.10.1.1:636/`,
 - *Base DN* do serwera AD/LDAP, np. `dc=company,dc=com`,
 - Login i hasło do serwera AD/LDAP, np. `cn=admin,dc=company,dc=com`,
 - Certyfikat CA do sprawdzania poprawności połączenia SSL z serwerem AD/LDAP.
-

1. Wybierz z lewego menu *Ustawienia > Zewnętrzne repozytoria haseł*.
 2. Kliknij *+ Dodaj serwer*.
 3. Z listy rozwijalnej *Typ* wybierz *Local Administrator Password Solutions (LAPS)*.
 4. Wprowadź nazwę obiektu.
 5. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.
-

Informacja: Obsługiwane formaty URL:

- `ldap://<serer>[:<port>]/` - dla połączenia przy użyciu protokołu TCP bez szyfrowania;
 - `ldaps://<serer>[:<port>]/` - dla połączenia przy użyciu protokołu SSL.
-

6. W polu *Login* wprowadź nazwę użytkownika uprawnionego do pobierania haseł.
7. W polu *Hasło* i *Powtórz hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
8. Podaj *Base DN* serwera AD/LDAP.
9. Podaj certyfikat SSL - jeśli w polu *URL* określono protokół LDAPS.

<p>Ostrzeżenie: W przypadku zastosowania protokołu LDAPS bez dostarczenia Certyfikatu SSL połączenie SSL zostanie zaakceptowane bez weryfikacji.</p>

10. Kliknij *Zapisz*.
11. 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*.

Informacja: Wyszukiwanie danego serwera/konta odbywa się na podstawie następujących atrybutów, które należy ustawić zgodnie z poniższymi zasadami:

- **dNSHostName** - nazwa serwera - musi być zgodna z unikalną nazwą serwera Fudo podaną podczas jego tworzenia (patrz np. rozdział *Dodawanie serwera TCP*),
- **sAMAccountName** - login do powyższego serwera - musi być identyczny z *Loginem* konta z sekcji *Dane uwierzytelniające* (patrz rozdział *Dodawanie konta typu regular*).

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*.

Informacja: Nie można usunąć definicji repozytorium haseł, jeśli jest ona przypisana do jakiegokolwiek konta.

Tematy pokrewne:

- *Uwierzytelnienie*
- *Opis systemu*
- *Integracja z serwerem CERB*

Tematy pokrewne:

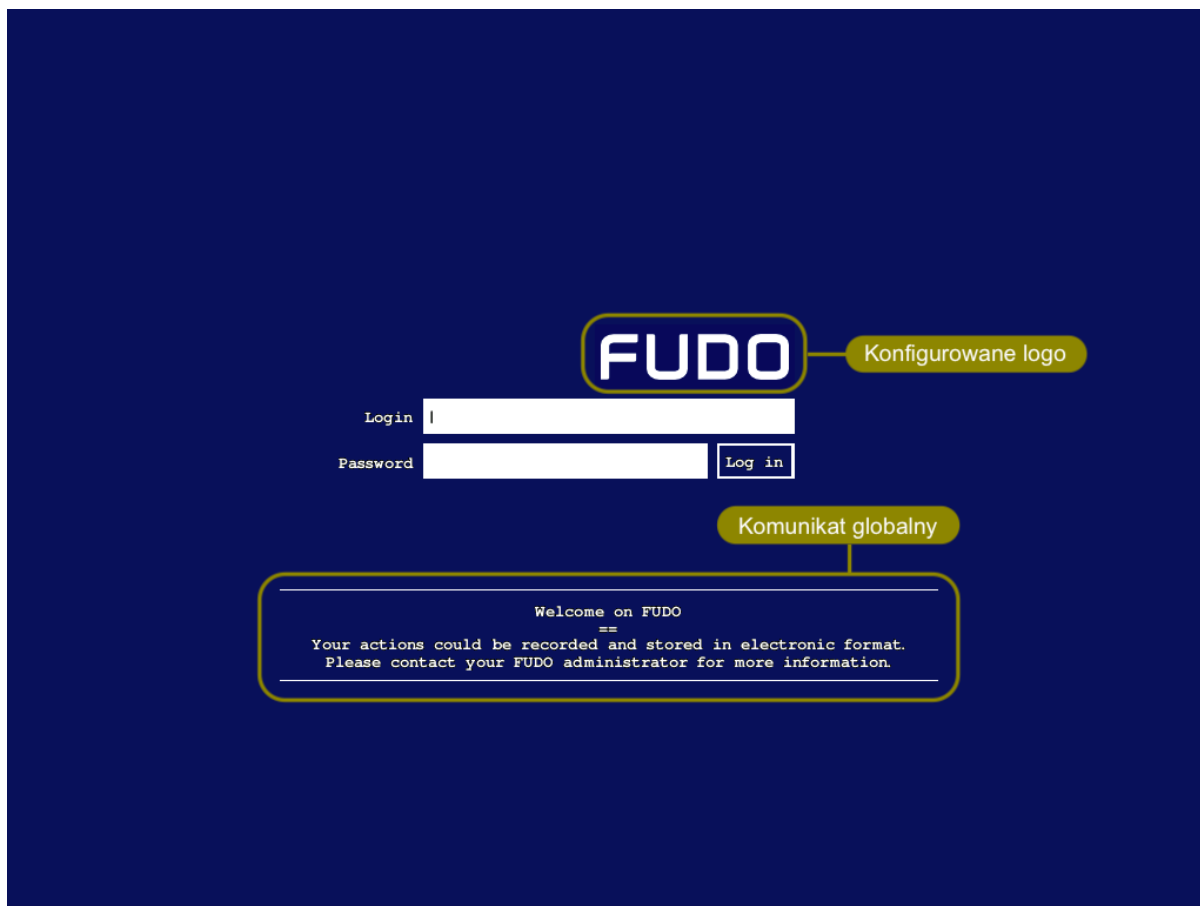
- *Uwierzytelnienie*

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

22.9 Zasoby

22.9.1 Konfiguracja ekranu logowania RDP/VNC

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



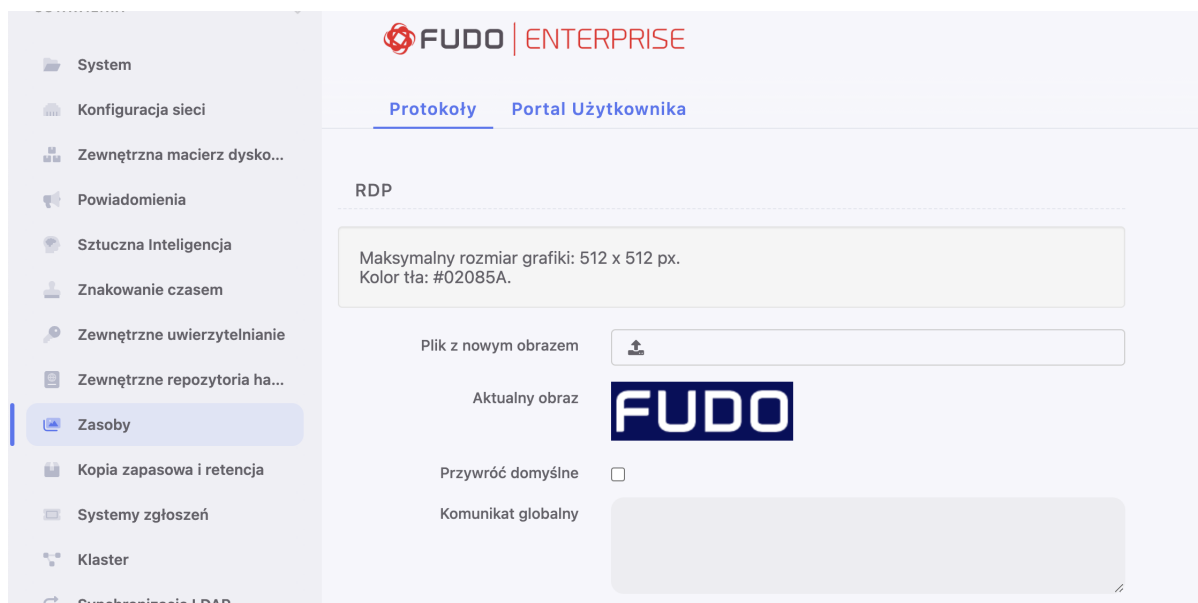
Ustawienia dla ekranu logowania RDP

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*.

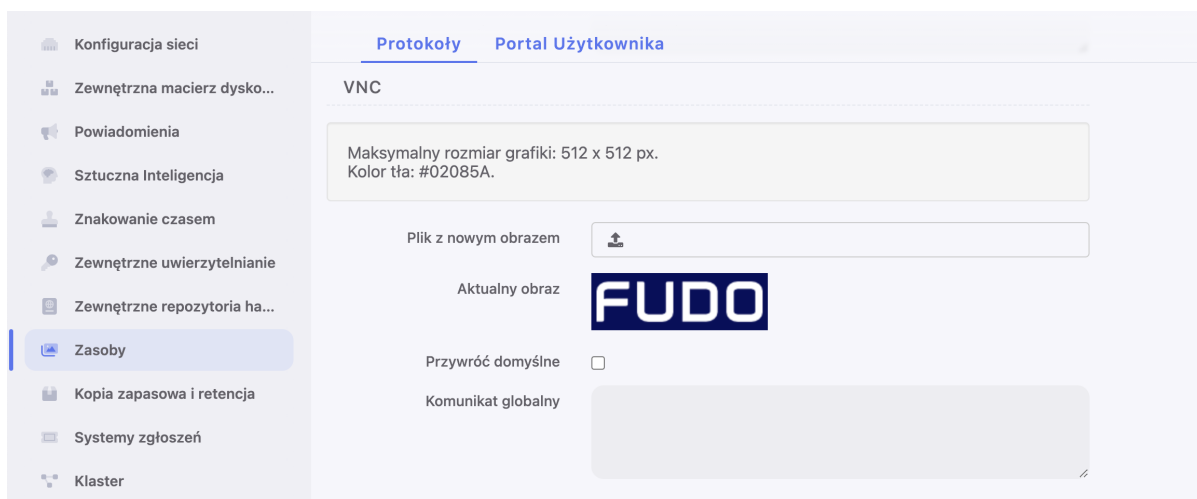
Ustawienia dla ekranu logowania VNC

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:

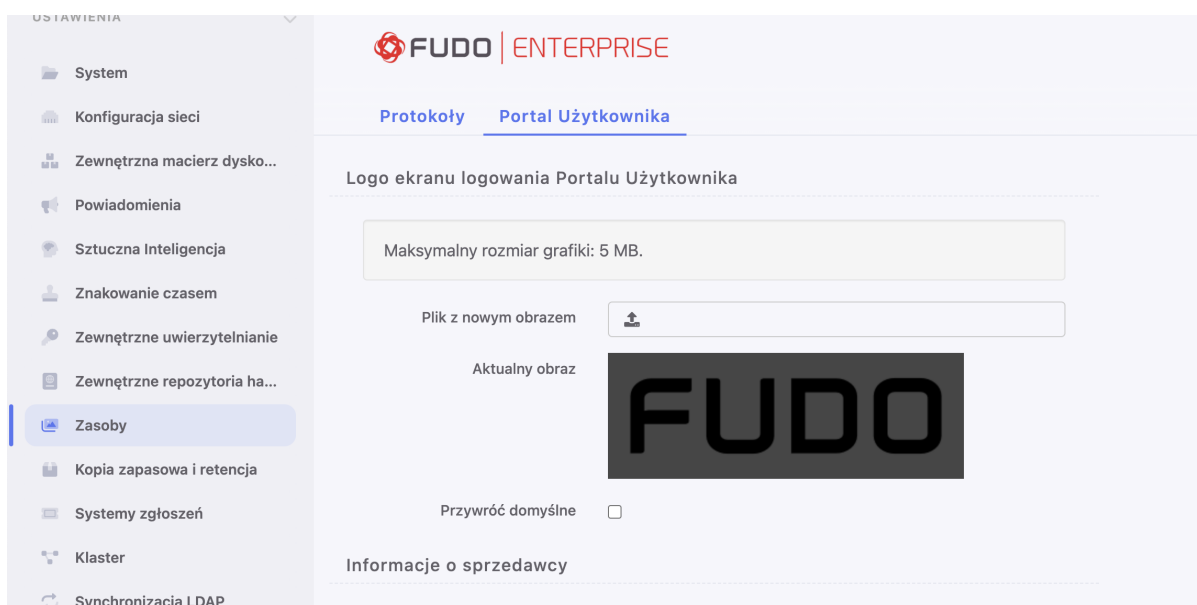
- *Szybki start - RDP*

22.9.2 Ekran logowania Portalu użytkownika

Fudo Enterprise 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*

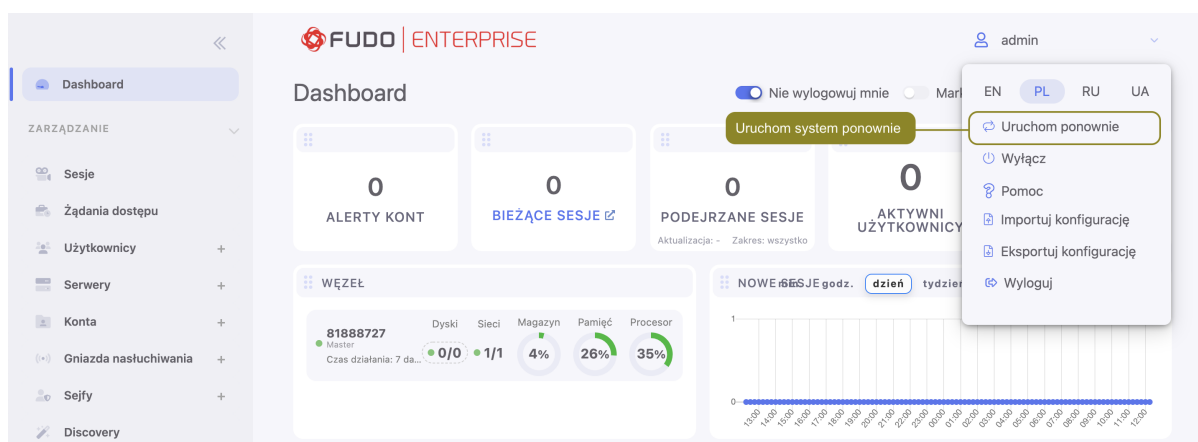
22.10 Przywracanie poprzedniej wersji systemu

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 jakiegokolwiek 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:

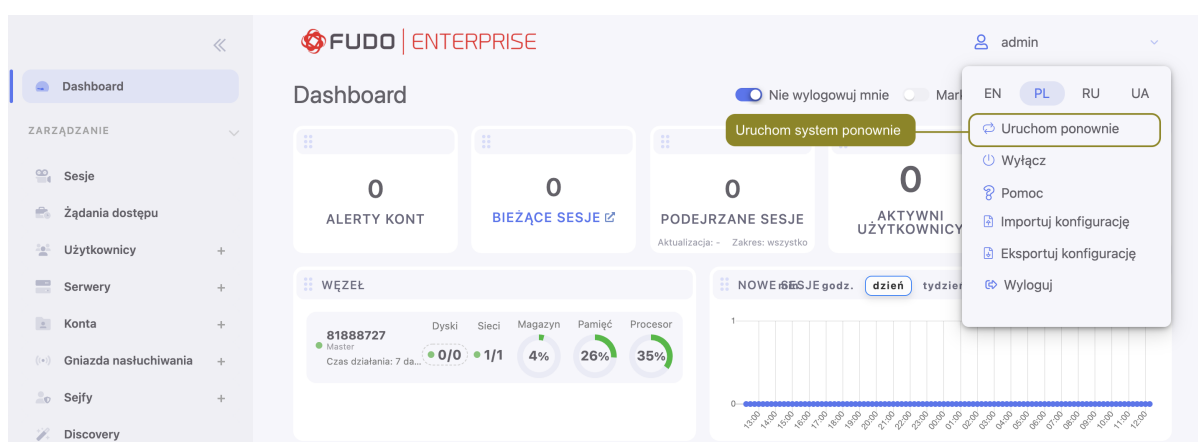
- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

22.11 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 jakiegokolwiek 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*

22.12 SNMP

Fudo Enterprise 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 użytkownika*.
7. Wpisz nazwę użytkownika i wybierz **Service** z listy rozwijanej *Rola*.
8. Uzupełnij pozostałe parametry tworzonego użytkownika według własnych wymagań.
9. Kliknij *Zapisz* w celu utworzenia użytkownika oraz umożliwienia dodania metod uwierzytelnienia.
10. W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Dodaj metodę uwierzytelnienia*, wybierz **Hasło statyczne** 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.

-
11. Przejdź do zakładki *Więcej* i w sekcji *SNMP*, zaznacz opcję *Włączone*.
 12. Z listy rozwijalnej *Metoda uwierzytelnienia*, wybierz metodę *SHA* lub *MD5*.
 13. Z listy rozwijalnej *Metoda szyfrowania*, wybierz algorytm szyfrujący komunikację SNMP (*AES* lub *DES*).
 14. Kliknij *Zapisz*.

Konfigurowanie SNMPv3 TRAP

Kiedy polityka zostaje naruszona, Fudo może wysłać SNMPv3 TRAP, `fudoPolicyViolationNotification` z informacją, zawierającą szczegóły której sesji, który użytkownik naruszył politykę. Po więcej informacji zjedź do definicji MIB Fudo niżej.

Aby powiadomienia SNMP TRAP były wysyłane zgodnie z konfiguracją *Polityki*, SNMPv3 TRAP powinno zostać odpowiednio ustawione oraz dodane do polityki.

Aby skonfigurować SNMP TRAP, postępuj zgodnie z instrukcją:

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

3. Wpisz nazwę użytkownika i wybierz **Service** z listy rozwijanej *Rola*.
4. Uzupełnij pozostałe parametry tworzonego użytkownika według własnych wymagań.
5. Kliknij *Zapisz* w celu utworzenia użytkownika oraz umożliwienia dodania metod uwierzytelnienia.
6. W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Dodaj metodę uwierzytelnienia*, wybierz **Hasło statyczne** 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.

7. Przejdź do zakładki *Więcej* i w sekcji *SNMP*, zaznacz opcję *Włączone*.
8. Z listy rozwijalnej *Metoda uwierzytelnienia*, wybierz metodę *SHA* lub *MD5*.
9. Z listy rozwijalnej *Metoda szyfrowania*, wybierz algorytm szyfrujący komunikację SNMP (*AES* lub *DES*).
10. Kliknij *Zapisz*.
11. Wybierz *Ustawienia > System*.
12. Przewiń do sekcji *Serwisowanie i nadzór*.
13. Podaj *adres* serwera SNMPv3 TRAP oraz *port*.
14. Wybierz użytkownika o roli **service**, stworzonego na kroku 1.
15. Kliknij *Zapisz*.

Ponieważ Fudo Enterprise korzysta z SNMPv3 do wysłania TRAPów, oprogramowanie zarządzające (takiej jak snmptrapd z Net-SNMP) powinno wiedzieć, jakie są login oraz hasło.

Informacja: Notyfikacja TRAP `fudoPolicyViolationNotification` zawiera identyfikatory

obiektów Fudo: `sessionId`, `userId` and `policyId`. Ponieważ wszystkie identyfikatory w Fudo - to są liczby całkowite 64-bitowe, a SNMP nie wspiera takich liczb w sposób natywny, te identyfikatory są zakodowane jako 8-bajtowa tablica rozpoczynająca się od najbardziej znaczącego bajtu.

SNMP MIBs

MIB wspierane przez Fudo Enterprise:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - częściowe wsparcie
- UCD-SNMP-MIB

22.12.1 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
<p>Informacja: Ta funkcja nie jest wspierana przez wszystkie urządzenia Fudo Enterprise. Skontaktuj się z działem wsparcia technicznego, aby uzyskać więcej informacji.</p>	
.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

22.12.2 Rozszerzenia SNMP Fudo Enterprise

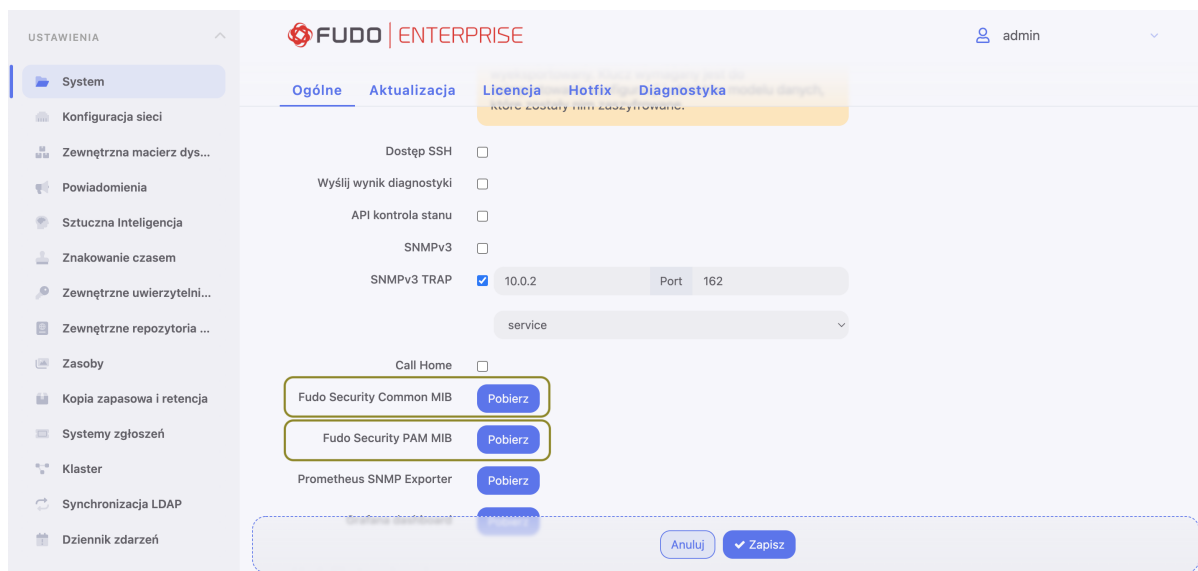
Informacje ogólne

Rozszerzenia SNMP umożliwiają monitorowanie liczby sesji SNMP, status ZFS, status zasilaczy (jeśli jest dostępny), temperaturę rdzeni procesorów, status S.M.A.R.T dysków twardej (temperatura, realokacja sektorów, stan urządzeń).

Specyfikacja pliku MIB rozszerzeń SNMP

Poniższe pliki MIB mogą zostać wczytane do menedżera SNMP w celu obsługi rozszerzeń specyficznych dla Fudo Enterprise.

Ostrzeżenie: W wersji 4.3 zmianie uległy nazwy plików MIB. Zamień dotychczasowe pliki MIB z nową definicją.



Tematy pokrewne:

- *Bezpieczeństwo*
- *Rozwiązywanie problemów*
- *Polityki*

22.13 Kopia zapasowa i retencja

22.13.1 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, FTP lub SFTP.

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

1. Wybierz z lewego menu *Ustawienia* > *Kopia zapasowa i retencja*.
2. Zaznacz opcję *Włączone* w podzakładce *Kopia zapasowa*.
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*.

4. Podaj nazwę dla miejsca docelowego.

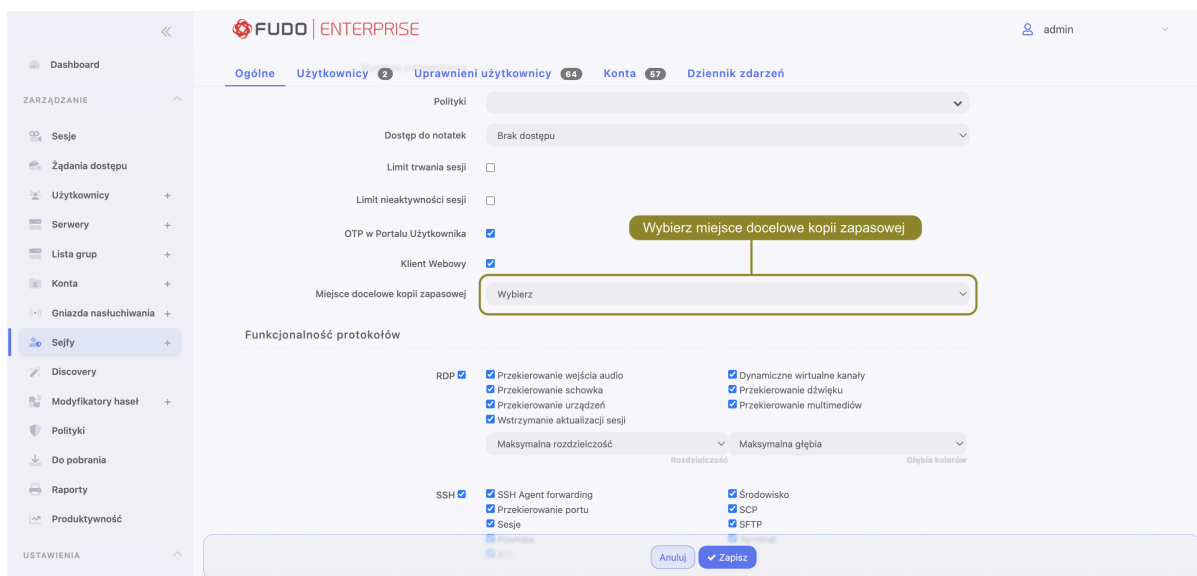
5. Wybierz typ: S3, Backblaze, FTP lub SFTP.

6. Podaj dodatkowe dane w zależności od wybranego typu:

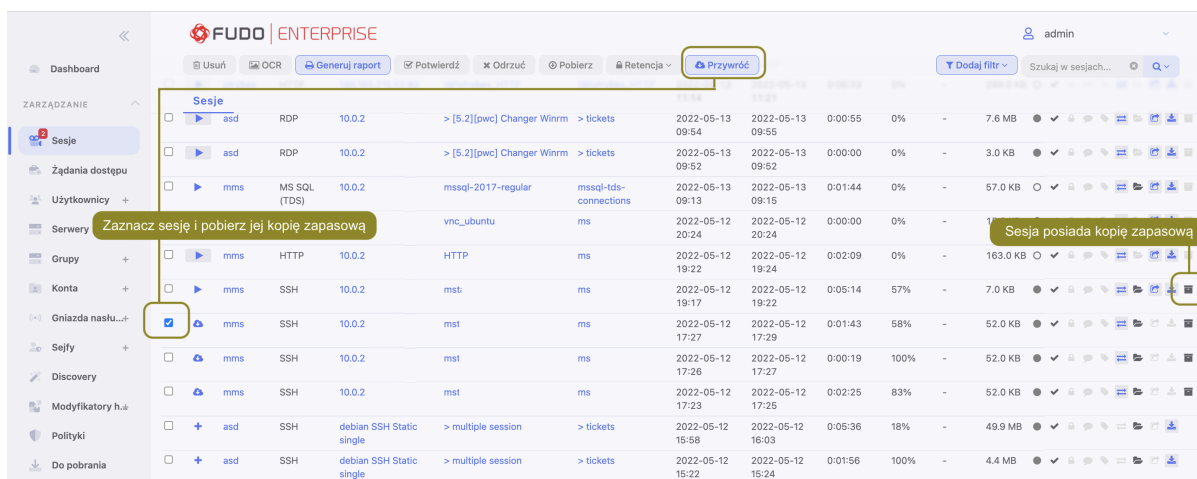
- Konfigurując miejsce docelowe kopii zapasowej w **S3** podaj dodatkowo: *Bucket*, *Katalog*, *Klucz dostępu*, *Tajny klucz dostępu*, *Region* i *Endpoint*.
- Konfigurując miejsce docelowe kopii zapasowej w **Backblaze**, podaj: *Bucket*, *Katalog* oraz poświadczenia, takie jak *Konto* i *Klucz*.
- Dla miejsca docelowego kopii zapasowej konfigurowanego poprzez **FTP** podaj: *Katalog*, *Adres serwera* oraz poświadczenia, takie jak *Login* i *Hasło*.
- Dla miejsca docelowego kopii zapasowej konfigurowanego poprzez **SFTP** podaj: *Katalog*, *Adres serwera*, *Login*, *Klucz prywatny użytkownika*, *Klucz publiczny serwera* oraz numer portu.

7. Kliknij *Zapisz*.

Informacja: Skonfigurowane miejsce docelowe może też zostać dodane do sejfów, aby dane sesji były przechowywane automatycznie.



Jeśli sesja posiada kopię zapasową poza Fudo Enterprise, dla niej jest dostępna opcja *Przywróć*, służąca do pobrania kopii zapasowej do lokalnej instancji Fudo Enterprise.



Tematy pokrewne:

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

22.13.2 Retencja danych

Fudo Enterprise obsługuje dwa scenariusze retencji danych w zależności od użycia pamięci zewnętrznej:

- **Dwuetaapowa retencja:** Początkowo dane są przenoszone z pamięci wewnętrznej do zewnętrznej pamięci połączonej w standardzie Fiber Channel. Po upływie zdefiniowanego okresu czasu dane sesji są automatycznie usuwane.
- **Jednoetaapowa retencja:** W przypadku braku pamięci zewnętrznej sesje zostaną natychmiast usunięte z Fudo Enterprise.

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.

Włączenie retencji danych

Aby włączyć retencję danych, postępuj zgodnie z poniższą instrukcją:

1. Wybierz z lewego menu *Ustawienia > Kopia zapasowa i retencja > Retencja*.
2. W sekcji *Retencja danych*, zaznacz opcję *Usuwanie danych sesji* oraz w polu *Usuwanie danych sesji po* podaj liczbę dni, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.
3. W sekcji *Retencja logów*, zaznacz opcję *Usuwanie logów debug* oraz w polu *Usuwanie logów debug po* podaj liczbę dni, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.
4. W sekcji *Retencja logów - wrażliwe* podaj liczbę dni, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.

Ostrzeżenie: Opcja *Usuwanie logów po* jest aktywna tylko w sytuacji, kiedy funkcja *Zezwól na usuwanie logów* w sekcji *Funkcjonalności wrażliwe i bezpieczeństwo systemu* zakładki *Ustawienia > System* została zaznaczona oraz potwierdzona przez dwóch administratorów.

5. Kliknij *Zapisz*.

Nadpisanie wartości parametru retencji danych dla konta

Istnieje możliwość nadpisania wartości parametru retencji danych dla wybranego konta. W tym celu edytuj ustawienia konta postępując zgodnie z poniższą instrukcją:

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

2. Odszukaj na liście definicję konta, którą chcesz edytować.
3. Kliknij nazwę konta.
4. 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.
5. Kliknij *Zapisz*.

Zarządzanie retencją wybranych sesji

Fudo Enterprise umożliwia wykluczenie wybranych sesji z procesu retencji, aby nie zostały automatycznie usunięte. Procedura wykluczania sesji opisana została w rozdziale *Zarządzanie retencją sesji*.

Tematy pokrewne:

- *Mechanizmy bezpieczeństwa*
- *Eksportowanie/importowanie konfiguracji systemu*
- *Creating a new safe*

22.14 Zewnętrzna macierz dyskowa

Fudo Enterprise 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.
-


22.14.1 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*.

22.14.2 Rozszerzanie zewnętrznej macierzy dyskowej

Po zmianie rozmiaru obiektu WWN, należy rozszerzyć dostępną powierzchnię przechowywania w panelu administracyjnym Fudo Enterprise.

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:

- *Kopia zapasowa systemu*

22.15 Eksportowanie/importowanie konfiguracji systemu

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

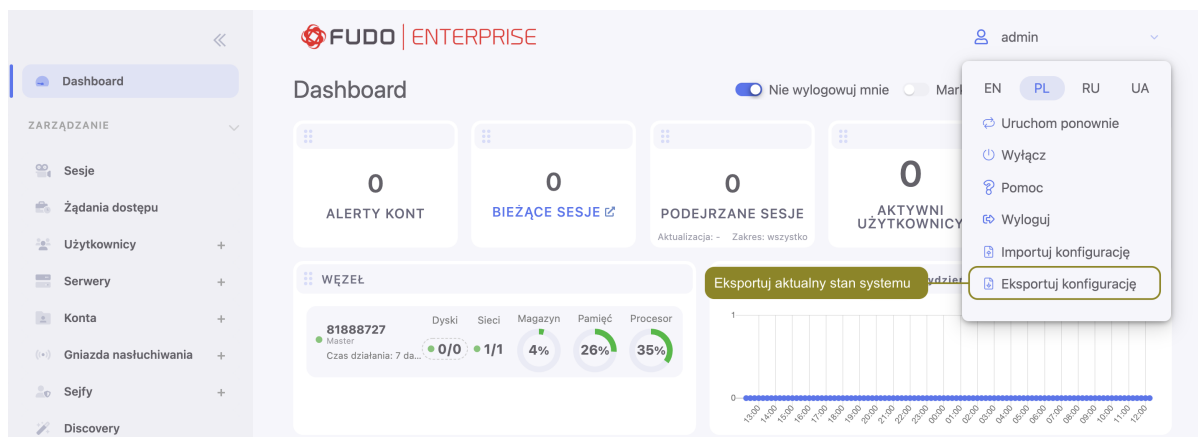
Ostrzeżenie: Wyeksportowana konfiguracja zawiera poufne informacje.

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

22.15.1 Eksportowanie konfiguracji

Aby wyeksportować konfigurację systemu, postępuj zgodnie z poniższą instrukcją.

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



22.15.2 Importowanie konfiguracji

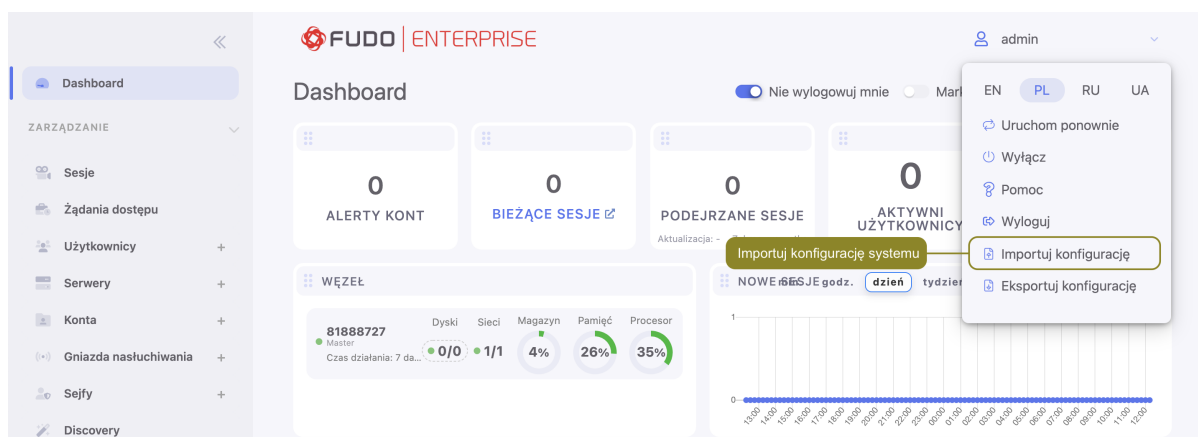
Ostrzeżenie: Zainicjowanie systemu wcześniej zapisaną konfiguracją spowoduje utratę wszystkich danych sesji.

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*
- *Kopia zapasowa systemu*
- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

22.16 Konfiguracja klastrowa

Klaster Fudo Enterprise 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*.

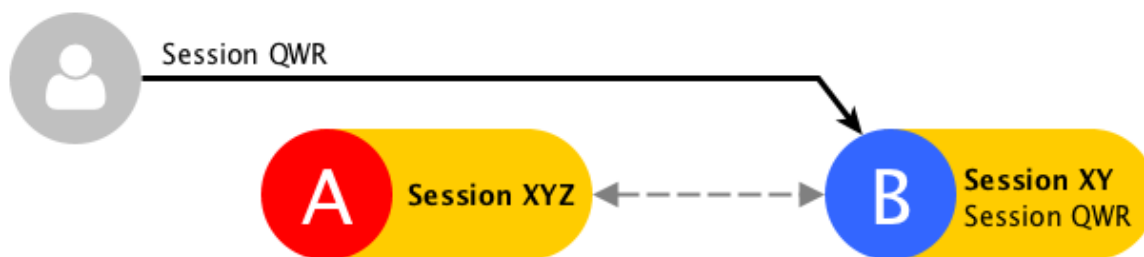
Dane bieżącej sesji są replikowane w trakcie jej trwania.



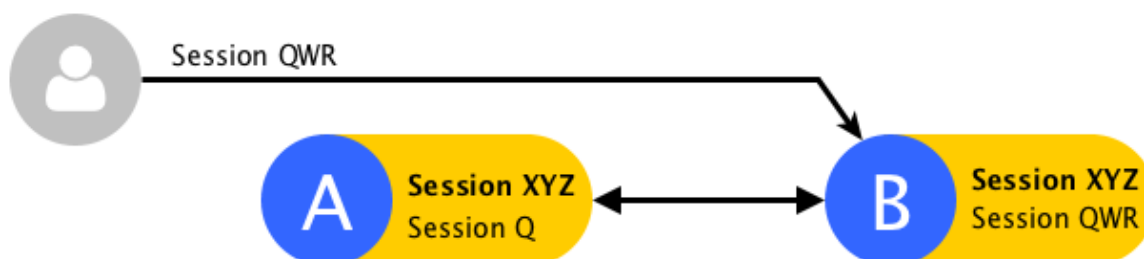
W przypadku, gdy węzeł ulegnie awarii, bieżące sesje zostaną zerwane. . .




. . . 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 zsynchronizowaniu danych.



Stan replikacji danych sesji można zweryfikować klikając ikonę  na liście sesji.

Użytkownik	Protokół	Adres doc.	Konto	Sejf	Rozpoczęta	Zakończona	Czas trwania	Aktywność	Limit czasu	Rozmiar	Status replikacji sesji
mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssq-connn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssq-connn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssq-connn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssq-connn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssq-connn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	


22.16.1 Inicjowanie klastra

Ostrzeżenie: Prawidłowe funkcjonowanie klastra wymaga skonfigurowania *serwera czasu NTP* na wszystkich węzłach klastra.

Aby zainicjować klaster Fudo Enterprise 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*

22.16.2 Zarządzanie węzłami klastra

22.16.2.1 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 wę-

złów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

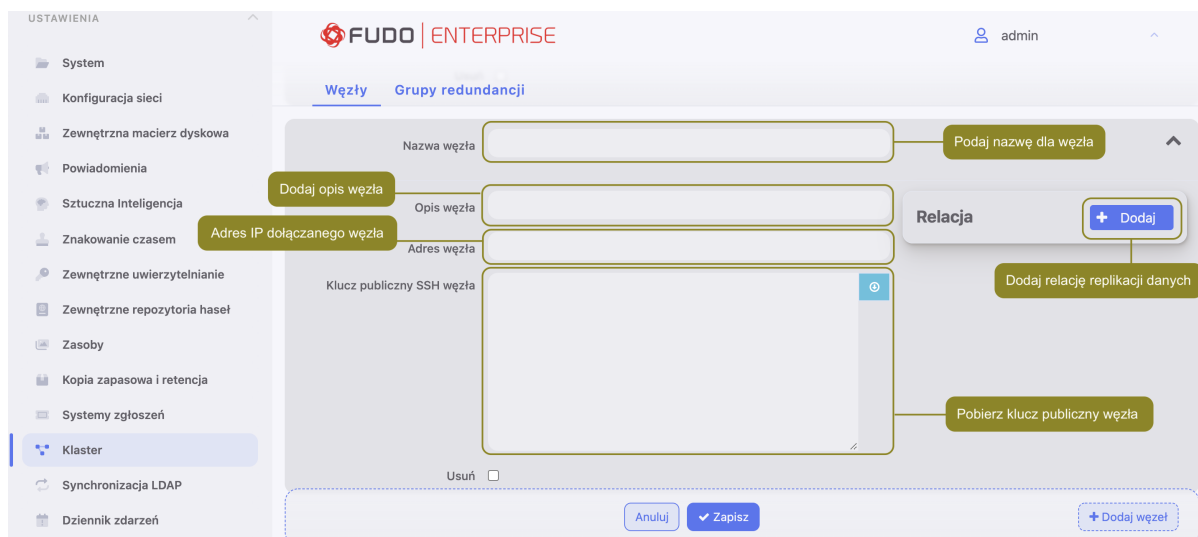
- Dane sesji oraz parametry konfiguracyjne (*serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, zewnętrzne serwery uwierzytelniania*) węzła dołączanego są usuwane i inicjowane na nowo danymi zreplikowanymi z klastra.


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

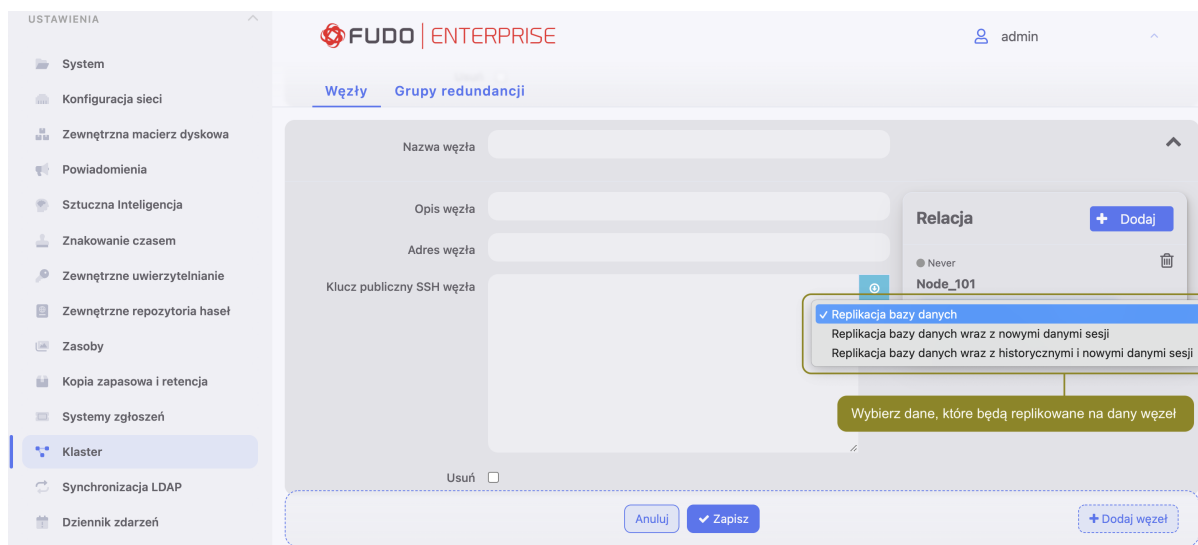
1. Zaloguj się do panelu administracyjnego Fudo Enterprise, na którym został *zainicjowany klaster*.
2. Wybierz z lewego menu *Ustawienia > Klaster*.
3. Kliknij *Dodaj węzeł*.

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

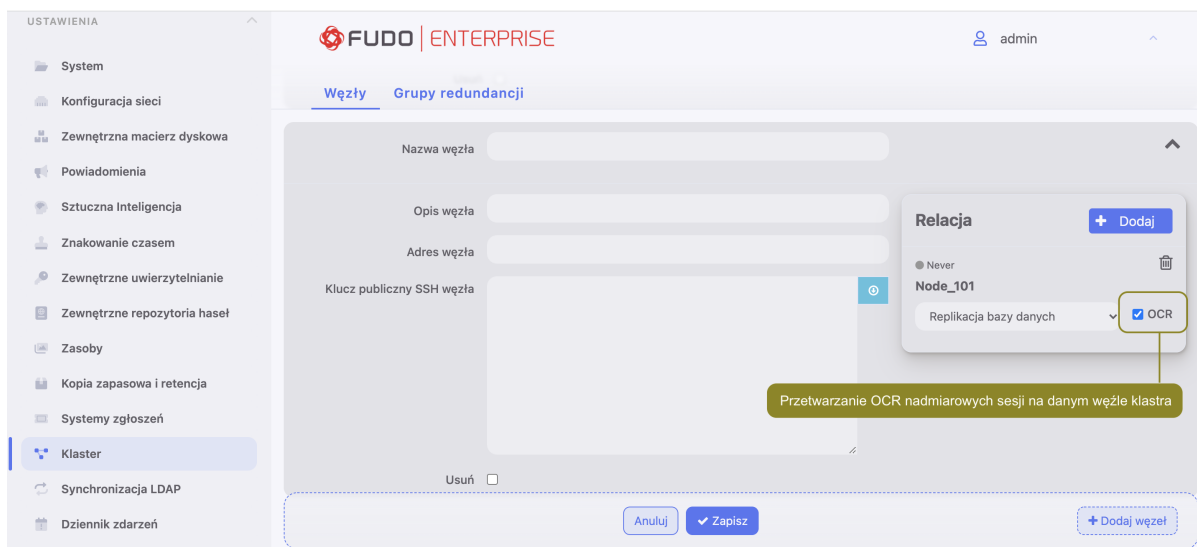
Informacja: Na wskazanym interfejsie sieciowym dołączanego węzła musi być aktywna opcja zarządzania urządzeniem. Informacje na temat konfigurowania ustawień sieciowych znajdziesz w rozdziale *Ustawienia sieci: Konfiguracja interfejsów sieciowych*.



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.

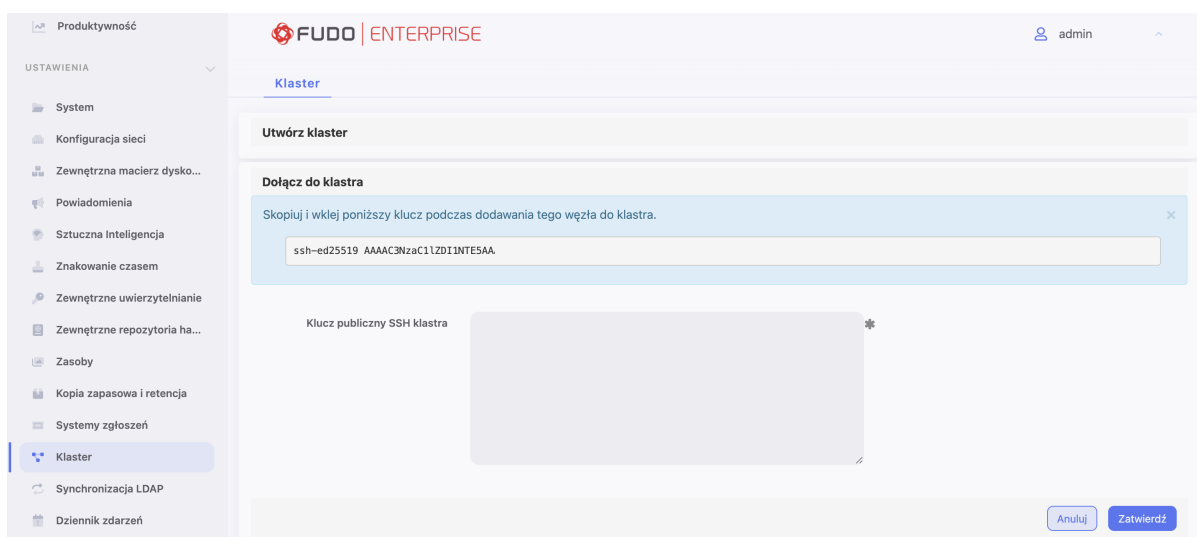


10. Zaznacz opcję *OCR*, aby wybrany węzeł przetwarzał nadwyżkę sesji graficznych.




Informacja: Każda instancja Fudo Enterprise ma ograniczoną, zdefiniowaną w licencji, liczbę procesów OCR przetwarzających sesje graficzne. Opcja *OCR* umożliwi oddelegowanie przetwarzania nadmiarowych sesji na wskazany węzeł, w sytuacji, w której liczba połączeń przekracza liczbę lokalnych procesów przetwarzających i indeksujących treści.

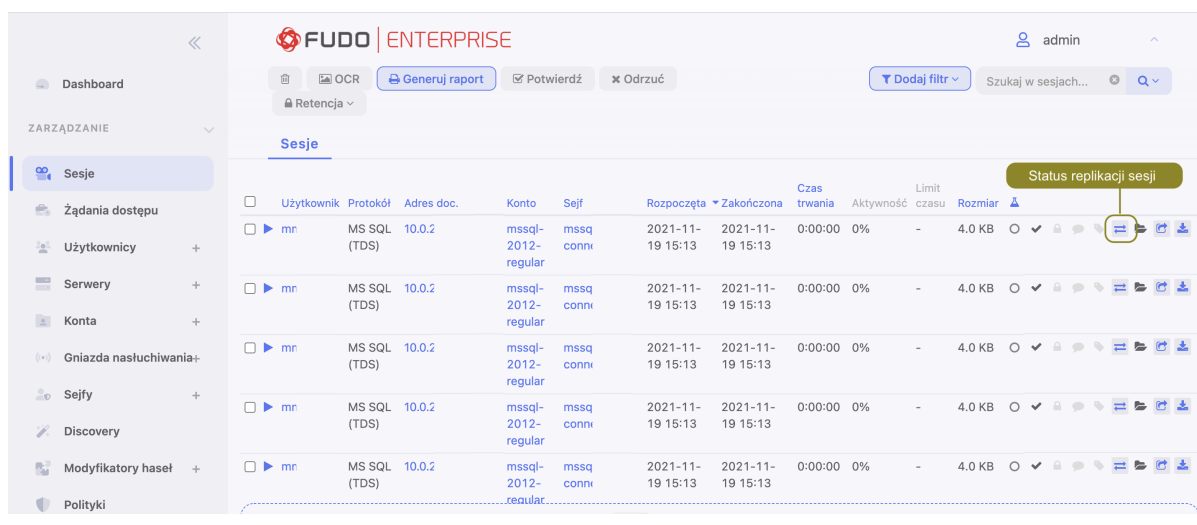
11. W sekcji *Relacje* węzła, na którym został zainicjowany klaster, kliknij przycisk *+ Dodaj*.
12. Wybierz z listy dołączany węzeł.
13. Z listy rozwijalnej, wybierz jakie dane mają podlegać replikacji na wybrany węzeł klastra.
14. Kliknij *Zapisz*.
15. Skopiuj klucz publiczny klastra.
16. Zaloguj się 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 .



	Użytkownik	Protokół	Adres doc.	Konto	Sejf	Rozpoczęta	Zakończona	Czas trwania	Aktywność	Limit czasu	Rozmiar	
<input type="checkbox"/>	mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
<input type="checkbox"/>	mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
<input type="checkbox"/>	mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
<input type="checkbox"/>	mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	
<input type="checkbox"/>	mr	MS SQL (TDS)	10.0.2	mssql-2012-regular	mssql-conn	2021-11-19 15:13	2021-11-19 15:13	0:00:00	0%	-	4.0 KB	

Tematy pokrewne:

- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

22.16.2.2 Edytowanie węzłów klastra

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

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

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

22.16.2.3 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 Enterprise, postępuj zgodnie z poniższą instrukcją.

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

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Edytowanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

22.16.3 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.

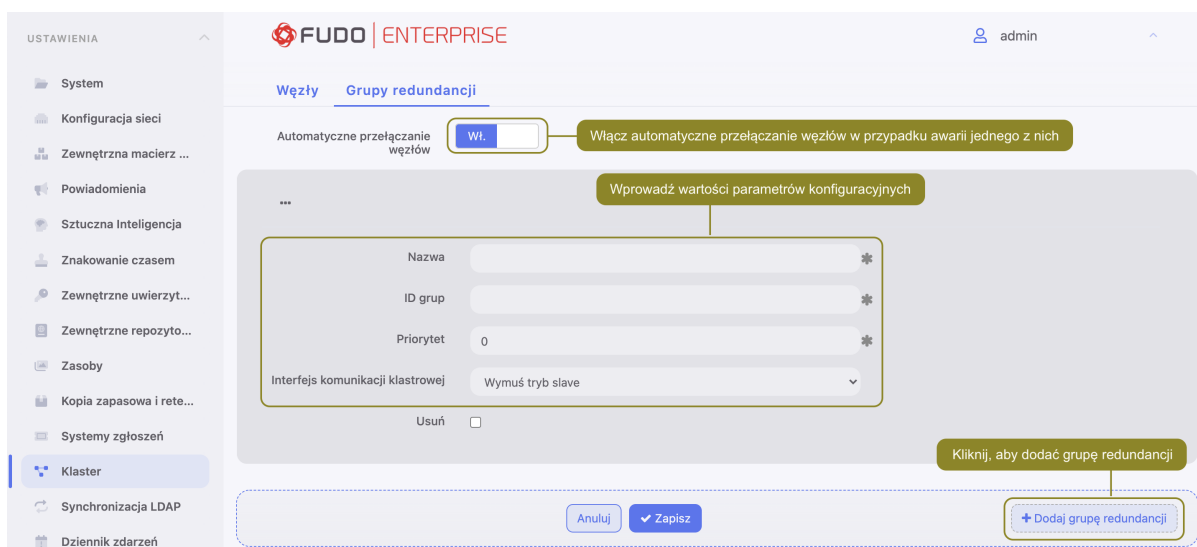
Dodawanie grup redundancji



Aby dodać grupę redundancji, postępuj zgodnie z poniższą instrukcją.

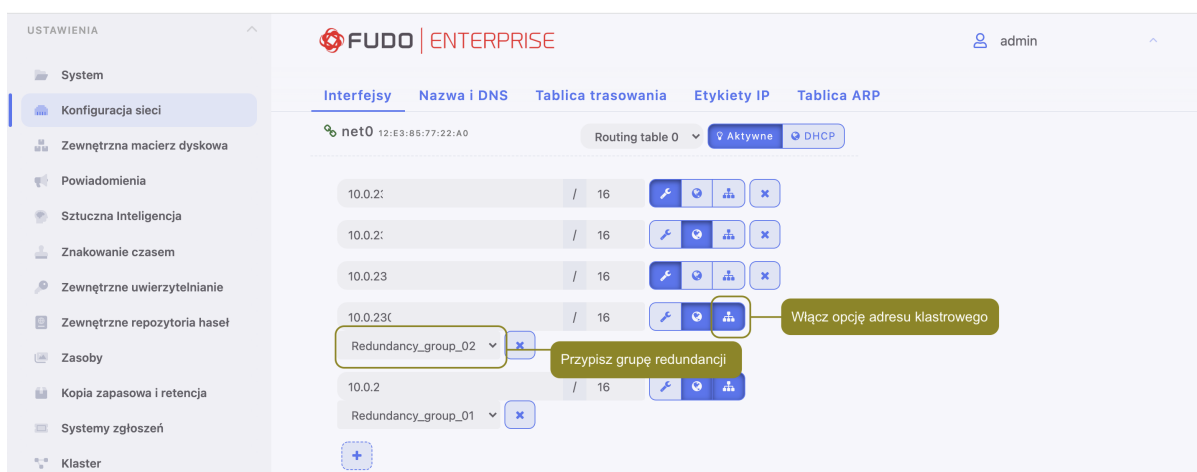
1. Wybierz z lewego menu *Ustawienia > Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Kliknij *+ Dodaj grupę redundancji*.
4. Zdefiniuj parametry grupy.

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 <i>master</i> 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.

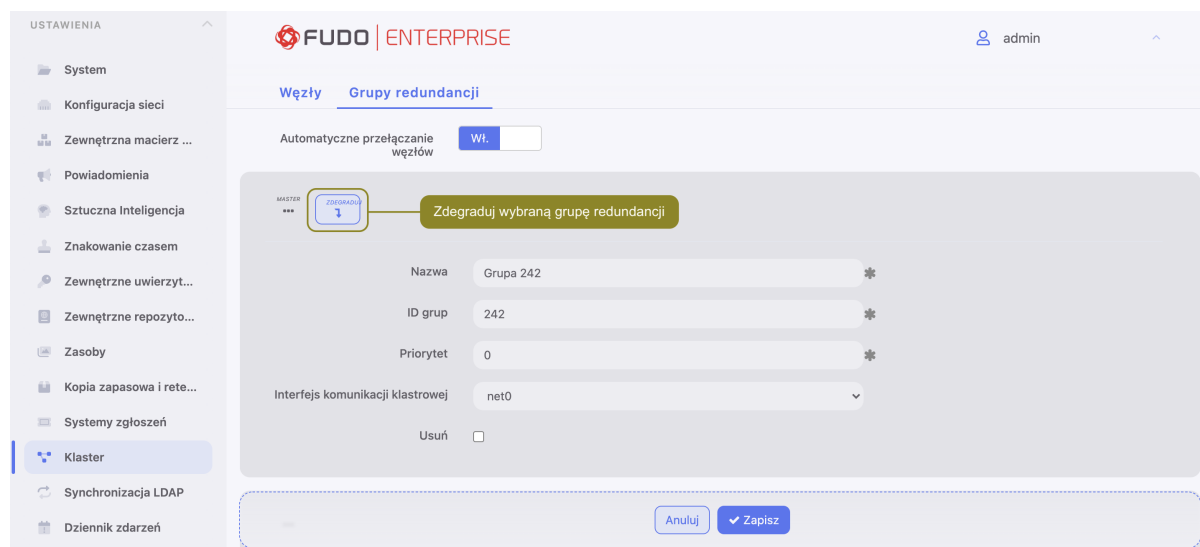
1. Wybierz z lewego menu *Ustawienia > Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Zaznacz opcję *Usuń* przy wybranej grupie redundancji.
4. Kliknij *Zapisz*.

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 oddzielnej 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*

22.17 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*.


The screenshot shows the 'Dziennik zdarzeń' (Event Log) page in the Fudo Enterprise interface. The page has a sidebar on the left with navigation options like 'Produktowność', 'USTAWIENIA', 'System', 'Konfiguracja sieci', etc. The main content area shows a table of events. A yellow callout box highlights the 'Włącz logowanie oraz wysyłanie logów' button. The table has columns: 'Czas', 'Poziom logowania', 'Typ', and 'Komunikat'. The events listed include 'User admin changed safe SSH' and 'Fudo started'.

Czas	Poziom logowania	Typ	Komunikat
2021-11-21 07:24:13	Informacje	admin	User admin changed safe SSH, (user: 2810246167479189505) (safe: 2810246167479189506)
2021-11-21 07:23:33	Informacje	admin	User admin changed safe SSH, (user: 2810246167479189505) (safe: 2810246167479189506)
2021-11-21 07:22:29	Informacje	admin	User admin changed safe SSH, (user: 2810246167479189505) (safe: 2810246167479189506)
2021-11-21 07:21:40	Informacje	admin	User admin changed safe SSH, (user: 2810246167479189505) (safe: 2810246167479189506)
2021-11-21 07:21:22	Informacje	user	User authenticated using password logged in from address: ...
2021-11-21 07:21:05	Informacje	admin	User admin changed safe SSH, (user: 2810246167479189505) (safe: 2810246167479189506)
2021-11-21 07:21:03	Informacje	admin	User admin changed safe SSH, (user: 2810246167479189505) (safe: 2810246167479189506)
2021-11-21 07:20:52	Informacje	admin	User admin changed safe SSH, (user: 2810246167479189505) (safe: 2810246167479189506)
2021-11-21 07:20:27	Informacje	user	User ...
2021-11-21 07:20:14	Informacje	admin	User admin changed safe SSH, (user: 2810246167479189505) (safe: 2810246167479189506)
2021-11-21 05:56:10	Informacje	user	User ...
2021-11-21 05:17:18	Informacje	user	User admin authenticated using password logged in from address: ...
2021-11-21 05:16:55	Ostrzeżenie	system	Fudo started.
2021-11-21 04:25:37	Ostrzeżenie	system	AI postponed training quantitative model "QuantitativeHourDurationModel-ssh". Not enough training data.
2021-11-21 04:25:37	Informacje	system	AI started training quantitative model "QuantitativeHourDurationModel-ssh".

22.17.1 Zewnętrzne serwery syslog

Fudo Enterprise pozwala na przesyłanie rejestrowanych zdarzeń do zewnętrznych serwerów syslog.

Informacja:

- W komunikacji z serwerami syslog, Fudo Enterprise 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
adres: 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 żadaną definicję serwera syslog i zmień żadaną 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*.

22.17.2 Eksportowanie dziennika zdarzeń

Aby wyeksportować zdarzenia zapisane w dzienniku zdarzeń, postępuj 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*

22.18 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*.

```

Tue Mar 13 10:49:41 CET 2018
FUDO, S/N 11111111, firmware 3.4-40163.
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: Mon Mar 12 14:12:31 on ttyv0
*** FUDO configuration utility ***
Logged into FUDO, S/N 11111111, firmware 3.4-40163.
1. Show status
2. Reset network settings
3. Change disk encryption passphrase
0. Exit
Choose an option (0):

```

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*.

```

3. Change disk encryption passphrase
0. Exit
Choose an option (0): 3
Are you sure you want to continue? [y/N] (n): y
Setup new non-empty passphrase for data encryption.
Press <CTRL+C> to cancel and return to main menu.
Enter passphrase:
Enter passphrase:
Note, that the master key encrypted with old keys and/or passphrase may still exist
in a metadata backup file.
0+1 records in
1+0 records out
1024 bytes transferred in 0.001268 secs (807628 bytes/sec)
adminsh: INFO: FSI0468 A passphrase used to decrypt disks was changed.
1. Show status
2. Reset network settings
3. Change disk encryption passphrase
0. Exit
Choose an option (0):

```

6. Uruchom ponownie system, aby zastosować zmiany.

Tematy pokrewne:

- *Aktualizacja systemu*
- *Kopia zapasowa systemu*

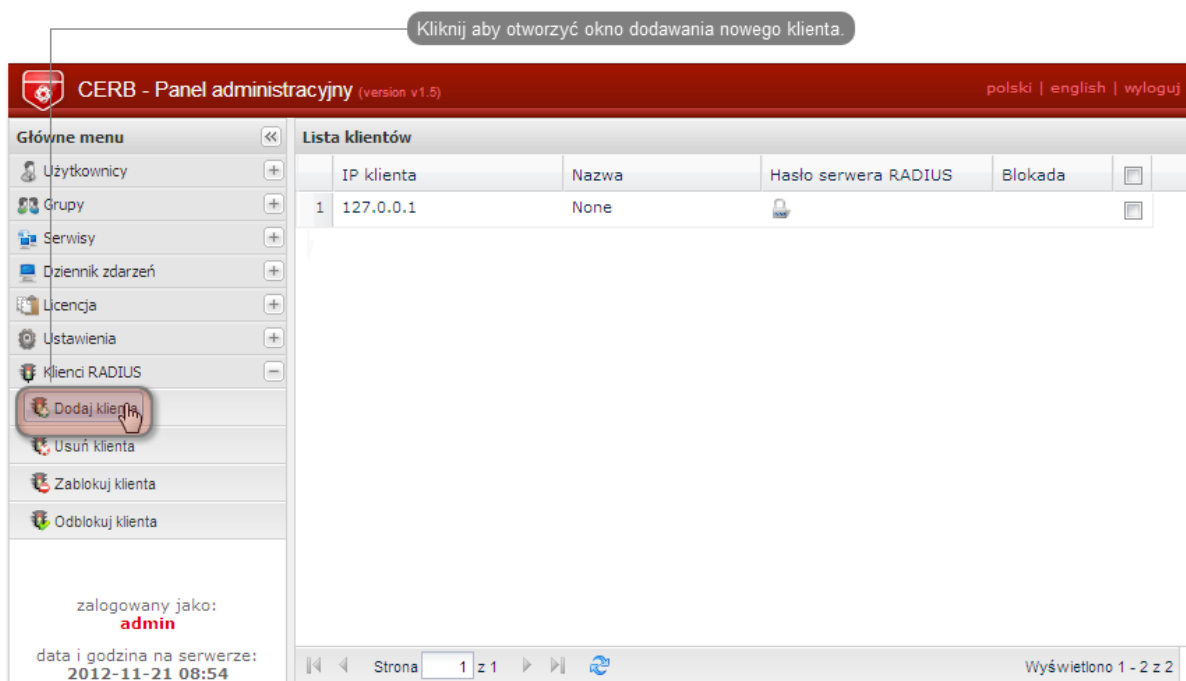
22.19 Integracja z serwerem CERB

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

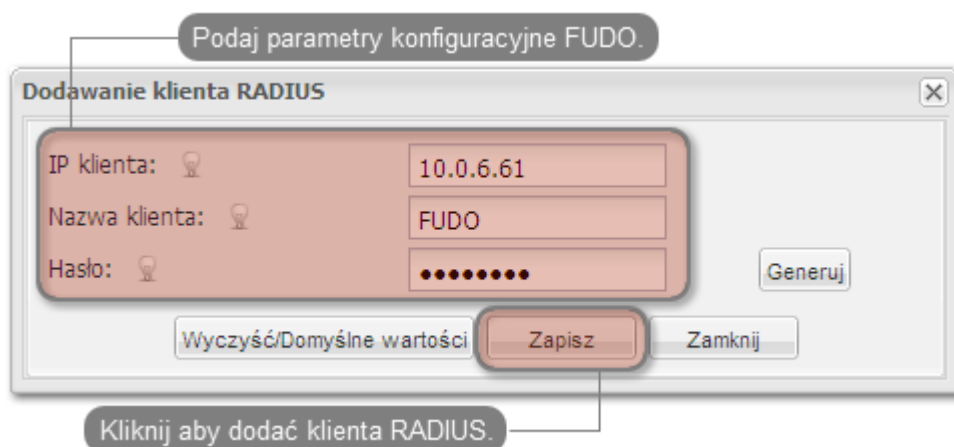
Konfiguracja serwera CERB

1. Dodanie klienta RADIUS.

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



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

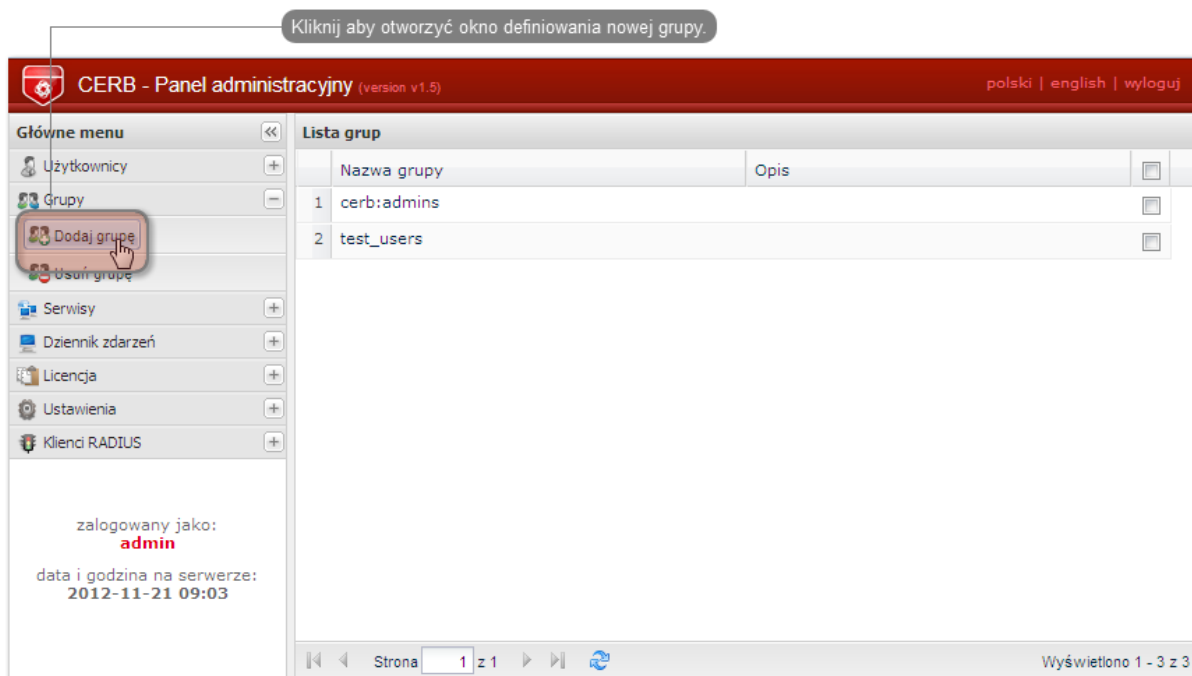


Informacja: Hasło będzie wymagane do skonfigurowania zewnętrznego serwera uwierzytelniania.

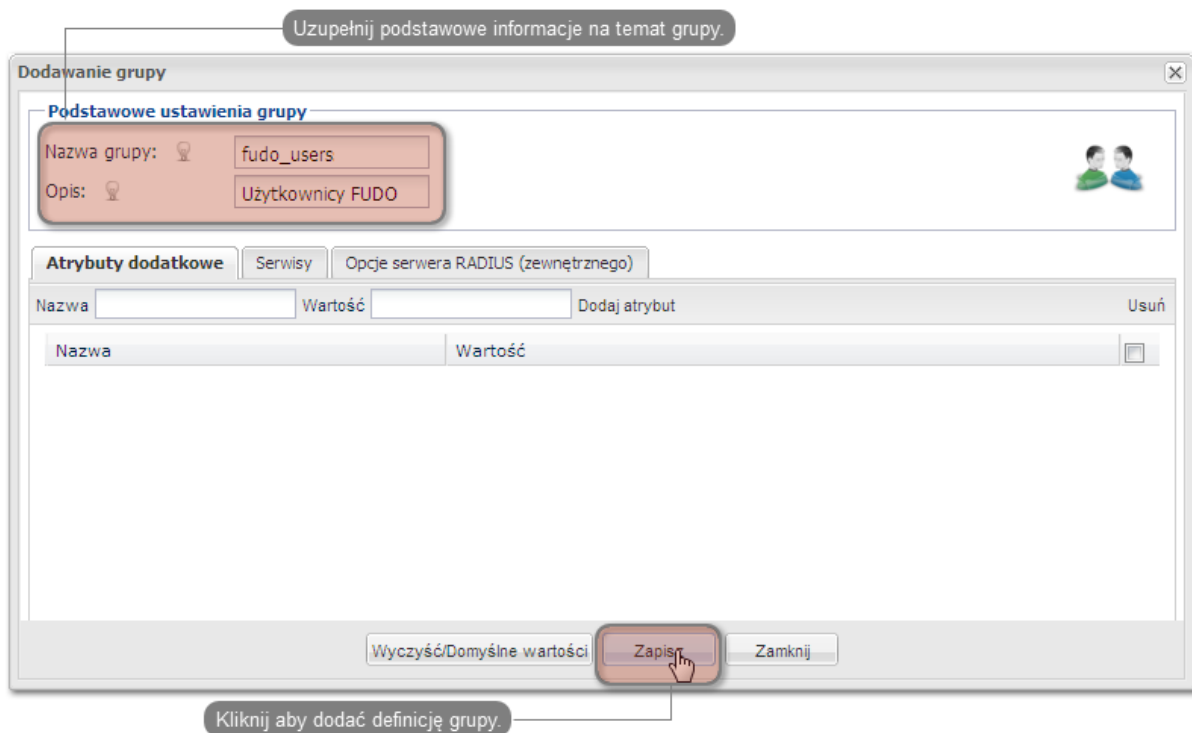
nia w panelu administracyjnym Fudo Enterprise.

2. Dodanie grupy użytkowników.

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

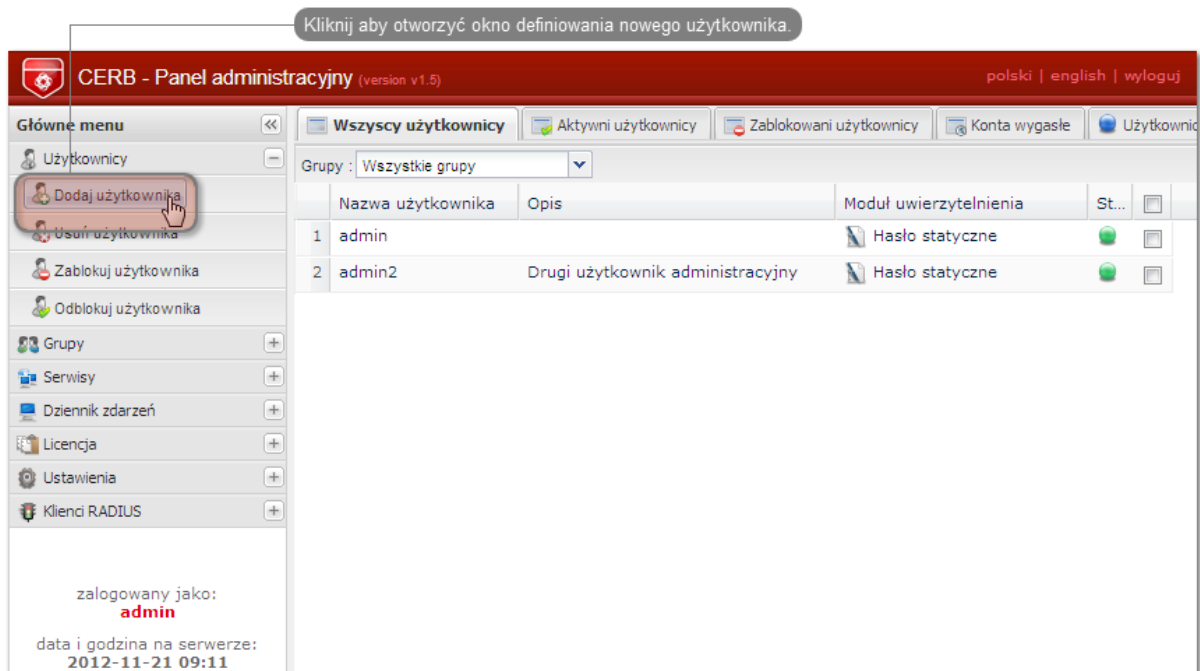


- Podaj nazwę grupy (*fudo_users*) i kliknij *Zapisz*.

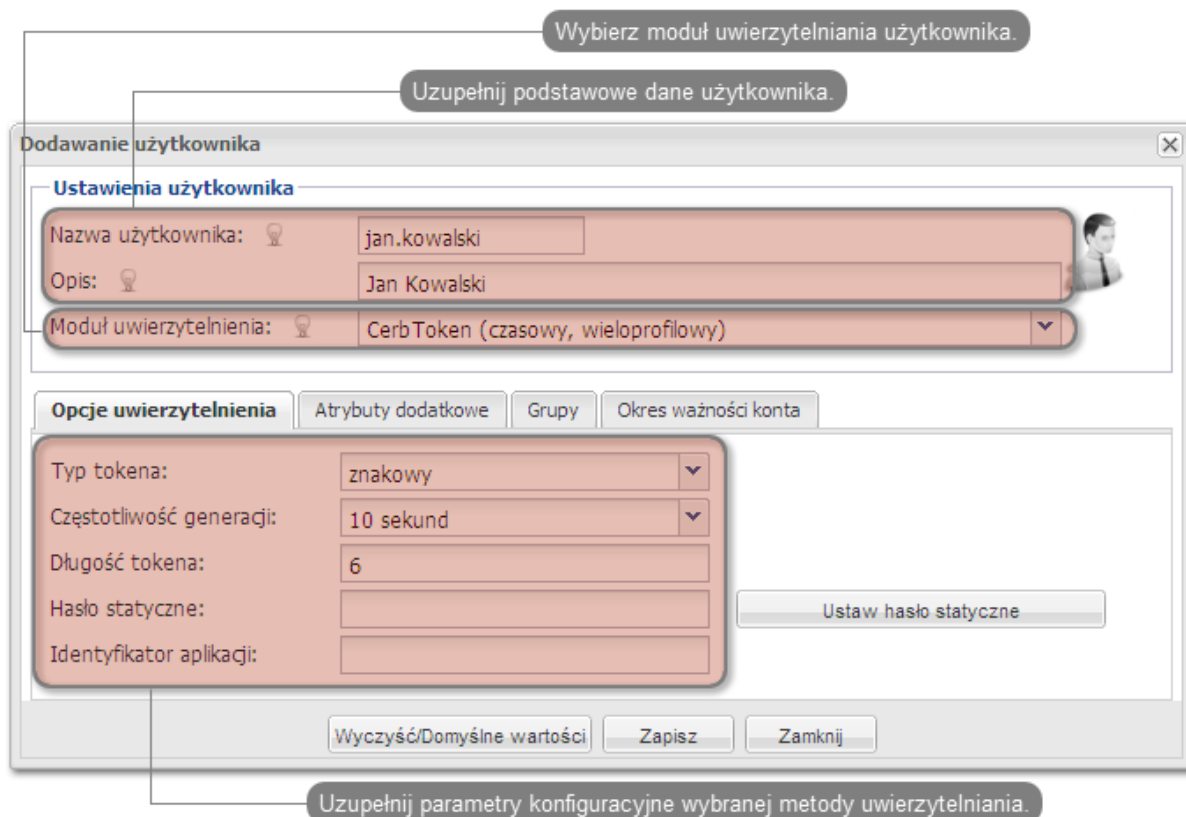


3. Dodanie użytkownika.

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



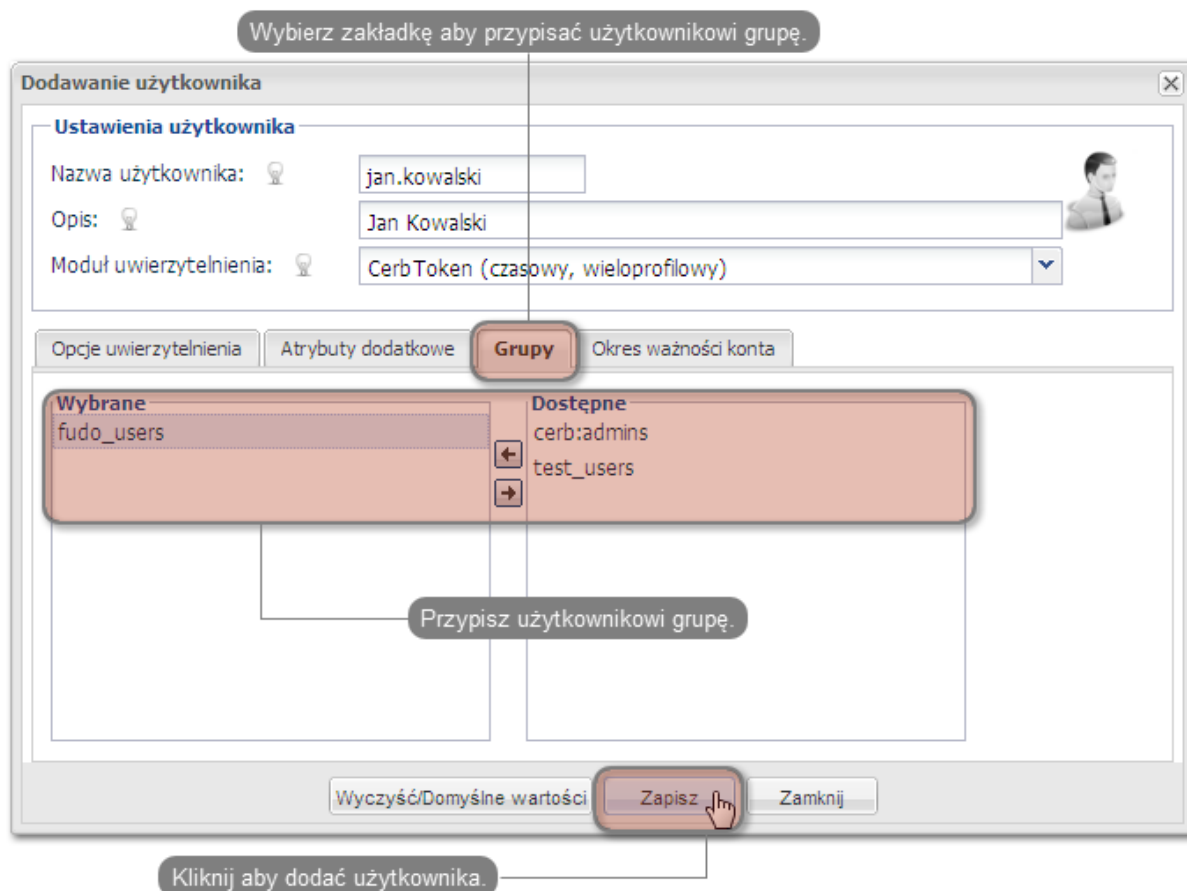
- Podaj nazwę użytkownika, opis oraz wybierz stosowny moduł uwierzytelniania (więcej informacji na temat modułów uwierzytelniania znajdziesz w dokumentacji serwera CERB).



Informacja: Nazwa użytkownika wykorzystywana jest w procesie uwierzytelniania użytkownika.

ków łączących się z Fudo Enterprise.

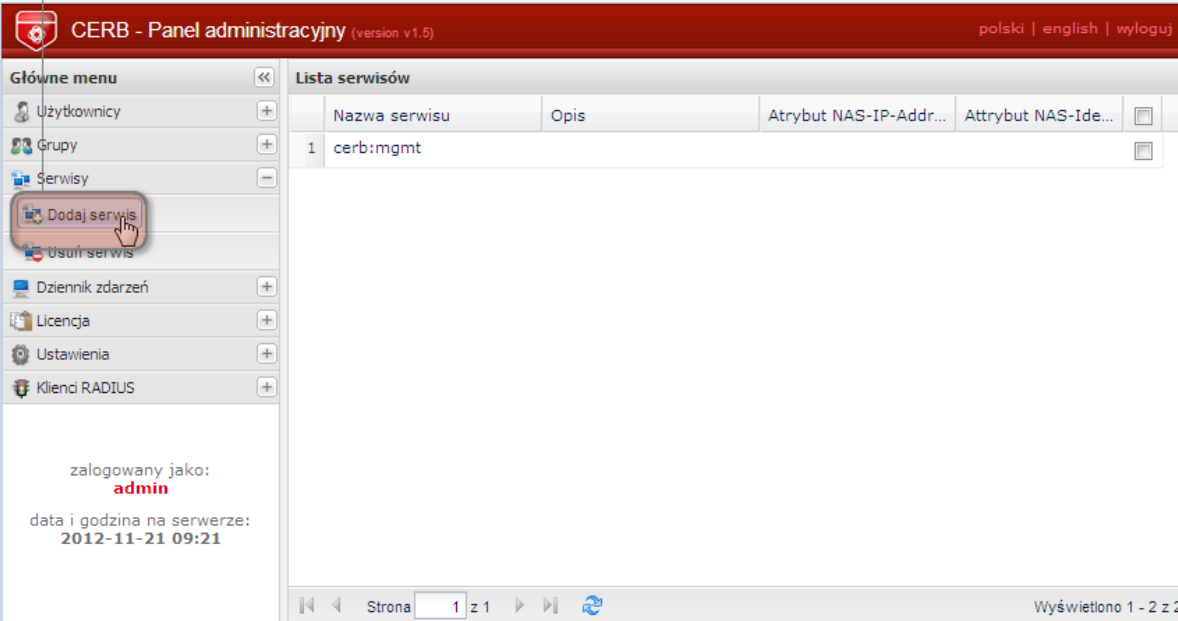
- Przypisz do użytkownika wcześniej dodaną grupę `fudo_users` i kliknij *Zapisz*.



4. Skonfigurowanie serwisu.

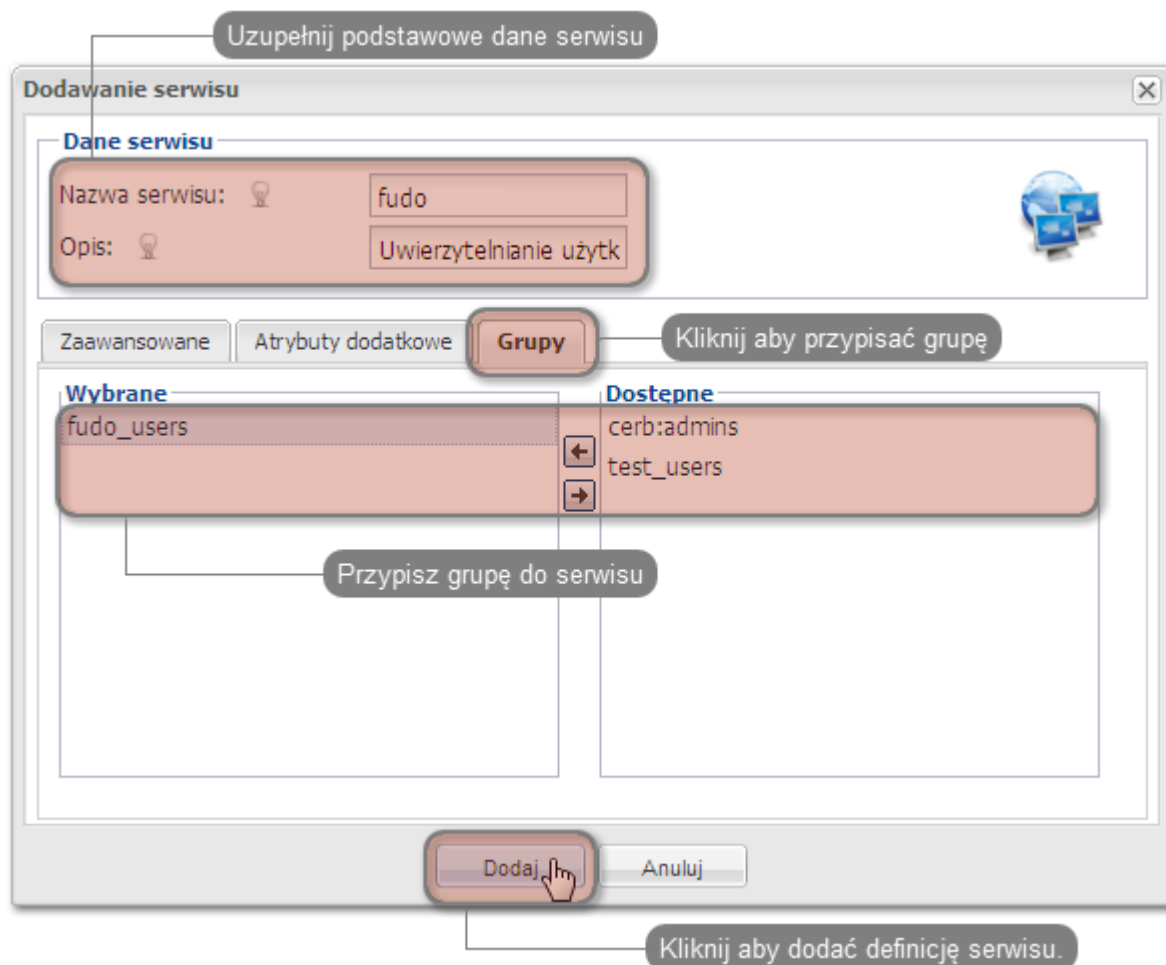
- Wybierz z lewego menu *Serwisy > Dodaj serwis*, aby otworzyć okno definiowania nowego serwisu.

Kliknij aby dodać okno definiowania nowego serwisu.



The screenshot shows the CERB administrative interface. The top header includes the CERB logo, the text 'CERB - Panel administracyjny (version v1.9)', and language options 'polski | english | wyloguj'. The left sidebar contains a 'Główne menu' with items: 'Użytkownicy', 'Grupy', 'Serwisy', 'Dodaj serwis', 'Usuń serwis', 'Dziennik zdarzeń', 'Licencja', 'Ustawienia', and 'Klienci RADIUS'. The 'Dodaj serwis' button is highlighted with a red box and a mouse cursor. The main content area is titled 'Lista serwisów' and contains a table with one entry: '1 cerb:mgmt'. The table has columns for 'Nazwa serwisu', 'Opis', 'Atrybut NAS-IP-Addr...', and 'Atrybut NAS-Ide...'. At the bottom, there is a pagination bar showing 'Strona 1 z 1' and 'Wyświetlono 1 - 2 z 2'. A status bar at the bottom left indicates the user is logged in as 'admin' and the server date/time is '2012-11-21 09:21'.

- 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 Enterprise

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 zidentyfikowana 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.

The screenshot shows a configuration form for 'Zewnętrzne uwierzytelnianie' (External authentication). The form includes the following fields and callouts:

- Typ:** Set to 'Cerb'. Callout: 'Wybierz Typ 'Cerb' i uzupełnij parametry serwera'.
- Adres hosta:** Set to '10.0.0.12'. Callout: 'Określ adres IP i numer portu'.
- Port:** Set to '1812'.
- Adres źródłowy:** Set to 'Dowolny'. Callout: 'Zdefiniuj adres IP pakietów wychodzących'.
- Serwis:** Set to 'fudo'. Callout: 'Wprowadź nazwę serwisu skonfigurowanego w systemie CERB na potrzeby uwierzytlenianie użytkowników FUDO'.
- Sekret:** A password field with asterisks.
- Powtórz sekret:** A second password field with asterisks.
- Callout at the bottom: 'Wprowadź hasło uwierzytelnienia klienta RADIUS'.

- 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.

Uwierzytelnienie

The screenshot shows the 'Uwierzytelnienie' configuration form with the following settings:

- Typ:** Dropdown menu set to 'Zewnętrzne uwierzytelnienie'.
- Zewnętrzne źródło uwierzytelnienia:** Dropdown menu set to 'Cerb 10.0.0.12 serwis:fudo'.
- Usuń:** An unchecked checkbox.

- Kliknij *Zapisz*.

Tematy pokrewne:

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

22.20 Czynności serwisowe

Poniższy rozdział zawiera opisy czynności serwisowych.

Fudo Enterprise 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.

22.20.1 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 Enterprise.

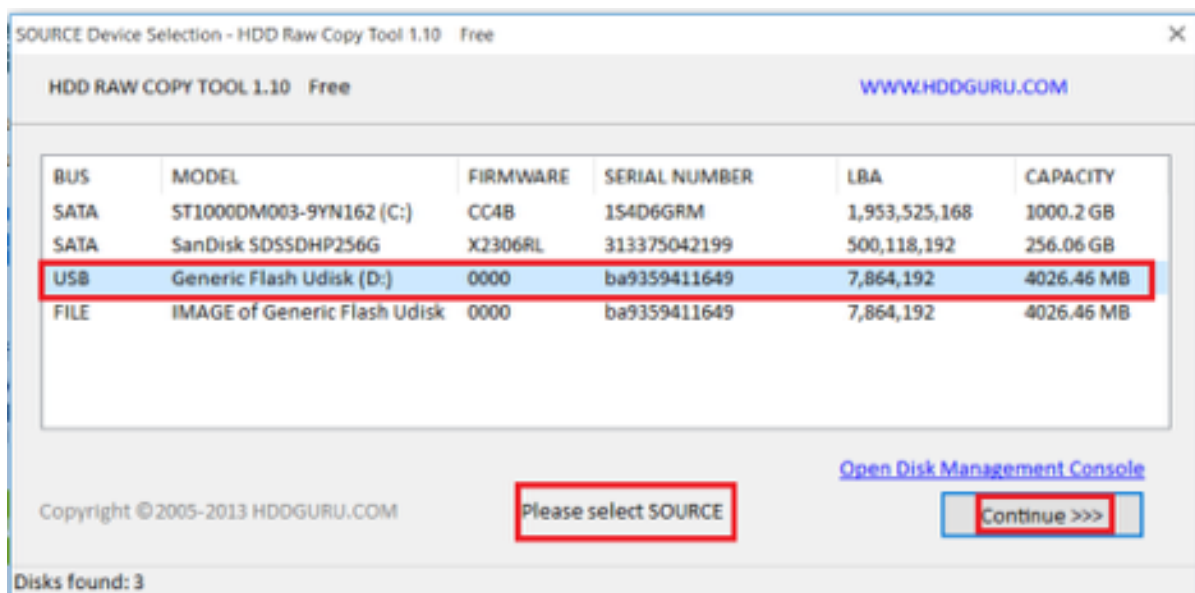
Microsoft Windows

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.

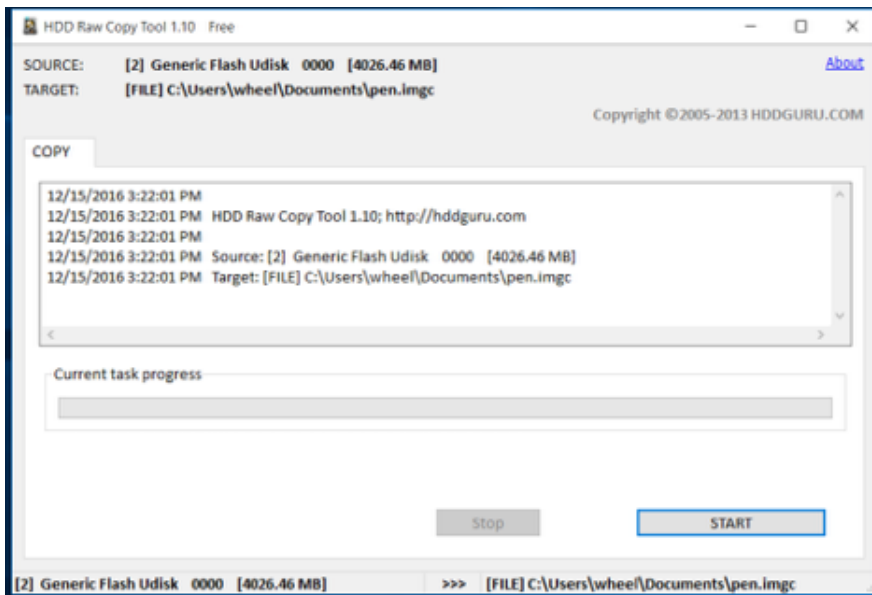
1. Pobierz i zainstaluj program *HDD Raw Copy Tool*.

<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*.

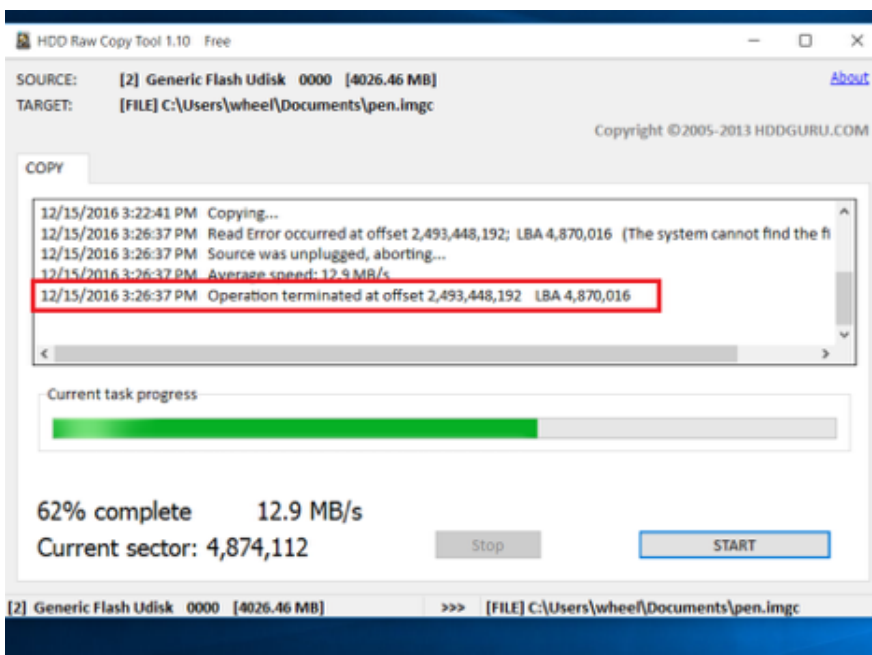


4. Kliknij dwukrotnie *FILE*, wskaż plik docelowy, w którym zapisany zostanie obraz dysku i kliknij *Continue*.
5. Kliknij *START*, aby rozpocząć procedurę kopiowania.

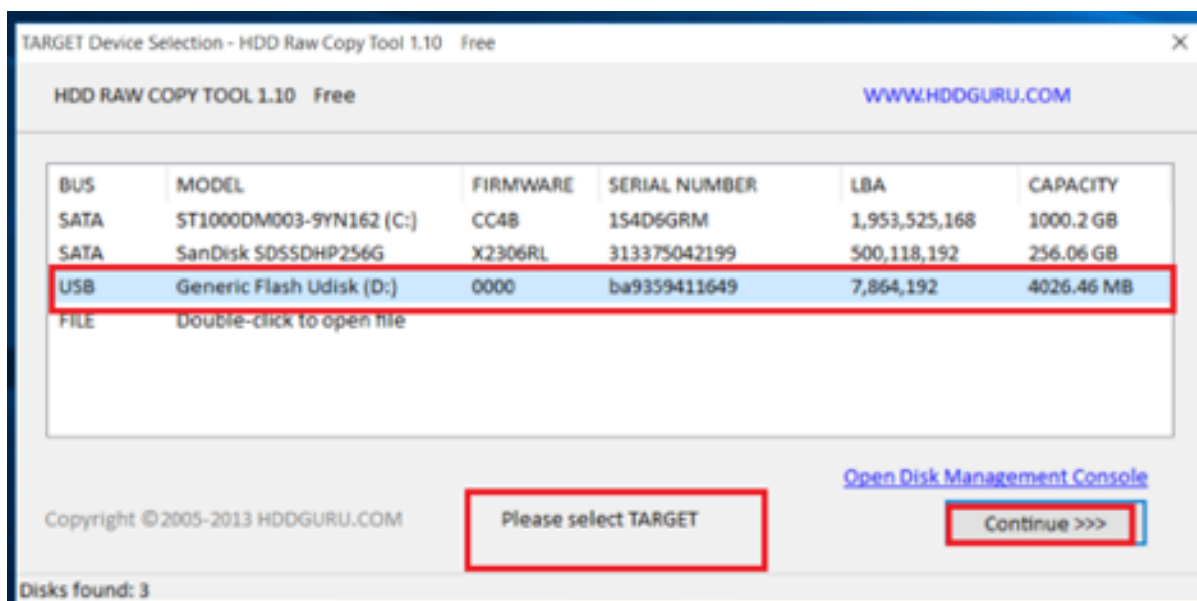


6. Z chwilą wystąpienia komunikatu

Operation terminated at offset..., zamknij okno i odłącz napęd USB.

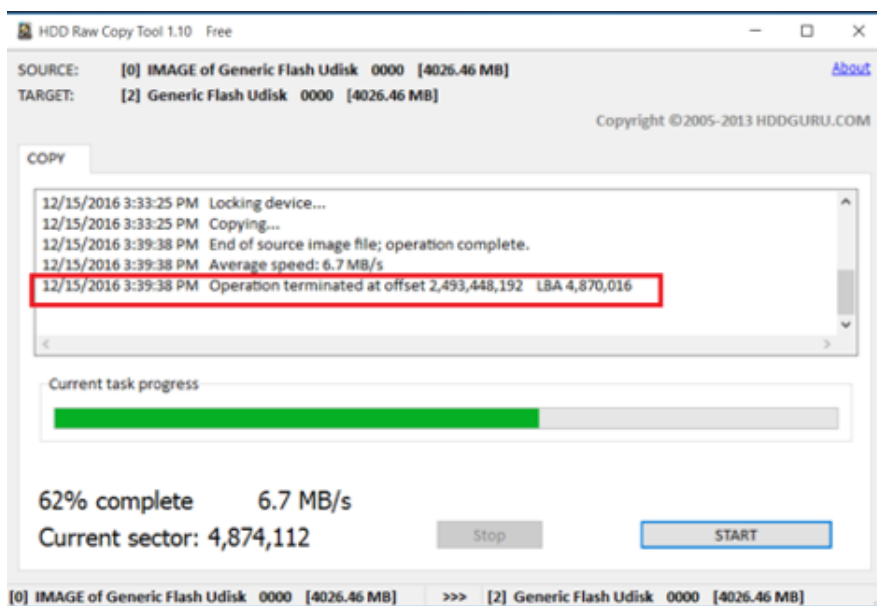


7. Podłącz nośnik pamięci flash i włącz program *HDD Raw Copy Tool*.
8. Na ekranie wyboru napędu źródłowego, zaznacz *FILE* i wskaż plik z obrazem kluczy szyfrujących.
9. Wybierz podłączony nośnik pamięci jako urządzenie docelowe i kliknij *Continue*.



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](#)

22.20.2 Monitorowanie stanu systemu

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

Monitorowanie aktywnych sesji

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

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

Monitorowanie przepustowości łącza sieciowego

1. Zaloguj się do panelu administracyjnego Fudo Enterprise.

2. Wybierz z lewego menu *Zarządzanie > Dashboard*.
3. Sprawdź bieżącą aktywność interfejsów sieciowych.

Informacja: Fudo Enterprise 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 Enterprise uniemożliwi nawiązywanie nowych połączeń z chwilą, gdy zajętość przestrzeni dyskowej osiągnie wartość 90%.

1. Zaloguj się do panelu administracyjnego Fudo Enterprise.
2. Wybierz z lewego menu *Zarządzanie > Dashboard*.
3. Sprawdź zajętość przestrzeni dyskowej, przejdź 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*

22.20.3 Kontrola Stanu

Fudo Enterprise 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.

22.20.3.1 API kontrola stanu

Funkcja API kontrola stanu jest dostępna w sekcji *Serwisowanie i nadzór* zakładki *Ustawienia > System*.

Dostarcza ona krótką informację o kontroli stanu systemu Fudo Enterprise. 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 Enterprise działa poprawnie
- **error**: jeśli Fudo Enterprise 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
```

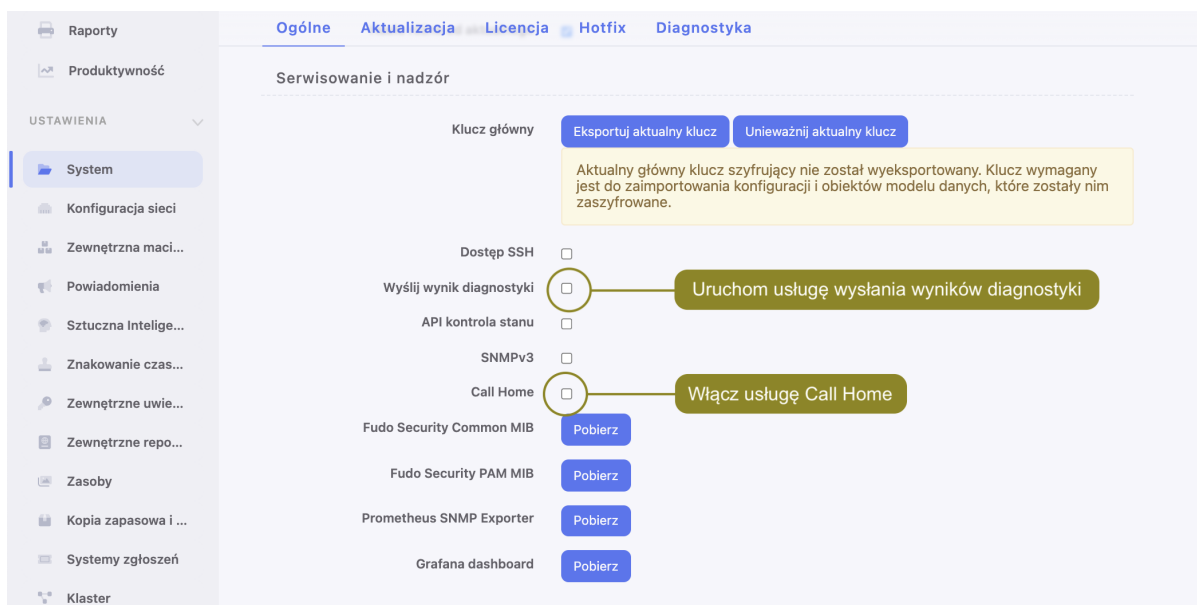
Ostrzeżenie: Opcja *API kontrola stanu* nie wymaga uwierzytelnienia. To oznacza, że każdy kto ma dostęp do TCP jest uprawniony do odczytu wyników stanu kontroli.

22.20.4 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 Enterprise.

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 Enterprise, 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 Enterprise. Sprawdź na stronie [Informacja ze stopki dolnej](#), gdzie możesz podejrzeć swój FUID.
- Urządzenie Fudo nawiąże wychodzące połączenia SSH z `home.fudosecurity.com`.

22.20.5 Wymiana dysku macierzy

W domyślnej konfiguracji, macierz dyskowa Fudo Enterprise składa się z 12 dysków twardech 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 twardego i wyjmij dysk z kieszeni.
4. Włóż nowy dysk twardego i wkręć śruby mocujące.
5. Włóż kieszeń z dyskiem twardego 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.

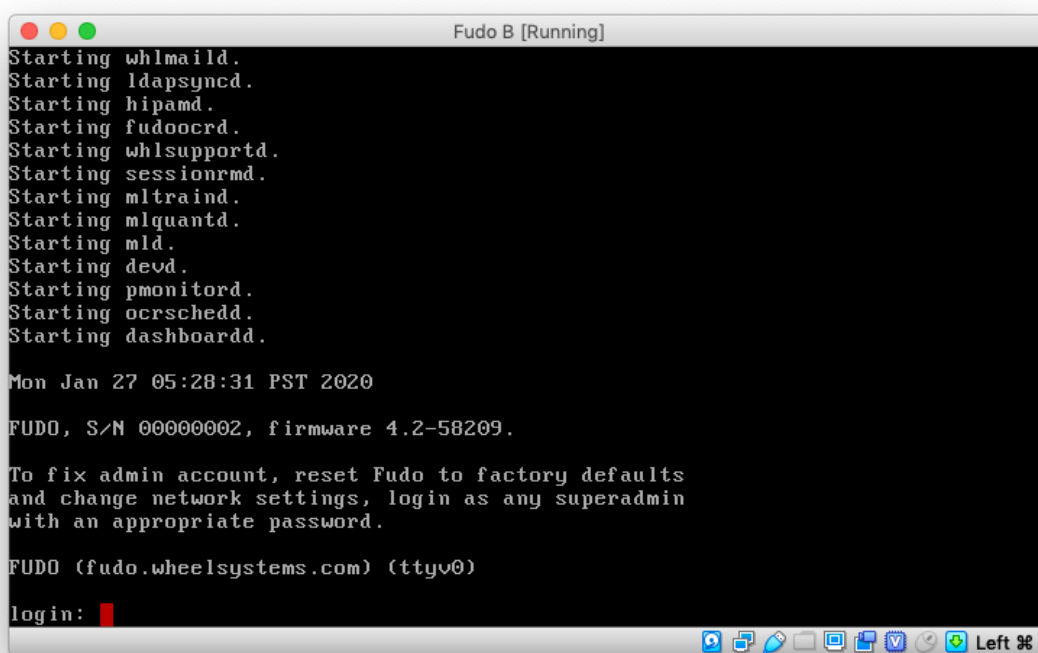
Tematy pokrewne:

- *Urządzenie*
- *Często zadawane pytania*

22.20.6 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**.



```
Fudo B [Running]
Starting whlmaild.
Starting ldapsyncd.
Starting hipamd.
Starting fudoocrd.
Starting whlsupportd.
Starting sessionrmd.
Starting mltraind.
Starting mlquantd.
Starting mld.
Starting devd.
Starting pmonitord.
Starting ocrschedd.
Starting dashboardd.

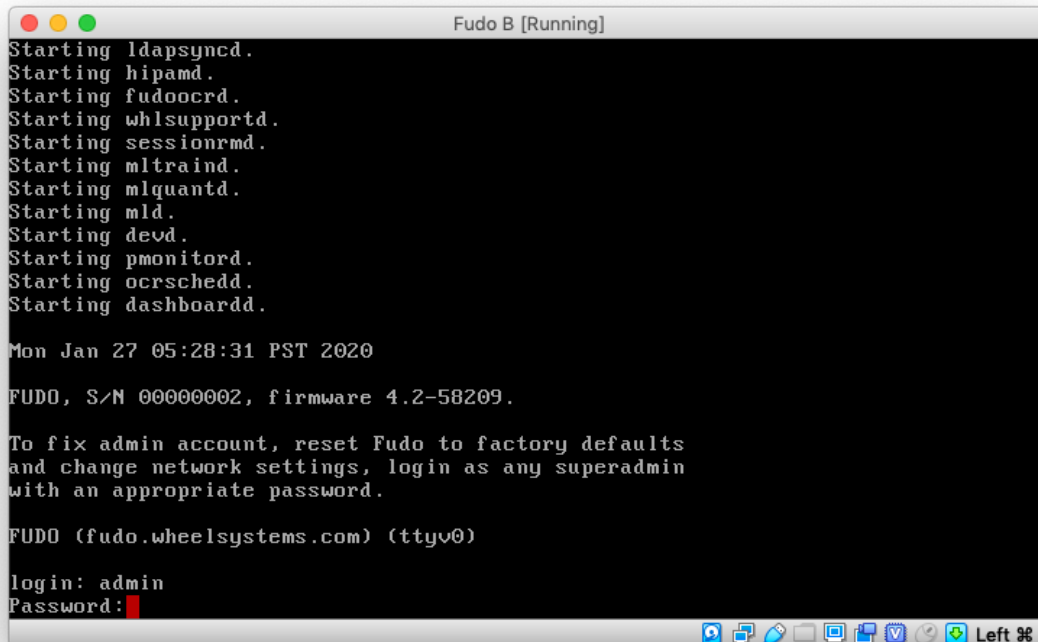
Mon Jan 27 05:28:31 PST 2020

FUDO, S/N 00000002, firmware 4.2-58209.

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

FUDO (fudo.wheelsystems.com) (ttyv0)
login: █
```

3. Wprowadź hasło i naciśnij klawisz Enter.



```
Fudo B [Running]
Starting ldapsyncd.
Starting hipamd.
Starting fudoocrd.
Starting whlsupportd.
Starting sessionrmd.
Starting mltraind.
Starting mlquantd.
Starting mld.
Starting devd.
Starting pmonitord.
Starting ocrschedd.
Starting dashboardd.

Mon Jan 27 05:28:31 PST 2020

FUDO, S/N 00000002, firmware 4.2-58209.

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

FUDO (fudo.wheelsystems.com) (ttyv0)
login: admin
Password: █
```

4. Wprowadź 9 i naciśnij klawisz Enter.



```
Mon Jan 27 05:28:31 PST 2020
FUDO, S/N 00000002, firmware 4.2-58209.

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

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Thu Dec 12 02:22:56 on ttyv0

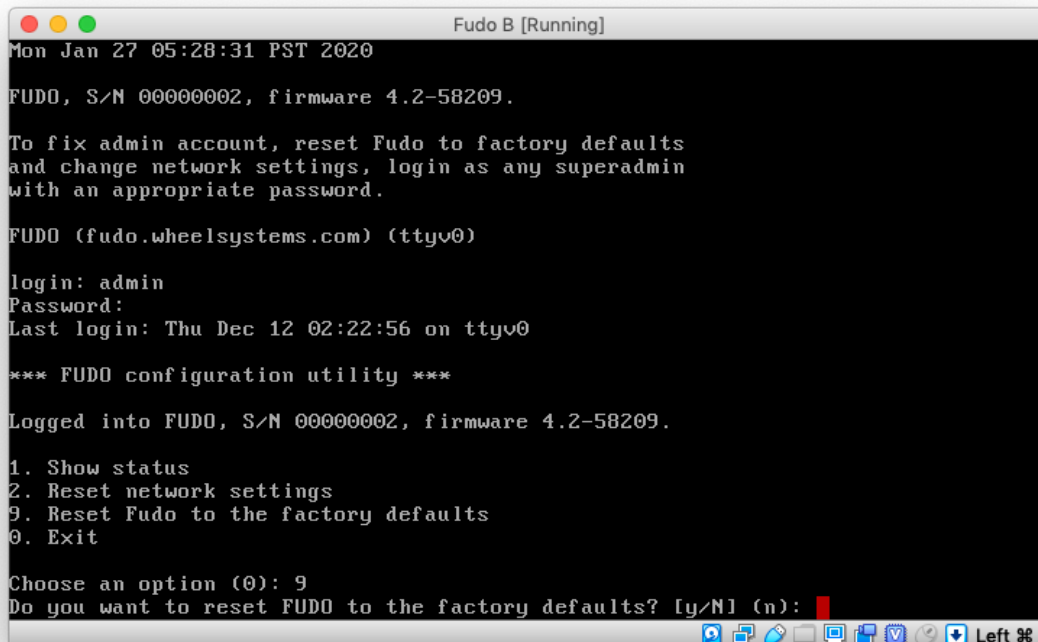
*** FUDO configuration utility ***

Logged into FUDO, S/N 00000002, firmware 4.2-58209.

1. Show status
2. Reset network settings
9. Reset Fudo to the factory defaults
0. Exit

Choose an option (0): █
```

5. Wprowadź y i naciśnij klawisz **Enter**, aby potwierdzić wybór.



```
Mon Jan 27 05:28:31 PST 2020
FUDO, S/N 00000002, firmware 4.2-58209.

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

FUDO (fudo.wheelsystems.com) (ttyv0)

login: admin
Password:
Last login: Thu Dec 12 02:22:56 on ttyv0

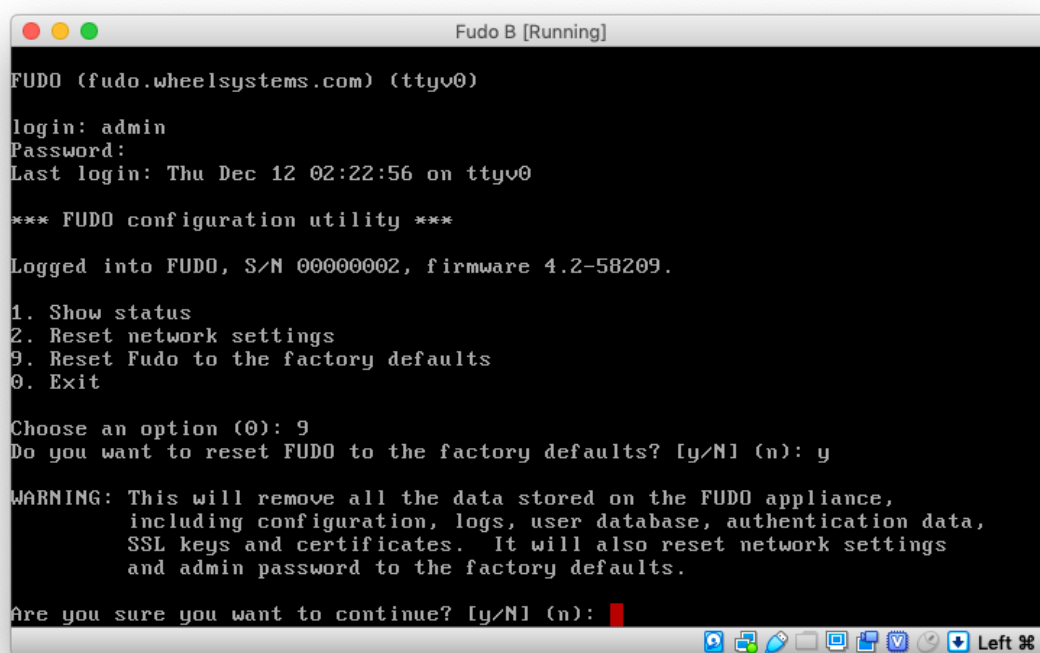
*** FUDO configuration utility ***

Logged into FUDO, S/N 00000002, firmware 4.2-58209.

1. Show status
2. Reset network settings
9. Reset Fudo to the factory defaults
0. Exit

Choose an option (0): 9
Do you want to reset FUDO to the factory defaults? [y/N] (n): █
```

6. Wprowadź y i naciśnij klawisz **Enter**, aby wykonać procedurę przywrócenia ustawień fabrycznych.



```
Fudo B [Running]
FUDO (fudo.wheelsystems.com) (ttyv0)
login: admin
Password:
Last login: Thu Dec 12 02:22:56 on ttyv0

*** FUDO configuration utility ***

Logged into FUDO, S/N 00000002, firmware 4.2-58209.

1. Show status
2. Reset network settings
9. Reset Fudo to the factory defaults
0. Exit

Choose an option (0): 9
Do you want to reset FUDO to the factory defaults? [y/N] (n): y

WARNING: This will remove all the data stored on the FUDO appliance,
including configuration, logs, user database, authentication data,
SSL keys and certificates. It will also reset network settings
and admin password to the factory defaults.

Are you sure you want to continue? [y/N] (n): █
```

Informacja: W przypadku zdawania urządzenia demonstracyjnego, należy również wyczyścić zawartość nośnika pamięci, na którym zainicjowany został klucz szyfrujący.

Tematy pokrewne:

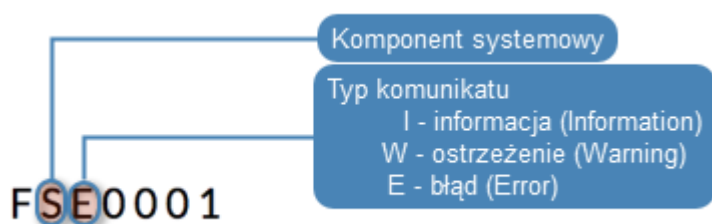
- *Konfiguracja ustawień sieciowych*
- *Czynności serwisowe*

Tematy pokrewne:

- *Model danych*
- *RDP*
- *Zarządzanie serwerami*
- *Konta*

23.2 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 ($\{\text{diskserial}\}$) $\{\text{disk}\}$.
FSI0025	Cluster node $\{\text{name}\}$ ($\{\text{address}\}$) host key set to $\{\text{hostkey}\}$.
FSE0026	Cluster communication error.
FSI0027	Cluster node $\{\text{name}\}$ initialized.
FSE0028	Unable to join node to cluster.
FSI0029	Resumed data synchronization.
FSI0030	Node $\{\text{node}\}$ initially synchronized.
FSE0031	Timestamping service communication error.
FSE0032	Unable to timestamp session.
FSE0033	Unknown timestamping service provider.
FSI0034	Session $\{\text{SESSION}\}$ was timestamped.
FSI0035	Email $\{\text{mailname}\}$ sent to $\{\text{admin_email}\}$.
FSW0036	Unable to send email $\{\text{mailname}\}$ to $\{\text{admin_email}\}$ through $\{\text{account}\}$ server.
FSW0037	Output from SMTP client: $\{\text{out}\}$.
FSI0038	Saved email $\{\text{mailname}\}$ sent to $\{\text{admin_email}\}$.
FSI0039	System image version $\{\text{FULLNEW}\}$ 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 between 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 password or 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 added 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-existent 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.
FUW0373	Session has been terminated due to exceeding the time window defined in a time policy for the user %s and the safe %s.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
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.
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.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
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 method %s from user %s.
FAI0427	User %s changed authentication method %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 account %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.
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.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
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.
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.
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.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
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): initial 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	Rollback to \${oldversion} failed.
FSW0523	Upgrade to \${oldversion} failed.
FSW0524	Rollback 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.
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.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Treść komunikatu
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 doesn'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.

23.3 Informacja ze stopki dolnej

Dolna stopka menu zawiera informacje systemowe obecnej instancji Fudo Enterprise.

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 Enterprise.
4. **Wersja** - Obecna wersja systemu.

The screenshot displays the Fudo Enterprise 5.4 dashboard. On the left is a navigation sidebar with categories like 'ZARZĄDZANIE' and 'Raporty'. The main area features several widgets: a top row with four summary cards (ALERTY KONT, BIEŻĄCE SESJE, PODEJRZANE SESJE, AKTYWNI UŻYTKOWNICY) and a 'LICENCJA' card; a 'WĘZŁ' widget showing node 81888727 with resource usage (Dyski, Sieci, Magazyn, Pamięć, Procesor); a 'NOWE SESJE' line chart; and a 'LOGI' table at the bottom. The log table has columns for DATA, WĘZŁ, TYP, and KOMUNIKAT. A search bar at the bottom right filters logs by date (5 days), node ID (81888727), and FUID (5-74030).

DATA	WĘZŁ	TYP	KOMUNIKAT
23 Nov 2021 05:41:55	81888727	user	User admin authentic...
23 Nov 2021 04:25:...	81888727	system	AI postponed training...

Fudo Officer 1.0 jest aplikacją mobilną, pozwalającą administratorom Fudo Enterprise zarządzać żądaniami użytkowników o dostęp do serwera. Żądania mogą być akceptowane bądź odrzucane przez administratorów w aplikacji Fudo Officer albo w panelu admina Fudo Enterprise 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: angielskim, polskim, rosyjskim oraz ukraińskim. 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.

24.1 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 Enterprise.

3.2. Przejdź do *Zarządzanie > Użytkownicy*. Wybierz użytkownika, dla którego chcesz założyć profil.

3.3. Edytuj wybranego użytkownika i przejdź do zakładki *Więcej*. W polu *Fudo Officer* 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 Enterprise.

3.5. Ustaw nazwę profilu i kliknij *Utwórz profil*. Nazwa profilu jest edytowalna.

3.6. Wróć do panelu Admin Fudo Enterprise i kliknij *OK* w okienku z QR kodem. Sekcja *Fudo Officer* powinna pokazywać *Platformę* powiązanego urządzenia oraz *Push ID*.

Fudo Officer

Platforma	ios
Push ID	dbzOq5nOA0TVo3u3mlecvv:APA91bH3DGAxz4blkhHe65BzANyul6g_gBf3wWeZjGf
<input type="button" value="Usuń urządzenie"/>	

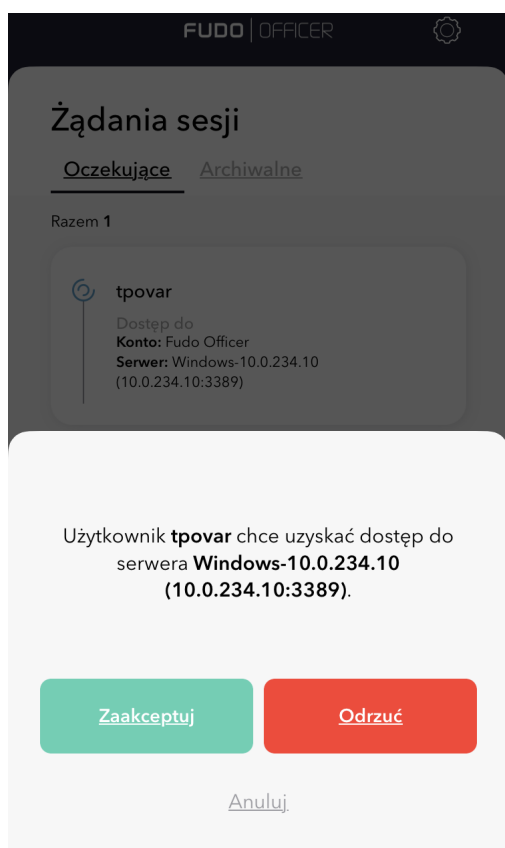
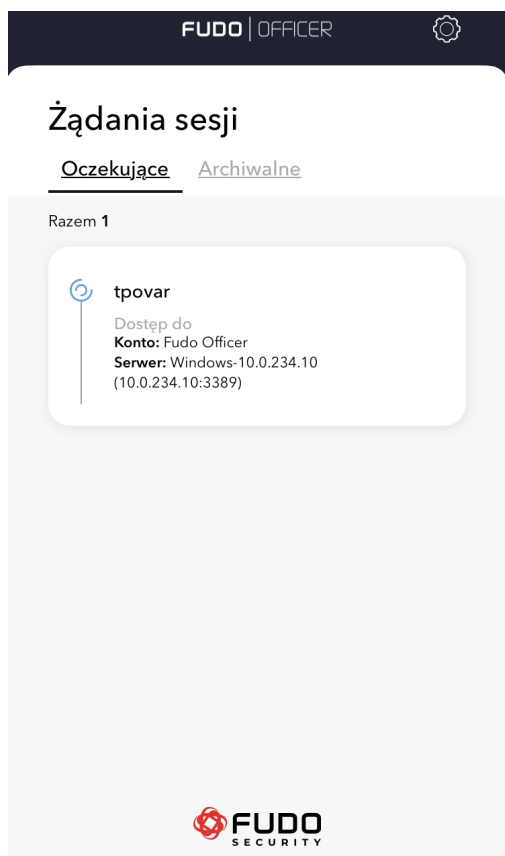
3.7. Kliknij *Zapisz*.

Teraz możesz zarządzać zadaniami użytkowników z poziomu stworzonego profilu.

Informacja: Profil jest unikalny dla jednego użytkownika jednej instancji Fudo Enterprise.

24.2 Zarządzanie zadaniami 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 żądanie, albo przewin w lewo, żeby go odrzucić.

The screenshot shows the 'FUDO OFFICER' interface. At the top, there is a dark header with the logo and a gear icon. Below the header, the title 'Żądania sesji' is displayed. Two tabs are visible: 'Oczekujące' (selected) and 'Archiwalne'. A summary bar indicates 'Razem 1'. A single session request card is shown with a green checkmark icon on the left. The card contains the following information: a user icon, the name 'tpovar', 'Dostęp do', 'Konto: Fudo Officer', and 'Serwer: Windows-10.0.234.10 (10.0.234.10:3389)'. The FUDO SECURITY logo is at the bottom.

The screenshot shows the 'FUDO OFFICER' interface. At the top, there is a dark header with the logo and a gear icon. Below the header, the title 'Żądania sesji' is displayed. Two tabs are visible: 'Oczekujące' and 'Archiwalne' (selected). A summary bar indicates 'Razem 1'. A single session request card is shown with a red 'X' icon on the right. The card contains the following information: a user icon, the name 'tpovar', 'Dostęp do', 'Konto: Fudo Officer', and 'Serwer: Windows-10.0.234.10 (10.0.234.10:3389)'. The FUDO SECURITY logo is at the bottom.

Przeprocesowane żądania (zaakceptowane oraz odrzucone) są dostępne w zakładce *Archiwalne*. Można je sortować według Daty, Nazwy serwera albo Użytkownika.

24.3 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 Enterprise.
2. Przejdź do *Zarządzanie > Użytkownicy*. Wybierz użytkownika, dla którego chcesz założyć profil.
3. Edytuj wybranego użytkownika i przejdź do zakładki *Więcej*. W polu *Fudo Officer* 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 Enterprise.
5. Ustaw nazwę profilu i kliknij *Utwórz profil*. Nazwa profilu jest edytowalna.
6. Wróć do panelu Admin Fudo Enterprise i kliknij *OK* w okienku z QR kodem. Sekcja *Fudo Officer* 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. Włącza on metodę uwierzytelnienia przy logowaniu do aplikacji.

AAPM (Application to Application Password Manager)

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą *Application to Application Password Manager*. Funkcjonalność modułu *AAPM* zostanie zastąpiona APIv2 w kolejnym wydaniu.

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 Enterprise skrypt `fudopv` jest uwierzytelniany na podstawie adresu IP oraz hasła statycznego.

Moduł AAPM wspiera systemy operacyjne Microsoft Windows oraz rodziny systemów BSD i Linux.

25.1 Kompilowanie narzędzia *fudopv*

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą *Application to Application Password Manager*. Funkcjonalność modułu *AAPM* zostanie zastąpiona APIv2 w kolejnym wydaniu.

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*.

25.1.1 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.
-

25.1.2 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, możesz skorzystać z znajdujących się w nim narzędzi *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
```

25.1.3 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.

25.1.4 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*

25.2 Wdrożenie *fudopv* bez kompilacji kodu źródłowego

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą *Application to Application Password Manager*. Funkcjonalność modułu *AAPM* zostanie zastąpiona APIv2 w kolejnym wydaniu.

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*

25.3 Uruchamianie *fudopv*

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą *Application to Application Password Manager*. Funkcjonalność modułu *AAPM* zostanie zastąpiona APIv2 w kolejnym wydaniu.

Parametry wywołania

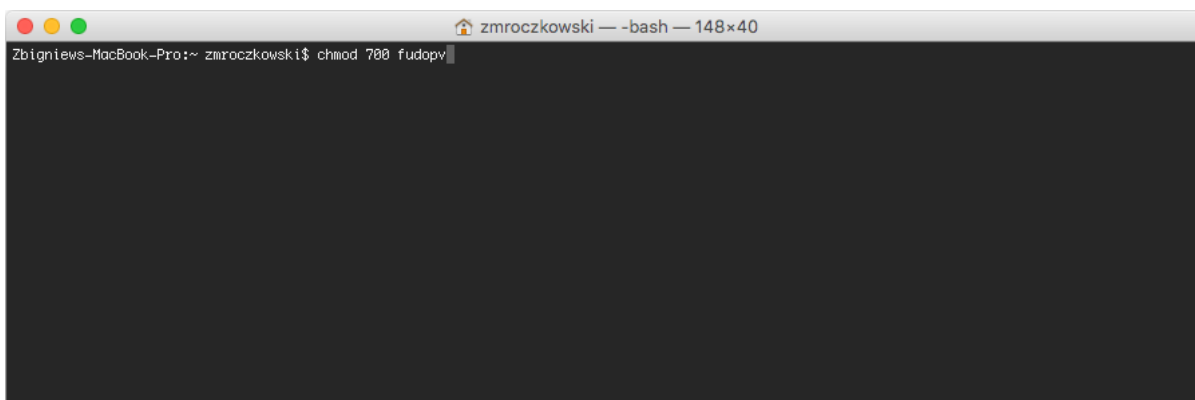
Podczas pracy z *fudopv* używany jest następujący format poleceń:

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

Poniższa tabela przedstawia listę opcji dostępnych dla polecenia *fudopv*.

Komenda/opcja/parametr	Opis
Komendy	
<code>getcrt</code>	Pobierz certyfikat SSL <i>Portalu Użytkownika</i> .
<code>getpass <typ> <nazwa_konta></code>	Pobierz hasło do wybranego konta. typ: <ul style="list-style-type: none"> • <code>direct</code> - połączenie bezpośrednie, niemonitowane; • <code>fudo</code> - połączenie monitorowane przez moduł PSM
Opcje dla typu fudo	
<code>-s <adres>, --server-address <adres></code>	Adres serwera, do którego będzie łączyć się konto.
<code>-p <port>, --port <port></code>	Port serwera, do którego będzie łączyć się konto
Opcje ogólne	
<code>-c <ścieżka>, --cfg <ścieżka></code>	Użyj pliku konfiguracyjnego znajdującego się we wskazanej lokalizacji.
<code>-h, --help</code>	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 Enterprise.
3. Stwórz konto użytkownika o roli *User*, uwierzytelnianego hasłem statycznym.

Informacja:

- Wybierz z lewego menu *Zarządzanie > Użytkownicy*.
- Kliknij *+Dodaj użytkownika*.
- 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 *Dodaj metodę uwierzytelnienia* wybierz *Hasło*.
- Wprowadź hasło w polu *Hasło*.

- Jeśli chcesz żeby zapytania API mogły być wysyłane tylko z określonego adresu IP, w zakładce *Więcej*, w polu *AAPM* wprowadź adres IP serwera, na którym uruchamiany będzie skrypt *fudopv*.
- Kliknij *Zapisz*.

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

```
zmroczkowski — -bash — 148x40
Zbigniew-MacBook-Pro:~ zmroczkowski$ chmod 700 fudopv
Zbigniew-MacBook-Pro:~ zmroczkowski$ ./fudopv getcert
Creating default configuration directory...
Configuration directory was successfully created.
Please set your configuration file before running. It can be find here: /Users/zmroczkowski/.fudopv/fudopv.cfg
Zbigniew-MacBook-Pro:~ zmroczkowski$
```

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

```
.fudopv — vi fudopv.cfg — 148x40
[FUDO]
address=10.0.45.47
cert_path=<CERT_PATH>

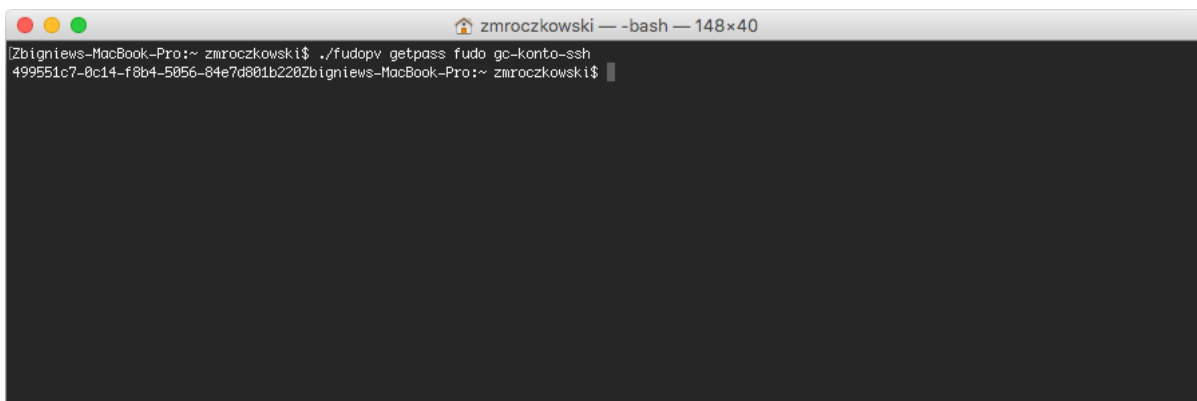
#[CONN]
bind_ip=10.0.1.35

[AUTH]
username=fudopv2
secret=/Users/zmroczkowski/.fudopv/secret.txt
~
~
~
~
~
~
~
~
~
~
```

Sekcja	Opis
[FUDO]	
address	Adres IP <i>Portalu Użytkownika</i> .
cert_path	Ścieżka pliku z certyfikatem SSL <i>Portalu Użytkownika</i> .
[CONN]	
bind_ip	Adres IP serwera, na którym uruchamiany jest skrypt <i>fudopv</i> . Adres IP musi być taki sam jak podany w sekcji <i>API</i> w konfiguracji użytkownika. Parametr opcjonalny.
[AUTH]	
username	Nazwa obiektu użytkownika zdefiniowanego w kroku 3.
secret	Lokalizacja pliku z hasłem statycznym.

Informacja:

- W sekcji [FUDO], w linii `address`, wprowadź adres IP *Portalu Użytkownika*.



```
zmroczkowski — -bash — 148x40
Zbigniew-MacBook-Pro:~ zmroczkowski$ ./fudopv getpass fudo gc-konto-ssh
499551c7-0c14-f8b4-5056-84e7d801b220Zbigniew-MacBook-Pro:~ zmroczkowski$
```

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

Tematy pokrewne:

- *Kompilowanie narzędzia fudopv*
- *Model danych*
- *Opis systemu*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

25.4 Sposoby uwierzytelnienia

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą *Application to Application Password Manager*. Funkcjonalność modułu *AAPM* zostanie zastąpiona *APIv2* w kolejnym wydaniu.

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),
- **SESSIONID**: token sesji,
- **method**: metoda protokołu HTTP: GET/POST/PUT,
- **{„key”: „value”}**: JSON przekazywany w zapytaniu/odpowiedzi.

25.4.1 Hasło statyczne

Styczne 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.*

Tematy pokrewne:

- *Uruchamianie fudopv*
- *Kompilowanie narzędzia fudopv*

Funkcja zdeprecjonowana od wersji 5.4

Fudo Enterprise 5.4 jest ostatnią wersją obsługującą usługę *Service now*. Funkcjonalność ta zostanie usunięta w kolejnym wydaniu.

27.1 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.

Połączenie

Tryb połączenia Pośrednik Adres IP, na którym nasłuchuje Fudo

Adres lokalny 10.0.150.151 Port 222

Certyfikat TLS

```
-----BEGIN CERTIFICATE-----
MIIC0TCCAbmgAwIBAgIJAKTblewxHLmgMA0GCSqGSIb3DQEBBQUAMBAQgNV
BAMMCXNzaF9wcm94eTAqFw0xNzExMjg0MTM5MzFaGA8yMDY3MTEyODEyMzQw
FDESMBAGA1UEAwwJc3NoX3R5b3h5MlIiBjJANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAoknjS0KL1NaQzYxI9kWorWs3gpEbTolquuC3e333fuOJHCm36wAFFxM
+5cxGBW4wnVN1BtyYtr6wp6a2/AoU0H+9FMGHVBJ4+B1O9zahwLVfDxTpH+MULK
AYCb5Gd33GLS721RLWKO3jOwwwFICNW/3w/HHjIAKJq1XbGD3LcBRO1c6UjNKo8e
51SHUCxIY0Z/b+c0v/AK0vjQARyheNGbxrONuedtkd0CV0uH22v0EuYMN4P8hgZ
xljGWBRIAG24eSIRokCfeBineD...f3h5aPMh72Gh9lYx7M8cDmIMZLkewk
-----
```

ssh_proxy Common Name

82:54:74:f7:27:d5:ae:ba:22:b3:e0:9b:f7:c9:50:4d:13:24:d1:9a SHA1

3. Wprowadź numer portu zgodnie z definicją w obiekcie.

Połączenie

Tryb połączenia: Pośrednik Numer portu nasłuchiwania

Adres lokalny: 10.0.150.151 Port: 222

Certyfikat TLS

```
-----BEGIN CERTIFICATE-----
MIIC0TCCAbmgAwIBAgIJAKTblewxHLmgMA0GCSqGSIb3DQEBBQUAMBAQgNV
BAMMCXNzaF9wcm94eTagFw0xNzExMjg0MTU1MzFhZG9wMDY3MTEyODEyMzIw
FDESMBAGA1UEAwwJc3NoX3Byb3h5MIIIBjANBgkqhkiG9w0BAQEFAAOCAQMIIB
CgKCAQEAoknjS0KL1NaQfXyxI9kWorWs3gpEbTOlquuC3e333fuOJHCm36wAFFxM
+5cxGBW4wnVN1BtyYtr6wp6a2/AoUOH+9FMGHVBJ4+B1O9zahwLVftDxTpH+MULK
AYCb5Gd33GLS721RLWKO3jOwwwFICNW/3w/HHjIAKJq1XbGD3LcBRO1c6UjNko8e
51SHUCxIYZ/b+o0v/AK0vjQARyheNGbXrONuedtkd0CV0uH22v0EuYMN4P8hgZ
+LIGWBR1AQ4eSIRokCfeBineD+iOns+f3h5ePMhH72Gh9LYk7MRcDm/MZ+kwuk
-----
```

ssh_proxy Common Name

82:54:74:f7:27:d5:ae:ba:22:b3:e0:9b:f7:c9:50:4d:13:24:d1:9a SHA1

4. W polu wyboru typu połączenia (*Connection type*), wybierz SSH.

PuTTY Configuration

Category:

- [-] Session
 - ... Logging
- [-] Terminal
 - ... Keyboard
 - ... Bell
 - ... Features
- [-] Window
 - ... Appearance
 - ... Behaviour
 - ... Translation
 - ... Selection
 - ... Colours
- [-] Connection
 - ... Data
 - ... Proxy
 - ... Telnet
 - ... Rlogin
 - [-] SSH
 - ... Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.0.150.151 Port: 222

Connection type:

Raw Telnet Rlogin SSH Serial

Load, save or delete a stored session

Saved Sessions

Default Settings Load

Save

Delete

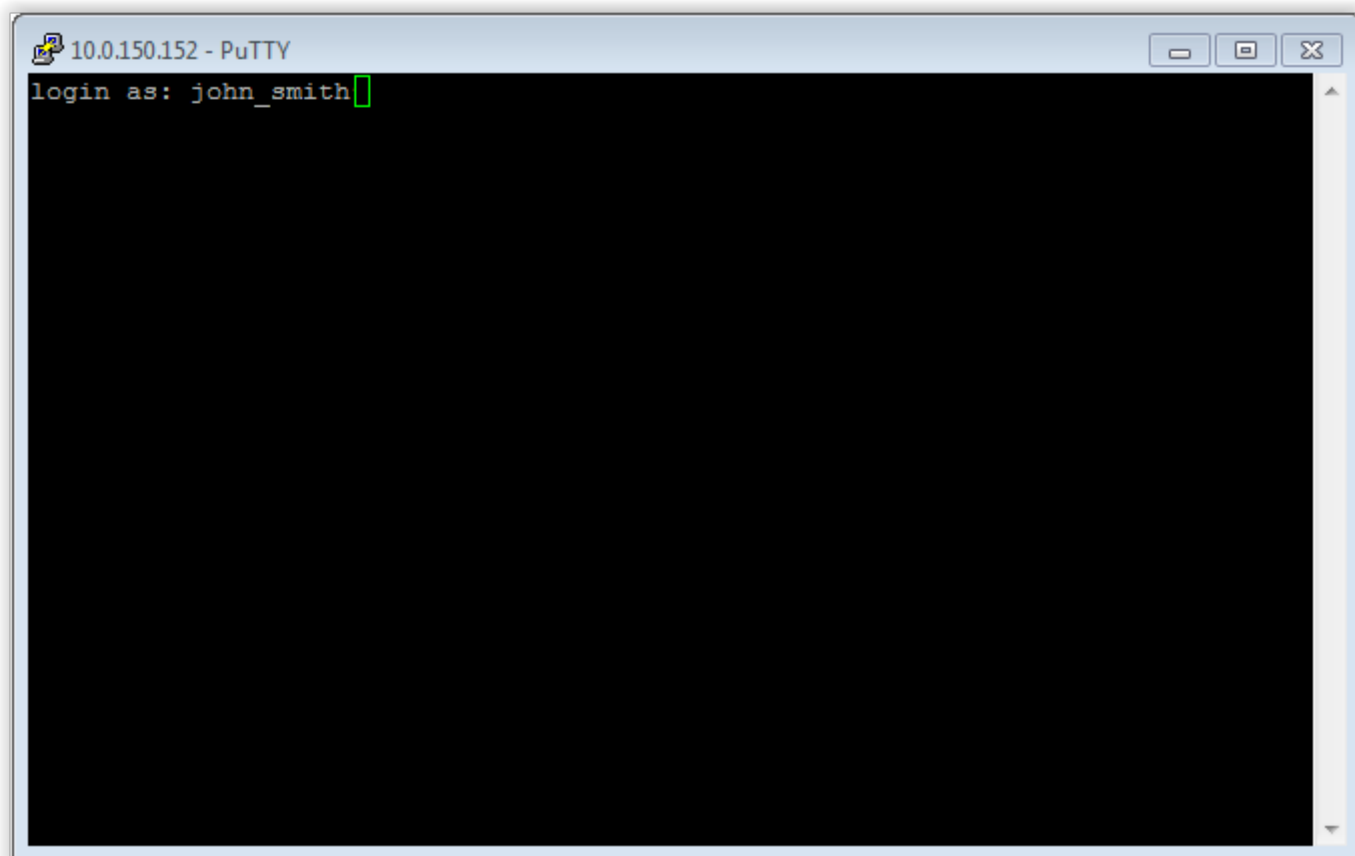
Close window on exit:

Always Never Only on clean exit

About Help Open Cancel

5. Kliknij *Open*.

6. Wprowadź nazwę użytkownika wraz z nazwą konta, na serwerze docelowym.



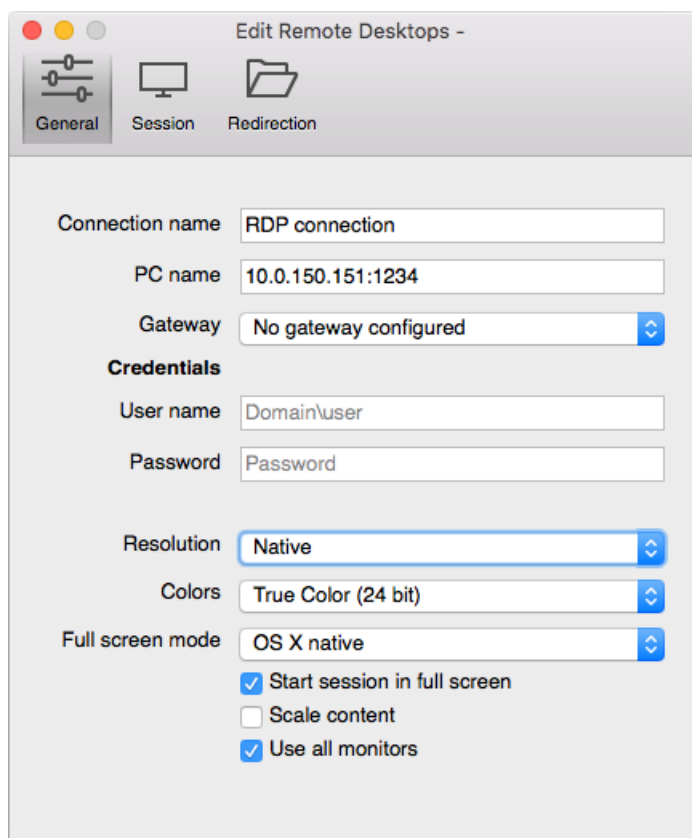
6. Wprowadź hasło użytkownika.

Tematy pokrewne:

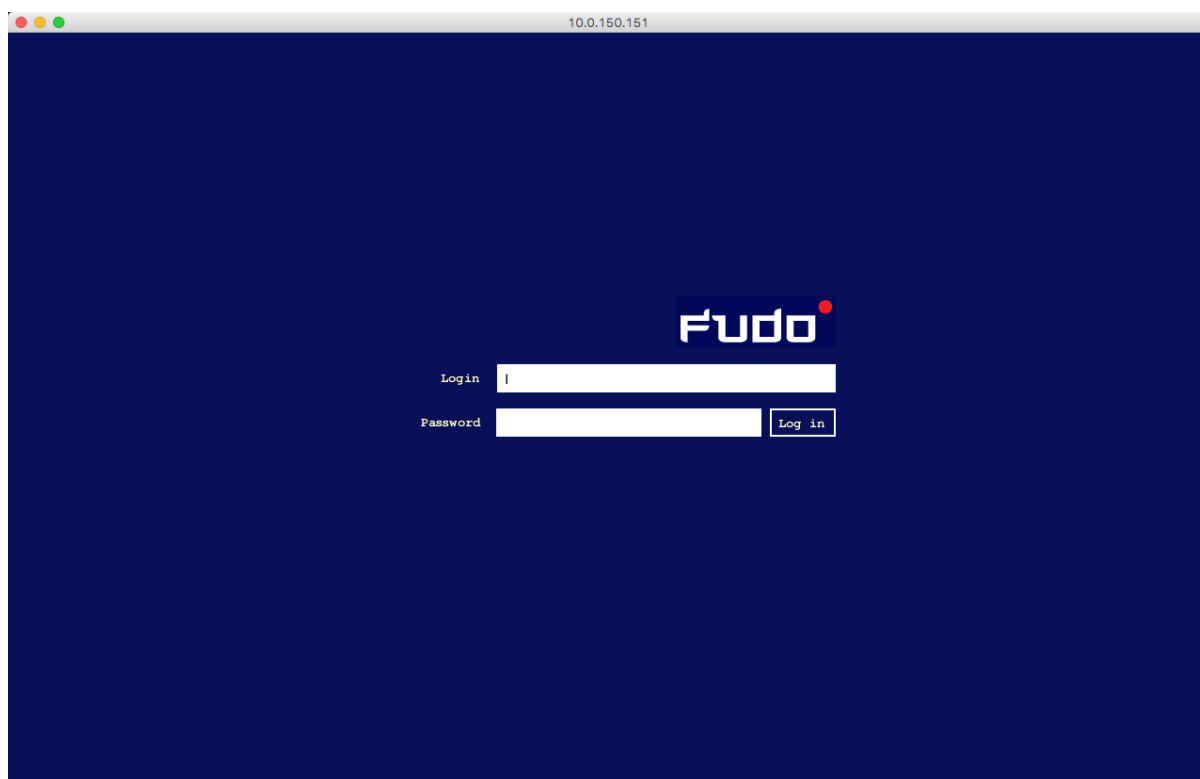
- *SSH*

27.2 Microsoft Remote Desktop

1. Uruchom klienta połączeń RDP.
2. W polu *PC name*, wprowadź adres IP oraz numer portu zdefiniowany w gnieździe nasłuchiwania.

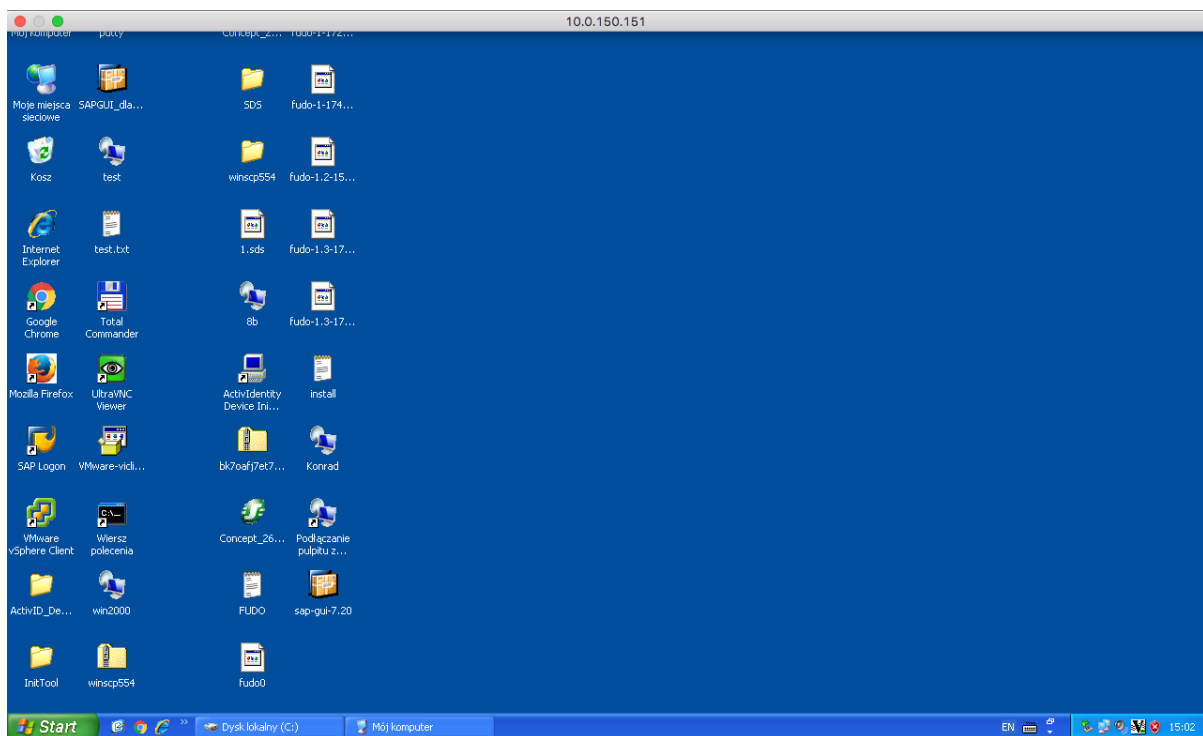


3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter].



Informacja: Fudo Enterprise pozwala na zastosowanie własnych ekranów logowania, braku dostępu i zakończenia sesji dla połączeń RDP i VNC. Więcej informacji na temat konfiguracji

własnych ekranów dla połączeń graficznych, znajdziesz w sekcji *Zasoby*.

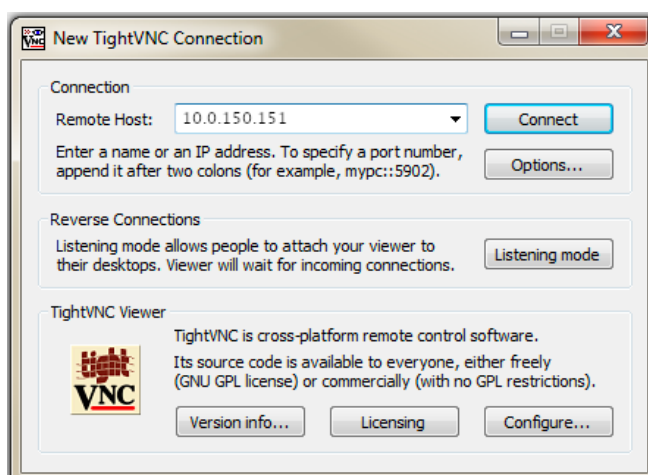


Tematy pokrewne:

- *RDP*

27.3 TightVNC Viewer

1. Uruchom aplikację kliencką *TightVNC Viewer* i w polu adresu wprowadź adres utworzonego gniazda nasłuchowania VNC 10.0.150.151 (sprawdź rozdział *Szybki start - VNC*).



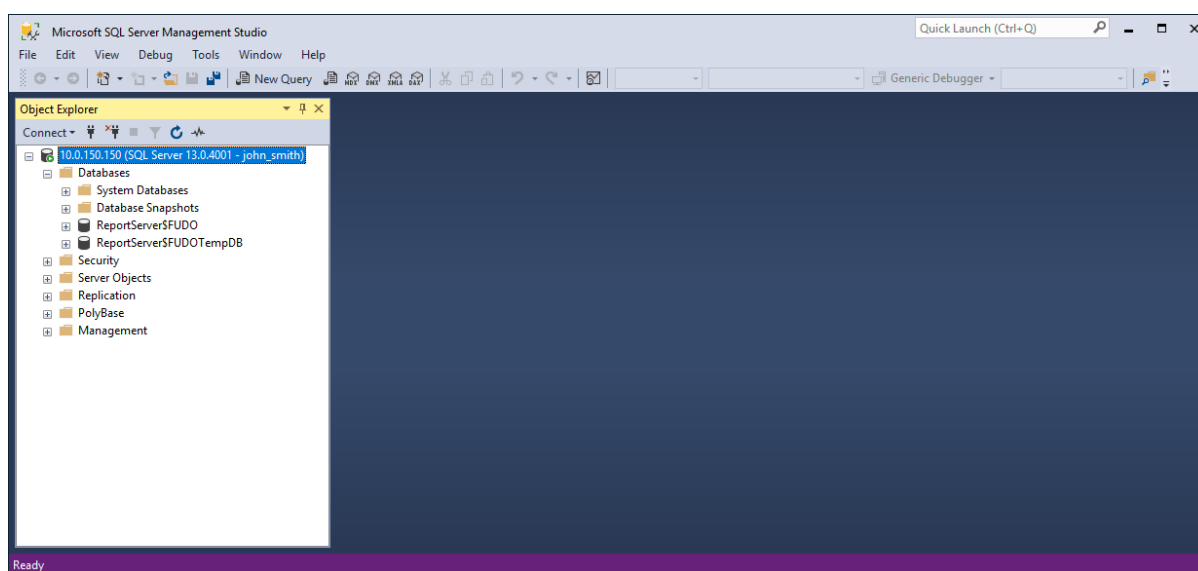
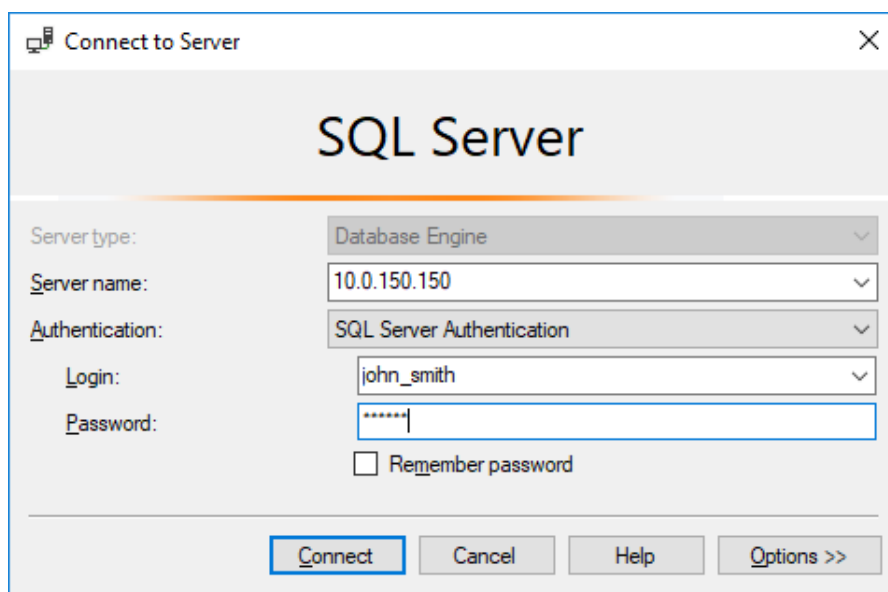
2. Wprowadź nazwę użytkownika, hasło i zatwierdź klawiszem enter.

Tematy pokrewne:

- *Szybki start*

27.4 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:

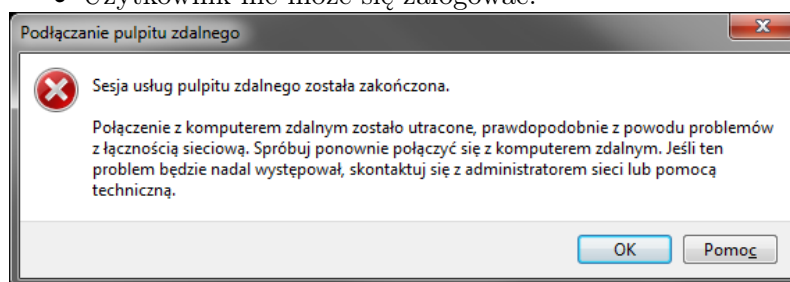
- *MS SQL*

28.1 Uruchamianie Fudo Enterprise

Problem	Objawy i opis rozwiązania
Fudo Enterprise nie uruchamia się	<ul style="list-style-type: none">• 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.

28.2 Połączenia z serwerami

Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem	<p>Objawy:</p> <ul style="list-style-type: none"> • 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 Enterprise.
- 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 Enterprise 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.

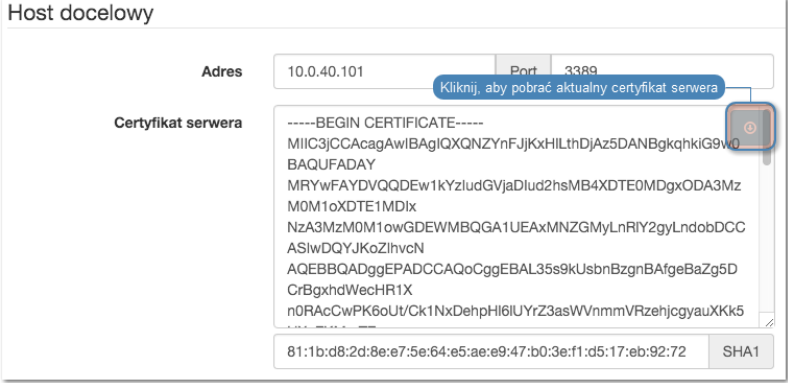
Rozwiązanie:

- Zweryfikuj poprawność definicji danego serwera (adres IP, numer portu).
- Sprawdź, czy serwer osiągalny jest przez Fudo Enterprise:
 1. Zaloguj się do panelu administracyjnego Fudo Enterprise.
 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 Enterprise.
 2. Wybierz *Ustawienia > System*, zakładka *Diagnostyka*.
 3. w sekcji *Netcat*, wprowadź adres IP serwera wraz z numerem portu wybranej usługi i wykonaj polecenie.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Problem	Objawy i opis rozwiązania
	<p>Objawy: Komunikat klienta: <i>Cannot establish new connection because the capacity of the filesystem has been reached.</i></p> <p>Przyczyna: Zajętość przestrzeni przechowywania przekroczyła 90%.</p> <p>Rozwiązanie: Zwolnij miejsce na dane usuwając archiwalne sesje. Więcej informacji znajdziesz w rozdziale <i>Usuwanie sesji</i>.</p>
Problem	Objawy i opis rozwiązania
Przy próbie logowania nie wszyscy użytkownicy widzą ekran logowania Fudo Enterprise (standardowy, z szarym tłem).	<p>Przyczyna:</p> <ul style="list-style-type: none"> • Zapisane poświadczenia w skrócie RDP skutkują ukryciem ekranu Fudo Enterprise i bezpośrednim zalogowaniem do serwera docelowego. • Zapisane poświadczenia w skrócie RDP, użytkownik używa poświadczeń lokalnych na Fudo Enterprise tak więc przed Fudo Enterprise jest poprawnie uwierzytelniany i nie pokazuje mu się ekran logowania. Następnie gdy Fudo Enterprise robi forward uwierzytelnień do docelowej maszyny to są one nie poprawne i użytkownikowi pokazuje się gina Windows gdzie sam się musi uwierzytelnić. <p>Objawy:</p> <ul style="list-style-type: none"> • Komunikat klienta: <i>Connection closed by remote host.</i> • Wpis w dzienniku zdarzeń: <i>Failed to authenticate against the server as user root using password.</i> <p>Przyczyna: niepoprawne dane logowania do serwera docelowego.</p> <p>Rozwiązanie: zmień dane logowania w konfiguracji obiektu serwera.</p>
	<p>Objawy:</p> <ul style="list-style-type: none"> • Komunikat klienta RDP: <i>Connection refused.</i> • Komunikat klienta SSH: <i>ssh: connect to host 10.0.1.111 port 10011: Connection refused</i> <p>Przyczyna: serwer jest zablokowany.</p> <p>Rozwiązanie: odblokuj serwer w panelu administracyjnym Fudo Enterprise.</p>

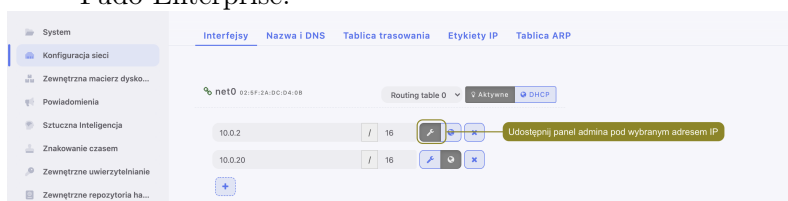
Problem	Objawy i opis rozwiązania
Połączenie jest zrywane	<p>Objawy:</p> <ul style="list-style-type: none"> • Użytkownik próbuje się połączyć z serwerem przez Fudo Enterprise, po wpisaniu nazwy użytkownika i hasła sesja od razu się zrywa. • Komunikat w dzienniku zdarzeń: <i>TLS certificate verification failed.</i>
Rozwiązanie:	
Pobierz nowy certyfikat serwera docelowego w sekcji <i>Host docelowy</i> .	
	
<p>Objawy:</p> <ul style="list-style-type: none"> • Po wpisaniu nazwy użytkownika i hasła następuje zerwanie połączenia. • Wpis w dzienniku zdarzeń: <i>RDP connection error.</i> 	
<p>Rozwiązanie: sprawdź czy w zakładce <i>General</i> we właściwościach TCP-Rdp, opcja <i>Encryption level</i> nie jest ustawiona na <i>FIPS Compliant</i>.</p>	
Brak połączenia z serwerem	<p>Objawy:</p> <ul style="list-style-type: none"> • Nie można zalogować się do serwera, komunikat <i>User user0 not allowed to connect to server.</i> • w dzienniku zdarzeń wpis: <i>Authentication failed: User user0 not allowed to connect to server.</i>
<p>Przyczyna: użytkownik nie jest dodany do połączenia.</p>	
<p>Rozwiązanie: dodaj użytkownika do odpowiedniego obiektu połączenia.</p>	

Problem	Objawy i opis rozwiązania
	<p>Objawy:</p> <ul style="list-style-type: none"> • Po wpisaniu nazwy użytkownika i hasła następuje jakby zamrożenie ekranu logowania. • Wpis w dzienniku zdarzeń <i>Terminating session: User user0 (id=848388532111147010) is blocked.</i> <p>Przyczyna: użytkownik jest zablokowany w Fudo Enterprise.</p> <p>Rozwiązanie: odblokuj użytkownika.</p>
<p>Użytkownik musi logować się dwukrotnie</p>	<p>Objawy: użytkownik łącząc się poprzez protokół RDP wpisuje login i hasło po czym po chwili jest proszony o ponowne wprowadzenie danych autoryzujących.</p> <p>Przyczyna: serwer stanowi część infrastruktury zarządzanej przez broker połączeń, który wykrył istniejącą aktywną sesję użytkownika na innym serwerze.</p>
	<p>Objawy: użytkownik nawiązując połączenie SSH wprowadza dane logowania po czym ponownie proszony jest o ich podanie.</p> <p>Przyczyna: w obiekcie <i>połączenie</i> 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.</p>
<p>Nie można nawiązać połączenia z serwerem RDP</p>	<p>Objawy:</p> <ul style="list-style-type: none"> • użytkownik nawiązując połączenie RDP zostaje rozłączony chwilę po uwierzytelnieniu. • w dzienniku zdarzeń wpis: <i>RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.</i>
	<p>Przyczyna: serwer docelowy, na który następuje przekierowanie, nie nasłuchuje na porcie 3389.</p> <p>Rozwiązanie: skonfiguruj serwer docelowy tak, by oczekiwał na połączenia użytkowników na porcie 3389.</p>
	<p>Objawy:</p> <ul style="list-style-type: none"> • w dzienniku zdarzeń wpis: <i>User user0 has no access to host 192.168.0.1:3389</i> <p>Przyczyna: broker stwierdza, że użytkownik ma aktywną sesję na innym serwerze i inicjuje przekierowanie, ale docelowy serwer nie jest skonfigurowany na Fudo Enterprise lub użytkownik nie jest uprawniony do nawiązywania połączeń z wybranym zasobem.</p>
	<p>Rozwiązanie:</p> <ul style="list-style-type: none"> • Upewnij się, że obiekt serwera jest dodany do Fudo. • Dodaj użytkownika do odpowiedniego <i>sejfu</i>.

Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem Telnet5250 poprzez aplikację PC5250 w wersji 20091005 S oraz 20111019 S	<p>Objawy: próba nawiązania połączenia kończy się niepowodzeniem.</p> <p>Przyczyna: w przypadku wymienionych wersji aplikacji klienckiej, konieczne jest skonfigurowanie ruchu TCP na portach 449, 8470 i 8476, celem poprawnego zestawienia połączenia.</p> <p>Rozwiązanie:</p> <ul style="list-style-type: none"> • Dodaj serwer Telnet TN5250, z domyślnym numerem portu, tj. 23. • Dodaj trzy obiekty typu serwer o protokole <i>TCP</i> i numerach portów odpowiednio 449, 8470 i 8476. • Dodaj gniazdo nasłuchiwania <i>TN5250</i>, w trybie <i>Pośrednik</i>, z domyślnym numerem portu. • Dodaj trzy gniazda nasłuchiwania <i>TCP</i>, w trybie <i>Pośrednik</i>, z numerami portów odpowiednio 449, 8470 i 8476. • Dodaj konto typu <i>regular</i>, określ parametry uwierzytelnienia i przypisz do głównej definicji serwera TN5250. • Dodaj trzy konta typu <i>anonymous</i> przypisując do kolejnych serwerów pomocniczych. • Dodaj sejf i przypisz konta wraz z odpowiadającymi gniazdami nasłuchiwania.

28.3 Logowanie do panelu administracyjnego

Problem	Objawy i opis rozwiązania
Nie można zalogować się do panelu administracyjnego	<ul style="list-style-type: none"> • Zweryfikuj czy wprowadzony adres Fudo Enterprise jest poprawny. • Ustaw adres IP Fudo Enterprise z poziomu konsoli, postępując zgodnie z instrukcją w rozdziale <i>Konfiguracja interfejsów sieciowych</i> w dokumentacji systemu Fudo Enterprise. • Upewnij się, że adres IP ma włączoną funkcję zarządzania Fudo Enterprise.




28.4 Odtwarzanie sesji

Problem	Objawy i opis rozwiązania
Nie można odtworzyć wyeksportowanego materiału	<p>Przyczyna: brak odpowiednich kodeków wideo.</p> <p>Rozwiązanie: zweryfikuj czy masz zainstalowane odpowiednie oprogramowanie.</p>
Użytkownik administrator nie widzi sesji	<p>Objawy: na liście sesji nie ma spodziewanych pozycji.</p> <p>Przyczyna: brak stosownych uprawnień.</p> <p>Rozwiązanie: nadaj użytkownikowi uprawnienia do określonego obiektu połączenia, serwera oraz użytkownika.</p>
Nie można odtworzyć sesji w odtwarzaczu	<p>Objawy: komunikat: Nie można odnaleźć danych sesji.</p> <p>Przyczyna: połączenie miało miejsce przy wyłączonej opcji rejestrowania sesji.</p> <p>Rozwiązanie: włącz opcję rejestrowania sesji, aby w przyszłości mieć możliwość odtworzenia materiału.</p>

28.5 Konfiguracja klastrowa

Problem	Objawy i opis rozwiązania
Obiekty nie replikują się na drugi węzeł	<p>Objawy: Obiekty utworzone na jednym węźle, nie pojawiają się automatycznie na pozostałych węzłach klastra.</p> <p>Rozwiązanie: Skontaktuj się z działem wsparcia technicznego.</p>

28.6 Znakowanie czasem

Problem	Objawy i opis rozwiązania
Sesje nie są znakowane znacznikiem czasu	<p>Objawy:</p> <ul style="list-style-type: none"> • Komunikat w dzienniku zdarzeń: <i>Timestamping service communication error.</i>
	<p>Przyczyna: brak komunikacji z serwerem usługi znakowania czasem.</p>
	<p>Rozwiązanie: Upewnij się, że serwer usługi znakowania czasem jest osiągalny przez system Fudo.</p> <ul style="list-style-type: none"> • adres IP serwera znakowania czasem PWPW: 193.178.164.5 • adres serwera znakowania czasem KIR: http://www.ts.kir.com.pl/HttpTspServer
	<p>Objawy:</p> <ul style="list-style-type: none"> • Komunikat w dzienniku zdarzeń: <i>Unable to timestamp session.</i> • Brak ikony  przy wybranej sesji.
	<p>Przyczyna: Problem z funkcjonowaniem usługi znakowania czasem.</p>
	<p>Rozwiązanie: Zweryfikuj poprawność <i>konfiguracji usługi znakowania czasem.</i></p>

28.7 Tryb serwisowy

Tryb serwisowy umożliwia diagnozowanie Fudo Enterprise 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 [1...
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 Enterprise i musi być osiągalny przez inżyniera wsparcia technicznego. W miarę możliwości, interfejs należy zaadresować tak samo jak przed wystąpieniem awarii.

```

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 [1...
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): █

```

5. Wprowadź adres IP bramy i zatwierdź klawiszem [Enter], aby umożliwić nawiązanie zdalnego połączenia z Fudo Enterprise.

```

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 [1...
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: █

```

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:dgu2Ec8deFWPZkIxJk6EU9loggw+OKXERsW+2PQBSY
res0: link state changed to UP
```

- 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:dgu2Ec8deFWPZkIxJk6EU9loggw+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*

29.1 Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator

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

29.1.1 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

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Platforma / Protokół	Tryb Challenge-Response	Hasło + Wygenerowany kod
TCP	nie dostępne	nie dostępne
MySQL	nie dostępne	nie dostępne
X11	nie dostępne	nie dostępne
Modbus	nie dostępne	nie dostępne

29.1.2 Konfiguracja domyślnych wartości OATH

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

Aby je skonfigurować, postępuj zgodnie z instrukcją:

1. Wybierz *Ustawienia > Uwierzytelnienie*.
2. Wybierz zakładkę **Uwierzytelnienie OATH**.
3. Podaj następujące wartości:
 - *Issuer*,
 - *Typ tokenu*,
 - *Długość tokenu* oraz
 - *Krok czasowy*, jeśli został wybrany czasowy typ tokenu.

4. Kliknij *Zapisz*.

29.1.3 Konfiguracja metody OATH użytkownikowi

Aby skonfigurować dla użytkownika metodę uwierzytelnienia OATH, postępuj zgodnie z instrukcją:

1. Wybierz z lewego menu *Zarządzanie > Użytkownicy*.
2. Odszukaj i kliknij użytkownika, dla którego chcesz włączyć dwuskładnikowe uwierzytelnienie.

- Przejdź do sekcji *Uwierzytelnianie* i wybierz typ OATH z listy rozwijanej *Dodaj metodę uwierzytelniania*.
- Wybierz *Pierwszy składnik: Hasło statyczne* lub *Zewnętrzne uwierzytelnienie*.

Jeśli zostało wybrane **Hasło statyczne**:

- Wprowadź część statyczną hasła.
- Pola *Typ Tokenu*, *Długość tokenu* i *Krok czasowy* wypełniane są automatycznie w oparciu o ustawienia domyślne, jednak wartości te są edytowalne.
- Wprowadź sekret, który będzie użyty do generowania części dynamicznej hasła przez aplikację *Google Authenticator*. Sekret musi być zgodny z formatem **Base32**. Alternatywnie, kliknij przycisk *Generuj*, aby wygenerować go automatycznie lub *QRCode*, aby wyświetlić kod QR.
- Zaznacz opcję *Wymagaj zmiany hasła przy kolejnym logowaniu*.

Jeśli zostało wybrane **Zewnętrzne uwierzytelnienie**:

- Wybierz źródło zewnętrznego uwierzytelnienia.
- Pola *Typ Tokenu*, *Długość tokenu* i *Krok czasowy* wypełniane są automatycznie w oparciu o ustawienia domyślne, jednak wartości te są edytowalne.
- Wprowadź sekret, który będzie użyty do generowania części dynamicznej hasła przez aplikację *Google Authenticator*. Sekret musi być zgodny z formatem **Base32**. Alternatywnie, kliknij przycisk *Generuj*, aby wygenerować go automatycznie lub *QRCode*, aby wyświetlić kod QR.

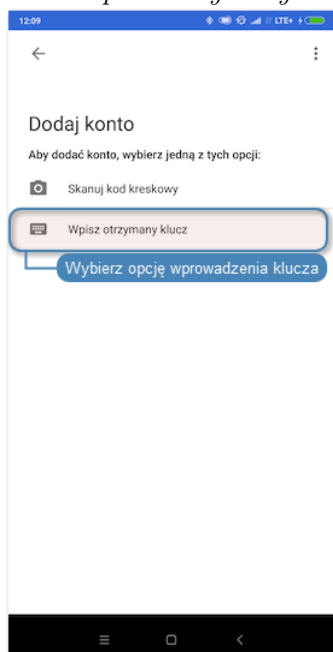
Informacja: Opcja *Zainicjowany* służy do inicjalizacji użytkownika za pomocą kodu QR. Przy podanym hasle albo wybranym źródle zewnętrznego uwierzytelnienia jako *Pierwszego składnika* części statycznej, kod QR wyświetla się użytkownikowi podczas jego pierwszego połączenia. W przypadku pomyślnego pierwszego uwierzytelnienia, opcja *Zainicjowany* jest zaznaczana i nabywa stanu nieedytowalnego.


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

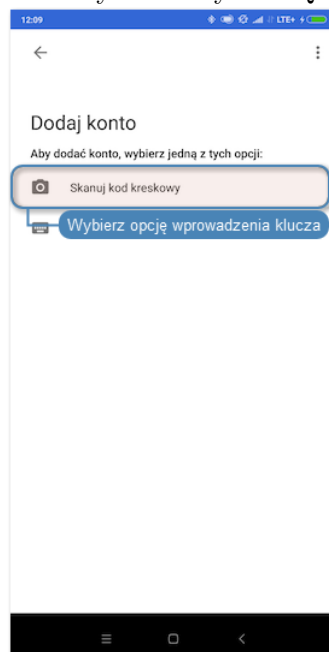
Ręczne wprowadzenie danych

Kod QR

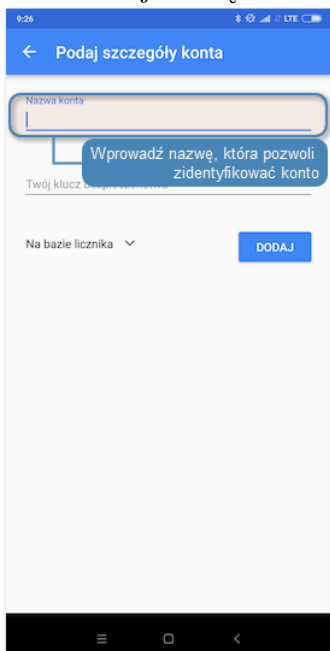
- Na ekranie dodawania konta, wybierz *Wpisz otrzymany klucz*.



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



- Nadaj nazwę konta.



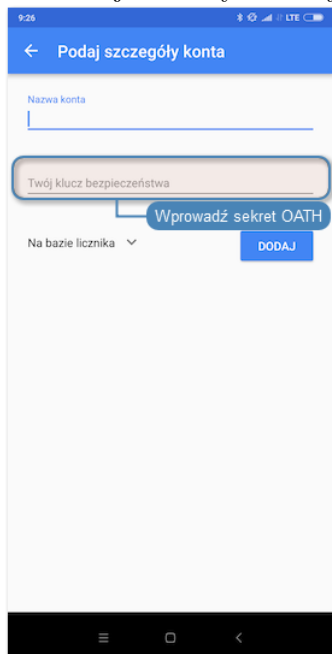
Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

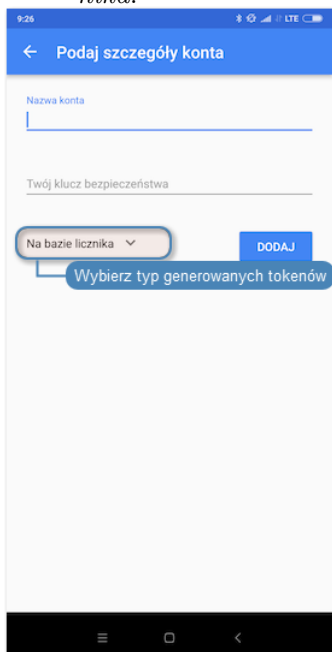
Ręczne wprowadzenie danych

Kod QR

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



- Z listy rozwijalnej wybierz *Na bazie licznika*.



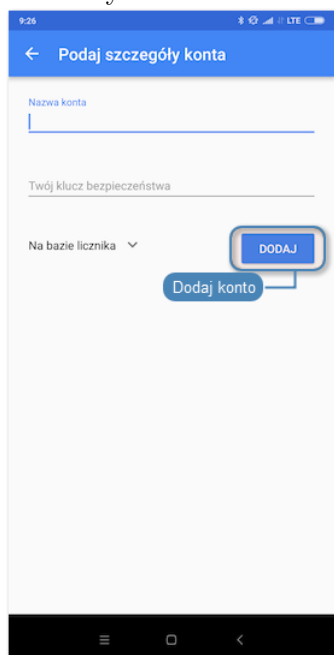
Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

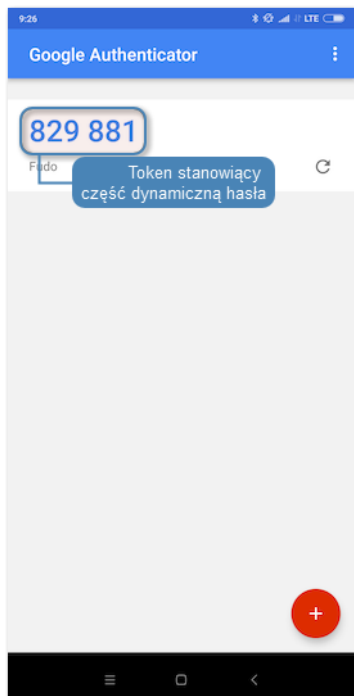
Ręczne wprowadzenie danych

Kod QR

- Wybierz DODAJ.



7. W procesie uwierzytelnienia, hasło stanowi sklejanie części statycznej z kodem wyświetlonym w aplikacji, np. password829881.



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*

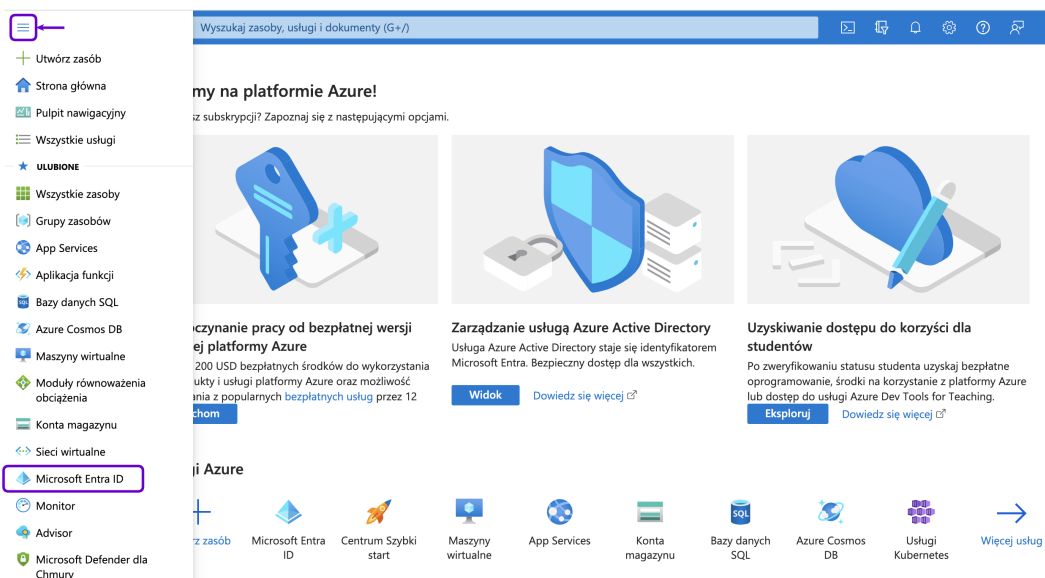
29.2 Konfiguracja uwierzytelnienia OpenID Connect w Azure

Aby skonfigurować metodę uwierzytelnienia OpenID Connect z Azure, postępuj zgodnie z poniższymi krokami.

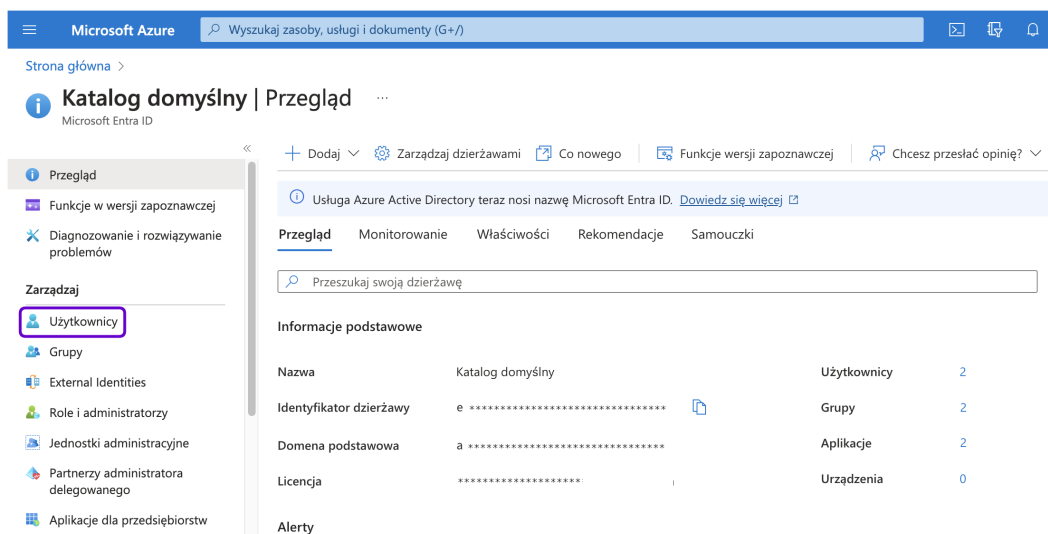
Informacja: Jest to ogólna instrukcja, mająca na celu przybliżenie procesu konfigurowania metody uwierzytelnienia OpenID Connect w Fudo Enterprise. Niektóre szczegóły mogą się różnić w zależności od posiadanej wersji oraz konfiguracji Azure. Szczegółową instrukcję znajdziesz w dokumentacji Azure.

Tworzenie użytkownika w Microsoft Entra ID (Azure Active Directory):

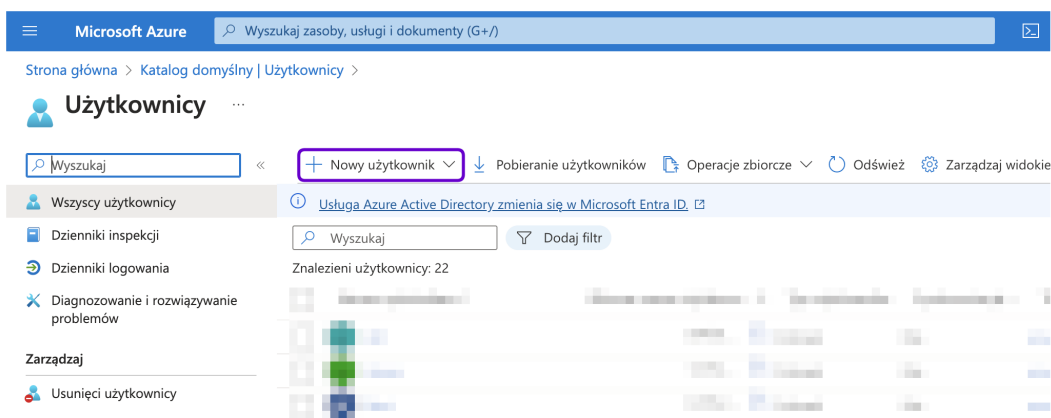
1. Przejdź do portalu Azure i zaloguj się przy użyciu swoich danych uwierzytelniających Azure.
2. Z lewego menu wybierz *Microsoft Entra ID*.



3. Z sekcji menu *Zarządzaj* wybierz *Użytkownicy*.



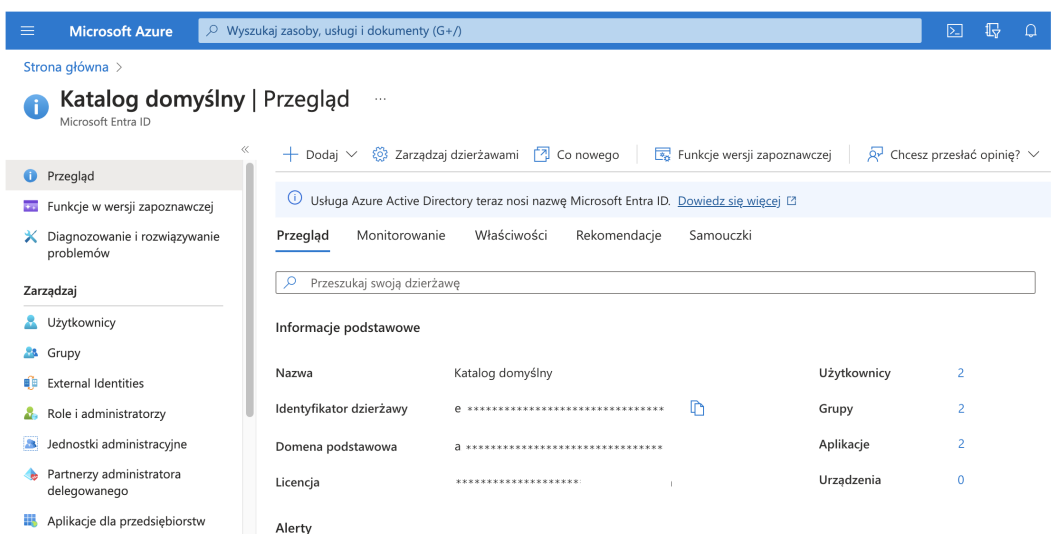
4. Kliknij przycisk *+ Nowy użytkownik*, aby utworzyć nowego użytkownika w Azure. Z listy rozwijanej wybierz opcję *Utwórz nowego użytkownika*.



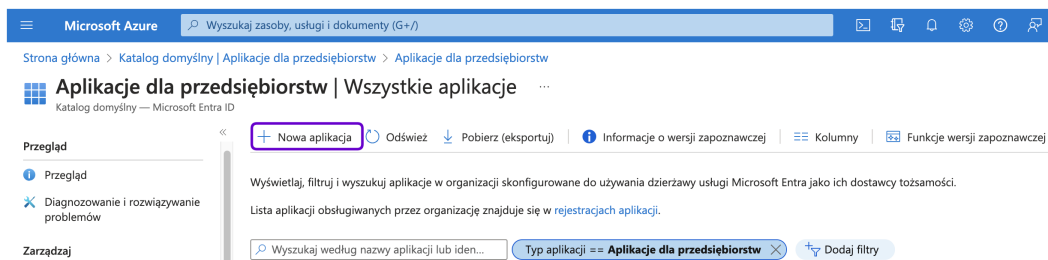
5. W polu *Nazwa główna użytkownika* wprowadź nazwę użytkownika konta. Na przykład: `user1@fudosecurity.com`.
6. W polu *Nazwa wyświetlana* podaj nazwę użytkownika konta.
7. Wprowadź hasło w polu *Hasło* lub kliknij opcję *Automatyczne generowanie hasła*, aby wygenerować hasło.
8. Wybierz opcję *Konto włączone*.
9. W zakładce *Właściwości*, w sekcji menu *Informacje kontaktowe*, w polu *E-mail* podaj adres e-mail. Na przykład: `user1@fudosecurity.com`.
10. Wprowadź pozostałe parametry wymagane dla użytkownika w zakładkach *Właściwości* i *Przypisania*.
11. Kliknij *Utwórz*.

Rejestracja Fudo w Microsoft Entra ID (Azure Active Directory):

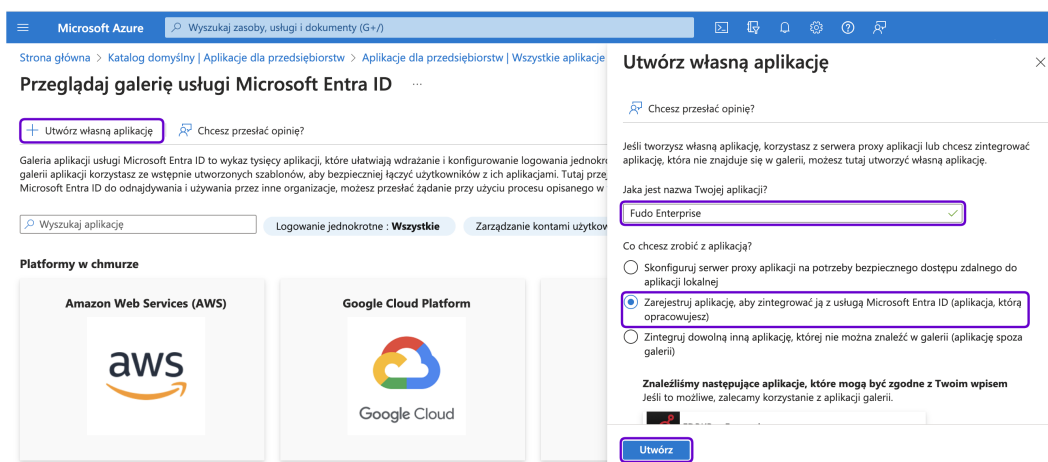
1. Wróć do menu *Microsoft Entra ID* i z sekcji menu *Zarządzaj* wybierz *Aplikacje dla przedsiębiorstw*.



2. Kliknij przycisk *+ Nowa aplikacja*, aby utworzyć nową aplikację.



3. Kliknij przycisk *+ Utwórz własną aplikację*.
4. W prawym oknie dialogowym podaj nazwę swojej aplikacji i wybierz opcję *Zarejestruj aplikację, aby zintegrować ją z usługą Microsoft Entra ID (aplikacja, którą opracowujesz)*.
5. Kliknij *Utwórz*.



6. Na kolejnej stronie, w sekcji menu *Obsługiwane typy kont*, wybierz opcję *Konta tylko w tym katalogu organizacyjnym (tylko Katalog domyślny — pojedyncza dzierżawa)*.
7. W sekcji menu *Identyfikator URI przekierowania* wybierz *Internet* z listy rozwijanej platformy i podaj adres do Portalu Użytkownika Fudo Enterprise z przyrostkiem `/oidc`. Na przykład: `https://10.0.58.239/oidc` lub `https://fudo.example.com/oidc`.

Informacja: Adres Portalu Użytkownika można znaleźć w Fudo Enterprise, w menu *Ustawienia > Konfiguracja sieci*. Więcej informacji znajdziesz w sekcji menu *Konfiguracja sieci*.

Microsoft Azure Wyszukaj zasoby, usługi i dokumenty (G+)

Strona główna > Katalog domyślny | Aplikacje dla przedsiębiorstw > Aplikacje dla przedsiębiorstw | Wszystkie aplikacje > Przeglądaj galerię usługi Microsoft Entra ID >

Zarejestruj aplikację

* Nazwa

Nazwa wyświetlana tej aplikacji widoczna dla użytkowników (można ją później zmienić).

Fudo Enterprise

Obsługiwane typy kont

Kto może korzystać z tej aplikacji lub uzyskiwać dostęp do tego interfejsu API?

- Konta tylko w tym katalogu organizacyjnym (tylko Katalog domyślny — pojedyncza dzierżawa)
- Konta w dowolnym katalogu organizacyjnym (dowolna dzierżawa usługi Microsoft Entra ID — wiele dzierżaw)
- Konta w dowolnym katalogu organizacyjnym (dowolna dzierżawa usługi Microsoft Entra ID — wiele dzierżaw) i osobiste konta Microsoft (np. Skype, Xbox)
- Tylko osobiste konta Microsoft

[Pomóż mi wybrać...](#)

Identyfikator URI przekierowania (opcjonalnie)

Pod ten identyfikator URI zostanie zwrócona odpowiedź uwierzytelniania po pomyślnym uwierzytelnieniu użytkownika. Podanie teraz tego identyfikatora URI jest opcjonalne i można go później zmienić, ale wartość jest wymagana w przypadku większości scenariuszy uwierzytelniania.

Internet

Zarejestruj tutaj aplikację, nad którą pracujesz. Zintegruj aplikację z galerii i inne aplikacje spoza Twojej organizacji, dodając je z obszaru [Aplikacje dla przedsiębiorstw](#).

Kontynuując, akceptujesz zasady platformy firmy Microsoft

Rejestruj

- Kliknij *Rejestruj*, aby utworzyć aplikację.
- Wróć do głównego menu *Microsoft Entra ID* i z sekcji menu *Zarządzaj* wybierz *Rejestracje aplikacji*.
- Przejdź do zakładki *Wszystkie aplikacje*, znajdź utworzoną aplikację na liście aplikacji i kliknij na nazwę, aby edytować jej parametry. Zapisz *Identyfikator aplikacji (klienta)* i *Identyfikator katalogu (dzierżawcy)*, ponieważ będziesz ich potrzebować na późniejszym etapie konfiguracji.

Microsoft Azure Wyszukaj zasoby, usługi i dokumenty (G+)

Strona główna > Katalog domyślny | Rejestracje aplikacji >

Fudo Enterprise PL Test

Wyszukaj

Przełącz

Szybki start

Asystent integracji

Zarządzaj

- Znakowanie i właściwości
- Uwierzytelnianie
- Certyfikaty i klucze tajne

Masz sekundę? Bardzo chcielibyśmy poznać Twoją opinię o platformie tożsamości Microsoft (wcześniej nazywanej usługą Azure AD dla developerów). →

Podstawowe elementy

Nazwa wyświetlana : Fudo Enterprise PL Test

Identyfikator aplikacji (kli... : 1.....

Identyfikator obiektu : 4.....

Identyfikator katalogu (d... : e.....

Obsługiwane typy kont : Tylko moja organizacja

Poświadczenia klienta : Dodaj certyfikat lub wpis tajny

Identyfikator URI przeki... : Internetowe: 1 aplikacja jednostronnych: 0 klientó...

Identyfikator URI identyfi... : Dodawanie identyfikatora URI identyfikatora aplikacji

Aplikacja zarządzana w k... : Fudo Enterprise PL Test

Konfiguracja ustawień uwierzytelnienia:

- Wróć do głównego menu *Microsoft Entra ID* i z sekcji menu *Zarządzaj* wybierz *Rejestracje aplikacji*.
- Znajdź utworzoną aplikację na liście aplikacji i kliknij na nazwę, aby edytować jej parametry.
- W sekcji menu *Zarządzaj* wybierz *Uwierzytelnianie*.
- W platformie *Internet* utworzonej dla Fudo Enterprise dodaj adres przekierowania do Panelu Administracyjnego Fudo, dodając odpowiednio przyrostek `/oidc`. Na przykład: `https://10.0.58.238/oidc` lub `https://fudo.example.com/oidc`.

Microsoft Azure Wyszukaj zasoby, usługi i dokumenty (G+/)

Strona główna > Katalog domyślny | Rejestracje aplikacji > Fudo Enterprise PL Test

Fudo Enterprise PL Test | Uwierzytelnianie

Wyszukaj << Chcesz przesłać opinię?

Konfiguracje platform

W zależności od docelowej platformy lub urządzenia tej aplikacji może być wymagana dodatkowa konfiguracja, np. identyfikatory URI przekierowania, konkretne ustawienia uwierzytelniania lub pola specyficzne dla platformy.

+ Dodaj platformę

Internet Szybki start Dokumentacja? 🗑️

Identyfikatory URI przekierowania

Identyfikatory URI, które będziemy akceptować jako miejsca docelowe podczas zwracania odpowiedzi uwierzytelniania (tokenów) po pomyślnym uwierzytelnieniu lub wylogowaniu użytkowników. Identyfikator URI przekierowania wysyłany w żądaniu do serwera logowania powinien być zgodny z podanym tutaj identyfikatorem, nazywanym również adresem URL odpowiedzi. [Dowiedz się więcej o identyfikatorach URI przekierowania i ich ograniczeniach](#)

https://10.0.58.239/oidc 🗑️

https://10.0.58.238/oidc ✓ 🗑️

Dodaj identyfikator URI

5. W sekcji menu *Przepływy niejawnego przyznania i hybrydowe* zaznacz opcje *Tokeny dostępu* i *Tokeny identyfikatorów*.

Microsoft Azure Wyszukaj zasoby, usługi i dokumenty (G+/)

Strona główna > Katalog domyślny | Rejestracje aplikacji > Fudo Enterprise PL Test

Fudo Enterprise PL Test | Uwierzytelnianie

Wyszukaj << Chcesz przesłać opinię?

Adres URL wylogowania kanału frontowego

To jest adres, pod który wysyłamy żądanie wyczyszczenia danych sesji użytkownika przez aplikację. Jest wymagany do poprawnego działania wylogowywania jednokrotnego.

np. https://example.com/logout ✓

Przepływy niejawnego przyznania i hybrydowe

Żądaj tokenu bezpośrednio z punktu końcowego autoryzacji. Jeśli aplikacja ma architekturę jednostronicową i nie korzysta z przepływu kodu autoryzacji lub jeśli wywołuje internetowy interfejs API za pomocą języka JavaScript, wybierz zarówno tokeny dostępu, jak i tokeny identyfikatorów. W przypadku aplikacji internetowych ASP.NET Core i innych aplikacji internetowych używających uwierzytelniania hybrydowego wybierz tylko tokeny identyfikatorów. [Dowiedz się więcej o tokenach](#).

Wybierz tokeny, które mają być wystawiane przez punkt końcowy autoryzacji:

Tokeny dostępu (używane na potrzeby niejawnych przepływów)

Tokeny identyfikatorów (używane na potrzeby niejawnych i hybrydowych przepływów)

Obsługiwane typy kont

Kto może korzystać z tej aplikacji lub uzyskiwać dostęp do tego interfejsu API?

Konta tylko w tym katalogu organizacyjnym (tylko Katalog domyślny — pojedyncza dzierżawa)

Konta w dowolnym katalogu organizacyjnym (dowolna dzierżawa usługi Microsoft Entra ID — wiele dzierżaw)

Pomóż mi podjąć decyzję...

6. W sekcji menu *Blokada właściwości wystąpienia aplikacji* kliknij *Konfiguruj* i w prawym oknie dialogowym wyłącz opcję *Włącz blokadę właściwości*. Kliknij *Zapisz*, aby zamknąć okno dialogowe.

7. Kliknij *Zapisz*, aby zapisać ustawienia uwierzytelnienia.

Generowanie sekretu klienta:

1. W ustawieniach aplikacji na portalu Azure przejdź do sekcji *Certyfikaty i klucze tajne*.

2. W zakładce *Wpisy tajne klienta* wybierz *+ Nowy klucz tajny klienta*.
3. Podaj opis, wybierz pożądaną okres ważności i kliknij *Dodaj*.

Ostrzeżenie: Zapisz *Identyfikator wpisu tajnego* oraz *Wartość* wygenerowanego sekretu, ponieważ będziesz ich potrzebować do konfiguracji Fudo Enterprise. Po zapisaniu wartość sekretu nie będzie widoczna.

Microsoft Azure | Wyszukaj zasoby, usługi i dokumenty (G+)

Strona główna > Katalog domyślny | Rejestracje aplikacji > Fudo Enterprise PL Test

Fudo Enterprise PL Test | Certyfikaty i klucze tajne

Wyszukaj | Chcesz przesłać opinię?

Masz chwilę, aby przekazać nam opinię? →

Poświadczenia umożliwiają poufnym aplikacjom identyfikowanie się w usłudze uwierzytelniania podczas odbierania tokenów w lokalizacji z adresem internetowym (przy użyciu schematu HTTPS). W celu zapewnienia wyższego poziomu bezpieczeństwa zalecane jest używanie certyfikatu (zamiast klucza tajnego klienta) jako poświadczenia.

Certyfikaty rejestracji aplikacji, wpisy tajne i poświadczenia federacyjne można znaleźć na poniższych kartach.

Certyfikaty (0) | **Wpisy tajne klienta (1)** | Poświadczenia federacyjne (0)

Ciąg klucza tajnego, którego aplikacja używa, aby potwierdzić swoją tożsamość podczas żądania tokenu. Może być również określany jako hasło aplikacji.

+ Nowy klucz tajny klienta

Opis	Wygasa	Wartość	Identyfikator wpisu tajnego
Password uploaded on Tue Sep 19 2023	17.03.2024	*****	*****

Pobieranie adresu URL konfiguracji OpenID Connect:

1. W ustawieniach aplikacji na portalu Azure przejdź do sekcji *Przegląd*.
2. Znajdź zakładkę *Punkty końcowe* i wyszukaj adres URL *Dokument metadanych protokołu OpenID Connect*. To jest Twój adres URL konfiguracji OpenID Connect. Skopiuj go, ponieważ będziesz go potrzebować do konfiguracji Fudo Enterprise.

Microsoft Azure | Wyszukaj zasoby, usługi i dokumenty (G+)

Strona główna > Katalog domyślny | Rejestracje aplikacji > Fudo Enterprise PL Test

Fudo Enterprise PL Test

Wyszukaj | Usurfi Punkty końcowe | Funkcje w w

Masz sekundę? Bardzo chcielibyśmy poznać Twój

Podstawowe elementy

Nazwa wyświetlana : Fudo Enterprise PL

Identyfikator aplikacji (kli... : *****

Identyfikator obiektu : *****

Identyfikator katalogu (d... : *****

Obsługiwane typy kont : Tylko moja organizacja

Począwszy od 30 czerwca 2020 r. nie będziemy nadal oferować pomoc techniczną i aktualizacji Authentication Library (MSAL) i programu Msal

Rozpocznij Dokumentacja

Utwórz aplikację

Platforma tożsamości
Możesz tworzyć no

Punkty końcowe

Punkt końcowy autoryzacji OAuth 2.0 (wersja 2)
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/oaauth2/v2.0/authorize>

Punkt końcowy tokenu OAuth 2.0 (wersja 2)
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/oaauth2/v2.0/token>

Punkt końcowy autoryzacji OAuth 2.0 (wersja 1)
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/oaauth2/authorize>

Punkt końcowy tokenu OAuth 2.0 (wersja 1)
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/oaauth2/token>

Dokument metadanych protokołu OpenID Connect
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/v2.0/well-known/openid-configuration>

Punkt końcowy interfejsu API programu Microsoft Graph
<https://graph.microsoft.com>

Dokument metadanych federacji
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/federationmetadata/2007-06/federationmetadata.xml>

Punkt końcowy logowania usług federacyjnych w sieci Web
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/wsfed>

Punkt końcowy logowania protokołu SAML-P
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/saml2>

Punkt końcowy wylogowania protokołu SAML-P
<https://login.microsoftonline.com/e150f013-757f-405d-be2c-accdd2b2983/saml2>

Konfiguracja metody uwierzytelnienia OpenID Connect w Fudo:

1. Przejdź do Panelu Administracyjnego Fudo Enterprise.
2. Wybierz *Ustawienia > Uwierzytelnienie*.
3. Wybierz zakładkę **Uwierzytelnienie OpenID Connect**.
4. Kliknij *Dodaj źródło zewnętrznego uwierzytelnienia*.
5. Zaznacz opcję *Włączone*, aby włączyć globalnie uwierzytelnienie przy użyciu OpenID Connect.
6. Podaj nazwę (np. *Azure*).
7. Wprowadź *Configuration URL* (*Dokument metadanych protokołu OpenID Connect* z Azure).
8. Podaj *Client ID* (*Identyfikator wpisu tajnego* z Azure).
9. Wprowadź *Client secret* (wartość certyfikatu, czyli *Wartość* z Azure).

The screenshot shows the 'Uwierzytelnienie OpenID Connect' configuration page in the Fudo Enterprise admin console. The 'Włączone' checkbox is checked. The configuration details are as follows:

- Name: Azure
- Configuration url: https://login.microsoftonline.com/e150f013-7571-405d-be2c-accdd42b2
- Client id: 8cfd1d1-ff9d-4a7d-829e-7dda0e6f2717
- Client secret: [masked]
- Username mapping: [empty field]
- Email mapping: [empty field]
- Bind to: Dowolny
- Usun:

Callout boxes provide the following information:

- 'Dokument metadanych protokołu OpenID Connect' z Azure (points to Configuration url)
- 'Identyfikator wpisu tajnego' z Azure (points to Client id)
- 'Wartość' certyfikatu z Azure (points to Bind to)

10. Dodaj *Username mapping* i *Email mapping*. Te pola są przydatne, gdy nazwa użytkownika ma przyjętą inną konwencję nazewnictwa.
11. Podaj *Bind address*.
12. Kliknij *Zapisz*.

Tworzenie użytkownika w Fudo:

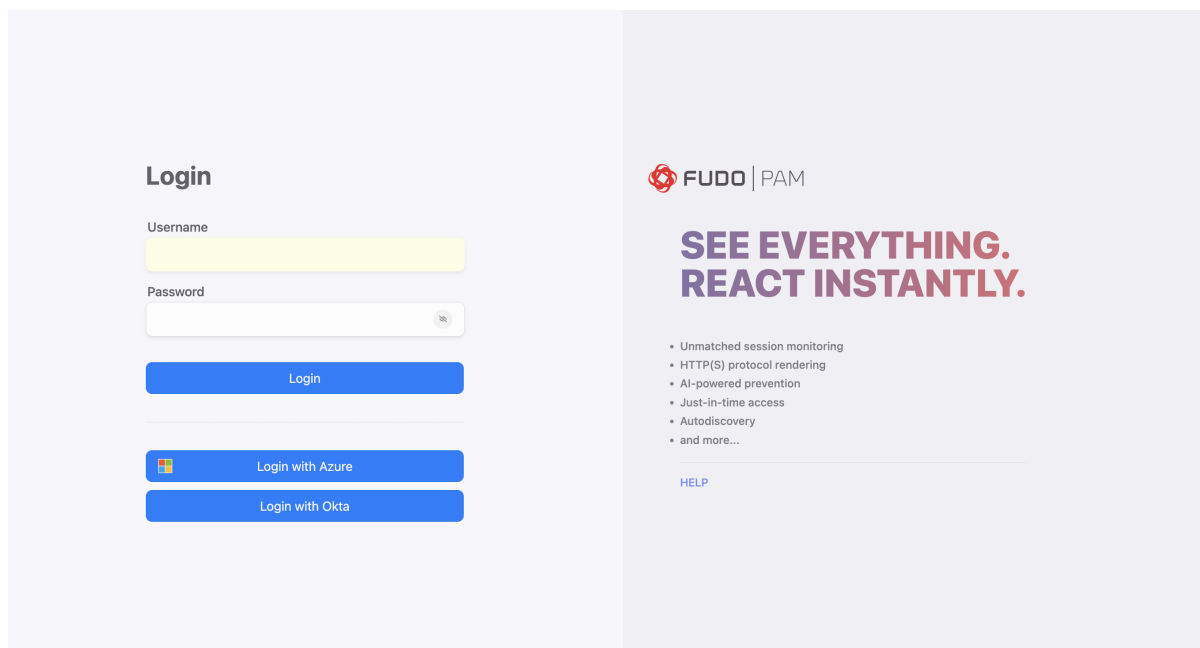
1. Wybierz *Zarządzaj > Użytkownicy*, a następnie kliknij *+ Dodaj użytkownika*.
5. Kliknij *Zapisz*.

Informacja: Podany adres e-mail jest wykorzystywany do powiązania użytkowników Fudo Enterprise z odpowiadającymi im kontami utworzonymi w Azure. Upewnij się, że adresy e-mail nie są zduplikowane wśród użytkowników.

Testowanie:

Możesz teraz przetestować uwierzytelnienie *OpenID Connect* próbując zalogować się do Panelu Administracyjnego lub Portalu Użytkownika Fudo Enterprise. Zaloguj się, korzystając z metody

uwierzytelniania Azure:



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Uwierzytelnienie*
- *Integracja z serwerem CERB*

29.3 Konfiguracja usługi Remote Desktop Services na serwerze Windows dla Fudo Enterprise

Przed rozpoczęciem procedury sprawdź następujące wymagania:

- Wszystkie serwery z systemem Windows Server 2019 lub 2022 są połączone w domenę;
- Istnieje skonfigurowany na serwerze Windows kontroler domeny z grupą użytkowników AD;
- Wszystkie serwery Windows mają zainstalowany patch CredSSP CVE-2018-0886;
- Masz dostęp do panelu administracyjnego Fudo Enterprise w celu skonfigurowania połączenia RDP.

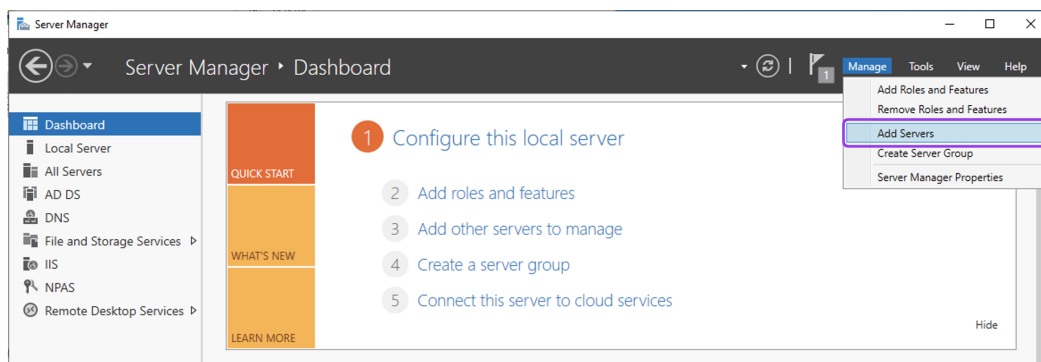
Aby skonfigurować i używać usługi Remote Desktop Services (RDS) wraz z Fudo Enterprise, postępuj zgodnie z poniższą instrukcją.

Informacja: Jest to ogólna instrukcja, mająca na celu przybliżenie procesu konfigurowania usługi Remote Desktop Services. Pewne aspekty mogą się różnić w zależności od konfiguracji środowiska Windows Server. Szczegółową instrukcję znajdziesz w dokumentacji Windows Server.

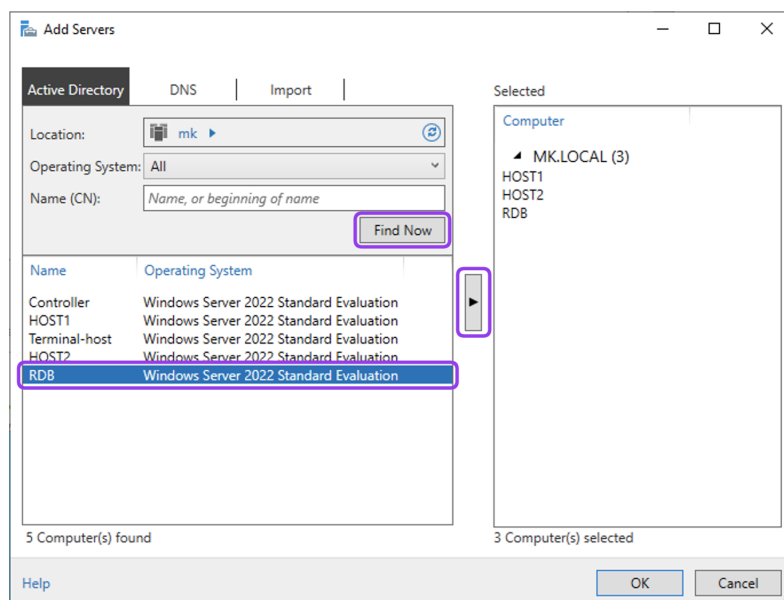
29.3.1 Konfiguracja usługi Remote Desktop Services (RDS)

Dodaj serwery:

1. Zaloguj się na serwerze, na którym chcesz skonfigurować usługę Remote Desktop Services.
2. Uruchom aplikację *Server Manager*.
3. Kliknij przycisk *Manage* w prawym górnym rogu okna, aby rozwinąć listę menu, a następnie wybierz *Add Servers*.

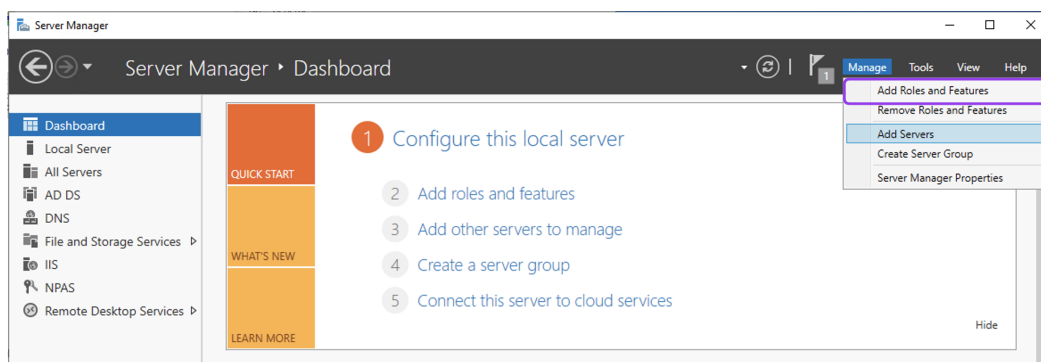


4. Kliknij *Find Now*.
5. Dodaj wszystkie serwery, które zamierzasz użyć w RDS, klikając na każdy serwer w konfiguracji. Kliknij *OK*. W tym przypadku dodajemy 3 serwery: *HOST1*, *HOST2*, i *RDB*, który będzie pełnił rolę *Brokera*.

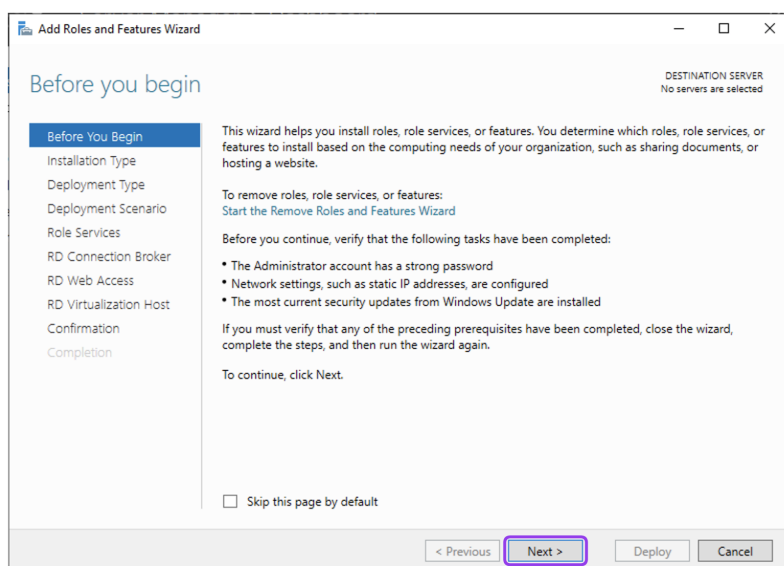


Dodaj komponenty usługi Remote Desktop Services:

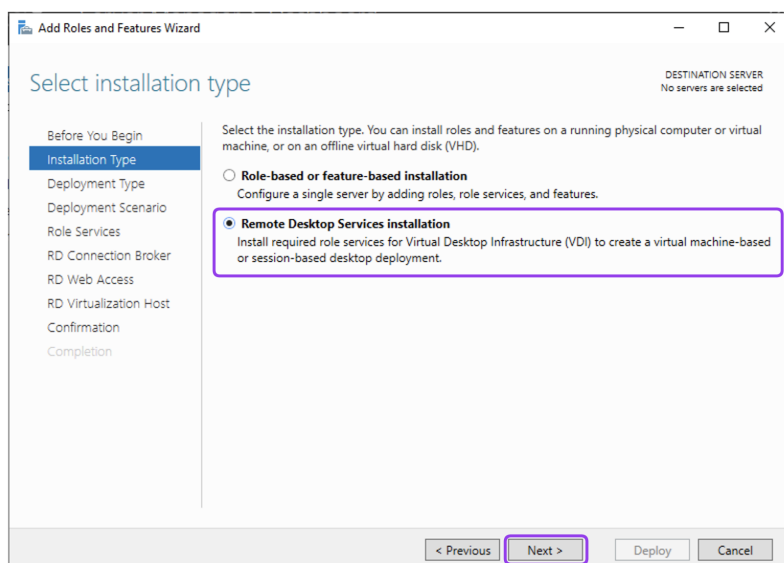
1. Kliknij przycisk *Manage* w prawym górnym rogu okna, aby rozwinąć listę menu, a następnie wybierz *Add Roles and Features*.



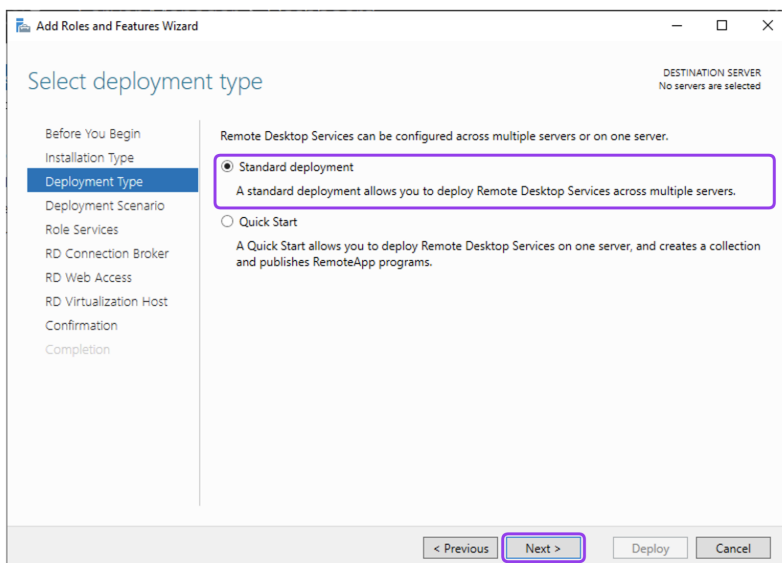
2. Na karcie *Before You Begin* kliknij *Next*, aby kontynuować.



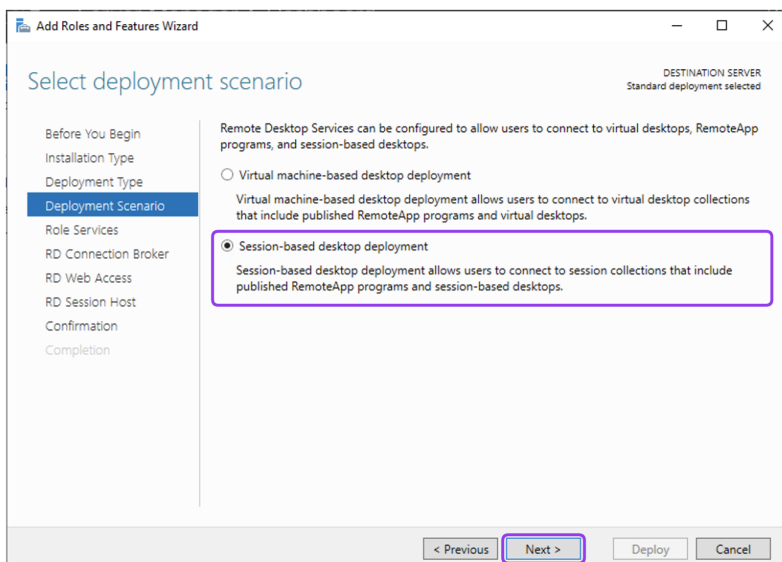
3. Na karcie *Installation Type* wybierz *Remote Desktop Services installation* i kliknij *Next*, aby kontynuować.



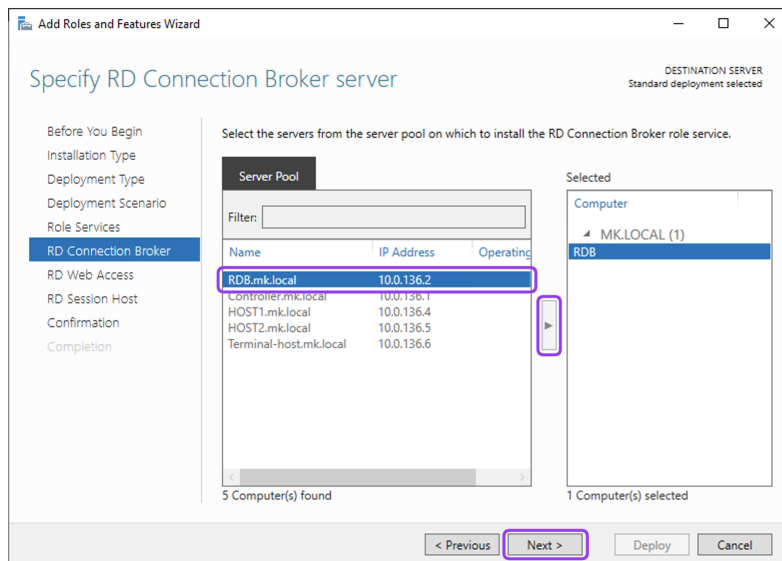
4. Na karcie *Deployment Type* wybierz *Standard Deployment*, aby uzyskać bardziej szczegółowe instrukcje dotyczące instalacji usługi Remote Desktop Services. Kliknij *Next*, aby kontynuować.



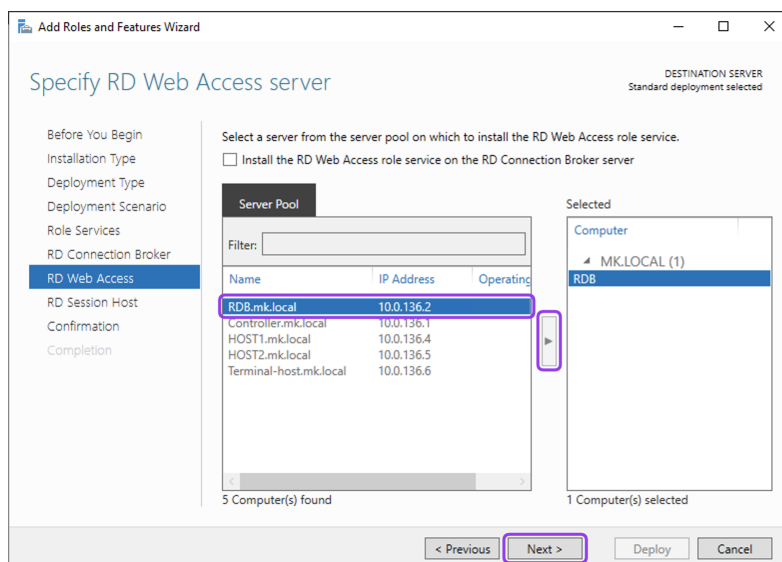
5. Na karcie *Deployment Scenario* wybierz *Session-based desktop deployment*. Kliknij *Next*, aby kontynuować.



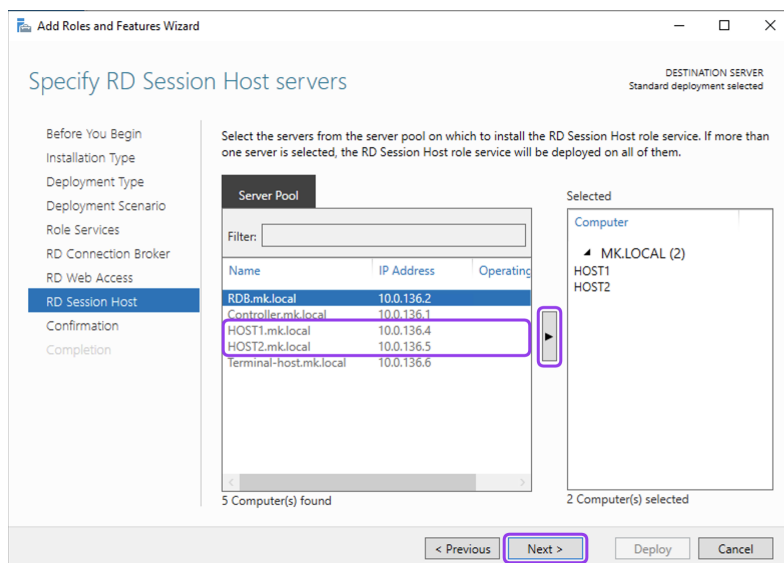
6. Na karcie *Role Services* sprawdź usługi, które zostaną zainstalowane. Kliknij *Next*, aby kontynuować.
7. Na karcie *RD Connection Broker* wybierz odpowiedni serwer, na którym zostanie zainstalowana usługa roli Brokera. W tym przykładzie wybrano serwer RDB. Kliknij *Next*, aby kontynuować.



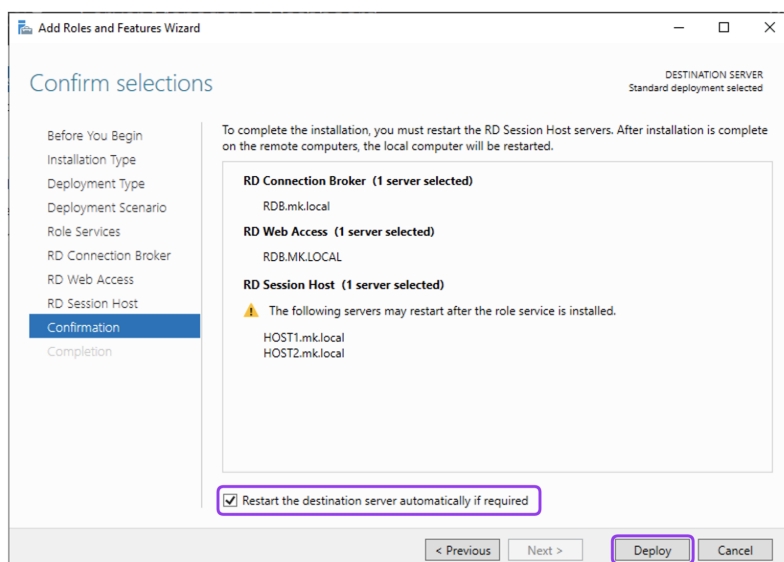
8. Na karcie *RD Web Access* wybierz odpowiedni serwer, na którym chcesz zainstalować rolę usługi *RD Web Access*. W tym przykładzie wybrano również serwer *RDB*. Kliknij *Next*, aby kontynuować.



9. Na karcie *RD Session Host* wybierz odpowiednie serwery, na których chcesz zainstalować rolę usługi *RD Session Host*. W tym przykładzie wybrano serwery *HOST1* i *HOST2*. Kliknij *Next*, aby kontynuować.



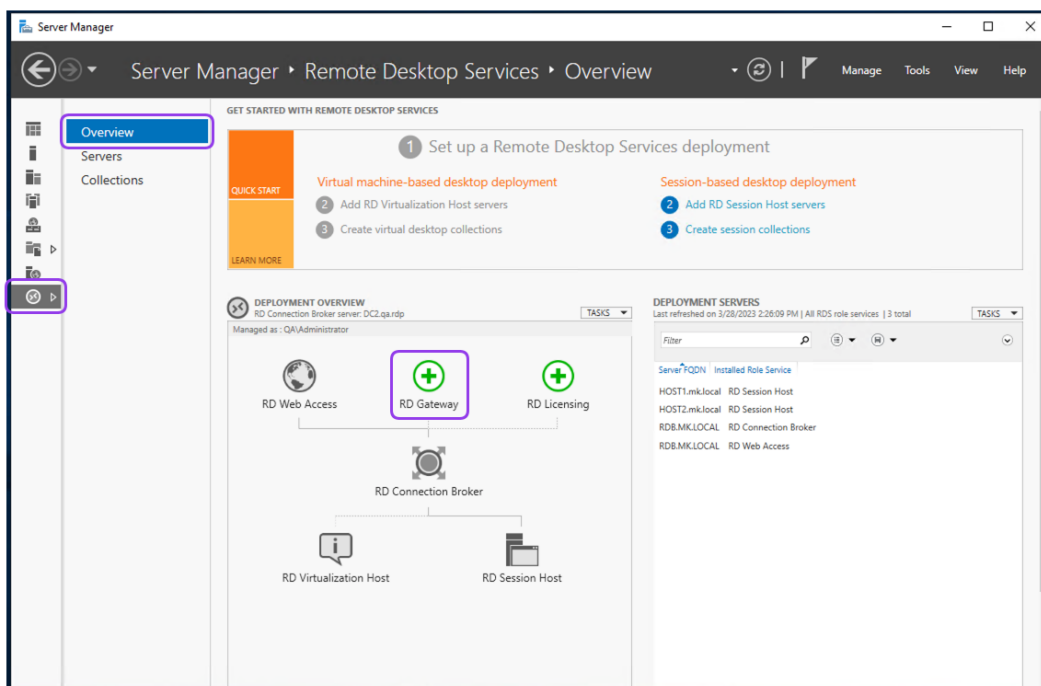
10. Na karcie *Confirmation* zaznacz *Restart the destination server automatically if required*, a następnie kliknij *Deploy*.



11. Poczekaj na pomyślne zakończenie wdrażania i kliknij *Close*.

Dodaj serwer RD Gateway i nazwę certyfikatu:

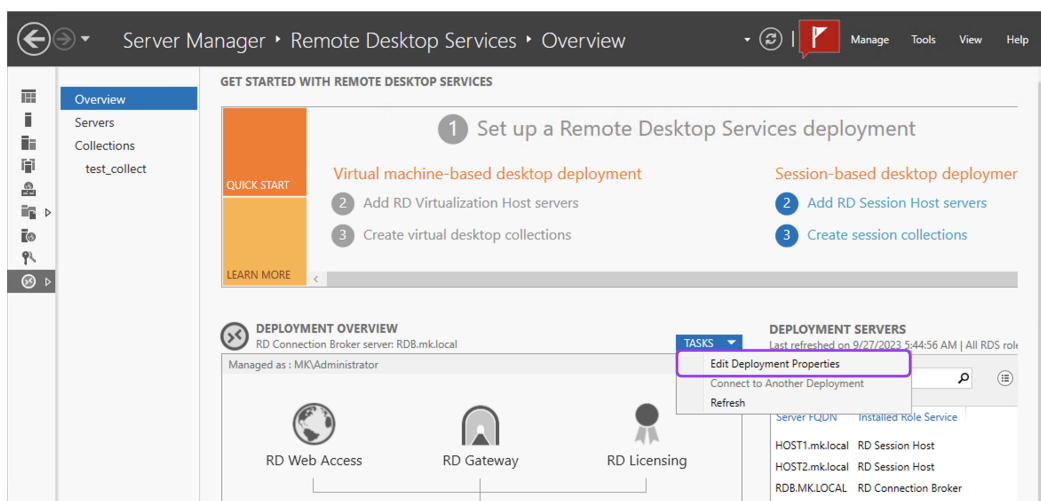
1. Z lewego menu wybierz sekcję *Remote Desktop Services* i przejdź do karty *Overview*.
2. Kliknij przycisk *+ RD Gateway* i w kreatorze *Add RD Gateway Servers wizard* wybierz maszynę wirtualną, na której chcesz zainstalować serwer RD Gateway. W tym przykładzie wybrano serwer RDB.



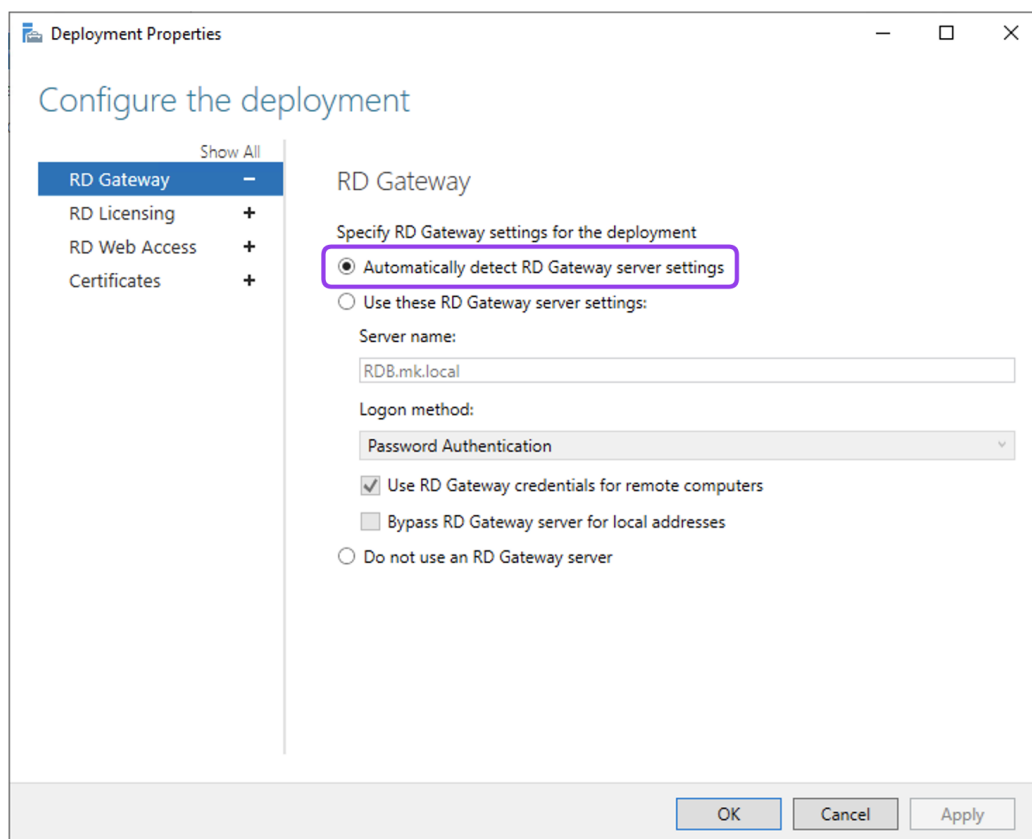
3. Kliknij *Next*.
4. Wprowadź nazwę certyfikatu SSL dla serwera RD Gateway, używając zewnętrznej, w pełni kwalifikowanej nazwy DNS (FQDN) serwera RD Gateway. Przykład, `cert.mk.local`.
5. Kliknij *Next*, a następnie *Add*.
6. Poczekaj, aż usługa roli zostanie wdrożona, i kliknij *Close*.

Konfiguracja właściwości RD Gateway i RD Licensing:

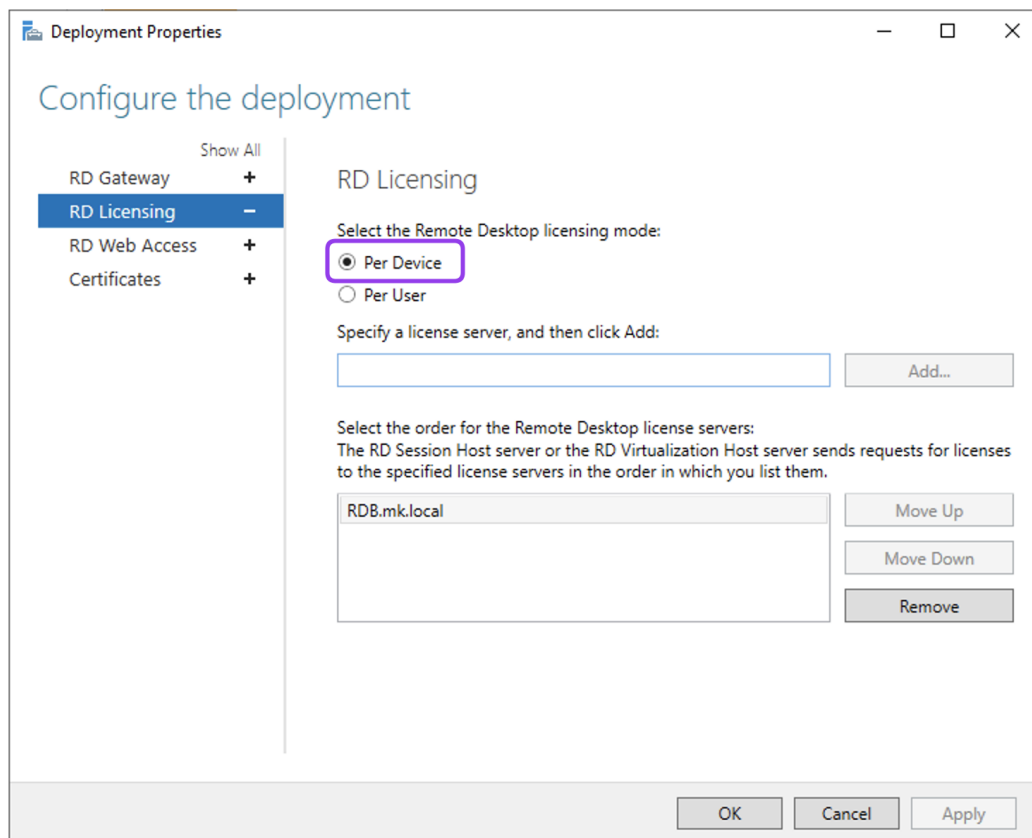
1. Wróć do karty *Overview*, kliknij *Tasks* i z listy rozwijanej wybierz *Edit Deployment Properties*.



2. Na karcie *RD Gateway* wybierz opcję *Automatically detect RD Gateway server settings* i kliknij *Apply*.

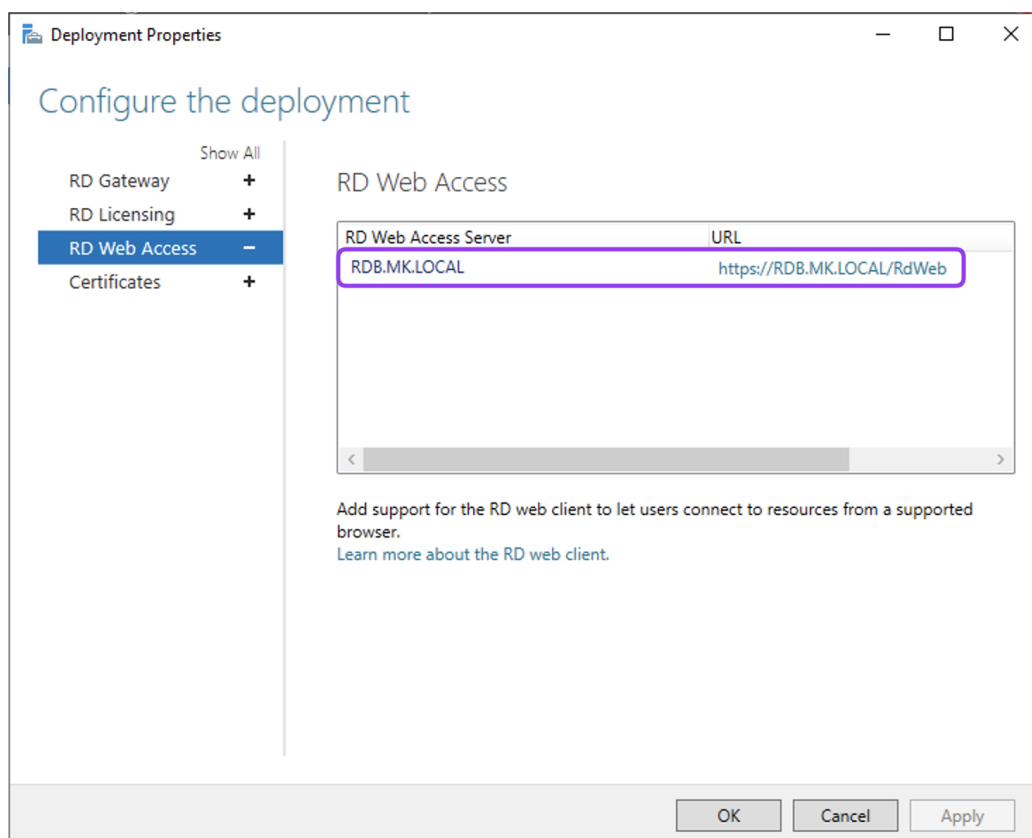


3. Rozwiń kartę *RD Licensing* i wybierz *Per Device*. Kliknij *Apply*.



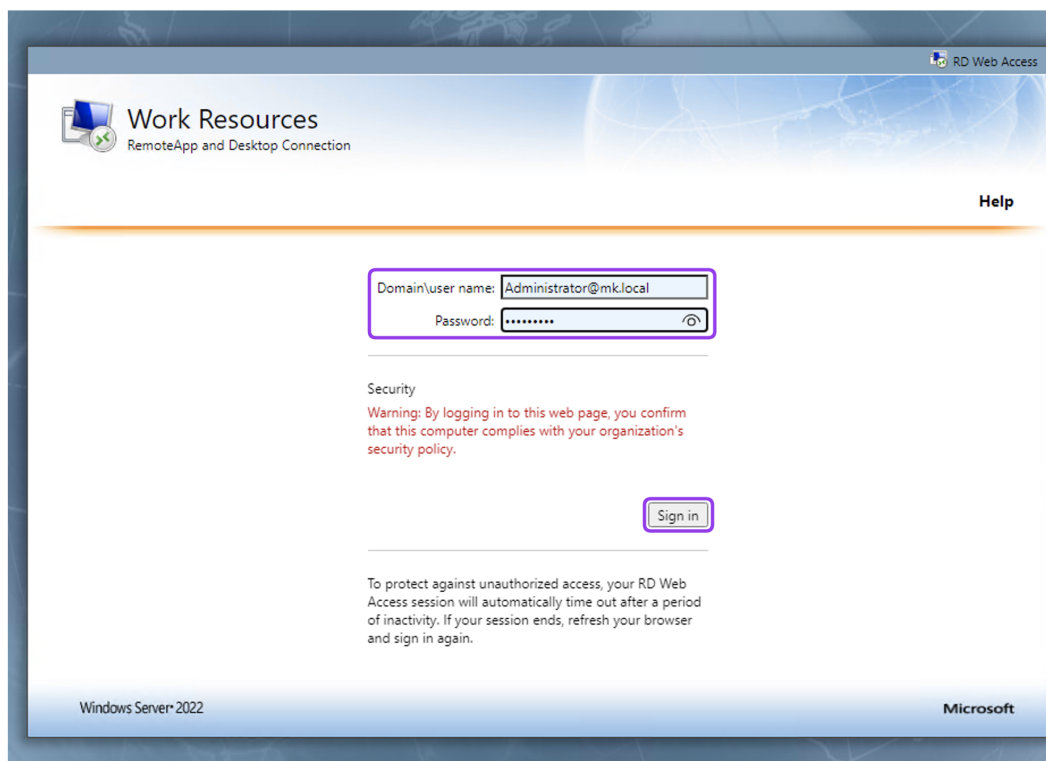
4. Rozwiń kartę «RD Web Access», aby sprawdzić adres URL dla RD Web Access

IIS. Domyślnie jest zainstalowana pod adresem /RdWeb.



5. Kliknij na wyświetlony adres URL, aby zweryfikować logowanie do RD Web Access za pomocą konta administratora.

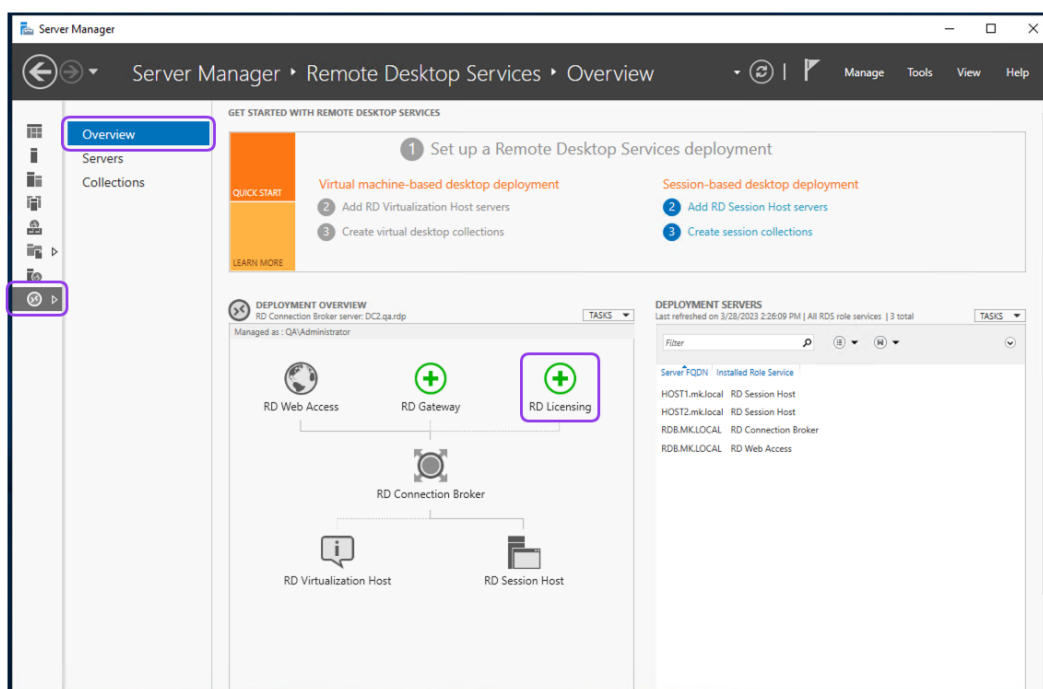
Informacja: Podczas logowania użyj domeny w polu *nazwa użytkownika*. Na przykład, Administrator@mk.local.



6. Zapisz ten adres na potrzeby kolejnych kroków konfiguracji.
7. Kliknij *OK* w oknie *Deployment Properties*, aby wrócić do karty *Przegląd* sekcji *Remote Desktop Services*.
8. Na karcie *RD Web Access* wybierz odpowiedni serwer, na którym chcesz zainstalować rolę usługi RD Web Access. W tym przykładzie wybrano również serwer RDB. Kliknij *Next*, aby kontynuować.

Dodaj RD License Server:

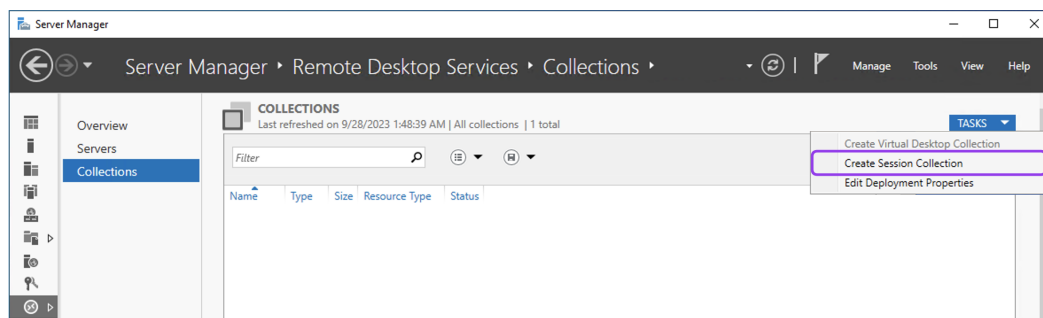
1. Kliknij przycisk *+ RD Licensing* na karcie *Overview* w sekcji *Remote Desktop Services*.



- Wybierz maszynę wirtualną, na której zostanie zainstalowany serwer licencji RD. W tym przykładzie wybrano serwer RDB. Kliknij *Next*, a następnie *Add*.
- Poczekaj, aż usługa roli zostanie wdrożona i kliknij *Close*.

Utwórz kolekcję:

- Przejdź do karty *Collections* w sekcji *Remote Desktop Services*, kliknij *Tasks* i z listy rozwijanej wybierz *Create Session Collection*.



- Na karcie *Before You Begin* kliknij *Next*.
- Na karcie *Collection Name* podaj opisową nazwę kolekcji. W tym przykładzie użyto nazwy *test-collection*. Kliknij *Next*, aby kontynuować.

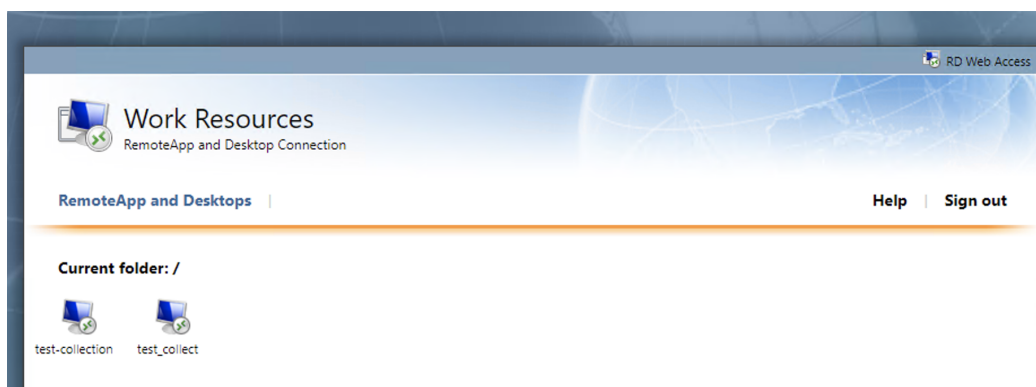
Informacja: Ta nazwa będzie wyświetlana pod ikoną w interfejsie Web Access.

- Na karcie *RD Session Host* wybierz serwery do dodania do tej kolekcji. W tym przykładzie wybrano serwery *HOST1* i *HOST2*.
- Na karcie *User Groups* zdefiniuj grupy użytkowników. Możesz zaakceptować domyślne grupy użytkowników lub dodać jedną lub więcej grup użytkowników uprawnionych do łączenia się za pomocą RDP z serwerami.

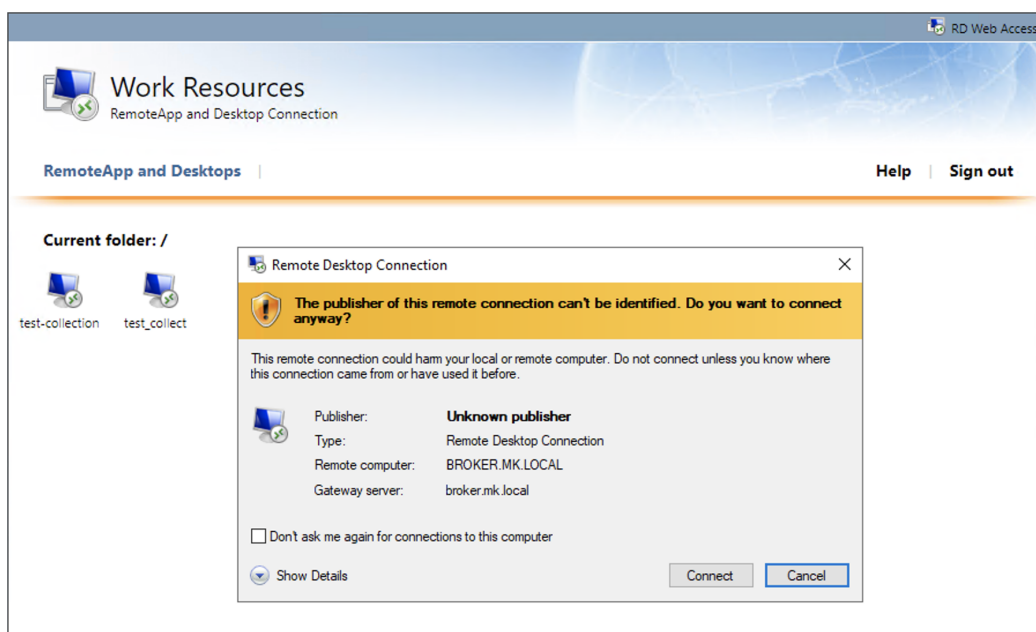
6. Na karcie *User Profile Disks* wybierz opcję *Enable User Profile Disks* i określ ustawienia, jeśli jest to konieczne. Możesz również pozostawić tę opcję wyłączoną.
7. Na karcie *Confirmation* przejrzyj wszystkie informacje, a następnie kliknij «Create».
8. Poczekaj, aż kolekcja zostanie utworzona. Kliknij *Close*.

Test połączenia:

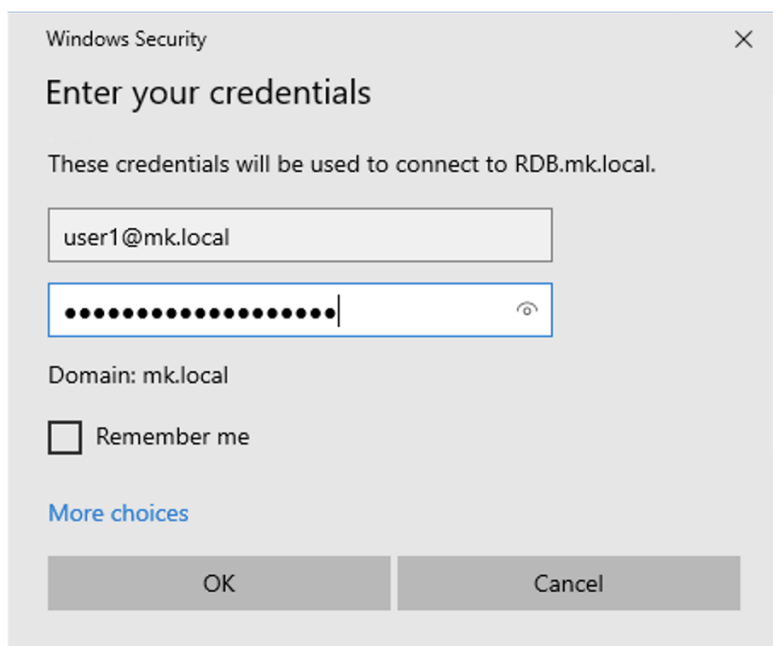
1. Otwórz zapisany wcześniej adres URL dla RD Web Access (np. `https://rdb.mk.local/RDWeb/`).
2. Wprowadź prawidłową nazwę użytkownika i hasło, a następnie kliknij *Sign in*. Możesz użyć konta administratora domeny do logowania, na przykład `Administrator@mk.local`.
3. Po zalogowaniu zostanie przedstawiona pełna kolekcja utworzonych sesji pulpitów zdalnych.



4. Kliknij na ikonę utworzonej kolekcji `test-collection`, aby pobrać plik połączenia RDP lub natychmiast nawiązać połączenie.



5. Podaj dane logowania jednego z użytkowników istniejących w domenie.



Informacja: W tej części instrukcji przedstawiono ogólny proces konfiguracji Usług pulpitu zdalnego. Aby wykorzystać funkcjonalność Fudo Enterprise podczas połączeń, należy postępować zgodnie z krokami opisanymi w kolejnej części instrukcji.

29.3.2 Konfiguracja Fudo Enterprise

Informacja: Ten przypadek użycia opisuje, jak skonfigurować Fudo Enterprise przy użyciu metody zewnętrznego uwierzytelnienia Active Directory. Należy pamiętać, że można dostosować uwierzytelnienie użytkowników za pomocą dowolnej innej metody obsługiwanej przez Fudo Enterprise, aby dopasować ją do swoich specyficznych wymagań, metod typowo stosowanych w środowisku i scenariuszy pracy.

Konfiguracja metody zewnętrznego uwierzytelnienia:

1. Zaloguj się do Panelu Administratora Fudo Enterprise.
2. Wybierz *Ustawienia > Uwierzytelnienie*.
3. W karcie **Uwierzytelnienie zewnętrzne** kliknij *Dodaj źródło zewnętrznego uwierzytelnienia*.
4. Z listy rozwijanej *Typ* wybierz *Active Directory*.
5. W polu *Adres hosta* podaj adres IP kontrolera domeny (np. 10.0.136.1).
6. Pozostaw domyślny numer portu: 389.
7. Ustaw *Adres źródłowy* na *Dowolny*.
8. Podaj nazwę domeny, która będzie używana do uwierzytelnienia użytkowników w Active Directory (np. `mk.local`).

9. W polach *Login*, *Sekret* i *Powtórz sekret* podaj dane logowania uprzywilejowanego konta używanego do dostępu do kontrolera domeny.

10. Kliknij *Zapisz*.

Utwórz użytkownika w Fudo:

1. Wybierz *Zarządzanie* > *Użytkownicy* i kliknij *+ Dodaj użytkownika*.
4. Kliknij *Zapisz*.
6. Przejdź do sekcji *Uwierzytelnienie* i z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz *Uwierzytelnienie zewnętrzne*.
7. Wybierz metodę Active Directory utworzoną w poprzednich krokach i kliknij *Zapisz*.
8. W razie potrzeby uzupełnij pozostałe parametry zgodnie z wymaganiami swojej specyficznej konfiguracji. Po więcej szczegółów zapoznaj się z sekcją *Dodawanie użytkownika*.
9. Kliknij *Zapisz* i zamknij.

Konfiguracja serwera o roli Connection Broker:

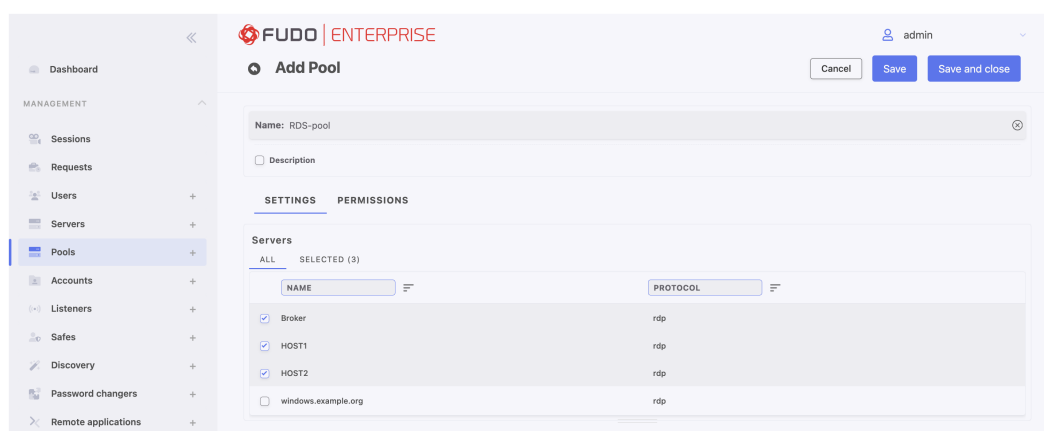
1. Wybierz *Zarządzanie* > *Serwery* i kliknij *+ Dodaj serwer*.
2. Wpisz unikalną nazwę serwera (np. *Broker*).
3. W sekcji *Uprawnienia* dodaj użytkowników uprawnionych do zarządzania tym obiektem.
4. W sekcji *Ustawienia* z listy dostępnych protokołów wybierz RDP.
5. Zaznacz opcje *TLS włączony* i *NLA włączony*.
6. W sekcji *Adres źródłowy* wybierz IPv4 i wprowadź adres IP serwera wybranego podczas konfiguracji RDS dla roli RD Broker (w naszym przykładzie serwer RDB z adresem IP 10.0.136.2).
7. Kliknij *Zapisz* i zamknij.

Konfiguracja serwerów o roli Session Hosts:

1. Wybierz *Zarządzanie* > *Serwery* i kliknij *+ Dodaj serwer*.
2. Wpisz unikalną nazwę serwera (np. HOST1).
3. W sekcji *Uprawnienia* dodaj użytkowników uprawnionych do zarządzania tym obiektem.
4. W sekcji *Ustawienia* z listy dostępnych protokołów wybierz RDP.
5. Zaznacz opcje *TLS włączony* i *NLA włączony*.
6. W sekcji *Adres źródłowy* wybierz IPv4 i wprowadź adres IP serwera (w naszym przykładzie 10.0.136.4).
7. Kliknij *Zapisz i zamknij*.
8. Powtórz wszystkie powyższe kroki, aby utworzyć drugi serwer o nazwie HOST2 i adresie IP 10.0.136.5.

Konfiguracja puli serwerów:

1. Wybierz *Zarządzanie* > *Pule* i kliknij *+ Dodaj pulę*.
2. Wpisz unikalną nazwę puli (np. RDS-pula).
3. W zakładce *Ustawienia* wybierz serwery, które mają zostać dodane do puli (np. HOST1, HOST2).
4. W sekcji *Uprawnienia* dodaj użytkowników uprawnionych do zarządzania tym obiektem (np. user1).



6. Kliknij *Zapisz i zamknij*.

Konfiguracja konta:

1. Wybierz *Zarządzanie* > *Konta* i kliknij *+ Dodaj*.
2. Zdefiniuj nazwę obiektu (np. user1).
3. Z listy rozwijanej *Typ* wybierz *forward*.
4. Przejdź do sekcji *Serwer / Pula* i z listy rozwijanej wybierz pulę utworzoną w poprzednim kroku (np. RDS-pula), aby przypisać utworzone konto do tej puli serwerów.
5. W sekcji *Dane uwierzytelniające* wybierz opcję *Przekieruj domenę* aby dołączyć nazwę domeny w ciągu identyfikującym użytkownika.

6. Kliknij *Zapisz*.

Konfiguracja gniazda nasłuchiwania:

1. Wybierz *Zarządzanie > Gniazda nasłuchiwania* i kliknij *+ Dodaj gniazdo nasłuchiwania*.
2. Wpisz unikalną nazwę gniazda nasłuchiwania (np. "rdp-broker-bastion").
3. Przejdź do zakładki *Uprawnienia* i dodaj użytkowników uprawnionych do zarządzania tym gniazdem nasłuchiwania (np. *user1*).
4. Przejdź do zakładki *Ustawienia* i w polu *Protokół* naciśnij przycisk *RDP*.
5. Zaznacz opcję *TLS włączony* aby włączyć szyfrowanie.
6. Zaznacz opcję *NLA włączony* dla dodatkowego zabezpieczenia.
7. W sekcji *Tryb połączenia* wybierz *bastion*.
8. Ustaw lokalny adres na *10.0.58.238* lub *Any*, i port *3389*.
9. W polu *Certyfikat CA* kliknij *Generuj certyfikat* aby wygenerować certyfikat TLS, lub kliknij *Prześlij* aby załadować plik certyfikatu serwera z dołączonym na końcu prywatnym kluczem.
10. Kliknij *Zapisz i zamknij*.

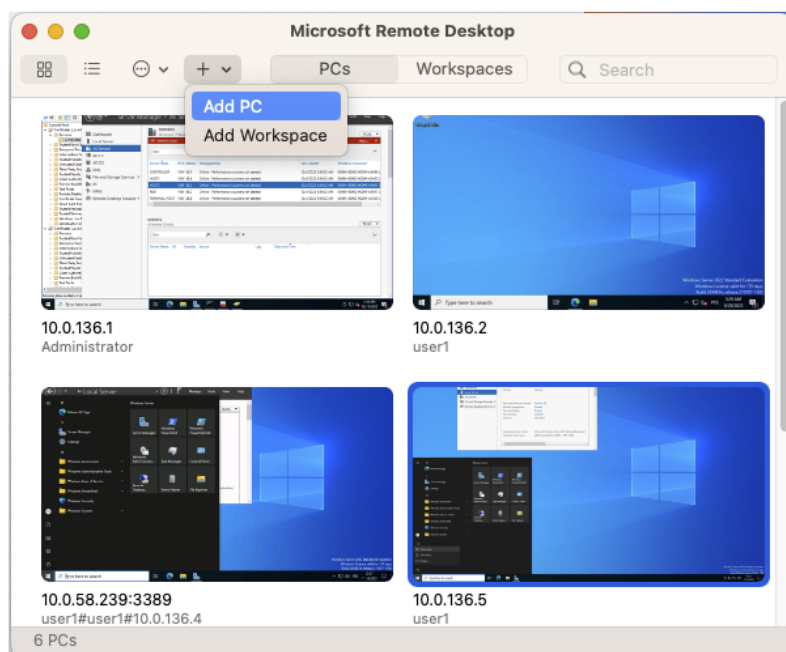
Nawiązanie sesji przez Portal Użytkownika Fudo:

Ostrzeżenie: Podczas nawiązywania połączeń za pomocą Remote Desktop Services zalecane jest korzystanie z opcji *Native client*. *Web client* nie obsługuje tego typu połączeń.

1. Zaloguj się do «Portal Użytkownika» Fudo Enterprise używając *user1* jako nazwy użytkownika i hasła skonfigurowanego dla tego użytkownika w Active Directory.
2. Najedź kursorem na nazwę konta *user1*, wybierz *Web client* i kliknij *Połącz* w celu pobrania pliku konfiguracyjnego RDP.
3. Otwórz pobrany plik, aby rozpocząć połączenie w natywnym kliencie RDP.
4. Podaj hasło użytkownika *user1*.

Przekierowanie połączenia przez Fudo w natywnym kliencie RDP:

1. Aby przekierować połączenie przez Fudo Enterprise, w trakcie konfiguracji klienta RDP musimy użyć adresu Portalu Użytkownika.
2. Wybierz ulubionego klienta protokołu RDP (jak np. Microsoft Remote Desktop) i postępuj zgodnie z jego instrukcją, aby dodać nowy komputer do połączenia.
3. Na przykładzie Microsoft Remote Desktop, kliknij ikonę plus w górnej części okna i wybierz *Dodaj komputer*.



4. W polu *Nazwa komputera* wprowadź adres IP Portalu Użytkownika Fudo Enterprise wraz z numerem portu i kliknij *Dodaj*.

Edit PC

PC name:

User account:

General | Display | Devices & Audio | Folders

Friendly name:

Group:

Gateway:

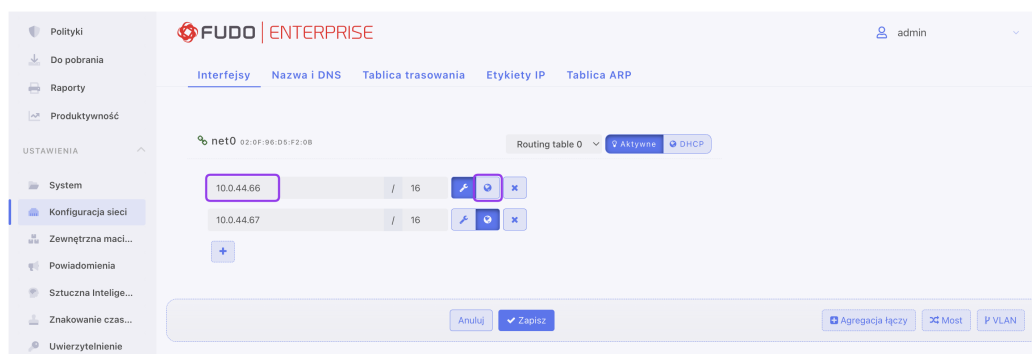
Bypass for local addresses

Reconnect if the connection is dropped

Connect to an admin session

Swap mouse buttons

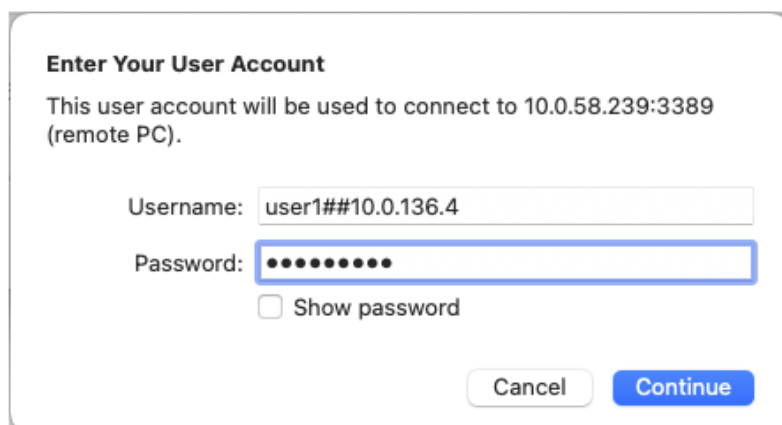
Informacja: Adres IP Portalu Użytkownika znajdziesz w zakładce *Ustawienia > Konfiguracja sieci*.



5. Połącz się z dodanym komputerem, podając w polu *Nazwa użytkownika* ciąg logowania dla połączeń bastion oraz hasło w polu *Hasło*.

Informacja:

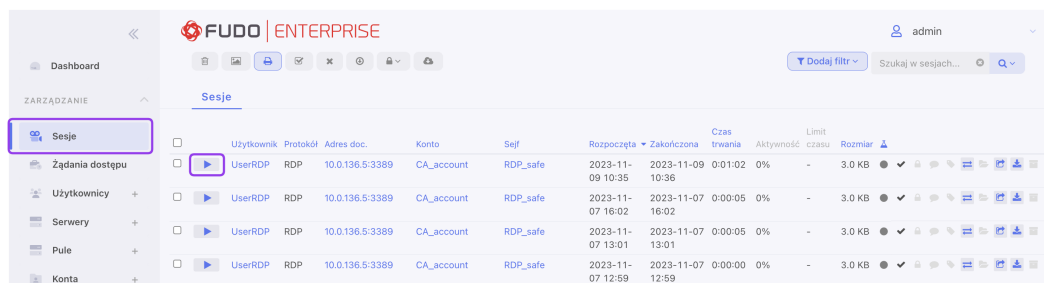
- Użyj następującego wzoru dla ciągu logowania bastion: nazwa użytkownika # login konta na docelowym serwerze # adres docelowego serwera (np. `user1#user1#10.0.136.4`).
- Można pominąć login konta, jeśli jest taki sam jak nazwa użytkownika, np. `user1##10.0.136.4`



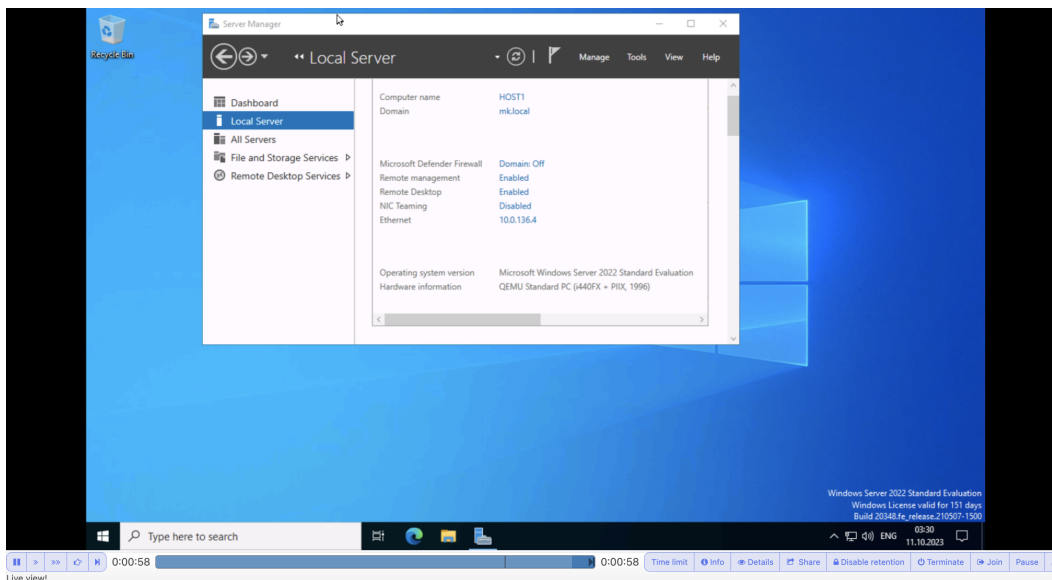
6. Klient RDP nawiąże połączenie z jednym z serwerów z kolekcji RDS.

Wyświetlanie aktywnej sesji w Panelu Administracyjnym Fudo Enterprise:

1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise.
2. Wybierz *Zarządzanie > Sesje*.
3. Znajdź żądaną sesję i kliknij ikonę odtwarzania obok niej.



	Użytkownik	Protokół	Adres doc.	Konto	Self	Rozpoczęta	Zakończona	Czas trwania	Aktywność	Limit czasu	Rozmiar
<input type="checkbox"/>	UserRDP	RDP	10.0.136.5-3389	CA_account	RDP_safe	2023-11-09 10:35	2023-11-09 10:36	0:01:02	0%	-	3.0 KB
<input type="checkbox"/>	UserRDP	RDP	10.0.136.5-3389	CA_account	RDP_safe	2023-11-07 16:02	2023-11-07 16:02	0:00:05	0%	-	3.0 KB
<input type="checkbox"/>	UserRDP	RDP	10.0.136.5-3389	CA_account	RDP_safe	2023-11-07 13:01	2023-11-07 13:01	0:00:05	0%	-	3.0 KB
<input type="checkbox"/>	UserRDP	RDP	10.0.136.5-3389	CA_account	RDP_safe	2023-11-07 12:59	2023-11-07 12:59	0:00:00	0%	-	3.0 KB



Tematy pokrewne:

- *RDP w trybie bastionu*
- *Uwierzytelnienie*
- *Integracja z serwerem CERB*

29.4 Zarządzanie certyfikatami na potrzeby połączeń RDP

Podczas *tworzenia serwera RDP* w Fudo Enterprise, można określić metodę uwierzytelnienia przy użyciu certyfikatu serwera lub certyfikatu CA. Poniższa instrukcja opisuje sposób zarządzania wymienionymi certyfikatami w środowisku Windows Server.

29.4.1 Lokalizacja certyfikatu dla protokołu RDP w Windows Server

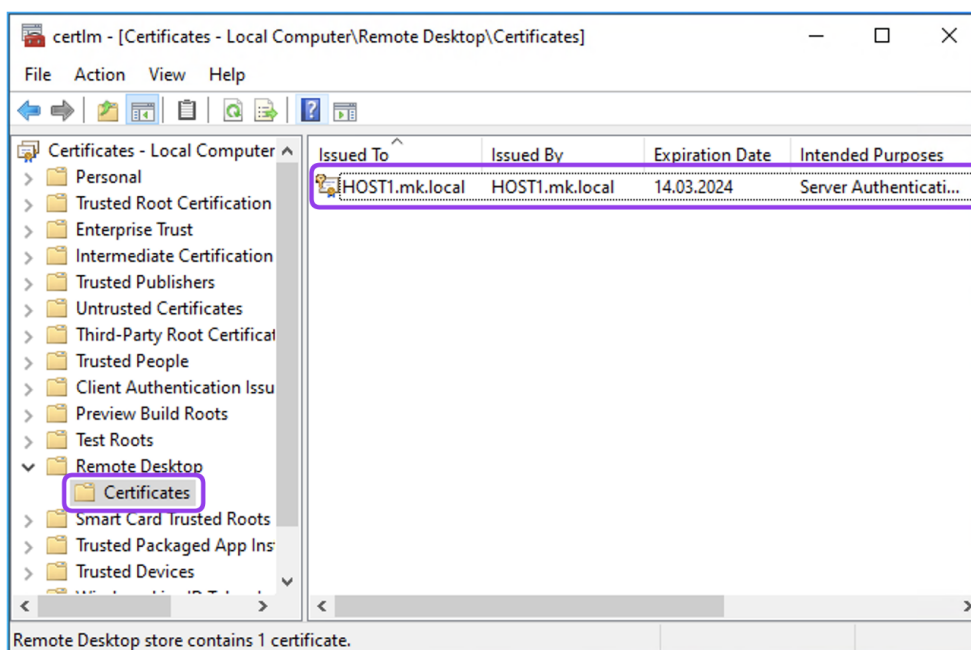
Postępuj zgodnie z jednym z poniższych scenariuszy, aby zlokalizować certyfikat pobrany przez Fudo Enterprise z Windows Server podczas tworzenia serwera RDP.

Lokalizowanie certyfikatu serwera w Menedżerze certyfikatów:

Możesz zlokalizować certyfikat pobrany przez Fudo Enterprise z Windows Server bezpośrednio w Menedżerze certyfikatów. Aby wyświetlić certyfikat, wykonaj poniższe kroki:

1. Wybierz *Run* z *Start menu* w Windows Server, a następnie wpisz `certlm.msc`.

- Wyświetli się okno Menedżera certyfikatów dla lokalnego urządzenia.
- Aby wyświetlić swój certyfikat, przejdź do *Remote Desktop* > *Certificates* w sekcji *Certificates - Local Computer* w lewym panelu okna Menedżera certyfikatów.



Lokalizacja certyfikatu serwera po numerze seryjnym:

Możesz również zlokalizować certyfikat używany przez Fudo Enterprise, wyodrębniając jego numer seryjny.

- Po kliknięciu przycisku *Pobierz certyfikat*, Fudo Enterprise łączy się z określonym adresem i portem w celu pobrania certyfikatu. Podobną akcję można wykonać z wiersza poleceń, wywołując poniższą komendę:

```
openssl s_client -connect adres:port
```

Example:

```
openssl s_client -connect 10.0.133.4:3389
```

- W odpowiedzi otrzymasz certyfikat, z którego możesz wyodrębnić numer seryjny, wpisując poniższe polecenie i podając otrzymaną zawartość certyfikatu:

```
c x509 -noout -serial

-----BEGIN CERTIFICATE-----
MIICHbdygdu656sdf65ac55mpn1PmpBK/
↪70WFeh+xjANBqkqhkIG9wOBAQsFADAZ
MRcwFQYDVQQDEw5IT1NUMS5tay5sb2NhbDAeFw0yMzaA5MTMxNzA2NTRAfw0yNDZM
MTQxNzA2NTRAmbkxZAVcas7c6c6sh83uydtLm1rLmxvY2FsMIIBIjANBqkqhkIG
9wOBAQEFAAOCAQ8AMIIBCgKCAQEANgYkoMa4dgLgG11+G+m2UEAIH/
↪6ttyQep5u
tUYkxKeuqpn9AWnYP8To1fornJN387ddhcy76d7jchc8Q093RWVb2cMKKjg0AW9w
qLFW+WrlEUPY8hYvsCFYgFH3H0HhKLEoWBN5qHH7vjIiW3Rb0Y7xeGb9x0FWItQX
mbF6sucGdlH+0sJepxMLPVh3Qpb2WQ18kSQGyS1ocbJxOWST9sH4MQkRVFL3rkxN
(ciąg dalszy na następnej stronie)
```

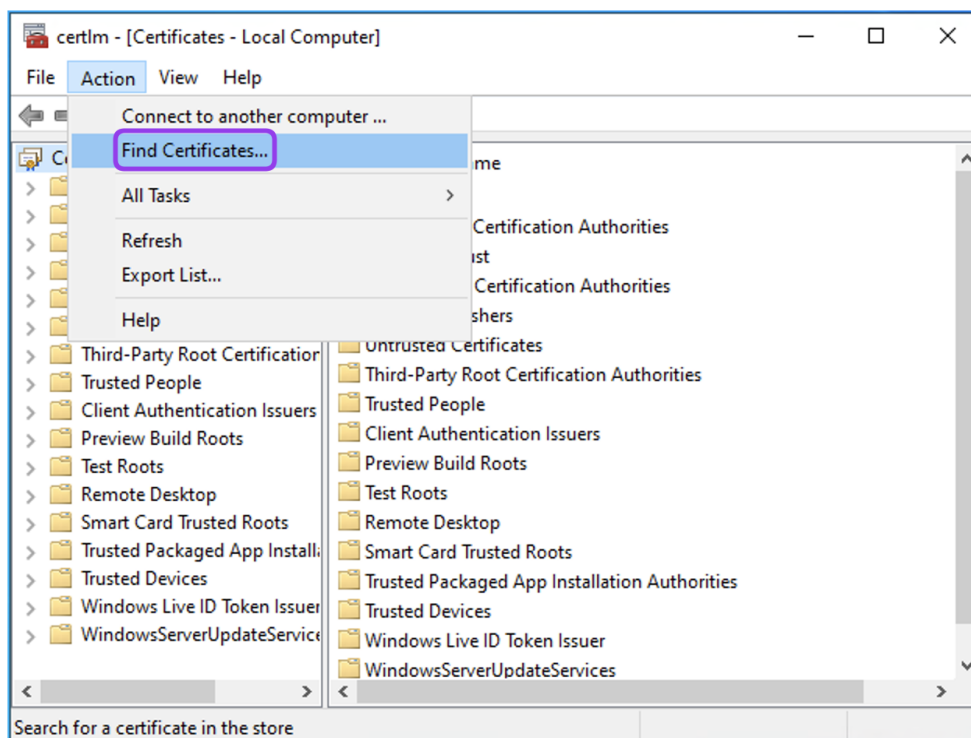
(kontynuacja poprzedniej strony)

```
f7/
↔qdJcdM6sFxEJTdp30CITRfbORXac184bStjW2MJzvJRqr94xDHonRdIM9tUka
06LVJQY6qiEpMVE8MpSDAfoZ+HeyVWt+2EfX1fWE4hiMJP1DoQIDAQABoyQwIjAT
BgNVHSUEDDAKBggrBgEFBQcDATA LBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQAD
ggEBAGNXzwnC4Dh0xyaVhVTPePsa97aeWJtp164cE4/ZdAfGBEIfH1BEh/
↔Tnrrn2
7pr0jLnCjUq9rxHC6jfMR0U2PT4qrMHvGD1nUwZdHuZPavPLFHh/
↔rYHZpizoS+9W
ggEBAGNXzwnC4Dh0xyaVhVTPePsa97aeWJtp164cE4/ZdAfGBEIfH1BEh/
↔Tnrrn2
xyXjeYdX8/U9EdgrXOLGX9U74rfGQTrQxZyjuY1Gxxqop/
↔y2V3n+3NnNzY+ehW1G
ggEBAGNXzwnC4Dh0xyaVhVTPePsa97aeWJtp164cE4/ZdAfGBEIfH1BEh/
↔Tnrrn2
ZUvdUnqtdH+ODdAWBo4P1dv0nL8=
-----END CERTIFICATE-----
```

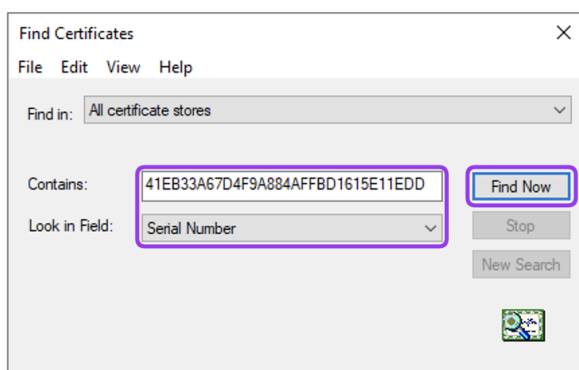
3. W odpowiedzi wyodrębniony zostanie numer seryjny, który możesz wykorzystać do wyszukania certyfikatu w Menedżerze certyfikatów.

```
serial=41EB33A67D4F9A884AFFBD1615E11EDD
```

4. Skopiuj wyodrębniony numer seryjny i przejdź do Windows Server.
5. Wybierz *Run* z *Start menu*, a następnie wpisz *certlm.msc*, aby otworzyć Menedżer certyfikatów.
6. Przejdź do *Action > Find Certificates...*



7. Wpisz skopiowany numer seryjny w polu *Contains* i z rozwijanego menu *Look in Field* wybierz *Serial Number*.



8. Kliknij *Find Now*.

29.4.2 Dostarczanie certyfikatu CA

Informacja:

- Jest to poglądowy przewodnik przedstawiający podstawową konfigurację CA dla protokołu RDP. Opisane kroki mogą różnić się w zależności od początkowych ustawień środowiska, w którym pracujesz.
- Aby przygotować certyfikat CA do użycia w Fudo Enterprise, konieczne jest skonfigurowanie CA (Certificate Authority) wraz z szablonem RDP do wydawania certyfikatów.

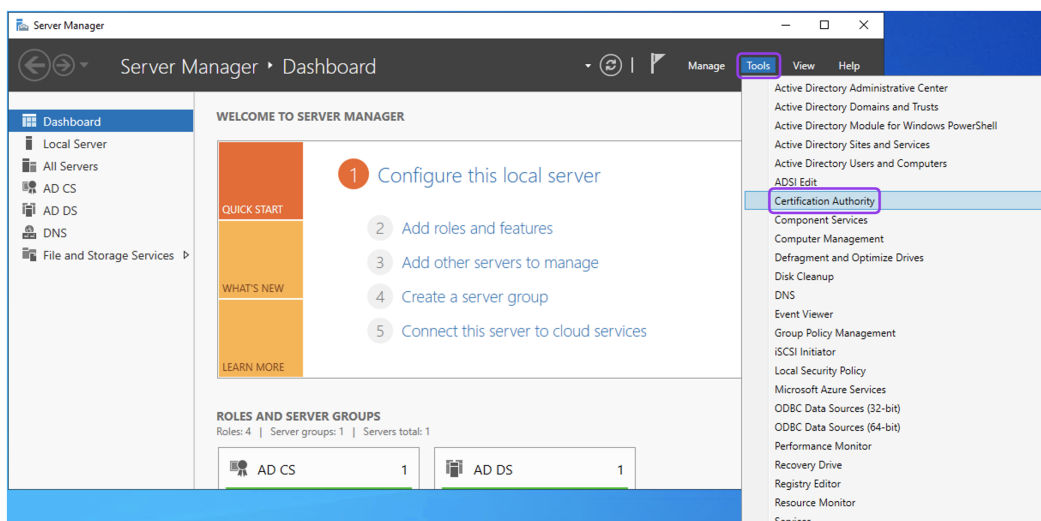
Instalacja Certificate Authority w Windows Server:

Aby zainstalować *Certificate Authority* w Windows Server, postępuj zgodnie z instrukcją Windows Server.

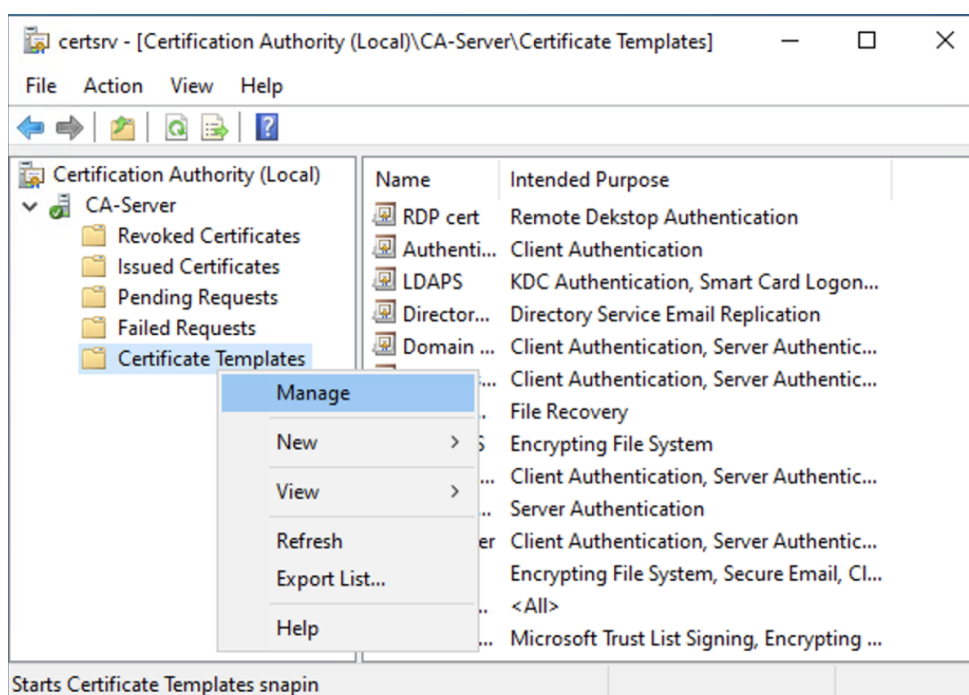
Informacja: W procedurze opisanej poniżej wykorzystano opcję *Enterprise CA*.

Tworzenie szablonu dla certyfikatu RDP:

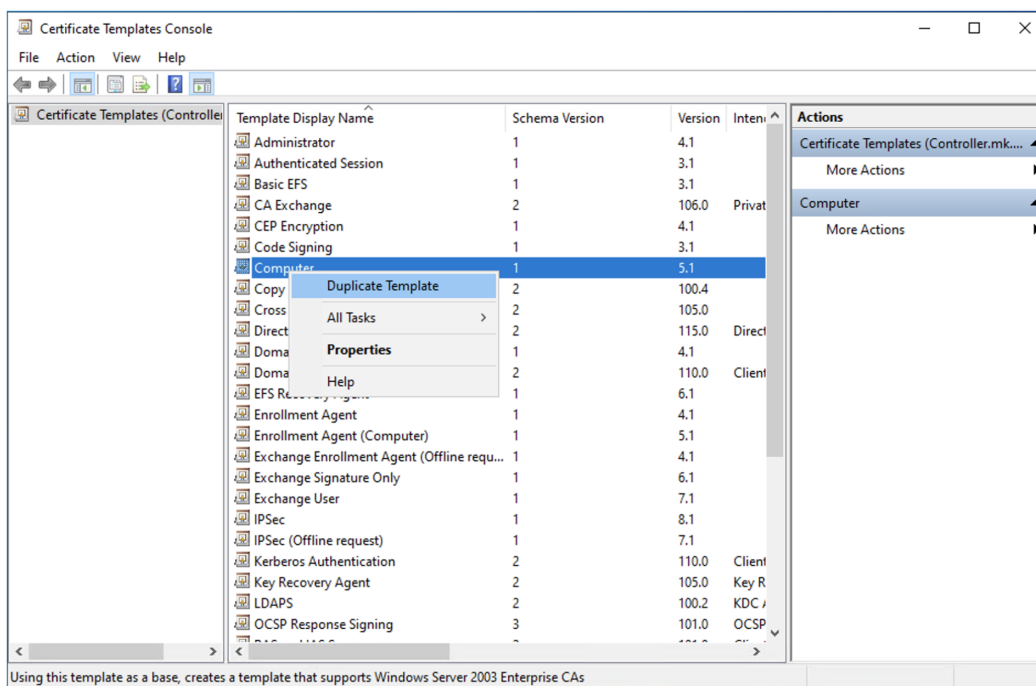
1. Otwórz *Certificate Authority* z poziomu narzędzia *Server Manager*, klikając *Tools > Certification Authority* w prawym górnym rogu okna.



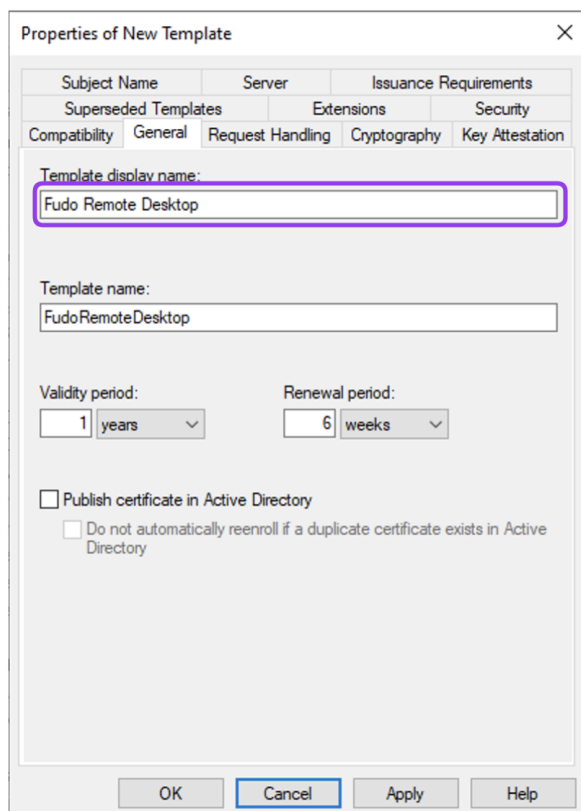
2. Kliknij prawym przyciskiem myszy na *Certificate Templates* i wybierz *Manage*.



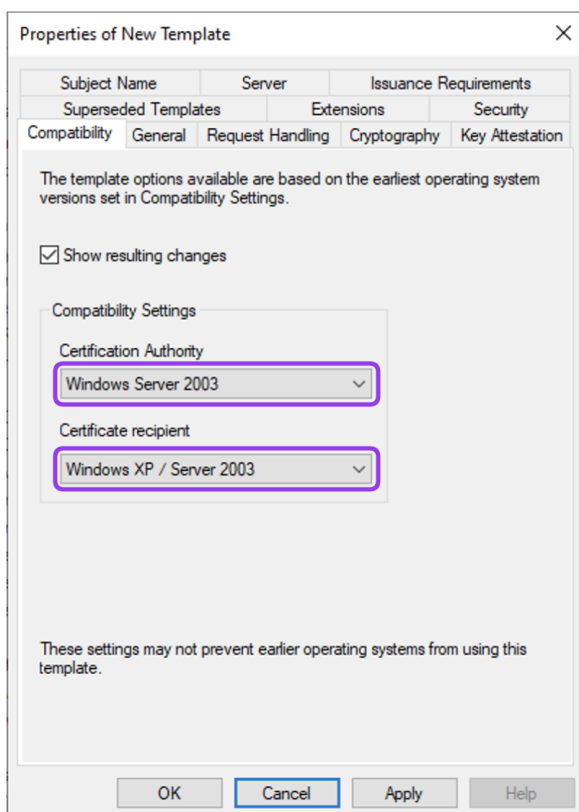
3. Znajdź szablon *Computer*, kliknij na nim prawym przyciskiem myszy i wybierz *Duplicate Template*.



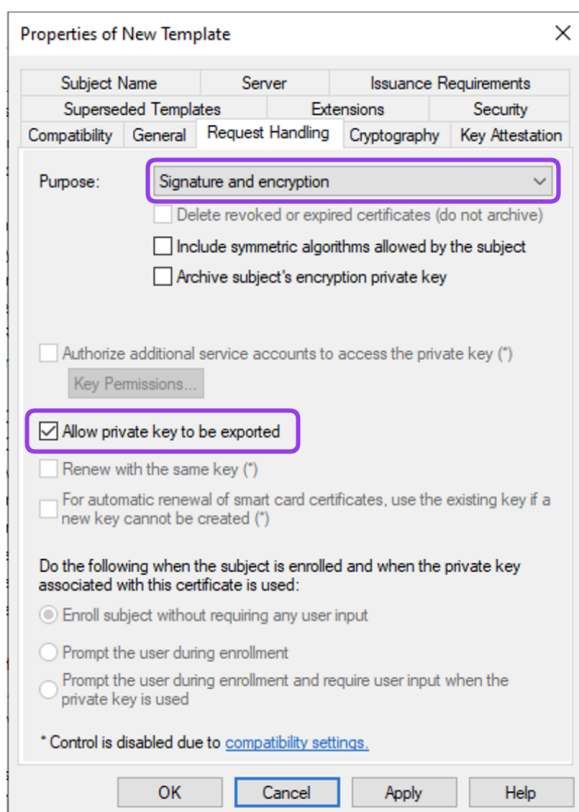
4. W zakładce *General*, wprowadź nazwę dla nowego szablonu oraz określ okres ważności i odnawiania według potrzeb.

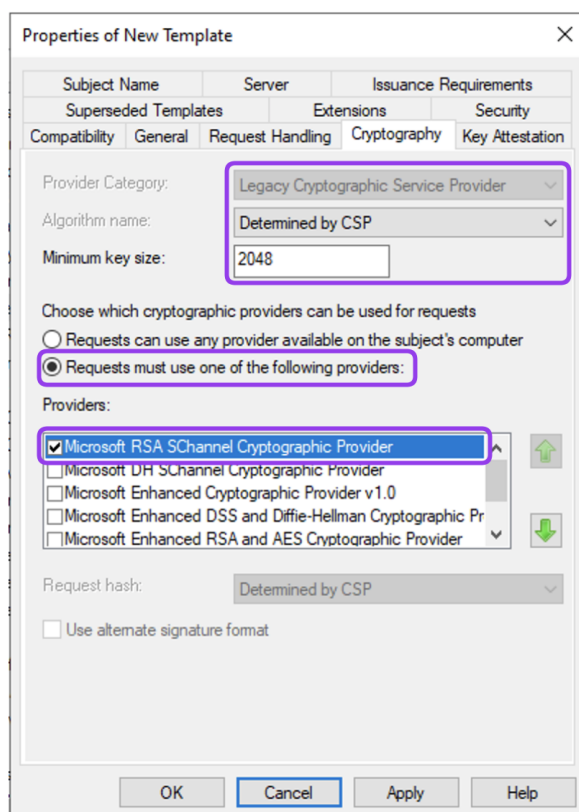


5. W zakładce *Compatibility*, z listy rozwijanej *Certification Authority* wybierz *Windows Server 2003*, natomiast z listy rozwijanej *Certificate recipient* wybierz *Windows XP/Server 2003*.

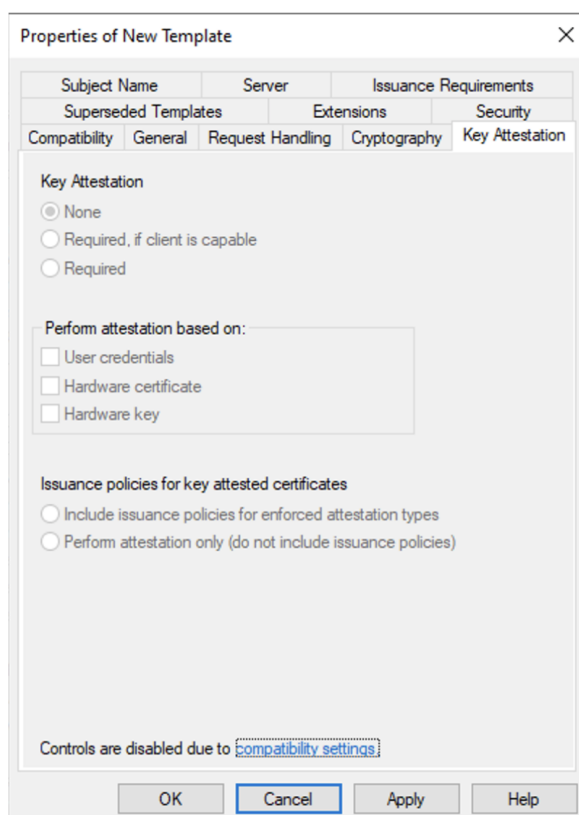


6. W zakładce *Request Handling*, ustaw *Purpose* na *Signature and encryption* i zaznacz opcję *Allow private key to be exported*.

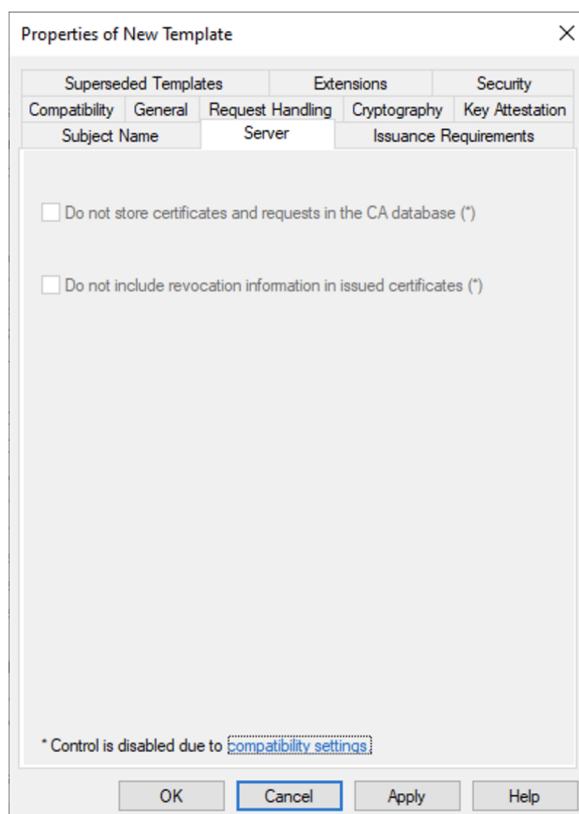




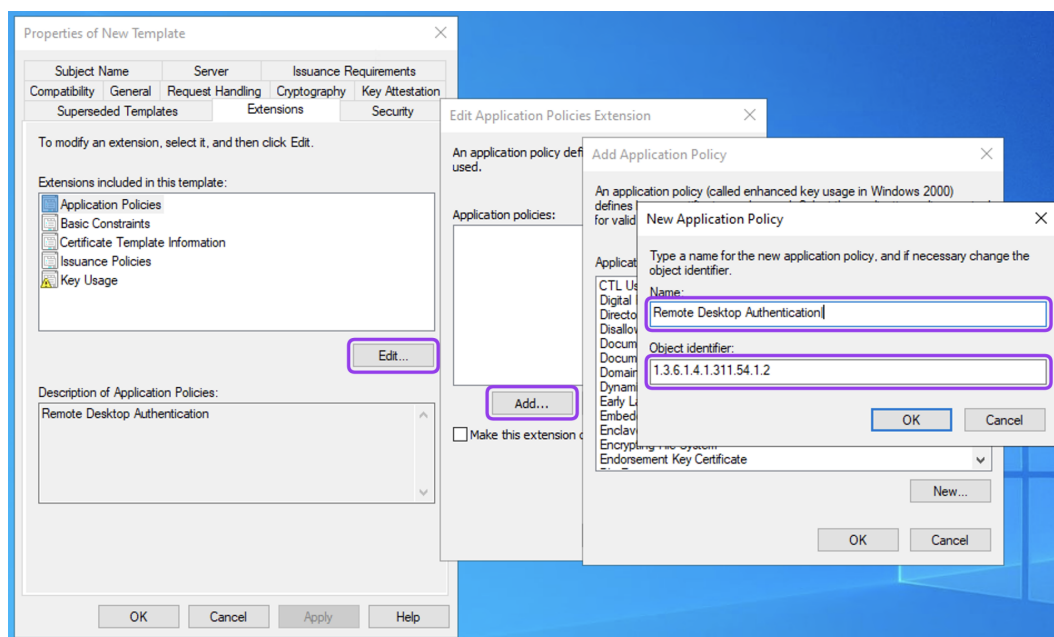
8. W zakładce *Key Attestation* pozostaw ustawienia domyślne.



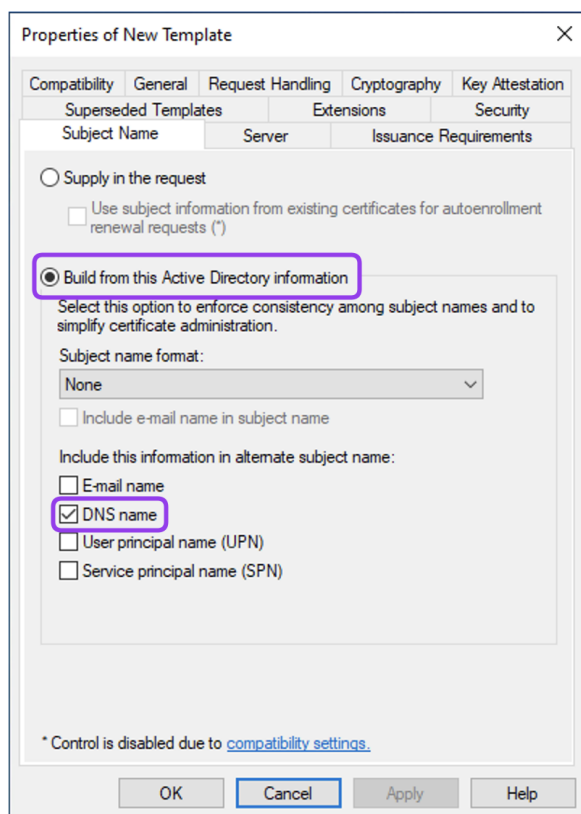
9. W zakładce *Server* pozostaw ustawienia domyślne.



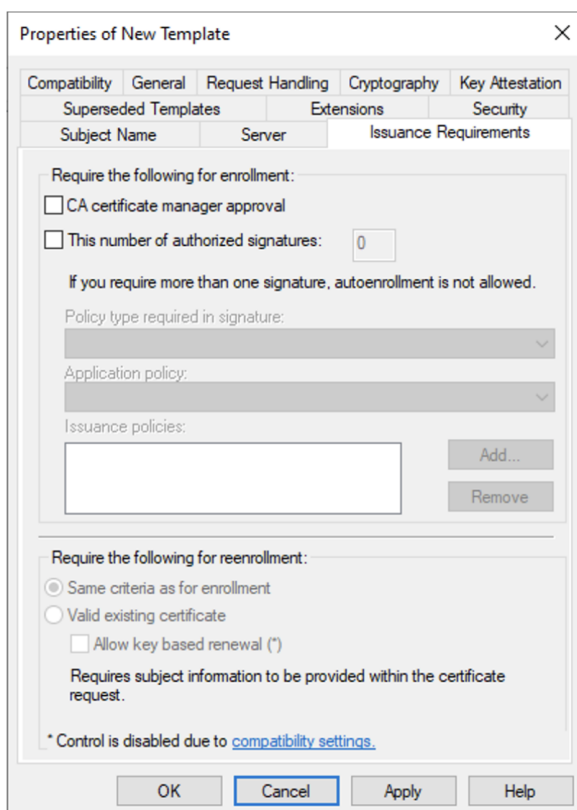
10. W zakładce *Security* dodaj komputery i grupy, które mają być uprawnione do używania tego szablonu. Sprawdź, czy grupa lub użytkownik, którego używasz, ma włączone uprawnienia *Read*, *Write* i *Enroll*. Jest to konieczne do żądania certyfikatu przy użyciu tego szablonu w następnych krokach.
11. W zakładce *Extensions* edytuj *Application Policies*.
12. Usuń polityki *Server Authentication* i *Client Authentication*.
13. Dodaj nową politykę klikając *Add*, a następnie *New*.
14. W polu *Name* wprowadź *Remote Desktop Authentication* a w polu *Object identifier* wpisz *1.3.6.1.4.1.311.54.1.2*.



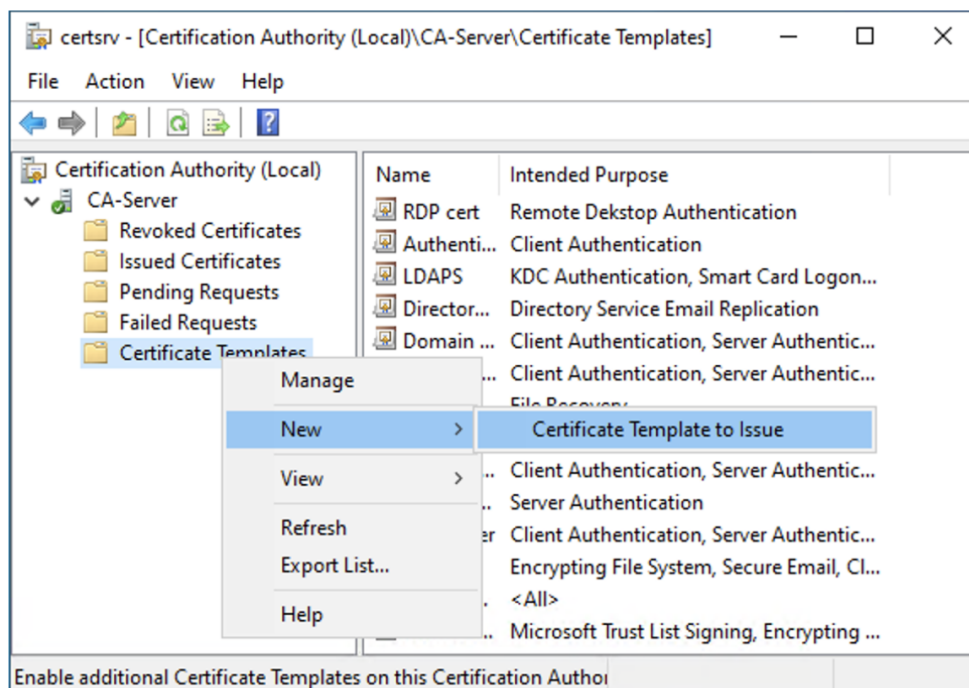
15. Kliknij trzy razy *OK*, aby wrócić do okna *Properties of New Template*.
16. W zakładce *Subject Name* wybierz opcję *Build from this Active Directory information* i następnie *DNS name*.



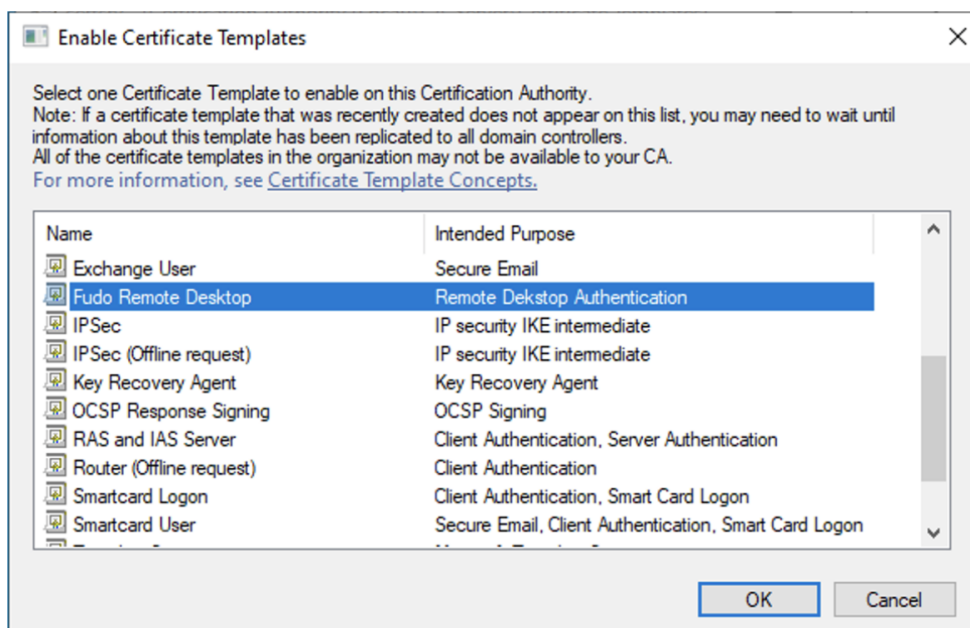
17. W zakładce *Issuance Requirements*, pozostaw ustawienia domyślne.



18. Kliknij *OK*, aby zapisać utworzony szablon. Zamknij *Certificate Templates Console*.
19. Wróć do okna *Certification Authority*, kliknij prawym przyciskiem myszy na *Certificate Templates* i wybierz *New > Certificate Template to Issue*.

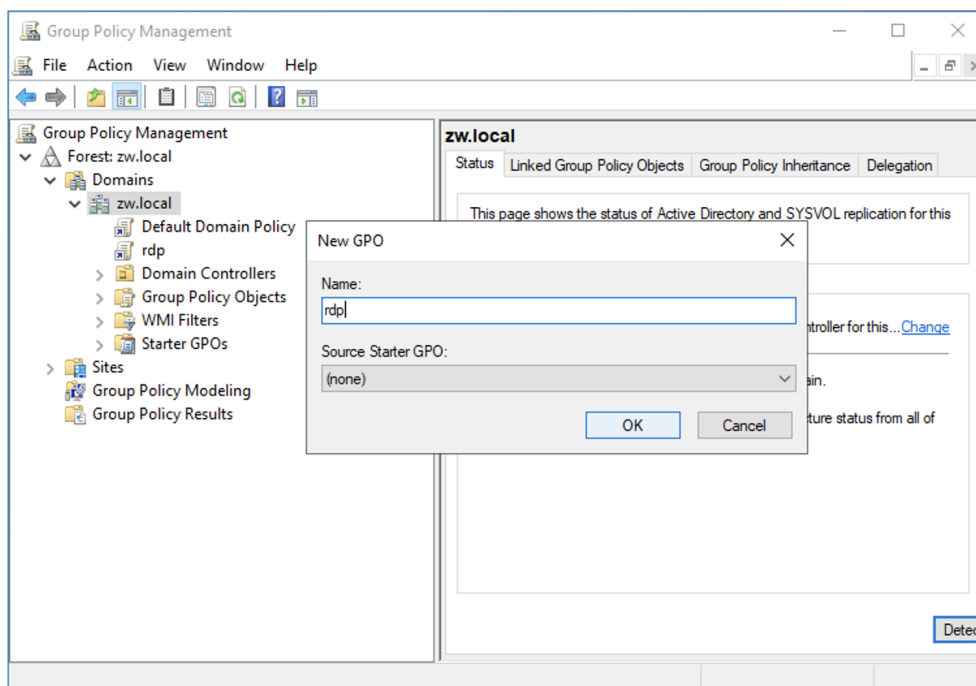


20. Wybierz utworzony szablon i kliknij *OK*.



Konfiguracja GPO:

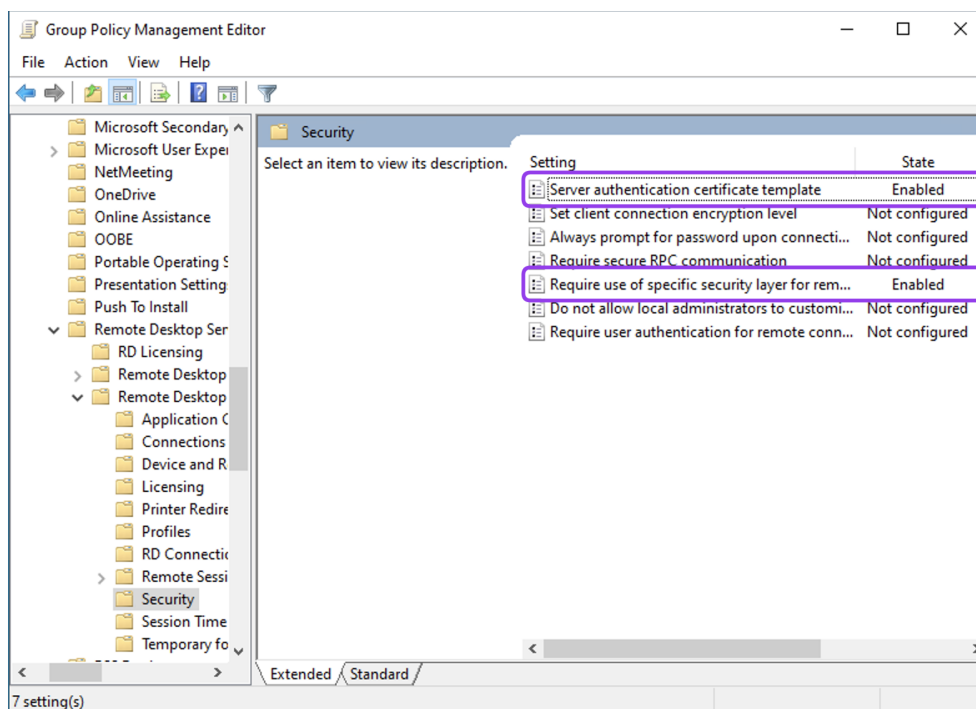
1. Naciśnij Win + R, wpisz `gpmc.msc`, i wciśnij *Enter*, aby otworzyć okno menedżera *Group Policy Management*.
2. Utwórz nowy *Group Policy Object (GPO)* lub przejdź do *GPO*, który zamierzasz edytować. W tym przykładzie utworzymy nowy obiekt.
3. Kliknij prawym przyciskiem myszy na nazwę domeny i wybierz *Create a GPO in this domain, and Link it here...*
4. Podaj nazwę dla nowego *GPO* (np. `rdp`) i kliknij *OK*.



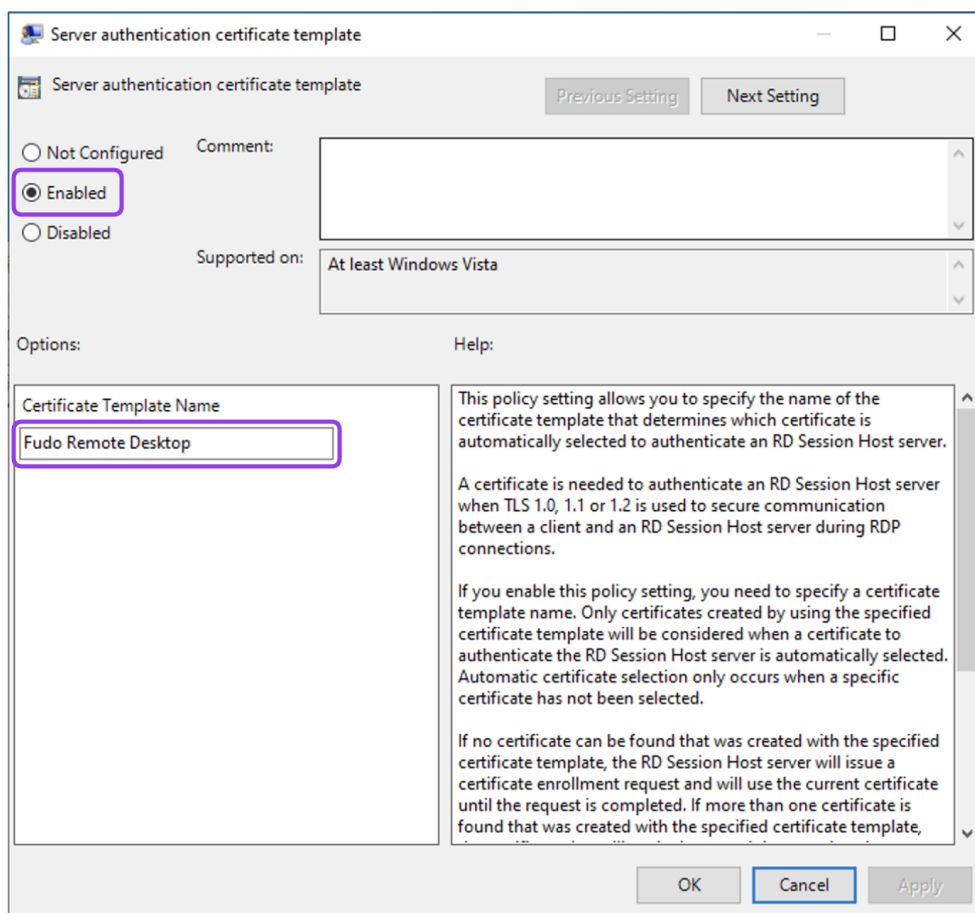
5. Kliknij prawym przyciskiem myszy na nazwę utworzonego *GPO* i wybierz

Edit. . .

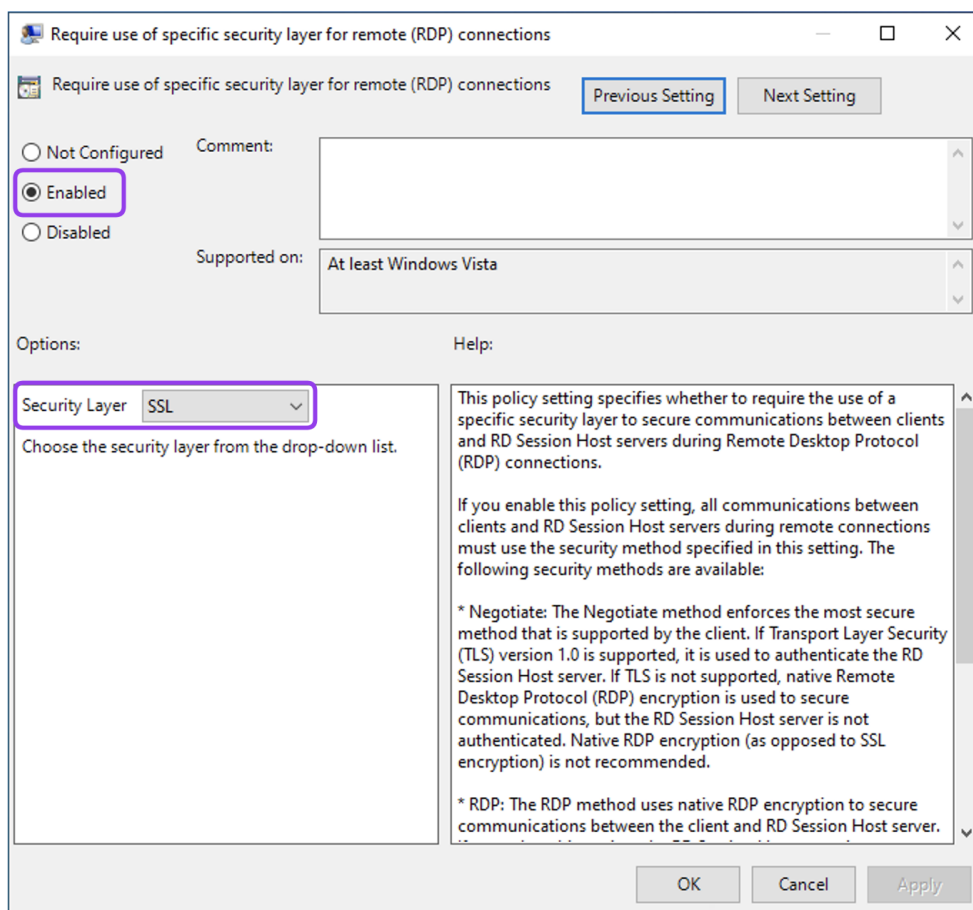
6. W *Group Policy Management Editor* przejdź do *Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security*.
7. Kliknij dwukrotnie na *Server authentication certificate template*, aby edytować to ustawienie.



8. Wybierz opcję *Enabled* i w polu *Certificate Template Name* wprowadź nazwę szablonu utworzonego w poprzednich krokach.



9. Kliknij *OK*.
10. Kliknij dwukrotnie na *Require use of specific security layer for remote (RDP) connections*, aby edytować to ustawienie.
11. Wybierz opcję *Enabled*, a następnie *SSL* z menu rozwijanego *Security Layer*.



12. Kliknij *OK*.
13. Powiąż GPO z jednostką organizacyjną (OU) zawierającą serwery / komputery stacjonarne, które wymagają certyfikatów RDP, jeśli jest to wymagane w Twoim środowisku. Polityki zostaną automatycznie zarejestrowane, gdy zaktualizowane zostaną polityki grupowe (Group Policy).

Rejestracja certyfikatu RDP:

1. Naciśnij *Win + R*, wpisz *certlm.msc* i naciśnij *Enter*, aby otworzyć narzędzie *Certificate Manager* dla lokalnego urządzenia.
2. Przejdź do *Personal > Certificates*.
3. Kliknij prawym przyciskiem myszy w oknie menedżera i wybierz *All Tasks > Request New Certificate...*
4. Kliknij *Next* w zakładkach *Before You Begin* i *Select Certificate Enrollment Policy*.
5. W zakładce *Request Certificate* wybierz szablon utworzony w poprzednich krokach i kliknij *Enroll*.
6. Skopiuj zarejestrowany certyfikat do katalogu *Trusted Root Certification Authorities > Certificates*.

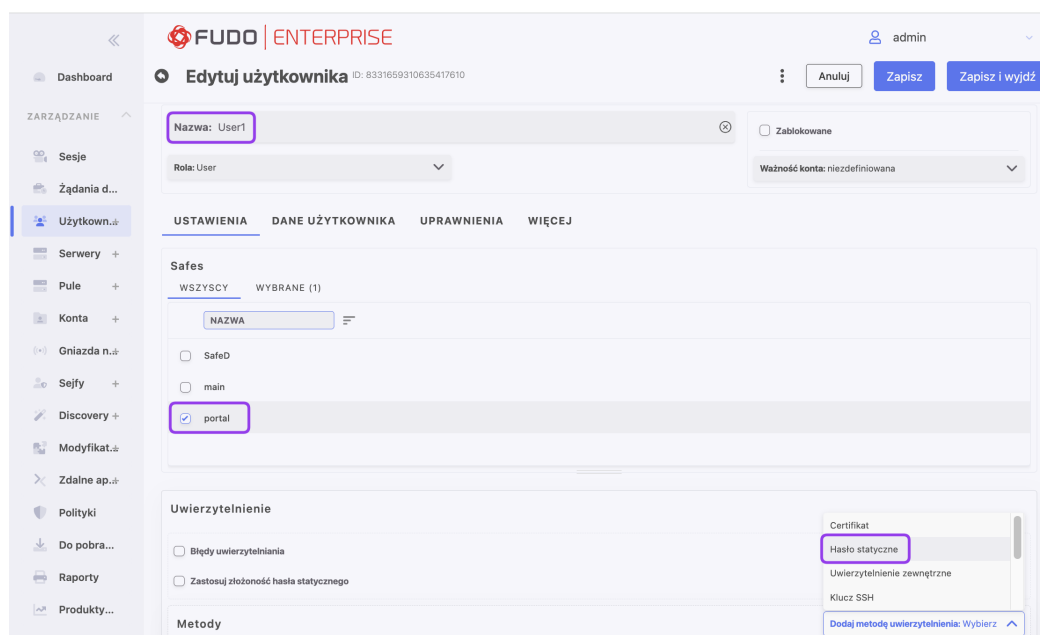
Eksport certyfikatu CA:

1. Naciśnij *Win + R*, wpisz *certlm.msc* i naciśnij *Enter*, aby otworzyć narzędzie *Certificate Manager* dla lokalnego urządzenia.

2. Przejdź do *Trusted Root Certification Authorities > Certificates*.
3. Kliknij prawym przyciskiem myszy na główny certyfikat CA (Root Certification Authority) i wybierz *All Tasks > Export...*
4. Kliknij *Next*.
5. Wybierz format *Base-64 encoded X.509 (.CER)* i kliknij *Next*.
6. Określ nazwę i lokalizację dla eksportowanego certyfikatu.
7. Kliknij *Next* i *Finish*, aby zapisać plik.

Utworzenie użytkownika w Fudo:

1. Wybierz *Zarządzanie > Użytkownicy*, a następnie kliknij *+ Dodaj użytkownika*.
2. Wprowadź nazwę użytkownika (np. *User1*).
3. W zakładce *Ustawienia*, w sekcji *Sejfy*, wybierz *portal*.
4. Kliknij *Zapisz*.
5. Przejdź do sekcji *Uwierzytelnienie* i z rozwijanej listy *Dodaj metodę uwierzytelnienia* wybierz *Hasło statyczne*.



6. Wprowadź hasło i kliknij *Zapisz*.
8. Uzupełnij pozostałe parametry według własnych wymagań (jeśli wymagane). W tym celu możesz zapoznać się z treścią rozdziału *Dodawanie użytkownika*.
9. Kliknij *Zapisz i zamknij*.

Konfiguracja serwera RDP:

1. Wybierz *Zarządzanie > Serwery*, a następnie kliknij *+ Dodaj serwer*.
2. Wprowadź unikalną nazwę serwera (np. *ServerRDP*).
3. W zakładce *Uprawnienia*, dodaj użytkowników upoważnionych do zarządzania tym obiektem.

4. W zakładce *Ustawienia* z listy dostępnych protokołów wybierz RDP.
5. Zaznacz opcje *TLS włączony* i *NLA włączony*.
6. W sekcji *Miejsce przeznaczenia* wybierz IPv4 i wprowadź adres IP serwera, dla którego chcesz skonfigurować połączenie RDP.
7. W sekcji *Weryfikacja serwera* wybierz *Certyfikat CA* i załaduj wyeksportowany plik certyfikatu CA.

The screenshot shows the 'Dodaj serwer' (Add server) configuration page in the Fudo Enterprise interface. The 'Protokół' (Protocol) section has 'RDP' selected. Under 'Włączony' (Enabled), 'TLS włączony' (TLS enabled) and 'NLA włączony' (NLA enabled) are checked. In the 'Miejsce przeznaczenia' (Destination) section, 'IPv4' is selected. In the 'Weryfikacja serwera' (Server verification) section, 'Certyfikat CA' (CA Certificate) is selected. A button 'Załaduj lub przeciągnij plik tutaj' (Load or drag file here) is highlighted.

8. Kliknij *Zapisz i zamknij*.

Konfiguracja konta:

1. Wybierz *Zarządzanie* > *Konta*, a następnie kliknij *+ Dodaj*.
2. Zdefiniuj nazwę obiektu (np. *CA-account*).
3. Z rozwijanej listy *Typ* wybierz *regular*.
4. Przejdź do sekcji *Serwer / Pula* i z listy rozwijanej wybierz serwer utworzony w poprzednim kroku (np. *ServerRDP*), aby przypisać utworzone konto do tego serwera.
5. W sekcji *Dane uwierzytelniające* podaj *Domenę* i *Login* używane do uwierzytelnienia na serwerze.
6. Z rozwijanej listy *Zastęp sekret* wybierz opcję *hasłem* i podaj hasło używane do uwierzytelnienia na serwerze.
7. Kliknij *Zapisz*.

Konfiguracja gniazda nasłuchiwania:




1. Wybierz *Zarządzanie* > *Nasłuchiwanie*, a następnie kliknij *+ Dodaj nasłuchiwanie*.
2. Wprowadź unikalną nazwę nasłuchiwania (np. *RDP-bastion*).

- Przejdź do zakładki *Uprawnienia* i dodaj użytkowników upoważnionych do zarządzania tym gniazdem nasłuchiwania (np. **User1**).
- Przejdź do zakładki *Ustawienia* i w polu *Protokół* naciśnij przycisk RDP.
- Zaznacz opcję *TLS włączony* aby włączyć szyfrowanie.
- Zaznacz opcję *NLA włączony* dla dodatkowego bezpieczeństwa.
- W sekcji *Tryb połączenia* wybierz *bastion*.
- Ustaw *Adres lokalny* na **Any** i port **3389**.
- W polu *Certyfikat serwera* kliknij *Wygeneruj certyfikat*, aby wygenerować certyfikat TLS, wybierając algorytm klucza i podając nazwę powszechną (nazwa serwera, na którym zainstalowany jest certyfikat).

- Kliknij *Zapisz i zamknij*.

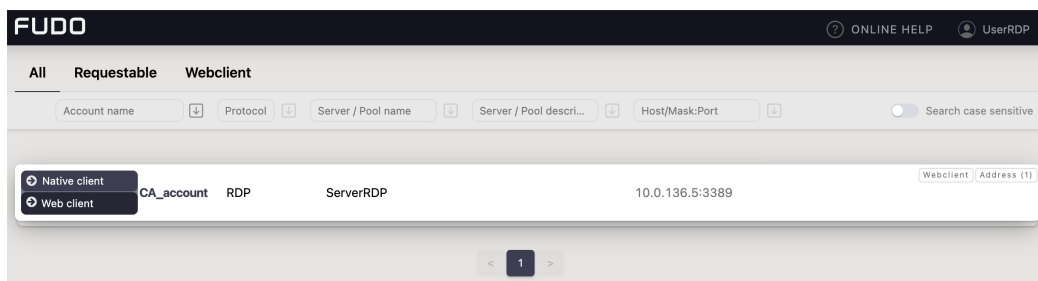
Konfiguracja Sejfu:

- Wybierz *Zarządzanie* > *Sejfy* i kliknij *+ Dodaj*.
- Wprowadź nazwę obiektu (np. **SafeRDP**).
- Wybierz opcję *Klient Webowy*, aby umożliwić nawiązanie sesji w przeglądarce.
- Wybierz zakładkę **Użytkownicy**, aby przypisać użytkowników uprawnionych do dostępu do kont przydzielonych do tego sejfu.
 - Kliknij *+ Dodaj użytkownika*, a następnie kliknij przycisk **+** obok **User1**, który został utworzony w poprzednich krokach, aby umożliwić dostęp do serwera przez monitorowany sejf.
 - Kliknij *ok*, aby zamknąć okno.
- Wybierz zakładkę **Konta**, aby dodać konta dostępne przez ten sejf.

- Kliknij «+ Dodaj konto», a następnie kliknij ikonę  obok CA-account, które zostało utworzone w poprzednich krokach.
 - Kliknij «ok», aby zamknąć okno.
 - Kliknij ikonę edycji , aby przypisać do konta gniazdo nasłuchiwania.
 - Kliknij ikonę , aby dodać gniazdo nasłuchiwania RDP-bastion utworzone w poprzednich krokach.
 - Kliknij «ok», aby zamknąć okno.
- 6. Kliknij *Zapisz*.

Nawiązywanie sesji:

1. Zaloguj się do *Portalu Użytkownika* Fudo Enterprise używając *User1* jako nazwy użytkownika i hasła podanego podczas tworzenia tego użytkownika.
2. Najedź kursorem na nazwę *CA_account* i wybierz *Klient webowy*, aby rozpocząć sesję.



Related topics:

- *Dodawanie serwera RDP*
- *Dodawanie użytkownika*

Często zadawane pytania

1. Jaka jest maksymalna ilość nagranych sesji na Fudo Enterprise dostępna z poziomu systemu?
2. W jaki sposób Fudo Enterprise 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 Enterprise?
5. W jaki sposób można stwierdzić próby uzyskania nieuprawnionego 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 Enterprise?
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 muszą 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 Enterprise 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 minuty 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 Enterprise pozwala określić, jak długo sesje mają być przechowywane i automatycznie usuwa dane sesji po upływie czasu określonego *parametrem retencji*.

2. W jaki sposób Fudo Enterprise obsługuje archiwizację sesji?

Wszystkie sesje archiwizowane są na wewnętrznej macierzy dyskowej urządzenia, przeznaczonej na rejestrowanie zdalnych połączeń. Fudo Enterprise 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 przypadku 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 Enterprise?

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 Enterprise 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 Enterprise?

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 muszą 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. Optymalne 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 Enterprise 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 Enterprise 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 Enterprise, 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*.

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.

certyfiat CA Certyfiat urzędu certyfikacji.

Czułość Czułość (ang. True Positive Rate) - to procent wszystkich złośliwych (malicious) sesji rozpoznanych przez model jako podejrzone (im wyższa, tym lepsza).

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 Enterprise 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.

FPR FPR (ang. False Positive Rate) - to procent wszystkich prawidłowych sesji niepoprawnie rozpoznanych przez model jako podejrzane (im niższy, tym lepszy).

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 uwierzytelnienia 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 dostęпами oraz tożsamościami cyfrowymi pracowników.

OpenID Connect OpenID Connect jest prostą warstwą tożsamości opartą na protokole OAuth 2.0.

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.

Prawdopodobieństwa zagrożenia Prawdopodobieństwo zagrożenia - to wartość procentowa, wskazująca poziom zagrożenia sesji.

PSM (Privileged Session Management) Moduł Fudo Enterprise 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 Enterprise.

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.

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 Enterprise lub nawiązywania połączenia z serwerami docelowymi.

znacznik czasu Znacznik będący skrótem danych, pozwalający zweryfikować czy dane nie zostały zmienione.

A

AAPM, **526**Active Directory, **526**

Active Directory

systemy zewnętrznego

uwierzytelniania, **359**AD, **526**

administracja

aktualizacja systemu, **321**import/eksport konfiguracji, **388**pierwsze uruchomienie, **40**ponowne uruchomienie, **378**przywracanie poprzedniej wersji, **378**

API

użytkownicy, **127**ARP, **526**Azure, **526**

B

blokowanie

serwery, **166**broker połączeń RDP, **526**broker połączeń RDP, **422**

C

CERB, **526**

CERB

systemy zewnętrznego

uwierzytelniania, **359**certyfikat CA, **526**Czułość, **526**

D

DHCP, **526**DNS, **526**

DNS

konfiguracja, **348**

dodawanie

serwery, **149**DoS (*Denial of Service*), **526**dostęp SSH, **526**DUO, **526**

E

Efficiency Analyzer/Productivity

Analyze, **527**

F

FPR, **527**fudopv, **527**

G

gniazda nasłuchiwania

HTTP, **200**konfiguracja, **188**Modbus, **205**MS SQL, **211**MySQL, **207**RDP, **193**SSH, **190**TCP, **209**Telnet, **213**Telnet 3270, **216**Telnet 5250, **219**VNC, **197**gniazdo nasłuchiwania, **527**grupa redundancji, **527**

H

Hasło statyczne, **527**heartbeat, **527**hot-swap, **527**

HTTP

gniazda nasłuchiwania, **200**protokoły, **8**protokół, **8**serwery, **149**

I

import
 serwery, 164

K

Klucz publiczny, **527**
 konfiguracja
 AI, 353
 gniazda nasłuchiwania, 188
 model danych, 31
 powiadomienia, 350
 serwery, 149
 synchronizacja użytkowników, 143
 ustawienia sieciowe, 337, 346
 użytkownicy, 125
 konto, **527**

L

LDAP, **527**
 LDAP
 systemy zewnętrznego
 uwierzytelniania, 359

M

Modbus
 gniazda nasłuchiwania, 205
 protokoły, 9
 protokół, 9
 serwery, 151
 model danych
 serwer, 31
 użytkownik, 31
 modyfikator haseł, **527**
 modyfikowanie
 serwery, 166
 MS SQL
 gniazda nasłuchiwania, 211
 serwery, 152
 MS SQL (*TDS*)
 protokoły, 9
 protokół, 9
 MySQL
 gniazda nasłuchiwania, 207
 protokoły, 10
 protokół, 10
 serwery, 154

N

notacja CIDR, **527**

O

OATH, **527**

OCR, **527**
 odblokowanie
 serwery, 167
 Odcisk Palca, **527**
 Okta, **527**
 OpenID Connect, **527**

P

polityka, **527**
 polityka czasowa, **528**
 Prawdopodobieństwa zagrożenia, **528**
 protocol
 secret, 21
 protocols
 secret, 21
 protokoły
 HTTP, 8
 Modbus, 9
 MS SQL (*TDS*), 9
 MySQL, 10
 RDP, 10
 SSH, 14
 TCP, 21
 Telnet, 19
 Telnet 3270, 18
 Telnet 5250, 18
 VNC, 19
 X11, 20
 protokół
 HTTP, 8
 Modbus, 9
 MS SQL (*TDS*), 9
 MySQL, 10
 RDP, 10
 SSH, 14
 TCP, 21
 Telnet, 19
 Telnet 3270, 18
 Telnet 5250, 18
 VNC, 19
 X11, 20
 PSM (*Privileged Session Management*), **528**

R

RADIUS, **528**
 RADIUS
 systemy zewnętrznego
 uwierzytelniania, 359
 RDP, **528**
 RDP
 gniazda nasłuchiwania, 193
 protokoły, 10

- protokół, 10
 - serwery, 155
 - repozytorium haseł, 528
 - retencja, 528
- S**
- scenariusze wdrożenia
 - bastion, 25
 - brama, 24
 - most, 22
 - pośrednik, 24
 - wymuszony routing, 22
 - secret
 - protocol, 21
 - protocols, 21
 - sejf, 528
 - sejf anonimowy, 528
 - serwer, 528
 - Serwery, 528
 - serwery
 - blokowanie, 166
 - dodawanie, 149
 - HTTP, 149
 - import, 164
 - konfiguracja, 149
 - Modbus, 151
 - modyfikowanie, 166
 - MS SQL, 152
 - MySQL, 154
 - odblokowanie, 167
 - RDP, 155
 - ssh, 156
 - TCP, 163
 - Telnet, 158
 - Telnet 3270, 159
 - Telnet 5250, 161
 - usuwanie, 167
 - VNC, 162
 - sesje, 278
 - dołączanie do trwającej sesji, 290
 - eksportowanie, 296
 - filtrowanie, 280
 - komentowanie, 293
 - odtwarzanie i podgląd, 282
 - SMS, 528
 - SSH, 528
 - SSH
 - gniazda nasłuchiwania, 190
 - protokoły, 14
 - protokół, 14
 - ssh
 - serwery, 156
 - synchronizacja użytkowników, 143
 - konfiguracja, 143
 - Syslog, 528
 - systemy zewnętrznego uwierzytelniania, 359
 - dodawanie serwera, 360
 - modyfikowanie serwera, 362
- T**
- TCP
 - gniazda nasłuchiwania, 209
 - protokoły, 21
 - protokół, 21
 - serwery, 163
 - Telnet
 - gniazda nasłuchiwania, 213
 - protokoły, 19
 - protokół, 19
 - serwery, 158
 - Telnet 3270
 - gniazda nasłuchiwania, 216
 - protokoły, 18
 - protokół, 18
 - serwery, 159
 - Telnet 5250
 - gniazda nasłuchiwania, 219
 - protokoły, 18
 - protokół, 18
 - serwery, 161
 - tryb połączenia
 - transparentny, 23
- U**
- ustawienia sieciowe
 - ARP, 349
 - etykiety adresów IP, 346
 - konfiguracja interfejsów, 337
 - serwery DNS, 348
 - trasa routingu, 347
 - usuwanie
 - serwery, 167
 - użytkownicy, 125
 - API, 127
 - konfiguracja, 125
 - prawa dostępu, 127, 141
 - role, 127, 141
 - zewnętrzne uwierzytelnianie, 359
 - użytkownik, 528
- V**
- VLAN, 528

VNC, **528**

VNC

gniazda nasłuchiwania, **197**

protokoły, **19**

protokół, **19**

serwery, **162**

W

WWN, **528**

X

X11

protokoły, **20**

protokół, **20**

Z

zewnętrzny serwer uwierzytelnienia, **528**

znacznik czasu, **528**