Fudo Enterprise 5.5 - Dokumentacja Systemu

Fudo Security

15.10.2024

Spis treści

1 O dokumentacji **1**

2 Motywy kolorystyczne Panelu Administracyjnego **4**

3 Wstęp **6**

3.1 Opis systemu . . . 6
3.2 Dostępne języki interfejsu . . . 8
3.3 Wspierane protokoły . . . 8
3.3.1 HTTP . . . 8
3.3.2 Modbus . . . 9
3.3.3 MS SQL (TDS) . . . 10
3.3.4 MySQL . . . 10
3.3.5 RDP . . . 11
3.3.6 SSH . . . 14
3.3.7 Telnet 3270 . . . 18
3.3.8 Telnet 5250 . . . 19
3.3.9 Telnet . . . 19
3.3.10 VNC . . . 20
3.3.11 X11 . . . 21
3.3.12 TCP . . . 21
3.3.13 Pobranie hasła . . . 21
3.4 Scenariusze wdrożenia . . . 22
3.5 Tryby połączenia . . . 24
3.6 Metody i tryby uwierzytelniania użytkowników . . . 26
3.7 Mechanizmy bezpieczeństwa . . . 29
3.7.1 Szyfrowanie danych . . . 29
3.7.2 Kopie zapasowe . . . 30
3.7.3 Uprawnienia użytkowników . . . 30
3.7.4 Sandboxing . . . 30
3.7.5 Niezawodność . . . 30
3.7.6 Konfiguracja klastrowa . . . 30
3.8 Model danych . . . 31
3.9 Dashboard . . . 32
3.9.1 Widgety . . . 33
3.9.2 Zarządzanie widgetami . . . 34
3.9.3 Status dysków . . . 34

3.10 Portal użytkownika . . . 35
3.11 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 . . . 135
6.3 Modyfikowanie użytkownika . . . 136
6.4 Blokowanie użytkownika . . . 137
6.5 Odblokowanie użytkownika . . . 138
6.6 Usuwanie użytkownika . . . 139
6.7 Zliczanie niepowodzeń uwierzytelnienia . . . 141
6.8 Role użytkownika . . . 142
6.9 Synchronizacja użytkowników z LDAP . . . 144

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 . . . 174
10.1.1 Dodawanie konta typu *anonymous* . . . 174
10.1.2 Tworzenie konta typu *forward* . . . 177
10.1.3 Tworzenie konta typu *regular* . . . 182
10.2 Edytowanie konta . . . 190
10.3 Blokowanie konta . . . 191
10.4 Odblokowywanie konta . . . 192
10.5 Usuwanie konta . . . 193
10.6 Zarządzanie ostrzeżeniami bezpieczeństwa . . . 194
10.6.1 Zmiana hasła konta . . . 195
10.6.2 Zignorowanie ostrzeżenia . . . 196

11 Gniazda nasłuchiwania **198**
11.1 Dodawanie gniazda nasłuchiwania . . . 198
11.1.1 Konfigurowanie gniazda nasłuchiwania SSH . . . 200
11.1.2 Konfigurowanie gniazda nasłuchiwania RDP . . . 203
11.1.3 Konfigurowanie gniazda nasłuchiwania VNC . . . 207
11.1.4 Konfigurowanie gniazda nasłuchiwania HTTP . . . 210
11.1.5 Konfigurowanie gniazda nasłuchiwania Modbus . . . 215
11.1.6 Konfigurowanie gniazda nasłuchiwania MySQL . . . 217
11.1.7 Konfigurowanie gniazda nasłuchiwania TCP . . . 219
11.1.8 Konfigurowanie gniazda nasłuchiwania MS SQL . . . 221
11.1.9 Konfigurowanie gniazda nasłuchiwania Telnet . . . 223
11.1.10 Konfigurowanie gniazda nasłuchiwania Telnet 3270 . . . 226
11.1.11 Konfigurowanie gniazda nasłuchiwania Telnet 5250 . . . 229
11.2 Modyfikowanie gniazda nasłuchiwania . . . 231
11.3 Blokowanie gniazda nasłuchiwania . . . 232
11.4 Odblokowanie gniazda nasłuchiwania . . . 233
11.5 Usuwanie gniazda nasłuchiwania . . . 234

12 Sejfy **236**
12.1 Dodawanie sejfu . . . 237
12.2 Modyfikowanie sejfu . . . 246
12.3 Blokowanie sejfu . . . 247
12.4 Odblokowanie sejfu . . . 248
12.5 Usuwanie sejfu . . . 249

13 Żądania dostępu **250**
13.1 Żądania oczekujące . . . 252
13.2 Żądania aktywne . . . 253
13.3 Archiwum żądań . . . 254

14 Wykrywanie (Discovery) **255**
14.1 Tworzenie reguły . . . 256
14.1.1 Tworzenie reguły dla kont . . . 256
14.1.2 Tworzenie reguły dla serwerów . . . 257
14.2 Zarządzanie regułami . . . 258
14.3 Tworzenie skanera . . . 259
14.3.1 Tworzenie skanera dla kont kontrolera domeny . . . 259
14.3.2 Tworzenie skanera dla serwerów kontrolera domeny . . . 261
14.3.3 Tworzenie skanera dla kont lokalnych . . . 263
14.4 Zarządzanie skanerami . . . 264

14.5 Zarządzanie wykrytymi kontami . . . 265
14.6 Zarządzanie wykrytymi serwerami . . . 267

15 Modyfikatory haseł **269**
15.1 Polityki haseł . . . 269
15.1.1 Dodawanie polityki zmiany haseł . . . 269
15.1.2 Edycja polityki zmiany haseł . . . 270
15.1.3 Usuwanie polityki zmiany haseł . . . 270
15.2 Uniwersalne modyfikatory haseł . . . 271
15.2.1 Definiowanie modyfikatora haseł . . . 271
15.2.2 Edycja modyfikatora haseł . . . 274
15.2.3 Usuwanie modyfikatora haseł . . . 275
15.3 Importowanie i eksportowanie modyfikatorów haseł . . . 275
15.3.1 Eksportowanie modyfikatora haseł . . . 275
15.3.2 Importowanie modyfikatora haseł . . . 275
15.4 Tryby połączenia . . . 276
15.4.1 SSH . . . 276
15.4.2 LDAP . . . 277
15.4.3 Telnet . . . 278
15.4.4 WinRM . . . 279
15.5 Konfigurowanie modyfikatora haseł Unix poprzez SSH . . . 280

16 Polityki **283**
16.1 Definiowanie polityki na podstawie modułu AI . . . 283
16.2 Przykłady polityk opartych na module AI . . . 285
16.3 Definiowanie polityki na podstawie wzorca . . . 288

17 Do pobrania **291**
17.1 Sesje . . . 291
17.2 Pliki . . . 291

18 Aktywność konta w Portalu Użytkownika **294**

19 Sesje **296**
19.1 Filtrowanie sesji . . . 298
19.1.1 Definiowanie filtrów . . . 298
19.1.2 Zarządzanie definicjami filtrowania . . . 299
19.1.3 Przeszukiwanie pełnotekstowe . . . 299
19.2 Odtwarzanie sesji . . . 300
19.3 Wstrzymywanie połączenia . . . 306
19.4 Przerywanie połączenia . . . 307
19.5 Dołączanie do sesji . . . 308
19.6 Udostępnianie sesji . . . 309
19.7 Komentowanie sesji . . . 311
19.8 Zarządzanie retencją sesji . . . 313
19.9 Eksportowanie sesji . . . 314
19.9.1 Dostępne formaty plików eksportu sesji . . . 316
19.10 Usuwanie sesji . . . 317
19.11 Przetwarzanie OCR sesji . . . 317
19.12 Replikacja sesji w konfiguracji klastrowej . . . 319
19.13 Znakowanie czasem wybranych sesji . . . 320
19.14 Anulowanie znakowania czasem . . . 321

19.15 Wymagane potwierdzenie dostępu . . . 322
19.15.1 Akceptowanie żądań użytkowników . . . 322
19.15.2 Odrzucanie żądań użytkowników . . . 323
19.16 Przetwarzanie sesji - uczenie maszynowe . . . 323
19.16.1 Model zawartości . . . 324
19.16.2 Ocena sesji . . . 324
19.16.3 Modele ilościowe . . . 326

20 Raporty **327**
20.1 Subskrybowanie raportu cyklicznego . . . 328
20.2 Rezygnacja z subskrypcji raportu cyklicznego . . . 329
20.3 Generowanie raportu na żądanie . . . 329
20.4 Wyświetlanie i zapisywanie raportów . . . 330
20.5 Usuwanie raportów . . . 330

21 Produktywność **331**
21.1 Zestawienie . . . 331
21.2 Analiza sesji . . . 332
21.3 Porównanie aktywności . . . 333

22 Administracja **334**
22.1 System . . . 334
22.1.1 Data i czas . . . 334
22.1.2 Certyfikaty HTTPS . . . 336
22.1.3 Blokowanie nowych połączeń . . . 337
22.1.4 Dostęp SSH . . . 337
22.1.5 Funkcjonalności wrażliwe . . . 338
22.1.6 Aktualizacja systemu . . . 339
22.1.6.1 Aktualizowanie systemu . . . 339
22.1.6.2 Przywrócenie poprzedniej wersji systemu . . . 341
22.1.6.3 Usuwanie migawki aktualizacji . . . 342
22.1.7 Licencja . . . 343
22.1.8 Hotfix . . . 343
22.1.9 Diagnostyka . . . 344
22.1.10 Szyfrowanie konfiguracji . . . 346
22.1.11 Modyfikatory haseł - aktywny węzeł klastra . . . 348
22.1.11.1 Manager haseł w klastrze . . . 349
22.2 Limit Czasu . . . 349
22.3 Konfiguracja sieci . . . 350
22.3.1 Konfiguracja ustawień sieciowych . . . 351
22.3.1.1 Zarządzanie interfejsami fizycznymi . . . 351
22.3.1.2 Ustawianie adresu IP z konsoli . . . 354
22.3.1.3 Konfigurowanie mostu sieciowego . . . 357
22.3.1.4 Konfigurowanie sieci wirtualnych (VLAN) . . . 358
22.3.1.5 Konfigurowanie agregacji połączeń LACP . . . 359
22.3.2 Etykiety adresów IP . . . 360
22.3.3 Konfiguracja tras routingu . . . 361
22.3.4 Konfiguracja DNS . . . 362
22.3.5 Konfiguracja tablicy ARP . . . 364
22.4 Powiadomienia . . . 364
22.5 Sztuczna inteligencja . . . 367
22.5.1 Konfiguracja trenera modeli . . . 368

22.5.2 Modele behawioralne . . . 369
22.6 Znakowanie czasem . . . 371
22.7 Model uwierzytelniania w oparciu o certyfikaty . . . 372
22.8 Uwierzytelnienie . . . 373
22.8.1 Definicja serwera uwierzytelnienia zewnętrznego . . . 374
22.8.2 Definicja uwierzytelniania OpenID Connect . . . 376
22.8.3 Global authentication settings . . . 379
22.8.3.1 Domyślna domena . . . 380
22.8.3.2 Złożoność haseł . . . 381
22.8.3.3 Definicja uwierzytelniania OATH . . . 383
22.8.3.4 Definicja uwierzytelniania SMS . . . 383
22.8.3.5 Definicja uwierzytelniania DUO . . . 385
22.8.3.6 Single Sign On . . . 386
22.8.3.6.1 Konfiguracja Fudo Enterprise dla SSO . . . 386
22.8.3.6.2 Konfiguracja kontrolera domeny . . . 386
22.8.3.6.3 Single Sign On w Panelu Administracyjnym . . . 387
22.8.3.6.4 Single Sign On w Portalu Użytkownika . . . 388
22.8.3.7 Ustawienia uwierzytelniania Kerberos . . . 388
22.8.3.7.1 Wyłączanie uwierzytelniania Kerberos . . . 389
22.8.3.7.2 Dodawanie serwerów KDC . . . 389
22.9 Zewnętrzne repozytoria haseł . . . 390
22.9.1 CyberArk Credential Provider . . . 390
22.9.2 Thycotic Secret Server . . . 393
22.9.3 Local Administrator Password Solutions (LAPS) . . . 394
22.10 Zasoby . . . 397
22.10.1 Konfiguracja ekranu logowania RDP/SSH/VNC . . . 397
22.10.2 Konfiguracja ekranu logowania *Portalu użytkownika* . . . 400
22.11 Przywracanie poprzedniej wersji systemu . . . 401
22.12 Ponowne uruchomienie systemu . . . 402
22.13 SNMP . . . 403
22.13.1 Odczytywanie informacji SNMP poprzez `snmpwalk` . . . 406
22.13.2 Rozszerzenia SNMP Fudo Enterprise . . . 406
22.14 Kopia zapasowa i retencja . . . 407
22.14.1 Kopia zapasowa systemu . . . 407
22.14.2 Retencja danych . . . 409
22.15 Zewnętrzna macierz dyskowa . . . 411
22.15.1 Konfigurowanie zewnętrznej macierzy dyskowej . . . 411
22.15.2 Rozszerzanie zewnętrznej macierzy dyskowej . . . 412
22.16 Eksportowanie/importowanie konfiguracji systemu . . . 412
22.16.1 Eksportowanie konfiguracji . . . 413
22.16.2 Importowanie konfiguracji . . . 413
22.17 Konfiguracja klastrowa . . . 414
22.17.1 Inicjowanie klastra . . . 415
22.17.2 Zarządzanie węzłami klastra . . . 416
22.17.2.1 Dodawanie węzłów klastra . . . 416
22.17.2.2 Edytowanie węzłów klastra . . . 420
22.17.2.3 Usuwanie węzłów klastra . . . 420
22.17.3 Grupy redundancji . . . 421
22.18 Dziennik zdarzeń . . . 424
22.18.1 Filtrowanie logów według daty i czasu . . . 424
22.18.2 Zewnętrzne serwery syslog . . . 425

22.18.3 Eksportowanie dziennika zdarzeń . . . 426
22.19 Zmiana frazy szyfrującej . . . 427
22.20 Integracja z serwerem CERB . . . 428
22.21 Czynności serwisowe . . . 434
22.21.1 Sporządzanie kopii zapasowej kluczy szyfrujących . . . 435
22.21.2 Monitorowanie stanu systemu . . . 438
22.21.3 Kontrola Stanu . . . 439
22.21.3.1 API kontrola stanu . . . 439
22.21.4 Call Home . . . 440
22.21.5 Wymiana dysku macierzy . . . 441
22.21.6 Przywracanie ustawień fabrycznych . . . 442

23 Informacje uzupełniające **446**
23.1 Broker połączeń RDP . . . 446
23.2 Komunikaty dziennika zdarzeń . . . 447
23.3 Informacja ze stopki dolnej . . . 464

24 Fudo Officer 2.0 **465**
24.1 Konfiguracja . . . 465
24.2 Zarządzanie Profilami . . . 467
24.2.1 Dodawanie Profilów . . . 467
24.2.2 Przełączanie Profilów . . . 469
24.2.3 Edytowanie Profilu . . . 469
24.2.4 Usuwanie Profilu . . . 470
24.3 Zarządzanie Żądaniami Sesji . . . 472
24.3.1 Żądania Oczekujące . . . 472
24.3.2 Żądania Aktywne . . . 473
24.3.3 Cofnięcie Żądania . . . 474
24.3.4 Żądania Archiwalne . . . 475
24.4 Ustawienia . . . 476
24.4.1 Uwierzytelnianie biometryczne . . . 476
24.4.2 Zmiana kodu PIN . . . 476
24.4.3 Język . . . 477

25 AAPM (Application to Application Password Manager) **478**
25.1 Kompilowanie narzędzia *fudopv* . . . 478
25.1.1 Python . . . 479
25.1.2 Środowisko wirtualne . . . 479
25.1.3 Pobranie zależności . . . 480
25.1.4 Zbudowanie narzędzia *fudopv* . . . 480
25.2 Wdrożenie *fudopv* bez kompilacji kodu źródłowego . . . 481
25.3 Uruchamianie *fudopv* . . . 481
25.4 Sposoby uwierzytelnienia . . . 486
25.4.1 Hasło statyczne . . . 487

26 Aplikacje klienckie **488**
26.1 PuTTY . . . 488
26.2 Microsoft Remote Desktop . . . 490
26.3 TightVNC Viewer . . . 492
26.4 SQL Server Management Studio . . . 493

27 Rozwiązywanie problemów **494**

27.1 Uruchamianie Fudo Enterprise . . . 494
27.2 Połączenia z serwerami . . . 494
27.3 Logowanie do panelu administracyjnego . . . 499
27.4 Odtwarzanie sesji . . . 500
27.5 Konfiguracja klastrowa . . . 500
27.6 Znakowanie czasem . . . 501
27.7 Tryb serwisowy . . . 501

28 Przypadki użycia **505**
28.1 Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator . . . 505
28.1.1 Protokoły obsługujące OATH . . . 505
28.1.2 Konfiguracja domyślnych wartości OATH . . . 506
28.1.3 Konfiguracja metody OATH użytkownikowi . . . 506
28.2 Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure) . . . 511
28.3 Konfiguracja usługi Remote Desktop Services na serwerze Windows dla Fudo Enterprise . . . 518
28.3.1 Konfiguracja usługi Remote Desktop Services (RDS) . . . 518
28.3.2 Konfiguracja Fudo Enterprise . . . 529
28.4 Zarządzanie certyfikatami na potrzeby połączeń RDP . . . 535
28.4.1 Lokalizacja certyfikatu dla protokołu RDP w Windows Server . . . 535
28.4.2 Dostarczanie certyfikatu CA . . . 538
28.5 Konfiguracja Single Sign On (SSO) . . . 553
28.5.1 Konfiguracja SSO na Windows Server 2019 . . . 554
28.5.2 Konfiguracja Fudo Enterprise . . . 558
28.5.3 Konfiguracja i sprawdzenie stacji roboczej użytkownika - klienta Windows 2010 . . . 561

29 Często zadawane pytania **565**

30 Słownik pojęć **570**

Indeks **574**

ROZDZIAŁ 1

O dokumentacji

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

Struktura dokumentacji

1. O dokumentacji

Rozdział zawiera informacje na temat tej dokumentacji.

2. Motywy kolorystyczne Panelu Administracyjnego

Rozdział zawiera informacje na temat dostępnych motywów kolorystycznych Fudo 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 szczegółach 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 żądaniami 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.

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

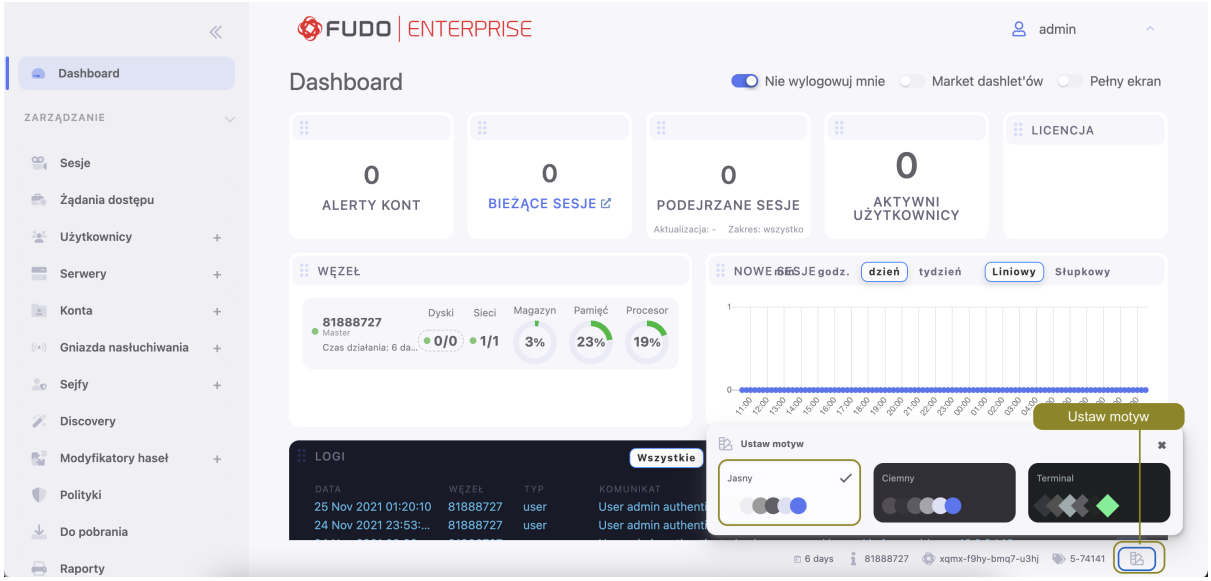
Nota prawna

ROZDZIAŁ 2

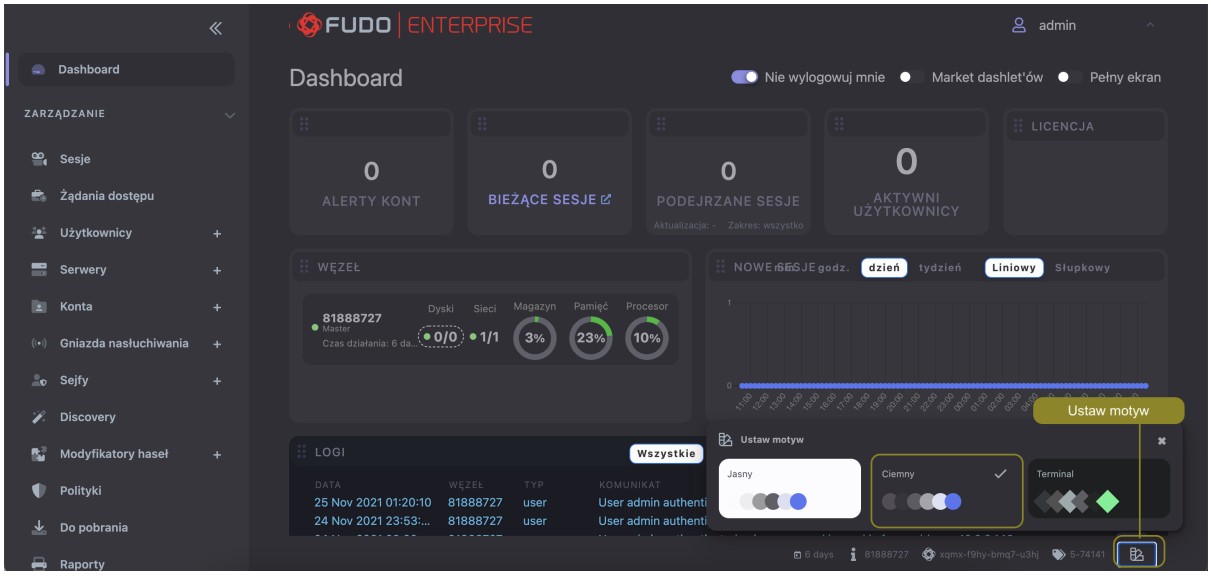
Motywy kolorystyczne Panelu Administracyjnego

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

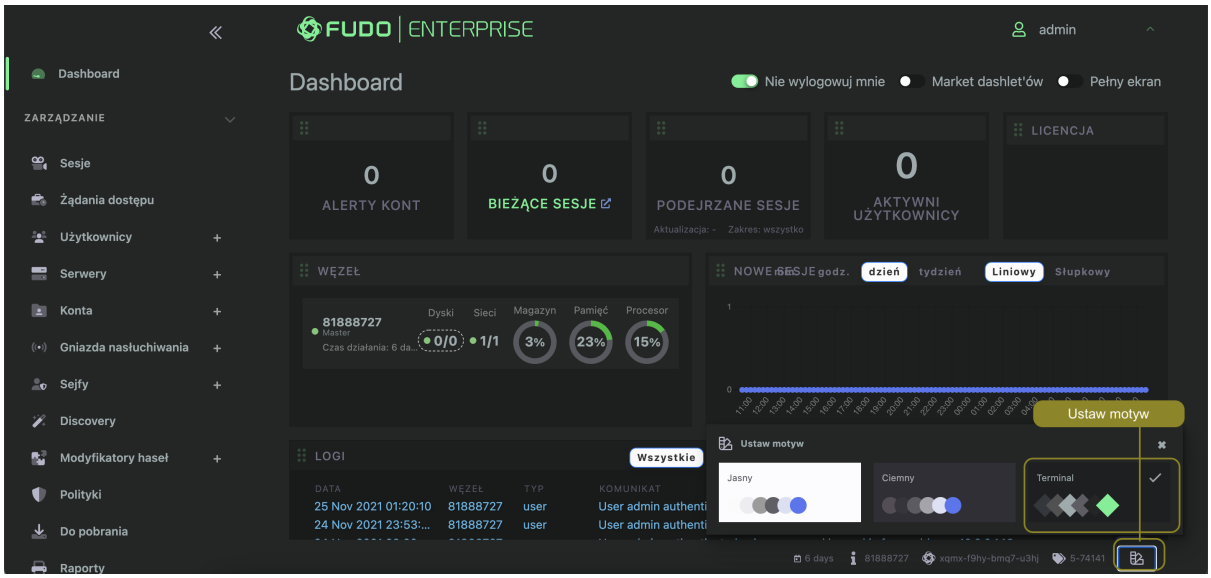
Jasny:



Ciemny:



Terminal:



Tematy pokrewne:

- *Wstęp*

ROZDZIAŁ 3

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 bezczynności.

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

Application to Application Password Manager (AAPM)

Moduł *AAPM* umożliwia bezpieczną wymianę haseł pomiędzy aplikacjami.

Systemy operacyjne wspierane przez moduł AAPM:

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

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

Tematy pokrewne:

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

3.2 Dostępne języki interfejsu

Interfejs Fudo Enterprise jest dostępny w następujących językach:

- Angielski,
- Polski,
- Ukraiński,
- Rosyjski,
- Kazachski.

Tematy pokrewne:

- *System overview*
- *Wspierane protokoły*
- *Quick start*

3.3 Wspierane protokoły

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

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

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

3.3.2 Modbus

Wspierane tryby połączenia:

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

Uwagi:

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

3.3.3 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 którejś z już trwających sesji. Jeśli tak jest, sesje są agregowane w jedną.

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

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

Wspierane tryby połączenia:

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

Wspierane aplikacje klienckie:

- SQL Server Management Studio,
- sqsh.

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.

3.3.4 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.

3.3.5 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`

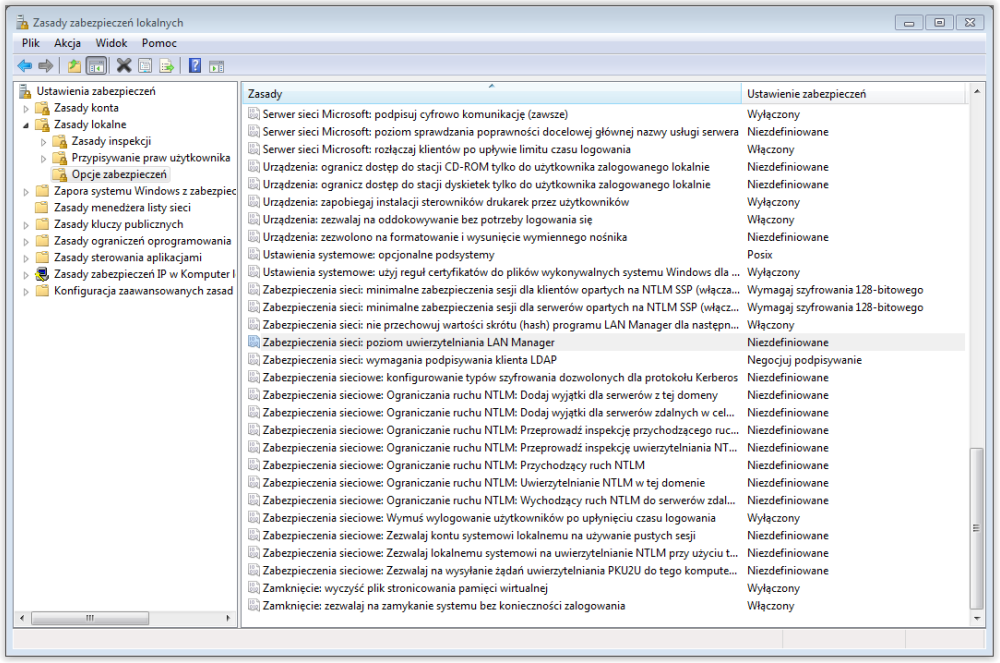
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-CHACHA20-POLY1305
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- 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:

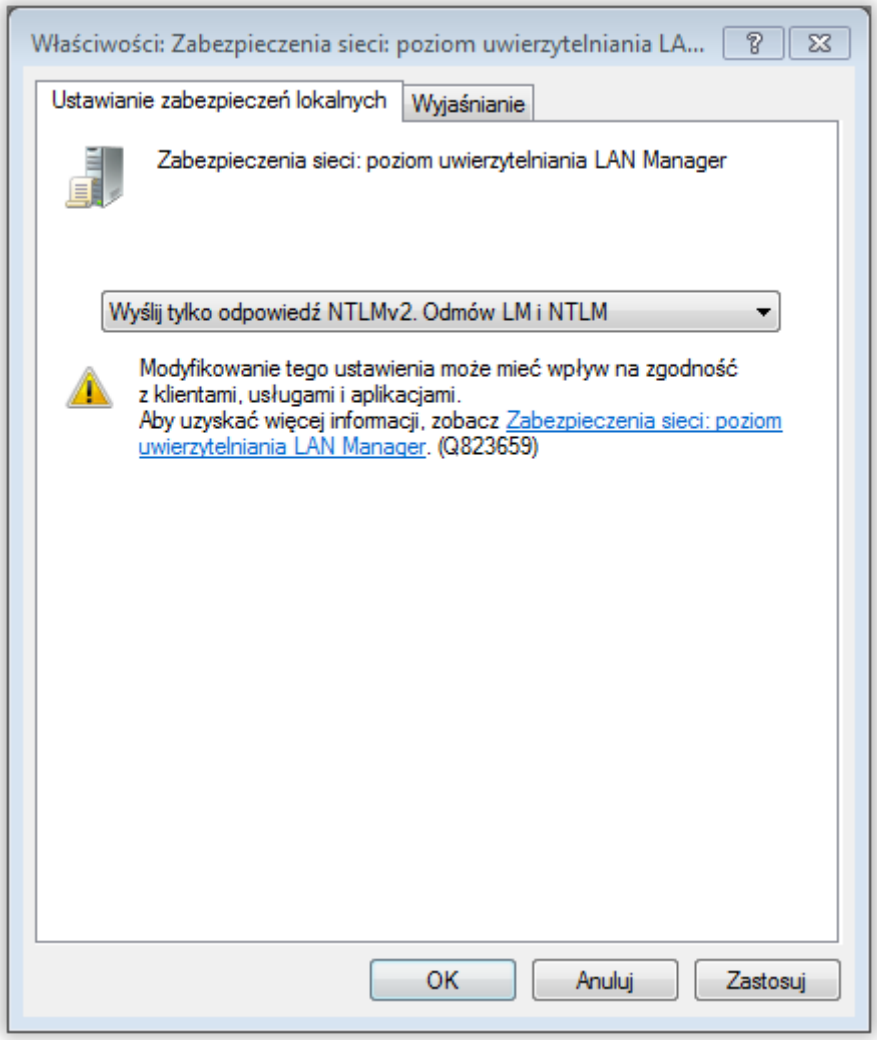
- Implementacja wsparcia dla protokołu RDP umożliwia uwierzytelnienie poprzez protokół RADIUS, w trybie *challenge-response*.
- Dla serwerów RDP są wspierane opcje NLA oraz TLS.
- Dla gniazd nasłuchiwania RDP, poza standardową opcją bezpieczeństwa jest wspierana opcja *Enhanced RDP Security (TLS)*.

- W przypakdu 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.

3.3.6 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 (przeźroczysty, nie rejestrujemy),
- X11 - w ramach protokołu SSH (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- Shell (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch),
- Terminal (wideo, przerwanie, pauza, dołączenie, podgląd, surowy ruch).

Wspierane algorytmy szyfrujące:

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

Wspierane funkcje skrótu (algorytmy hashujące):

- MD5
- SHA256

Wspierane typy kluczy SSH:

- RSA
- ED25519, ED25519-SK
- ECDSA, ECDSA-SK
- DSA (z włączoną opcją *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`

dodatkowo 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*.

3.3.7 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 na-

wiązywania 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.

3.3.8 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 nawiązywania sesji automatycznie przekazuje login użytkownika do serwera docelowego. Jest to związane z domyślnie włączonym parametrem `-a`, odpowiadającym za przekazywanie loginu. W konsekwencji, uwierzytelniając się przed serwerem docelowym, użytkownik nie będzie poproszony o login. Aby wyłączyć domyślne przekazywanie loginu, należy użyć parametru `-K` bądź parametru `-l` z pustym loginem. Zatem należy pamiętać, aby zwrócić uwagę na domyślne zachowanie używanego programu klienckiego.

3.3.9 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 nawiązywania sesji automatycznie przekazuje login użytkownika do serwera docelowego. Jest to związane z domyślnie włączonym parametrem `-a`, odpowiadającym za przekazywanie loginu. W konsekwencji, uwierzytelniając się przed serwerem docelowym, użytkownik nie będzie poproszony o login. Aby wyłączyć domyślne przekazywanie loginu, należy użyć parametru `-K` bądź parametru `-l` z pustym loginem. Zatem należy pamiętać, aby zwrócić uwagę na domyślne zachowanie używanego programu klienckiego.

3.3.10 VNC

Wspierane tryby połączenia:

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

Proponowane 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);

3.3.11 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.

3.3.12 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.

3.3.13 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 uwierzytelniające*.

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

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

Uwagi:

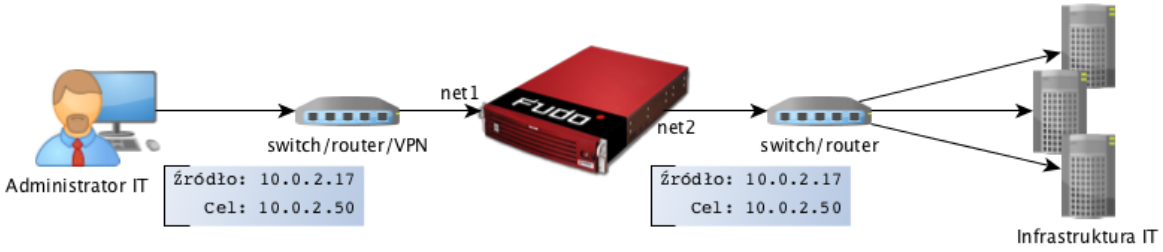
- Brak wsparcia mechanizmu dołączania do sesji.
- Brak wsparcia odtwarzacza.

3.4 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.



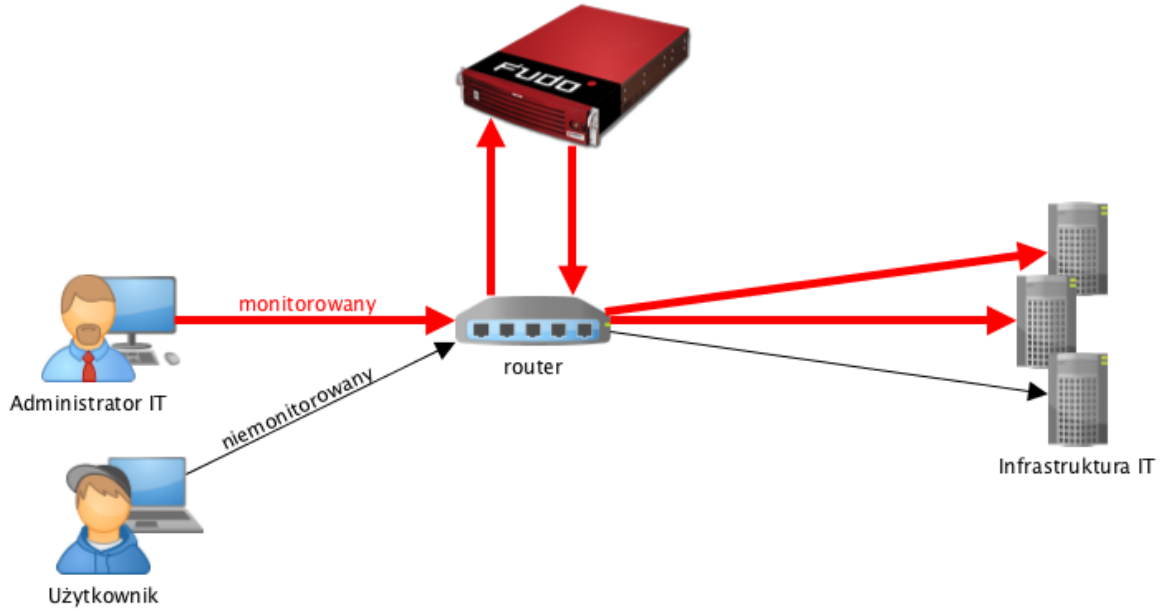
Fudo Enterprise pośrednicząc w przekazywaniu ruchu, zachowuje źródłowy adres IP klienta wysyłającego zapytania do serwerów.

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*

3.5 Tryby połączenia

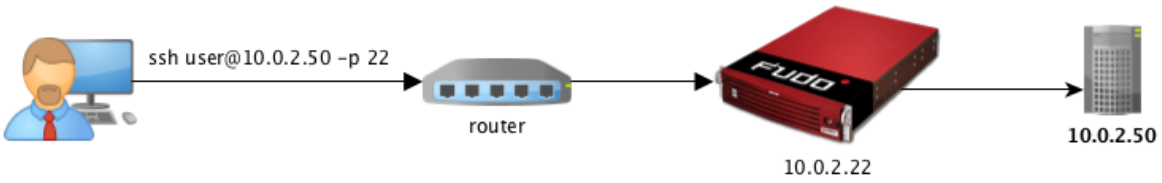
Funkcja zdeprecjonowana od wersji 5.4

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).

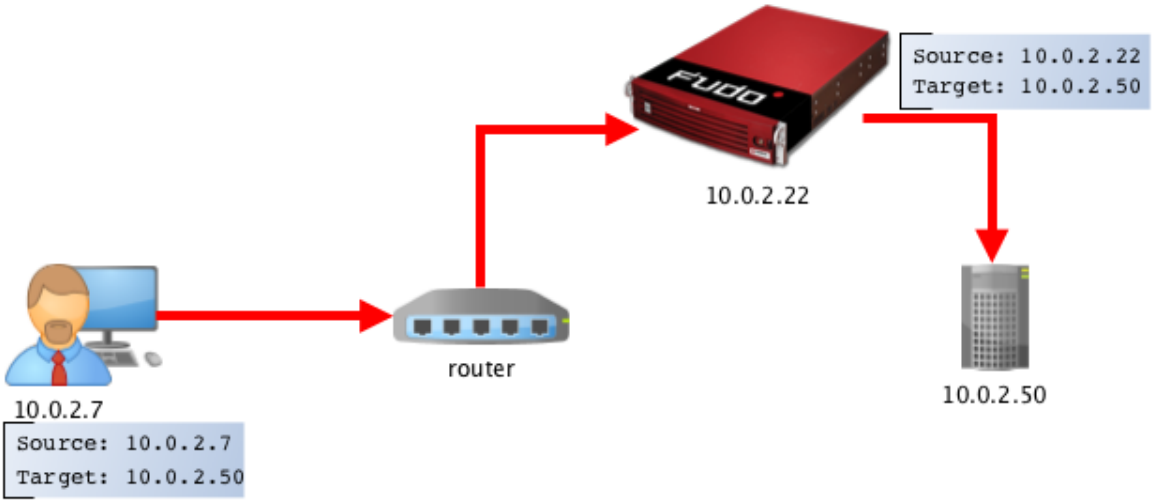
Przezroczysty

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

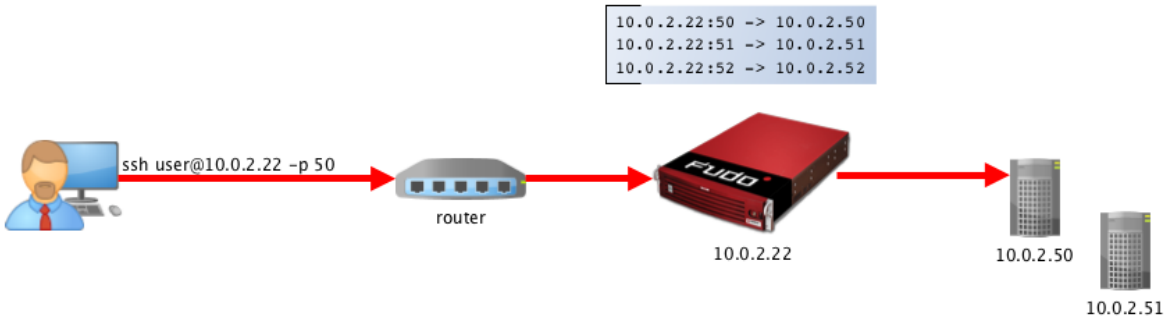
W trybie bramy, klient łączy się z serwerem docelowym wskazując bezpośrednio jego adres IP. Fudo Enterprise zestawiając połączenie z monitorowanym zasobem używa własnego adresu IP. Tryb pracy bramy pozwala na sterowanie ruchem sieciowym, by ten stale przechodził przez Fudo Enterprise, w przypadku gdy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

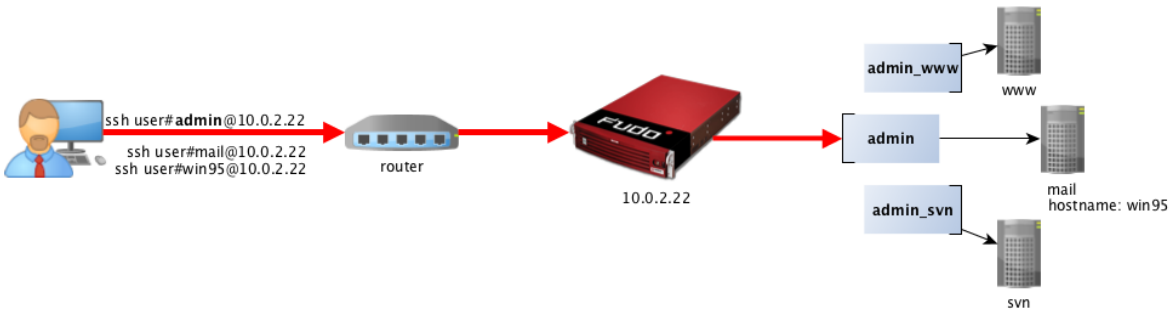


Takie rozwiązanie ukrywa faktyczną adresację serwerów, a odpowiednie ich skonfigurowanie pozwala na odrzucanie zapytań ze źródłowym adresem IP innym niż adres IP Fudo Enterprise.

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#root#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 adresa 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 odwróconego DNS i dokonuje próby dopasowania zwrócenej 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*

3.6 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. *challange-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 użytownika 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*

3.7 Mechanizmy bezpieczeństwa

3.7.1 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 „zapieczętowania" zaszyfrowanych danych. Klucz główny (Master Key) może zostać wyeksportowany przez superadministratora, ale tylko wtedy, gdy ten przed eksportem prześle do Fudo klucz do zaszyfrowania samego klucza głównego. Dopiero wtedy będzie możliwe odtworzenie Master Key, a co za tym idzie danych zaszyfrowanych kluczami wynikającymi z klucza głównego.

3.7.2 Kopie zapasowe

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

3.7.3 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*.

3.7.4 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.

3.7.5 Niezawodność

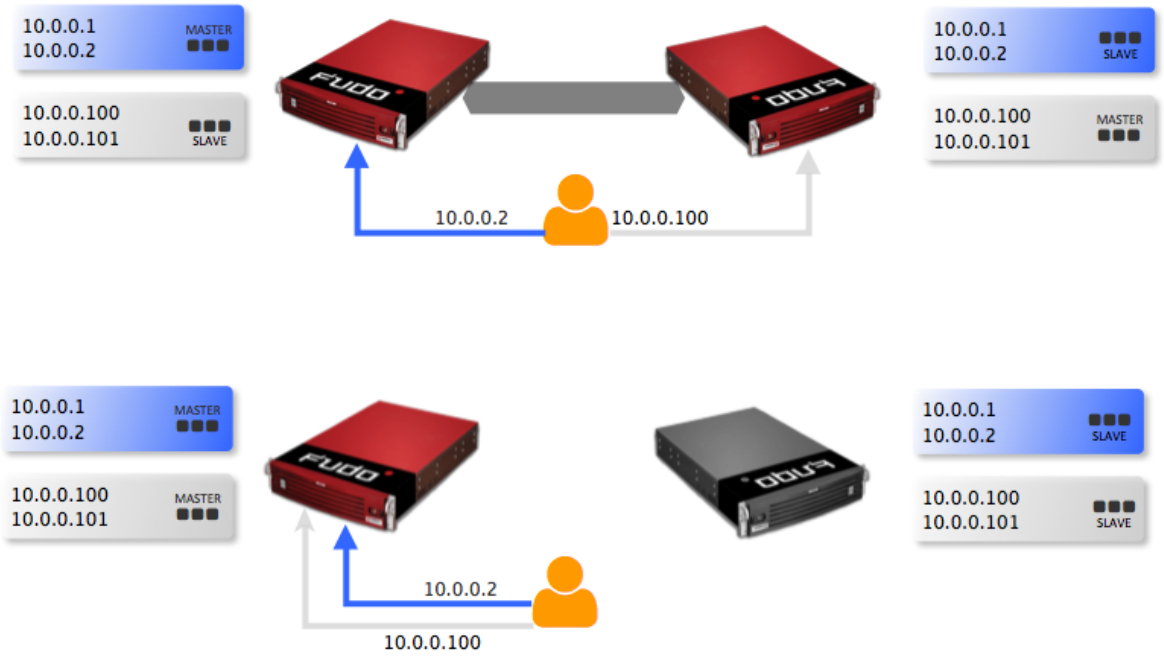
Fudo Enterprise dostarczane jest w konfiguracji sprzętowej zapewniającej optymalną wydajność i wysoką niezawodność systemu.

3.7.6 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*

3.8 Model danych

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

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

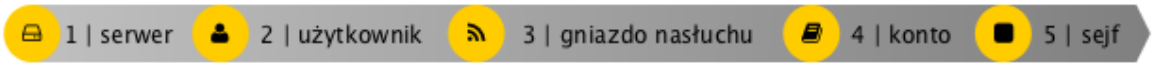
Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

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

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

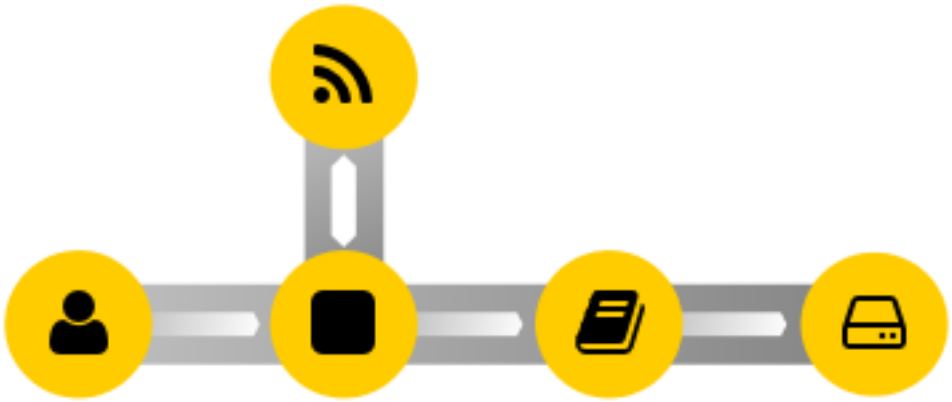
Gniazdo nasłuchiwania determinuje tryb połączenia serwera (proxy, brama, pośrednik, przezroczysty) oraz protokół komunikacji.

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



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

Schemat relacji obiektów



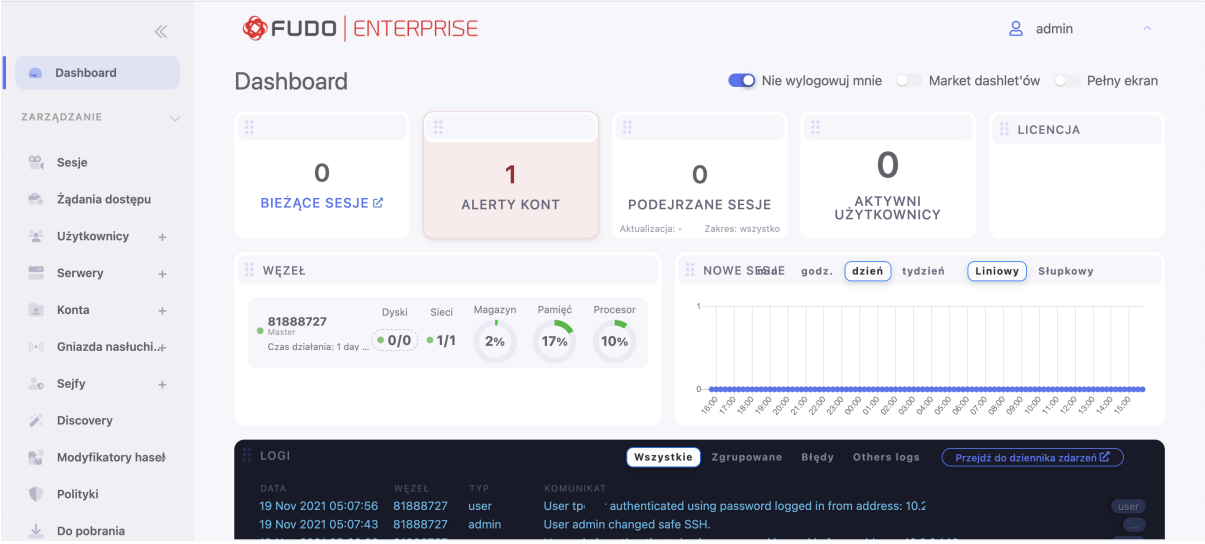
Sejf jest centralnym obiektem modelu danych, który reguluje dostęp do monitorowanych serwerów. Wskazuje konta uprzywilejowane na systemach docelowych, wraz z gniazdami nasłuchiwania określającymi właściwe dla *wybranego trybu* parametry połączenia (np. adres IP, numer portu). Taki model danych pozwala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

Tematy pokrewne:

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

3.9 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.

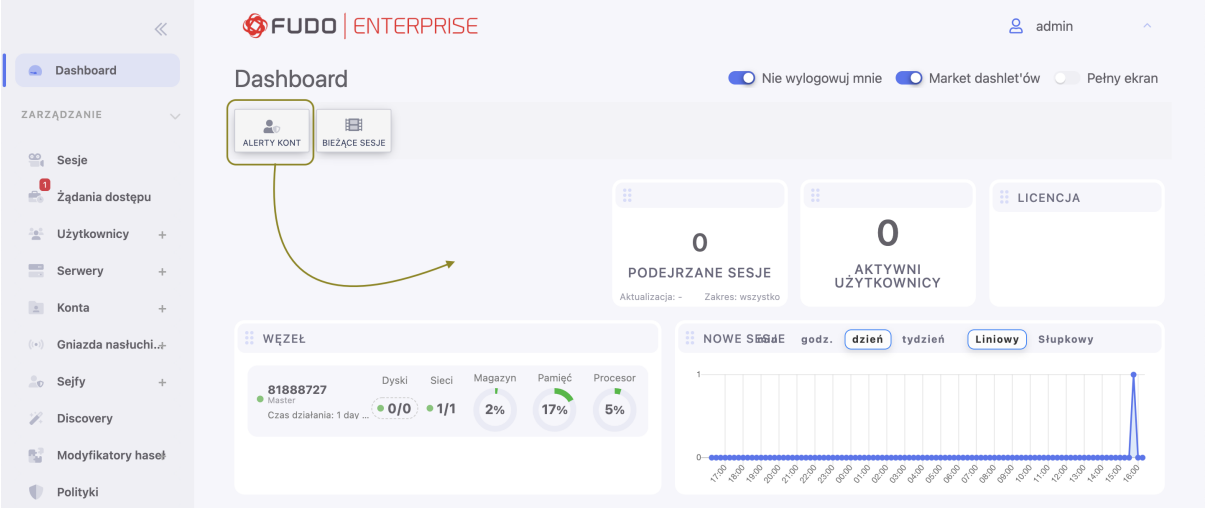
3.9.1 Widgety

Nowe sesje	Wykres obrazujący liczbę nowo nawiązanych połączeń w jednostce czasu.
Aktualne sesje	Liczba aktualnie zestawionych połączeń.
Sesje podejrzane	Liczba sesji o wysokim stopniu zagrożenia. Widget pozwala wyświetlać podejrzane sesje według następujących konfiguracji czasowych: z ostatnich 12 godzin, ostatniego dnia, ostatniego tygodnia, lub z ostatniego miesiąca. Na widgecie 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.

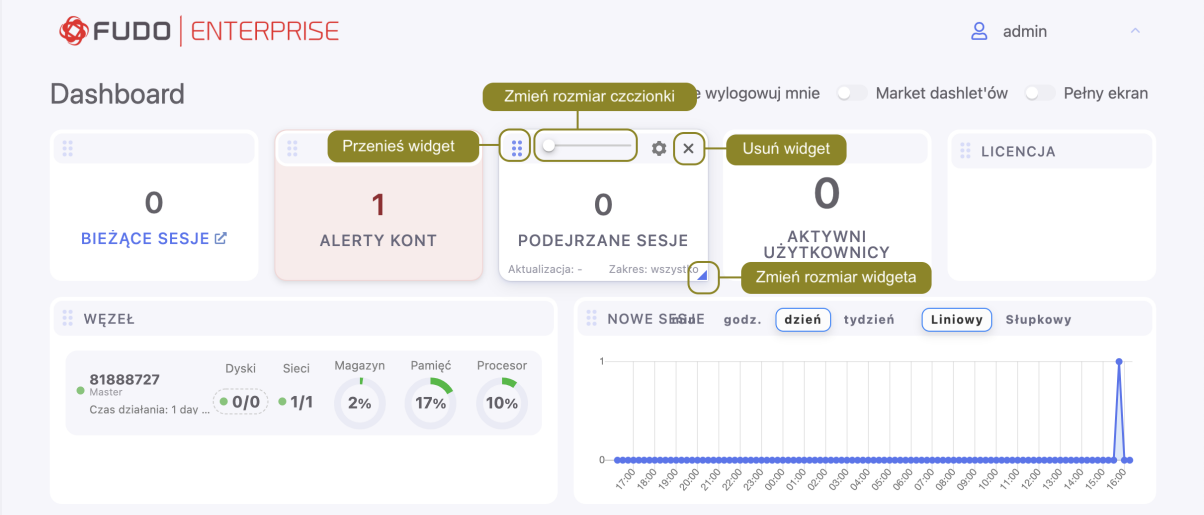
Informacja: Dostępność widgetów zależy od *roli przypisanej użytkownikowi*.

3.9.2 Zarządzanie widgetami

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



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

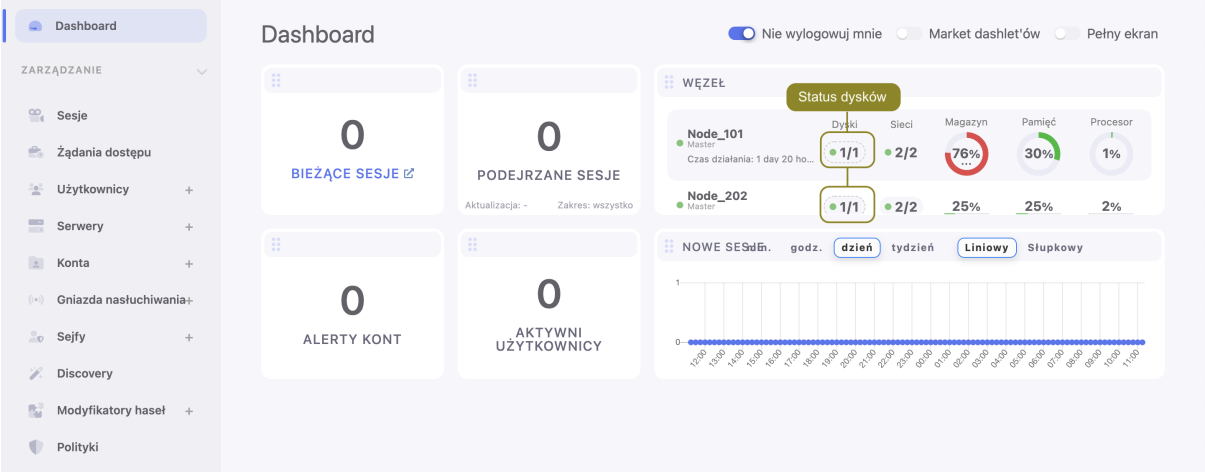


- Kliknij *Usuń*, aby potwierdzić usunięcie widgetu.

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

3.9.3 Status dysków

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



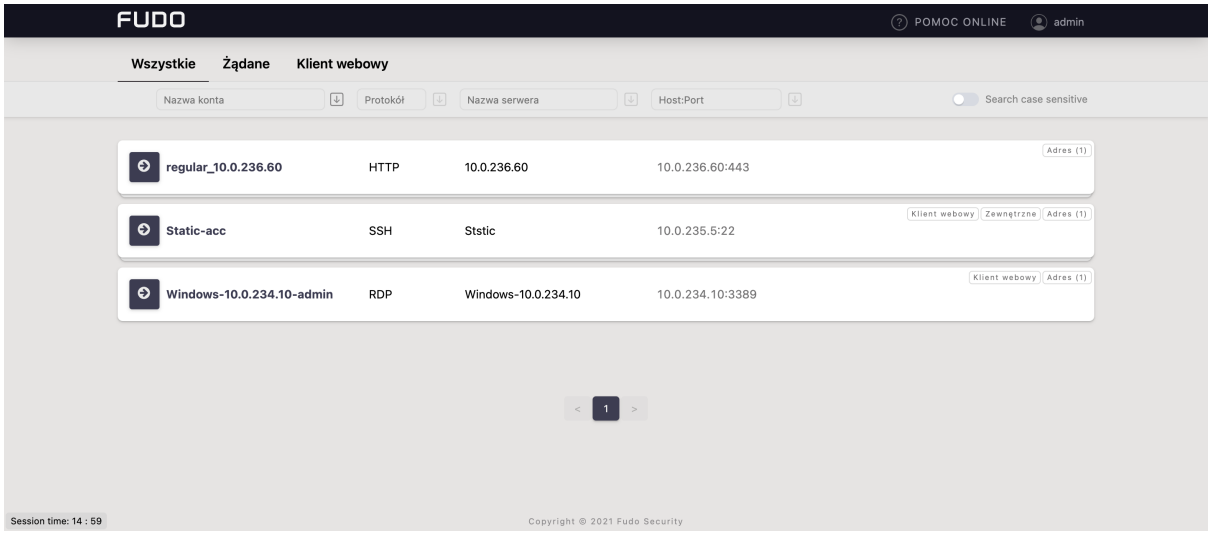
	Dysk pracuje prawidłowo.
	Dysk w trakcie synchronizacji danych.
	Błędy odczytu/zapisu danych - dysk nie działa prawidłowo i może wkrótce ulec awarii - skontaktuj się z działem wsparcia technicznego w celu omówienia dalszych kroków mających na celu przywrócenie urządzenia do pełnej sprawności.
	Awaria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

Tematy pokrewne:

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

3.10 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.



3.11 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.

ROZDZIAŁ 4

Instalacja i pierwsze uruchomienie

Ten rozdział opisuje urządzenie fizyczne i procedurę pierwszego uruchomienia.

4.1 Wymagania

Panel zarządzający

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

Wymagania sieciowe

Poprawne działanie Fudo 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 *Call Home*.
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*.

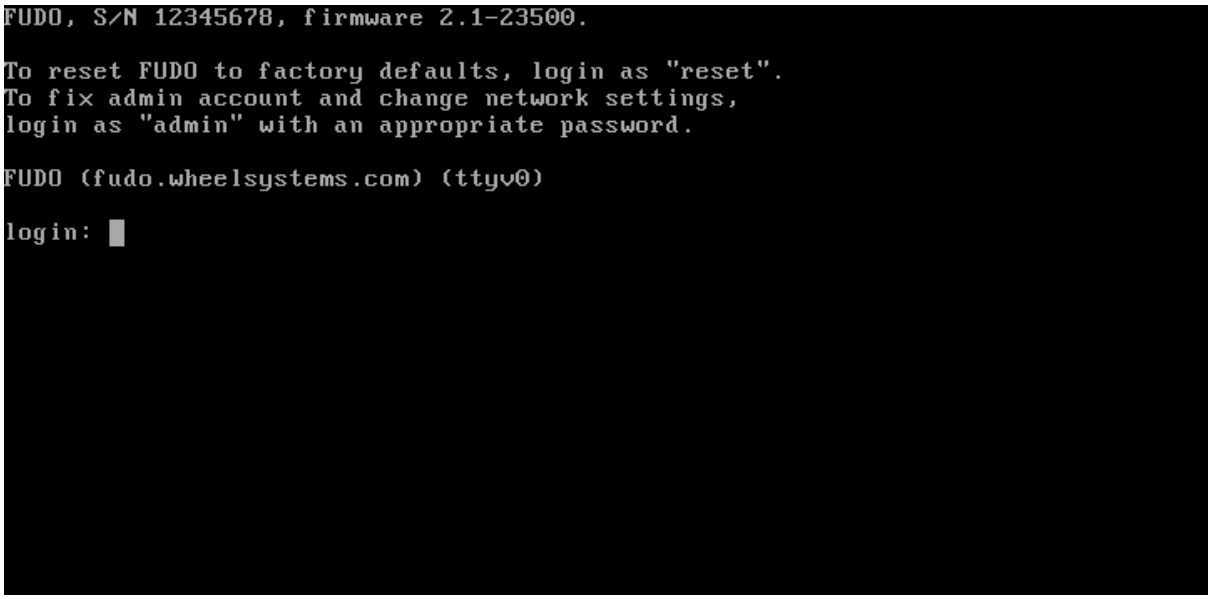
Ustawienie adresu IP z konsoli

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

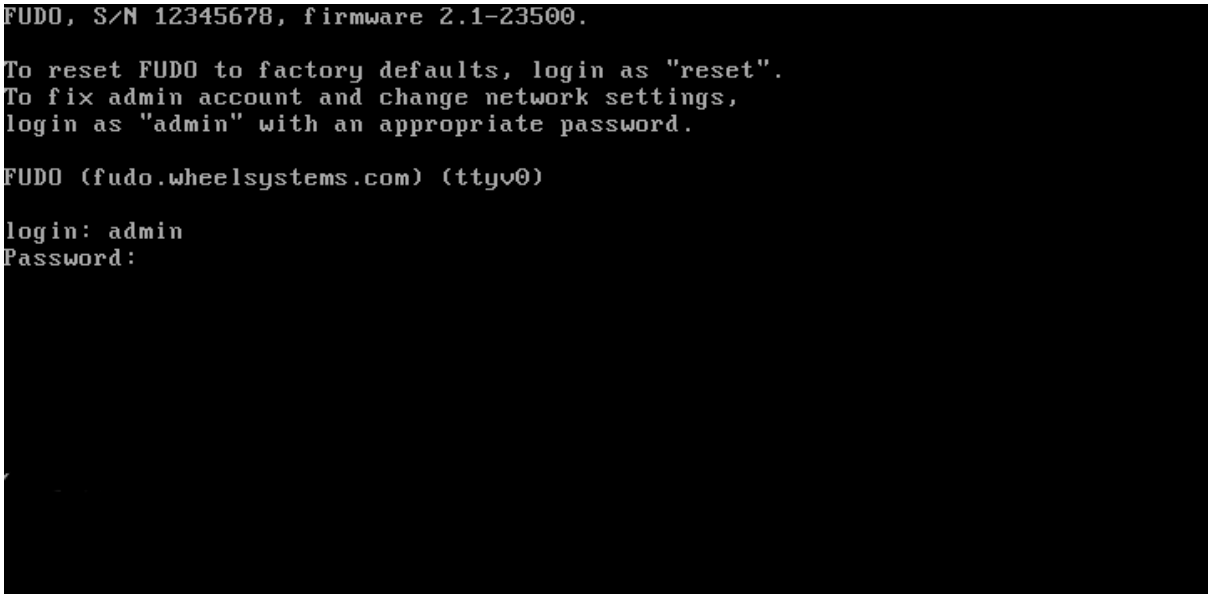
Informacja: Domyślne dane logowania:

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.



3. Wprowadź hasło do konta administratora.



4. Wpisz 2 i naciśnij klawisz *Enter*.

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

Choose an option (0):
```

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

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

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

6. Wprowadź nazwę interfejsu zarządzającego (poprzez interfejs zarządzający udostępniany jest panel administracyjny Fudo 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*.

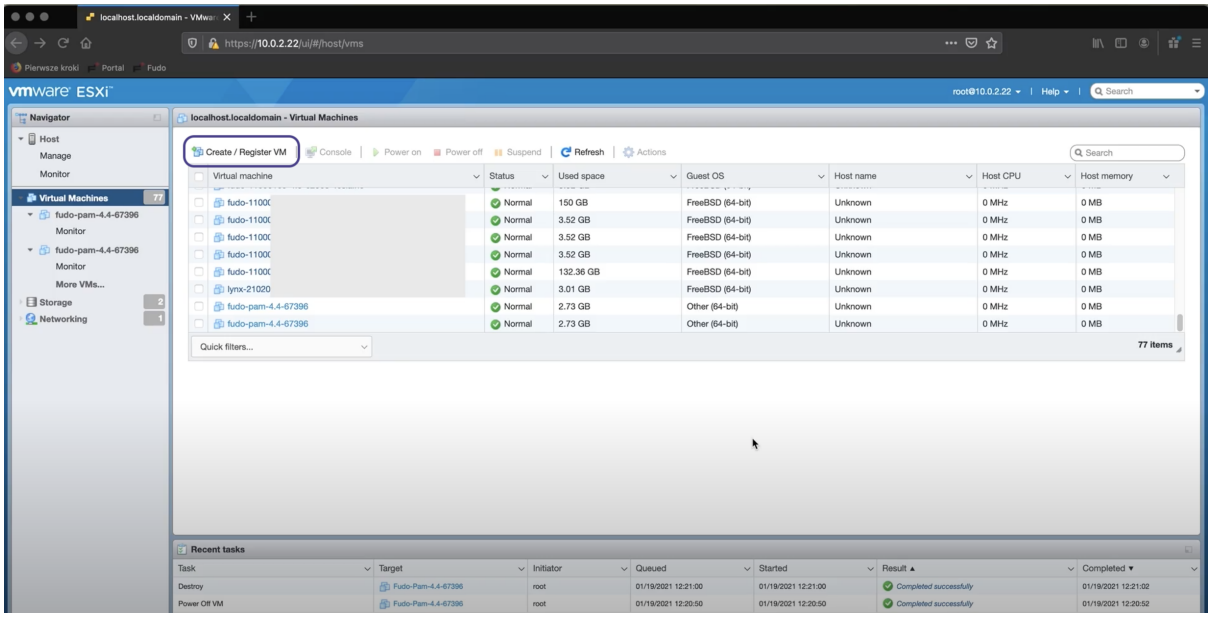
```
FUDO, S/N 12345678, firmware 2.1-23500.

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.

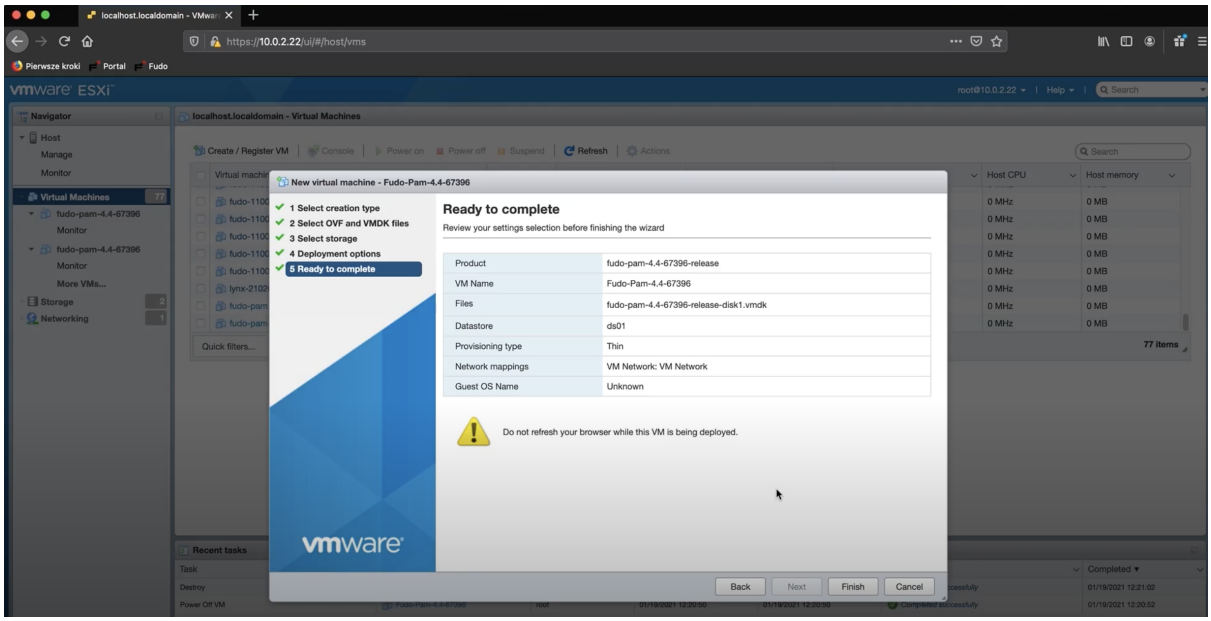
Inicjacja w VMware przy użyciu pliku OVA

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

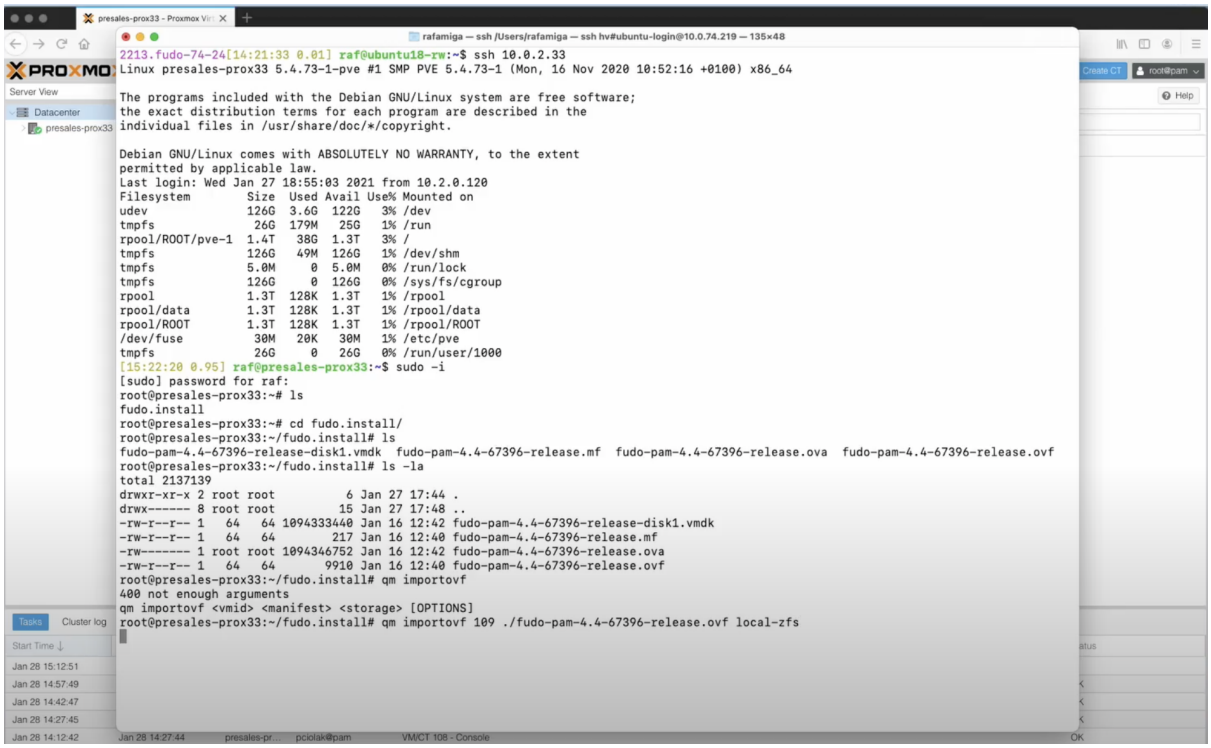
1. Utwórz nową maszynę wirtualną używając parametrów z manifestu pliku OVF, a następnie zaimportuj dyski do lokalizacji `local-zfs`:

   a. Zaloguj się do komputera zdalnego, np. za pomocą `ssh 10.0.2.33` i podaj hasło.

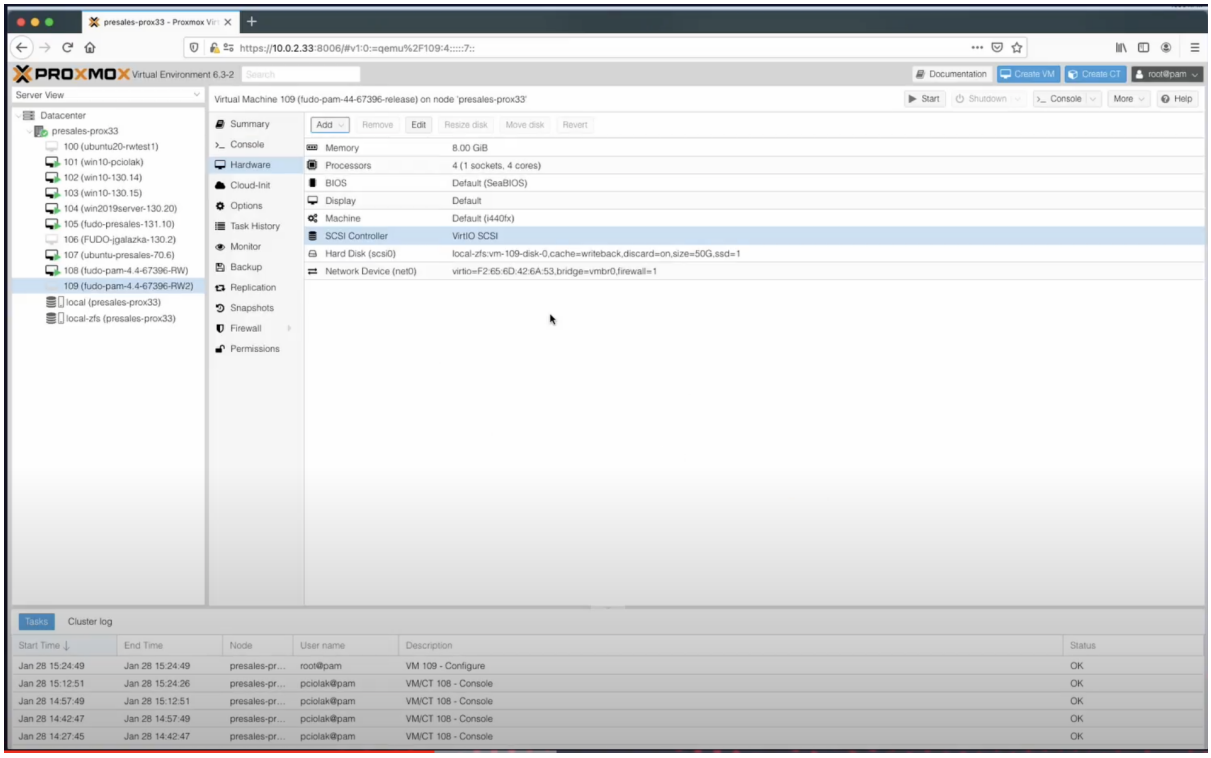
   b. W katalogu *fudo.install* wywołaj komendę: `qm importovf <vmid> <manifest> <storage> [OPTIONS]`

   Np:

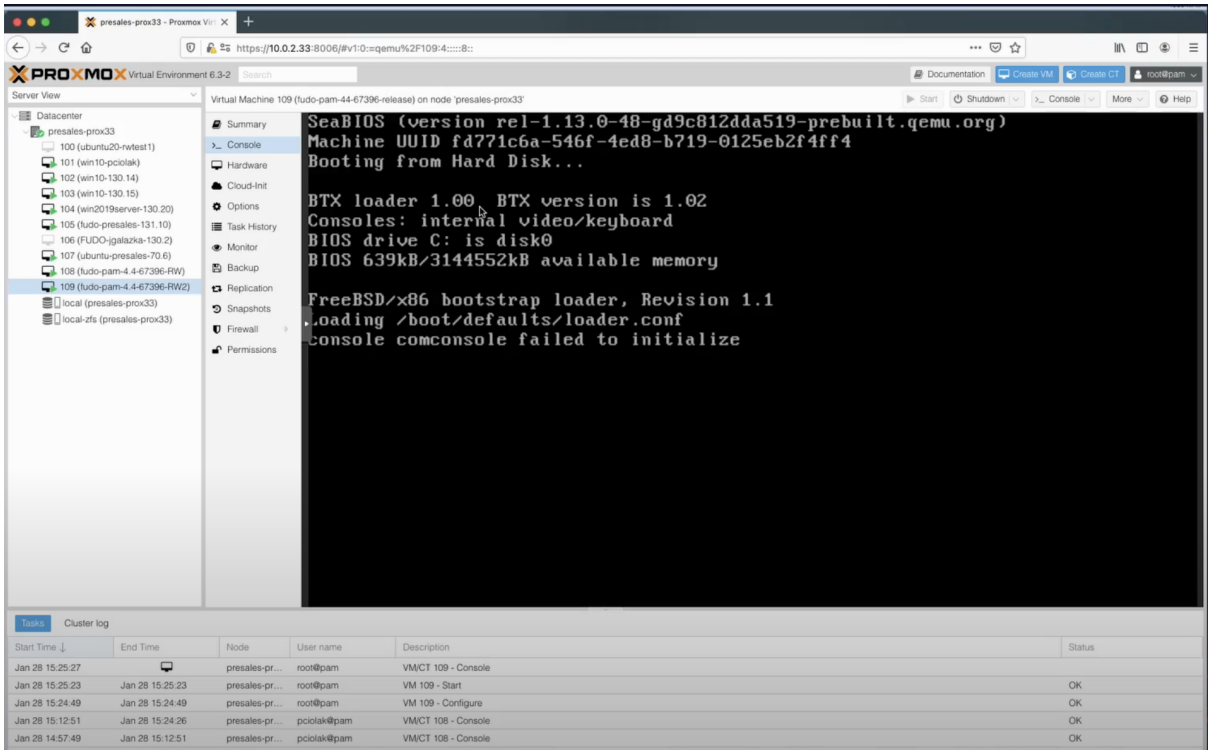
   ```
   qm importovf 109 ./fudo-one-36271-release.ovf local-zfs
   ```



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

ROZDZIAŁ 5

Szybki start

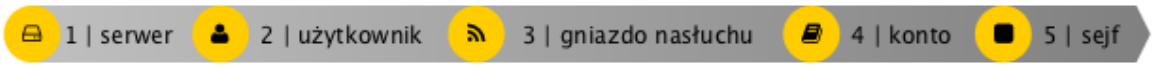
5.1 SSH

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



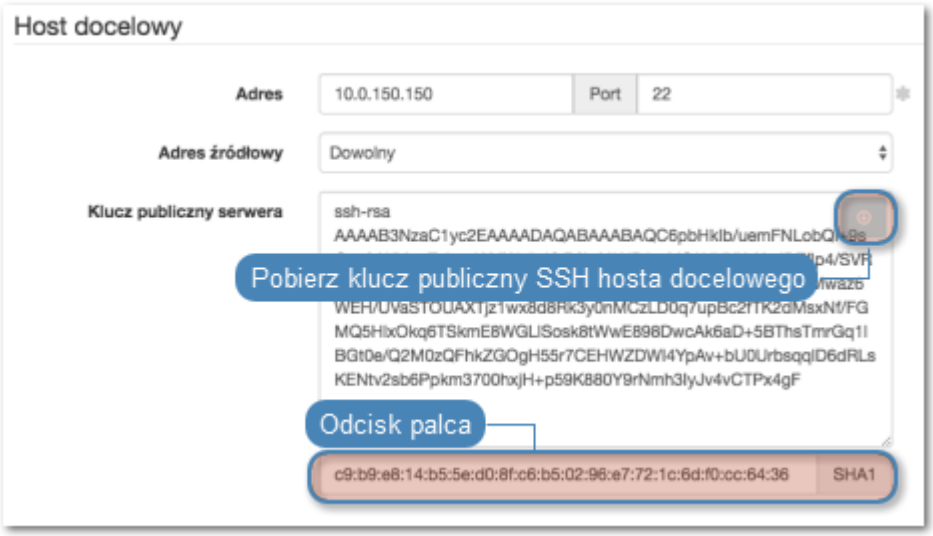
Dodanie serwera

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`
Uprawnienia	
Uprawnieni użytkownicy	✘
Adresy serwerów	
Adres IP	`10.0.150.150`
Port	`22`

4. Pobierz lub wprowadź klucz publiczny SSH hosta docelowego.



5. Kliknij *Zapisz*.

Dodanie użytkownika

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

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

3. Uzupełnij dane personalne użytkownika:

Parametr	Wartość
Ogólne	
Login	`john_smith`
Rola	`user`
Zablokowane	✗
Ważność konta	`Bezterminowe`

Zakładka *Ustawienia*	
Sejfy	✗

Zakładka *Dane Użytkownika*	
Domena Fudo	✗
Domena AD	✗
Baza LDAP	✗
Imię i nazwisko	`John Smith`
Email	✗
Organizacja	✗
Telefon	✗

Sekcja *Uwierzytelnienie*	
Niepowodzenia uwierzytelnienia	✗
Zastosuj złożoność hasła	✗
Dodaj metodę uwierzytelnienia	`Hasło statyczne`
Hasło	`john`

Zakładka *Uprawnienia*	
Uprawnieni użytkownicy	✗

4. Kliknij *Zapisz*.

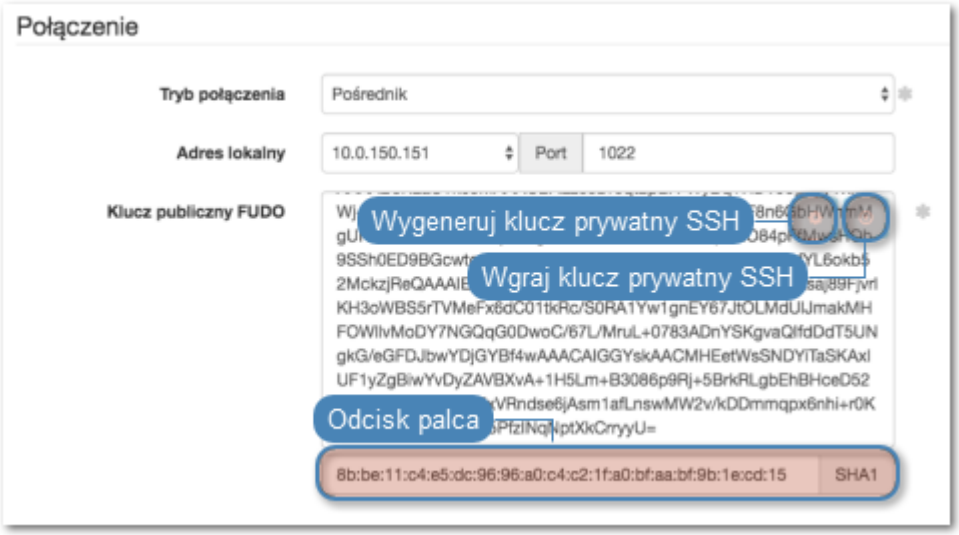
Dodanie gniazda nasłuchiwania

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	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`1022`
Adres zewnętrzny	✗
Port zewnętrzny	✗

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



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

5. Kliknij *Zapisz*.

Dodanie konta

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

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

Parametr	Wartość
Ogólne	
Nazwa	`admin_ssh_server`
Zablokowane	✘
Typ	`regular`
Nagrywanie sesji	`wszystko`
Notatki	✘
Retencja danych	
Nadpisz globalne ustawienia retencji	✘
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✘
Serwer	
Serwer	`ssh_server`
Dane uwierzytelniające	
Domena	✘
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✘

4. Kliknij *Zapisz*.

Dodanie sejfu

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

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

Parametr	Wartość
Nazwa	`ssh_safe`
Zablokowane	✘
Powiadomienia	✘
Powód logowania	✘
Wymagaj potwierdzenia	✘
Polityki	✘
Note access	`No access`

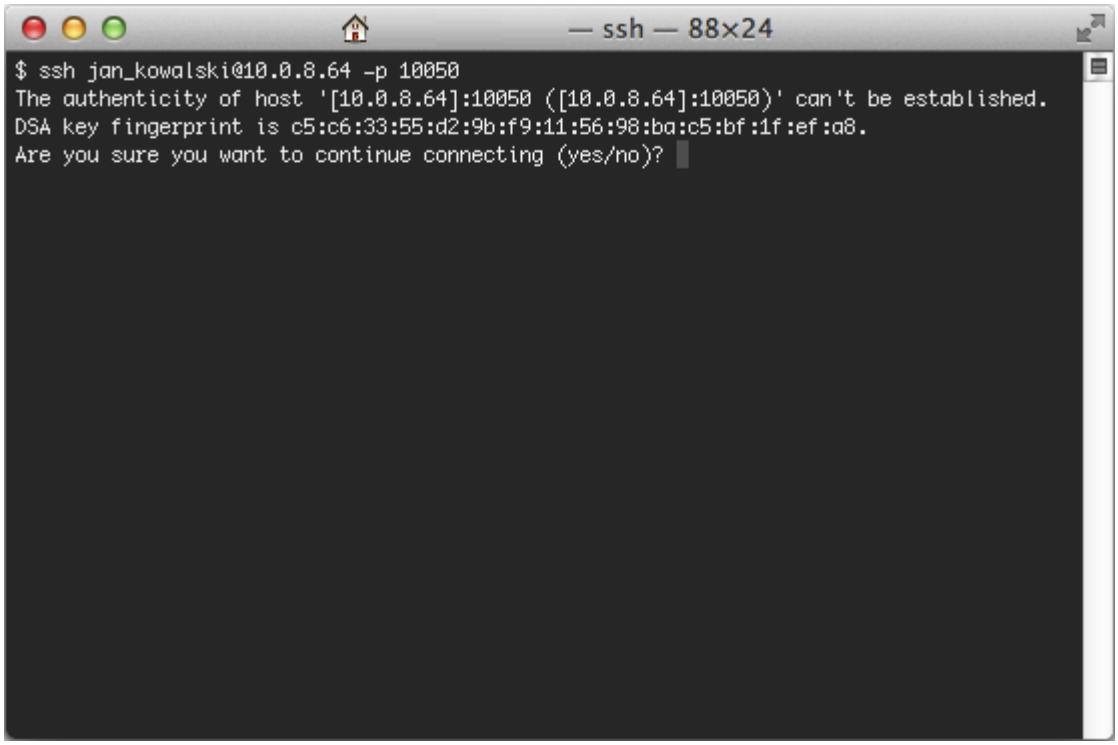
Funkcjonalność protokołów	
RDP	✘
SSH	✔
VNC	✘

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

5.1.3 Nawiązanie połączenia

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

Przykład:



Informacja: Zwróć uwagę na *Odcisk Palca* (fingerprint), który wyświetla się przy pierwszym połączeniu. Jest to ten sam odcisk, który został wygenerowany w czasie dodawania serwera.

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

5.1.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres `10.0.150.151`.
2. Wprowadź nazwę użytkownika oraz hasło, aby zalogować się do interfejsu administracyjnego Fudo 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

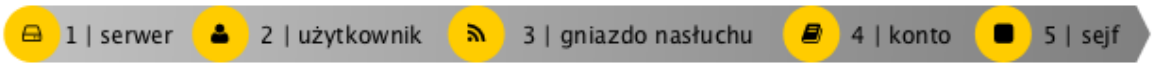
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie połączeń SSH ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *SSH* uwierzytelnia się przed Fudo Enterprise używając własnego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

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	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Tryb połączenia	`Bastion`
Adres lokalny	`10.0.150.151`
Port	22
Adres zewnętrzny	✗
Port zewnętrzny	✗

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

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

---

5. Kliknij *Zapisz*.

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

Dodanie konta

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

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

Parametr	Wartość
Ogólne	
Nazwa	`admin_ssh_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`ssh_server`
Dane uwierzytelniające	
Domena	✗
Login	`root`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	`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
Ogólne	
Nazwa	`ssh_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

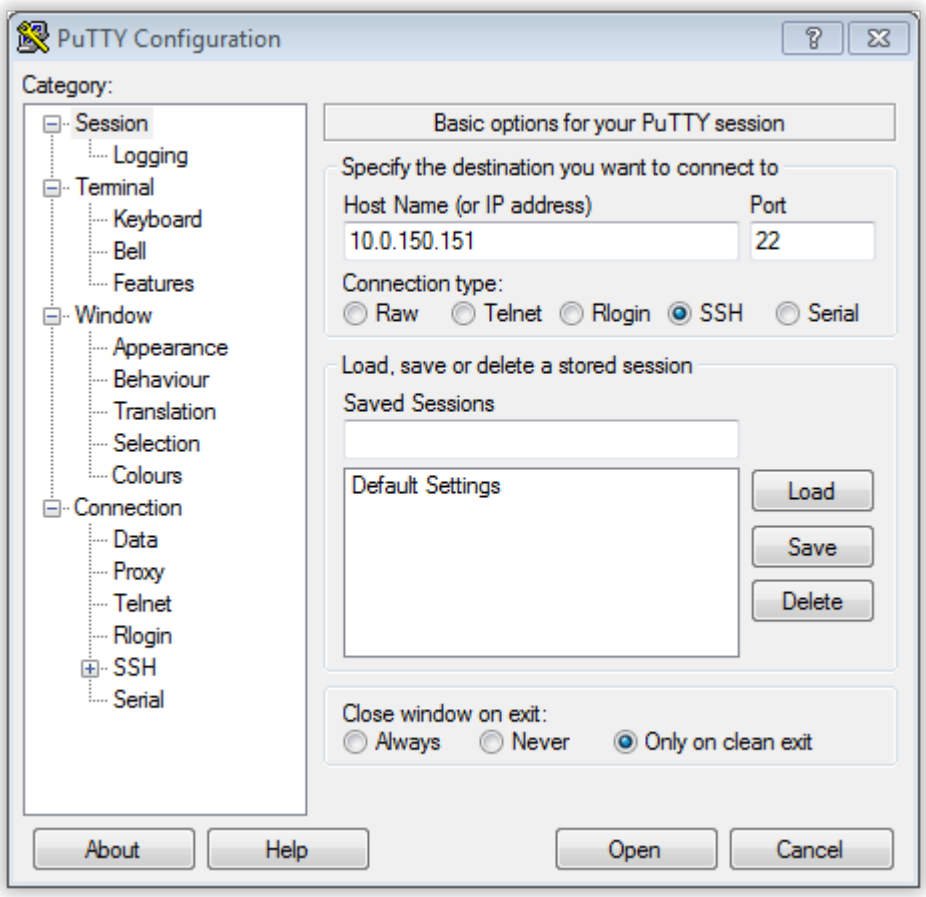
Funkcjonalność protokołów	
RDP	✗
SSH	✓
VNC	✗

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

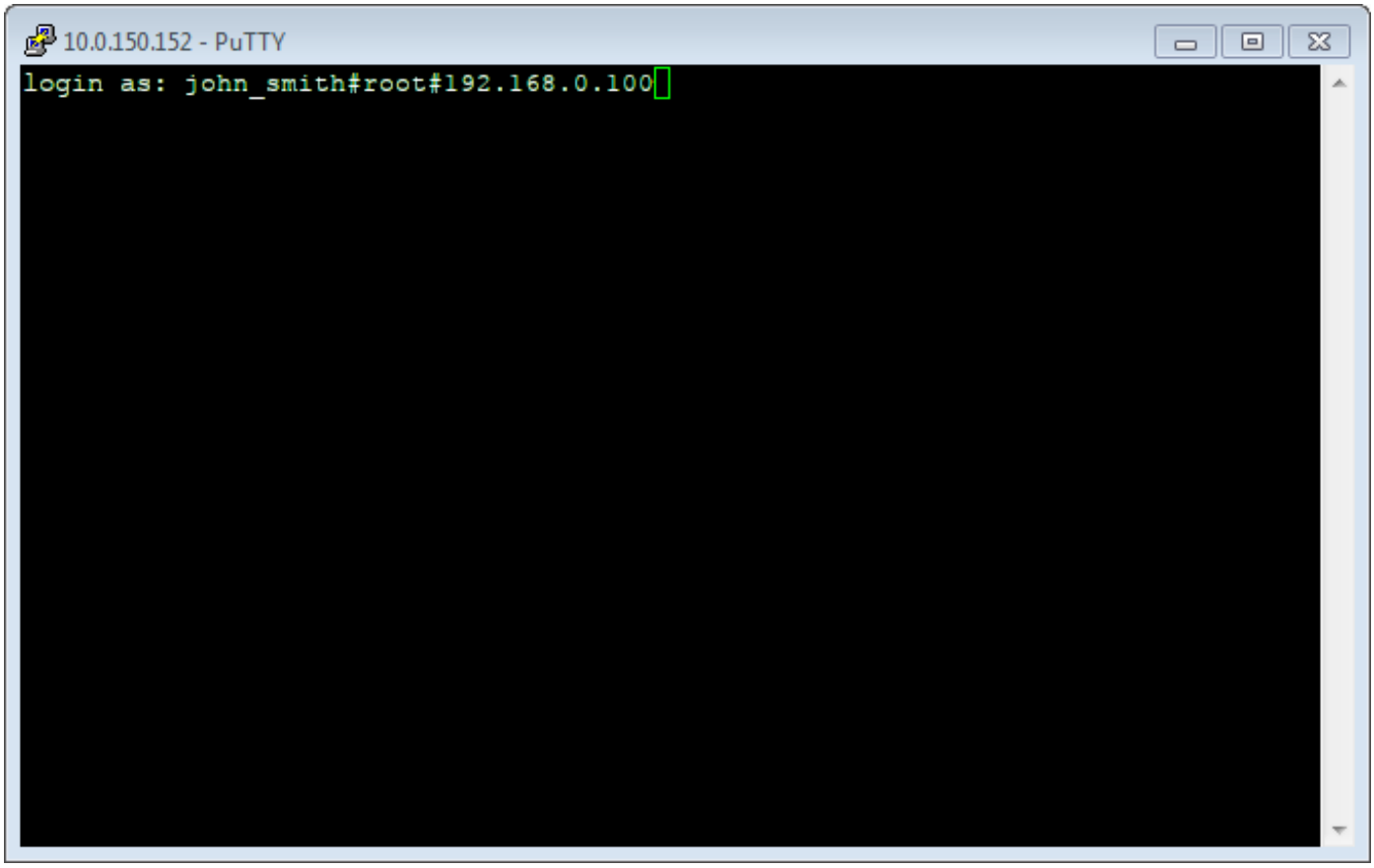
5.2.3 Nawiązanie połączenia

PuTTY - klient SSH dla systemu operacyjnego Microsoft Windows

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



4. Kliknij *Open*.
5. Wprowadź nazwę użytkownika, 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*

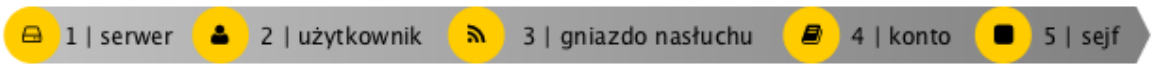
5.3 RDP

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`

Uprawnienia	
Uprawnieni użytkownicy	✗

Adresy serwerów	
Adres IP	`10.0.35.10`
Port	`3389`

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

Dodanie użytkownika

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

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

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

4. Kliknij *Zapisz*.

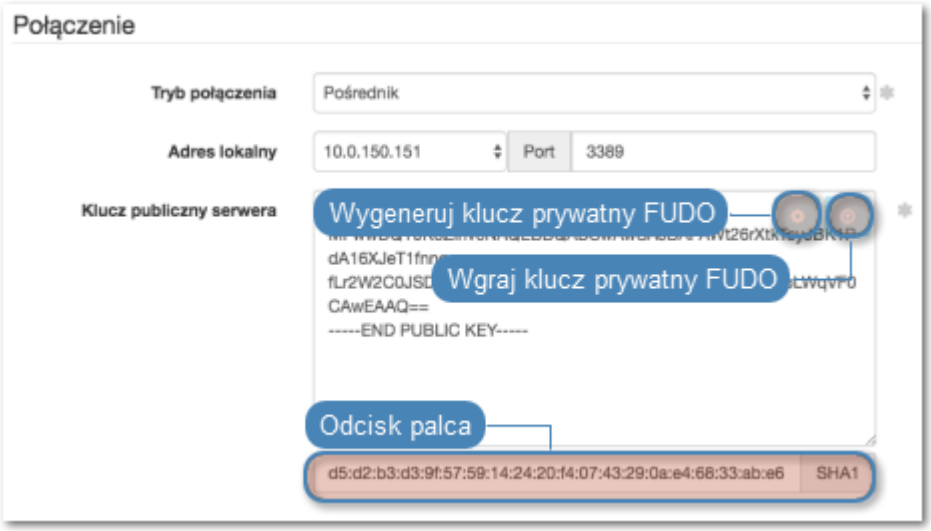
Dodanie gniazda nasłuchiwania

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

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

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

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



5. Kliknij *Zapisz*.

Dodanie konta

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

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

Parametr	Wartość
Ogólne	
Nazwa	`admin_rdp_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✓
Język OCR	`Angielski`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`rdp_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

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

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

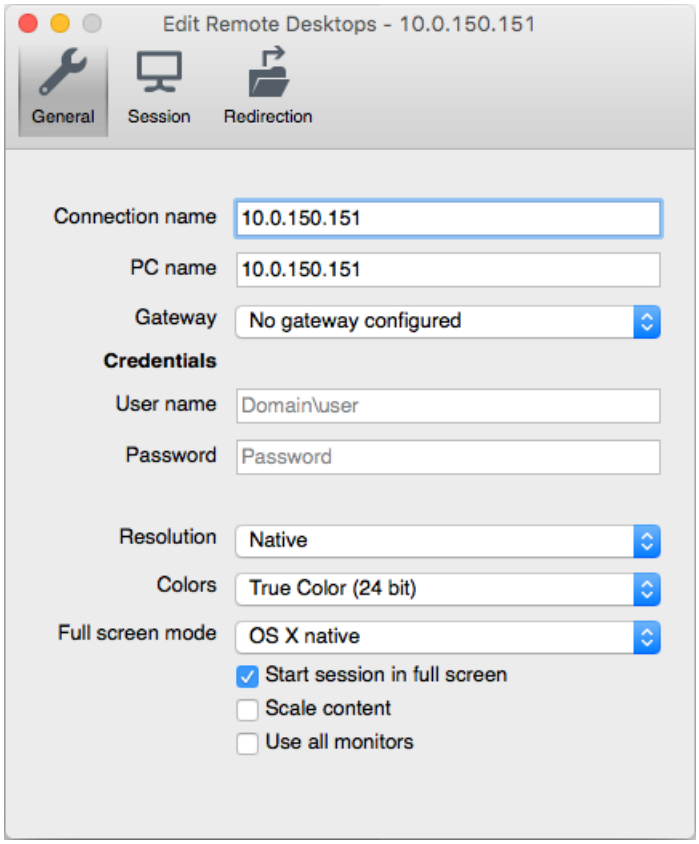
Parametr	Wartość
Ogólne	
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

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

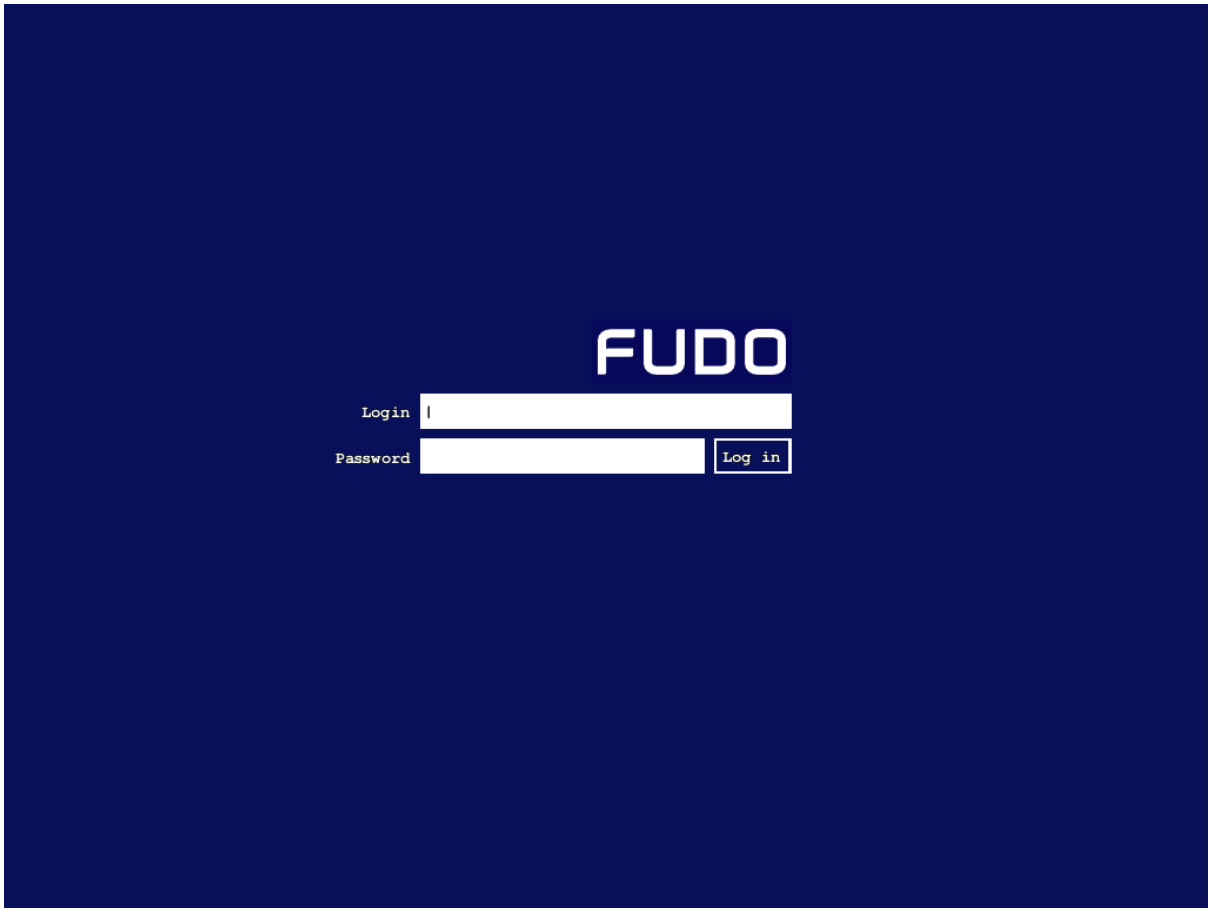
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_ smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_rdp_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.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

5.3.3 Nawiązanie połączenia

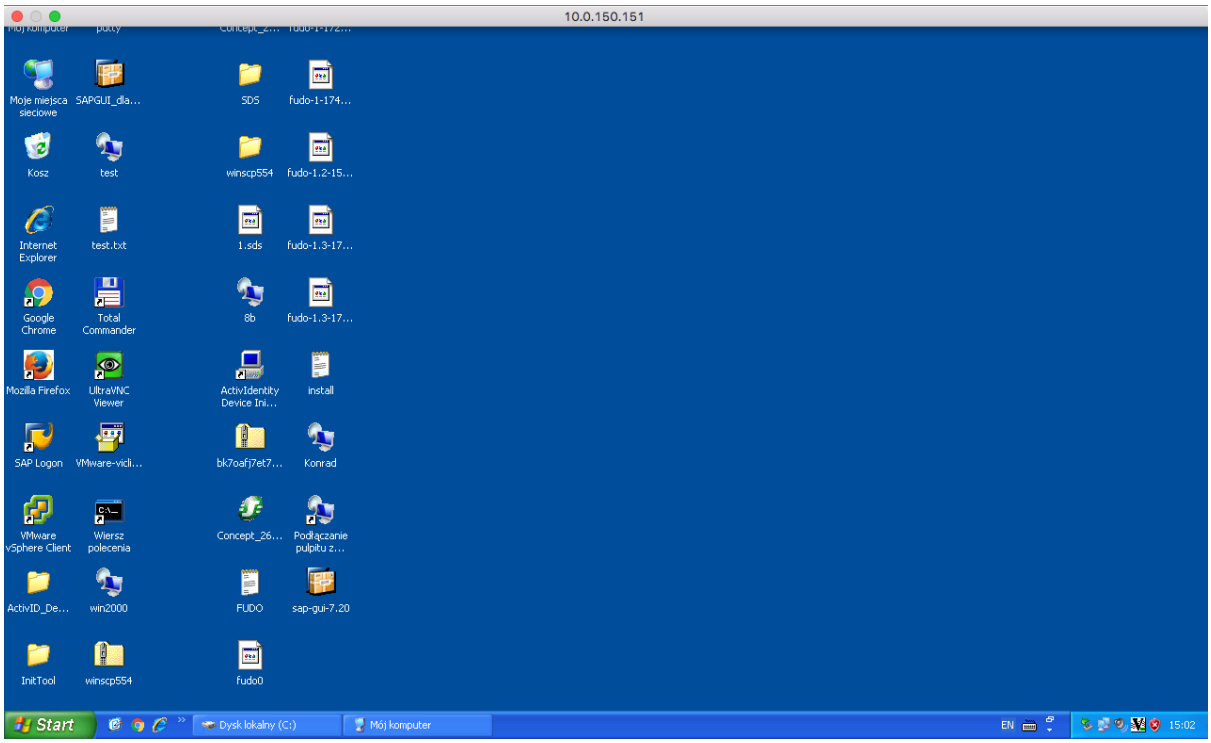
1. Uruchom klienta połączeń RDP.
2. Skonfiguruj połączenie zdalnego pulpitu.



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



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

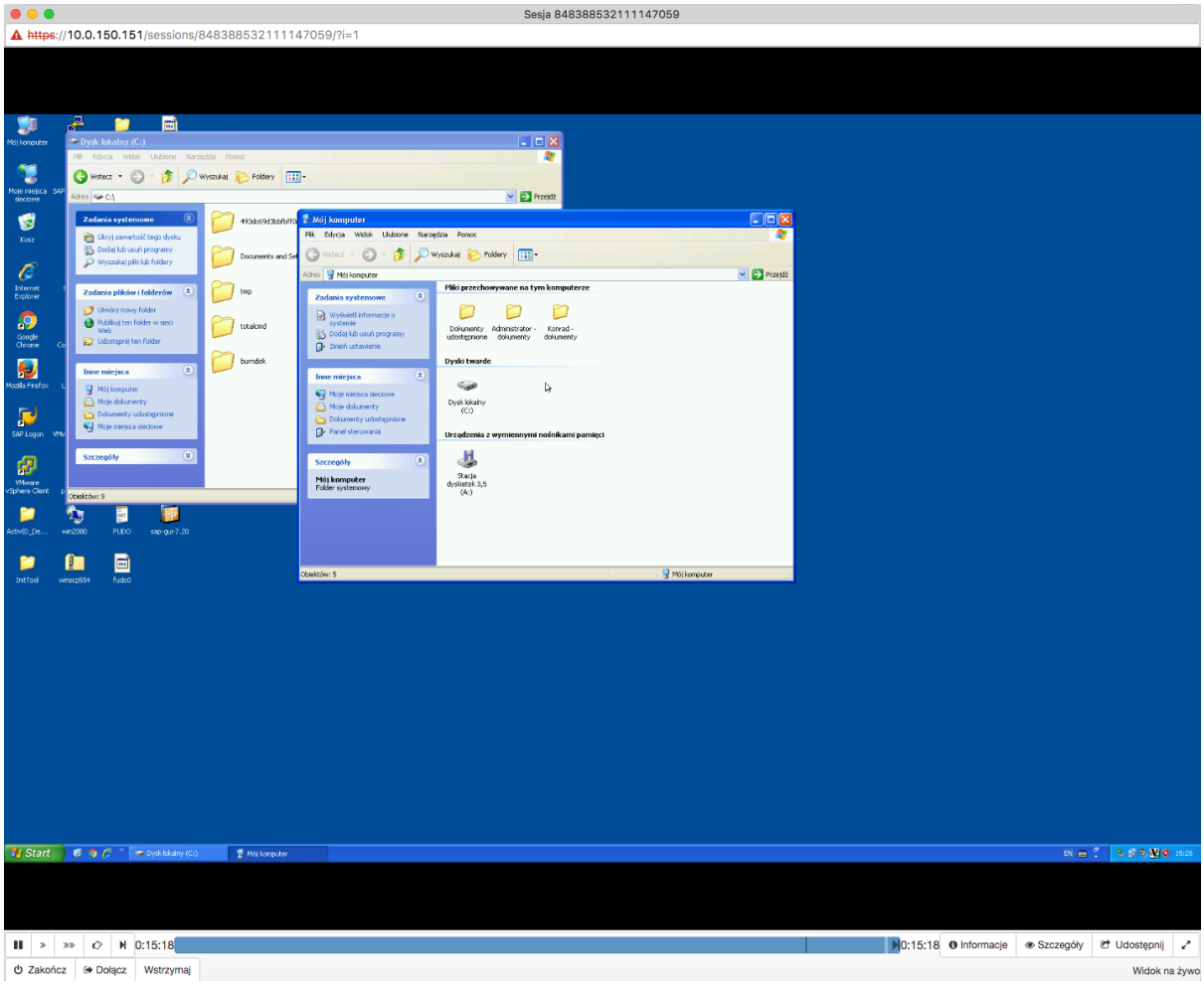


5.3.4 Podgląd sesji połączeniowej

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

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

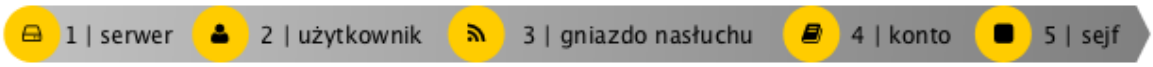
5.4 RDP w trybie bastionu

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`

Uprawnienia	
Uprawnieni użytkownicy	✘

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

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

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

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

Parametr	Wartość
Ogólne	
Nazwa	`rdp_listener_bastion`
Zablokowane	✗
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Komunikat	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`bastion`
Adres lokalny	`10.0.150.151`
Port	`3389`
Adres zewnętrzny	✗
Port zewnętrzny	✗

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

Dodanie konta

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

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

Parametr	Wartość
Ogólne	
Nazwa	`admin_rdp_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
OCR sesji	✓
Język OCR	`Angielski`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`rdp_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	`Statyczne, bez ograniczeń`

4. Kliknij *Zapisz*.

Dodanie sejfu

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

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

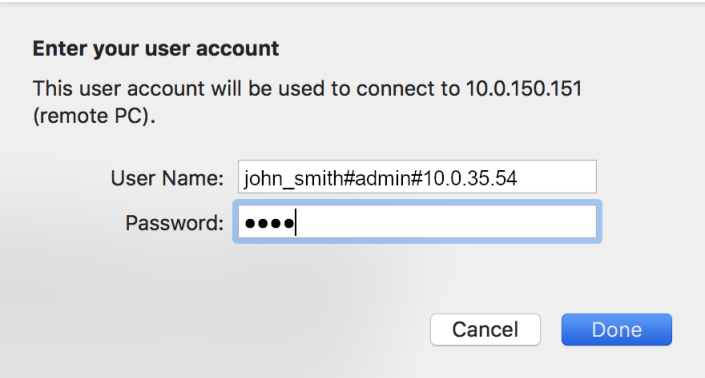
Parametr	Wartość
Ogólne	
Nazwa:	`rdp_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

Funkcjonalność protokołów	
RDP	✓
SSH	✗
VNC	✗

4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij [+].
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_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*.

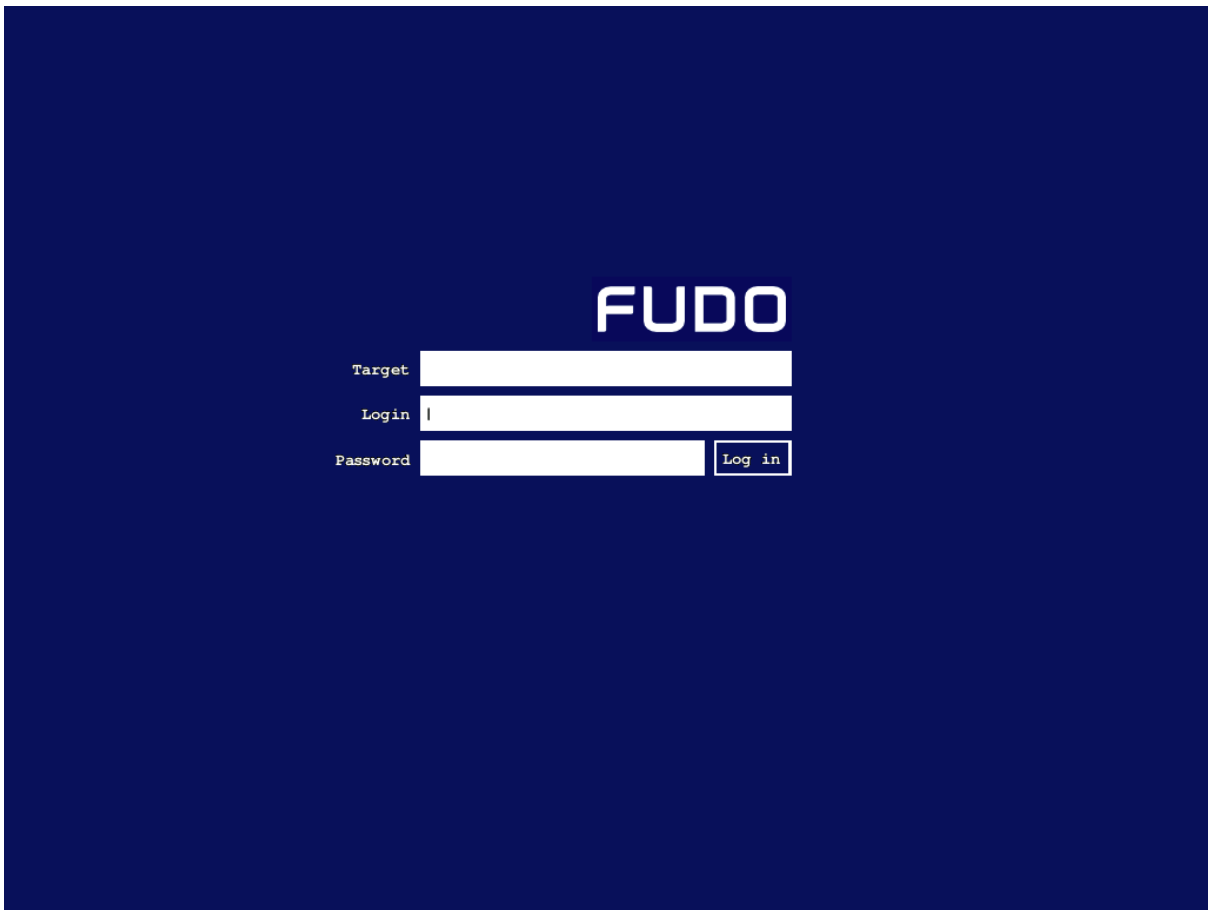
5.4.3 Nawiązanie połączenia

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.

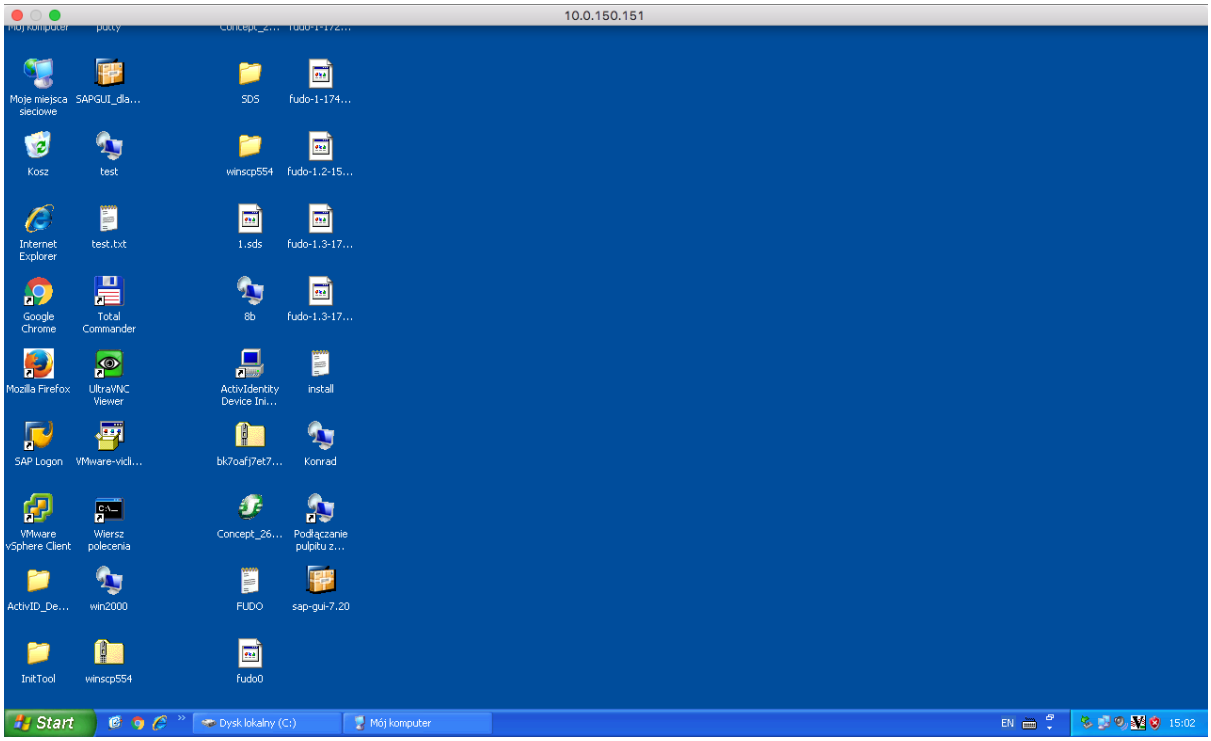


Informacja:

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



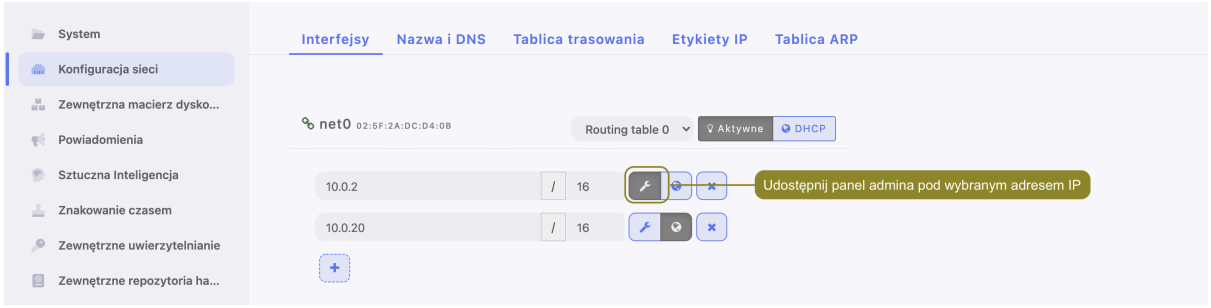
- W przypadku gdy wskazane konto nie istnieje, Fudo Enterprise dokona próby dopasowania podanego ciągu znaków do nazwy serwera. Jeśli system nie stwierdzi istnienia obiektu serwera o takiej nazwie, spróbuje dokonać dopasowania na podstawie nazwy DNS hosta.
- Fudo Enterprise pozwala na zastosowanie własnego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



5.4.4 Podgląd sesji połączeniowej

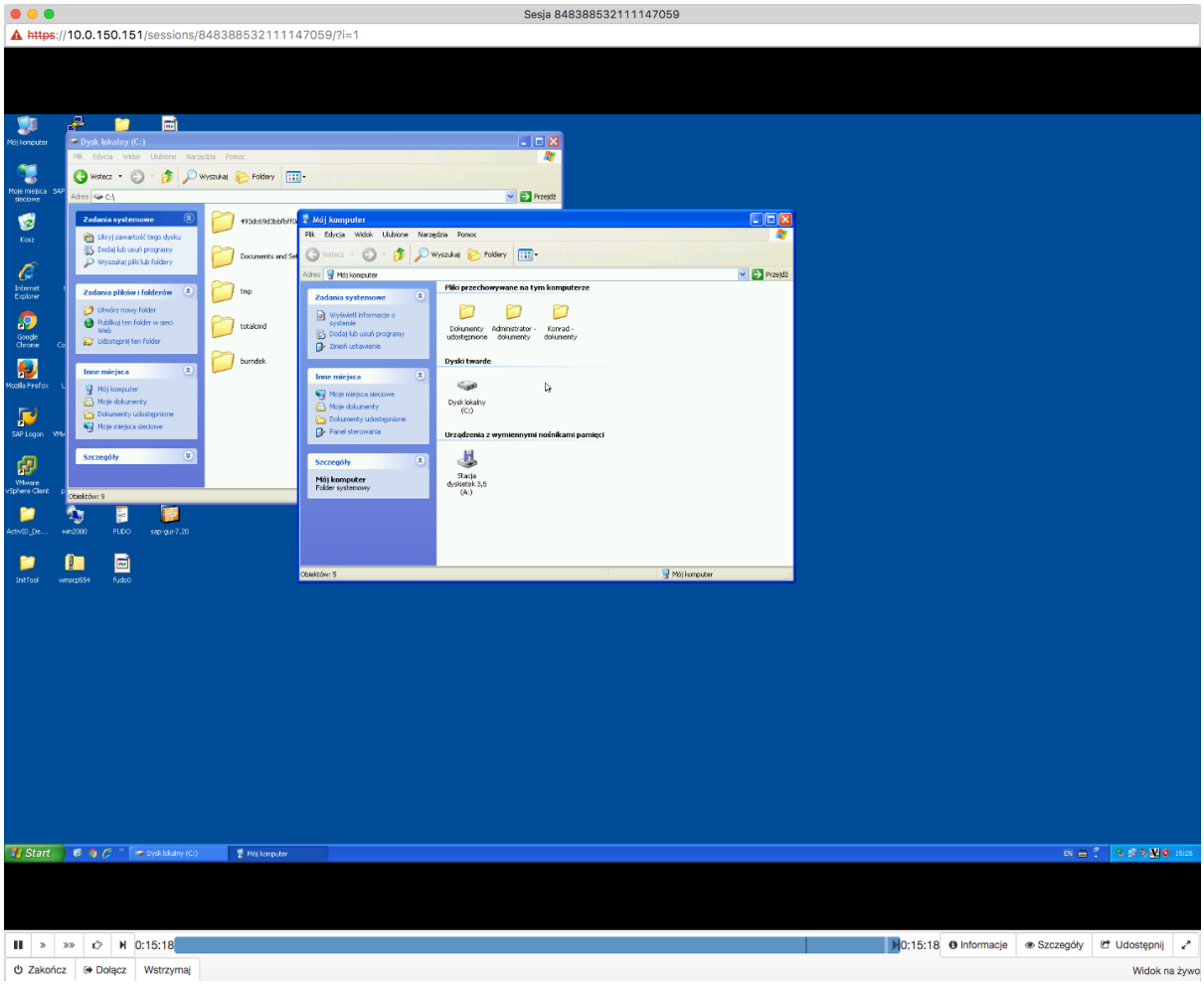
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Fudo Enterprise.

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.

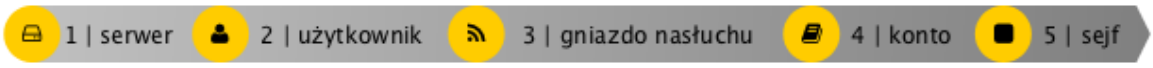
Informacja: Połączenia telnet realizowane za pośrednictwem Fudo Enterprise nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu

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

4. Kliknij *Zapisz*.

Dodanie użytkownika

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

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

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

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

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

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

3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`telnet_listener`
Zablokowane	✗
Protokół	`Telnet`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`23`
Użyj szyfrowania TLS	✗

4. Kliknij *Zapisz*.

Dodanie konta

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

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

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

4. Kliknij *Zapisz*.

Dodanie sejfu

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

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

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

Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

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

5.5.3 Nawiązanie połączenia

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

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

3. Wprowadź dane uwierzytelniające użytkownika na Fudo 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,

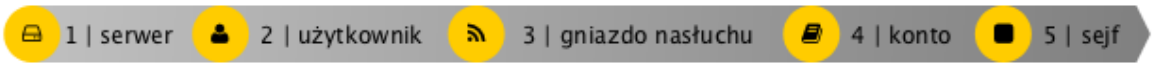
że użytkownik łączy się ze zdalnym serwerem za pomocą klienta protokołu Telnet używając indywidualnego loginu i hasła. Fudo Enterprise uwierzytelnia administratora na podstawie danych zapisanych w lokalnej bazie użytkowników, zestawia połączenie ze zdalnym zasobem i rozpoczyna rejestrowanie akcji użytkownika.

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	✗
Zablokowane	✗
Protokół	`Telnet 5250`
Adres źródłowy	`Dowolny`
Użyj szyfrowania TLS	✗

Uprawnienia	
Uprawnieni użytkownicy	✗

Adresy serwerów	
Adres IP	`10.0.35.137`
Port	`23`

4. Kliknij *Zapisz*.

Dodanie użytkownika

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

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

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

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

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

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

Parametr	Wartość
Nazwa	`telnet_listener`
Zablokowane	✗
Protokół	`Telnet 5250`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.150.151`
Port	`23`
Użyj szyfrowania TLS	✗

4. Kliknij *Zapisz*.

Dodanie konta

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

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

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

4. Kliknij *Zapisz*.

Dodanie sejfu

Sejf bezpośrednio reguluje dostęp użytkowników do monitorowanych serwerów. Określa dostępną

dla użytkowników funkcjonalność protokołów, polityki proaktywnego monitoringu połączeń i szczegóły relacji użytkownik-serwer.

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

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

Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

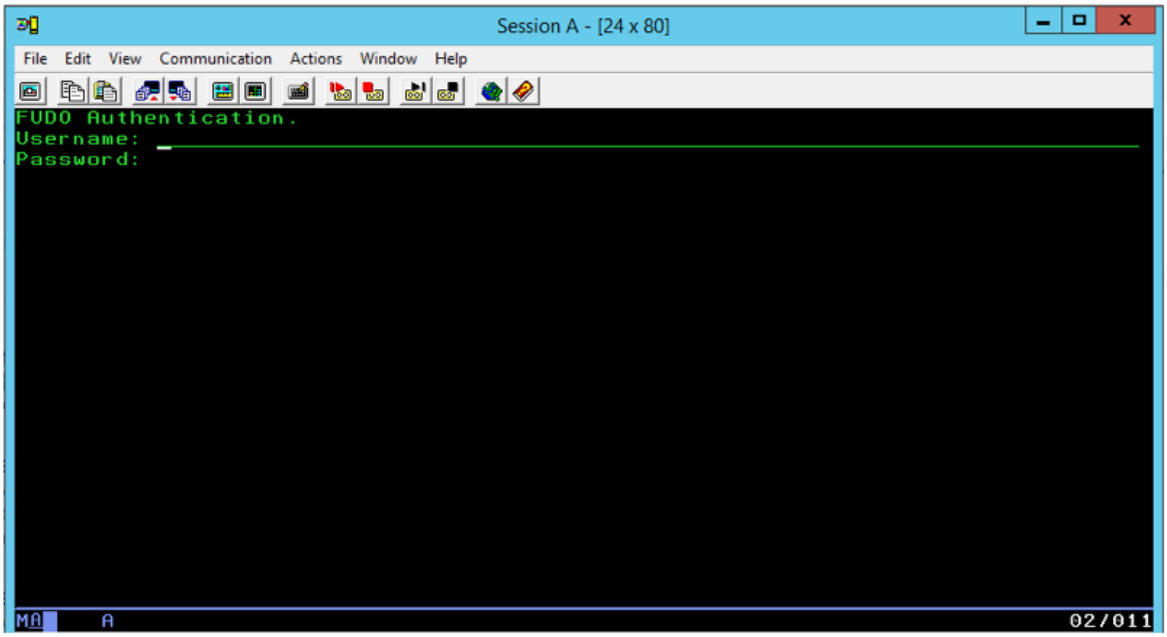
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij + *Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij + *Dodaj konto*.
10. Znajdź konto `admin_telnet_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda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

5.6.3 Nawiązanie połączenia

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

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

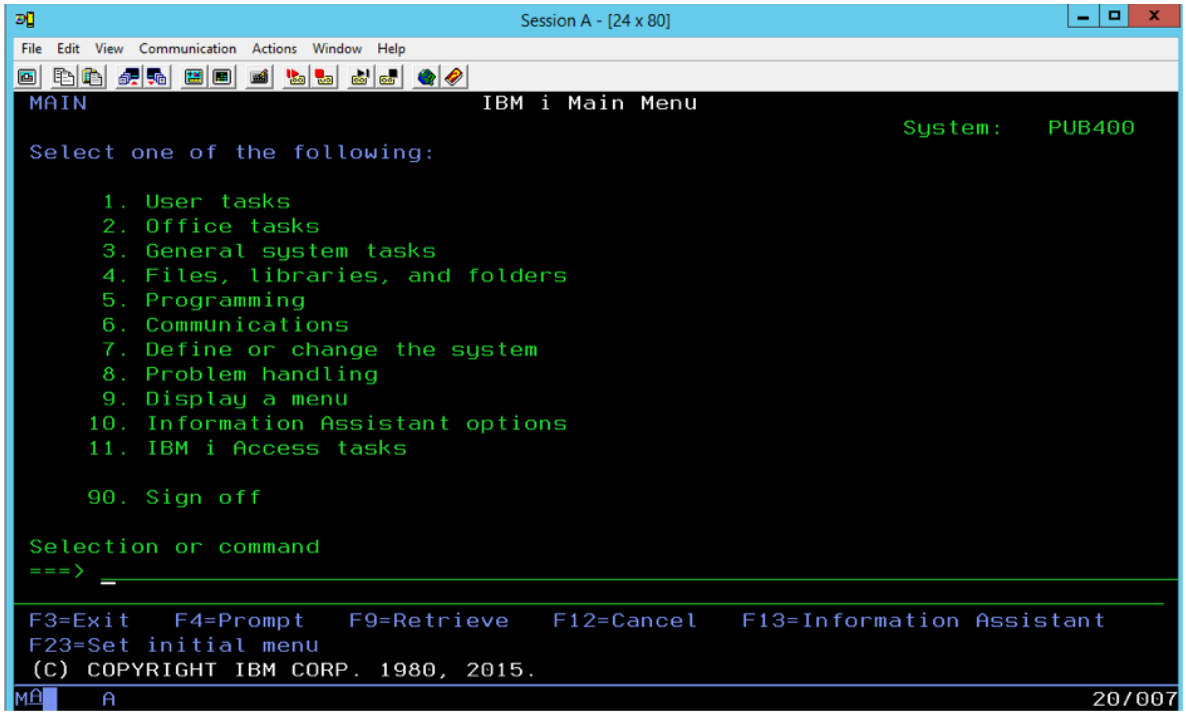
3. Wprowadź dane uwierzytelniające użytkownika na Fudo Enterprise.



4. Wprowadź dane uwierzytelniające użytkownika na serwerze:

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

Informacja: Połączenia telnet nie wspierają mechanizmów podmiany danych logowania.



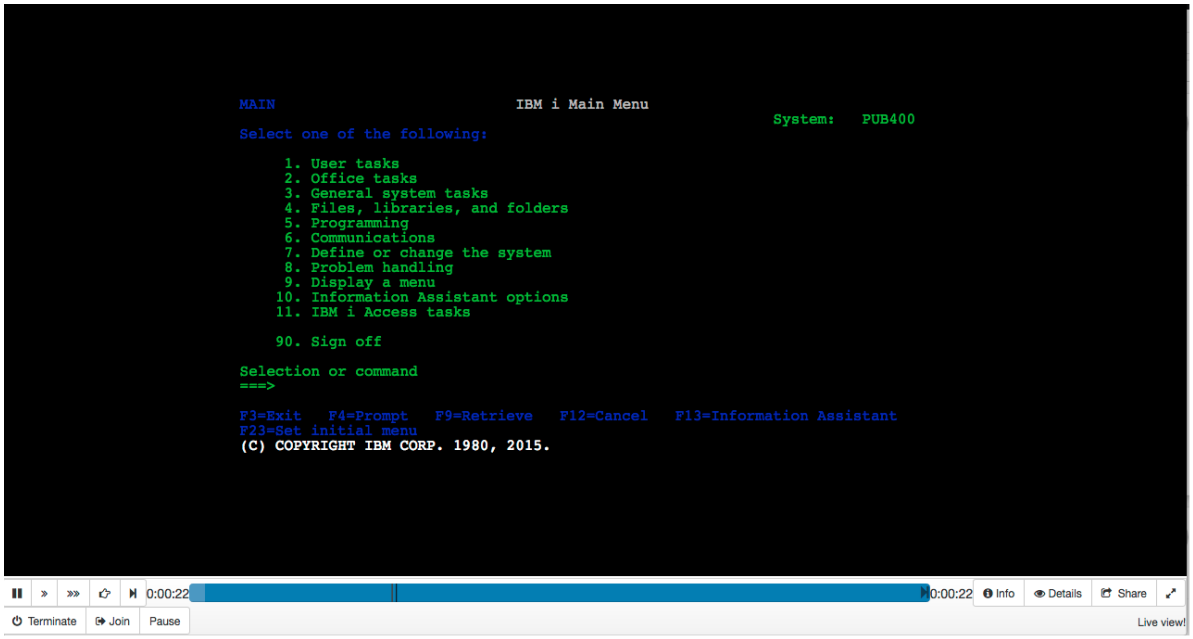
5.6.4 Podgląd sesji połączeniowej

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

5.7 MySQL

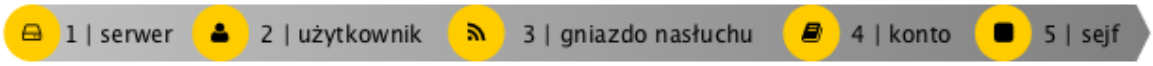
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie połączeń ze zdalnym serwerem baz danych MySQL. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem za pomocą klienta MySQL używając indywidualnego loginu i hasła. Fudo Enterprise 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`
Uprawnienia	
Uprawnieni użytkownicy	✗
Adresy serwerów	
Adres IP	`10.0.1.35`
Port	`3306`

4. Kliknij *Zapisz*.

Dodanie użytkownika

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

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

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

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

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

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

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

4. Kliknij *Zapisz*.

Dodanie konta

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

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

Parametr	Wartość
Ogólne	
Nazwa	`admin_mysql_server`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji po upływie	`61 dni`
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`mysql_server`
Dane uwierzytelniające	
Domena	✗
Login	`admin`
Zastąp sekret	`hasłem`
Hasło	`password`
Powtórz hasło	`password`
Polityka modyfikatora haseł	✗

4. Kliknij *Zapisz*.

Dodanie sejfu

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

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

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

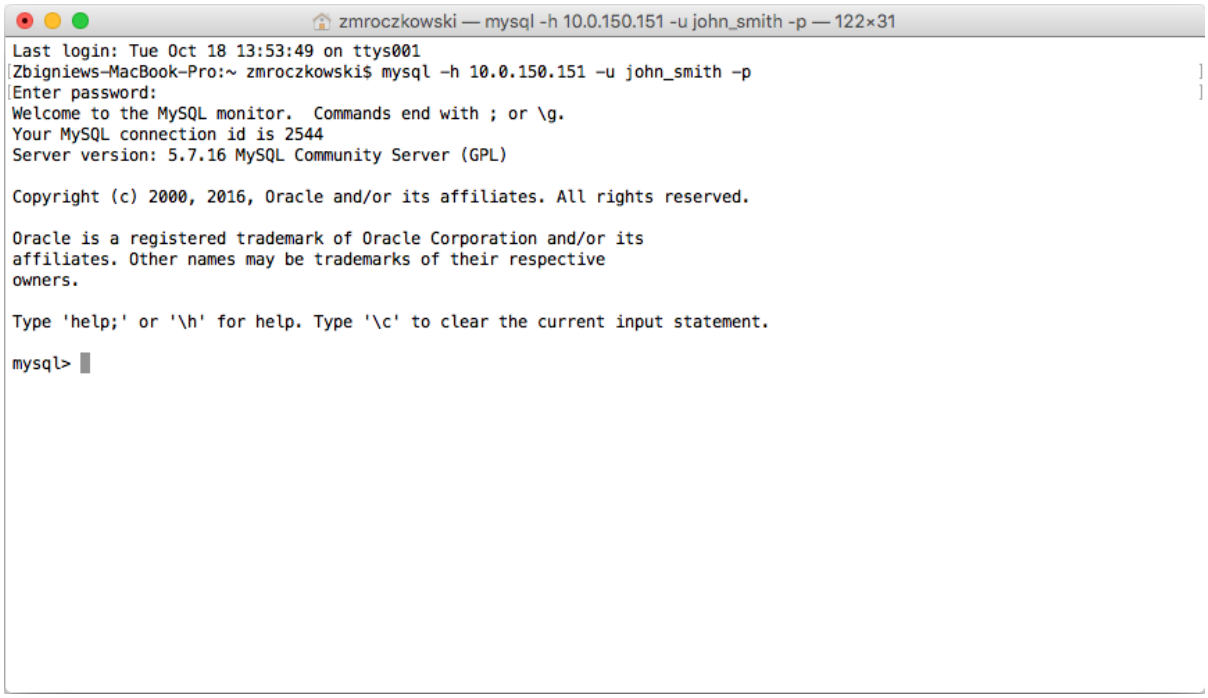
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

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

5.7.3 Nawiązanie połączenia

1. Uruchom terminal tekstowy.

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



4. Kontynuuj przeglądanie zawartości serwera poprzez zapytania sql.

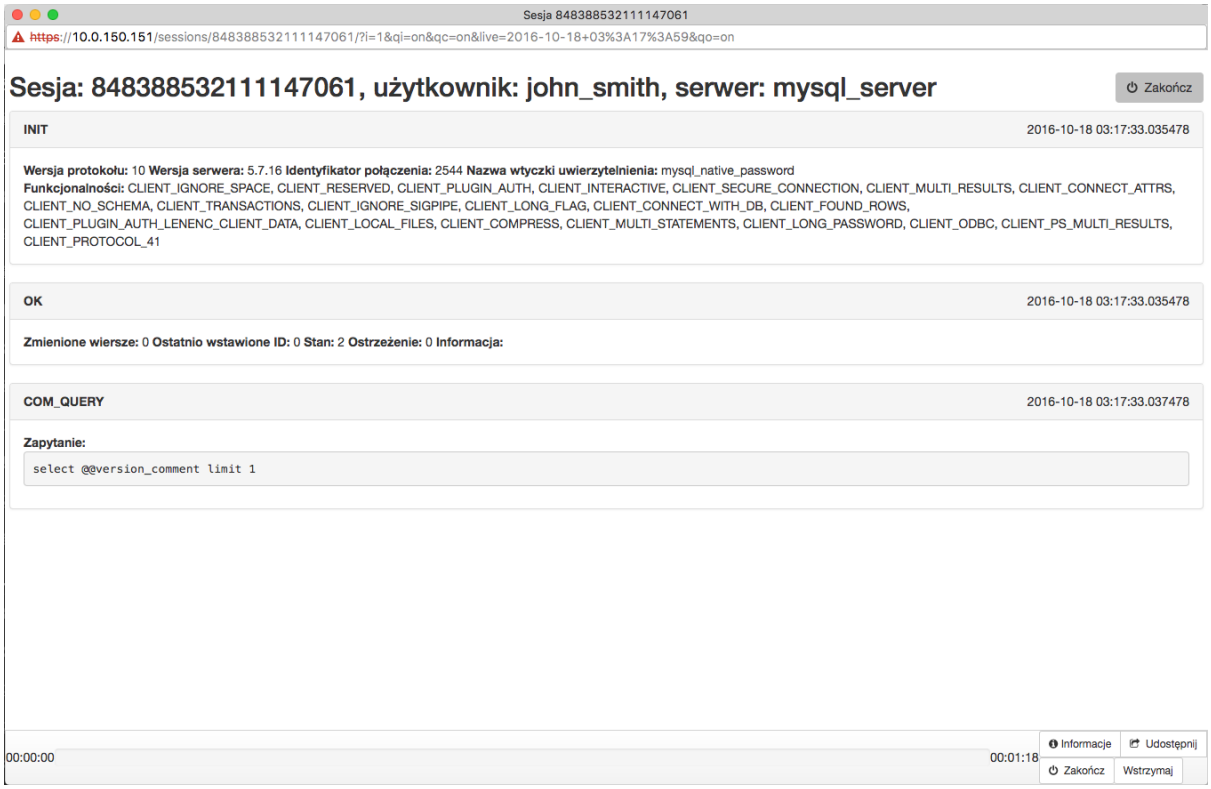
5.7.4 Podgląd sesji połączeniowej

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

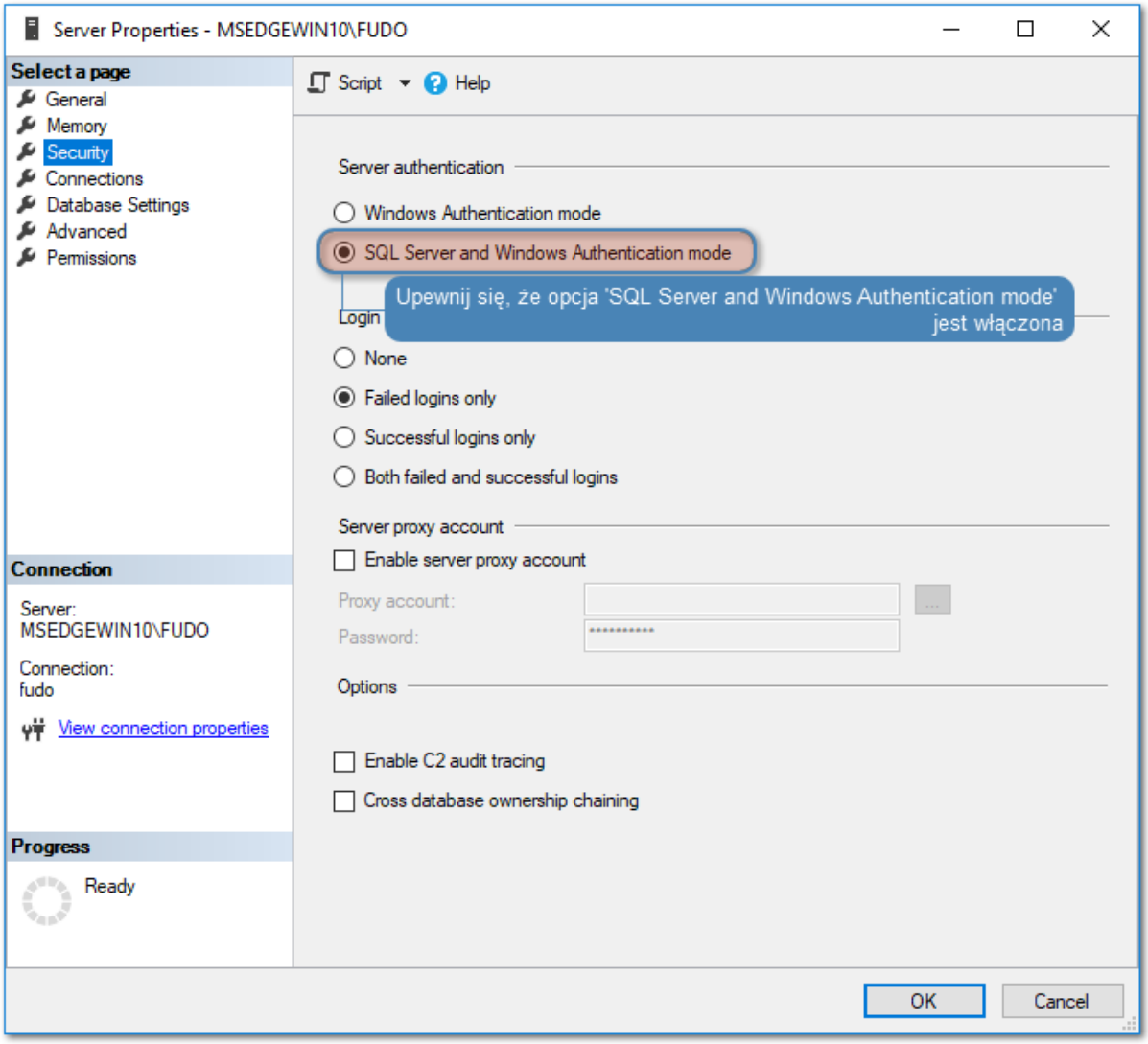
5.8 MS SQL

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*).

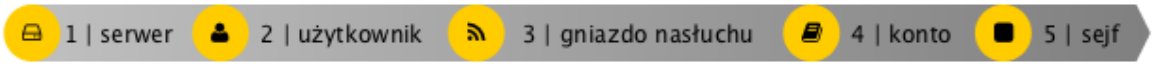
5.8.1 Założenia

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

4. Kliknij *Zapisz*.

Dodanie użytkownika

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

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

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

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

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

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

Parametr	Wartość
Ogólne	
Nazwa	`MSSQL_proxy`
Zablokowane	✗
Protokół	`MS SQL (TDS)`
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`proxy`
Adres lokalny	`10.0.150.150`
Port	`1433`

4. Kliknij *Zapisz*.

Dodanie konta

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

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

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

4. Kliknij *Zapisz*.

Dodanie sejfu

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

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

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

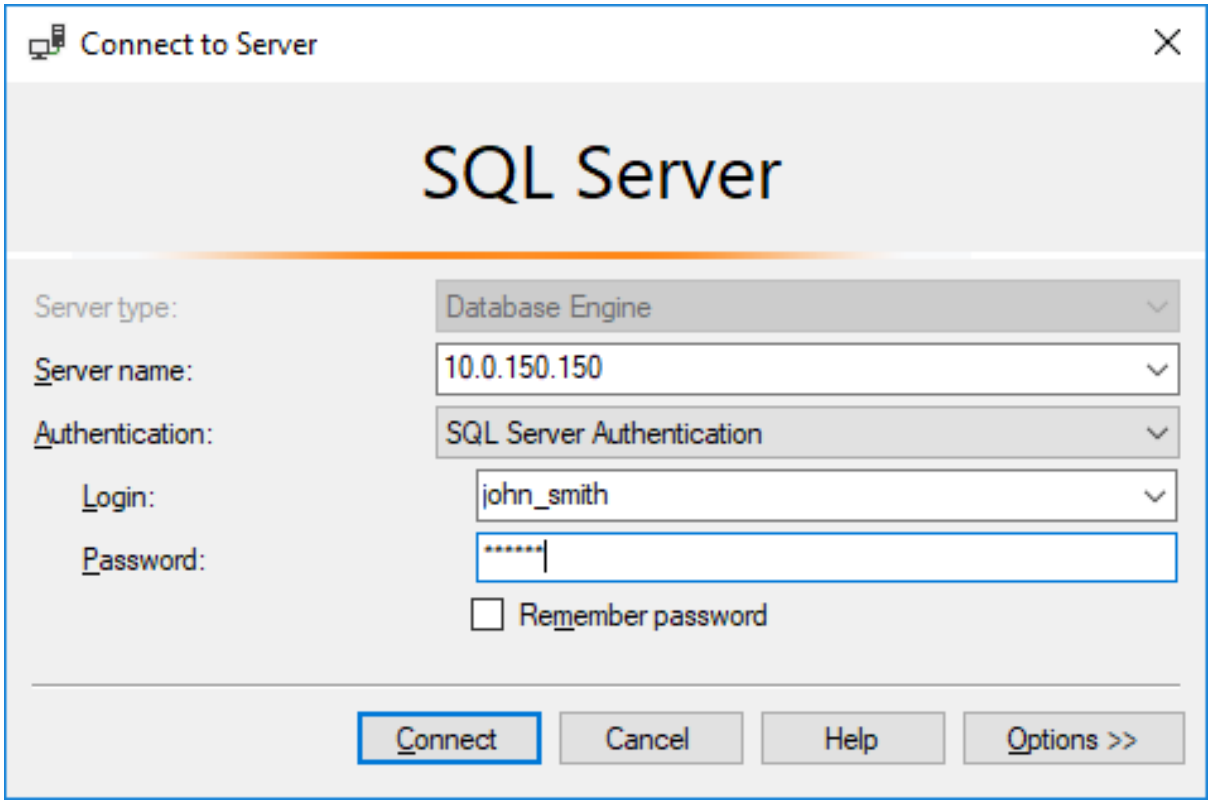
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

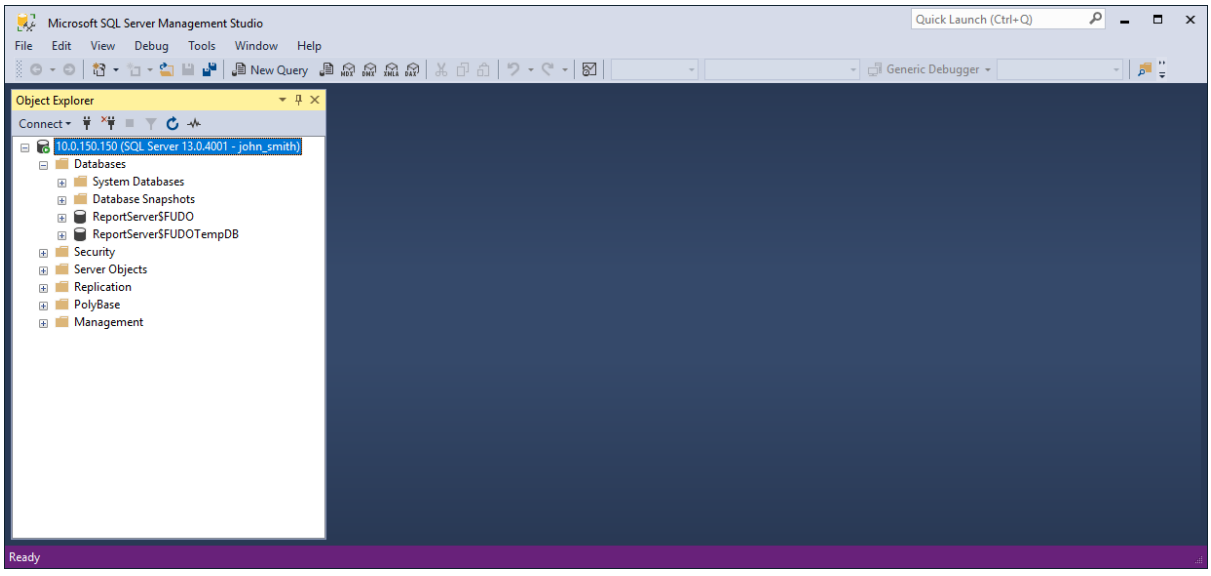
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij + *Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij + *Dodaj konto*.
10. Znajdź konto `admin_mssql_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.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

5.8.3 Nawiązanie połączenia

1. Uruchom *SQL Server Management Studio*.

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





5.8.4 Podgląd sesji połączeniowej

1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Fudo 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 którejś z już trwających sesji. Jeśli tak jest, sesje są agregowane w jedną.

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

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

Tematy pokrewne:

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

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

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

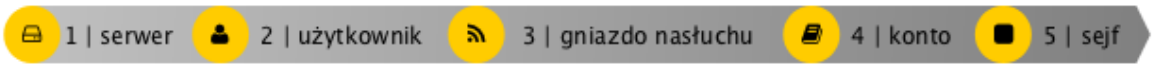
Model	Maksymalna zalecana liczba jednoczesnych połączeń HTTP*
F100x	2
F300x	5
F500x	10

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

Uprawnienia	
Uprawnieni użytkownicy	✗

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

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

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

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

Parametr	Wartość
Ogólne	
Nazwa	`twitter_listener`
Zablokowane	✘
Protokół	`HTTP`
Renderuj sesje	✔
Uprawnienia	
Uprawnieni użytkownicy	✘
Połączenie	
Tryb połączenia	`Pośrednik`
Adres lokalny	`10.0.236.70`
Port	`997`
Użyj szyfrowania TLS	✔
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 podmianą loginu i hasła) lub z przekazywaniem danych logowania; politykę zmiany haseł a także login i hasło konta uprzywilejowanego.

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

Parametr	Wartość
Ogólne	
Nazwa	`twitter_admin`
Zablokowane	✗
Typ	`regular`
Nagrywanie sesji	`wszystko`
Notatki	✗
Retencja danych	
Nadpisz globalne ustawienia retencji	✗
Usuń dane sesji	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Serwer	
Serwer	`twitter`
Dane uwierzytelniające	
Domena	✗
Login	`Tweety`
Zastąp sekret	`hasłem`
Hasło	`*****`
Powtórz hasło	`*****`
Polityka modyfikatora hasła	`Statyczne, bez ograniczeń`

4. Kliknij *Zapisz*.

Dodanie sejfu

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

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

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

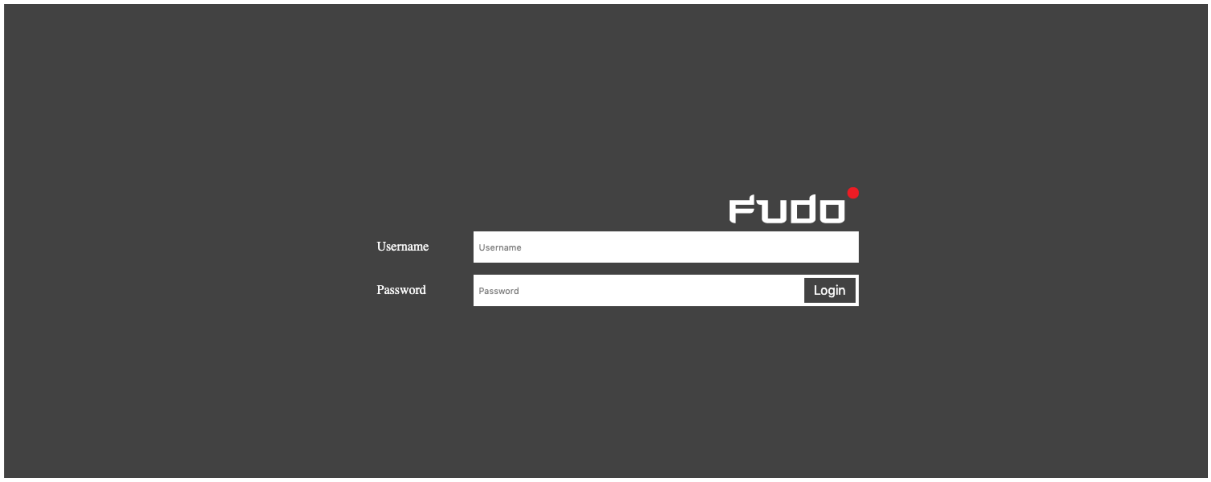
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

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

5.9.3 Nawiązanie połączenia

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

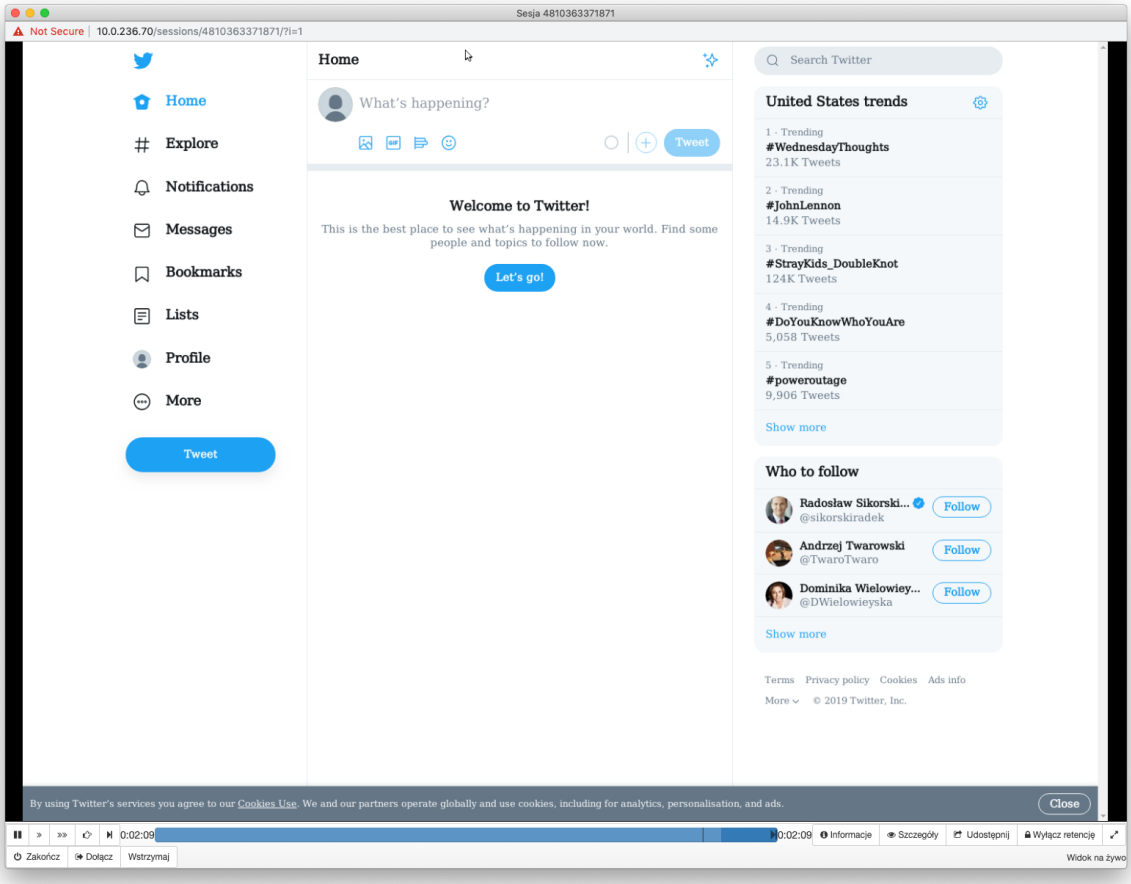
Informacja: W przypadku uwierzytelniania dwuskładnikowego, wprowadź hasło statyczne wraz ze składnikiem dynamicznym (wskazanie tokena) jako jeden ciąg znaków.



4. Kontynuuj przeglądanie serwisu.

5.9.4 Podgląd sesji połączeniowej

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

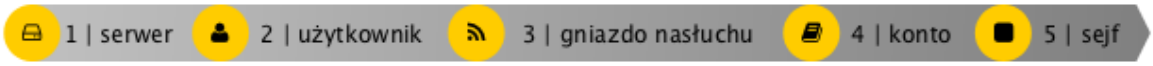
Informacja: Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedy-

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`
Uprawnienia	
Uprawnieni użytkownicy	✗
Adresy serwerów	
Adres IP	`10.0.40.230`
Port	`5900`

4. Kliknij *Zapisz*.

Dodanie użytkownika

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

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

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

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

4. Kliknij *Zapisz*.

Dodanie gniazda nasłuchiwania

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

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

Parametr	Wartość
Nazwa	`vnc_listener`
Zablokowane	✗
Protokół	`VNC`
Komunikat	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Połączenie	
Tryb połączenia	`proxy`
Adres lokalny	`10.0.150.151`
Port	`5900`
Adres zewnętrzny	✗
Port zewnętrzny	✗

4. Kliknij *Zapisz*.

Dodanie konta

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

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

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

4. Kliknij *Zapisz*.

Dodanie sejfu

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

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

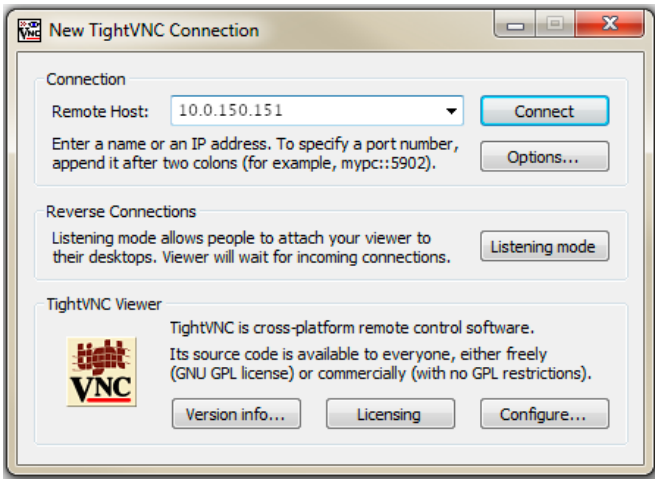
Parametr	Wartość
Nazwa	`vnc_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`

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

4. Kliknij *Zapisz*.

5.10.3 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*

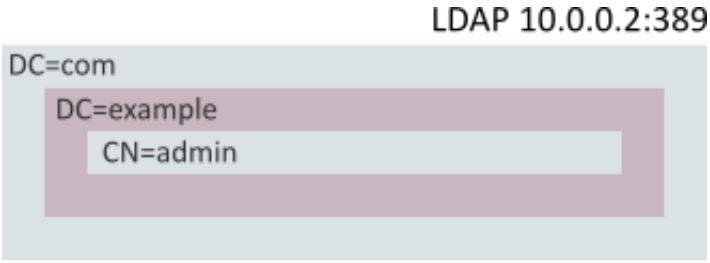
5.11 Uwierzytelnienie użytkowników w katalogu LDAP

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	✗

4. Kliknij *Zapisz*.

Dodanie metody uwierzytelnienia użytkownika

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Odszukaj na liście i kliknij użytkownika `admin`.
3. W polu *Baza LDAP* wprowadź ciąg definiujący obiekt *admin* w strutkurze katalogowej `cn=admin,dc=example,dc=com`.

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

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

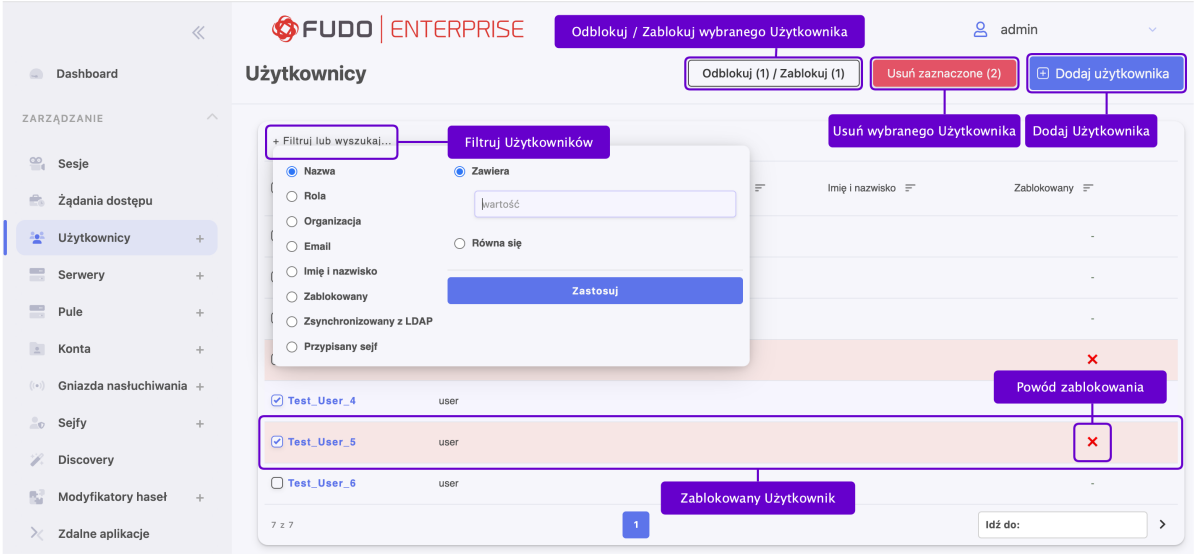
Tematy pokrewne:

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

ROZDZIAŁ 6

Użytkownicy

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



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*.

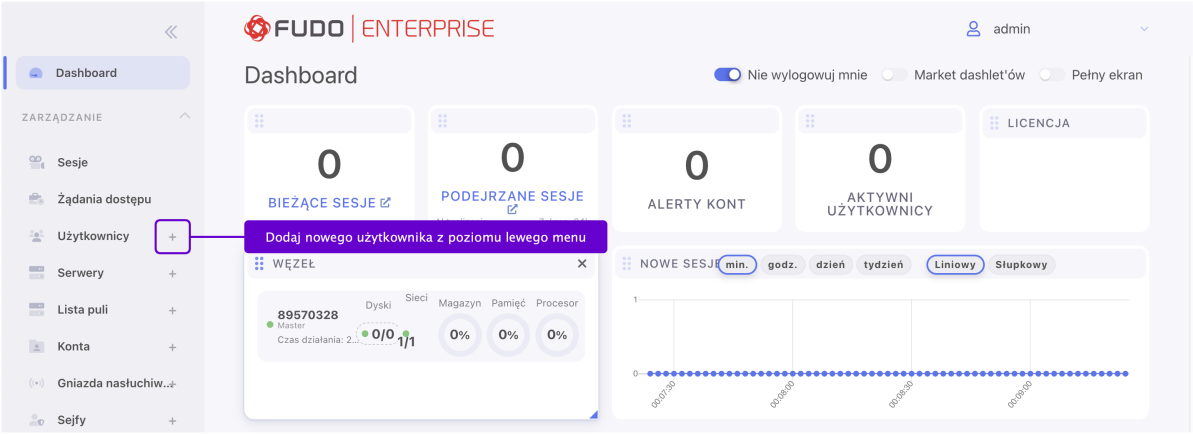
6.1 Dodawanie użytkownika

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.

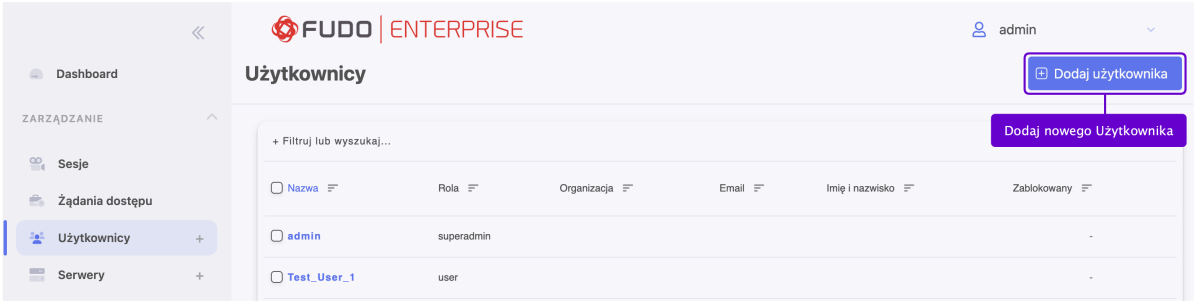
Ostrzeżenie: Tworząc obiekt Użytkownik dla połączeń MySQL, miej na uwadze, że domyślny plugin MySQL `caching_sha2_password` nie jest obecnie wspierany przez Fudo Enterprise. Wspierane plugin'y dla połączeń MySQL to: `mysql_native_password` oraz `mysql_old_password`. W celu zapewnienia kompatybilności 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 rolą uprawnienia dotyczą także dostępu do modelu danych poprzez interfejs API.

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

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Rola	Prawa dostępu
admin	• logowanie do panelu administracyjnego, • zarządzanie obiektami: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, do których użytkownik posiada uprawnienia, • blokowanie/odblokowywanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, • generowanie i subskrybowanie raportów, • konwersja sesji, w której pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału, • włączanie/wyłączanie powiadomień email, • zarządzanie politykami, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, • zarządzanie modyfikatorami haseł, • pobieranie haseł do serwerów (wymaga stosownego uprawnienia), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych. • dostęp do aplikacji Fudo Officer 2.0.
superadmin	• zarządzanie obiektami bez ograniczeń, • zarządzanie konfiguracją urządzenia bez ograniczeń, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • pobieranie haseł do serwerów (wymaga stosownego uprawnienia), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych, licencja, dziennik zdarzeń systemowych. • dostęp do aplikacji Fudo Officer 2.0.

Kontynuacja na następnej stronie

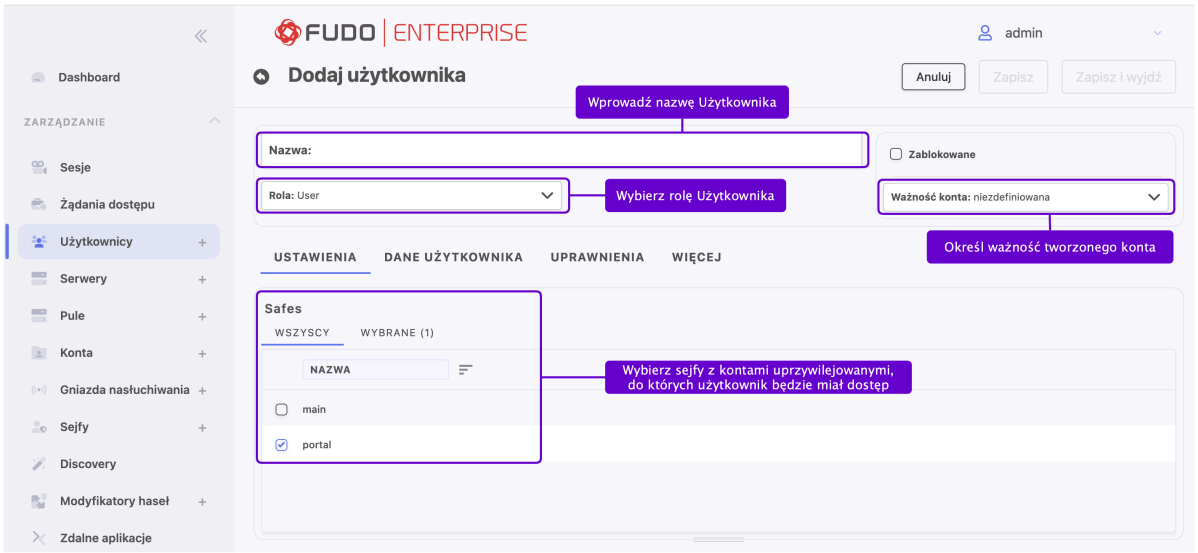
Tabela 1 – kontynuacja poprzedniej strony

Rola	Prawa dostępu
session viewer	• logowanie do panelu administracyjnego, • dostęp do sesji, w których pośredniczyły tylko obiekty (użytkownik, serwer, sejf, konto, gniazdo nasłuchiwania), do których użytkownik posiada uprawnienia, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • dostęp tylko do widoku głównego oraz zakładki *Sesje,* • podgląd sesji na żywo, dołączanie do sesji, wstrzymywanie sesji, przerywanie sesji z jednoczesnym zablokowaniem użytkownika, odtwarzanie zapisów sesji, • brak uprawnień do kasowania, pobierania i eksportowania sesji, • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, wykres sesji równoczesnych.

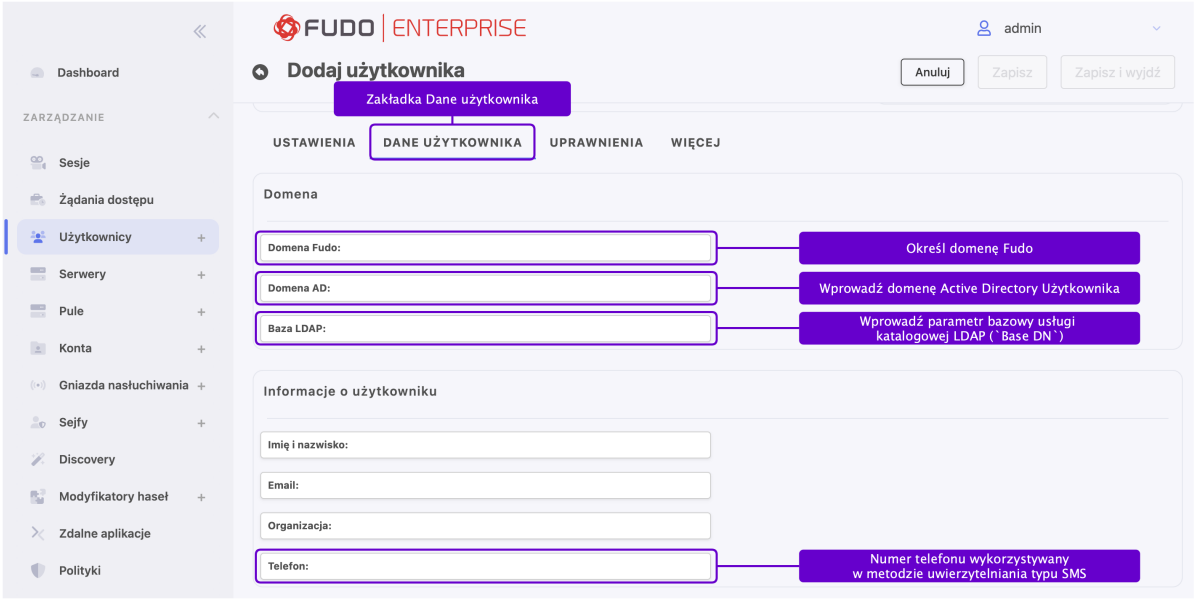
5. Zaznacz opcję *Zablokowane*, aby uniemożliwić użytkownikowi zalogowanie zaraz po utworzeniu konta.
6. Określ ważność tworzonego konta.
7. W zakładce *Ustawienia*, w polu *Sejfy* wybierz sejfy z kontami uprzywilejowanymi, do których użytkownik będzie miał dostęp.

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 *Domenę 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 *Domeną 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 domenę *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*.

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*.

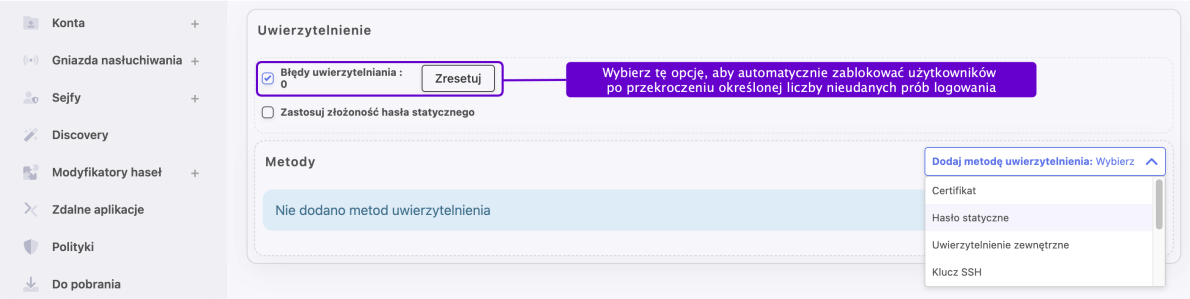
---

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

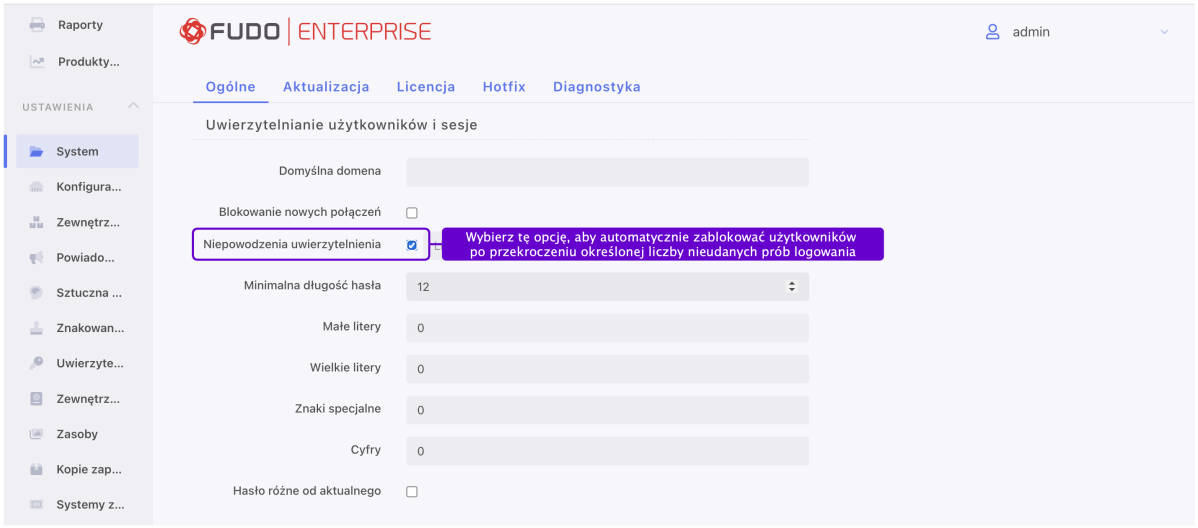
Informacja: Konfiguracja SNMP jest dostępna tylko dla użytkownika o roli *Service*.

---

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.

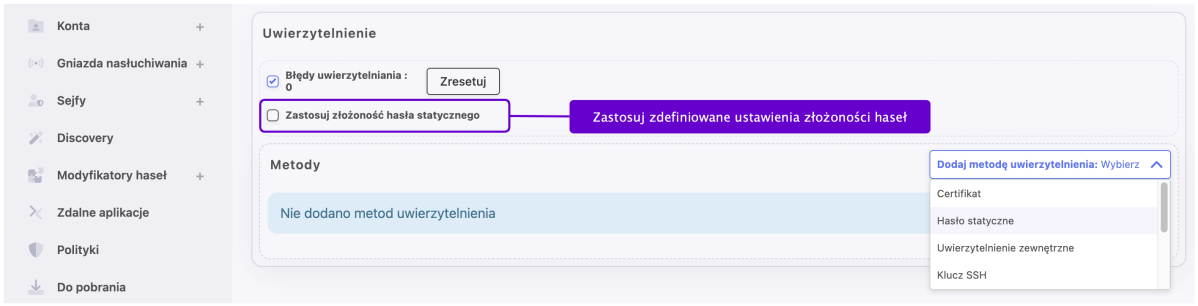


Informacja: Nieudane próby logowania są rejestrowane, jeśli włączona jest opcja Niepowodzenia uwierzytelnienia dla konkretnego użytkownika oraz w zakładce *Ustawienia* > *System*, w sekcji *Uwierzytelnianie użytkowników i sesje*.



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

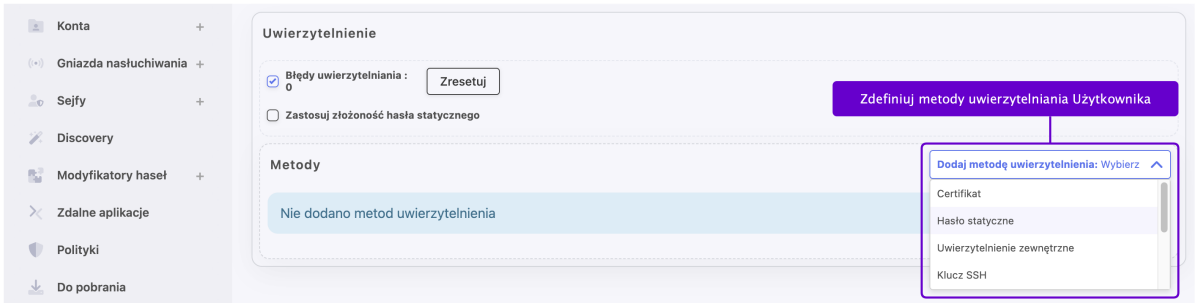
Informacja: Złożoność hasła definiowana jest w menu *Ustawienia* > *Uwierzytelnienie*. Zapoznaj się z rozdziałem *Złożoność haseł*.



18. Określ sposób uwierzytelnienia użytkownika.

Informacja: Aby włączyć możliwość konfiguracji metod uwierzytelnienia, należy najpierw zapisać tworzony obiekt.

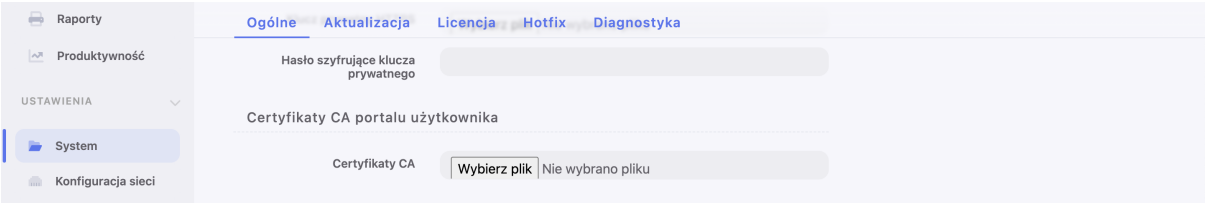
19. Aby dodać metodę uwierzytelnienia, wybierz żądany typ z listy rozwijanej *Dodaj metodę uwierzytelnienia*. Poniżej znajduje się opis procedur specyfikacji dostępnych metod uwierzytelnienia.



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 bezpośrednie (z pominięciem *Portalu Użytkownika*) zalogowanie się do monitorowanych serwerów za pomocą aplikacji klienckiej wybranego protokołu. Użytkownik będzie musiał zmienić hasło poprzez *Portal użytkownika*.

Zewnętrzne uwierzytelnienie

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

Informacja: Procedura definiowania zewnętrznych źródeł uwierzytelnienia opisana jest w rozdziale *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 *QR-Code*, 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.

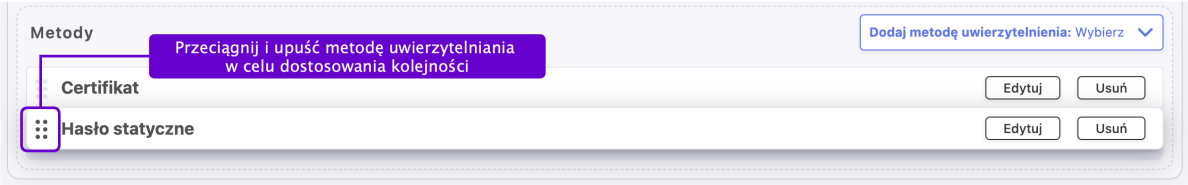
Informacja: Po zapisaniu klucza API nie ma możliwości jego podglądu.

---

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*
- *Uwierzytelnienie*
- *Model danych*
- *Złożoność haseł*

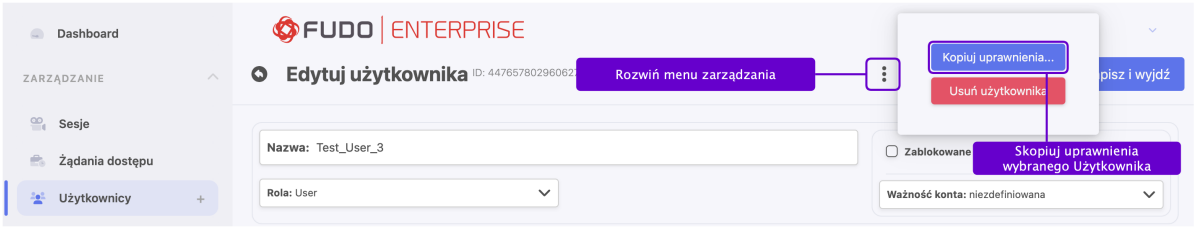
6.2 Kopiowanie uprawnień użytkownika

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 skopiowania 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:

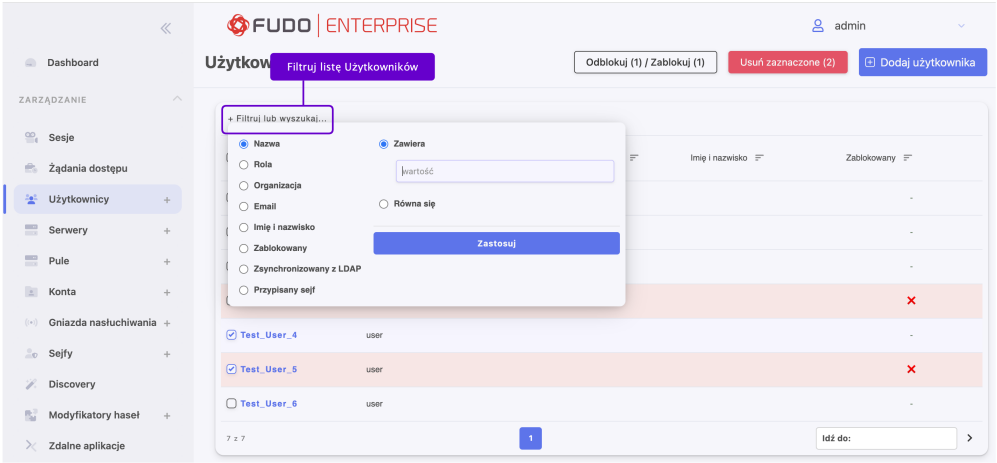
- *Synchronizacja użytkowników z LDAP*

- *Model danych*
- *Pierwsze uruchomienie*

6.3 Modyfikowanie użytkownika

Aby zmodyfikować definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

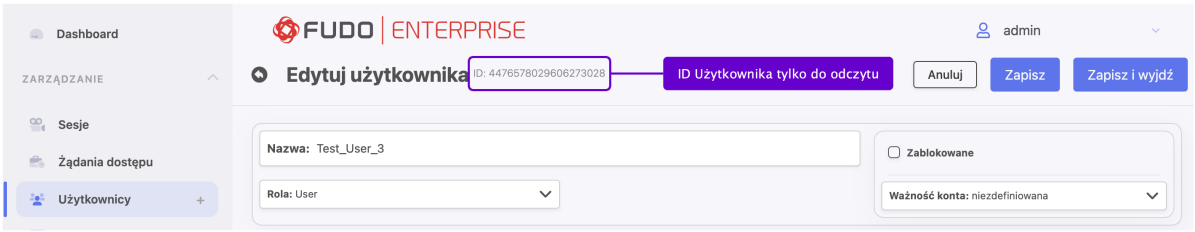
1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



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 użytkowika 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*

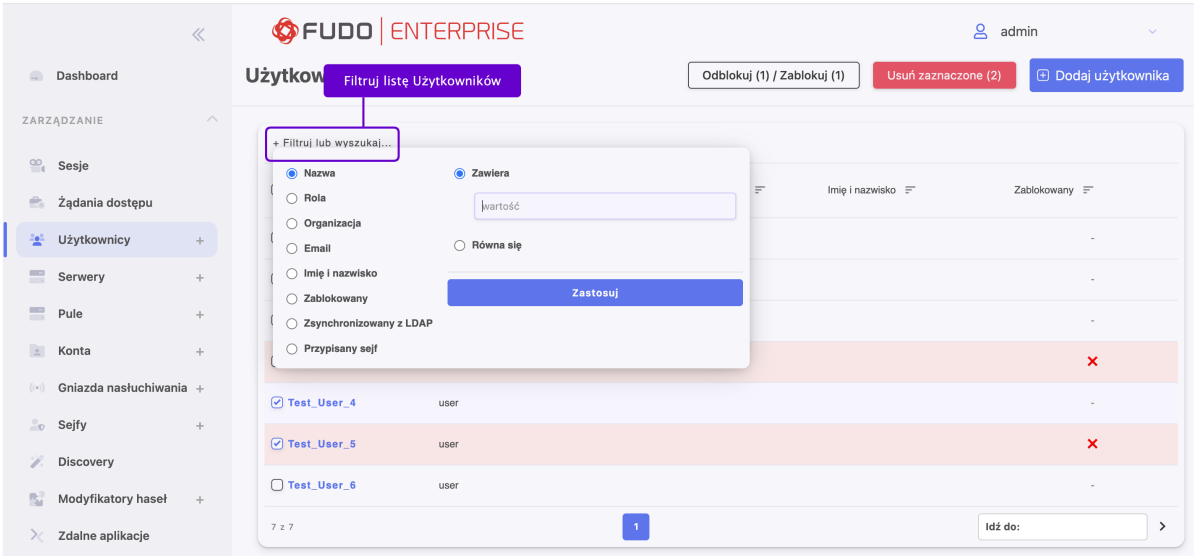
- *Sejfy*

6.4 Blokowanie użytkownika

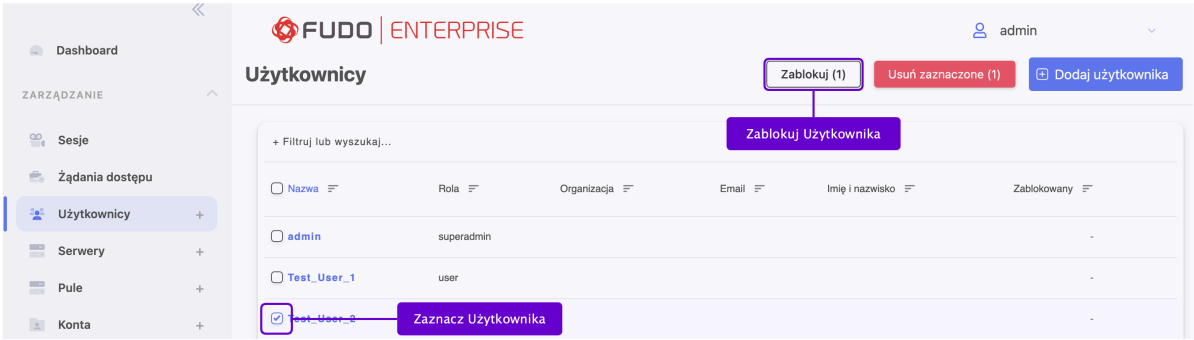
Aby zablokować użytkownikowi możliwość nawiązywania połączeń ze zdefiniowanymi zasobami, postępuj zgodnie z poniższą instrukcją.

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.

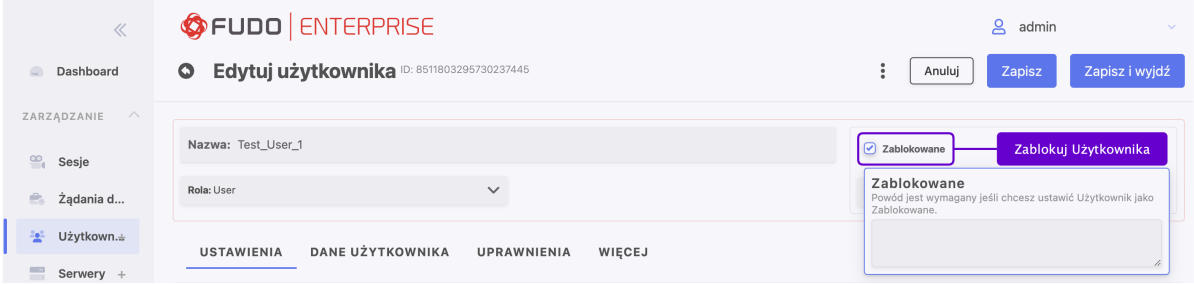


4. Wprowadź wymagany powód zablokowania zasobu i kliknij *Zablokuj*.

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*

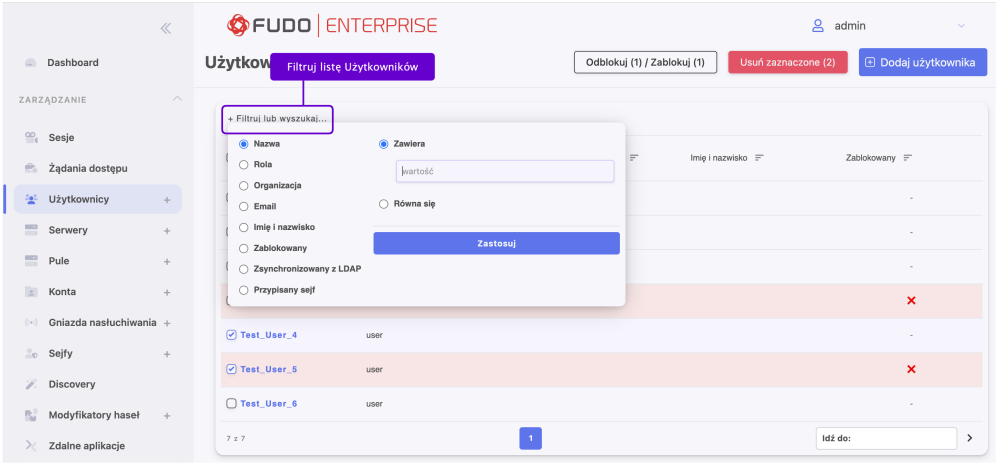
Tematy pokrewne:

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

6.5 Odblokowanie użytkownika

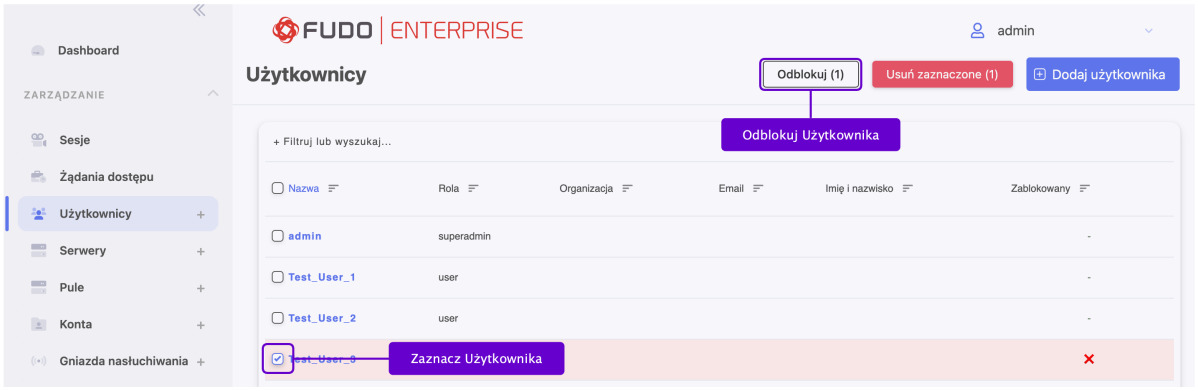
Aby odblokować użytkownikowi możliwość nawiązywania połączeń ze zdefiniowanymi zasobami, postępuj zgodnie z poniższą instrukcją.

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.

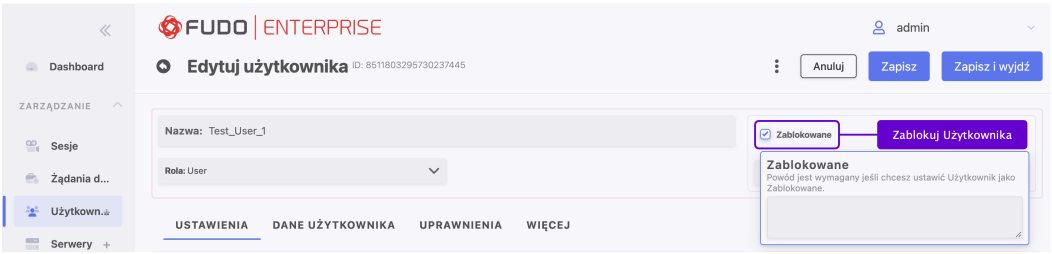
4. Kliknij *Odblokuj*, aby umożliwić użytkownikowi nawiązywanie połączeń.



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*

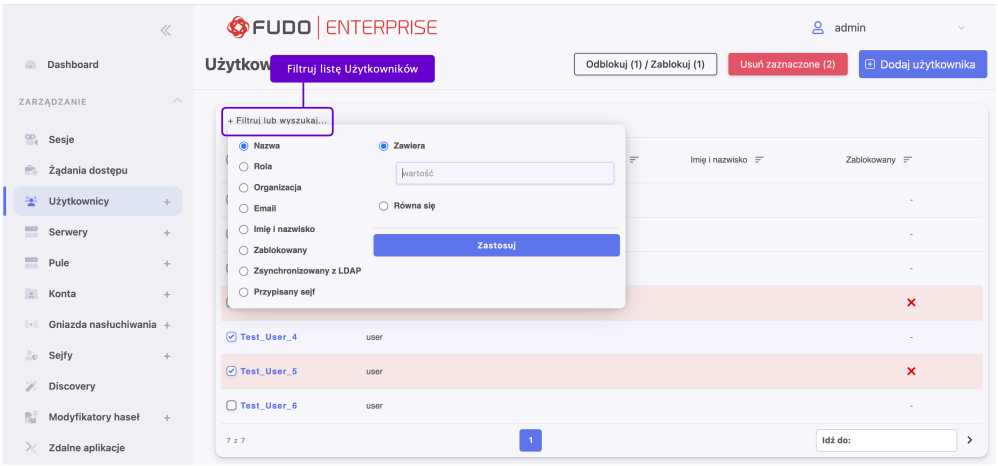
6.6 Usuwanie użytkownika

Aby usunąć definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

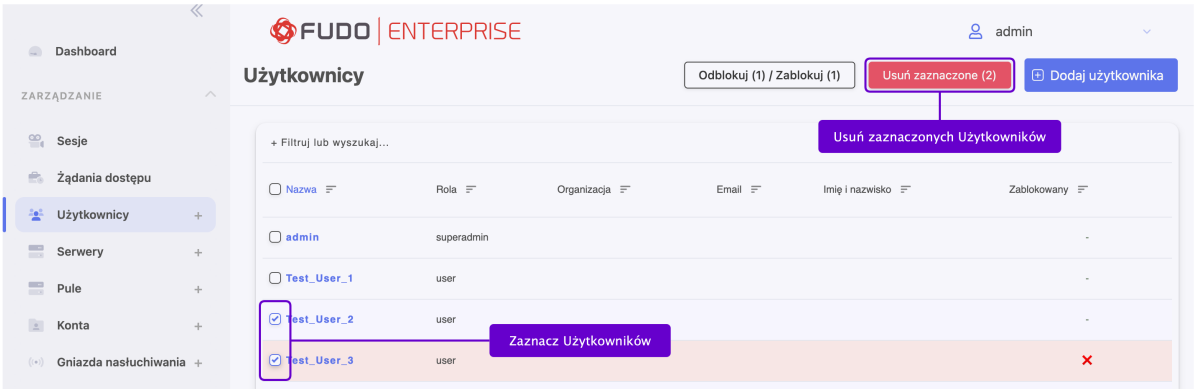
Informacja: Usunięcie definicji użytkownika nie skutkuje usunięciem skojarzonych, zarejestrowanych sesji. Sesje usuniętych użytkowników charakteryzują się przekreślonym loginem użytkownika.

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.

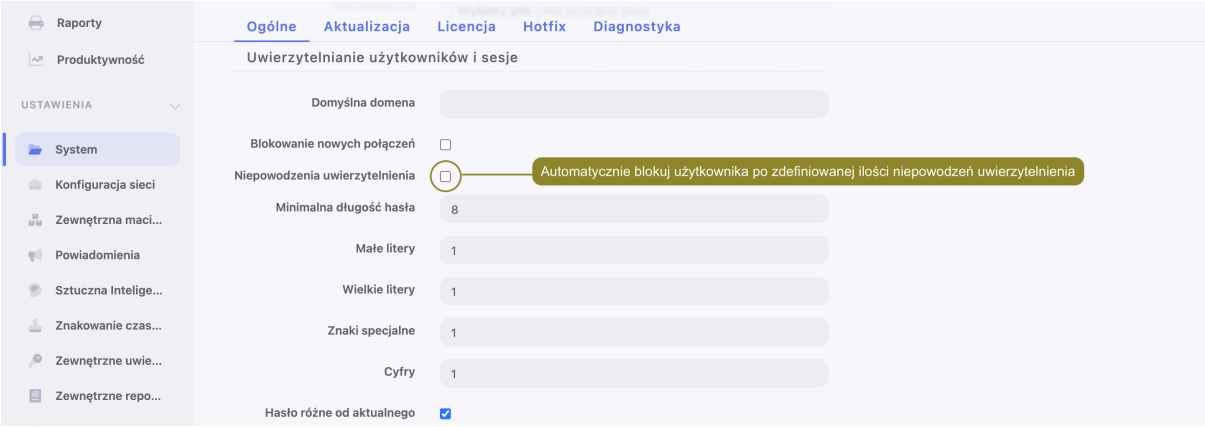
Tematy pokrewne:

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

6.7 Zliczanie niepowodzień uwierzytelnienia

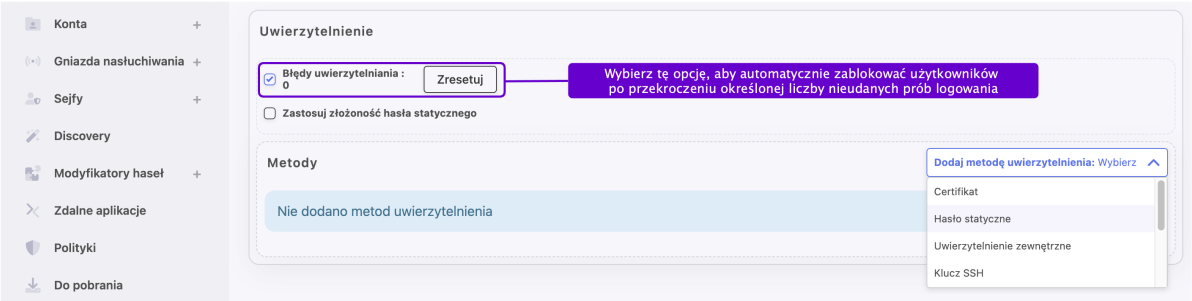
Fudo może zliczać niepowodzenia logowania i automatycznie blokować konto użytkownika, z chwilą gdy licznik nieudanych prób uwierzytelnienia osiągnie zdefiniowaną wartość.

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



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

Informacja: Kliknij Reset aby zresetować wskazanie licznika.



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*

6.8 Role użytkownika

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

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

Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

Rola	Prawa dostępu
admin	• logowanie do panelu administracyjnego, • zarządzanie obiektami: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, do których użytkownik posiada uprawnienia, • blokowanie/odblokowywanie obiektów: serwery, użytkownicy, konta, sejfy, gniazda nasłuchiwania, • generowanie i subskrybowanie raportów, • konwersja sesji, w której pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, i pobieranie skonwertowanego materiału, • włączanie/wyłączanie powiadomień email, • zarządzanie politykami, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • podgląd sesji na żywo i odtwarzanie zapisów sesji, w których pośredniczyły obiekty (użytkownik, serwer, sejf, konto), do których użytkownik posiada uprawnienia, • zarządzanie modyfikatorami haseł, • pobieranie haseł do serwerów (wymaga stosownego uprawnienia), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych. • dostęp do aplikacji Fudo Officer 2.0.
superadmin	• zarządzanie obiektami bez ograniczeń, • zarządzanie konfiguracją urządzenia bez ograniczeń, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • pobieranie haseł do serwerów (wymaga stosownego uprawnienia), • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, naruszenia bezpieczeństwa kont, aktywni użytkownicy, informacje statusowe, wykres sesji równoczesnych, licencja, dziennik zdarzeń systemowych. • dostęp do aplikacji Fudo Officer 2.0.

Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

Rola	Prawa dostępu
session viewer	• logowanie do panelu administracyjnego, • dostęp do sesji, w których pośredniczyły tylko obiekty (użytkownik, serwer, sejf, konto, gniazdo nasłuchiwania), do których użytkownik posiada uprawnienia, • logowanie do portalu użytkownika (wymaga dodania użytkownika do sejfu `portal`), • dostęp tylko do widoku głównego oraz zakładki *Sesje,* • podgląd sesji na żywo, dołączanie do sesji, wstrzymywanie sesji, przerywanie sesji z jednoczesnym zablokowaniem użytkownika, odtwarzanie zapisów sesji, • brak uprawnień do kasowania, pobierania i eksportowania sesji, • dostępne widgety widoku głównego: sesje równoległe, sesje podejrzane, wykres sesji równoczesnych.

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*.

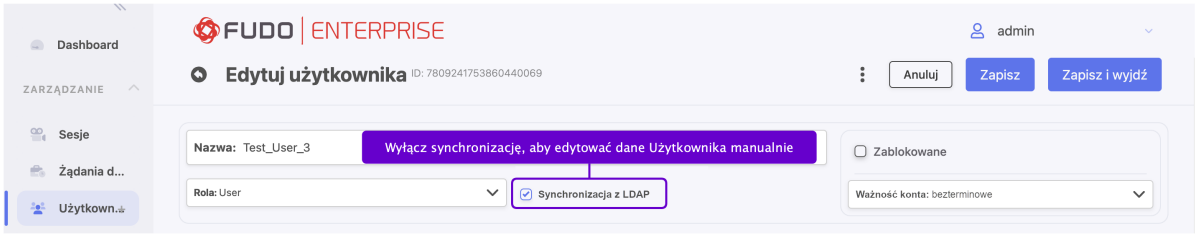
Ostrzeżenie: Dla skutecznej konfiguracji synchronizacji opartej o protokół LDAP jest konieczne wsparcie parametru `memberOf` na serwerze LDAP. Atrybut ten służy do wskazania grup, do których należy użytkownik.

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.

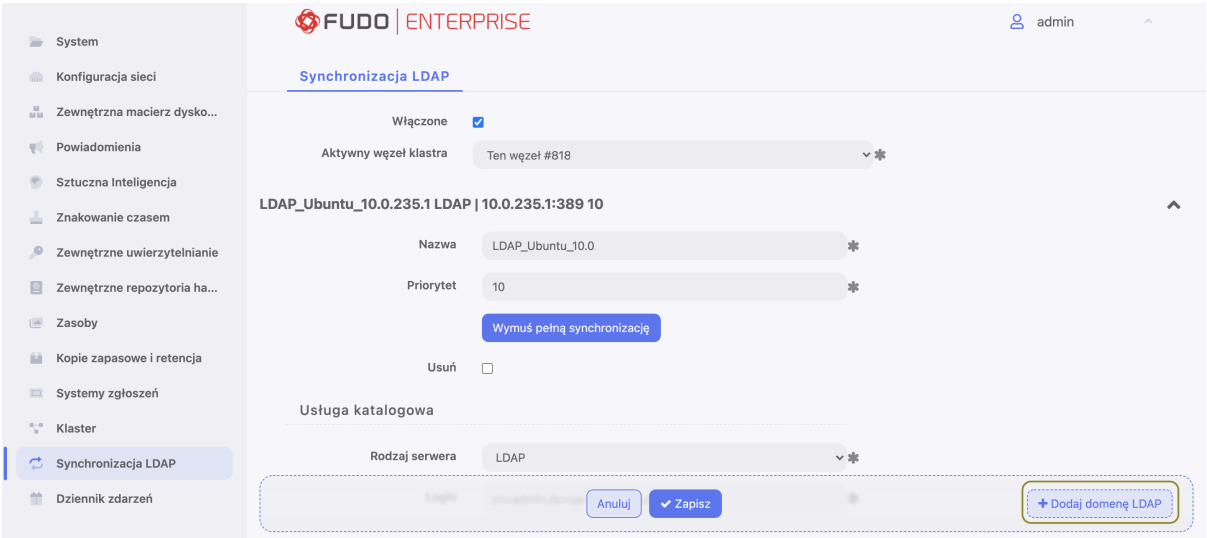


Konfiguracja usługi synchronizacji użytkowników

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=whl`).

Informacja: Synchronizacja użytkowników przechowywanych w strukturze LDAP wymaga:

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

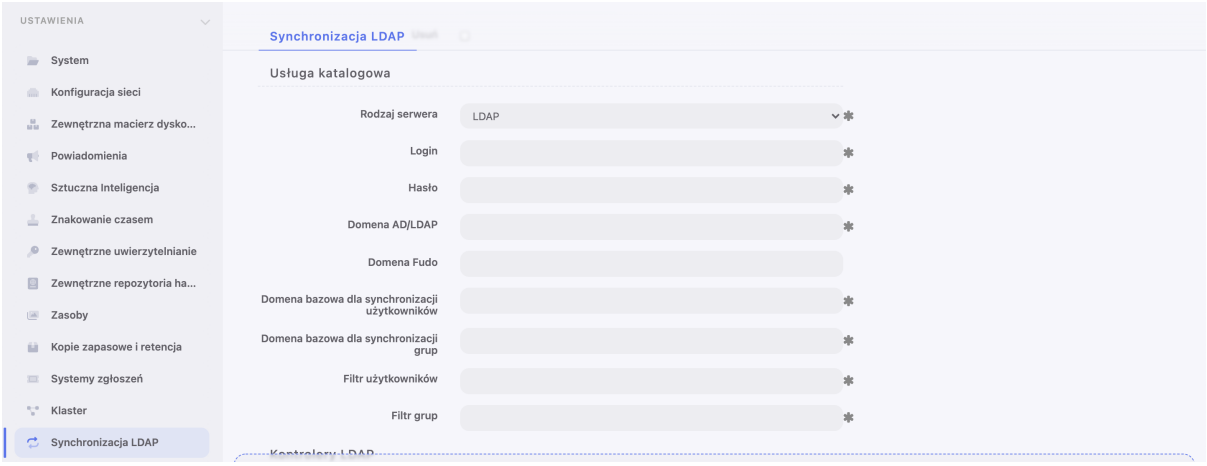
---

12. Określ miejsce przechowywania grup w strukturze katalogowej.

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

---

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



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

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

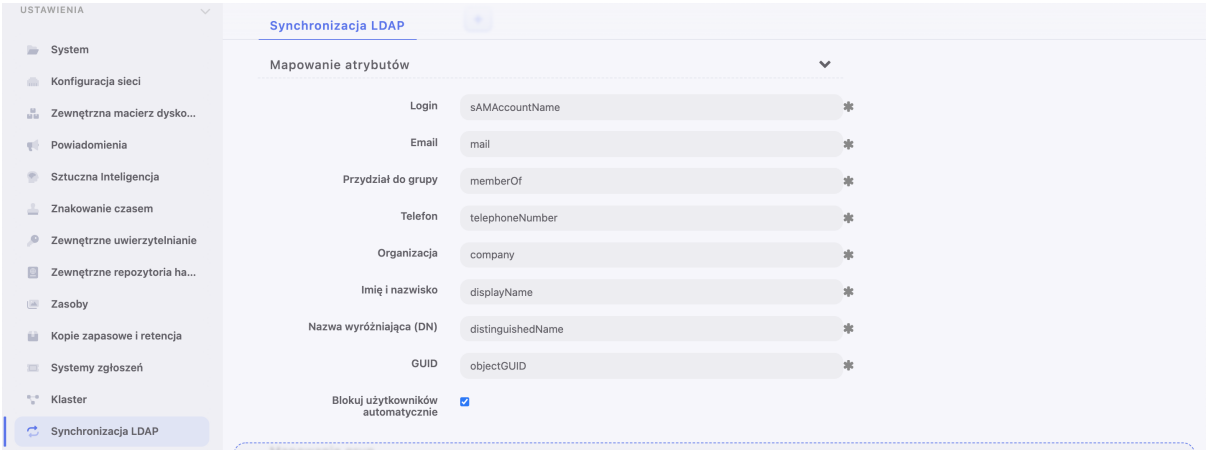
---

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

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

---

19. Zdefiniuj mapowanie pól atrybutów definicji użytkowników.



Informacja: Mapowanie pól pozwala na pobranie informacji o użytkownikach z atrybutów

o niestandardowych nazwach, np. numeru telefonu zdefiniowanego w atrybucie *mobile* zamiast standardowego *telephoneNumber*.

---

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

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

Na przykład:

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

Fudo 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 uwierzytelnienia.
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*

ROZDZIAŁ 7

Serwery

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 instacji 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 upłynięciu 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 nasłuchiwania HTTP zostanie włączona opcja *Renderuj sesje*. Aby włączyć opcję *Renderuj sesje*, zapoznaj się z tematem *Konfigurowanie gniazda nasłuchiwania 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 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.

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 nasłuchiwania RDP*. Opcja *NLA enabled* dla serwera RDP jest równoznaczna z opcją *Enhanced RDP Security (TLS)* dla gniazda nasłuchiwania 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 podsieci, 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 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*

7.1.8 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 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*

7.1.9 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 nasłuchiwania*
- *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*.

---

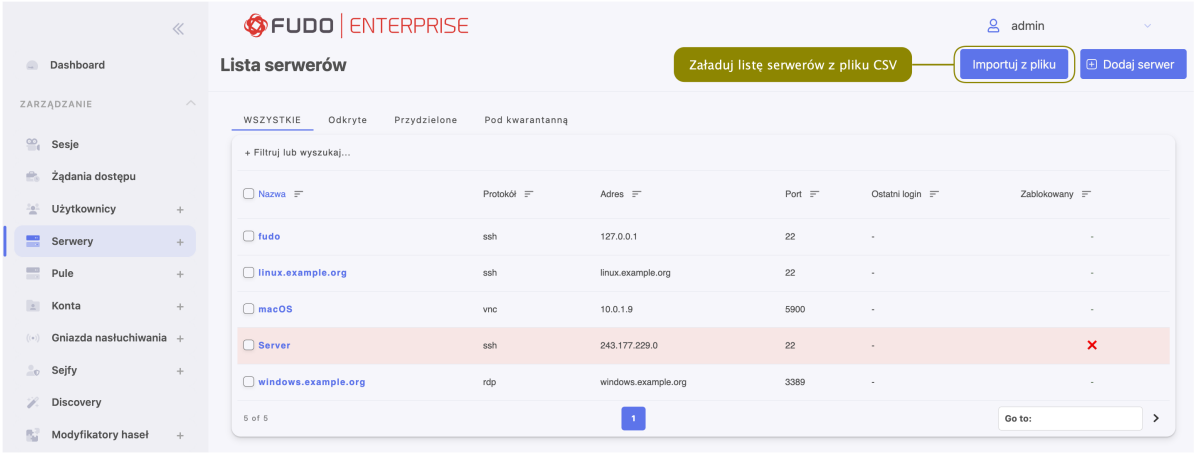
10. Kliknij *Zapisz* albo *Zapisz i wyjdź*.

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 *Przeglądaj 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 nasłuchiwania*
- *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*.

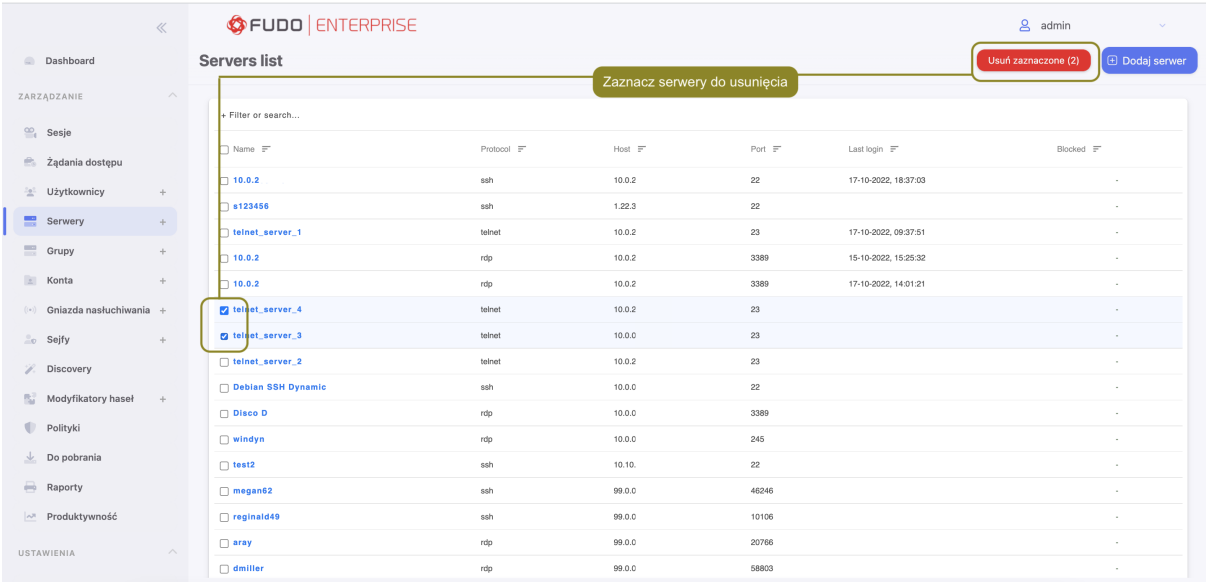
Tematy pokrewne:

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



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*

ROZDZIAŁ 8

Pule

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. Wpsiz 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*

ROZDZIAŁ 9

Zdalne aplikacje

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:

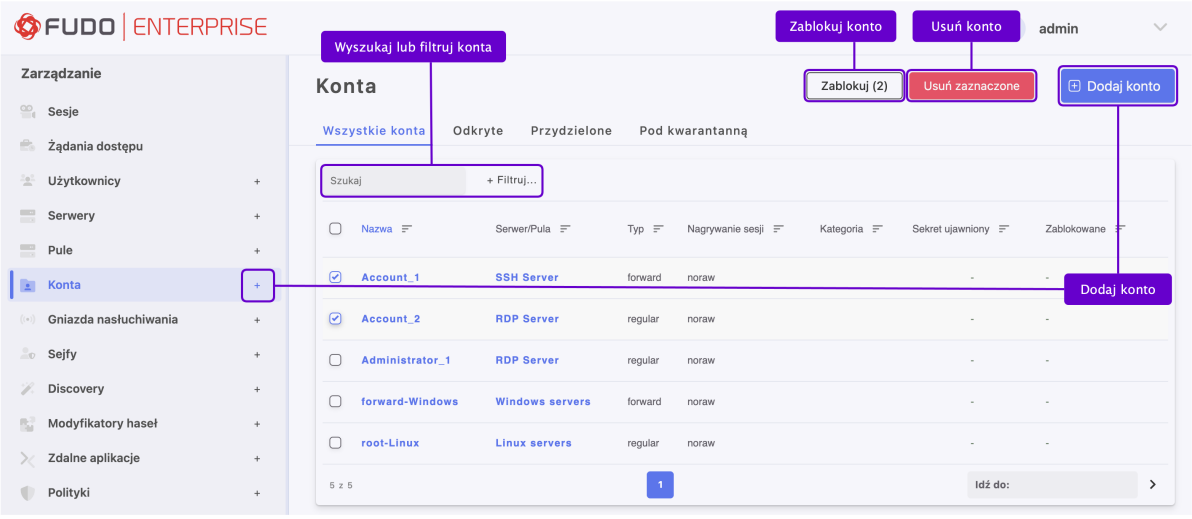
- *Data model*
- *System initiation*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*
- *Konta*
- *Dodawanie konta*

ROZDZIAŁ 10

Konta

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

Informacja: W przypadku połączeń Telnet użytkownik musi przejść proces uwierzytelniania dwukrotnie. Najpierw, aby uwierzytelnić się w Fudo Enterprise, a następnie, aby połączyć się z docelowym hostem.



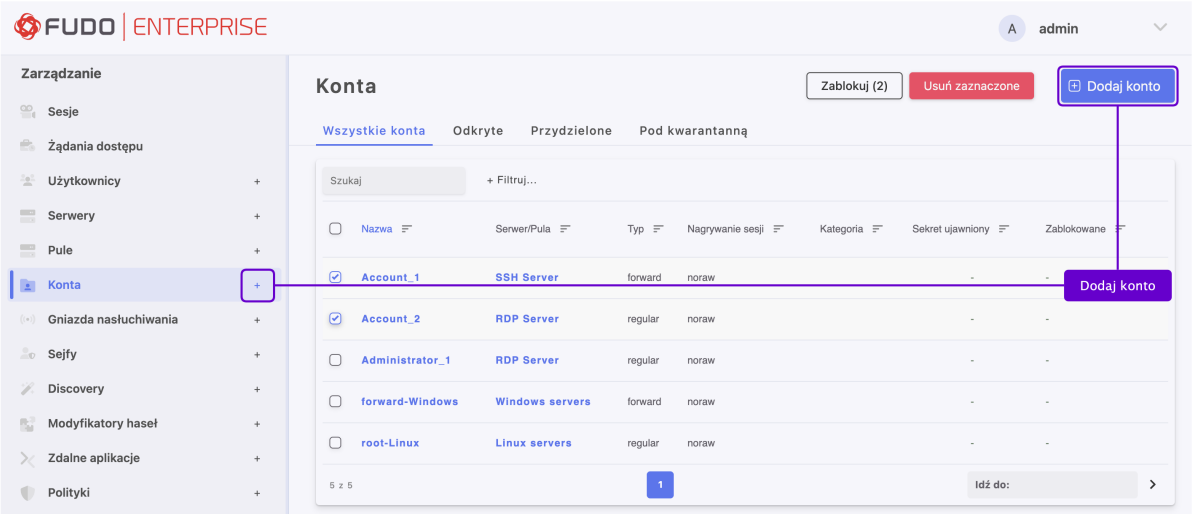
10.1 Dodawanie konta

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

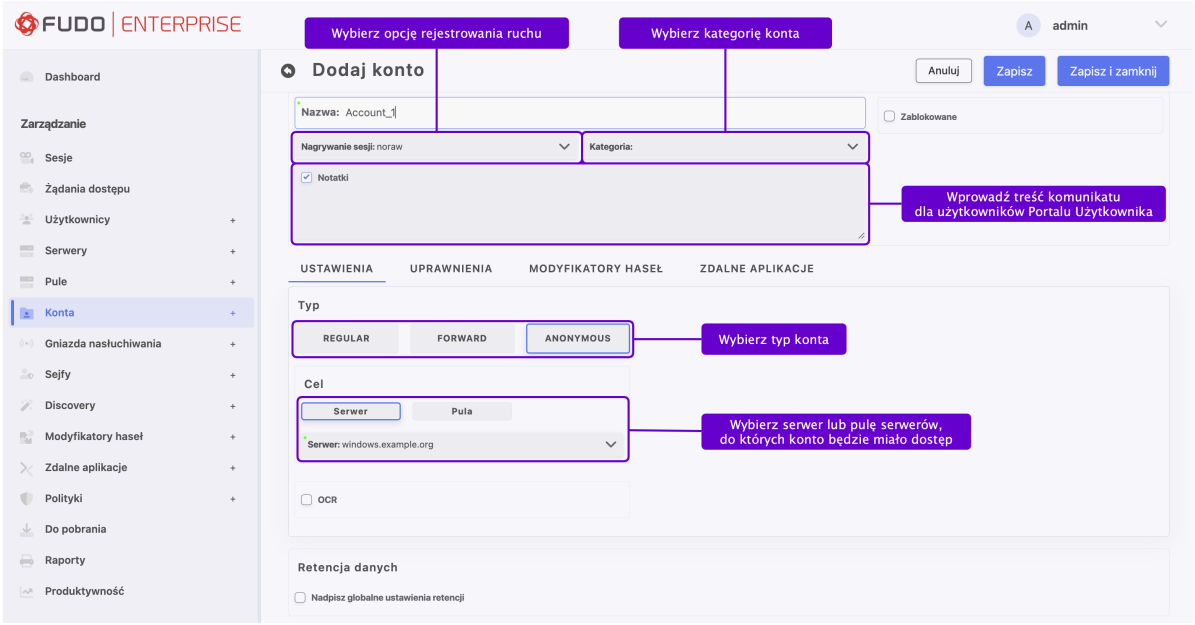
10.1.1 Dodawanie konta typu *anonymous*

Aby utworzyć definicję konta, postępuj zgodnie z poniższymi instrukcjami.

1. Kliknij ikonę + obok zakładki *Konta* w podsekcji *Zarządzanie*, lub
2. Wybierz *Zarządzanie* > *Konta*, a następnie kliknij + *Dodaj konto*.



3. Zdefiniuj nazwę obiektu.
4. Wybierz opcję *Zablokowane*, jeśli chcesz, aby konto było niedostępne po utworzeniu.



5. Wybierz żądaną opcję nagrywania sesji.

6. Z listy rozwijanej *Kategoria* wybierz kategorię konta `uprzywilejowane` lub `nieuprzywilejowane`.

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.

---

7. Wybierz opcję *Notatki*, aby aktywować pole, w którym można wprowadzić treść komunikatu dla użytkowników *User Portal (Access Gateway)*. Jeśli uprawnienia są przyznane, notatki mogą być również edytowane. Uprawnienia są nadawane z poziomu sejfu.

Informacja: Notatki konta mogą być wyświetlane w *User Portal (Access Gateway)*.

---

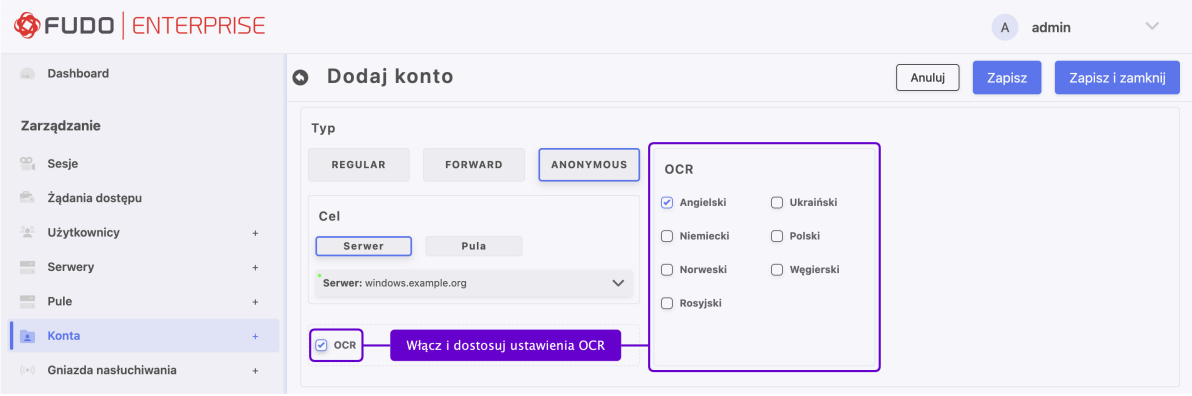
8. W zakładce *Ustawienia*, w polu Typ, naciśnij przycisk *ANONYMOUS*.

9. W sekcji *Cel*, wybierz przycisk *Serwer* lub *Pula*, aby przypisać konto do konkretnego serwera lub puli serwerów, wybierając go w następnym kroku z listy rozwijanej *Serwer* lub *Pula*.
10. Wybierz opcję *SSH Agent forwarding* w celu uwierzytelnienia na serwerze docelowym wykorzystując klucz SSH klienta.

Informacja: Ta opcja jest dostępna tylko po wybraniu serwera SSH. Użyj opcji -A, aby połączyć się z serwerem SSH.

---

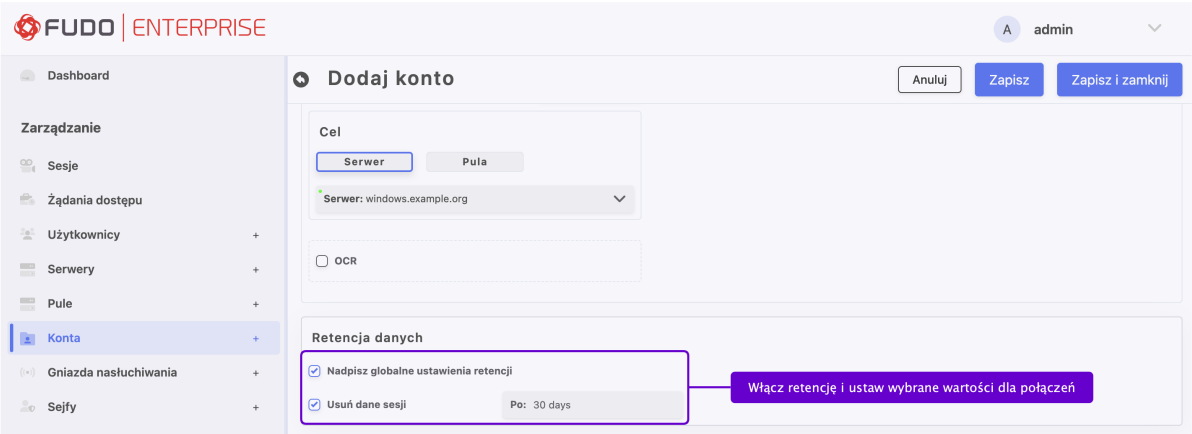
11. Aby automatycznie przetwarzać sesje RDP, VNC lub renderowane HTTP, możesz włączyć opcję *Sesja OCR* dla tego konta i wybrać język przetwarzanych danych.



Informacja: Opcja *OCR* jest dostępna tylko po wybraniu serwera RDP, VNC lub HTTP.

---

12. W sekcji *Retencja danych* zdefiniuj ustawienia automatycznego usuwania danych sesji.
    - Wybierz 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.
    - Obok pola *Usuń dane sesji* zdefiniuj 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*.

13. Kliknij *Zapisz*, aby przejść do dalszej konfiguracji.
14. Przejdź do zakładki *Uprawnienia*, aby dodać użytkowników uprawnionych do zarządzania tym obiektem.
15. Kliknij *Zapisz*.

Informacja: Zakładka *Modyfikatory haseł* i zakładka *Zdalne aplikacje* są aktywne tylko podczas tworzenia konta typu *regular* lub *forward*.

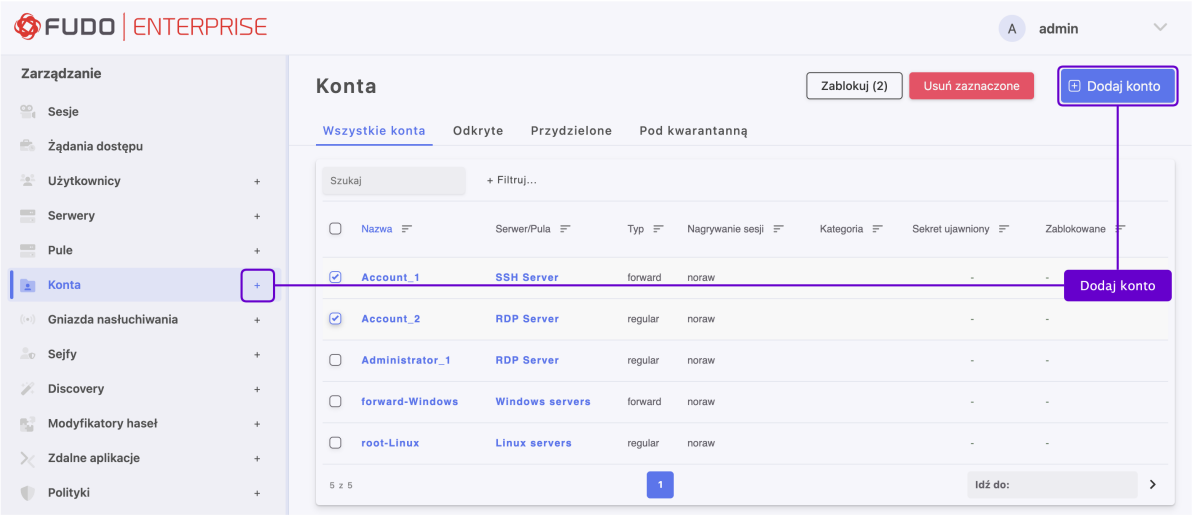
Tematy pokrewne:

- *Model danych*
- *Usuwanie konta*
- *Edytowanie konta*
- *Odblokowywanie konta*
- *Blokowanie konta*

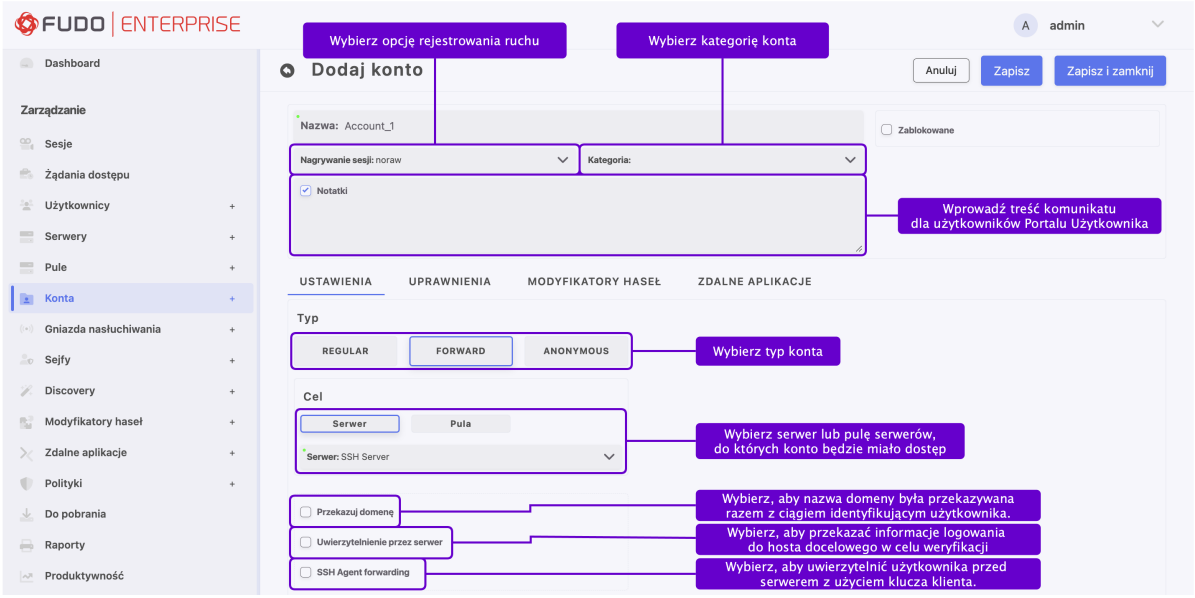
10.1.2 Tworzenie konta typu *forward*

Aby utworzyć definicję konta, postępuj zgodnie z poniższymi instrukcjami.

1. Kliknij ikonę + obok zakładki *Konta* w podsekcji *Zarządzanie*, lub
2. Wybierz *Zarządzanie* > *Konta*, a następnie kliknij + *Dodaj konto*.



3. Zdefiniuj nazwę obiektu.
4. Wybierz opcję *Zablokowane*, jeśli chcesz, aby konto było niedostępne po utworzeniu.



5. Wybierz żądaną opcję nagrywania sesji.

   - `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. Z listy rozwijanej *Kategoria* wybierz kategorię konta `uprzywilejowane` lub `nieuprzywilejowane`.

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.

---

7. Wybierz opcję *Notatki*, aby aktywować pole, w którym można wprowadzić treść komunikatu dla użytkowników *User Portal (Access Gateway)*. Jeśli uprawnienia są przyznane, notatki mogą być również edytowane. Uprawnienia są nadawane z poziomu sejfu.

Informacja: Notatki konta mogą być wyświetlane w *User Portal (Access Gateway)*.

8. W zakładce *Ustawienia*, w polu Typ, naciśnij przycisk *FORWARD*.
9. W sekcji *Cel*, wybierz przycisk *Serwer* lub *Pula*, aby przypisać konto do konkretnego serwera lub puli serwerów, wybierając go w następnym kroku z listy rozwijanej *Serwer* lub *Pula*.
10. 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 następ

- 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.

---

11. 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*.

Informacja: 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 samo dotyczy Duo, SMS i innych schematów uwierzytelniania użytkowników 2FA, które można skonfigurować w Fudo. To ograniczenie dotyczy tylko typów kont forward.

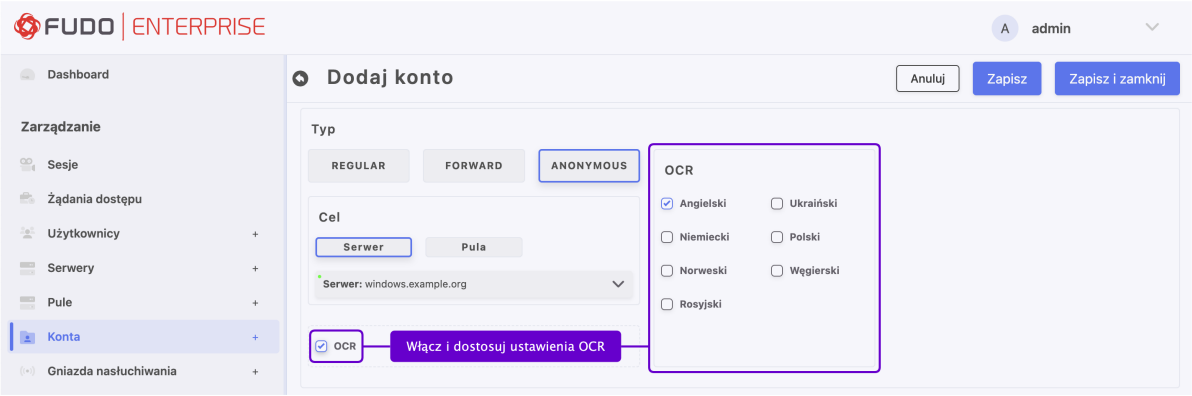
---

12. Wybierz 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.

13. Aby automatycznie przetwarzać sesje RDP, VNC lub renderowane HTTP, możesz włączyć opcję *Sesja OCR* dla tego konta i wybrać język przetwarzanych danych.

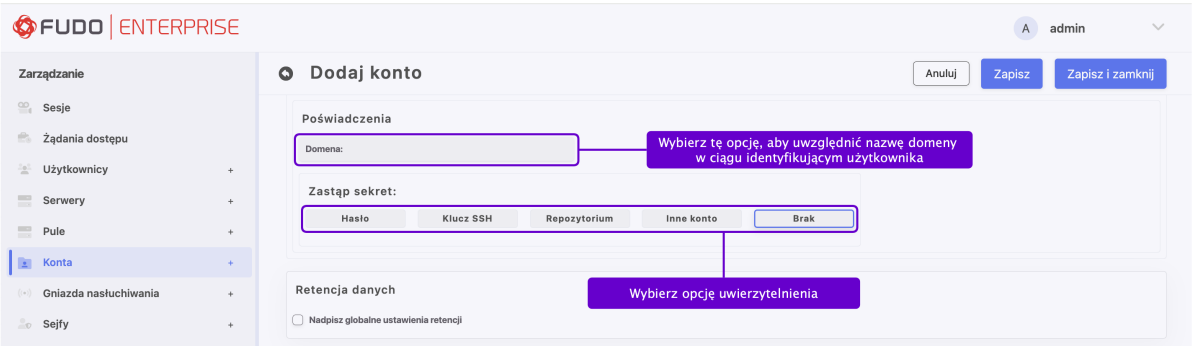


Informacja: Opcja *OCR* jest dostępna tylko po wybraniu serwera RDP, VNC lub HTTP.

14. W sekcji *Dane uwierzytelniające* wprowadź domenę konta uprzywilejowanego.

Informacja: Jeśli domena zostanie wprowadzona w polu *Domena*, Fudo Enterprise zawsze użyje jej do uwierzytelniania wobec serwera. Domena zostanie automatycznie dodana do logowania użytkownika.

15. W sekcji *Zastąp sekret* kliknij przycisk odpowiadający jednej z pożądanych opcji.



Hasło

- Podaj hasło konta w polu *Sekret*.

Informacja: *Uwierzytelnianie dwuskładnikowe*

Przy włączonym uwierzytelnianiu dwuskładnikowym użytkownik jest proszony o podanie danych logowania dwukrotnie. Raz do uwierzytelnienia w Fudo Enterprise, a następnie ponownie do uzyskania dostępu do docelowego systemu.

Aby włączyć uwierzytelnianie dwuskładnikowe, wybierz `Hasło` z sekcji *Zastąp sekret* i pozostaw

puste pola hasła i logowania.

Klucz SSH

- Kliknij przycisk *Generuj* i wybierz algorytm klucza.
- Lub kliknij przycisk *Wczytaj* i przeszukaj system plików, aby znaleźć plik definicji klucza. Podaj *Hasło do klucza*, jeśli jest wymagane dla przesłanego pliku.

Repozytorium

- Wybierz nazwę zewnętrznego repozytorium.

Informacja: Aby dowiedzieć się więcej o definiowaniu zewnętrznego repozytorium haseł, zapoznaj się z sekcją *Zewnętrzne repozytoria haseł*.

Inne konto

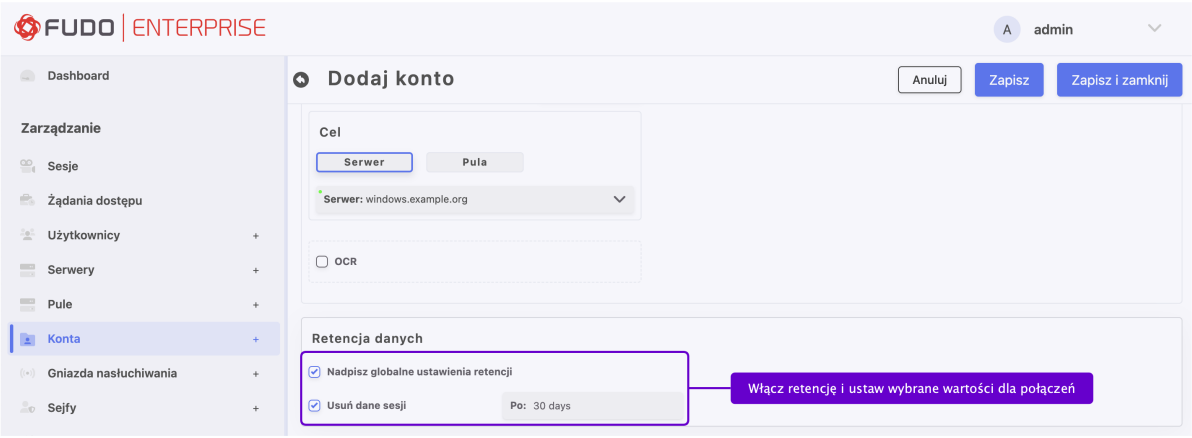
- Z listy rozwijanej *Konto* wybierz obiekt konta, którego dane uwierzytelniające będą używane do uwierzytelniania użytkownika podczas nawiązywania połączenia z monitorowanym serwerem.

Informacja: Lista zawiera tylko obiekty, do których masz uprawnienia dostępu.

Brak

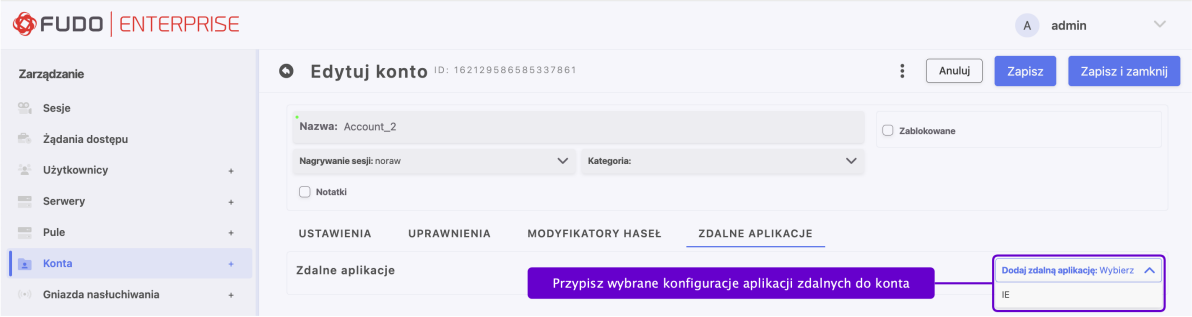
- W takim przypadku żadne dane uwierzytelniające nie będą przesyłane.

16. W sekcji *Retencja danych* zdefiniuj ustawienia automatycznego usuwania danych sesji.
    - Wybierz 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.
    - Obok pola *Usuń dane sesji* zdefiniuj liczbę dni, po których dane sesji zostaną przeniesione z lokalnego systemu plików na zewnętrzną macierz. Wartość domyślna dla zaznaczonej opcji to 30 dni.



17. Przejdź do zakładki *Uprawnienia*, aby dodać użytkowników uprawnionych do zarządzania tym obiektem.

18. Przejdź do zakładki *Zdalne aplikacje*, aby przypisać wybrane konfiguracje aplikacji zdalnych do konta, umożliwiając bezpośrednie połączenia RDP z nimi.



Informacja: Aby dowiedzieć się więcej o definiowaniu aplikacji zdalnych, zapoznaj się z sekcją *Zdalne aplikacje*.

Informacja:

- Zakładka *Aplikacje zdalne* jest aktywna tylko podczas tworzenia konta typu *forward* lub *regular* z przypisanym serwerem lub pulą RDP.
- Zakładka *Modyfikatory haseł* jest aktywna tylko podczas tworzenia konta typu *regular*.

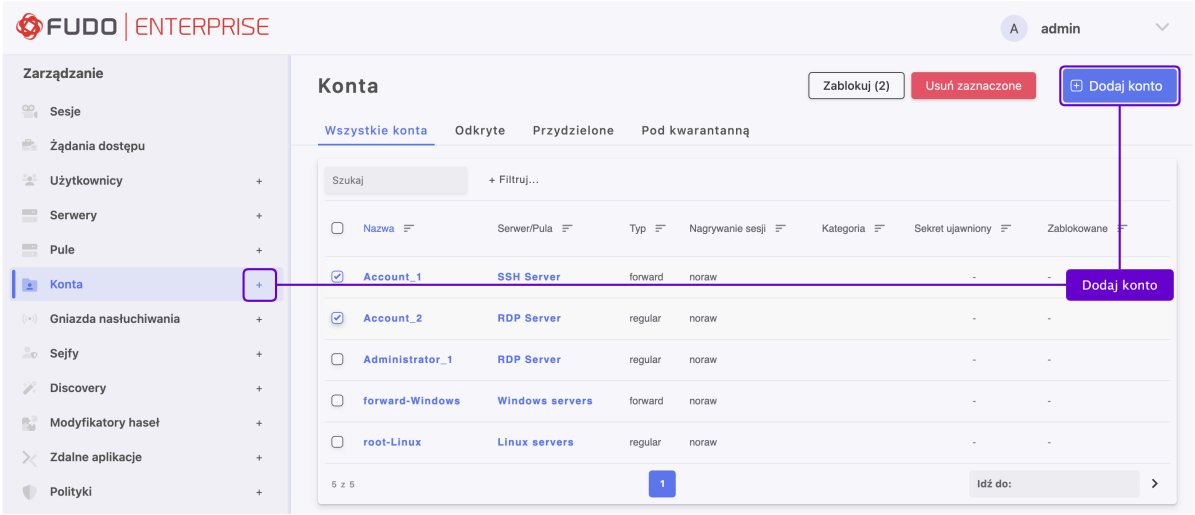
Tematy pokrewne:

- *Model danych*
- *Usuwanie konta*
- *Edytowanie konta*
- *Odblokowywanie konta*
- *Blokowanie konta*

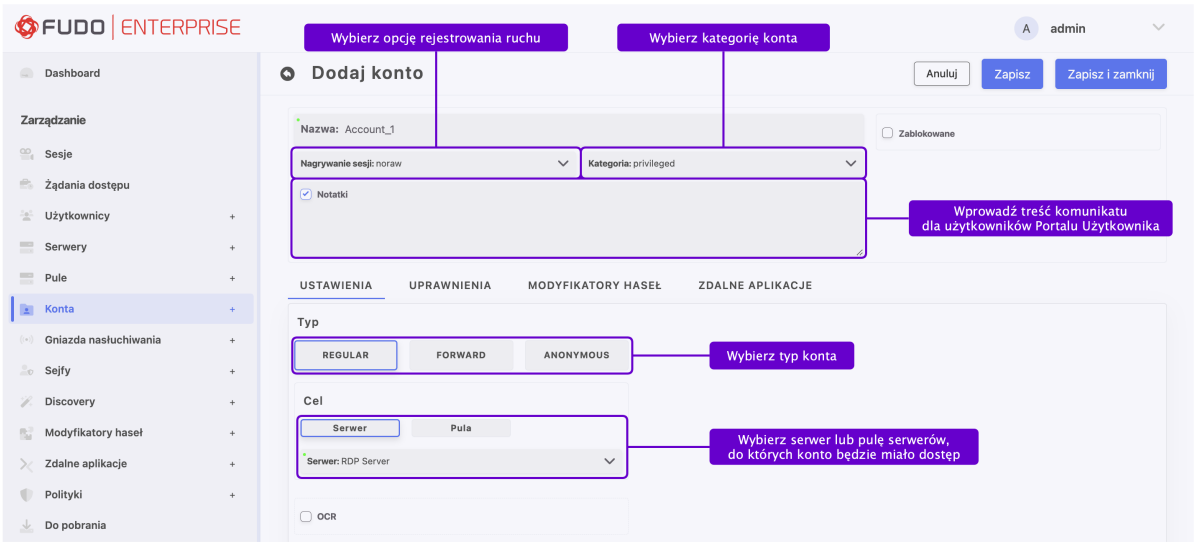
10.1.3 Tworzenie konta typu *regular*

Aby utworzyć definicję konta, postępuj zgodnie z poniższymi instrukcjami.

1. Kliknij ikonę + obok zakładki *Konta* w podsekcji *Zarządzanie*, lub
2. Wybierz *Zarządzanie* > *Konta*, a następnie kliknij + *Dodaj konto*.



3. Zdefiniuj nazwę obiektu.
4. Wybierz opcję *Zablokowane*, jeśli chcesz, aby konto było niedostępne po utworzeniu.



5. Wybierz żądaną opcję nagrywania sesji.

   - `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. Z listy rozwijanej *Kategoria* wybierz kategorię konta `uprzywilejowane` lub `nieuprzywilejowane`.

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.

---

7. Wybierz opcję *Notatki*, aby aktywować pole, w którym można wprowadzić treść komunikatu dla użytkowników *User Portal (Access Gateway)*. Jeśli uprawnienia są przyznane, notatki mogą być również edytowane. Uprawnienia są nadawane z poziomu sejfu.

Informacja: Notatki konta mogą być wyświetlane w *User Portal (Access Gateway)*.

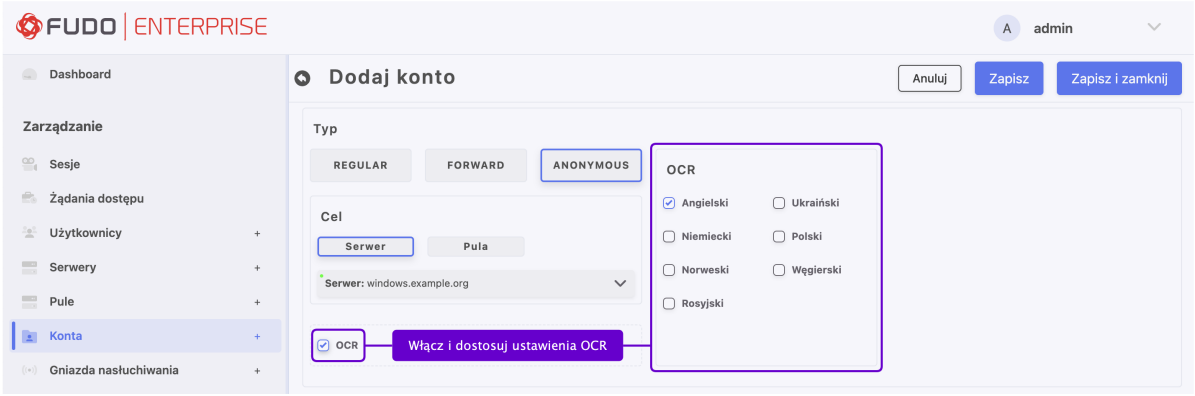
---

8. W zakładce *Ustawienia*, w polu Typ, naciśnij przycisk *REGULAR*.
9. W sekcji *Cel*, wybierz przycisk *Serwer* lub *Pula*, aby przypisać konto do konkretnego serwera lub puli serwerów, wybierając go w następnym kroku z listy rozwijanej *Serwer* lub *Pula*.
10. Wybierz 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.

---

11. Aby automatycznie przetwarzać sesje RDP, VNC lub renderowane HTTP, możesz włączyć opcję *Sesja OCR* dla tego konta i wybrać język przetwarzanych danych.

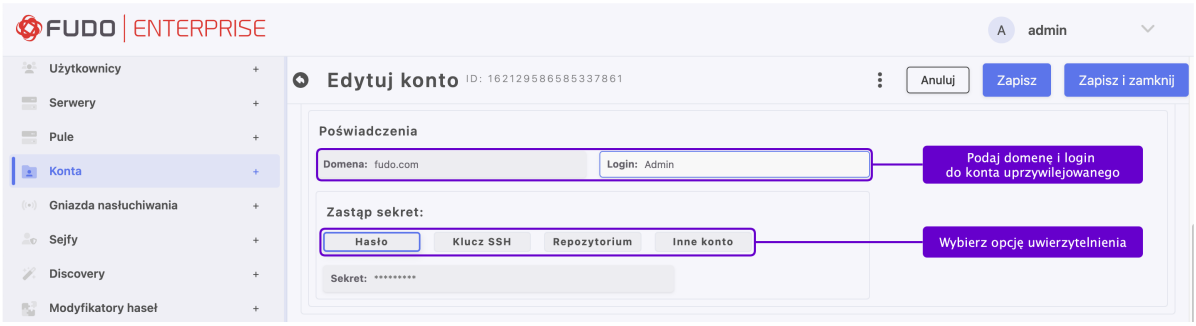


Informacja: Opcja *OCR* jest dostępna tylko po wybraniu serwera RDP, VNC lub HTTP.

12. W sekcji *Dane uwierzytelniające* wprowadź domenę konta uprzywilejowanego.

Informacja: Jeśli domena zostanie wprowadzona w polu *Domena*, Fudo Enterprise zawsze użyje jej do uwierzytelniania wobec serwera. Domena zostanie automatycznie dodana do logowania użytkownika.

13. Wprowadź login do konta uprzywilejowanego.
14. W sekcji *Zastąp tajemnicę* kliknij przycisk odpowiadający jednej z pożądanych opcji.



Hasło

- Podaj hasło konta w polu *Sekret*.

Informacja: *Uwierzytelnianie dwuskładnikowe*

Przy włączonym uwierzytelnianiu dwuskładnikowym użytkownik jest proszony o podanie danych logowania dwukrotnie. Raz do uwierzytelnienia w Fudo Enterprise, a następnie ponownie do uzyskania dostępu do docelowego systemu.

Aby włączyć uwierzytelnianie dwuskładnikowe, wybierz `hasło` z listy rozwijanej *Zastąp sekret* i pozostaw puste pola hasła i logowania.

Klucz SSH

- Kliknij przycisk *Generuj* i wybierz algorytm klucza.

- Lub kliknij przycisk *Wczytaj* i przeszukaj system plików, aby znaleźć plik definicji klucza. Podaj *Hasło do klucza*, jeśli jest wymagane dla przesłanego pliku.

Repozytorium

- Wybierz nazwę zewnętrznego repozytorium.

Informacja: Aby dowiedzieć się więcej o definiowaniu zewnętrznego repozytorium haseł, zapoznaj się z sekcją *Zewnętrzne repozytoria haseł*.

Inne konto

- Z listy rozwijanej *Konto* wybierz obiekt konta, którego dane uwierzytelniające będą używane do uwierzytelniania użytkownika podczas nawiązywania połączenia z monitorowanym serwerem.

Informacja: Lista zawiera tylko obiekty, do których masz uprawnienia dostępu.

---

14. Jeśli wybrano opcję Hasło jako metodę uwierzytelniania, skonfiguruj dodatkowo zakładkę *Modyfikatory haseł*. W przeciwnym razie przejdź do kroku 28 tego podręcznika.

Informacja: Zakładka *Modyfikatory haseł* jest aktywna tylko podczas tworzenia konta *regular* z wybraną metodą *Hasło* i podanym loginem do konta uprzywilejowanego w sekcji *Dane uwierzytelniające*.

---

15. Wybierz *Polityki haseł* z listy skonfigurowanych polityk zmiany haseł.
16. W polu *Limit czasu wypożyczenia hasła* określ czas, po którym hasło zostanie automatycznie zwrócone.

Informacja: Określenie limitu czasu wypożyczenia hasła automatycznie włącza funkcję *Secret Checkout* dla danego Sejfu.

---

17. Wybierz opcję *Zmień hasło po ostatnim zdaniu hasła*, aby automatycznie zmienić hasło po jego zwróceniu przez ostatniego użytkownika.

Informacja: Opcja ta jest dostępna tylko dla funkcji Secret Checkout i jest włączana po określeniu limitu czasu wypożyczenia hasła.

---

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

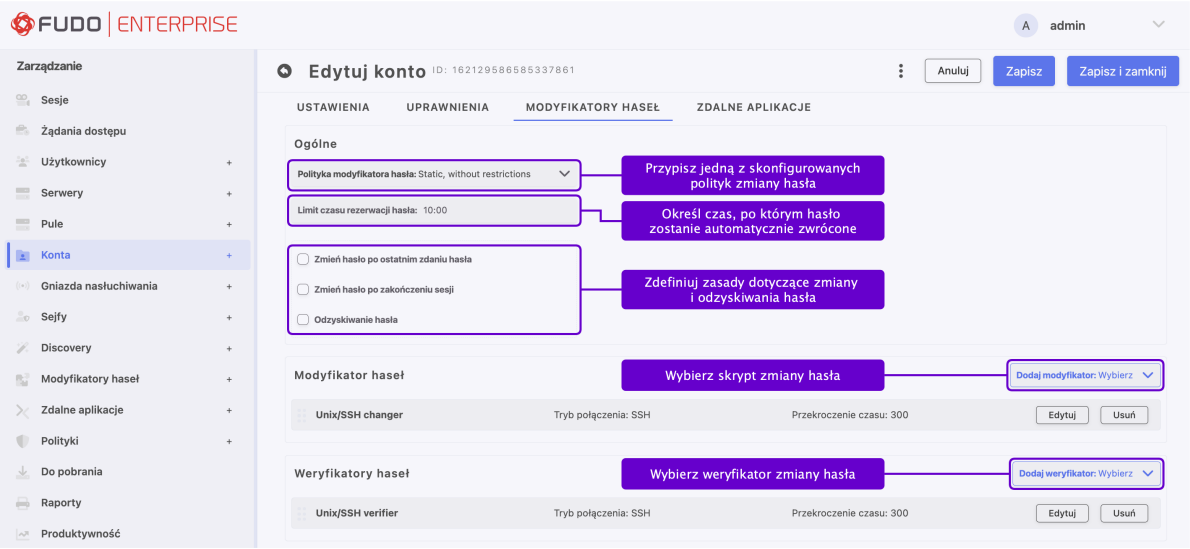
Informacja: Opcja ta wymaga wybrania co najmniej jednego *Modyfikatora hasła* i *Polityki zmiany haseł* **innej niż** `Static, without restrictions`.

Zapoznaj się z tematem *Modyfikatory haseł* w celu uzyskania szczegółowych informacji na temat ich konfiguracji.

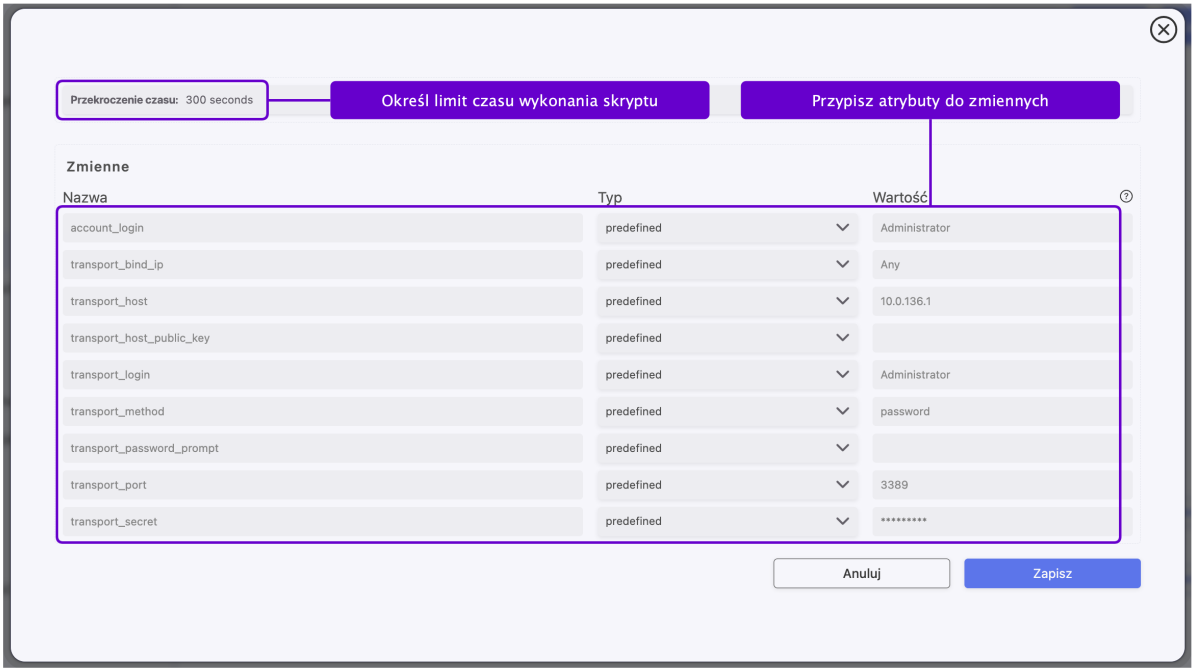
---

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

Informacja: Po włączeniu opcji *Odzyskiwanie hasła*, *Weryfikator Haseł* uruchamia akcję „Trigger password changer" na koncie. Kiedy opcja ta jest wyłączona, *Weryfikator Haseł* wysyła komunikat: „Nie udało się zweryfikować hasła dla konta <nazwa_konta>".



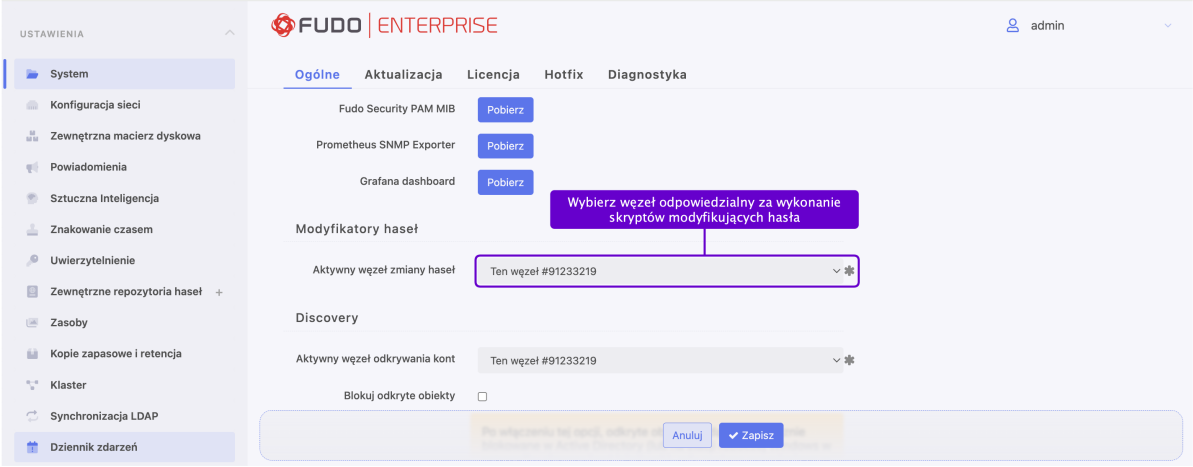
20. W polu *Modyfikatory haseł* wybierz z listy żądany skrypt zmiany hasła, aby hasło do konta było automatycznie zmieniane zgodnie z *polityką zmiany hasła*.
21. W oknie *Modyfikatory haseł*, w polu *Przekroczenie czasu*, określ limit czasu wykonania skryptu.
22. W sekcji *Zmienne* przypisz atrybuty do zmiennych.



23. Kliknij *Zapisz*, aby zamknąć okno.
24. W polu *Weryfikatory haseł* wybierz z listy żądany weryfikator haseł, aby hasło do konta było automatycznie weryfikowane zgodnie z *polityką zmiany hasła*.
25. W oknie *Weryfikatory haseł*, w polu *Przekroczenie czasu*, określ limit czasu wykonania skryptu.
26. W sekcji *Zmienne* przypisz atrybuty do zmiennych.
27. Kliknij *Zapisz*, aby zamknąć okno.

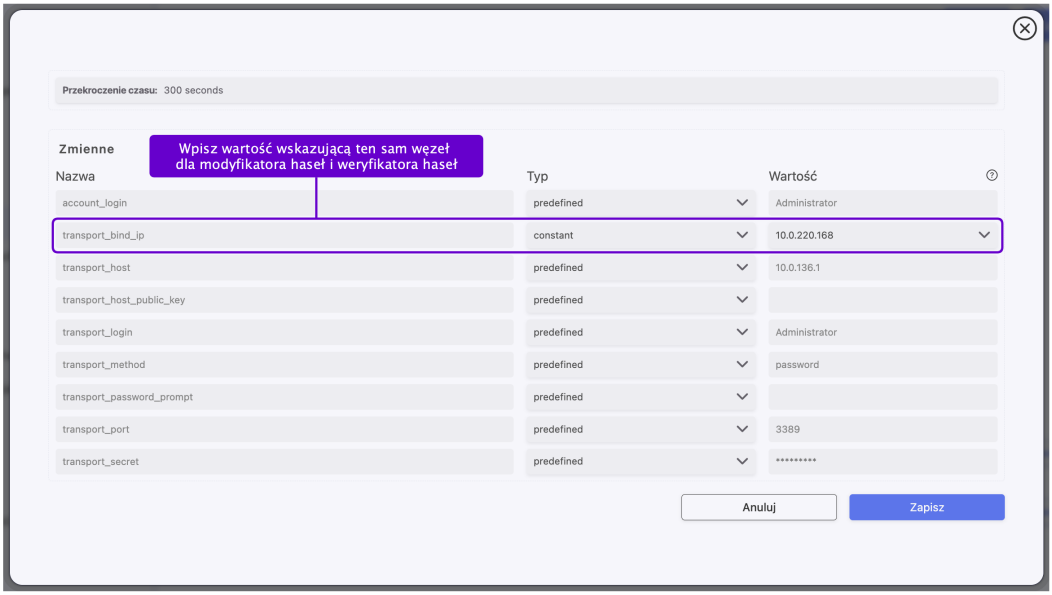
Informacja:

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



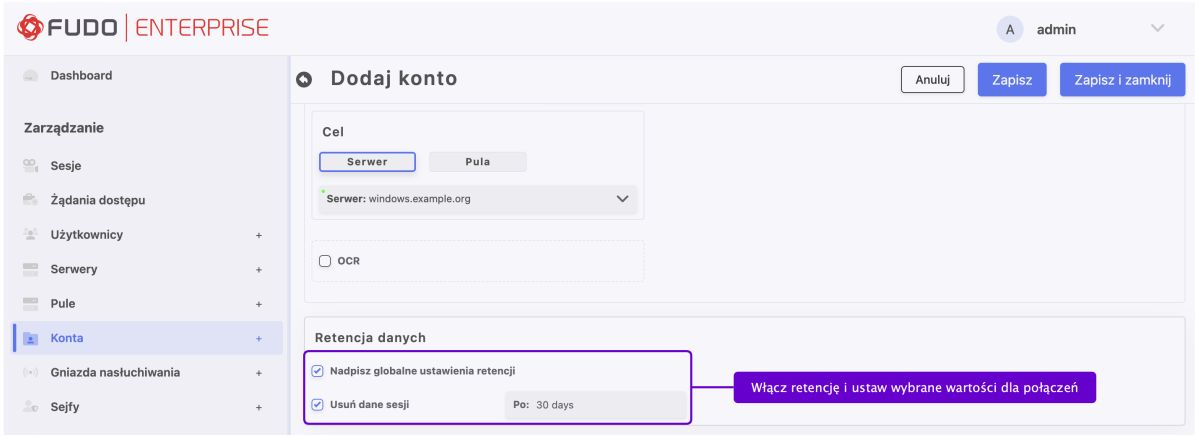
W celu konfiguracji powyższego scenariusza, następujący warunek powinien zostać spełniony:

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

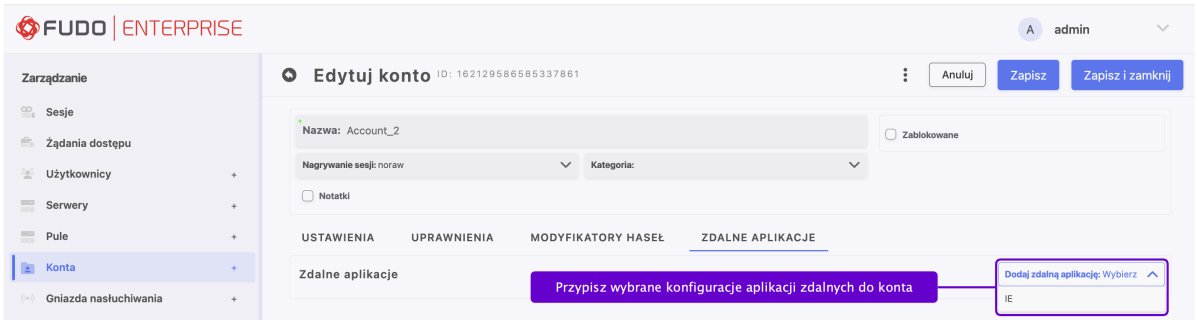


- Jeśli wartości zmiennej `transport_bind_ip` będą wskazywać różne węzły klastra, Modyfikator / Weryfikator hasła będą działać na węźle, wskazanym jako *aktywny węzeł klastra dla Modyfikatorów haseł*.

28. W sekcji *Retencja danych* zdefiniuj ustawienia automatycznego usuwania danych sesji.
    - **Wybierz opcję *Nadpisz globalne ustawienia retencji*, aby dla sesji nawiązanych za pośrednic**
      - Zaznacz opcję *Usuń dane sesji*, aby wykluczyć sesje z mechanizmu retencji.
      - Obok pola *Usuń dane sesji* zdefiniuj liczbę dni, po których dane sesji zostaną przeniesione z lokalnego systemu plików na zewnętrzną macierz. Wartość domyślna dla zaznaczonej opcji to 30 dni.



29. Przejdź do zakładki *Uprawnienia*, aby dodać użytkowników uprawnionych do zarządzania tym obiektem.
30. Przejdź do zakładki *Zdalne aplikacje*, aby przypisać wybrane konfiguracje aplikacji zdalnych do konta, umożliwiając bezpośrednie połączenia RDP z nimi.



Informacja: Aby dowiedzieć się więcej o definiowaniu aplikacji zdalnych, zapoznaj się z sekcją *Zdalne aplikacje*.

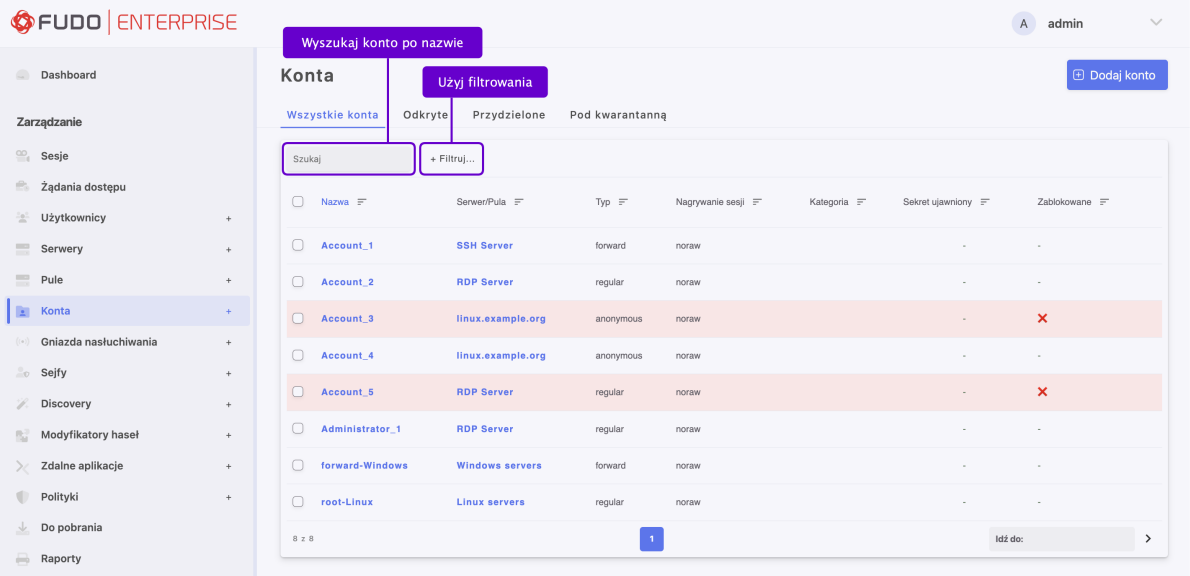
Informacja: Zakładka *Aplikacje zdalne* jest aktywna tylko podczas tworzenia konta typu *forward* lub *regular* z przypisanym serwerem lub pulą RDP.

Tematy pokrewne:

- *Model danych*
- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowywanie konta*
- *Usuwanie konta*
- *Modyfikatory haseł - aktywny węzeł klastra*

10.2 Edytowanie konta

1. Wybierz *Zarządzanie* > *Konta*.
2. Zdefiniuj filtry, aby ograniczyć liczbę obiektów wyświetlanych na liście, lub użyj paska wyszukiwania.



3. Znajdź i kliknij nazwę żądanego obiektu, aby otworzyć jego stronę konfiguracji.
4. Zmodyfikuj parametry konfiguracji według potrzeb.
5. Kliknij *Zapisz*.

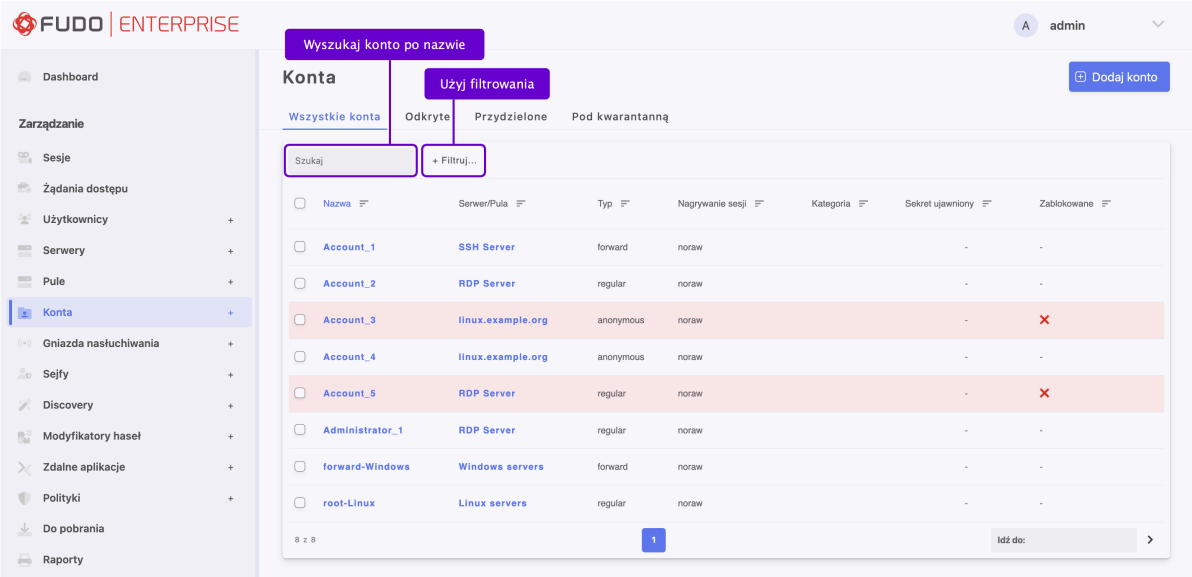
Tematy pokrewne:

- *Dodawanie konta*
- *Blokowanie konta*
- *Odblokowywanie konta*
- *Usuwanie konta*

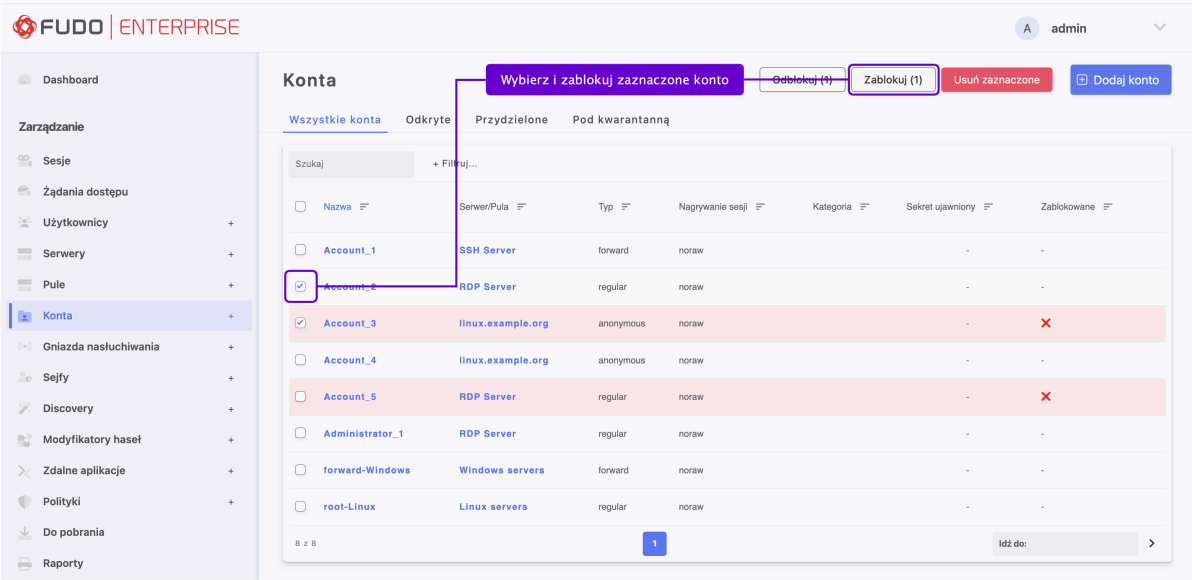
10.3 Blokowanie konta

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

1. Wybierz *Zarządzanie* > *Konta*.
2. Zdefiniuj filtry, aby ograniczyć liczbę obiektów wyświetlanych na liście, lub użyj paska wyszukiwania.



3. Kliknij *Blokuj*.



4. Podaj obowiązkowy powód blokady i kliknij *Potwierdź*.

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

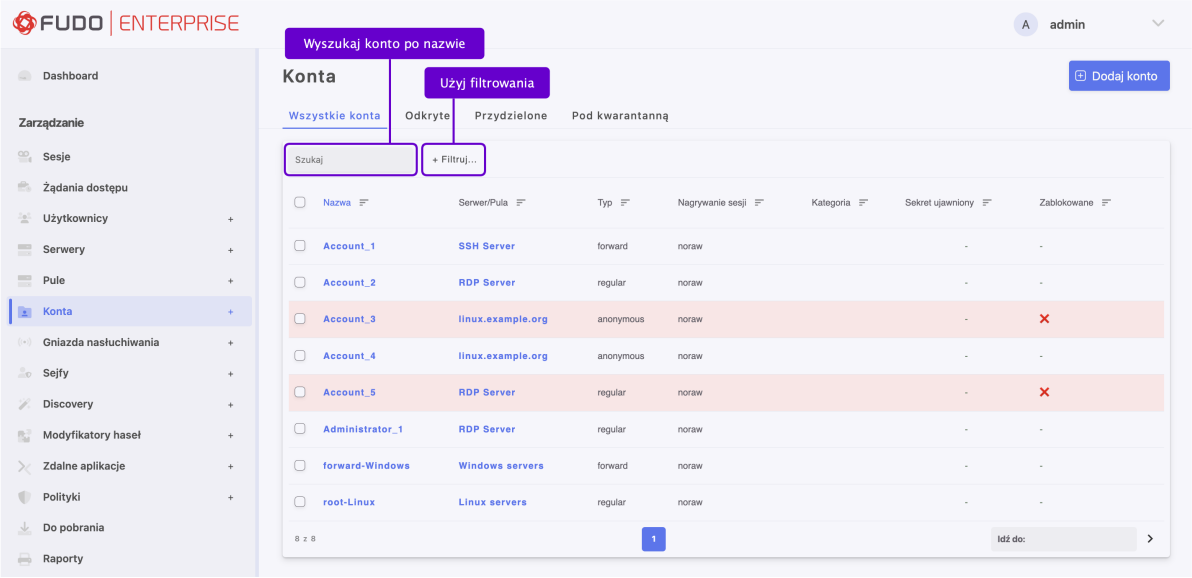
na ikonę czerwonego krzyżyka.

Tematy pokrewne:

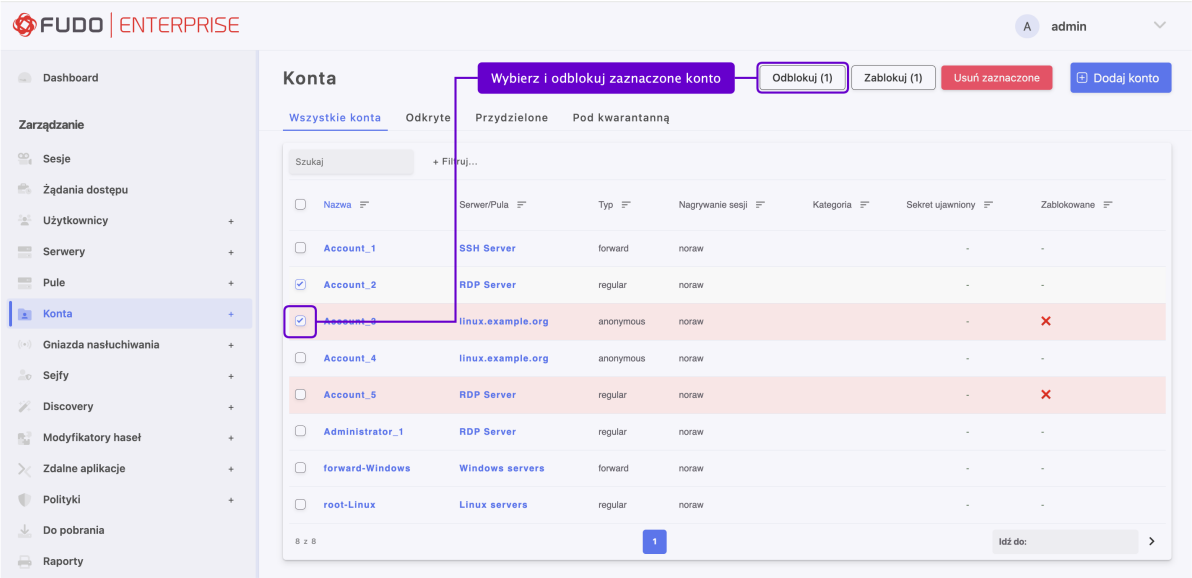
- *Dodawanie konta*
- *Edytowanie konta*
- *Odblokowywanie konta*
- *Usuwanie konta*

10.4 Odblokowywanie konta

1. Wybierz *Zarządzanie* > *Konta*.
2. Zdefiniuj filtry, aby ograniczyć liczbę obiektów wyświetlanych na liście, lub użyj paska wyszukiwania.



3. Kliknij *Odblokuj*.



4. Potwierdź odblokowanie wybranych obiektów.

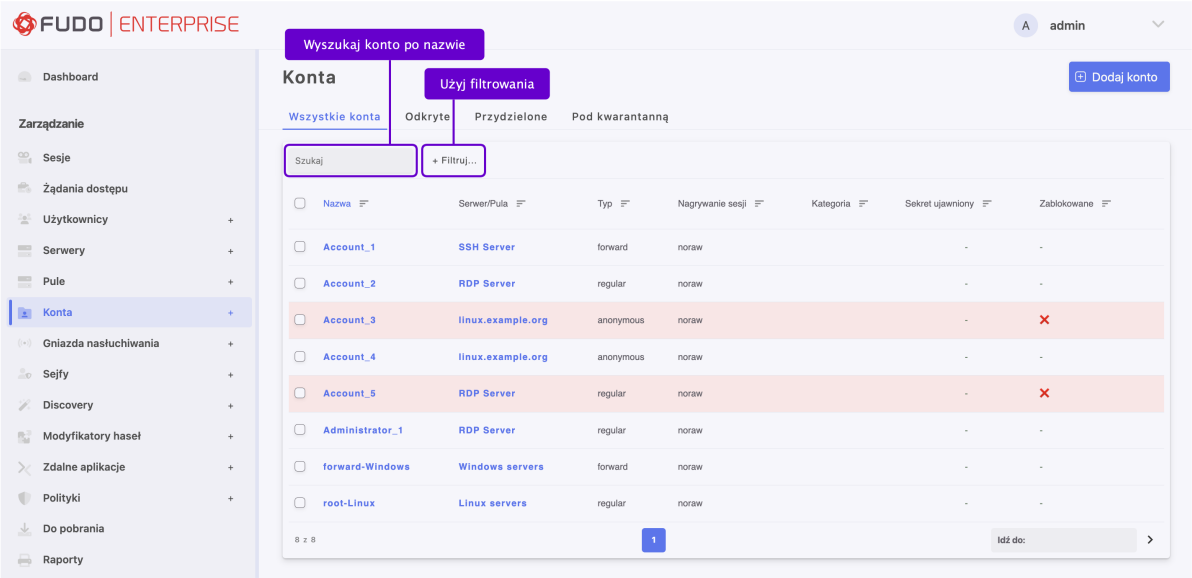
Tematy pokrewne:

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

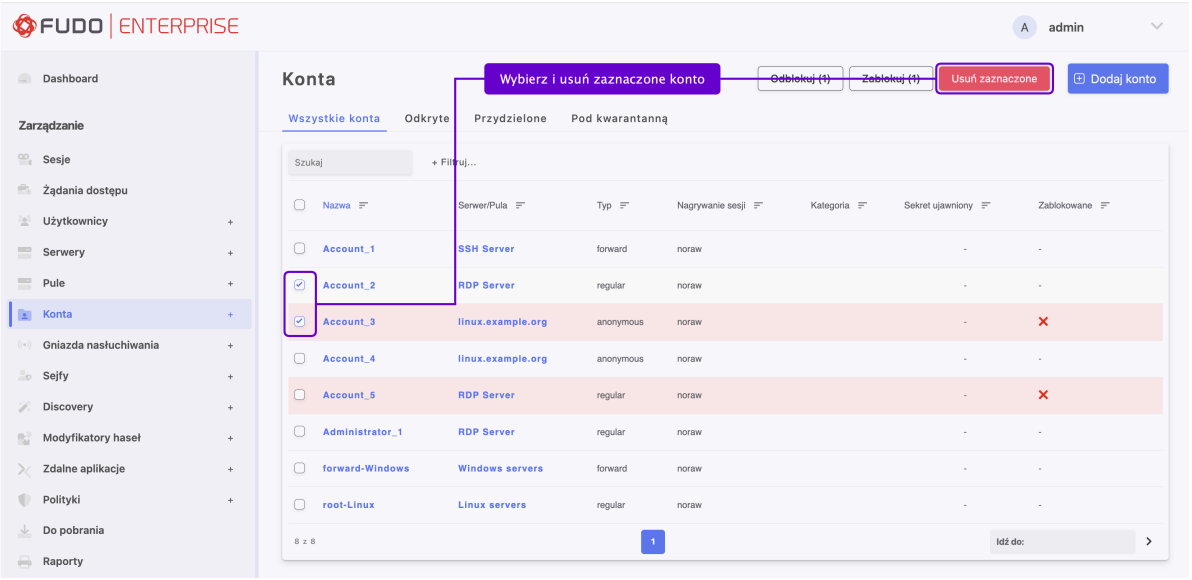
10.5 Usuwanie konta

Ostrzeżenie: Usunięcie definicji konta zakończy wszystkie bieżące połączenia z serwerami, które używają wybranego konta do uzyskania dostępu.

1. Wybierz *Zarządzanie* > *Konta*.
2. Zdefiniuj filtry, aby ograniczyć liczbę obiektów wyświetlanych na liście, lub użyj paska wyszukiwania.



3. Kliknij *Usuń wybrane*.



4. Potwierdź usunięcie wybranych obiektów.

Tematy pokrewne:

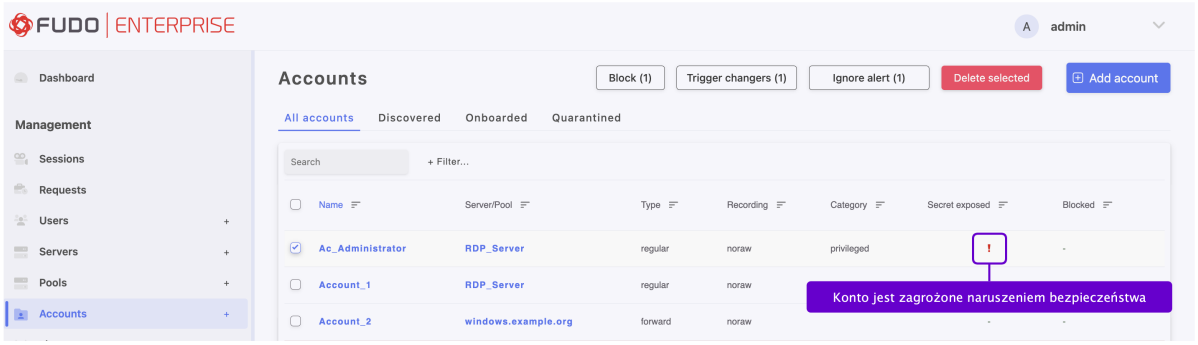
- *Dodawanie konta*
- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowywanie konta*

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, może ograniczyć ryzyko potencjalnego naruszenia zasad bezpieczeństwa. Fudo Enterprise identyfikuje takie zdarzenia i komunikuje administratorom systemu.

Informacja: Wywołanie zmiany hasła jest dostępne tylko dla kont z przypisanym modyfikatorem haseł i polityką zmiany haseł, która ma aktywną opcję *Zmiana hasła włączona*.

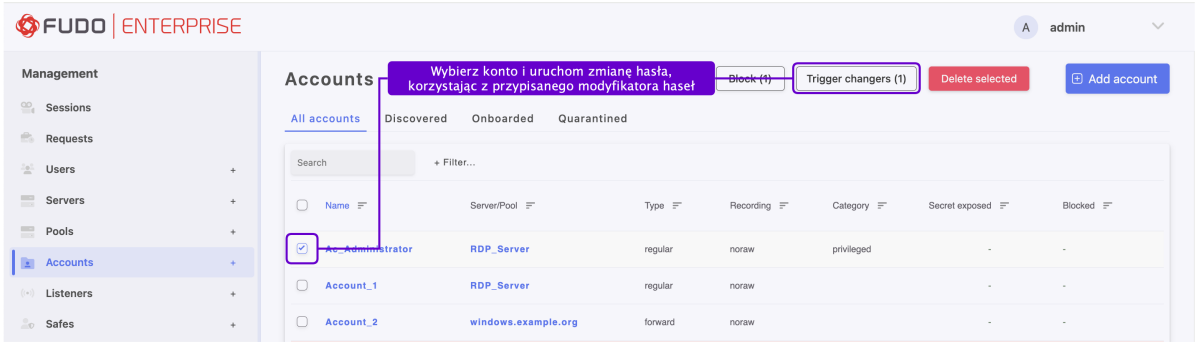


Administrator może zignorować alarm dla wybranego konta lub wymusić zmianę hasła za pomocą przypisanego *modyfikatora haseł*.

10.6.1 Zmiana hasła konta

Zmiana hasła z poziomu listy kont

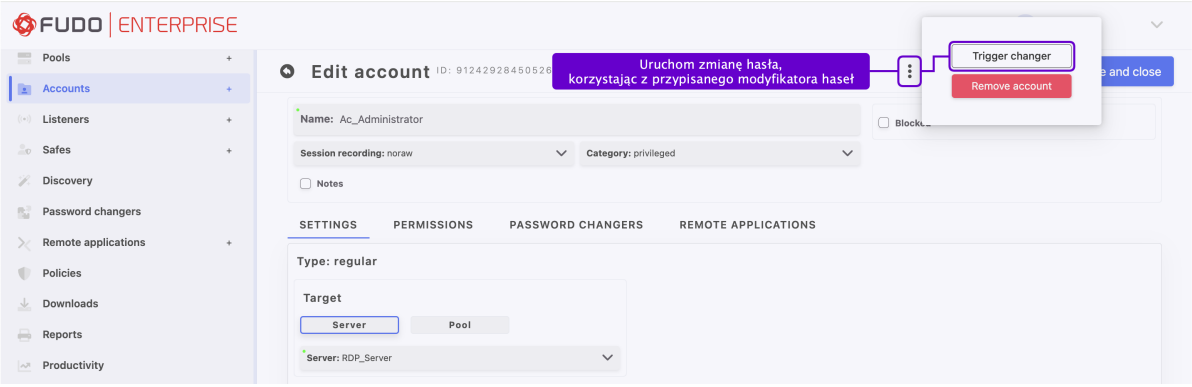
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz konta, dla których chcesz zmienić hasło.
3. Kliknij *Aktywuj modyfikatory*.



4. Kliknij *Zatwierdź*.

Zmiana hasła z poziomu formularza edycji konta

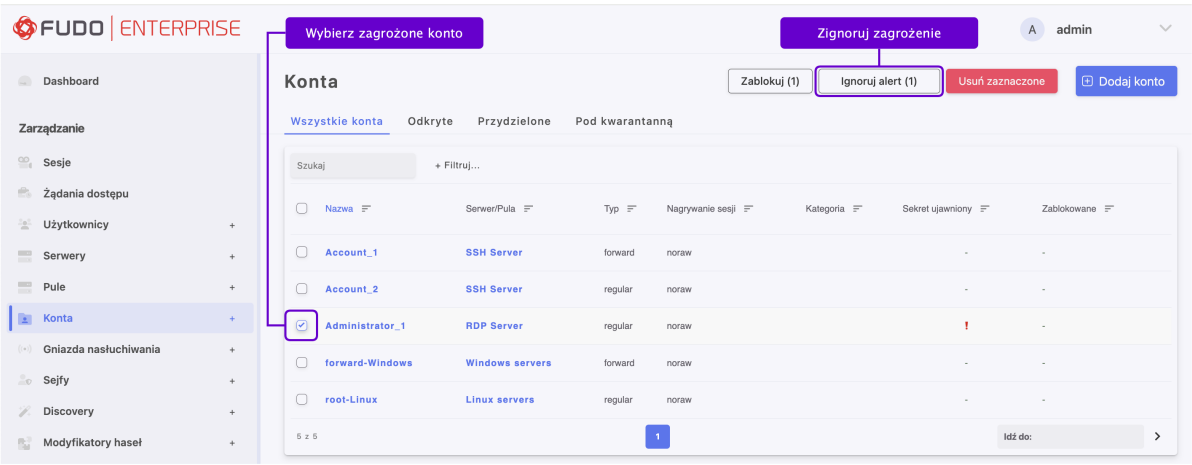
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i kliknij wybrane konto, aby otworzyć formularz edycji.
3. Kliknij symbol trzech kropek przed przyciskami *Anuluj* i *Zapisz*, aby odsłonić dodatkowe menu, a następnie kliknij *Aktywuj modyfikator*.



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*.

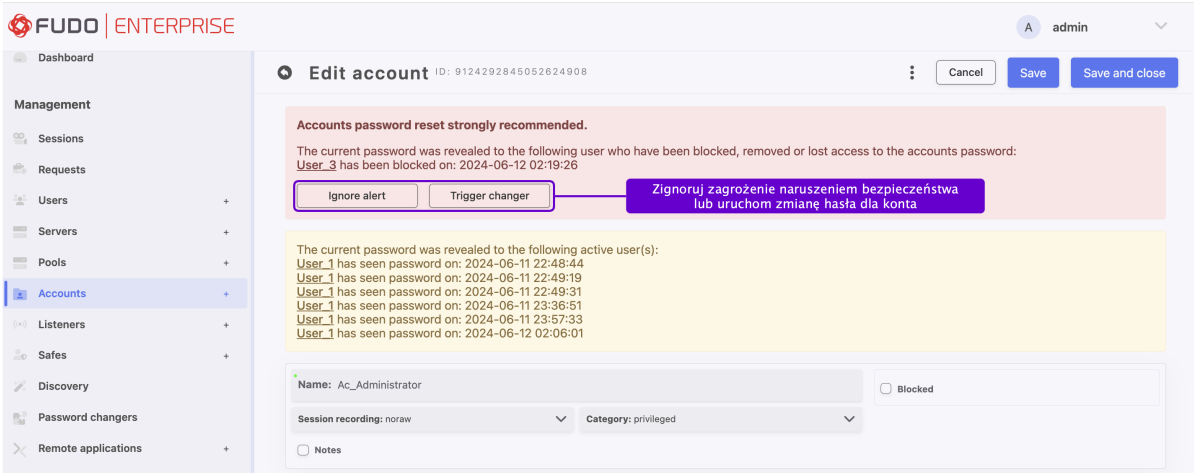


4. Kliknij *Zatwierdź*.

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.

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



3. Kliknij *Zignoruj alert* lub *Uruchom modyfikator*.

Tematy pokrewne:

- *Modyfikatory haseł*
- *Portal użytkownika*

ROZDZIAŁ 11

Gniazda nasłuchiwania

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 jest ostatnią wersją obsługującą tryby **transparent** i **gateway** w **konfiguracji gniazd nasłuchiwania**. Gniazda nasłuchiwania korzystające z tych trybów muszą zostać przekonfigurowane na tryby proxy lub 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.

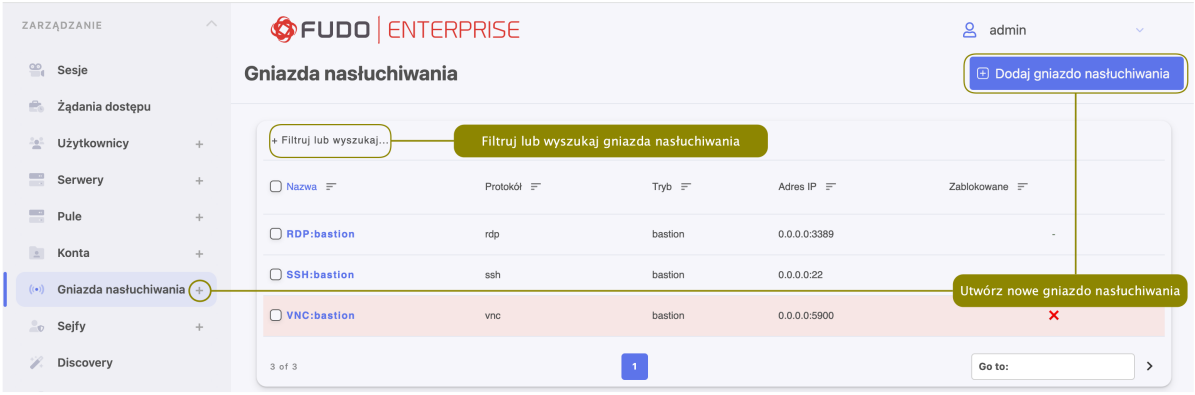
Informacja:

- 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.

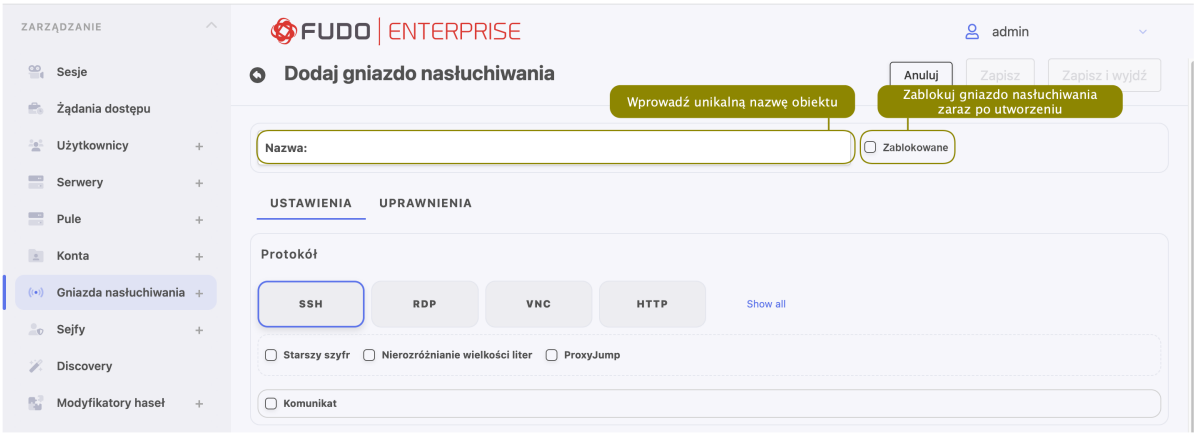
- Gniazdo nasłuchiwania nie może być przypisane do jednego konta anonimowego poprzez dwa sejfy.
- Gniazdo nasłuchiwania nie może zawierać konta anonimowego i *regular* lub *forward* do tego samego serwera o tym samym protokole, co protokół gniazda nasłuchiwania.
- Gniazdo nasłuchiwania nie może być przypisane 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.

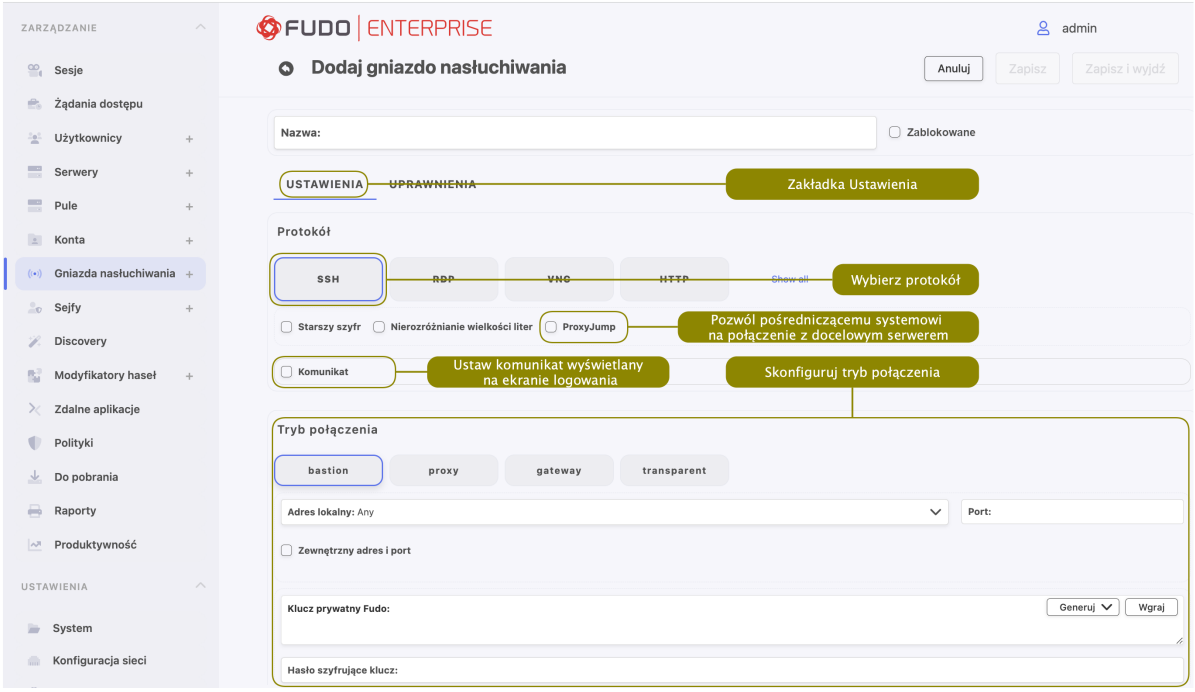
5. Wróć do zakładki *Ustawienia*, a następnie przejdź do rozdziału opisującego dalszą konfigurację gniazda nasłuchiwania zgodnie z wybranym protokołem:

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

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

- 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 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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:

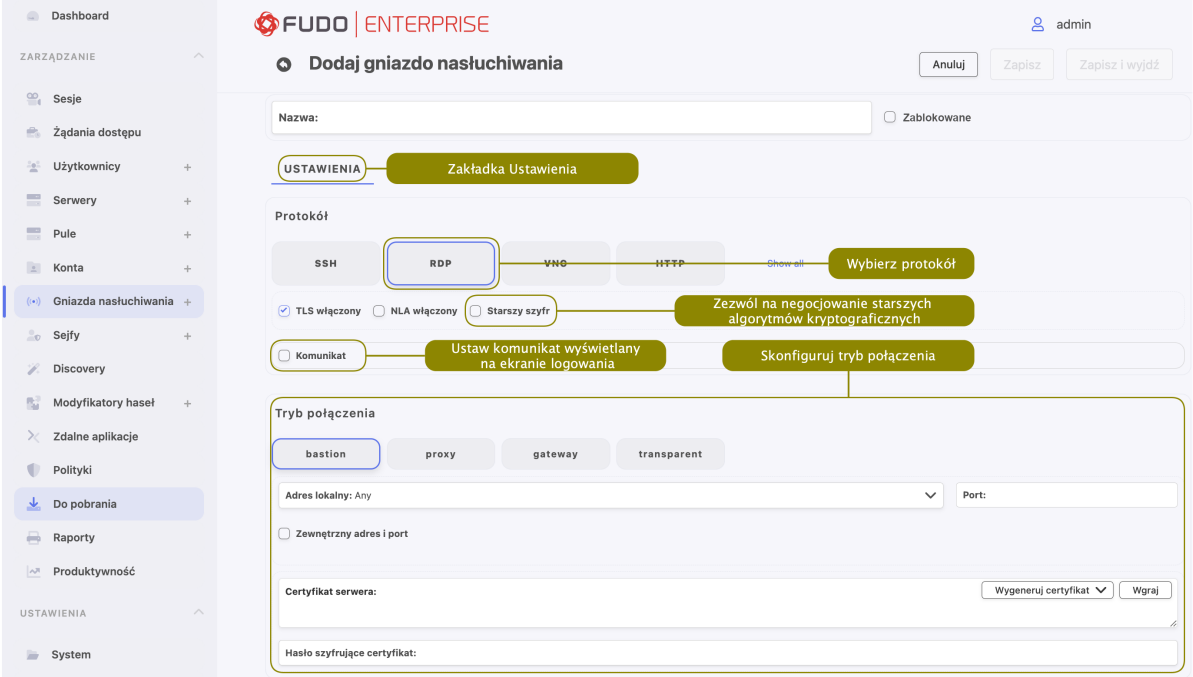
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

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

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

- 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 5.5

Fudo Enterprise 5.5 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

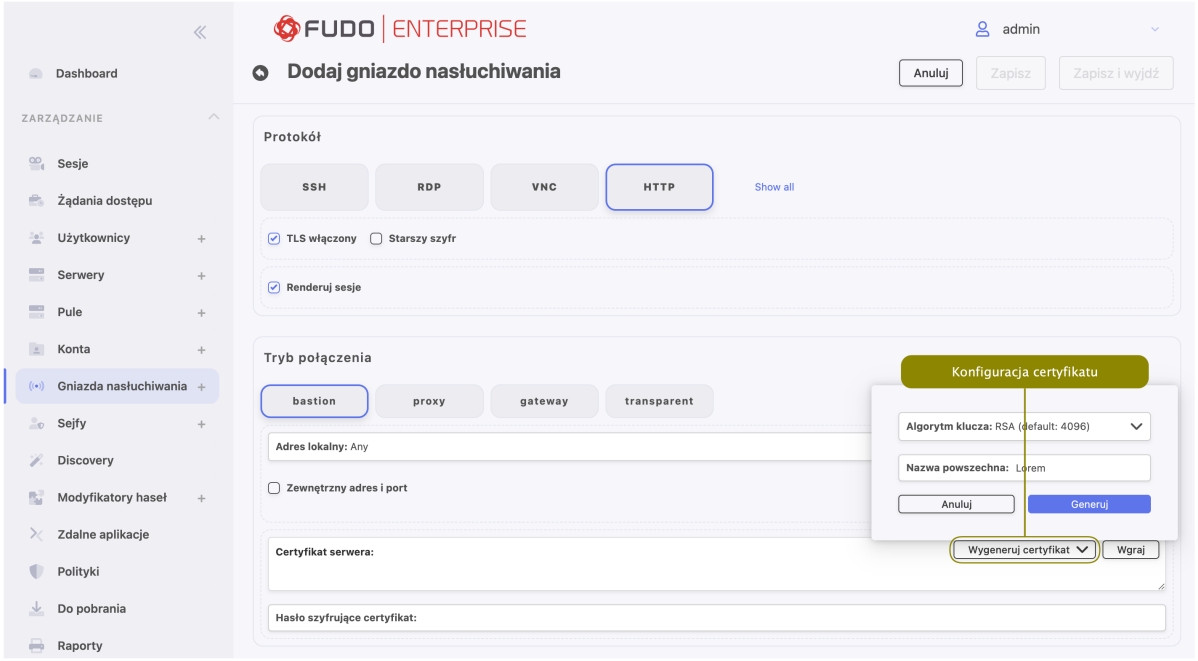
Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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*.

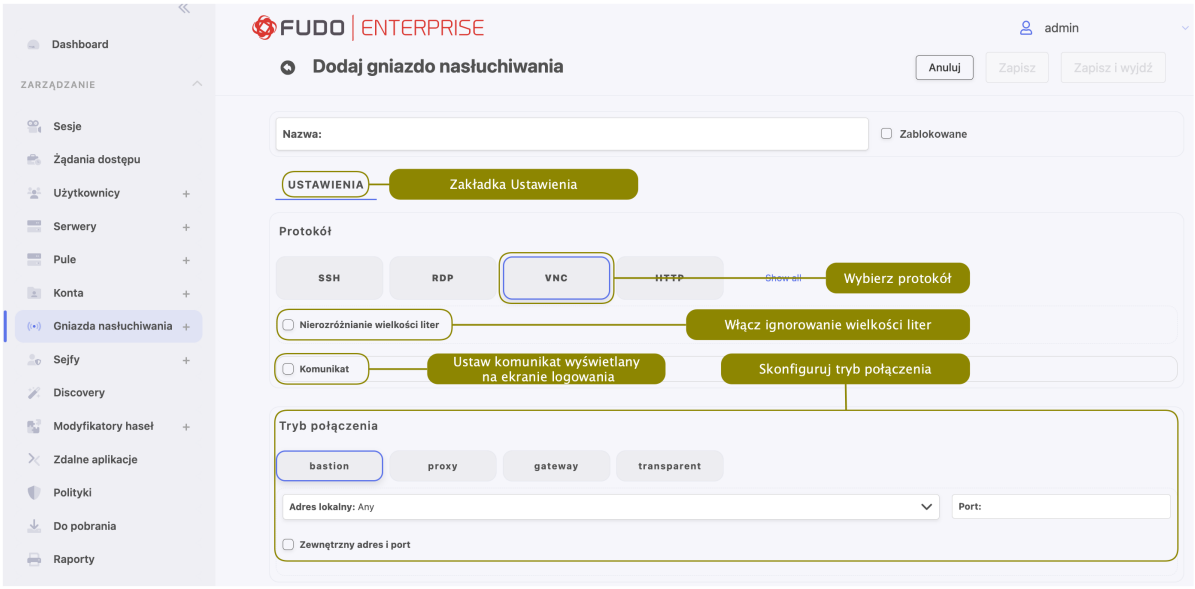
Tematy pokrewne:

- *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 nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta

posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

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

- 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 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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:

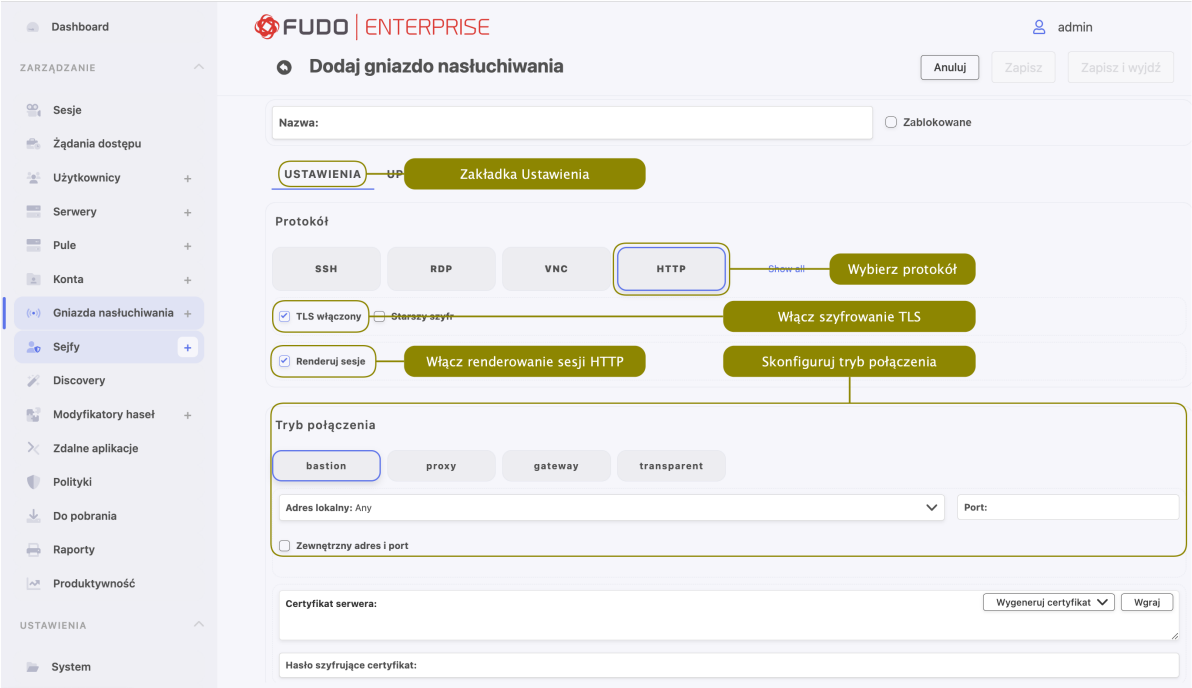
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

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 instacji 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*).
- Aby zobaczyć przykład renderowanej sesji HTTP i sesji HTTP-raw, przejdź do rozdziału *Odtwarzanie sesji*.

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

Informacja: Szczegółowe informacje na temat trybów połączenia znajdziesz w roz-

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

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

- 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 5.5

Fudo Enterprise 5.5 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

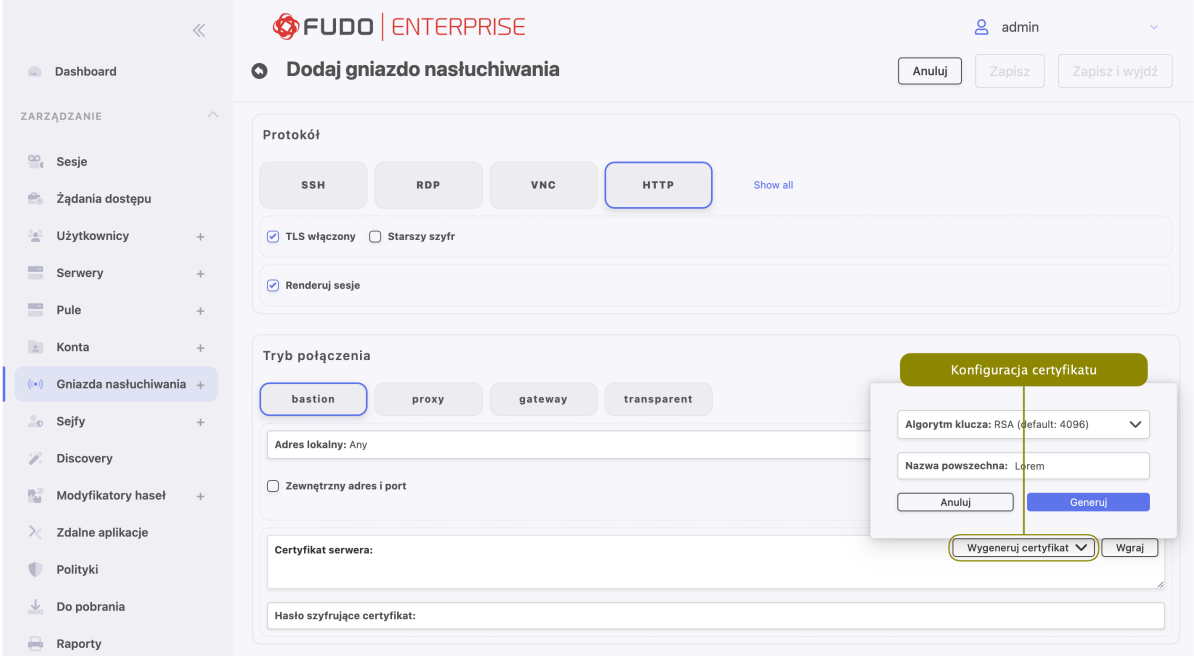
Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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`.



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

7. Kliknij *Zapisz*.

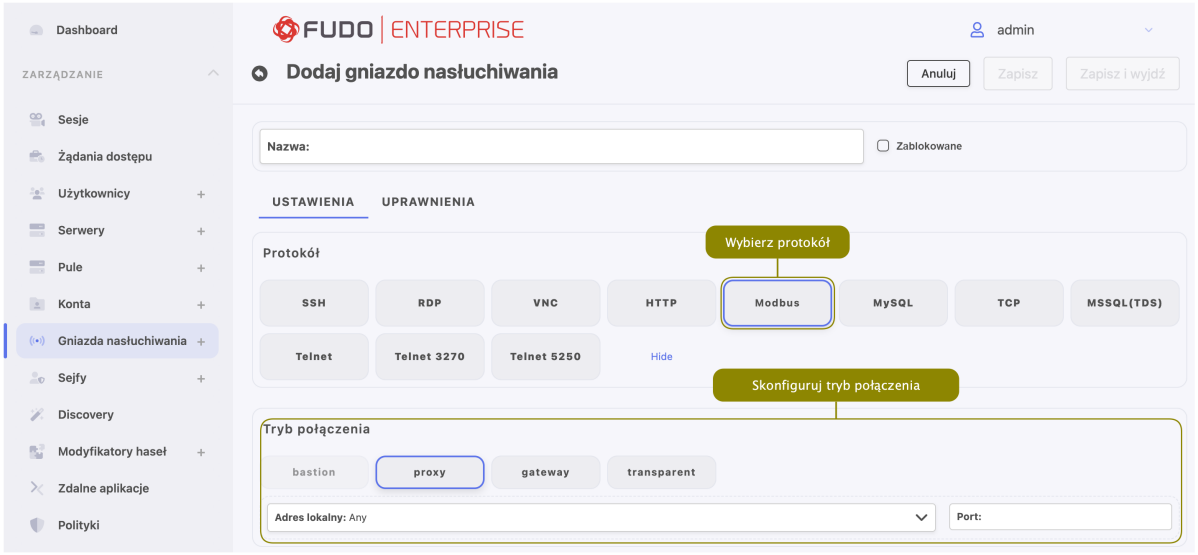
Tematy pokrewne:

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

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 nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.

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

---

gateway

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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:

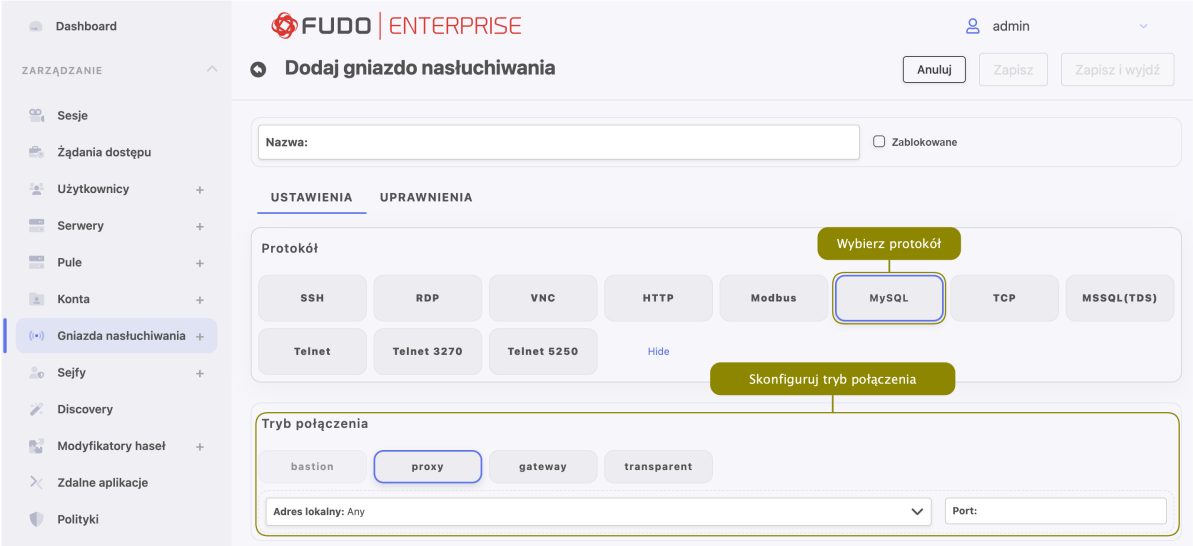
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*

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

---

gateway

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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:

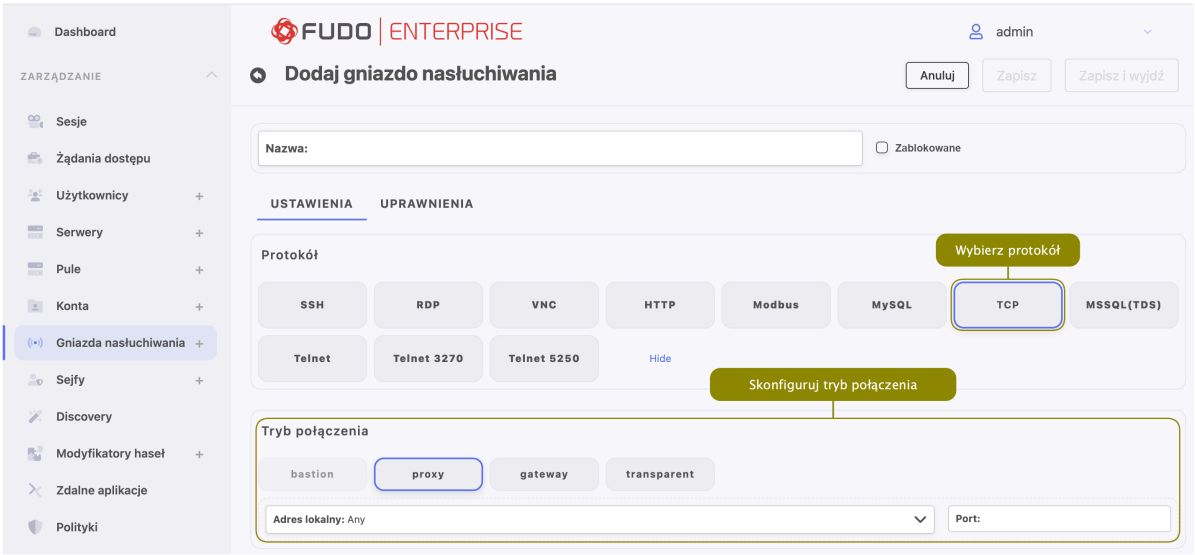
- *Model danych*

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

---

gateway

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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*.

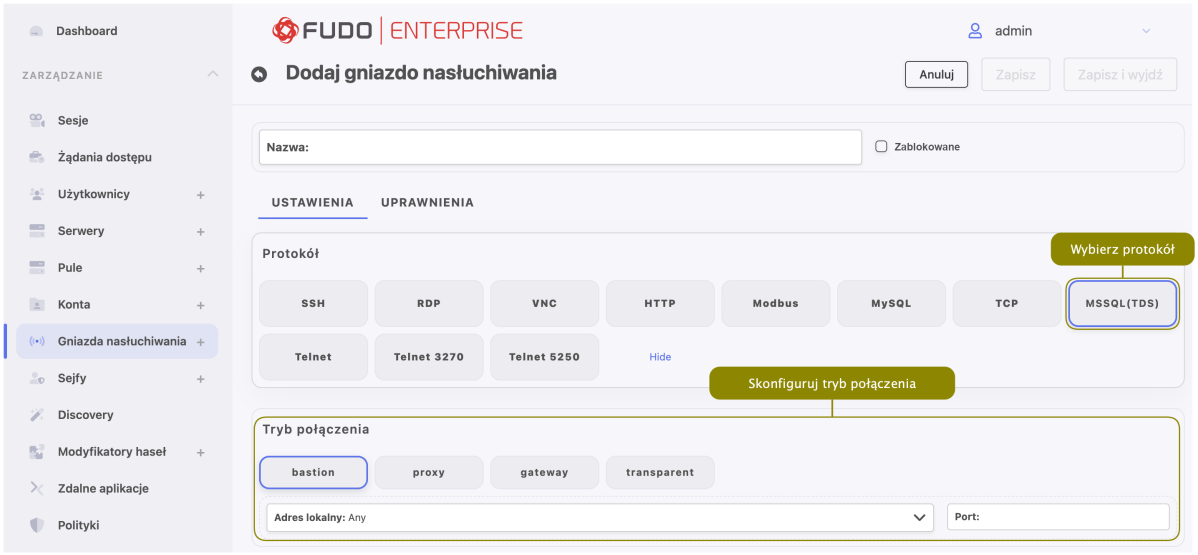
Tematy pokrewne:

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

---

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

---

gateway

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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*.

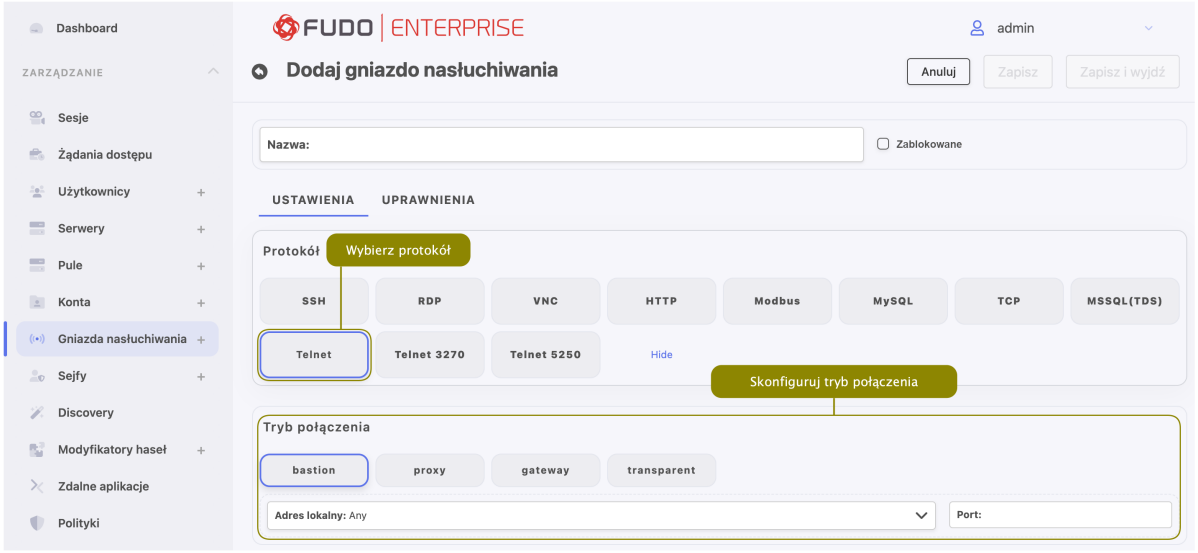
Tematy pokrewne:

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

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

gateway

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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*.

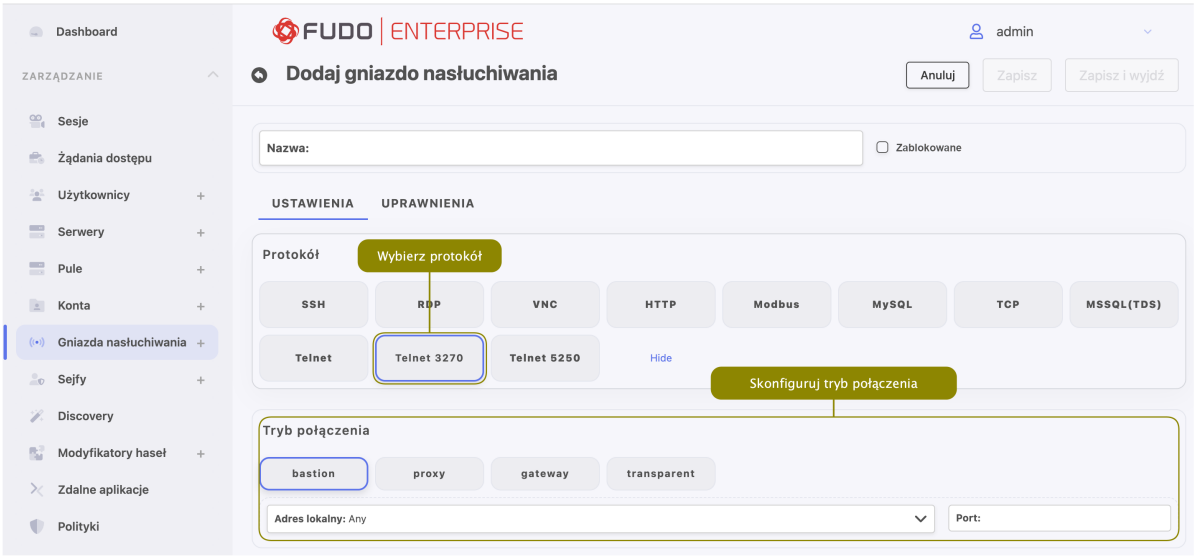
Tematy pokrewne:

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

---

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

---

gateway

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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 nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wybierz etykietowany adres IP i upewnij się, że na pozostałych węzłach wybrana etykieta posiada przypisany adres IP odpowiedni dla danego węzła. Więcej informacji na temat etykietowanych adresów IP znajdziesz w rozdziale *Etykiety adresów IP*.

---

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

---

gateway

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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 5.5

Fudo Enterprise 5.5 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*.

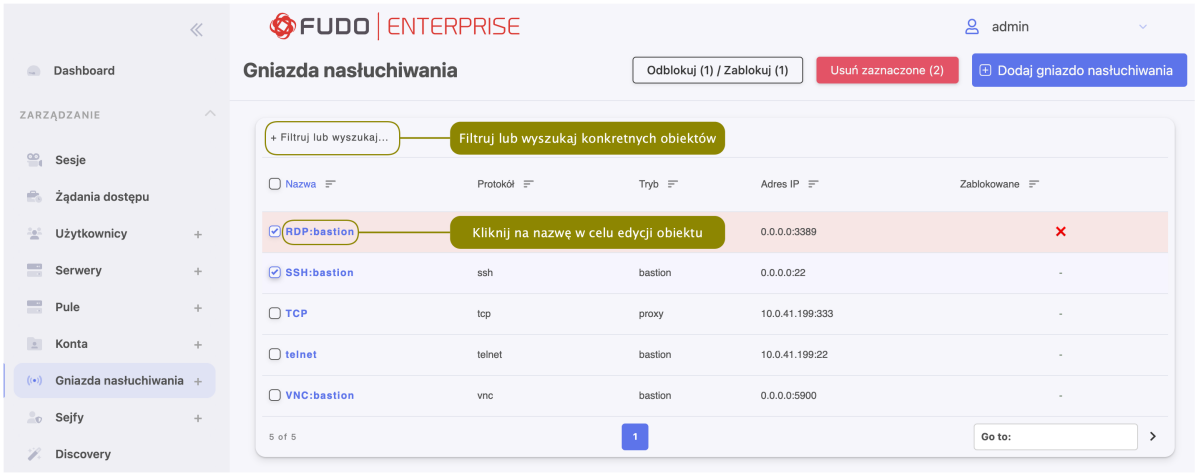
Tematy pokrewne:

- *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:

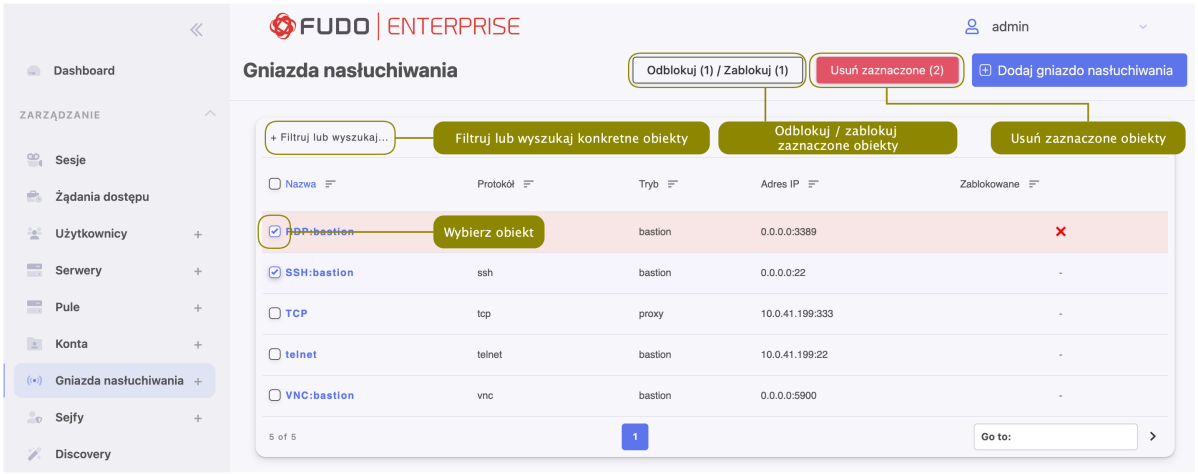
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

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*.

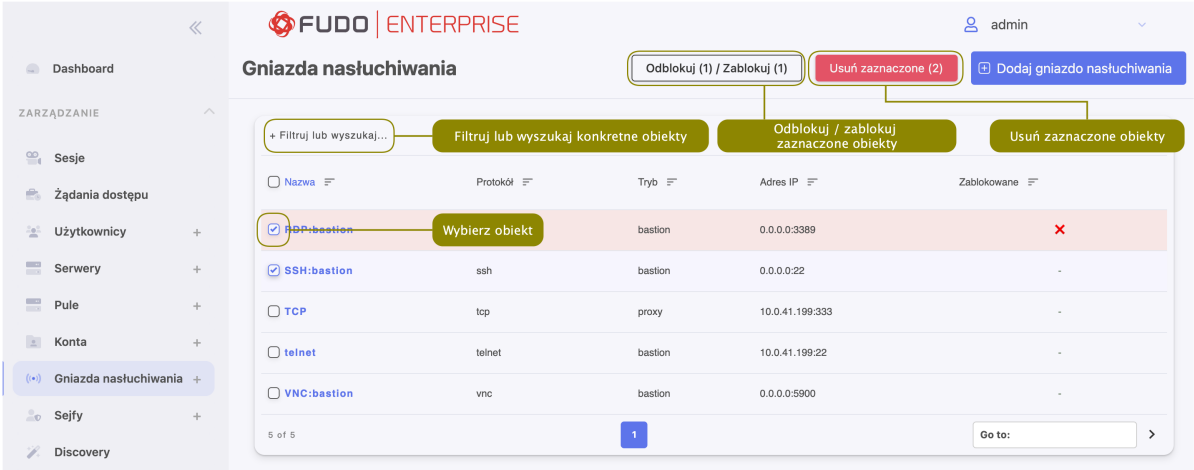
Tematy pokrewne:

- *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:

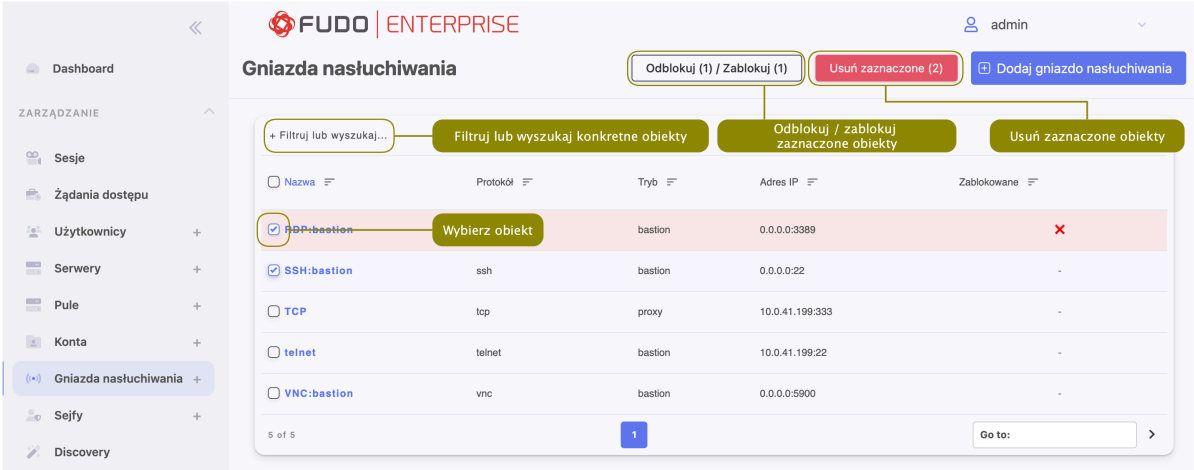
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

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.



3. Kliknij *Usuń zaznaczone*.
4. Kliknij *Potwierdź*, aby zatwierdzić usunięcie zaznaczonych obiektów.

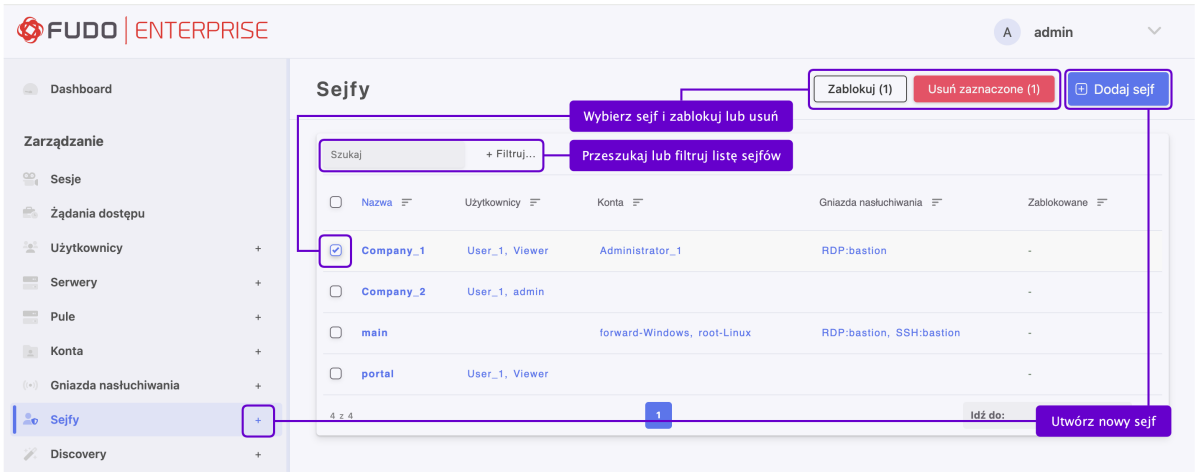
Tematy pokrewne:

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

ROZDZIAŁ 12

Sejfy

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



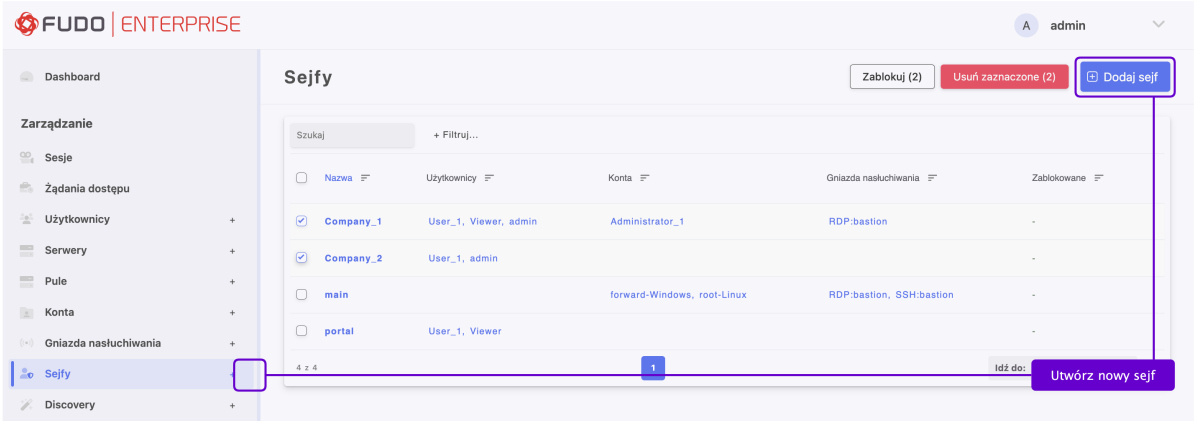
Informacja:

- Sejf `system` może mieć przypisane tylko konto `system`.
- Sejf `portal` może mieć przypisane tylko konto `portal`.
- Użytkownik o roli `operator`, `admin` lub `superadmin` zawsze posiada dostęp do sejfu `system`.
- Użytkownik o roli `user` nie może posiadać dostępu do sejfu `system`.
- Użytkownik anonimowy musi mieć dostęp do sejfów, które zawierają konta anonimowe.

12.1 Dodawanie sejfu

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

1. Kliknij ikonę + w menu głównym obok zakładki *Sejfy* w podsekcji *Zarządzanie*, lub
2. Wybierz *Zarządzanie* > *Sejfy*, a następnie kliknij + *Dodaj sejf*.

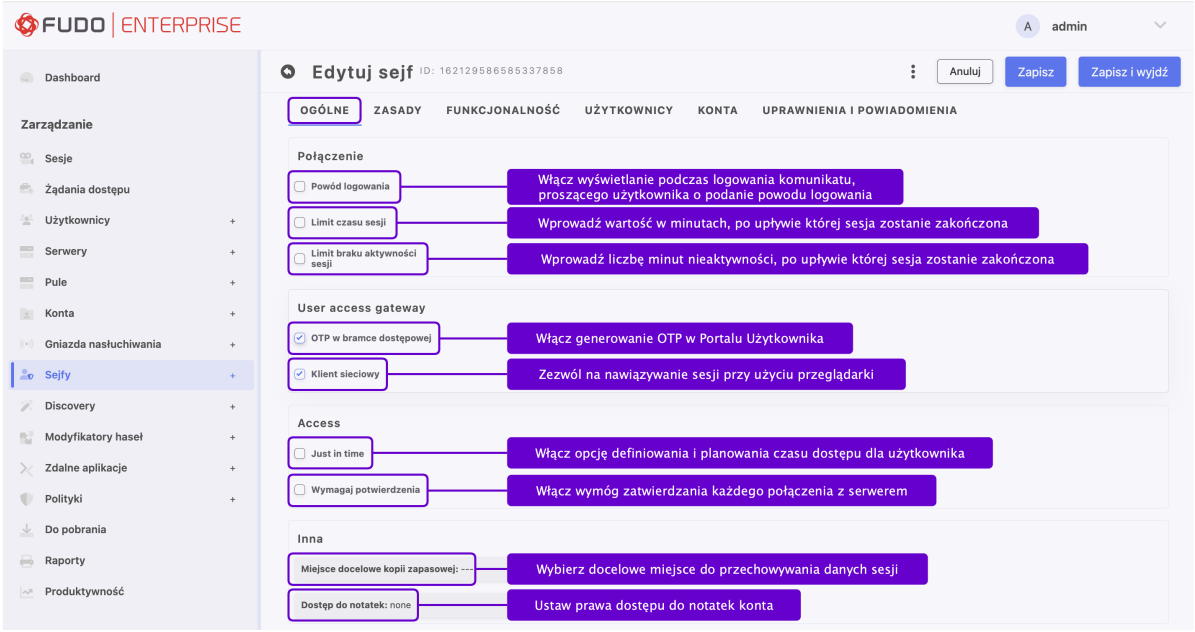


2. Wprowadź nazwę obiektu.
3. Wybierz opcję *Zablokowany*, jeśli chcesz uniemożliwić dostęp do obiektu po jego utworzeniu.
4. Kliknij *Zapisz*, aby zapisać obiekt i kontynuować dalszą konfigurację.

ZAKŁADKA OGÓLNE

5. W zakładce *Ogólne*, w polu *Połączenie*, wybierz opcję *Powód logowania*, aby przy logowaniu wyświetlić monit z zapytaniem o podanie powodu logowania.

Informacja: Powód logowania nie jest obsługiwany w połączeniach *HTTP*.



6. Wybierz opcję *Limit czasu sesji* i wprowadź wartość w minutach, po upływie których sesja zostanie zakończona.
7. Wybierz opcję *Limit nieaktywności sesji* i wprowadź liczbę minut nieaktywności, po upływie których sesja zostanie zakończona.
8. Opcja *OTP w Portalu Użytkownika* jest domyślnie włączona i odpowiada za generowanie OTP w Portalu Użytkownika.

Ostrzeżenie: Wyłączenie opcji *OTP w Portalu Użytkownika* uniemożliwi połączenie przez Klienta natywnego oraz Klienta sieciowego w Portalu Użytkownika. Tylko dostęp przez *Żądania dostępu* będzie wtedy dostępny.

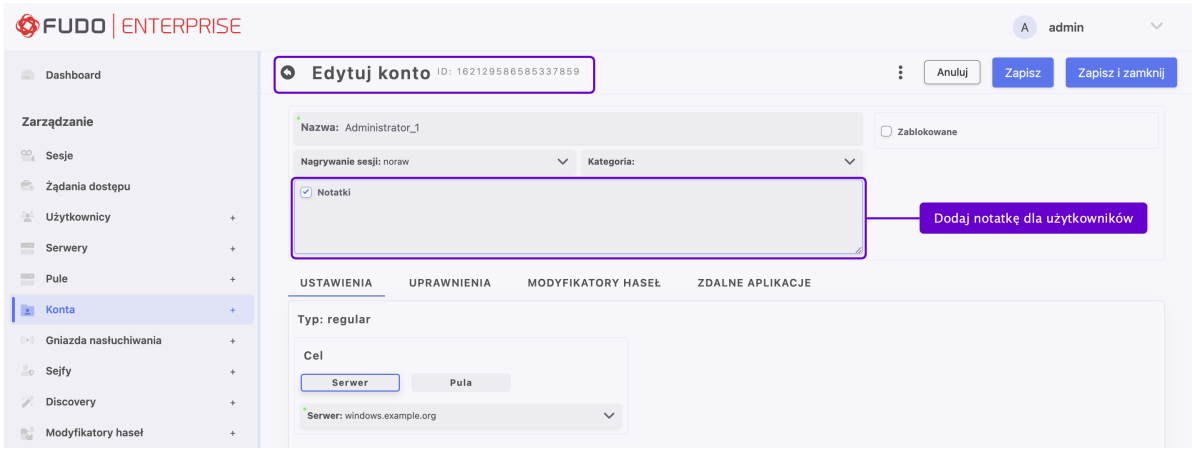
9. W przypadku sejfów opartych na protokołach RDP, VNC oraz SSH, wybierz opcję *Klient sieciowy* w celu połączenia z serwerem w przeglądarce.

Informacja: Opcja *Klient sieciowy* nie może być włączona, gdy opcja *OTP w Portalu Użytkownika* jest wyłączona.

10. Wybierz opcję *Just in time* i podaj liczbę głosujących. Ta funkcja pozwala na definiowanie i planowanie czasu, kiedy użytkownik może uzyskać dostęp do określonych zasobów przez określony czas. Użytkownik wysyła żądania przez Portal Użytkownika, a głosujący akceptują lub odrzucają je w panelu administracyjnym. Przeczytaj więcej o funkcji Just-In-Time w sekcji *Żądania dostępu*.
11. Wybierz 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.
12. W polu *Inne*, wybierz *Miejsce docelowe kopii zapasowej* jako miejsce przechowywania danych. Aby utworzyć miejsce docelowe kopii zapasowej, przejdź do sekcji *Kopia zapasowa i retencja*.

13. Z rozwijanego menu *Dostęp do notatek*, wybierz prawa dostępu do notatek danego konta: `read`, `write` lub `none`.

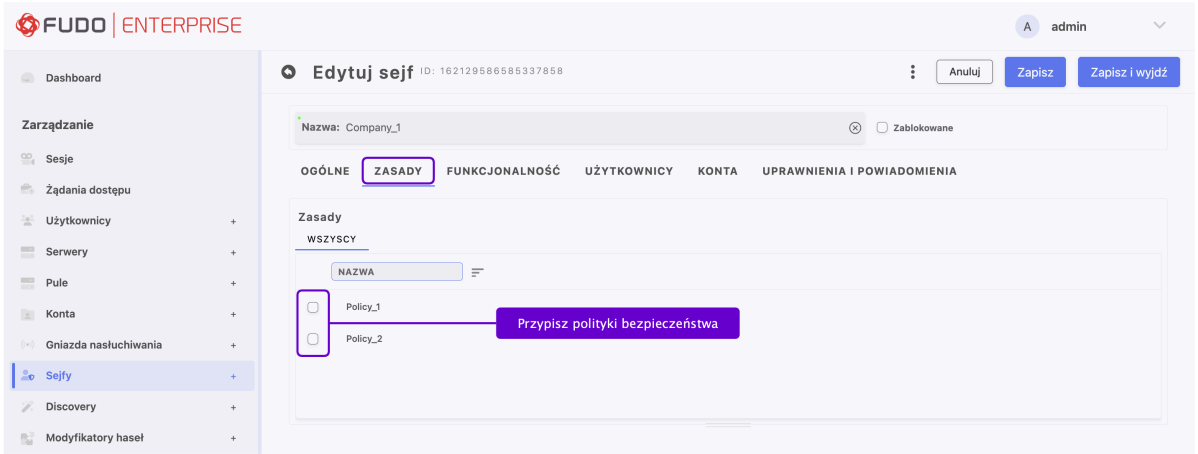
Informacja: Notatki mogą być dostępne zarówno z formularza edycji konta



lub w *Access Gateway*.

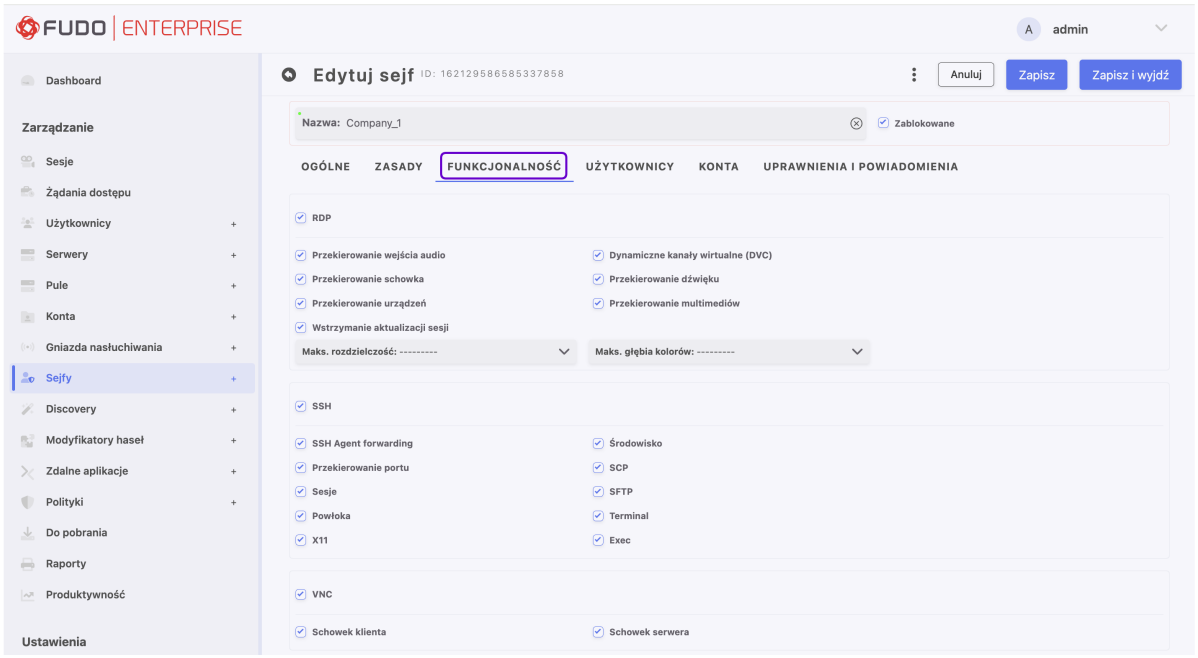
ZAKŁADKA POLITYKI

14. Przejdź do zakładki *Polityki* i przypisz wybrane *polityki bezpieczeństwa* poprzez zaznaczenie pól wyboru przed ich nazwami.



ZAKŁADKA FUNKCJONALNOŚĆ

15. Przejdź do zakładki *Funkcjonalność* i włącz wybrane funkcje protokołów.



Informacja: Funkcjonalność protokołów - przegląd opcji:

- RDP
  - **Przekierowanie wejścia audio** - Przekierowuje dźwięk z urządzenia klienta do pulpitu zdalnego, umożliwiając działanie aplikacji wykorzystujących dźwięk.
  - **Dynamiczne wirtualne kanały** - Włącza obsługę funkcji wielu kanałów wirtualnych w jednej sesji RDP.
  - **Przekierowanie schowka** - Udostępnia zawartość schowka między klientem a pulpitem zdalnym, umożliwiając funkcjonalność kopiuj/wklej.
  - **Przekierowanie dźwięku** - Przekierowuje dźwięk z pulpitu zdalnego do urządzenia klienta.
  - **Przekierowanie urządzeń** - Umożliwia użycie peryferyjnych urządzeń (np. drukarek, urządzeń USB, kart typu *smart-card*) podłączonych do urządzenia klienta w sesji pulpitu zdalnego.
  - **Przekierowanie multimediów** - Poprawia odtwarzanie multimediów poprzez przeniesienie procesu dekodowania na urządzenie klienta, zapewniając płynniejsze odtwarzanie wideo i audio.
  - **Wstrzymanie aktualizacji sesji** - Wstrzymuje i zapisuje bieżącą sesję, umożliwiając jej wznowienie później bez konieczności ponownego uruchamiania. Zaznaczenie opcji spowoduje, że treść sesji nie będzie dostępna w odtwarzaczu przez okres, w którym aplikacja kliencka będzie zminimalizowana.
  - **Maksymalna rozdzielczość** - Ustawia maksymalną rozdzielczość dla sesji pulpitu zdalnego, wpływając na jakość wyświetlania i zużycie przepustowości.
  - **Maksymalna głębia** - Ustawia maksymalną głębię kolorów dla sesji pulpitu zdalnego, wpływając na jakość wizualną i zużycie przepustowości.

  - **Konfiguracja indywidualna** – Umożliwia wpisanie własnej treści, która zostanie dołączona do pobieranego pliku konfiguracyjnego RDP.

- SSH*
  - **SSH Agent Forwarding** - Umożliwia użytkownikowi korzystanie z opcji *SSH Agent Forwarding* podczas uwierzytelnienia.
  - **Środowisko** - Wyłączenie tej opcji uniemożliwi przekazywanie zmiennych środowiskowych do serwera za pomocą `-o SendEnv=`. Ta opcja nie blokuje używania zmiennych środowiskowych na serwerze docelowym.
  - **Przekierowanie portu** - Obsługuje przekierowanie ruchu sieciowego z jednego portu na inny, umożliwiając bezpieczne połączenia z usługami za zaporami lub NAT.
  - **SCP (Secure Copy Protocol)** - Umożliwia bezpieczny transfer plików między lokalnym a zdalnym systemem przy użyciu SSH.
  - **Sesje** - Wyłączenie tej opcji uniemożliwi inicjowanie interaktywnych sesji i wykonywanie zdalnych poleceń. Niemniej jednak pewne opcje, takie jak przekazywanie portów, pozostaną dostępne.
  - **SFTP (Secure File Transfer Protocol)** - Umożliwia bezpieczny transfer plików i zarządzanie nimi przez SSH.
  - **Powłoka** - Wyłączenie tej opcji uniemożliwi inicjowanie interaktywnych sesji. Jednakże nadal możliwe będzie wykonanie zdalnych poleceń oraz przekazywanie portów.
  - **Terminal** - Umożliwia obsługę funkcjonalności *pseudo-terminal*.
  - **X11** - Umożliwia obsługę protokołu X11.
  - **Exec** - Umożliwia wykonanie pojedynczego polecenia na zdalnym serwerze bez uruchamiania interaktywnej sesji powłoki.

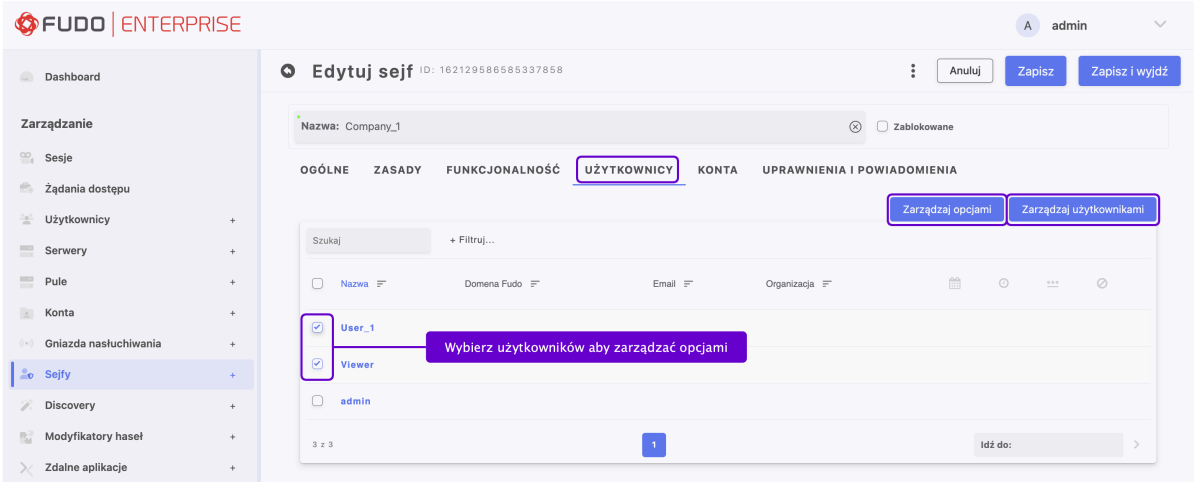
- VNC
  - **Schowek klienta** - Opcja umożliwia użytkownikowi wklejanie danych ze schowka do komputera serwera VNC.
  - **Schowek serwera** - Opcja umożliwia użytkownikowi kopiowanie oraz wklejanie danych z komputera serwera VNC do swojego komputera.

*Aby uzyskać szczegółowe informacje na temat funkcji SSH, zapoznaj się z dokumentem *RFC 4254 - The Secure Shell (SSH) Connection Protocol.*

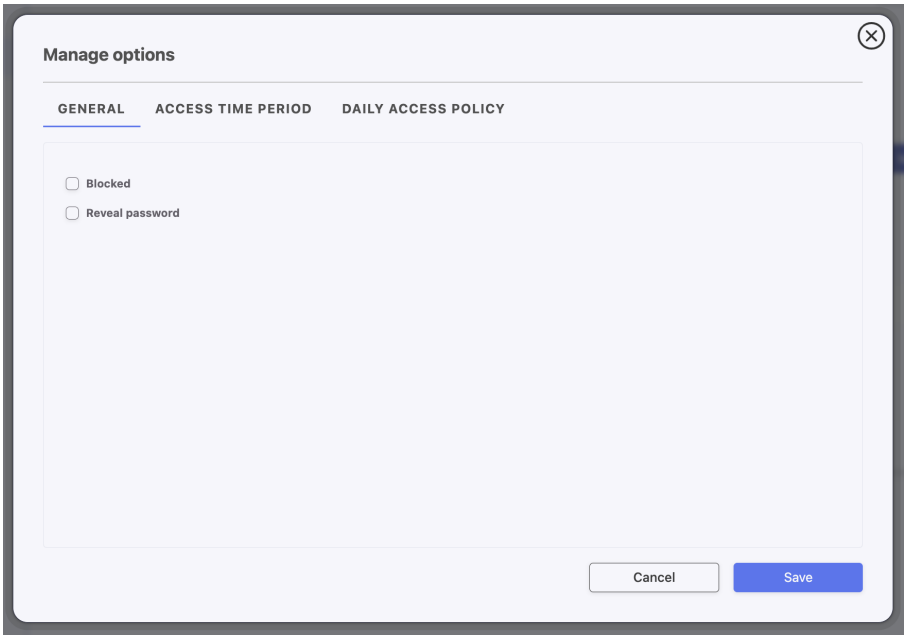
ZAKŁADKA UŻYTKOWNICY

16. Przejdź do zakładki *Użytkownicy*, aby przypisać użytkowników, którym będzie wolno uzyskiwać dostęp do kont przypisanych do tego sejfu.

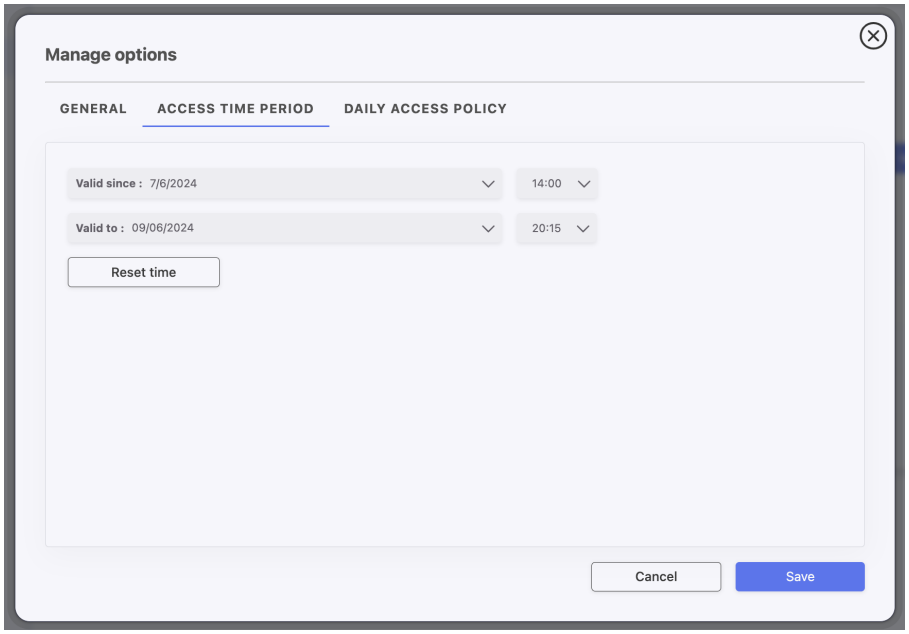
- Kliknij *Zarządzaj użytkownikami*.
- Zaznacz pole wyboru przed nazwami użytkowników, aby umożliwić im dostęp do serwerów poprzez monitorowany sejf.



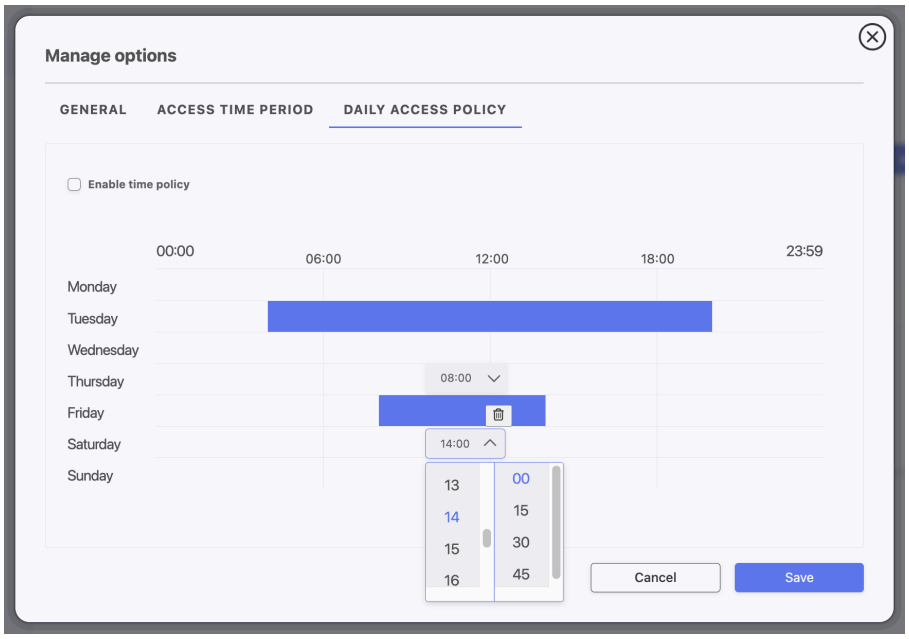
- Kliknij *Zapisz*, aby zamknąć okno dialogowe.
- Aby zdefiniować opcje dostępu do sejfu dla użytkownika, zaznacz pole wyboru przed nazwami pożądanych użytkowników i kliknij *Zarządzaj opcjami*.
  - Przejdź do zakładki *Ogólne* i wybierz opcję *Zablokowany*, jeśli chcesz zablokować użytkowników wybranych w poprzednim kroku.
  - Wybierz *Pokaż hasło*, aby umożliwić wybranym użytkownikom korzystanie z funkcji Secret Checkout i przeglądanie haseł w Portalu Użytkownika.



  - Wybierz zakładkę *Okres dostępu*, aby wypełnić pola *Ważne od* i *Ważne do* datą i godziną, kiedy użytkownik będzie miał dostęp do serwerów przez dany sejf. Dostęp do danego sejfu jest automatycznie przyznawany użytkownikowi w zdefiniowanej dacie i godzinie.



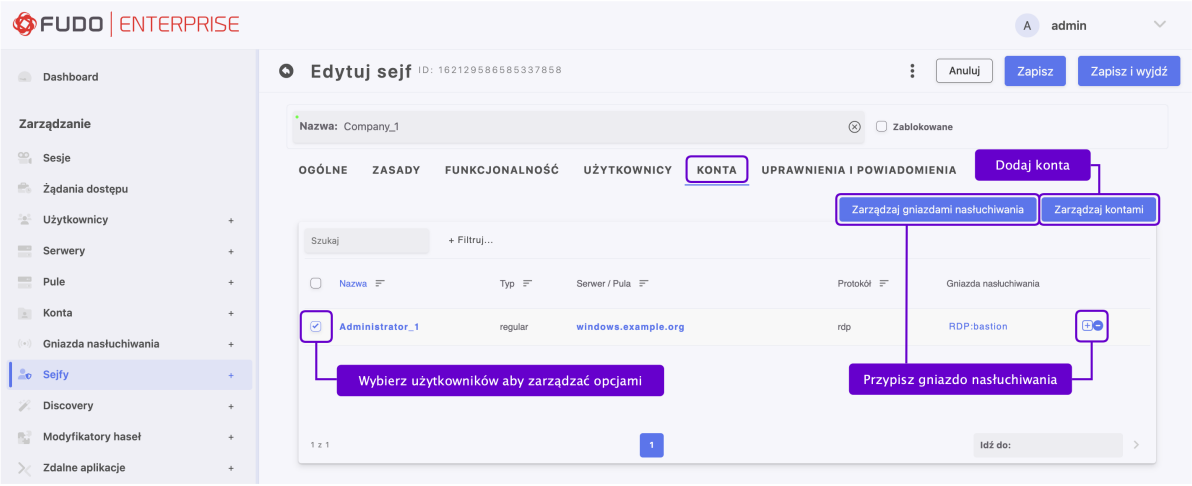
– Wybierz zakładkę *Dzienna polityka dostępu*, aby włączyć i zdefiniować przedziały czasowe, w których użytkownik będzie mógł łączyć się z serwerami. Wystarczy kliknąć w wiersz na wysokości wybranego dnia tygodnia, aby dodać zakres, a następnie kliknąć ten zakres, aby otworzyć menu edycji zakresu czasowego.



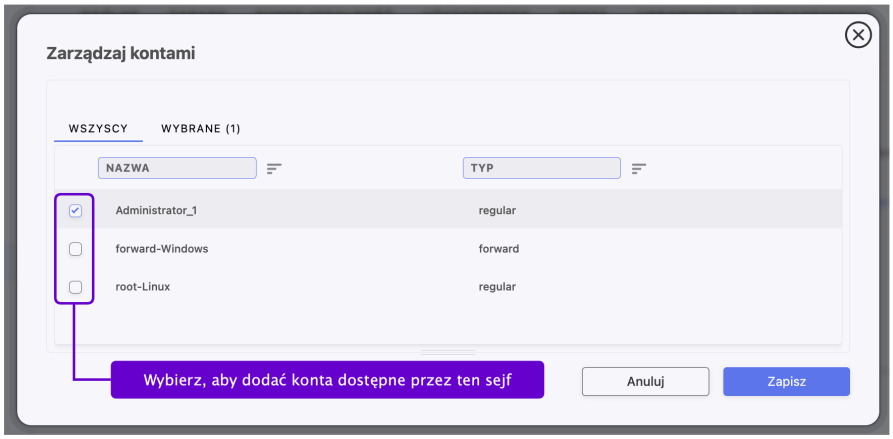
Informacja: Opcje polityki czasu dostępu są wyłączone, gdy dla sejfu jest włączona opcja *Just in time*.

ZAKŁADKA KONTA

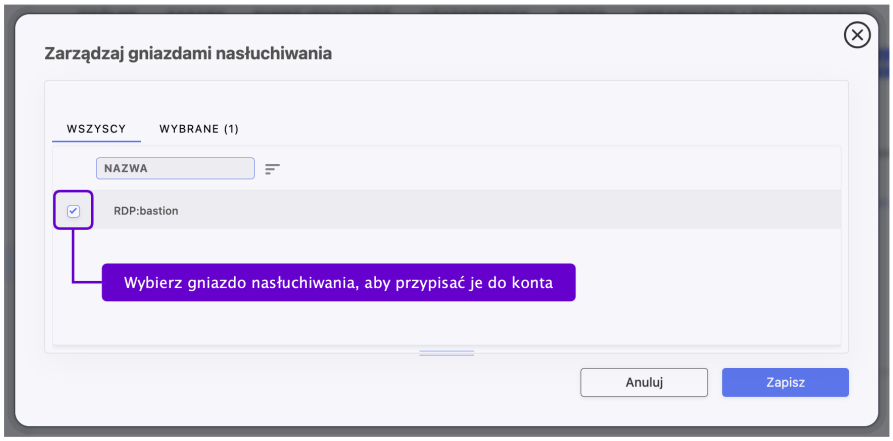
17. Wybierz zakładkę *Konta*, aby dodać konta dostępne przez ten sejf.



- Kliknij *Zarządzaj kontami*.
- Zaznacz pole wyboru przed nazwami kont, aby je dodać.



- Kliknij *Zapisz*, aby zamknąć okno dialogowe.
- Wybierz żądane konto i kliknij *Zarządzaj gniazdami nasłuchiwania*, aby przypisać je do kont.



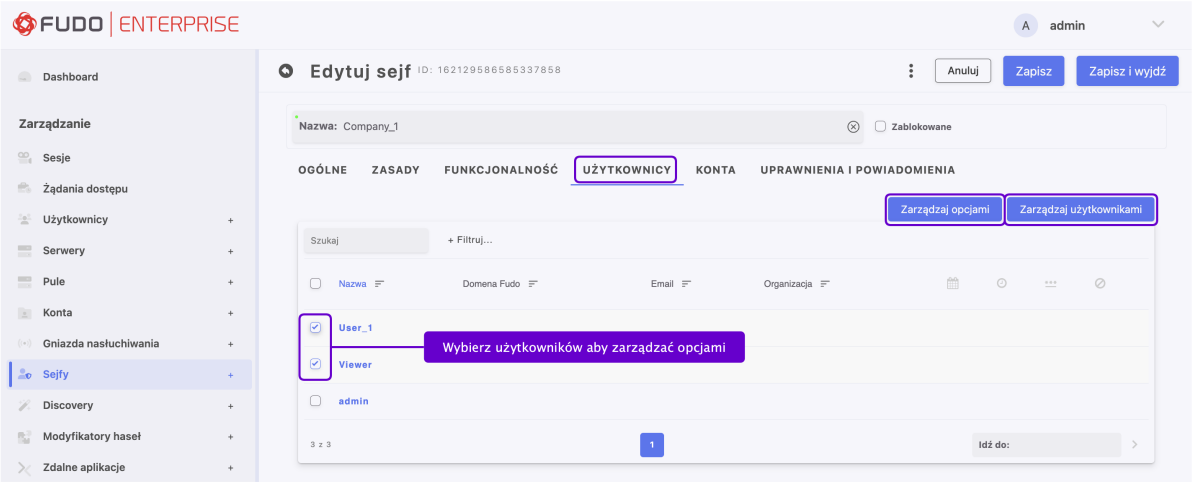
- Kliknij *Zapisz*, aby zamknąć okno dialogowe.

ZAKŁADKA UPRAWNIENIA I POWIADOMIENIA

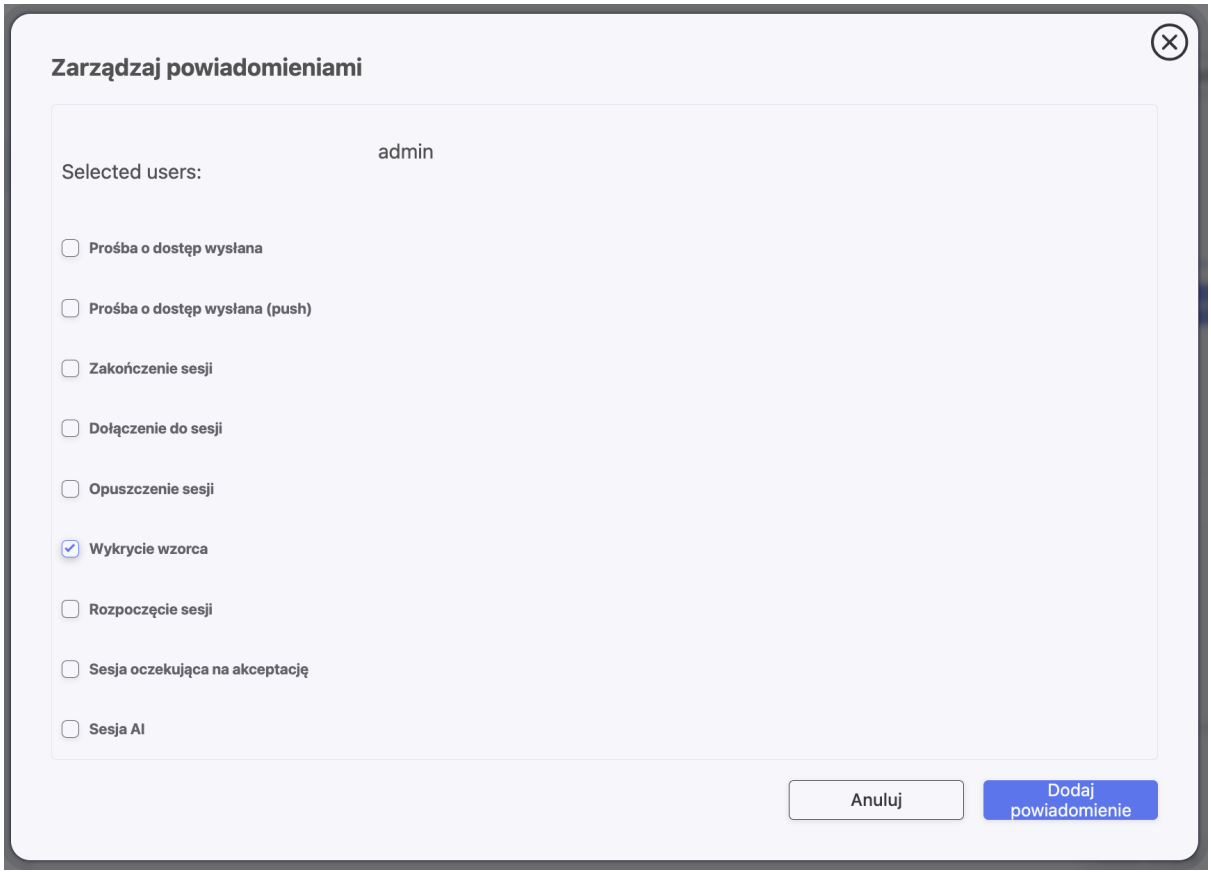
18. Wybierz zakładkę *Uprawnienia i Powiadomienia*, aby przypisać użytkowników mających

prawo zarządzania tym sejfem i określić powiadomienia, które będą wysyłane do danego użytkownika. Więcej informacji możesz znaleźć w sekcji *Powiadomienia*.

- Kliknij *Zarządzaj użytkownikami*.
- Zaznacz pole wyboru przed nazwami użytkowników, aby przypisać użytkowników mających prawo zarządzania tym sejfem.



- Kliknij *Zapisz*, aby zamknąć okno dialogowe.
- Aby zdefiniować określone typy powiadomień dla użytkownika, zaznacz pole wyboru przed nazwami wybranych użytkowników i kliknij *Zarządzaj opcjami*.



- Kliknij *Dodaj powiadomienie*, aby zamknąć okno dialogowe.

19. Kliknij *Zapisz* lub *Zapisz i zamknij*, aby zapisać konfigurację sejfu.

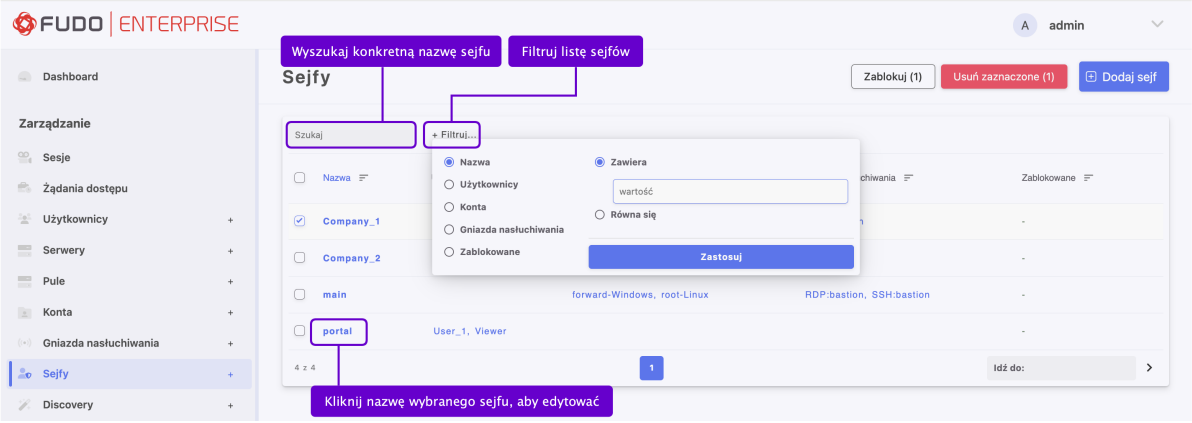
19. Kliknij Zapisz lub Zapisz i zamknij, aby zapisać konfigurację sejfu.

Tematy pokrewne:

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

12.2 Modyfikowanie sejfu

1. Wybierz *Zarządzanie* > *Sejfy*.
2. Zdefiniuj filtry, aby ograniczyć liczbę obiektów wyświetlanych na liście, lub użyj paska wyszukiwania.



3. Znajdź i kliknij nazwę żądanego obiektu, aby otworzyć stronę jego konfiguracji.
4. Zmodyfikuj parametry konfiguracji według potrzeb.
5. Kliknij *Zapisz*.

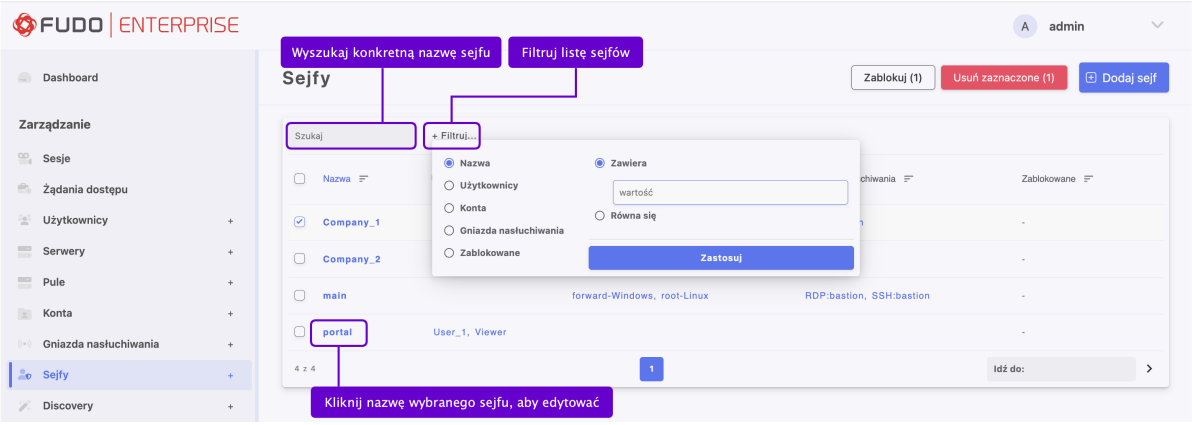
Tematy pokrewne:

- *Model danych*
- *Dodawanie sejfu*
- *Blokowanie sejfu*
- *Usuwanie sejfu*

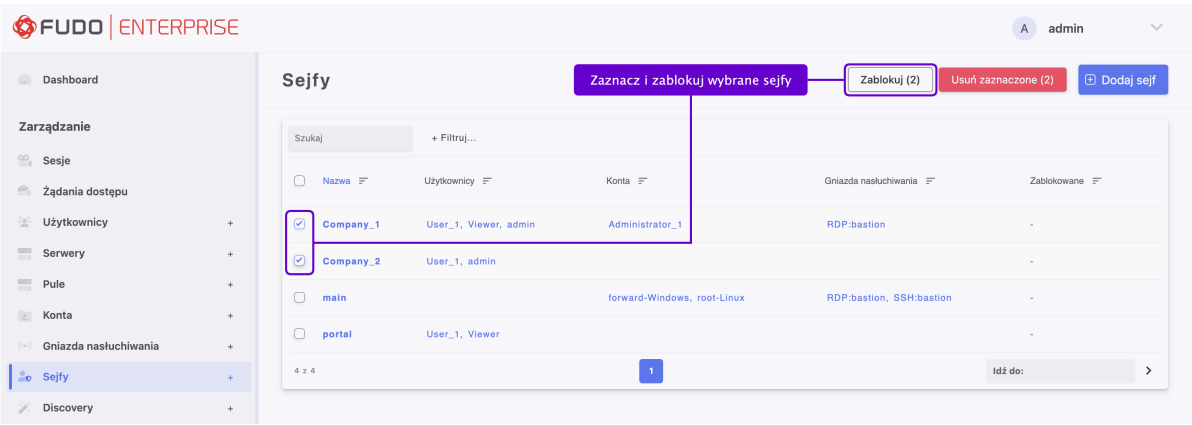
12.3 Blokowanie sejfu

Ostrzeżenie: Zablokowanie sejfu spowoduje zerwanie aktualnie trwających sesji połączeniowych, wykorzystujących konta przypisane wybranego obiektu.

1. Wybierz *Zarządzanie* > *Sejfy*.
2. Zdefiniuj filtry, aby ograniczyć liczbę wyświetlanych obiektów na liście, lub użyj paska wyszukiwania.



3. Wybierz jeden lub więcej sejfów do zablokowania, zaznaczając pole obok nazwy sejfu.
4. Kliknij przycisk *Blokuj*, aby zablokować wybrane sejfy.



5. Podaj opisowy powód zablokowania danego zasobu (wymagane) i kliknij *Potwierdź* w wyświetlonym oknie dialogowym.

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

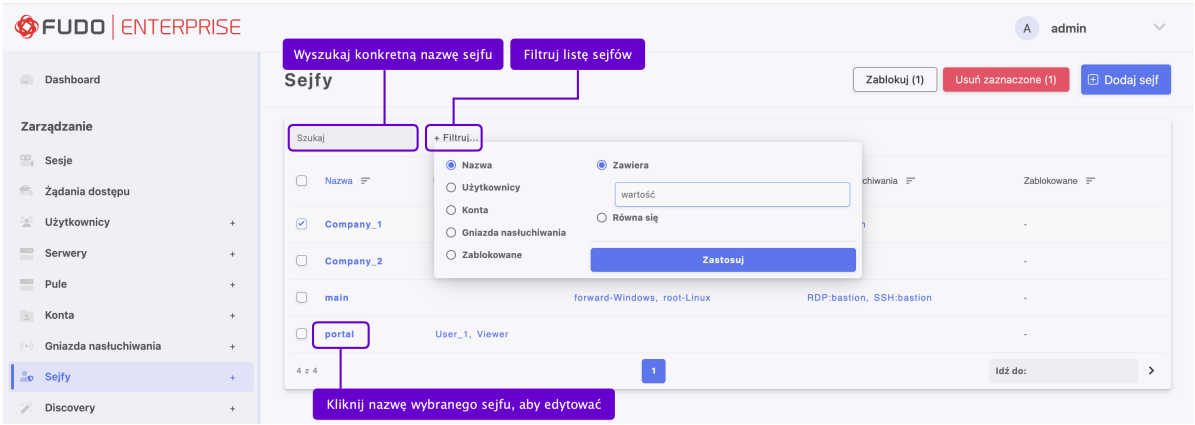
Tematy pokrewne:

- *Odblokowanie sejfu*
- *Model danych*

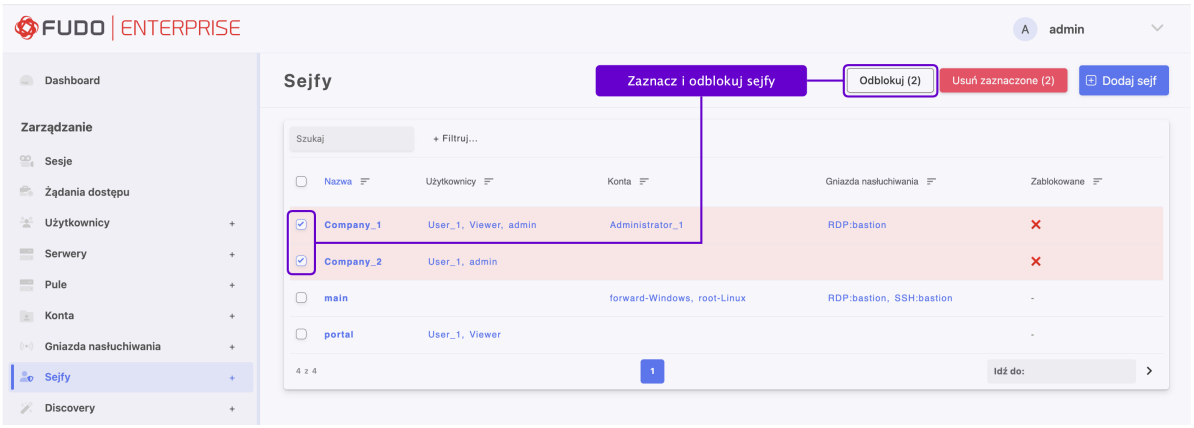
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*

12.4 Odblokowanie sejfu

1. Wybierz *Zarządzanie* > *Sejfy*.
2. Zdefiniuj filtry, aby ograniczyć liczbę obiektów wyświetlanych na liście, lub użyj paska wyszukiwania.



3. Wybierz jeden lub więcej sejfów do odblokowania, zaznaczając pole obok nazwy sejfu.
4. Kliknij przycisk *Odblokuj*, aby odblokować wybrane sejfy.



5. Kliknij *Potwierdź*, aby odblokować wybrane obiekty.

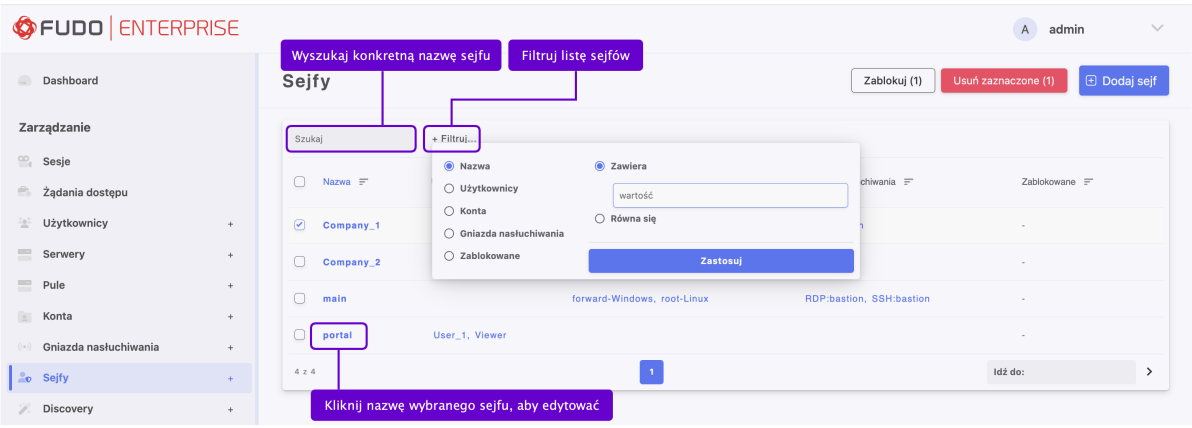
Tematy pokrewne:

- *Model danych*
- *Blokowanie sejfu*
- *Dodawanie sejfu*
- *Modyfikowanie sejfu*
- *Usuwanie sejfu*

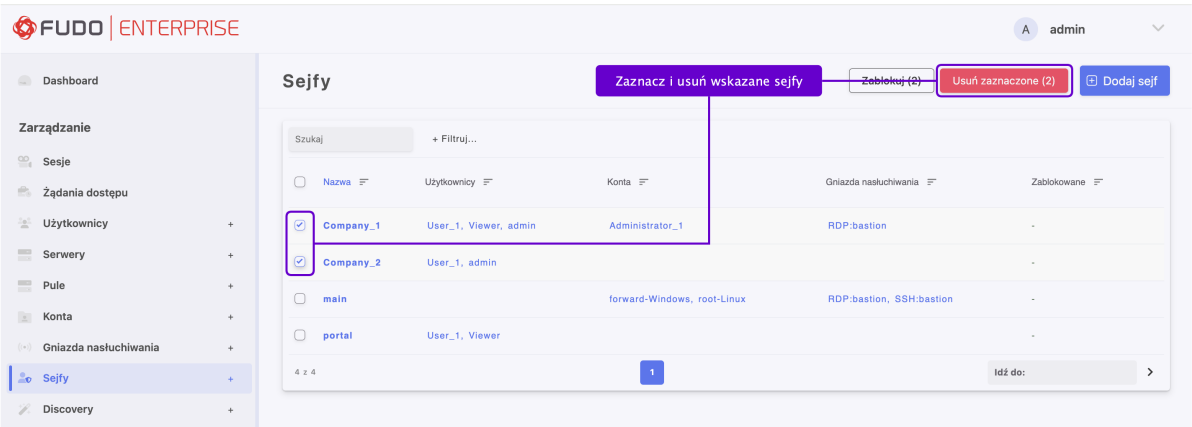
12.5 Usuwanie sejfu

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

1. Wybierz *Zarządzanie* > *Sejfy*.
2. Zdefiniuj filtry, aby ograniczyć liczbę obiektów wyświetlanych na liście lub użyj paska wyszukiwania.



3. Wybierz jeden lub więcej sejfów do usunięcia, zaznaczając pole obok nazwy sejfu.
4. Kliknij przycisk *Usuń wybrane*, aby usunąć wybrane sejfy.



5. Potwierdź usunięcie wybranych obiektów, wybierając przycisk *Potwierdź* w wyświetlonym oknie dialogowym.

Tematy pokrewne:

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

ROZDZIAŁ 13

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**.

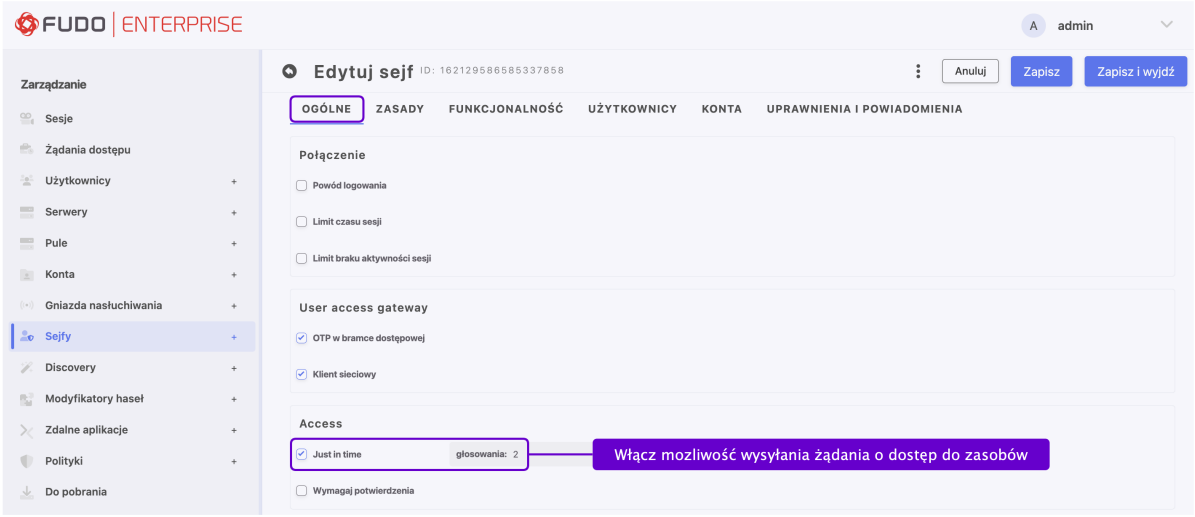
W przypadku wybrania **natychmiastowego** typu żądania, użytkownik może ustalić okres dostępu od zaraz do maksymalnie 24 godzin. Okres dostępu użytkownika zaczyna się w momencie zatwierdzenia żądania przez administratora - wtedy ma on 24 godziny na rozpoczęcie sesji. Kiedy użytkownik rozpoczyna sesję,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

1. Wybierz *Zarządzanie* > *Sejfy* i znajdź żądany sejf, bądź stwórz nowy.
2. W sekcji *Dostęp* zaznacz opcję *Just In Time*. 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.

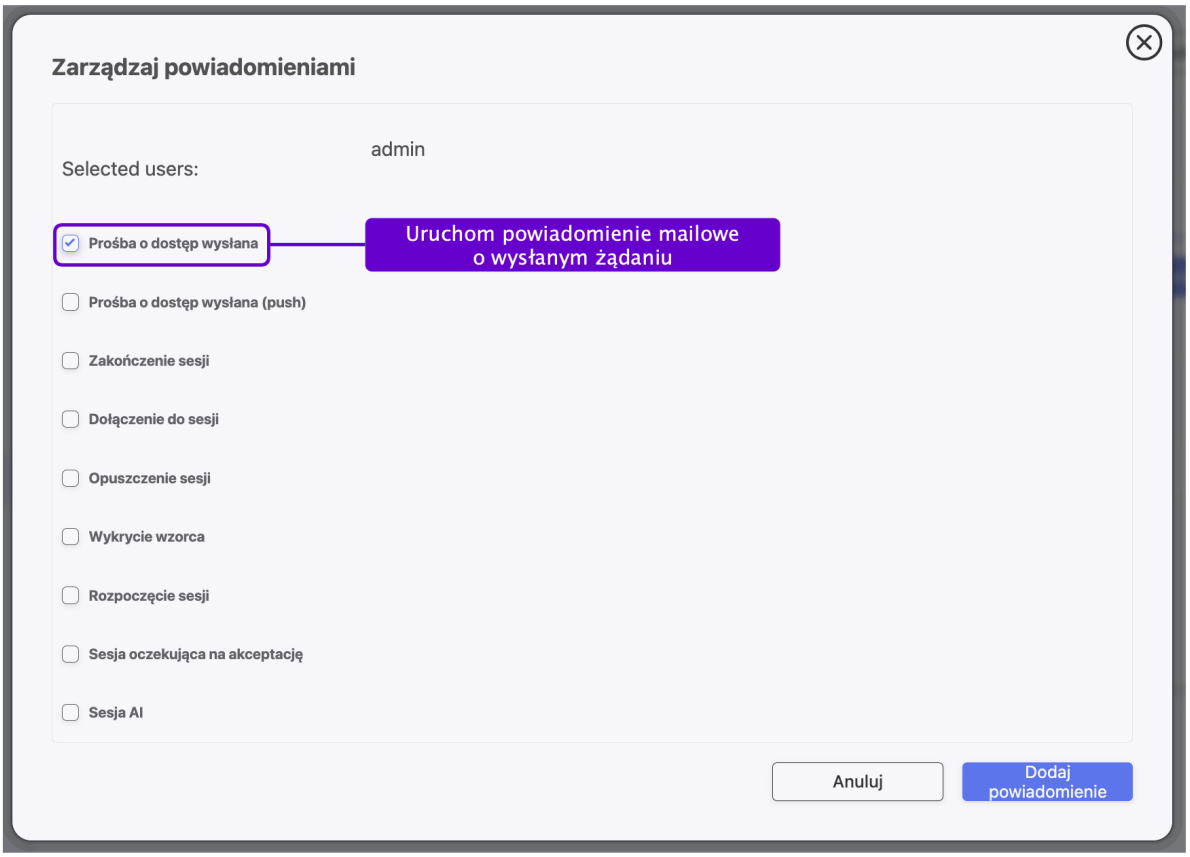
Użytkownik, który wysłał żądanie o dostęp nie może udzielać dostępu na swoje własne żądanie, więc wysłane przez niego żądania nie są dla niego widoczne.

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. Przejdź do zakładki *Uprawnienia i Powiadomienia*, wybierz konkretnego użytkownika i kliknij przycisk *Zarządzaj powiadomieniami*.
4. Wybierz typ powiadomienia *Wysłano żądanie dostępu* i kliknij *Dodaj powiadomienie*, aby zamknąć okno.

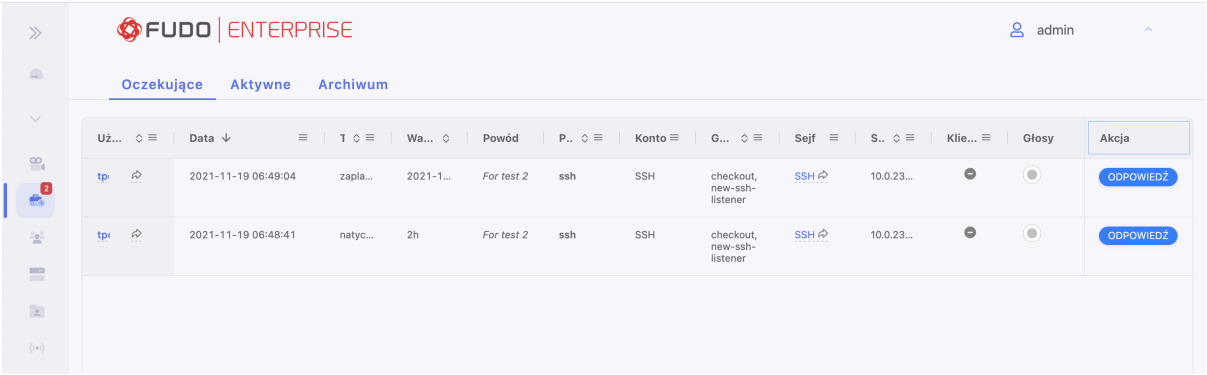
Informacja: Powiadomienia są ustawiane per węzeł - zgodnie z ustawieniami w zakładce *Powiadomienia*. W przypadku wybrania notyfikacji typu *Wysłano żądanie dostępu*, powiadomienie mailowe zostanie wysłane z tego węzła, z którego zostało wysłane żądanie. Więcej na temat wysłania notyfikacji znajdziesz pod linkiem *Powiadomienia*.



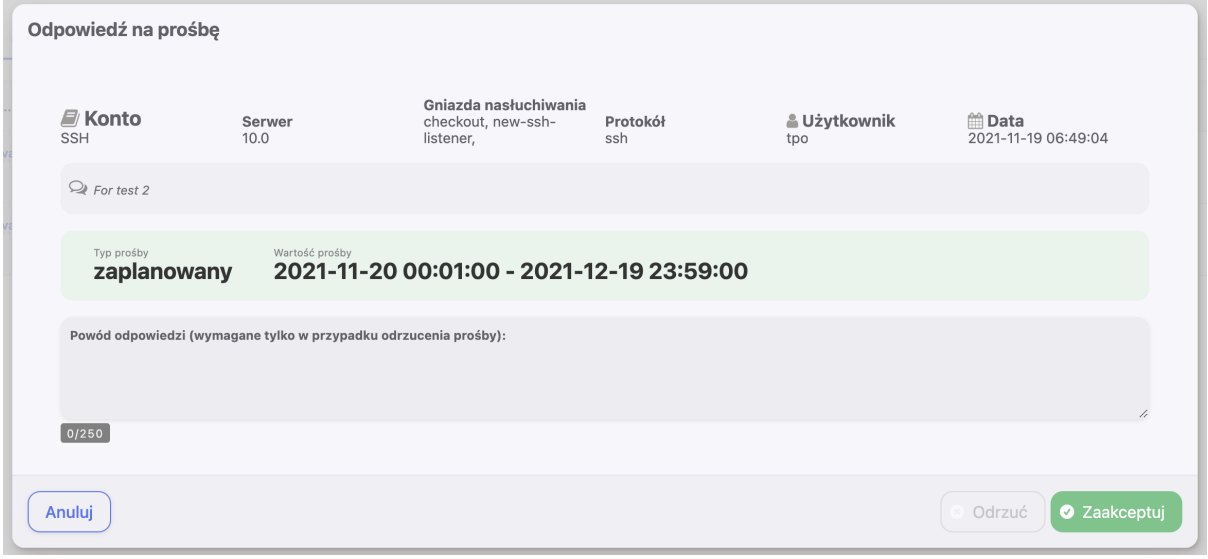
4. Kliknij *Zapisz*.

13.1 Żądania oczekujące

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



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

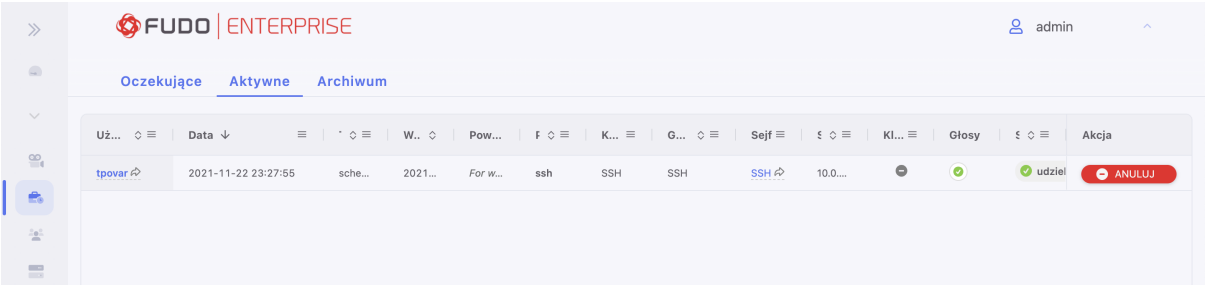


Informacja:

- Użytkownicy, którzy wysłali żądanie o dostęp oraz mają skonfigurowane adresy mailowe w Panelu Admina, dostaną powiadomienie, kiedy ich żądanie zostanie zaakceptowane bądź odrzucone.
- Jeśli użytkownik próbuje się połączyć do serwera (przykładowo, o protokole SSH) korzystając z opcji *klient natywny*, ale nie wysłał żądania o dostęp, stosowny komunikat o błędzie uwierzytelnienia będzie zapisany w Dzienniku zdarzeń: `Unable to authenticate user: safe requires acceptance`.

13.2 Żądania aktywne

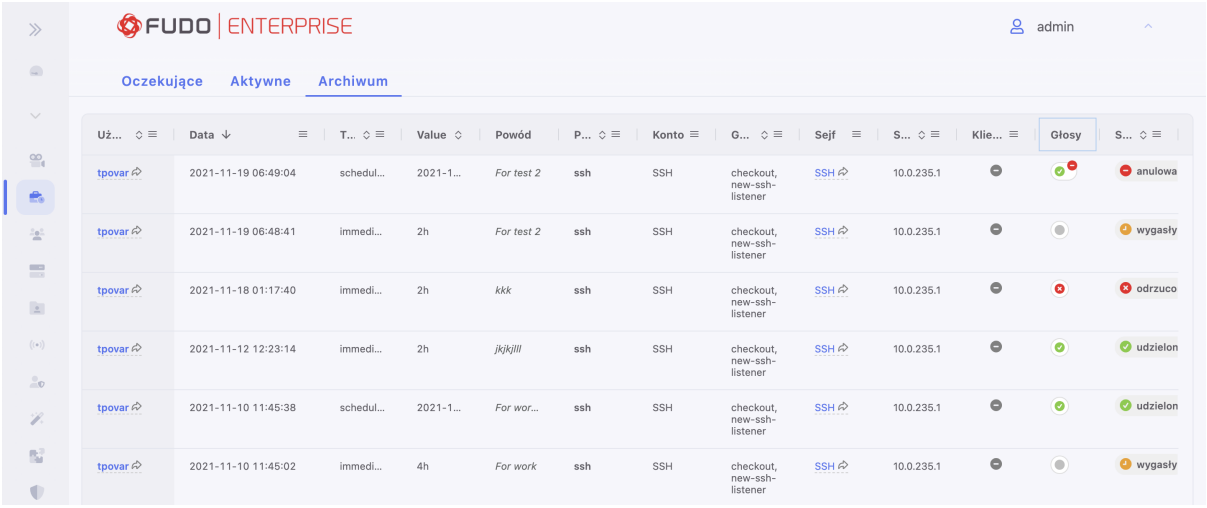
Pod zakładką *Aktywne* są widoczne dwa typy żądań: 1) te, które zostały zaakceptowane, i je sesje obecnie trwają, oraz 2) te, które dalej oczekują na część głosów. W kolumnie *Głosy* można sprawdzić aktualny stan żądania oraz ile głosów konkretne żądanie potrzebuje.



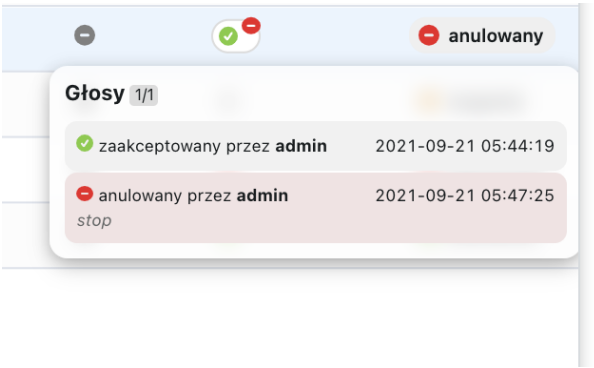
Stąd też można odwołać dostęp użytkownikowi poprzez wciśnięcie przycisku *Anuluj*, dostępnego dla żądań z już uznanym dostępem. Ta opcja też jest przydatna w sytuacji, kiedy użytkownik skończył pracę wcześniej - administrator może odwołać dostęp w celu uniknięcia nadużycia zasobów.

13.3 Archiwum żądań

Historia skompletowanych żądań jest widoczna w zakładce *Archiwum*.



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



Funkcjonalność **Just In Time** działa też w obrębie klastra połączonych instancji Fudo. Żądania oraz głosy są replikowane na poszczególnych węzłach klastra.

Informacja: W przypadku, gdy użytkownik zagłosował na kilku maszynach w obrębie klastra, i jego głosy były sprzeczne, system potraktuje żądanie jako odrzucone.

Tematy pokrewne:

- *Dodawanie sejfu*

ROZDZIAŁ 14

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.

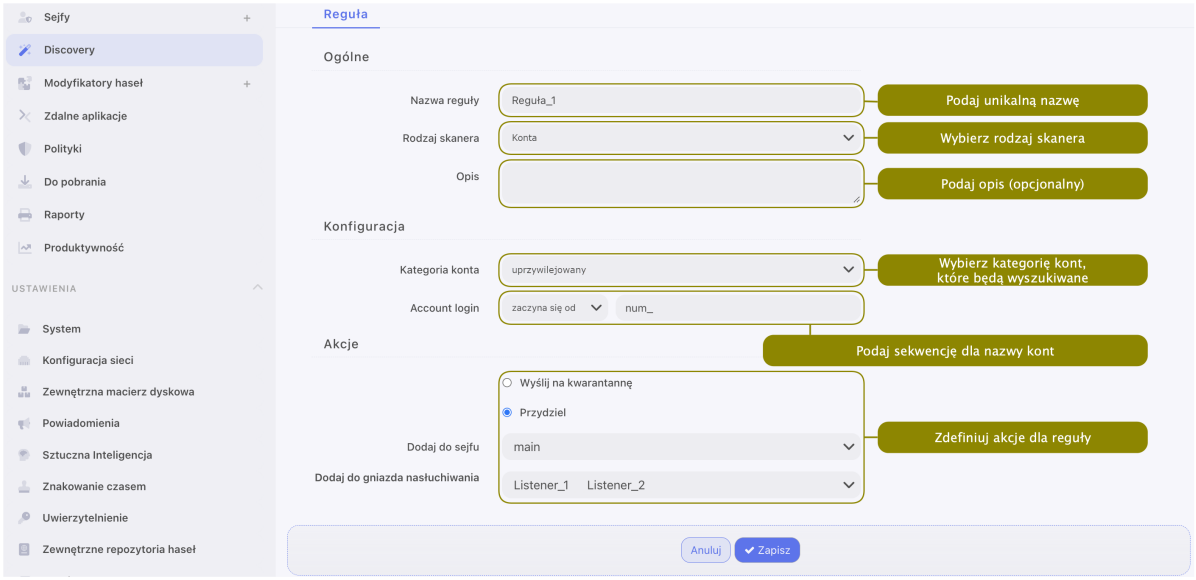
4. Z rozwijanej listy *Typ skanera* wybierz *Konta*.
5. Opcjonalnie, wprowadź opis reguły.
6. W sekcji *Konfiguracja*:

   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

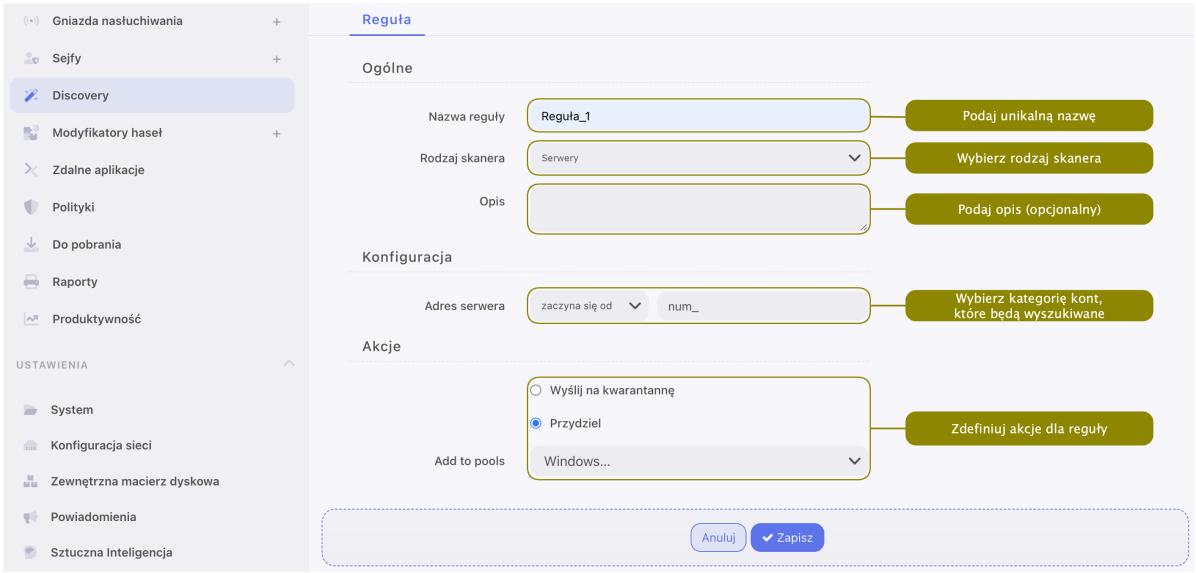
W celu stworzenia reguły postępuj zgodnie z poniższą instrukcją:

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

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 `zawiera`, `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.

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.

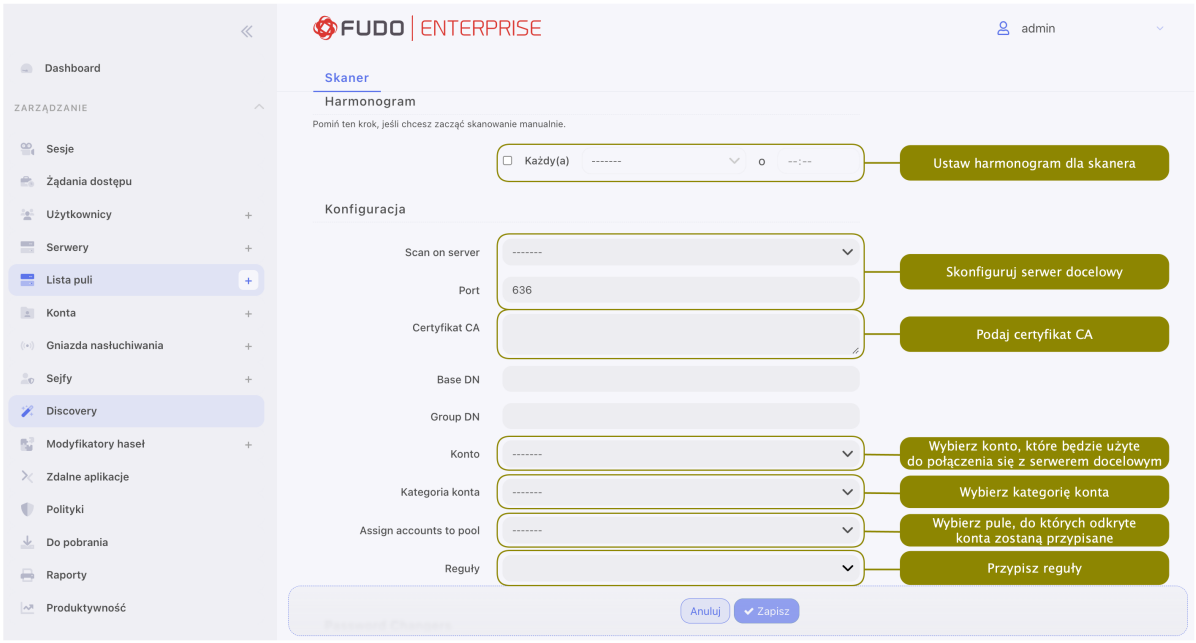
   7.7. Wybierz *Kategorię konta* (`uprzywilejowany`, `nieuprzywilejowany` lub `wszystko`).

   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`.

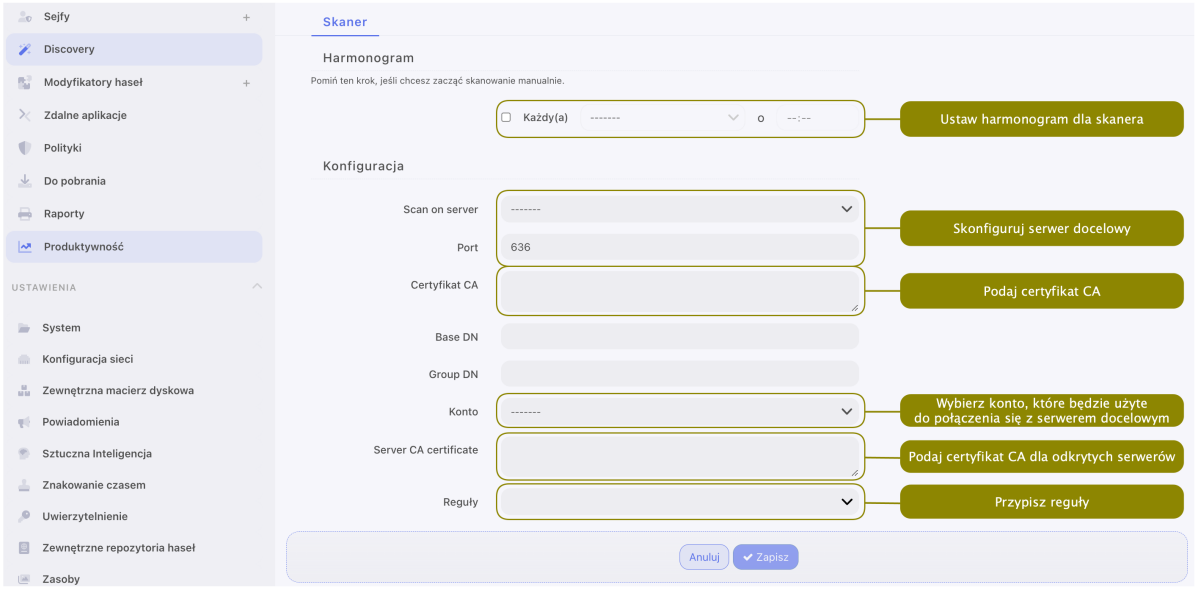
   7.5. Opcjonalnie podaj wartość *Group DN* wskazującą konkretną grupę w domenie. Użyj następującego formatu: `cn=##username##,dc=example,dc=com`.

   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 chcę 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.

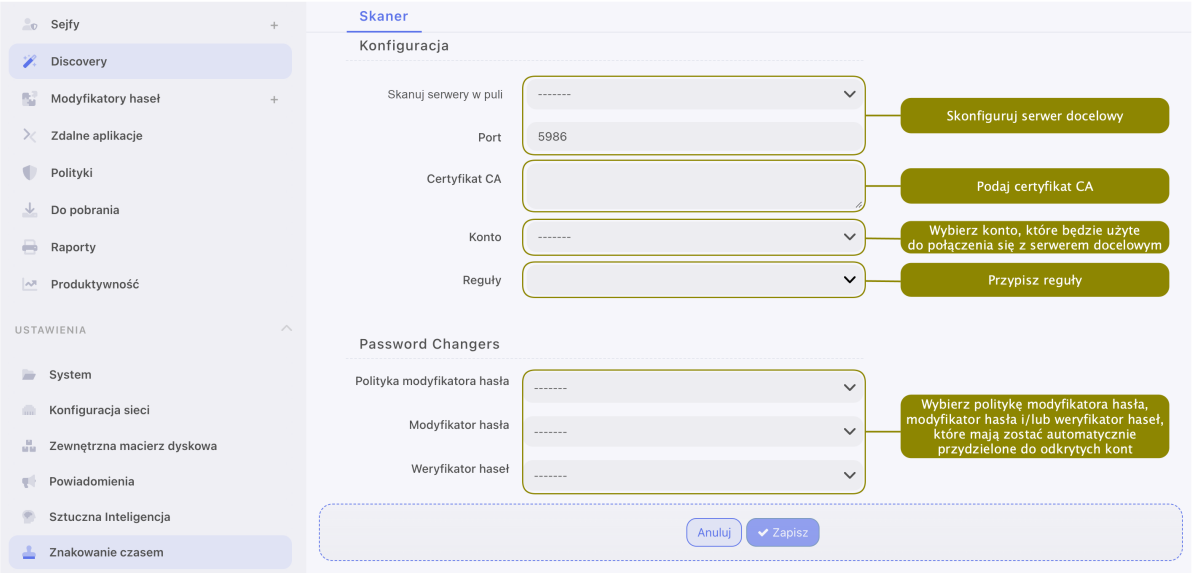
   Informacja: Do utworzenia jednego skanera do skanowania kont lokalnych na wielu serwerach, wymagane jest posiadanie na każdym ze skanowanych serwerów konta administratora z dokładnie tą samą metodą uwierzytelniania.

   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 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*

14.4 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.

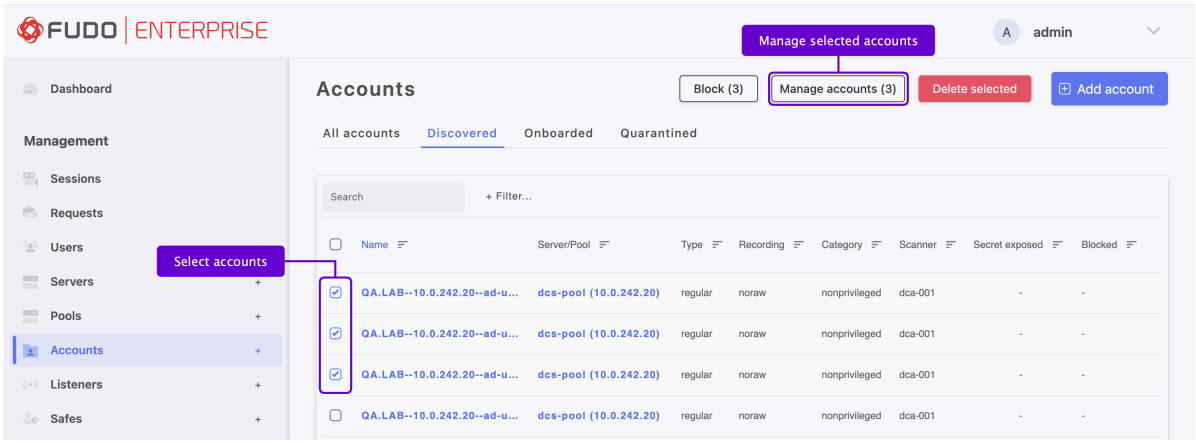
Można jednocześnie uruchomić lub usunąć kilka skanerów poprzez ich zaznaczenie i wybranie *Start* lub *Usuń*.

Tematy pokrewne:

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

14.5 Zarządzanie wykrytymi kontami

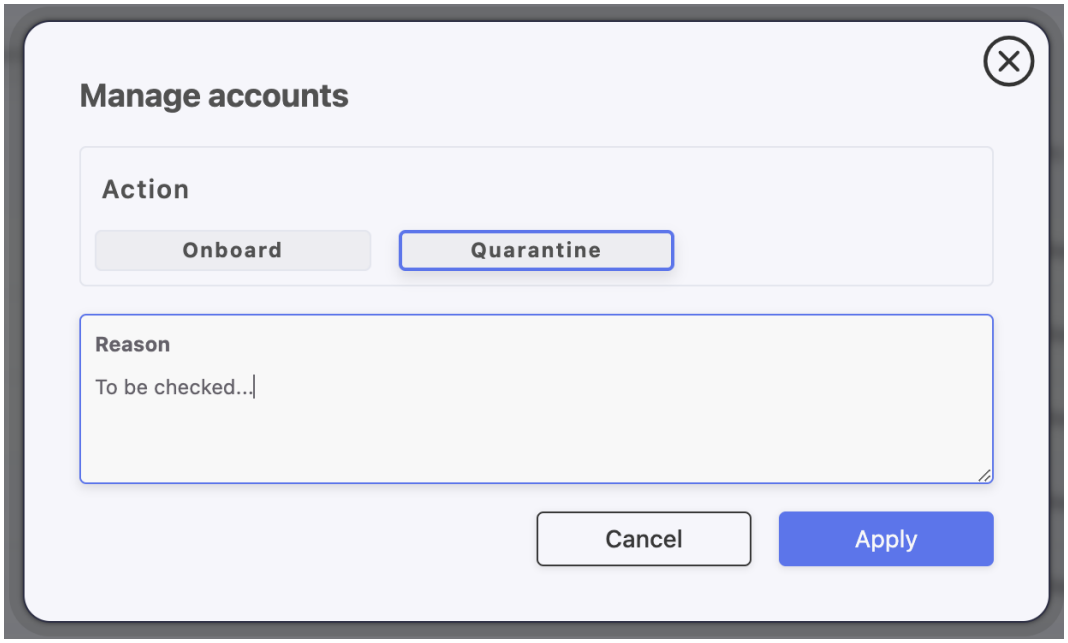
Konta *odkryte*, *przydzielone* oraz konta *pod kwarantanną* dostępne są w głównym widoku zakładki *Konta*.



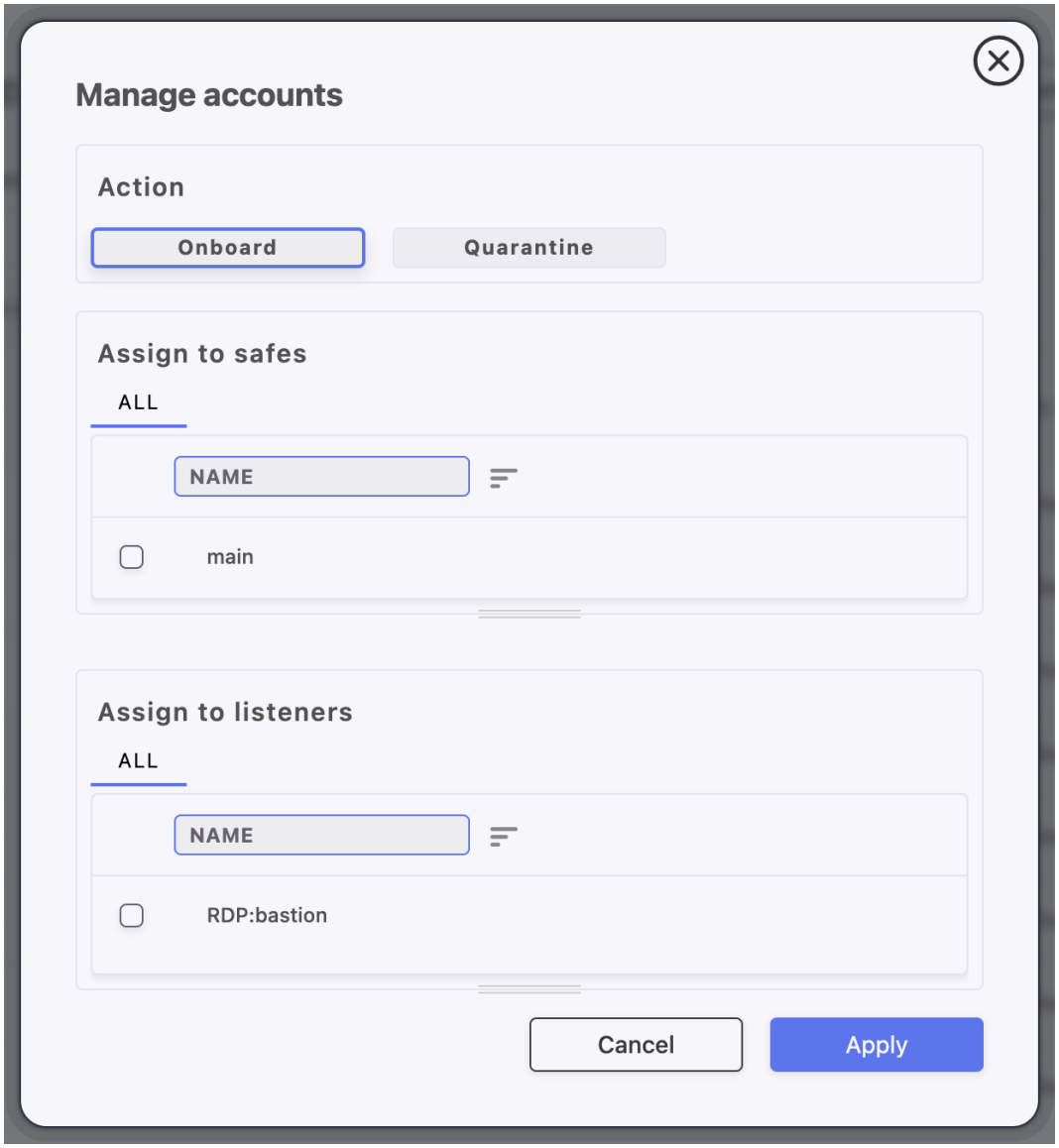
Informacja: Konta, które znajdą się w zakładce *Odkryte* zostały wykryte przez skaner, lecz nie zostały ani przydzielone, ani wysłane na kwarantannę. Jest to zazwyczaj spowodowane brakiem ustawienia automatycznej reguły. Administrator może je przydzielić lub wysłać na kwarantannę manualnie, korzystając 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** (wymagany 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*

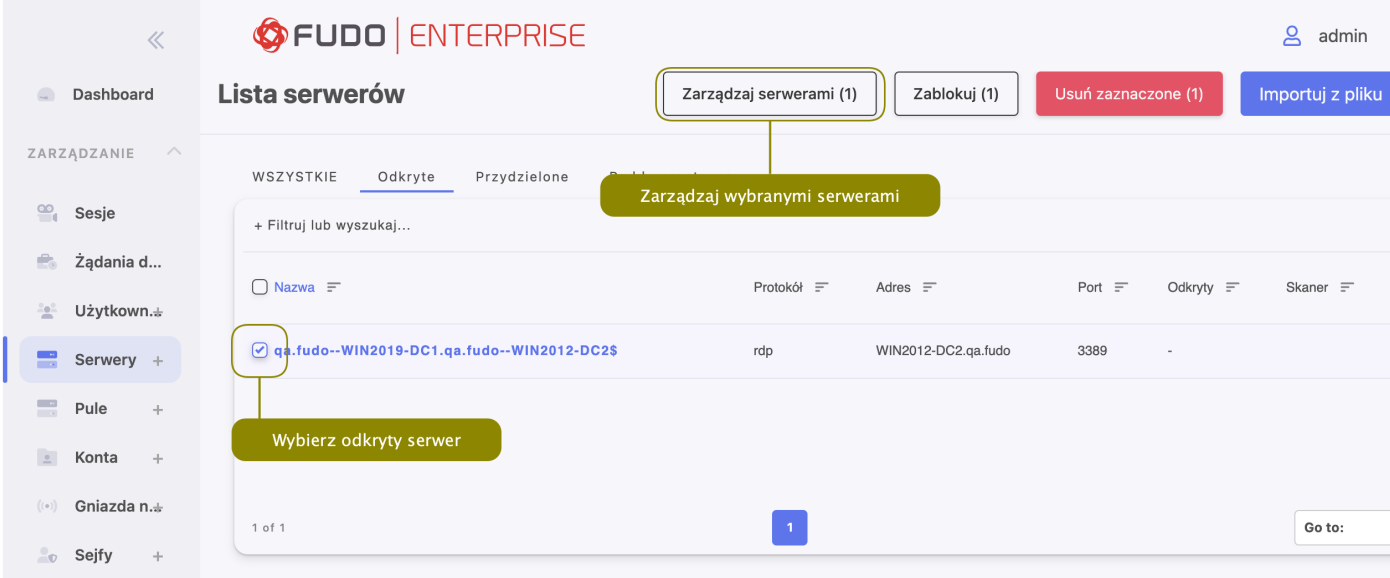
14.6 Zarządzanie wykrytymi serwerami

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

Informacja: Serwery, które znajdą 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.

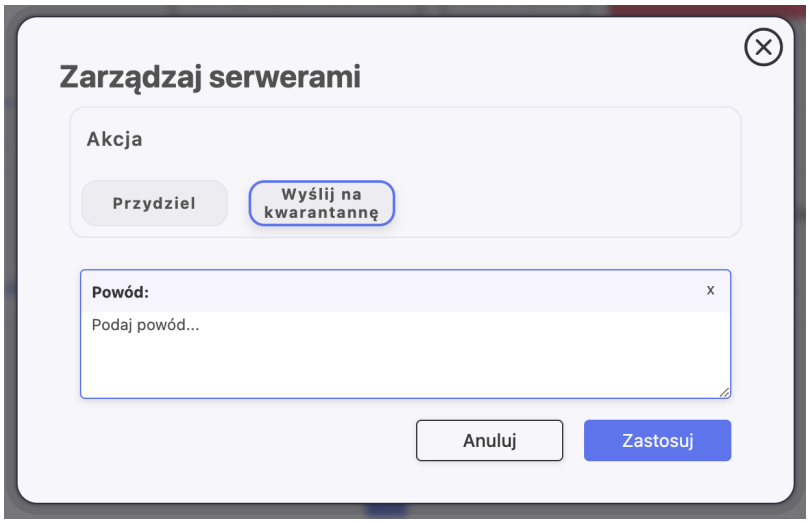
1. Wybierz *Zarządzanie* > *Serwery* > *Odkryte*
2. Zaznacz serwery, które chcesz przydzielić albo wysłać na kwarantannę.
3. Wybierz opcję *Zarządzaj serwerami*.



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*

ROZDZIAŁ 15

Modyfikatory haseł

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*.

Wbydowane modyfikatory haseł obejmują następujące scenariusze:

- Unix poprzez SSH
- MySQL na serwerze Unix poprzez SSH
- Cisco poprzez SSH i Telnet
- Cisco Enable Password poprzez SSH i Telnet
- WinRM
- LDAP

15.1 Polityki haseł

Polityka zmiany haseł określa, jak często hasło powinno być zmieniane oraz wymagania dotyczące złożoności hasła.

15.1.1 Dodawanie polityki zmiany haseł

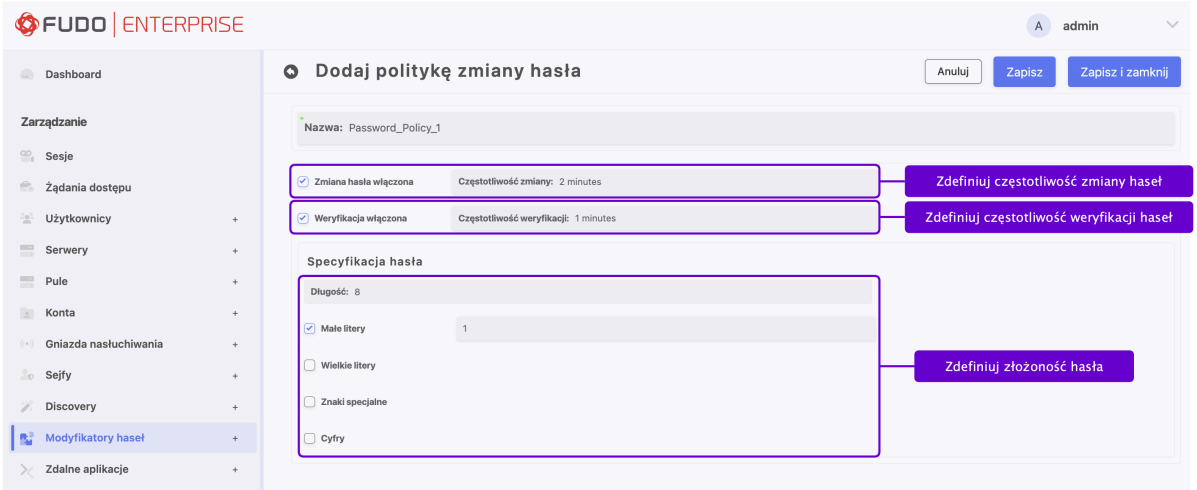
1. Wybierz *Zarządzanie* > *Modyfikatory haseł*.
2. Przejdź do zakładki *Polityki haseł*.
3. Kliknij + *Dodaj politykę haseł*.
4. Wprowadź nazwę obiektu.
5. Wybierz opcję *Zmiana hasła włączona* i określ przedział czasu między każdą zmianą hasła.

6. Wybierz opcję *Weryfikacja włączona* i określ przedział czasu między każdą weryfikacją hasła.
7. Zdefiniuj złożoność hasła.

Parametr	Opis
Długość	Podaj liczbę znaków składających się na hasło.
Małe litery	Wybierz, aby uwzględnić małe litery, zdefiniuj ich minimalną liczbę.
Wielkie litery	Wybierz, aby uwzględnić wielkie litery, zdefiniuj ich minimalną liczbę.
Znaki specjalne	Wybierz, aby uwzględnić znaki specjalne, zdefiniuj ich minimalną liczbę.
Cyfry	Wybierz, aby uwzględnić cyfry, zdefiniuj ich minimalną liczbę.

Informacja: Suma wymagań dotyczących hasła nie może być większa niż określona długość hasła.

7. Kliknij *Zapisz*.



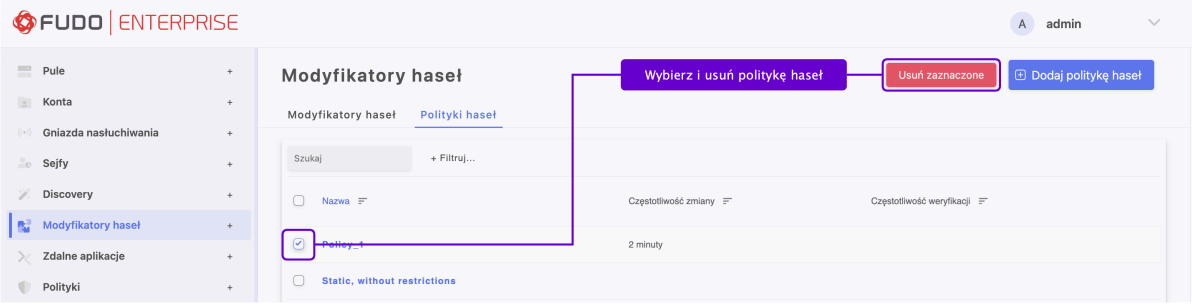
15.1.2 Edycja polityki zmiany haseł

1. Wybierz *Zarządzanie* > *Modyfikatory haseł* > *Polityki haseł*.
2. Przejdź do zakładki *Polityki haseł*.
3. Znajdź i kliknij żądany obiekt, aby otworzyć jego stronę konfiguracyjną.
4. Zmodyfikuj parametry konfiguracji według potrzeb.
4. Kliknij *Zapisz*.

15.1.3 Usuwanie polityki zmiany haseł

1. Wybierz *Zarządzanie* > *Modyfikatory haseł*.

2. Przejdź do zakładki *Polityki haseł*.
3. Znajdź i wybierz żądane obiekty.
4. Kliknij *Usuń*.
5. Kliknij *Potwierdź*, aby potwierdzić usunięcie wybranych obiektów.



Tematy pokrewne:

- *Model danych*
- *Konta*
- *Uniwersalne modyfikatory haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

15.2 Uniwersalne modyfikatory haseł

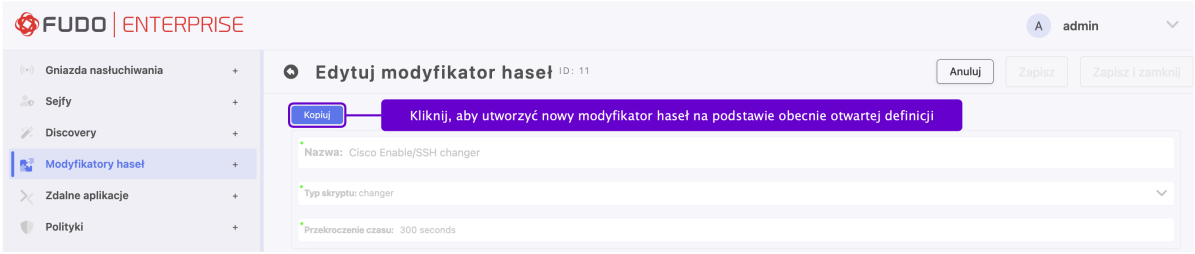
Uniwersalne modyfikatory haseł umożliwiają zdefiniowanie sekwencji komend, które zostaną wykonane na zdalnej maszynie w celu zmiany hasła.

Informacja: W konfiguracji klastra, węzeł odpowiedzialny za zmianę haseł na monitorowanych systemach jest konfigurowany w ustawieniach systemu. Więcej informacji można znaleźć w temacie *Modyfikatory haseł - aktywny węzeł klastra*.

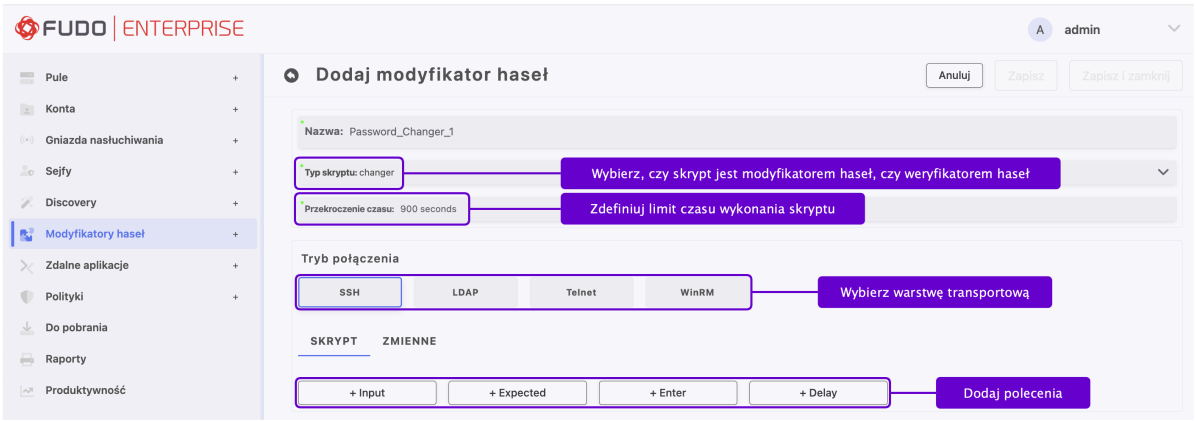
15.2.1 Definiowanie modyfikatora haseł

1. Kliknij ikonę + w głównym menu obok zakładki *Modyfikatory haseł*, lub
2. Wybierz *Zarządzanie* > *Modyfikatory haseł* i kliknij + *Dodaj modyfikator haseł*.

Informacja: Alternatywnie, możesz edytować istniejący modyfikator haseł i kliknąć *Kopiuj*, aby utworzyć nowy modyfikator haseł na podstawie aktualnie otwartej definicji.



3. Zdefiniuj nazwę modyfikatora haseł.
4. Z listy rozwijanej *Typ skryptu* wybierz, czy skrypt jest modyfikatorem haseł, czy weryfikatorem haseł.
5. W polu *Limit czasu* zdefiniuj limit czasu wykonywania skryptu.
6. W sekcji *Tryb połączenia* kliknij *SSH*, *LDAP*, *Telnet* lub *WinRM*, aby wybrać warstwę transportową.
7. W zakładce *SKRYPT* kliknij jedną z dostępnych opcji, aby dodać polecenie.



Informacja: Dostępne polecenia zależą od wybranej warstwy transportowej. Więcej informacji na temat trybów połączenia można znaleźć w temacie *Tryby połączenia*.

- `+Input` - komenda wykonywana po stronie serwera.
- `+Expected` - oczekiwany rezultat wykonania komendy.
- `+Enter`
- `+Delay` - opóźnienie między wykonywaniem poleceń.
- `DN` - parametr DN (Distinguished Name) usługi katalogowej.
- `Filter` - filtr użytkownika w usłudze katalogowej.

Ostrzeżenie: Aby skonfigurować modyfikatory haseł **WinRM**, musisz podać dane uwierzytelniające użytkownika z uprawnieniami do zmiany haseł (zwykle konto na poziomie administratora). Ważne jest jednak, aby nie używać tego konta do zmiany jego własnego hasła,

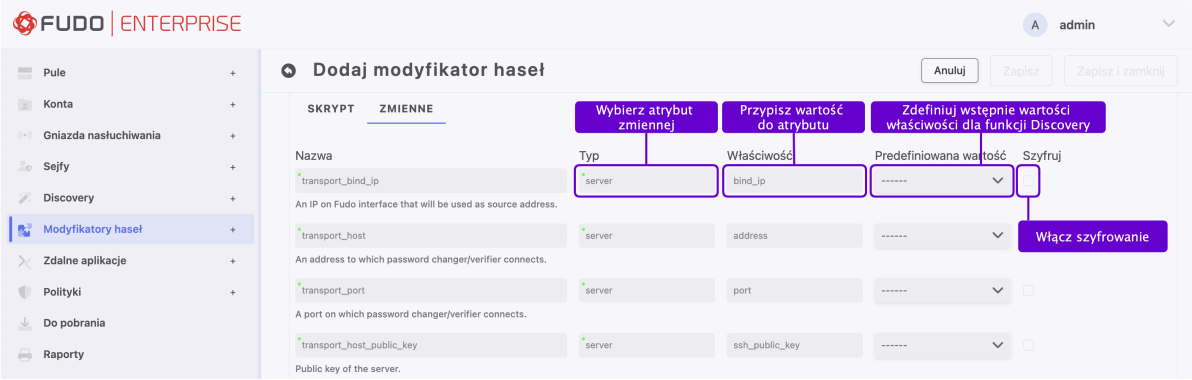
ponieważ WinRM zwróci błąd, którego Fudo Enterprise nie może obsłużyć. **Upewnij się, że zmienne ‘‘account_login‘‘ i ‘‘transport_login‘‘ mają różne wartości.**

8. Wprowadź polecenie lub zdefiniuj parametry działania.

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%%`.

---

9. Powtórz kroki 7-8, aby dodać kolejne polecenia.
10. W zakładce *Zmienne* zdefiniuj atrybuty zmiennych występujących w skrypcie.



Informacja:

- Zmienne mogą być inicjowane wartościami odwołującymi się do innych obiektów lub mogą mieć przypisaną stałą wartość.
- Dzięki predefiniowanym wartościom modyfikator haseł przypisany do konta podczas procesu *Wykrywanie (Discovery)* nie wymaga żadnej dodatkowej konfiguracji.

---

10. Kliknij *Zapisz*.
11. *Zdefiniuj politykę zmiany haseł* i *przypisz modyfikator haseł do konta*.

Informacja: Przykład

W tym przykładzie modyfikatora haseł, zmiana hasła jest uruchamiana poleceniem `passwd` wykonywanym z uprawnieniami *sudo* na hoście z systemem operacyjnym FreeBSD.

Lista poleceń

	Akcja	Treść	Komentarz
1	EXPECTED	`Password`	Spodziewany wyraz «Password» w treści konsoli.
2	INPUT	`%%transport_secret%%`	Zmienna `transport_secret` reprezentuje sekret uwierzytelniający konto, uprawnione do zmiany hasła.
3	EXPECTED	`\[john@john-laptop.*\]`	Spodziewana treść odpowiadająca wyrażeniu regularnemu przedstawiona na konsoli.
4	INPUT	`sudo passwd %%account_login%%`	Komenda zmiany hasła na koncie; zmienna `account_login` reprezentuje login użytkownika, któremu jest zmieniane hasło.
5	EXPECTED	`Password`	Spodziewany wyraz «Password» w treści konsoli.
6	INPUT	`%%transport_secret%%`	Zmienna `transport_secret` reprezentuje sekret uwierzytelniający konto, uprawnione do zmiany hasła.
7	EXPECTED	`Changing local password`	Spodziewany wyraz «Changing local password» w treści konsoli.
8	EXPECTED	`New Password`	Spodziewany wyraz «New Password» w treści konsoli.
9	INPUT	`%%account_new_secret%%`	Nowe hasło
10	EXPECTED	`Retype New Password`	Spodziewany wyraz «Retype New Password» w treści konsoli.
11	INPUT	`%%account_new_secret%%`	Nowe hasło
12	INPUT	`echo $?`	
13	EXPECTED	`0`	

Zmienne

Nazwa zmiennej	Rodzaj obiektu	Atrybut	Zaszyfruj
transport_method	constant		✗
transport_bind_to	server_property	bind_ip	✗
transport_user	account	login	✗
transport_host	server_address_property	host	✗
transport_port	server_property	port	✗
transport_secret	account	secret	✓
transport_host_public_key	constant		✗
account_login	account	login	✗

15.2.2 Edycja modyfikatora haseł

1. Wybierz *Zarządzanie* > *Modyfikatory haseł*.
2. Kliknij nazwę żądanego modyfikatora haseł.

3. W zakładce *Skrypt* edytuj wybrane polecenia.
4. Kliknij *Usuń*, aby usunąć wybrane polecenie.
5. Kliknij *Zapisz*.

15.2.3 Usuwanie modyfikatora haseł

1. Wybierz *Zarządzanie* > *Modyfikatory haseł*.
2. Wybierz modyfikator haseł i kliknij *Usuń*.
3. Potwierdź usunięcie wybranych obiektów.

Tematy pokrewne:

- *Modyfikatory haseł - aktywny węzeł klastra*
- *Tryby połączenia*
- *Konta*
- *Polityki haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

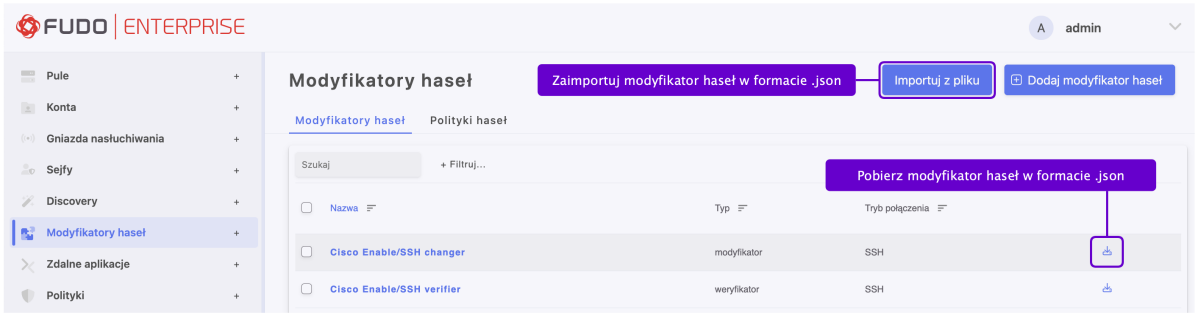
15.3 Importowanie i eksportowanie modyfikatorów haseł

Modyfikatory haseł utworzone w Fudo Enterprise mogą być pobrane i zaimportowane do innej instancji Fudo Enterprise.

15.3.1 Eksportowanie modyfikatora haseł

Aby pobrać wybrany modyfikator haseł:

1. Wybierz *Zarządzanie* > *Modyfikatory haseł*.
2. Przejdź do zakładki *Modyfikatory haseł*.
3. Kliknij ikonę pobierania obok wybranego modyfikatora haseł, aby go pobrać.



15.3.2 Importowanie modyfikatora haseł

Aby zaimportować plik `.json` modyfikatora haseł:

1. Wybierz *Zarządzanie* > *Modyfikatory haseł*.
2. Przejdź do zakładki *Modyfikatory haseł*.
3. Kliknij przycisk *Importuj z pliku*.
4. Przeciągnij i upuść plik do okna importu lub przeszukaj system plików, aby zlokalizować wybrany plik `.json` modyfikatora haseł.
5. Kliknij *Wyślij dane*, aby zaimportować plik, lub *Wyczyść dane*, aby przerwać import.

Tematy pokrewne:

- *Model danych*
- *Konta*
- *Uniwersalne modyfikatory haseł*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

15.4 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.

15.4.1 SSH

Tryb połączenia SSH używa protokołu SSH w celu nawiązania połączenia ze zdalnym systemem.

Komendy

Komenda	Opis
INPUT	Komenda wykonana na zdalnym systemie.
EXPECTED	Oczekiwany rezultat wykonania komendy.
ENTER	
DELAY	Opóźnienie pomiędzy wykonanywanymi komendami.

Zmienne

Zmienna	Opis
transport_bind_ip	Adres IP używany przez Fudo przy komunikacji ze zdalnym systemem.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_host_public_key	Klucz publiczny zdalnego systemu.
transport_login	Nazwa konta na systemie docelowym, uprawnionego do zmiany hasła.
transport_method	Metoda uwierzytelnienia konta uprawnionego do zmiany hasła. Dopuszczalne wartości: `password` or `sshkey`.
transport_password_prompt	Wyrażenie regularne opisujące zapytanie systemowe o podanie hasła. **Informacja:** W przypadku zdefiniowania parametru jako wartość stałą, nie uzupełnienie wartości zmiennej po przypisaniu modyfikatora hasła do konta, poskutkuje przyjęciem domyślnej postaci wyrażenia.
transport_port	Numer portu, służący do nawiązania połączenia z systemem docelowym.
transport_secret	Sekret służący do uwierzytelnienia konta wykorzystywanego w procesie zmiany hasła.
account_login	Login użytkownika, któremu jest zmieniane hasło.
account_new_secret	Zmienna systemowa, inicjowana wartością automatycznie wygenerowaną przez Fudo.

15.4.2 LDAP

Warstwa transportowa LDAP wykonuje zapytanie LDAP do zmiany hasła obiektu zdefiniowanego w usłudze katalogowej.

Komendy

Komenda	Opis
DN	Parametr DN (Distinguished Name) usługi katalogowej.
FILTER	Filtr użytkowników usługi katalogowej.

Informacja: Modyfikatory haseł oparte o warstwę transportową LDAP, mogą mieć zdefinowaną tylko jedną komendę.

Zmienne

Zmienna	Opis
transport_base	Parametr *base DN* usługi katalogowej.
transport_bind_ip	Adres IP Fudo, wykorzystywany do nawiązania połączenia z systemem docelowym.
transport_ca_certificate	Certyfikat CA systemu docelowego.
transport_domain	Domena służąca do logowania do systemu docelowego.
transport_encoding	Kodowanie tekstu na systemie docelowym.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_login	Nazwa konta na systemie docelowym, uprawnionego do zmiany hasła.
transport_port	Numer portu, służący do nawiązania połączenia z systemem docelowym.
transport_secret	Sekret służący do uwierzytelnienia konta wykorzystywanego w procesie zmiany hasła.
transport_server_certificate	Certyfikat serwera docelowego.
account_domain	Domena użytkownika, któremu jest zmieniane hasło.
account_new_secret	Zmienna systemowa, inicjowana wartością automatycznie wygenerowaną przez Fudo.

15.4.3 Telnet

Tryb połączenia Telnet, wykorzystuje protokół *Telnet* w celu nawiązania połączenia ze zdalnym systemem w celu zmiany hasła.

Komendy

Komenda	Opis
INPUT	Komenda wykonana na zdalnym systemie.
EXPECTED	Oczekiwany rezultat wykonania komendy.
ENTER	
DELAY	Opóźnienie pomiędzy wykonanywanymi komendami.

Zmienne

Zmienna	Opis
transport_bind_ip	Adres IP używany przez Fudo przy komunikacji ze zdalnym systemem.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_login	Nazwa konta na systemie docelowym, uprawnionego do zmiany hasła.
transport_port	Numer portu, służący do nawiązania połączenia z systemem docelowym.
transport_secret	Sekret służący do uwierzytelnienia konta wykorzystywanego w procesie zmiany hasła.
account_login	Login użytkownika, któremu jest zmieniane hasło.
account_new_secret	Zmienna systemowa, inicjowana wartością automatycznie wygenerowaną przez Fudo.

15.4.4 WinRM

Warstwa transportowa WinRM wykorzystuje protokół Windows Remote Management w celu nawiązania połączenia ze zdalnym systemem. Warstwa transportowa WinRM jest kompatybilna z Listą unieważnionych certyfikatów (listą CRL), co powoduje, że używane certyfikaty są potwierdzone i ważne.

Informacja: Domyślnie, Modyfikator oraz Weryfikator haseł na bazie warstwy transportowej WinRM, działają tylko dla użytkowników *lokalnych*. W celu konfiguracji Modyfikatora oraz Weryfikatora haseł WinRM dla użytkowników *domenowych*, należy dodać ich do grupy "Allow log on locally".

Komendy

Komenda	Opis
INPUT	Komenda wykonana na zdalnym systemie.
EXPECTED	Oczekiwany rezultat wykonania komendy.
ENTER	
DELAY	Opóźnienie pomiędzy wykonanywanymi komendami.

Zmienne

Ostrzeżenie: Aby skonfigurować modyfikator haseł **WinRM**, musisz podać dane uwierzytelniające użytkownika z uprawnieniami do zmiany haseł (zwykle konto na poziomie administratora). Nie należy używać tego konta do zmiany własnego hasła, ponieważ WinRM zwróci błąd, którego Fudo Enterprise nie może obsłużyć. **Upewnij się, że zmienne account_login i transport_login mają różne wartości.**

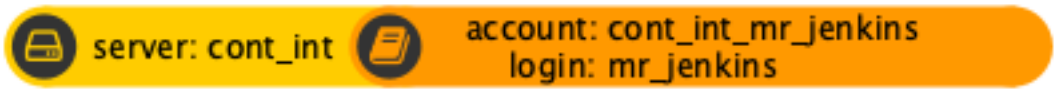
Zmienna	Opis
transport_bind_ip	Adres IP używany przez Fudo przy komunikacji ze zdalnym systemem.
transport_ca_certificate	Certyfikat CA systemu docelowego.
transport_encoding	Kodowanie tekstu na systemie docelowym.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_login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

Tematy pokrewne:

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

15.5 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.

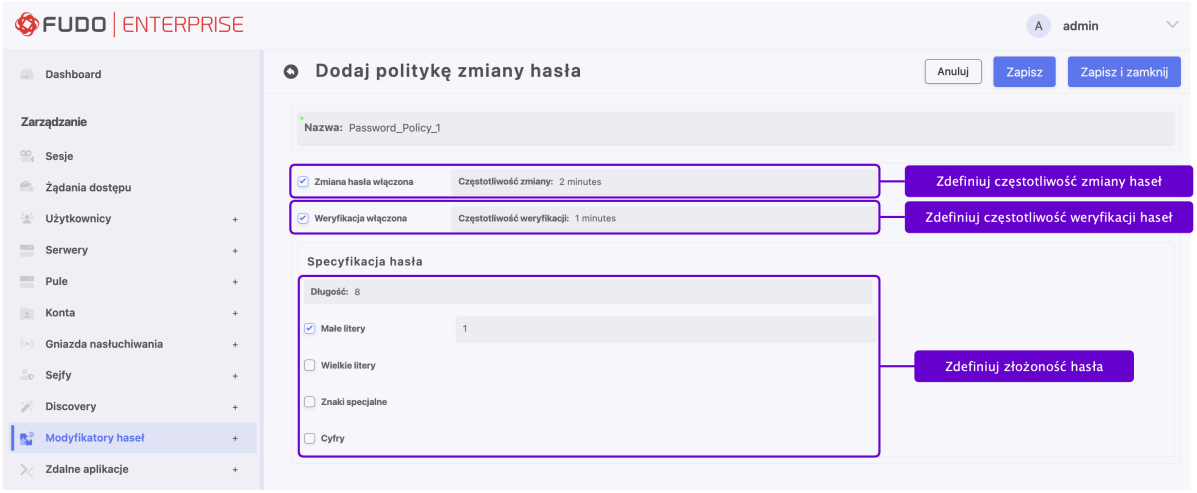
Dodawanie polityki zmiany hasła

1. Wybierz *Zarządzanie* > *Modyfikatory haseł*.
2. Przejdź do zakładki *Polityki haseł*.
3. Kliknij + *Dodaj politykę haseł*, aby utworzyć nową politykę zmiany hasła.
4. Podaj nazwę polityki zmiany hasła.

Informacja: Opisowa nazwa pozwoli administratorom Fudo Enterprise szybko zorientować się, co dana polityka robi. Np. `10 minut, 20 znaków, znaki specjalne, wielkie litery`.

---

5. Wybierz opcję *Zmiana hasła włączona* i zdefiniuj, jak często hasło będzie zmieniane.
6. Wybierz opcję *Weryfikacja hasła włączona* i zdefiniuj, jak często menedżer powinien weryfikować, czy hasło nie zostało zmienione w inny sposób niż przez niego.
7. Podaj liczbę znaków składających się na hasło.
8. Wybierz pożądane opcje złożoności hasła i podaj minimalną liczbę znaków dla każdej z nich.



9. Kliknij *Zapisz*, aby zapisać politykę zmiany hasła.

Przypisywanie modyfikatora i weryfikatora do konta uprzywilejowanego

1. Wybierz *Zarządzanie* > *Konta*.
2. Znajdź i kliknij wybrane konto, aby je edytować.
3. Przejdź do zakładki *MODYFIKATORY HASEŁ*.

Informacja: Do skonfigurowania modyfikatorów haseł wymagane są: typ konta regular, metoda *hasło* oraz login.

---

4. W polu *Modyfikator hasła* wybierz skrypt `Unix/SSH changer` z listy rozwijanej *Dodaj modyfikator*.
5. W oknie *Modyfikator hasła*, w polu *Limit czasu*, zdefiniuj limit czasu wykonywania skryptu.
6. Przejrzyj i zmodyfikuj domyślne wartości.

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	`stały`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`
account_login	`cont_int_mr_jenkins: mr_jenkins`

7. Kliknij *Zapisz*, aby zamknąć okno *Modyfikatory haseł*.

Informacja:

- Zmienne rozpoczynające się od `transport_` to zmienne warstwy transportowej określające parametry połączenia z serwerem docelowym.

- Zmiennym można przypisać wartości ręcznie lub zainicjować je właściwościami innych obiektów.

8. W polu *Weryfikator hasła* wybierz skrypt `Unix/SSH verifier` z listy rozwijanej *Dodaj weryfikator*.
9. W oknie *Weryfikator hasła*, w polu *Limit czasu*, zdefiniuj limit czasu wykonywania skryptu.
10. Przejrzyj i zmodyfikuj domyślne wartości.

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: password`
transport_password_prompt	`stały`
transport_port	`cont_int: 22`
transport_secret	`cont_int_mr_jenkins: *****`

11. Kliknij *Zapisz*, aby zamknąć okno *Weryfikatory haseł*.
12. Następnie kliknij *Zapisz* w prawym górnym rogu, aby zapisać zmiany w definicji konta.

Tematy pokrewne:

- *Tryby połączenia*
- *Uniwersalne modyfikatory haseł*

ROZDZIAŁ 16

Polityki

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 `moduł 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 opartą na module AI, postępuj zgodnie z poniższymi krokami:

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

4. Wybierz *Poziom zagrożenia*. Ten parametr jest wykorzystywany przy wysłaniu wiadomości mailowej oraz dodawany do Dziennika zdarzeń z kodem `FSW0284`.
5. W sekcji *Typ polityki* wybierz przycisk *Moduł AI*.
6. Wybierz opcję `min`, `średni` albo `maks` w polu *Prawdopodobieństwo zagrożenia*, podaj wartość.

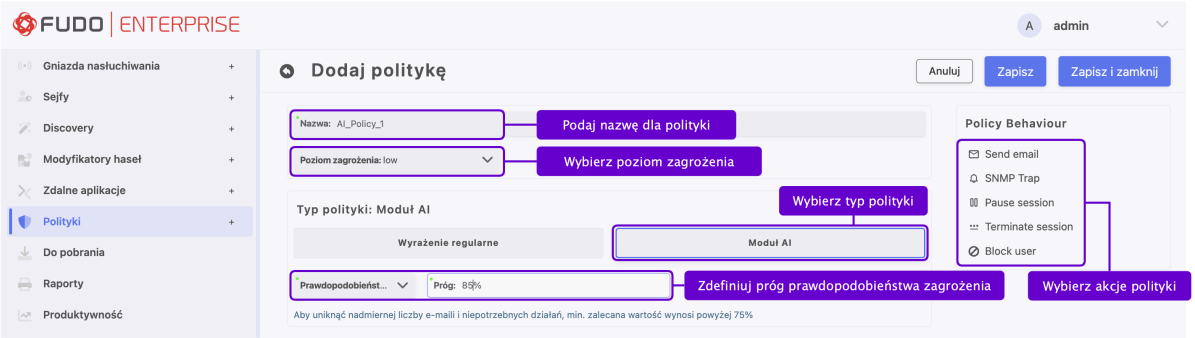
Informacja: Wartości dla *Prawdopodobieństwa zagrożenia* są kalkulowane *modelem behawioralnym* dla każdego segmentu sesji. Oceny segmentów są uśredniane per model (Mouse Biometric, Keyboard Biometric), tworząc *Prawdopodobieństwo zagrożenia Modelu*, co powoduje, że moduł AI dostarcza jedną wartość dla 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%.

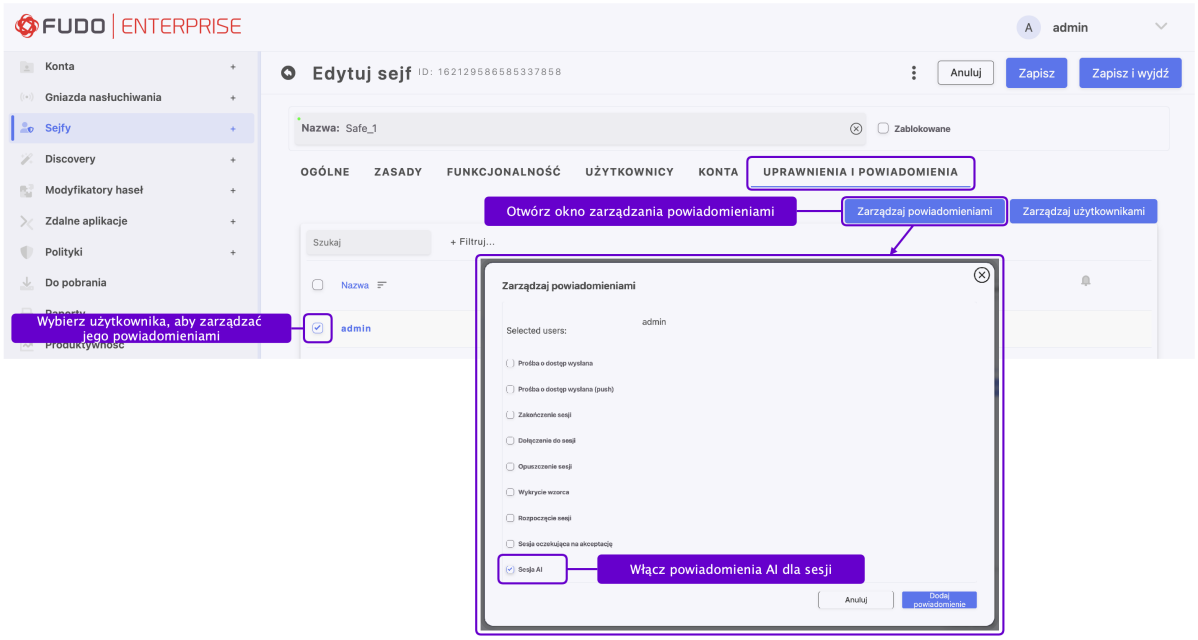
Dla drastycznych akcji, na przykład przerwanie połączenia bądź blokowania użytkownika, jest polecane korzystanie z maksymalnych progów, aby zminimalizować konsekwencje fałszywie dodatnich wyników.



7. Wybierz akcje, które zostaną wykonane w przypadku naruszenia polityki:
   - wysłanie powiadomienia e-mail do administratora systemu,
   - wysłanie powiadomienia SNMP TRAP do odbiorcy,
   - wstrzymanie połączenia,
   - zakończenie połączenia,
   - zablokowanie użytkownika.

Informacja:

- Wysyłanie powiadomień e-mail wymaga skonfigurowania i włączenia *usługi powiadomień* oraz włączenia powiadomień *Sesja AI* w konfiguracji Sejfu.



- Wysyłanie powiadomień SNMP TRAP wymaga skonfigurowania SNMPv3 TRAP w zakładce Ustawienia > System. Sprawdź rozdział *SNMP* aby uzyskać więcej informacji.

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

8. Kliknij *Zapisz*.

16.2 Przykłady polityk opartych na module AI

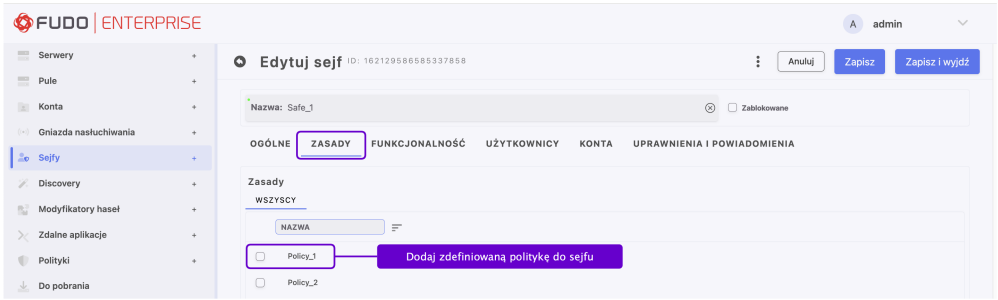
Przykład 1. Wysyłanie powiadomień SNMP TRAP o podejrzanych sesjach.

Aby skonfigurować politykę do wysyłania powiadomień SNMPv3 TRAP o podejrzanych sesjach, postępuj zgodnie z procedurą:

1. Utwórz użytkownika o roli `service` dla usługi SNMPv3:
   - Wybierz *Zarządzanie* > *Użytkownicy*.
   - Utwórz nowego użytkownika.
   - Wprowadź Login.
   - Wybierz `service` w polu *Rola*.
   - Wybierz `Hasło` w sekcji *Uwierzytelnianie* i podaj swoje hasło.
   - Przejdź do zakładki *Więcej*, do sekcji *SNMP* i zdefiniuj ustawienia:

  - Włącz SNMP.
  - Wybierz `SHA` lub `MD5` w polu *Metoda uwierzytelniania*.
  - Wybierz *AES* lub *DES* w polu *Szyfrowanie*.
- Kliknij *Zapisz*.

2. Skonfiguruj SNMPv3 TRAP:
   - Wybierz *Ustawienia* > *System*.
   - Przewiń do sekcji *Serwisowanie i nadzór*.
   - Wybierz opcję *SNMPv3 TRAP*.
   - Skonfiguruj adres *serwera* SNMPv3 TRAP oraz *port*.
   - Wybierz użytkownika z rolą `service` utworzonego w kroku 1.
   - Kliknij *Zapisz*.
3. Utwórz politykę:
   - Wybierz *Zarządzanie* > *Polityki*.
   - Kliknij + *Dodaj politykę*.
   - Podaj nazwę dla polityki.
   - Wybierz `Moduł AI` w polu *Typ polityki*.
   - Wybierz opcję *Prawdopodobieństwo zagrożenia* (np. `średni`) i podaj jego wartość (np. `90%`).
   - Wybierz opcję *SNMP TRAP* w polu *Akcje*.
   - Kliknij *Zapisz*.
4. Przypisz politykę do *sejfu*, który jest używany do nawiązywania połączeń z serwerami.
   - Wybierz *Zarządzanie* > *Sejfy*.
   - Edytuj wybrany sejf, klikając jego nazwę.
   - Przejdź do zakładki *Polityki* i wybierz politykę utworzoną w poprzednim kroku.
   - Kliknij *Zapisz*.



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

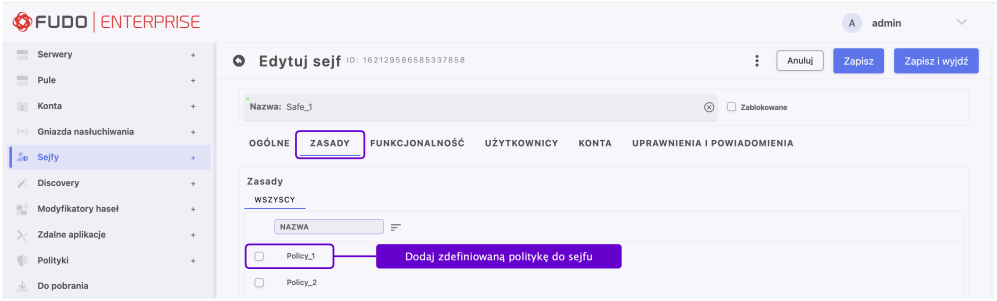
by skonfigurować politykę, przerywającą podejrzane sesje, kiedy próg Prawdopodobieństwa zagrożenia zostanie przekroczony, postępuj zgodnie z instrukcją:

1. Utwórz politykę:
   - Wybierz *Zarządzanie* > *Polityki*.
   - Kliknij + *Dodaj politykę*.
   - Podaj nazwę dla polityki.
   - Wybierz `Moduł AI` w polu *Typ polityki*.
   - Wybierz opcję *Prawdopodobieństwo zagrożenia* (np. `średni`) i podaj jego wartość (np. `90%`).
   - Wybierz opcję *Zakończ sesję* w polu *Akcje*.
   - Kliknij *Zapisz*.

Informacja: Dla drastycznych akcji, takich jak wstrzymanie lub zakończenie sesji czy zablokowanie użytkownika, zaleca się stosowanie maksymalnych progów, aby zminimalizować konsekwencje fałszywie dodatnich wyników.

---

2. Przypisz politykę do *sejfu*, który jest używany do nawiązywania połączeń z serwerami.
   - Wybierz *Zarządzanie* > *Sejfy*.
   - Edytuj wybrany sejf, klikając jego nazwę.
   - Przejdź do zakładki *Polityki* i wybierz politykę utworzoną w poprzednim kroku.
   - Kliknij *Zapisz*.



Tematy pokrewne:

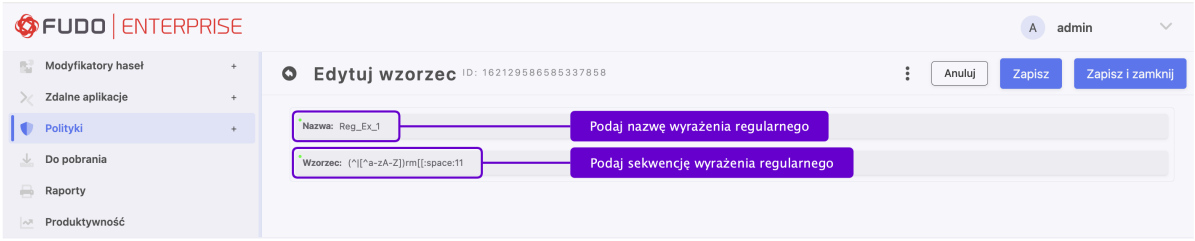
- *Sztuczna inteligencja*
- *Przetwarzanie sesji - uczenie maszynowe*
- *Sejfy*
- *Terminating connection*
- *Notifications*
- *Security*

16.3 Definiowanie polityki na podstawie wzorca

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

Aby skonfigurować politykę opartą na wyrażeniach regularnych, postępuj zgodnie z poniższymi krokami:

1. Wybierz *Zarządzanie* > *Polityki*.
2. Wybierz zakładkę *Wzorce*.
3. Kliknij *+ Dodaj wzorzec*.
4. Wprowadź nazwę wzorca.
5. Zdefiniuj sam wzorzec.



Informacja:

- Wzorce mogą być definiowane jako wyrażenia regularne.
- Fudo Enterprise nie rozpoznaje wyrażeń używających znaku *backslash*, np. `\d`, `\D`, `\w`, `\W`.

6. Powtórz kroki 3-5, aby zdefiniować dodatkowe wzorce.
7. Kliknij *Zapisz i zamknij*.

Informacja: Przykłady wyrażeń regularnych

Komenda `rm`

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

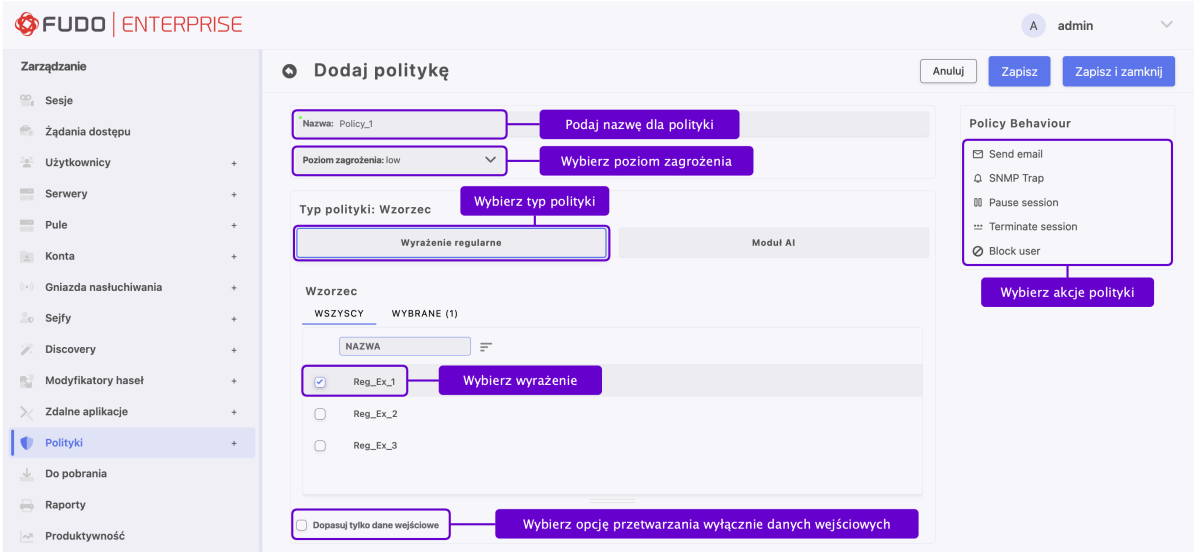
Komenda `rm -rf` (*także* `-fr`; `-Rf`; `-fR`)

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

Komenda `rm file`

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

8. Wróć do zakładki *Polityki*.
9. Kliknij *Dodaj politykę*.



10. Wprowadź nazwę polityki.
11. Określ poziom zagrożenia dla dodawanej polityki.

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

---

12. Kliknij przycisk *Wyrażenie regularne* w sekcji *Typ polityki*.
13. W polu *Wzorce* wybierz wcześniej utworzony wzorzec monitorowania.
14. Wybierz opcję *Przetwarzaj tylko dane wejściowe*, aby system reagował tylko na treści wprowadzone przez użytkownika.

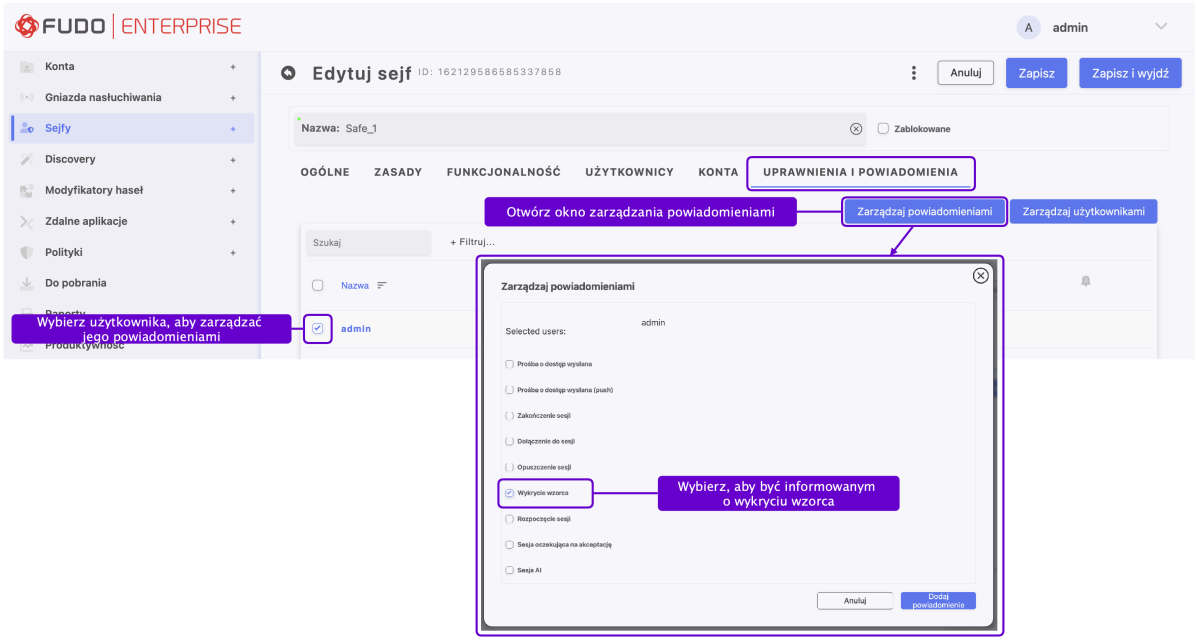
Informacja: W protokołach RDP, VNC i MySQL przetwarzane są tylko dane wejściowe.

---

15. W polu *Zachowanie polityki* wybierz pożądane akcje, które Fudo Enterprise podejmie z chwilą stwierdzenia wystąpienia któregoś ze wzorców:
    - *Wyślij e-mail* - wyślij powiadomienie e-mail do administratora systemu,
    - *SNMP Trap* - wyślij powiadomienie SNMP TRAP,
    - *Wstrzymaj sesję*,
    - *Zakończ sesję*,
    - *Zablokuj użytkownika*.

Informacja:

- Wysyłanie powiadomień e-mail wymaga skonfigurowania i włączenia *usługi powiadomień* oraz włączenia powiadomień *Wykrycie wzorca* w *konfiguracji sejfu*.



- Wysyłanie powiadomień SNMP TRAP wymaga skonfigurowania SNMPv3 TRAP w zakładce *Ustawienia* > *System*. Sprawdź rozdział *SNMP* w celu uzyskania dodatkowych informacji.
- Zablokowanie użytkownika powoduje automatyczne przerwanie połączenia.

16. Kliknij *Zapisz*.
17. Po zdefiniowaniu polityki przypisz ją do *sejfu*, który jest używany do nawiązywania połączeń z serwerami.

Tematy pokrewne:

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

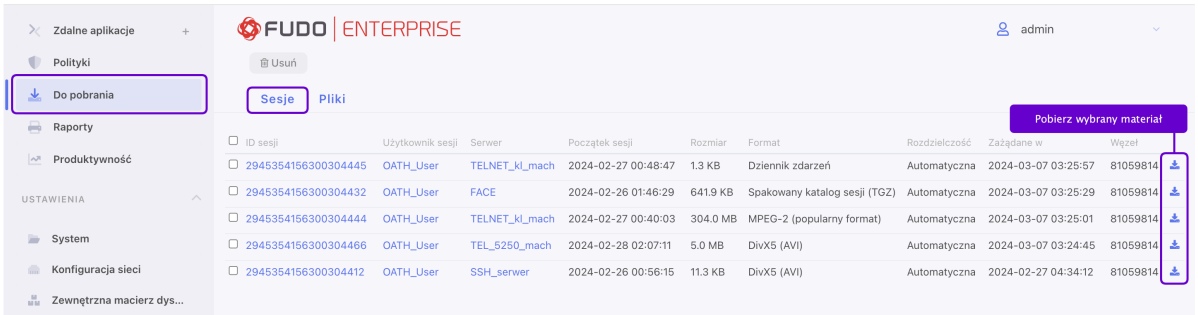
ROZDZIAŁ 17

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*.



17.2 Pliki

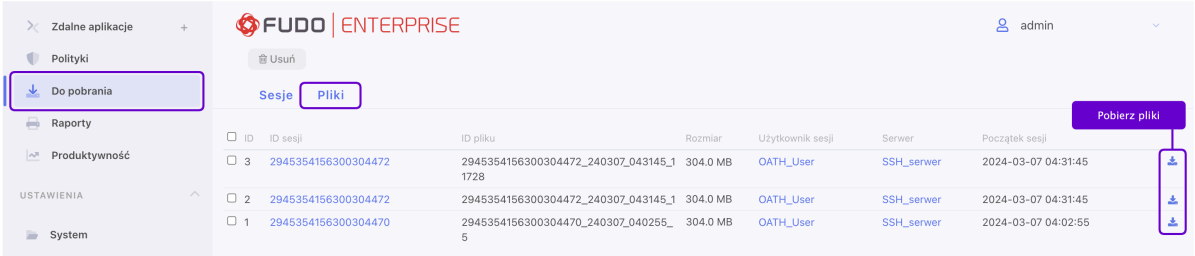
Zakładka **Pliki** jest przeznaczona do zarządzania pobieraniem dużych plików pochodzących z sesji SFTP. Jeśli rozmiar wybranego pliku przekracza 50 MB, przechodzi on proces konwersji i w następnym kroku jest gotowy do pobrania w zakładce **Pliki**. Pliki mniejsze niż 50 MB są pobierane bezpośrednio 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**.

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



Tematy pokrewne:

- *Eksportowanie sesji*

- *Sesje*

ROZDZIAŁ 18

Aktywność konta w Portalu Użytkownika

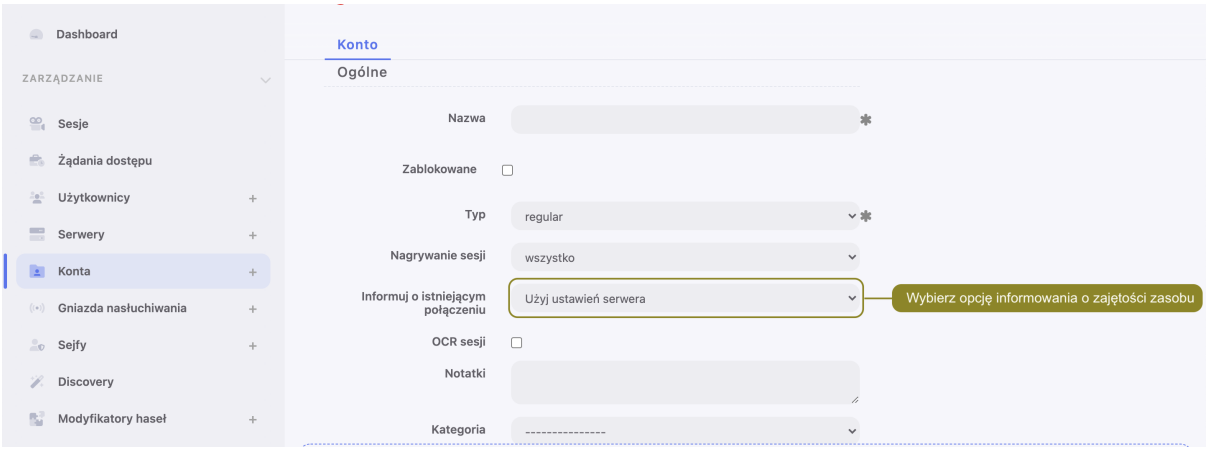
Fudo Enterprise pozwala być informowanym o istniejących połączeniach przez Portal Użytkownika.

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*
- *Konfiguracja ekranu logowania Portalu użytkownika*

ROZDZIAŁ 19

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 (*dotyczy sesji nagranych z opcją rejestrowania pełnego ruchu*).
	Sesja opatrzona znacznikiem czasu.
	Powód nawiązania sesji.
	Sesja zawiera naniesione komentarze.
	Sesja została przetworzona na potrzeby przeszukiwania pełnotekstowego.
	Sprawdź status replikacji sesji.
	Otwórz zarządzanie udostępnianiem sesji.
	Pobierz materiał sesji w wybranym formacie (*dotyczy sesji nagranych z opcją rejestrowania pełnego lub surowego ruchu*).
	Monitor aktywności użytkownika (*dotyczy sesji aktualnie trwających*).
	Nazwa użytkownika, który zaakceptował sesję wymagającą autoryzacji.
	Akceptacja żądania oczekującego.
	Odrzucenie żądania oczekującego.
	Żądanie oczekujące na akceptację.
	Element agregujący połączenia nawiązane w ramach tej samej sesji.
	Sesja *niepodlegająca retencji*.
	Status analizy behawioralnej sesji. *Jest to wersja ewaluacyjna komponentu AI.* ○ - sesja w trakcie analizy, wstępny wynik analizy - brak zagrożenia. ○ - sesja w trakcie analizy, wstępny wynik analizy - średni poziom zagrożenia. ○ - sesja w trakcie analizy, wstępny wynik analizy - wysoki poziom zagrożenia. ○ - sesja oczekuje na analizę lub jest wstępnie przetwarzana. ○ - sesja nie poddana analizie z uwagi na brak wyuczonego modelu. ● - sesja przetworzona - brak zagrożenia. ● - sesja przetworzona - średni poziom zagrożenia. ● - sesja przetworzona - wysoki poziom zagrożenia. ● - sesja przetworzona - brak wyniku analizy.

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

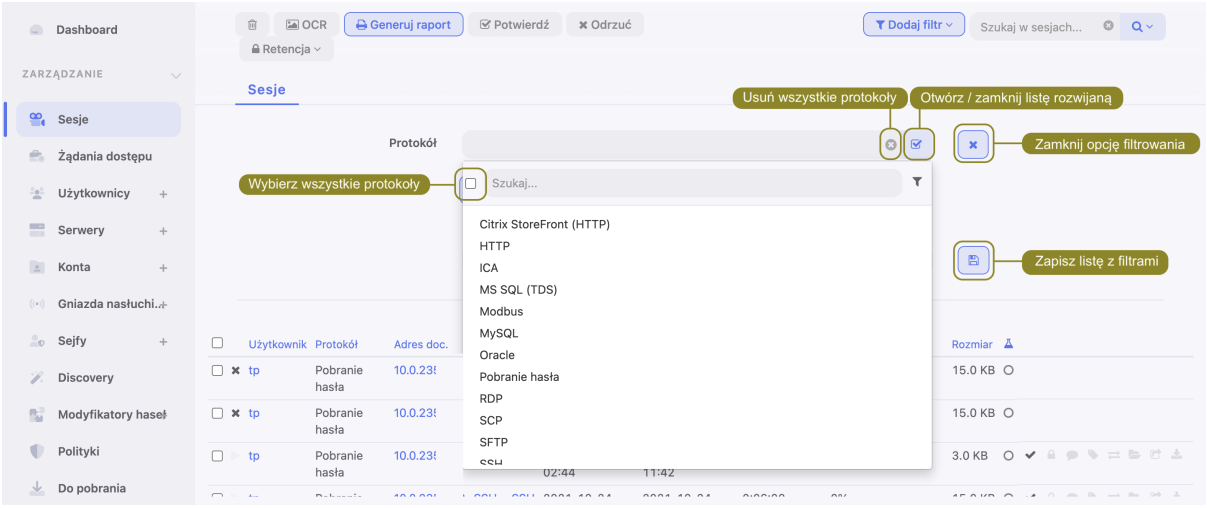
Informacja: Fudo Enterprise przechowuje materiał sesji w formie skompresowanej, z czego wynikać mogą różnice pomiędzy podawanym a faktycznym rozmiarem sesji.

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.

---

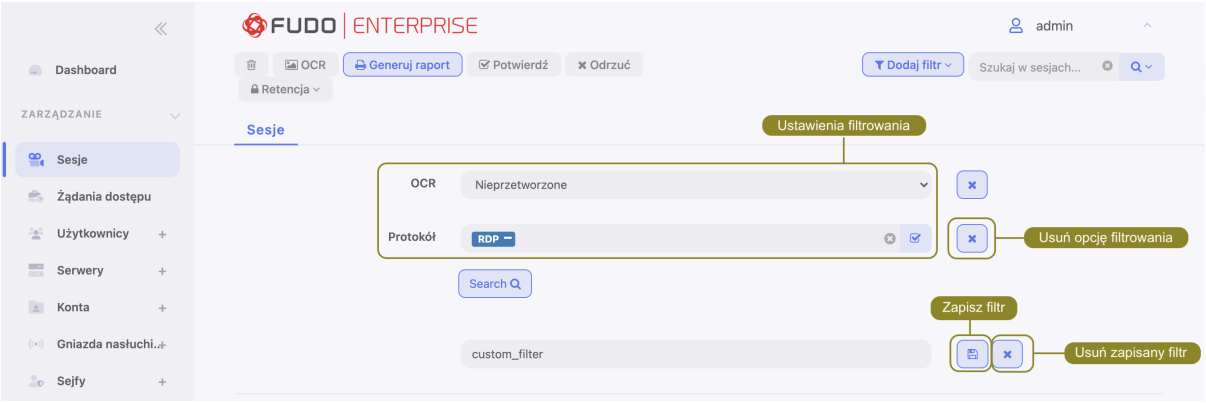
4. Kliknij *Dodaj filtr* i wybierz ponownie wcześniej zaznaczony parametr filtrowania, aby wyłączyć filtrowanie według zadanego parametru.

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 żądaną definicję filtrowania.
2. Zmodyfikuj opcje filtrowania zgodnie z potrzebą.
3. Kliknij ikonę dyskietki, aby zapisać ustawienia.

Usuwanie definicji filtrowania

1. Kliknij *Dodaj filtr* i wybierz żądaną definicję filtrowania.
2. Kliknij ikonę usunięcia definicji filtrowania.
3. Potwierdź usunięcie wybranej definicji filtrowania.

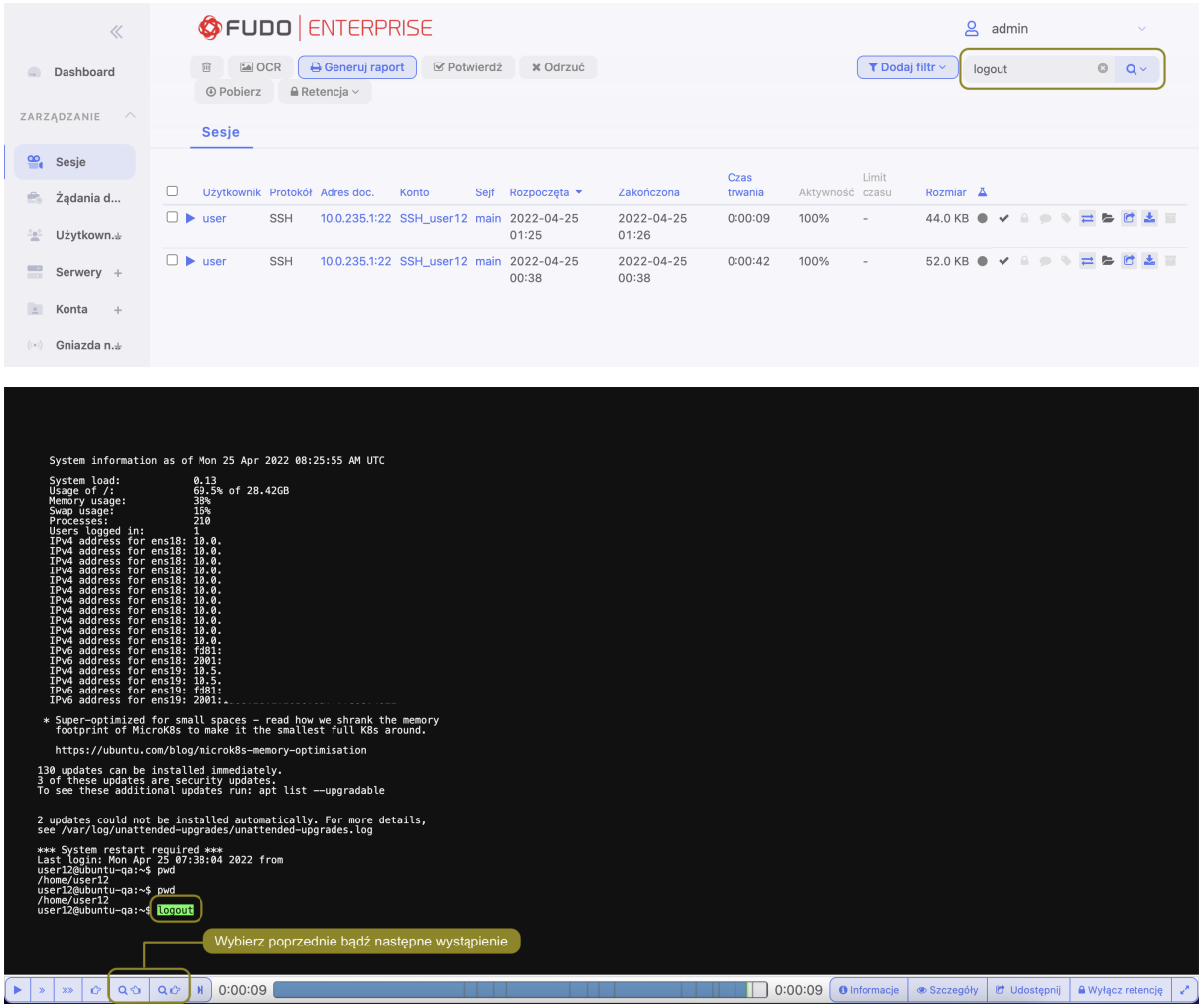
19.1.3 Przeszukiwanie pełnotekstowe

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.

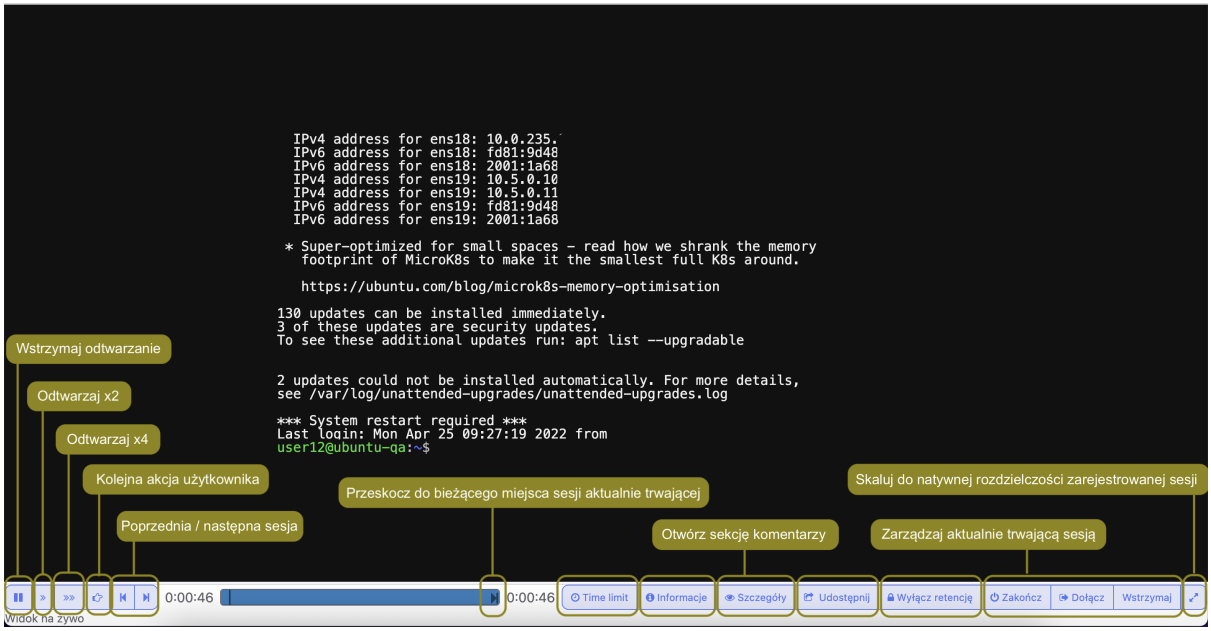
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Wyszukaj na liście żądaną sesję i kliknij ikonę rozpoczęcia odtwarzania.

Informacja: Użyj opcji filtrowania, aby wyświetlić sesje aktywne:

- Kliknij *Dodaj filtr* i z listy wybierz *Aktywne*.
- Z listy rozwijalnej wybierz *Tak*.

Opcje odtwarzacza

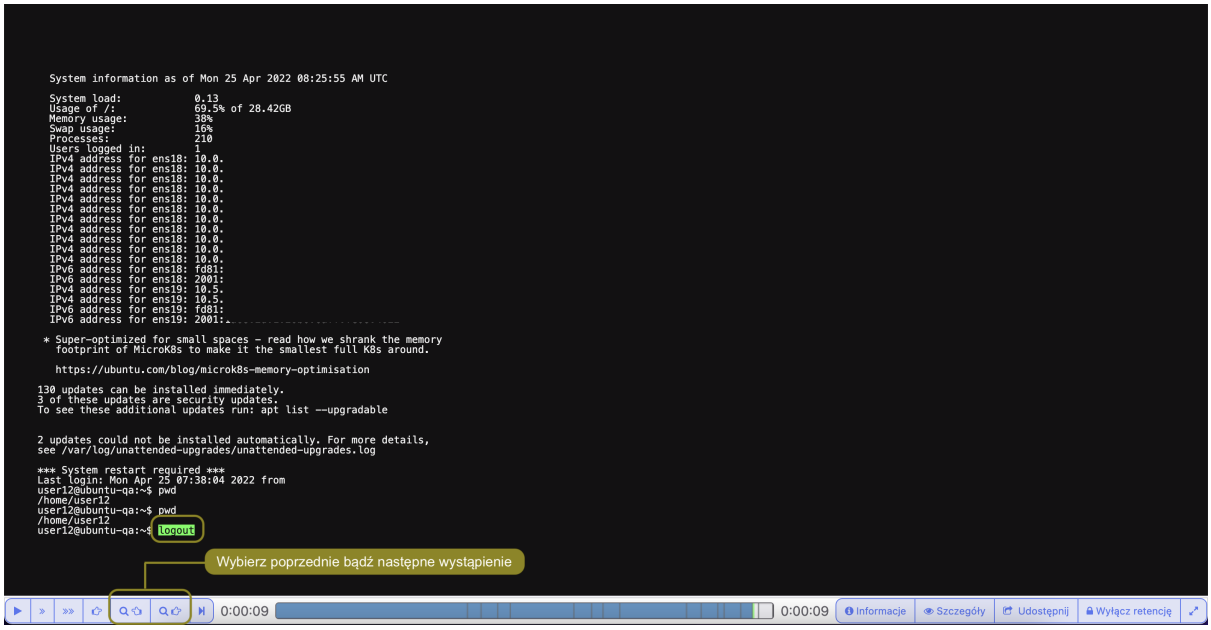
SSH, RDP, Telnet, X11



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

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

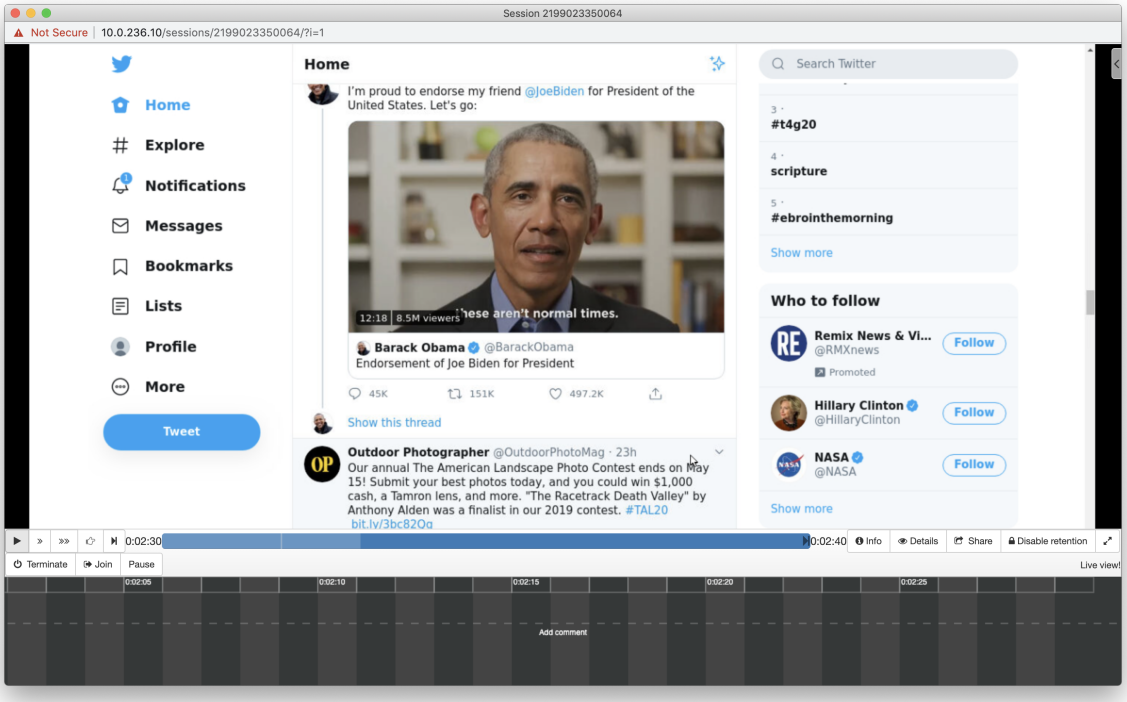
Odtwarzacz pozwala na przeskakiwanie pomiędzy wystąpieniami wprowadzonego ciągu znaków.



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

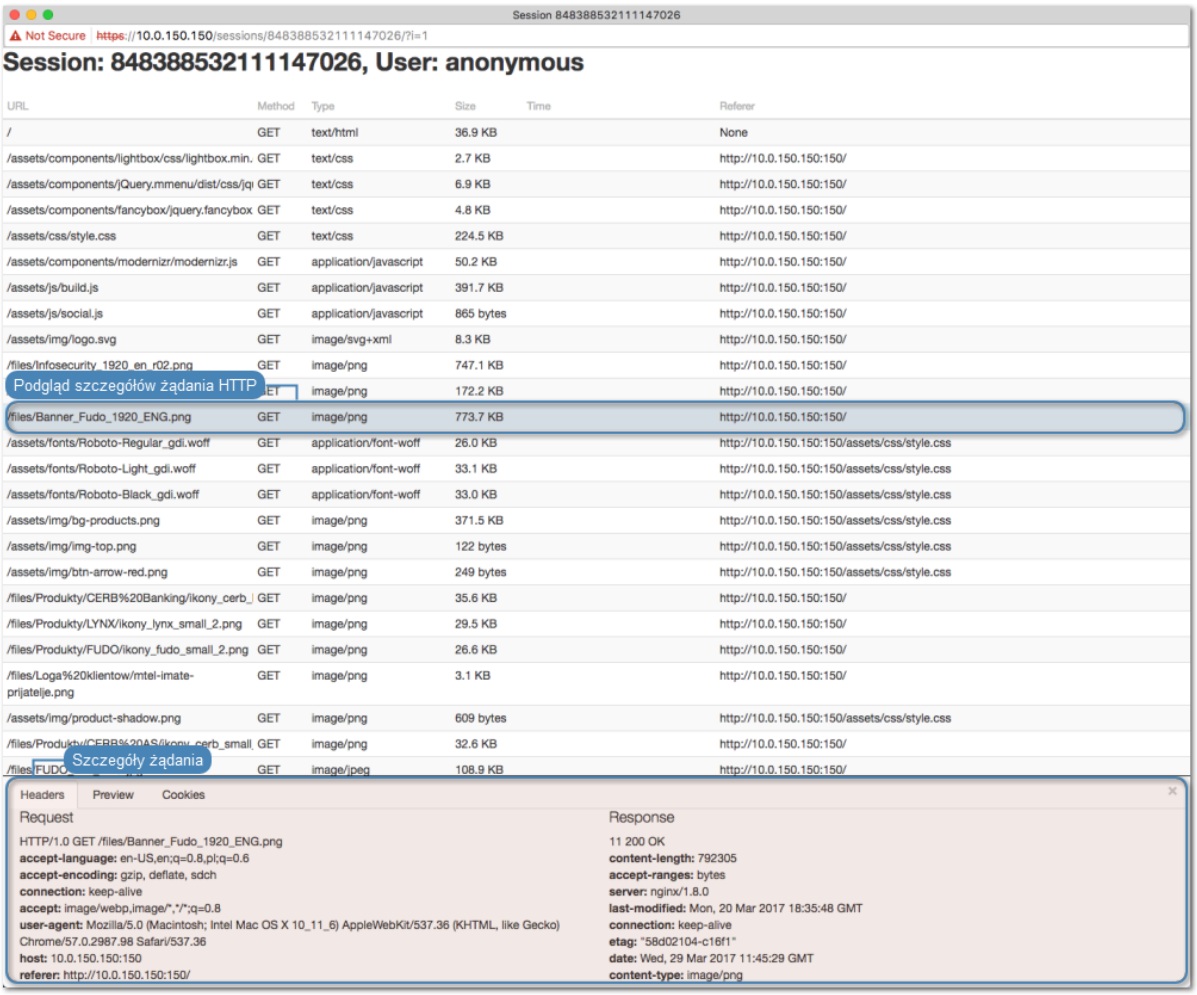
Poniżej przedstawione zostały zrzuty ekranu przedstawiające widoki sesji ustanowionych za pomocą protokołów, takich jak HTTP, SSH, SFTP, MySQL, MSSQL i SCP.

HTTP - renderowane



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

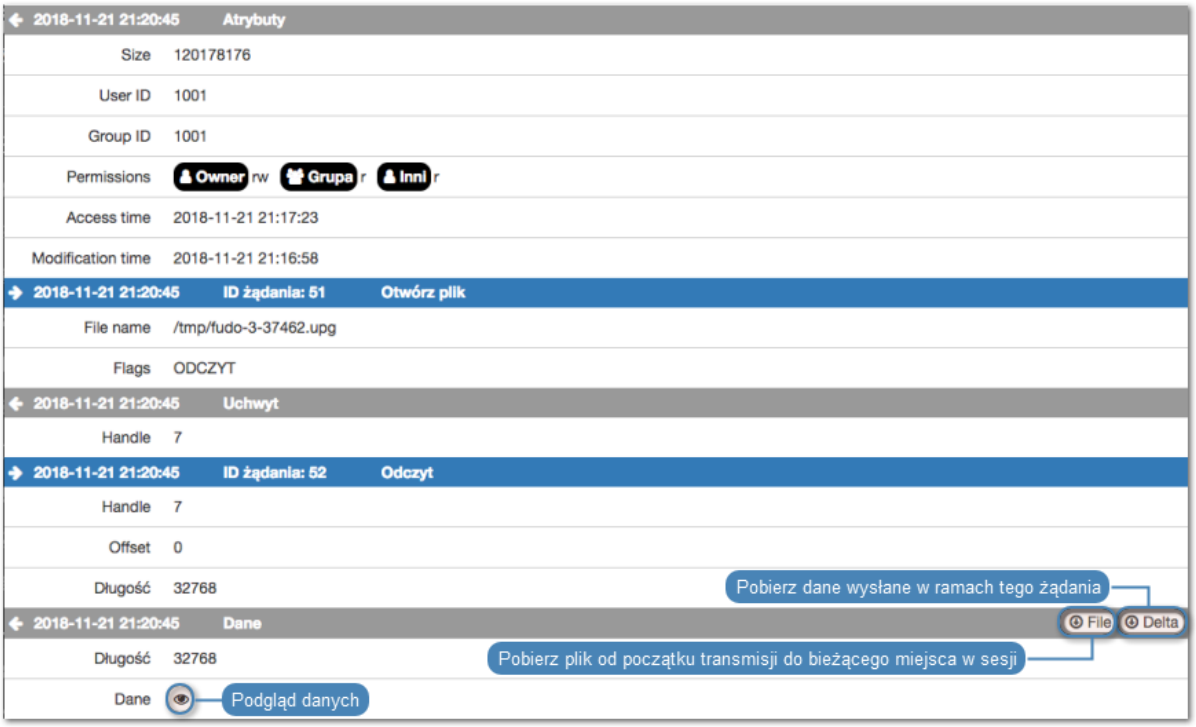
HTTP


Session 848388532111147026
Not Secure https://10.0.150.150/sessions/848388532111147026/?i=1
Session: 848388532111147026, User: anonymous
URL Method Type Size Time Referer
/ GET text/html 36.9 KB None
/assets/components/lightbox/css/lightbox.min. GET text/css 2.7 KB http://10.0.150.150:150/
/assets/components/jQuery.mmenu/dist/css/jq GET text/css 6.9 KB http://10.0.150.150:150/
/assets/components/fancybox/jquery.fancybox GET text/css 4.8 KB http://10.0.150.150:150/
/assets/css/style.css GET text/css 224.5 KB http://10.0.150.150:150/
/assets/components/modernizr/modernizr.js GET application/javascript 50.2 KB http://10.0.150.150:150/
/assets/js/build.js GET application/javascript 391.7 KB http://10.0.150.150:150/
/assets/js/social.js GET application/javascript 865 bytes http://10.0.150.150:150/
/assets/img/logo.svg GET image/svg+xml 8.3 KB http://10.0.150.150:150/
/files/Infosecurity_1920_en_r02.png GET image/png 747.1 KB http://10.0.150.150:150/
Podgląd szczegółów żądania HTTP
/files/Banner_Fudo_1920_ENG.png GET image/png 773.7 KB http://10.0.150.150:150/
/assets/fonts/Roboto-Regular_gdi.woff GET application/font-woff 26.0 KB http://10.0.150.150:150/assets/css/style.css
/assets/fonts/Roboto-Light_gdi.woff GET application/font-woff 33.1 KB http://10.0.150.150:150/assets/css/style.css
/assets/fonts/Roboto-Black_gdi.woff GET application/font-woff 33.0 KB http://10.0.150.150:150/assets/css/style.css
/assets/img/bg-products.png GET image/png 371.5 KB http://10.0.150.150:150/assets/css/style.css
/assets/img/img-top.png GET image/png 122 bytes http://10.0.150.150:150/assets/css/style.css
/assets/img/btn-arrow-red.png GET image/png 249 bytes http://10.0.150.150:150/assets/css/style.css
/files/Produkty/CERB%20Banking/ikony_cerb_ GET image/png 35.6 KB http://10.0.150.150:150/
/files/Produkty/LYNX/ikony_lynx_small_2.png GET image/png 29.5 KB http://10.0.150.150:150/
/files/Produkty/FUDO/ikony_fudo_small_2.png GET image/png 26.6 KB http://10.0.150.150:150/
/files/Loga%20klientow/mtel-imate-prijatelje.png GET image/png 3.1 KB http://10.0.150.150:150/
/assets/img/product-shadow.png GET image/png 609 bytes http://10.0.150.150:150/assets/css/style.css
/files/Produkty/CERB%20AS/ikony_cerb_small GET image/png 32.6 KB http://10.0.150.150:150/
Szczegóły żądania
/files/FUDO GET image/jpeg 108.9 KB http://10.0.150.150:150/
Headers Preview Cookies
Request
HTTP/1.0 GET /files/Banner_Fudo_1920_ENG.png
accept-language: en-US,en;q=0.8,pl;q=0.6
accept-encoding: gzip, deflate, sdch
connection: keep-alive
accept: image/webp,image/*,*/*;q=0.8
user-agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/57.0.2987.98 Safari/537.36
host: 10.0.150.150:150
referer: http://10.0.150.150:150/
Response
11 200 OK
content-length: 792305
accept-ranges: bytes
server: nginx/1.8.0
last-modified: Mon, 20 Mar 2017 18:35:48 GMT
connection: keep-alive
etag: "58d02104-c16f1"
date: Wed, 29 Mar 2017 11:45:29 GMT
content-type: image/png

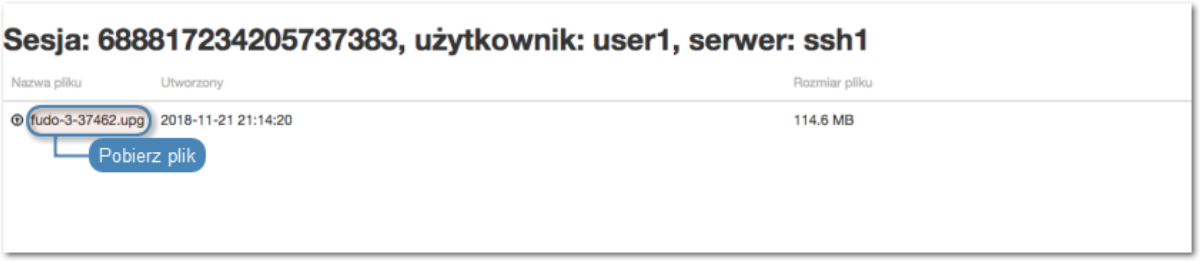
SSH


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

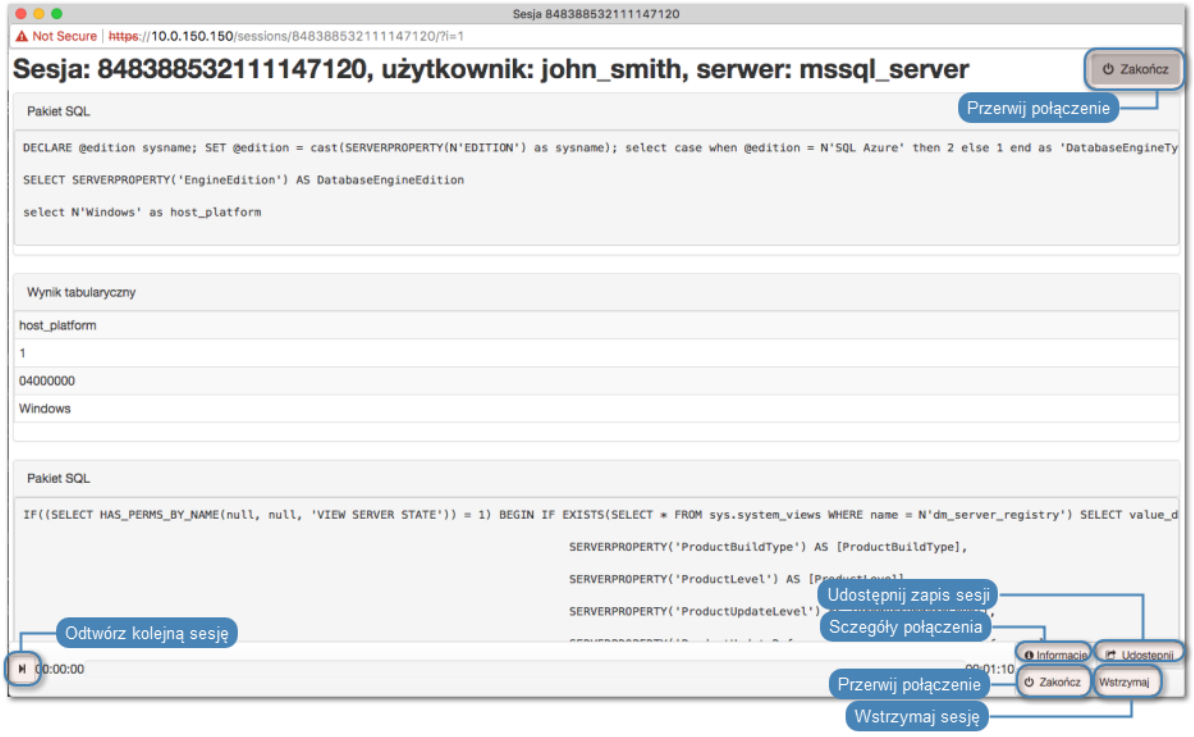
SFTP


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
File
Delta
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


Sesja 848388532111147120
Not Secure | https://10.0.150.150/sessions/848388532111147120/?i=1
Sesja: 848388532111147120, użytkownik: john_smith, serwer: mssql_server
Zakończ
Przerwij połączenie
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 [
SERVERPROPERTY('ProductUpdateLevel')
Udostępnij zapis sesji
Szczegóły połączenia
Odtwórz kolejną sesję
00:00:00
Informacje
Udostępnij
Zakończ
Wstrzymaj
Przerwij połączenie
Wstrzymaj sesję

Modbus

Tematy pokrewne:

- *Funkcjonalności wrażliwe*

19.3 Wstrzymywanie połączenia

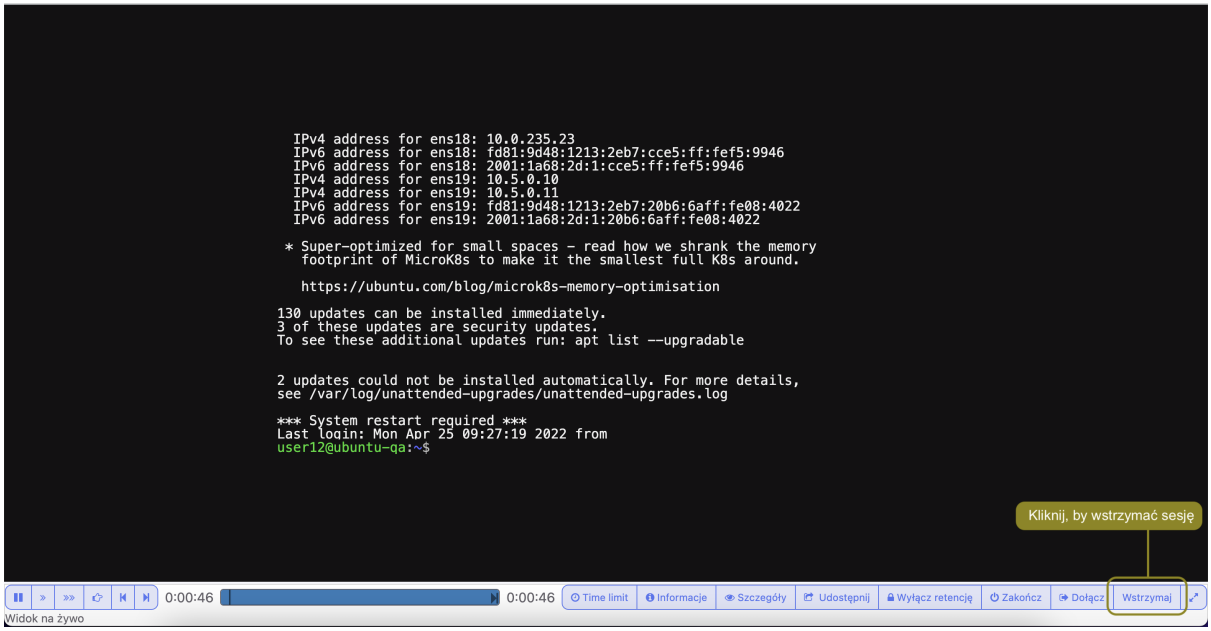
W przypadku gdy aktualne akcje użytkownika wymagają analizy, połączenie może zostać wstrzymane.

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 żądaną sesję i kliknij ikonę rozpoczęcia odtwarzania.
5. Kliknij *Wstrzymaj*.



Tematy pokrewne:

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

19.4 Przerywanie połączenia

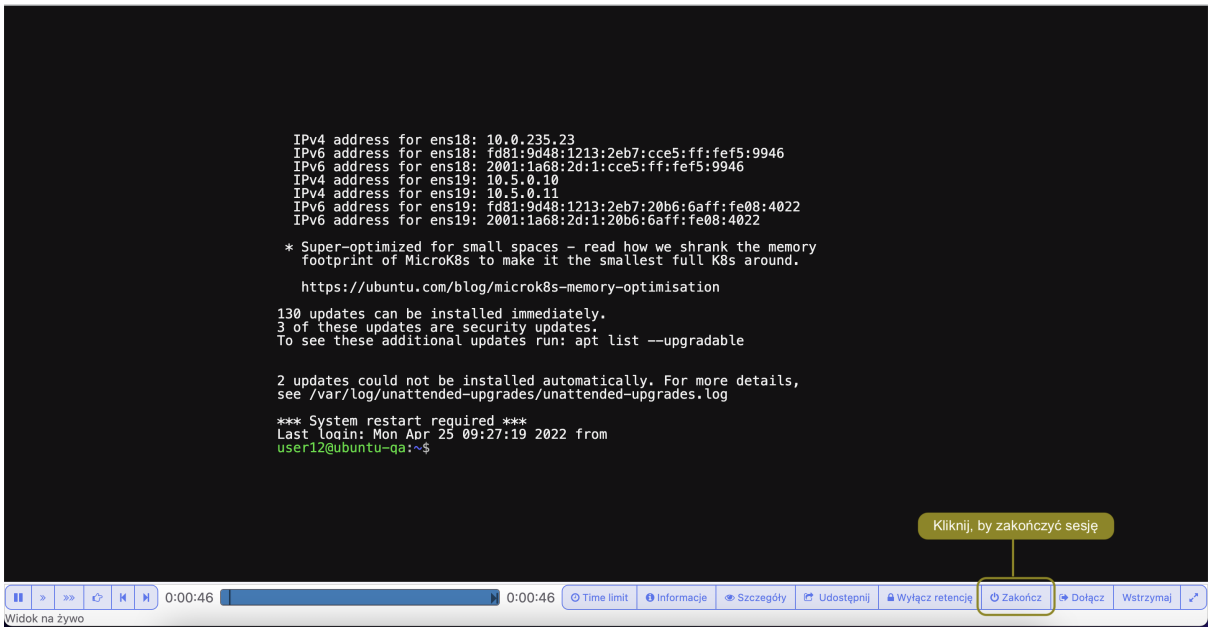
W przypadku gdy administrator stwierdzi nadużycie praw dostępu, może przerwać sesję połączeniową użytkownika.

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.



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 jednoczesną pracę z użytkownikiem.

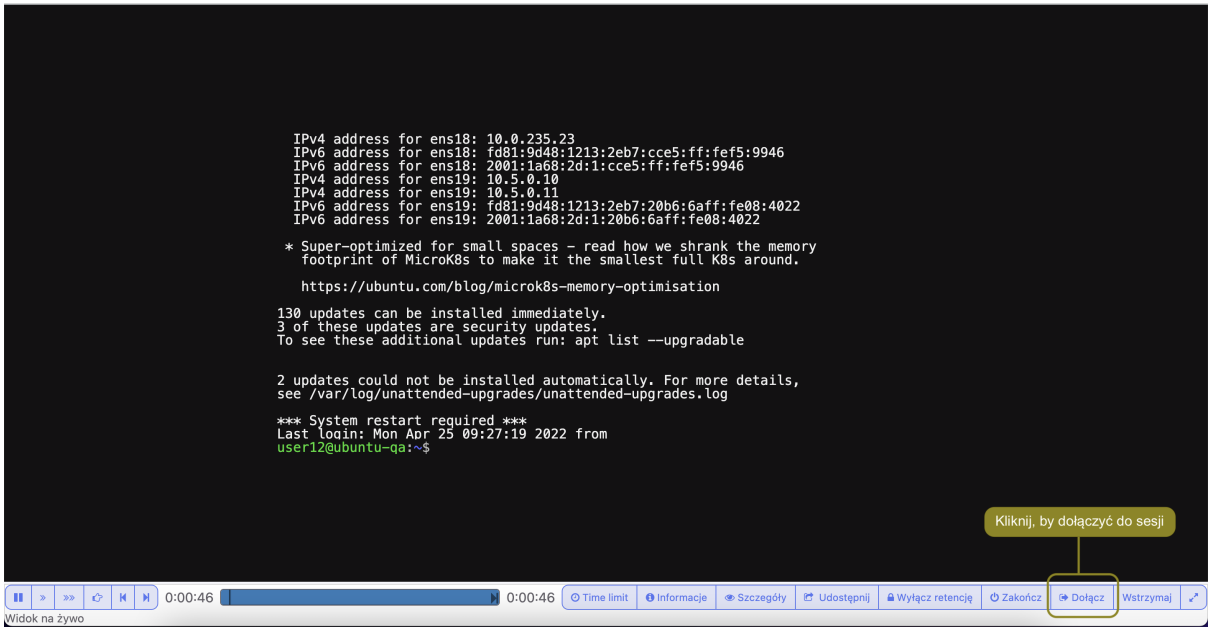
Informacja:

- Funkcja dołączania do sesji jest możliwa w połączeniach SSH, RDP, VNC oraz Telnet (z wyłączeniem Telnet 5250 oraz Telnet 3270).
- W przypadku konfiguracji klastrowej, dołączenie do sesji jest możliwe po zalogowaniu do panelu administracyjnego Fudo na węźle, który obsługuje daną sesję.

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

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij *Dodaj filtr* i z listy wybierz *Aktywne*.
3. Z listy rozwijalnej wybierz *Tak*.
4. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.

5. Kliknij przycisk *Dołącz*.



Tematy pokrewne:

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

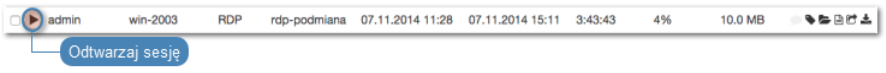
19.6 Udostępnianie sesji

Fudo Enterprise umożliwia udostępnienie innemu użytkownikowi sesji zapisanej oraz aktualnie trwającej.

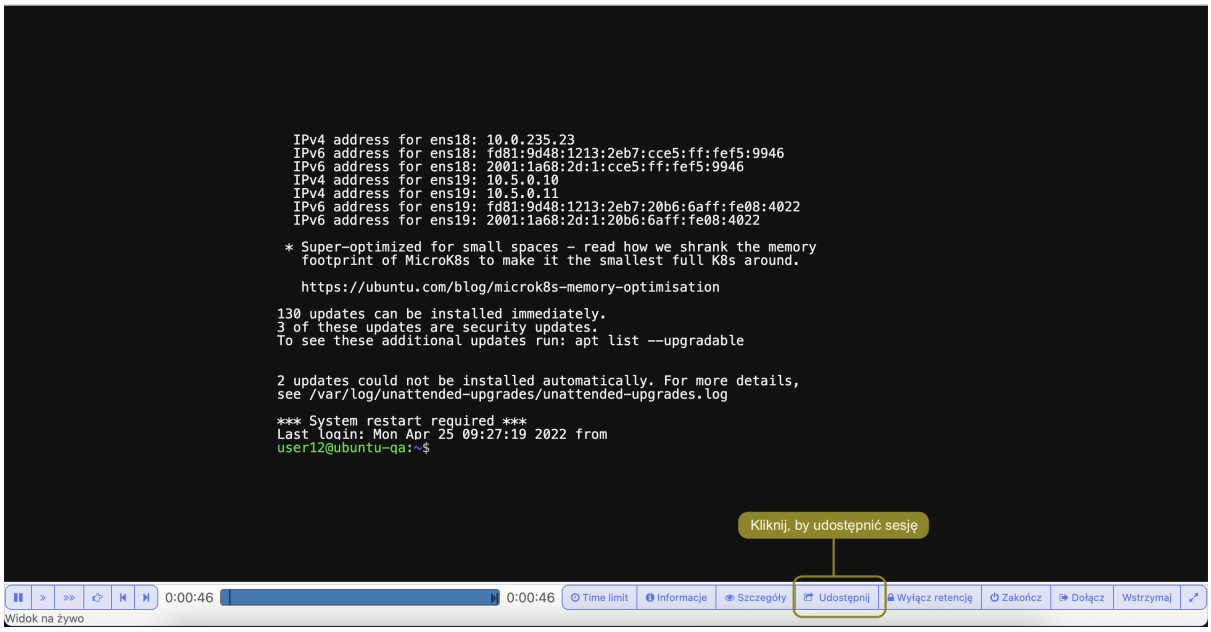
Udostępnianie sesji

Aby udostępnić sesję, postępuj zgodnie z poniższą instrukcją.

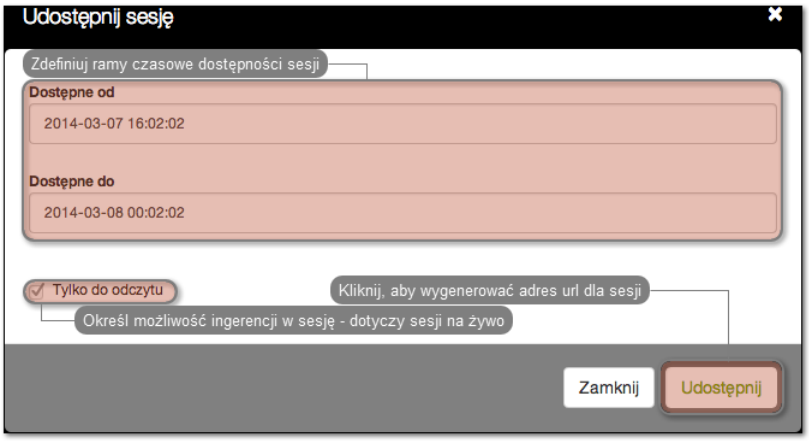
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Wyszukaj wybraną sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.



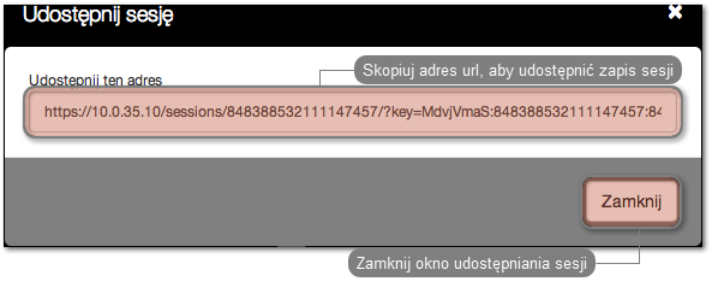
3. Kliknij *Udostępnij*.



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

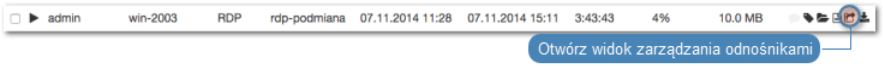


5. Skopiuj odnośnik i kliknij *Zamknij*.

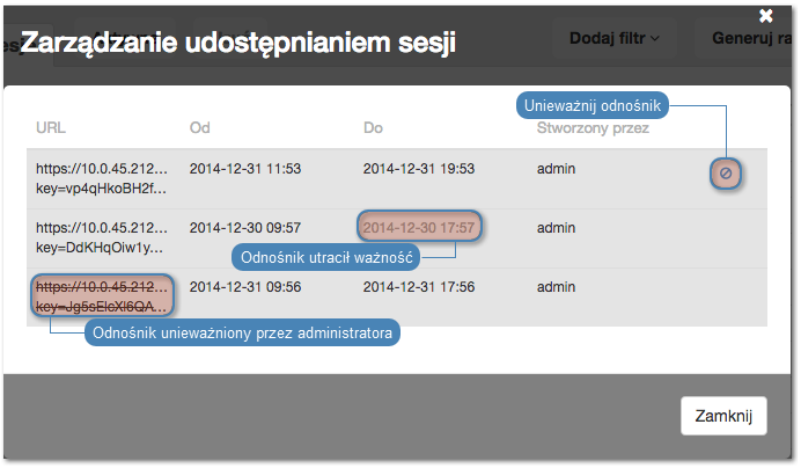


Unieważnienie odnośnika

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



3. Kliknij ikonę unieważnienia odnośnika.



Tematy pokrewne:

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

19.7 Komentowanie sesji

Fudo Enterprise pozwala na dodawanie komentarzy i znaczników do zarejestrowanych sesji.

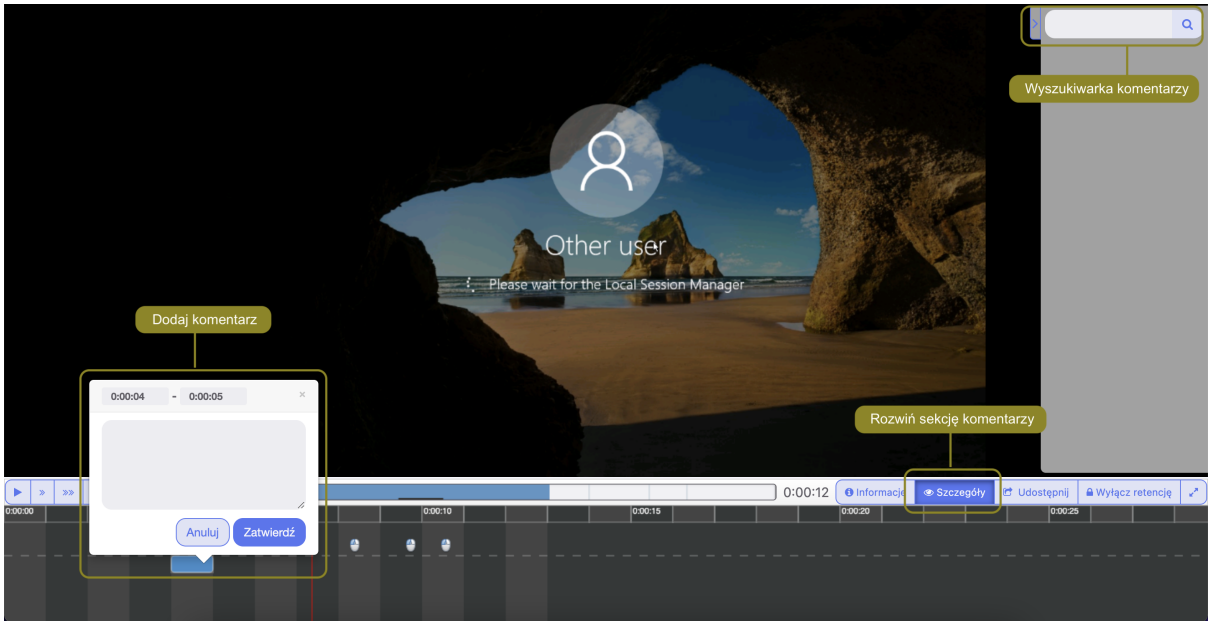
Dodawanie komentarza

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:

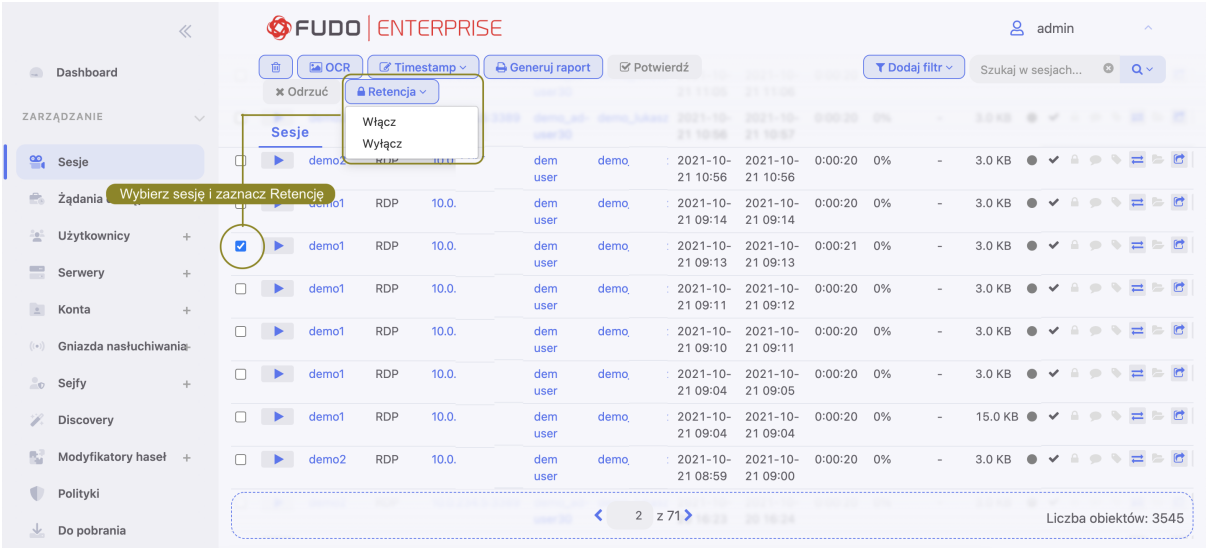
- *Funkcjonalności wrażliwe*

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.

Wyłączanie retencji dla wybranych sesji

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



3. Kliknij *Retencja* i wybierz opcję *Wyłącz retencję*.
4. Kliknij *Zatwierdź*, aby wyłączyć wybrane pozycje z retencji danych.

Włączanie retencji dla wybranych sesji

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Zaznacz żądane sesje.
3. Kliknij *Retencja* i wybierz opcję *Włącz retencję*.
4. Kliknij *Zatwierdź*, aby włączyć retencję dla wybranych pozycji.

Ostrzeżenie: Sesje zostaną usunięte zgodnie z bieżącymi parametrami retencji danych.

Tematy pokrewne:

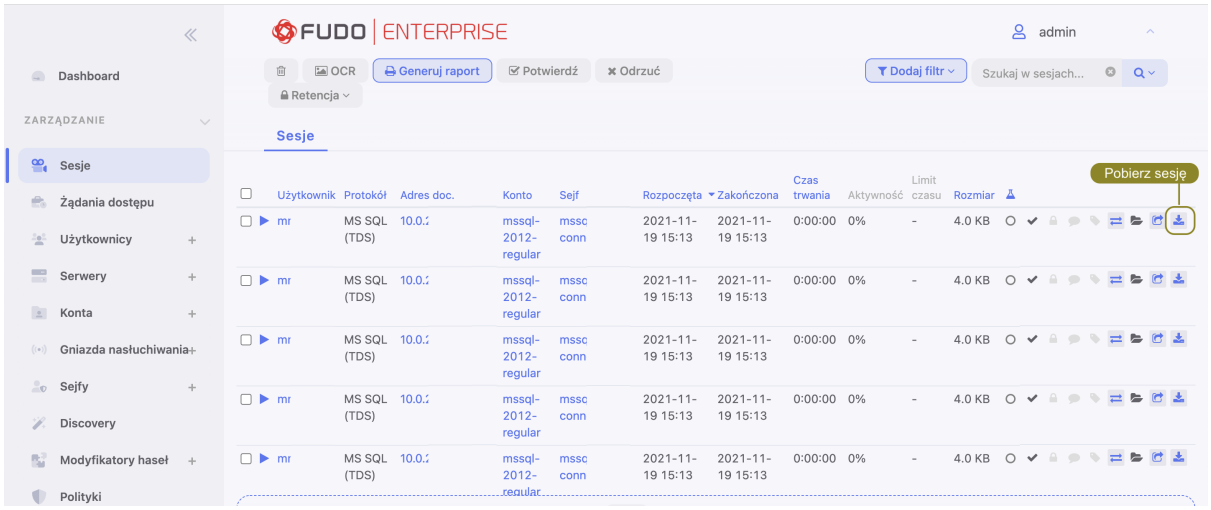
- *Kopia zapasowa systemu*
- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

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 żądaną sesję i kliknij ikonę eksportu zarejestrowanego materiału.



3. Wybierz format pliku wyjściowego.

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

---

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

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

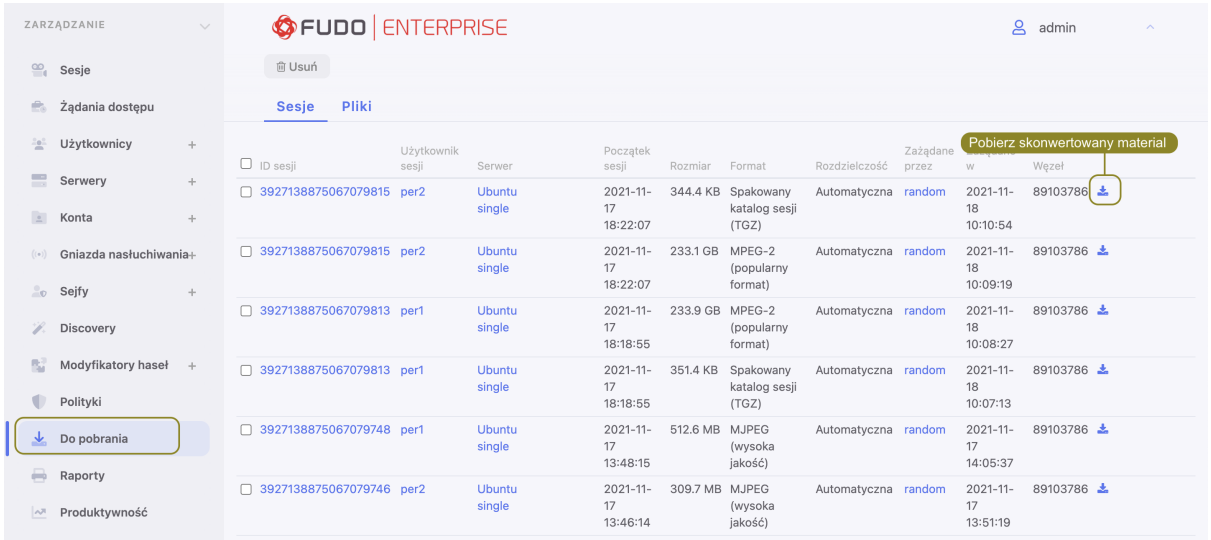
---

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

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

---

6. Kliknij ikonę pobrania sesji.



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:

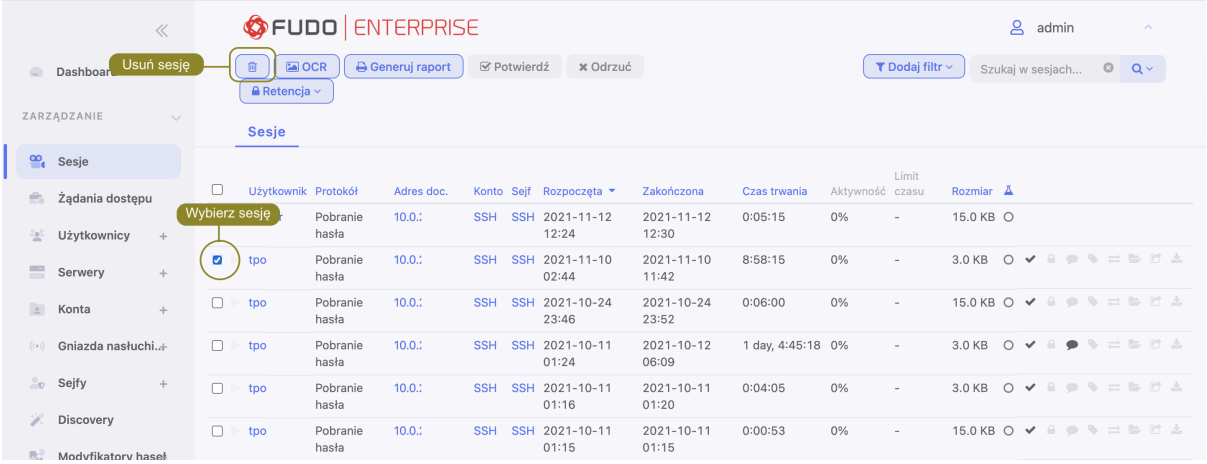
- *Filtrowanie sesji*
- *Udostępnianie sesji*
- *Odtwarzanie sesji*
- *Dołączanie do sesji*

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.



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.

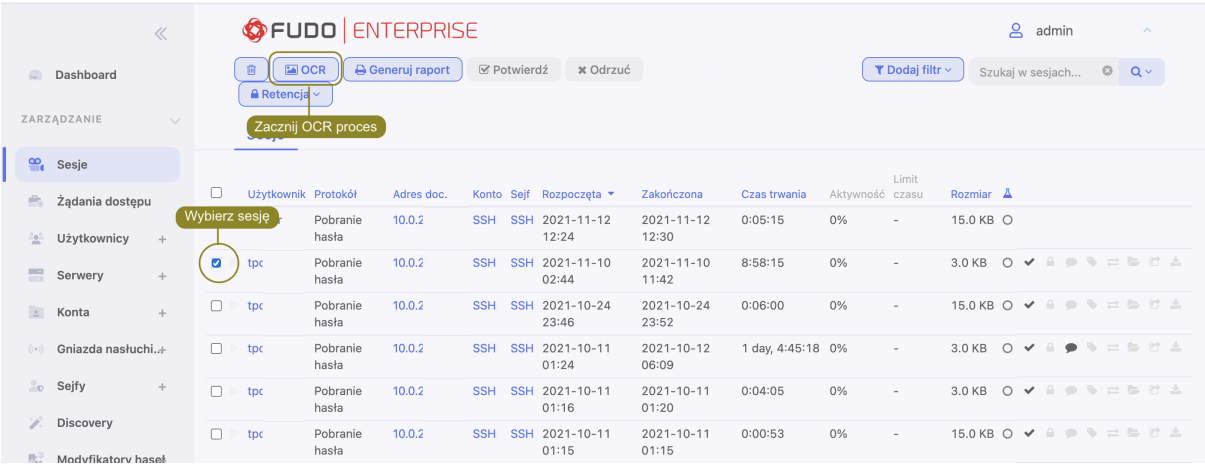
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Znajdź i wybierz żądane konto.
3. Zaznacz opcję *OCR sesji*.
4. Wybierz język przetwarzanych treści.

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.

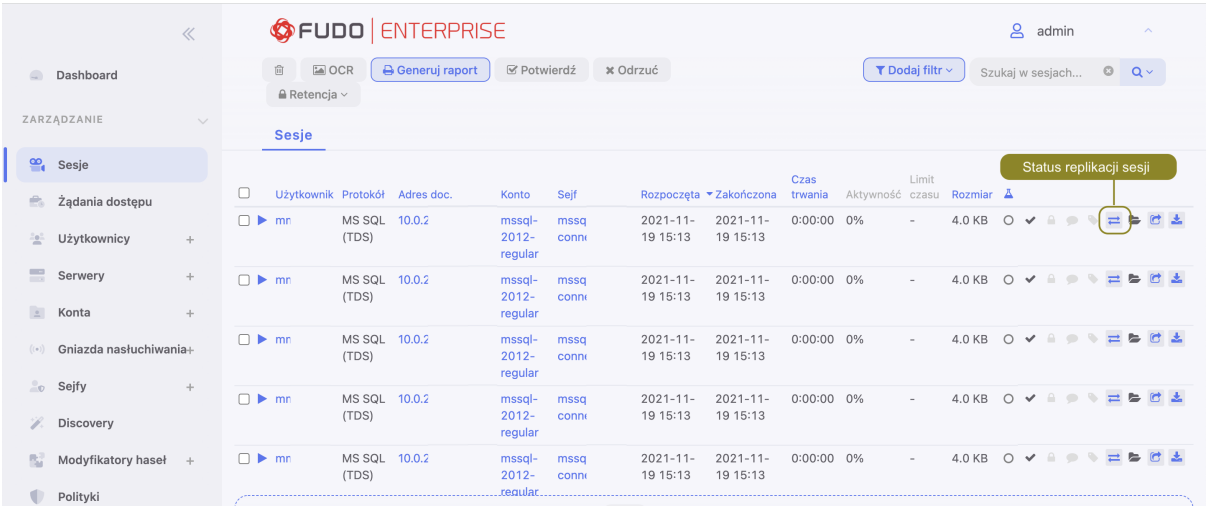
Tematy pokrewne:

- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

19.12 Replikacja sesji w konfiguracji klastrowej

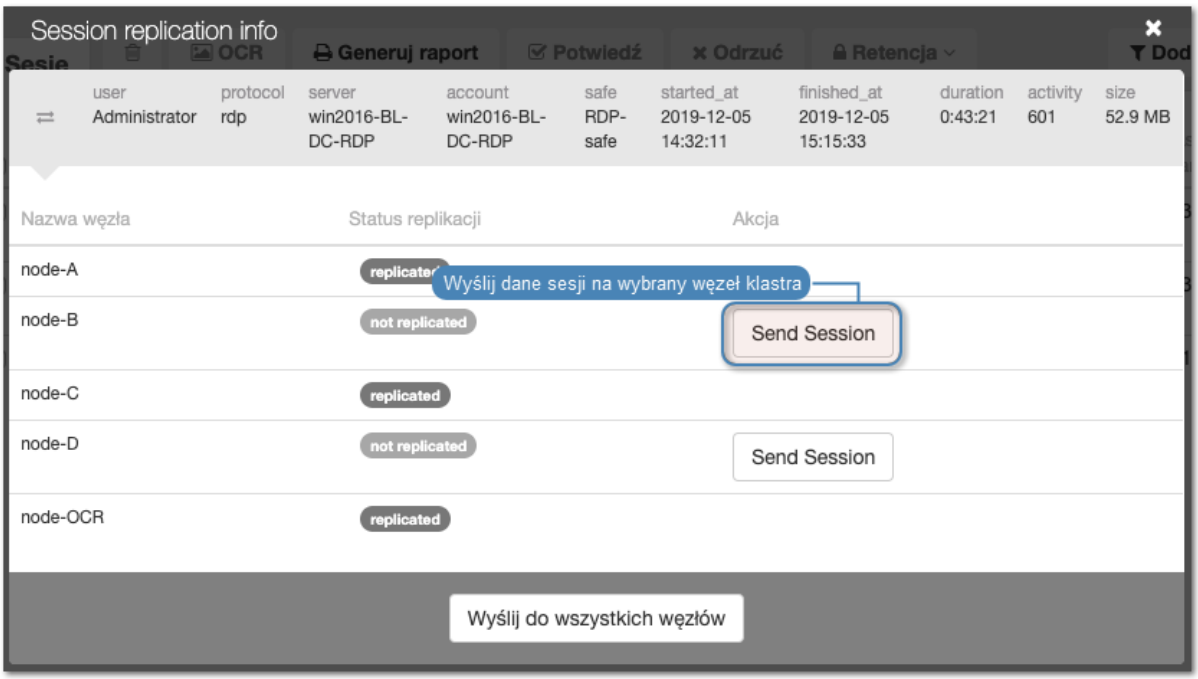
Poza automatyczną replikacją danych w ramach konfiguracji klastrowej, Fudo Enterprise umożliwia ręczne zreplikowanie pojedynczych sesji na węzły, na które dana sesja nie jest przesyłana automatycznie.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij ⇄ przy wybranej sesji.

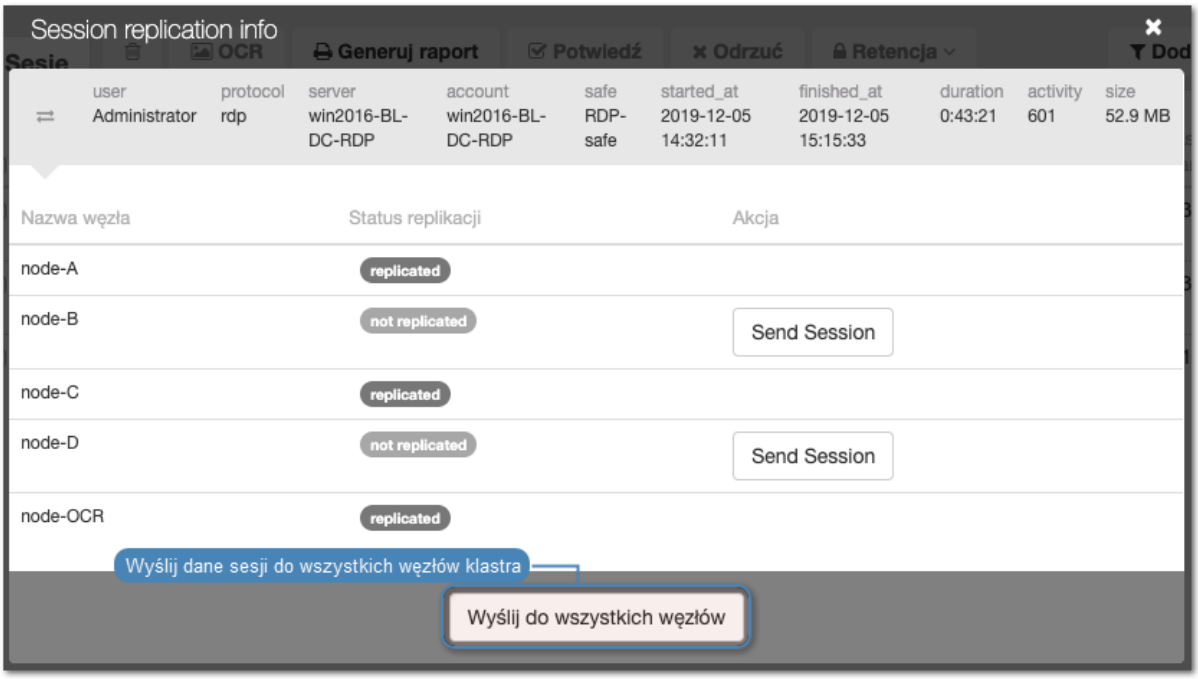


Informacja: Opcja wysłania sesji do wybranych instancji Fudo Enterprise dotyczy węzłów, na które dane wybranej sesji nie są replikowane automatycznie.

3. Kliknij *Wyślij sesję* przy wybranym węźle, aby zreplikować dane na wskazany węzeł



lub *Wyślij do wszystkich węzłów*, aby dane sesji zostały zreplikowane na wszystkie węzły klastra.



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 opatrzyć znacznikiem czasu wybrane sesje, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Zaznacz żądane sesje, kliknij *Timestamp* i wybierz *Oznakuj sesje*.

3. Kliknij *Zatwierdź*.

Informacja: Po włączeniu opcji znakowania czasem na liście sesji pojawi się dodatkowa kolumna zawierająca status znakowania. Sesje opatrzone znacznikiem czasu wyróżnione są aktywną ikoną zegara. Klikając na ikonę można przeglądać szczegółowe informacje o znaczniku oraz pobrać podpis.

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 Wymagane potwierdzenie dostępu

Opcja **Wymagaj potwierdzenia** wprowadza wymóg złożenia żądania o dostęp do serwera, przed nawiązaniem połączenia. Gdy opcja jest włączona, uprawnieni do akceptacji żądania użytkownicy mają określony czas na zaakceptowanie lub odrzucenie prośby o dostęp. Mechanizm ten zapewnia kontrolę i monitorowanie dostępu do krytycznych systemów, zmniejszając ryzyko nieautoryzowanego lub niewłaściwego użycia. Opcja **Wymagaj potwierdzenia** jest zgodna z zasadą **4-Eyes**, zapewniając dodatkową warstwę nadzoru i kontroli.

Informacja: Zasada **4-Eyes** to środek bezpieczeństwa, który poprawia zarządzanie dostępem poprzez wymóg akceptacji lub obecności dwóch uprawnionych osób przy wykonywaniu krytycznych operacji. Takie podejście gwarantuje, że żadna pojedyncza osoba nie ma pełnej kontroli nad działaniami wrażliwymi, zmniejszając ryzyko błędów, oszustw lub nieautoryzowanego dostępu.

Aby umożliwić wysyłanie próśb użytkowników, konieczne jest zaznaczenie opcji *Wymagaj potwierdzenia* w konfiguracji sejfu. Aby uzyskać więcej informacji, zapoznaj się z sekcją *Dodawanie sejfu*.

Informacja: Aby otrzymywać powiadomienia e-mail o oczekujących sesjach, wybierz powiadomienie *Sesja oczekująca na akceptację* w konfiguracji sejfu.

Akceptowanie i odrzucanie żądań użytkowników jest również możliwe za pośrednictwem aplikacji *Fudo Officer*.

19.15.1 Akceptowanie żądań użytkowników

Informacja: Aby otrzymywać powiadomienia email o połączeniu oczekującym na akceptację, zaznacz opcję *Sesja oczekująca na akceptację* w konfiguracji powiadomień dla sejfu.

---

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij ✔ przy wybranym połączeniu, lub zaznacz żądane sesje oczekujące i kliknij *Potwierdź*.

Tematy pokrewne:

- *Filtrowanie sesji*
- *Konta*
- *Gniazda nasłuchiwania*

19.15.2 Odrzucanie żądań użytkowników

1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij ✖ przy wybranym połączeniu, lub zaznacz żądane sesje oczekujące i kliknij *Odrzuć*.

3. Opcjonalnie, wprowadź powód odrzucenia żądania.

Informacja: Powód odrzucenia wyświetlany jest na liście sesji po najechaniu kursorem na ikonę 💬.

---

4. Opcjonalnie, zaznacz opcję zablokowania konta użytkownika, aby trwale uniemożliwić użytkownikowi nawiązywanie połączeń.
5. Kliknij *Zatwierdź*.

Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Akceptowanie żądań użytkowników*
- *Przerywanie połączenia*
- *Blokowanie użytkownika*
- *Sesje*

19.16 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 podejrzanie długo trwającej sesji.

19.16.1 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.

19.16.2 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 udostępniał 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 zbior akcji/działań 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.

19.16.3 Modele ilościowe

Fudo Enterprise monitoruje liczbę połączeń oraz ich czas trwania i może zaalarmować administratora jeśli stwierdzi nadzwyczaj dużą liczbę połączeń jednoczesnych lub podejrzanie długo trwającą sesję.

Ocena bieżąca dokonywana jest w odniesieniu do danych historycznych, zebranych dla użytkowników, kont i serwerów dla każdego dnia tygodnia i każdej godziny.

Tematy pokrewne:

- *Sztuczna inteligencja*
- *Sesje*
- *Często zadawane pytania*
- *Polityki*

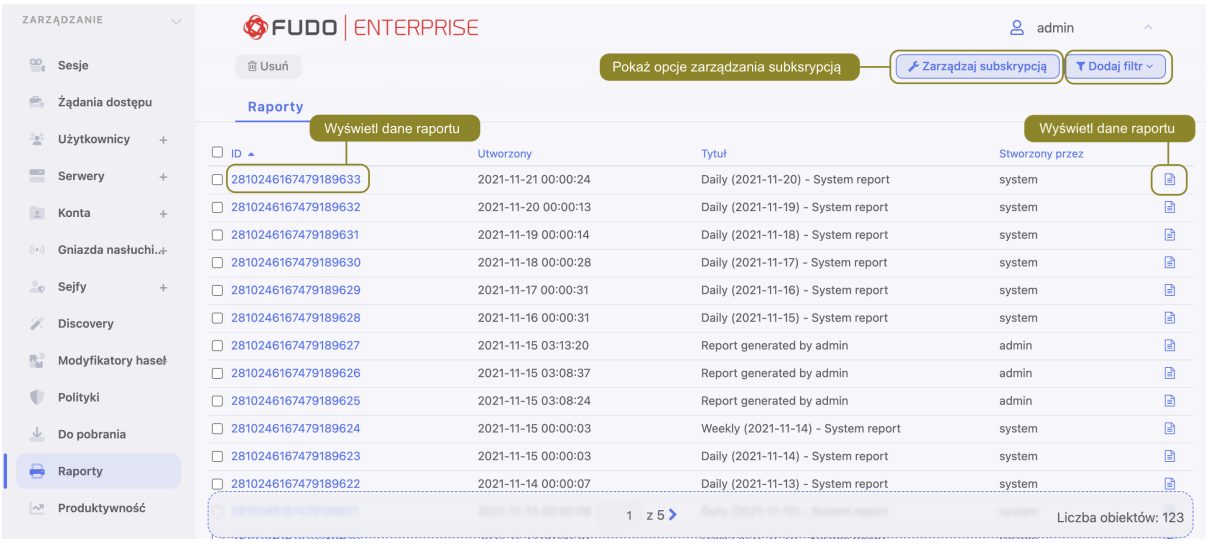
ROZDZIAŁ 20

Raporty

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

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

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



Raporty predefiniowane

Raport dostępu do kont	Raport zawiera konta, wraz ze skojarzonymi serwerami docelowymi oraz sejfami, do których dostęp miał miejsce w określonym przedziale czasu.
Raport dostępu do sejfów	Raport zawiera sejfy, wraz ze skojarzonymi serwerami, do których dostęp miał miejsce w określonym przedziale czasu.
Raport dostępu do serwerów	Raport zawiera serwery wraz ze skojarzonymi sejfami, do których dostęp miał miejsce w określonym przedziale czasu.
Sesje zatwierdzone przez użytkownika	Raport zawiera sesje zatwierdzone przez administratora.
Udostępnianie sesji	Raport zawiera sesje, których zapis został udostępniony osobom trzecim, w określonym przedziale czasu.
Podsumowanie sesji	Raport zawiera sesje zarejestrowane w określonym przedziale czasu.
Raport sesji per serwer	Raport zawiera listę zarejestrowanych sesji w zestawieniu z serwerami w określonym przedziale czasu.
Raport dostępu użytkownika	Raport zawiera użytkowników w zestawieniu z serwerami, do których się logowali, oraz w zestawieniu z sejfami, gniazdami nasłuchiwania oraz kontami, które pośredniczyły w zestawieniu połączenia.
Raport praw dostępu użytkownika	Raport zawiera użytkowników w zestawieniu z obiektami, do których posiadają uprawnienia dostępu.
Raport użytkownika	Raport zawiera zestawienie użytkowników wraz z podstawowymi informacjami: rolą, statusem, datą utworzenia, ostatnim logowaniem oraz użytkownikiem, który utworzył dany obiekt.

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.

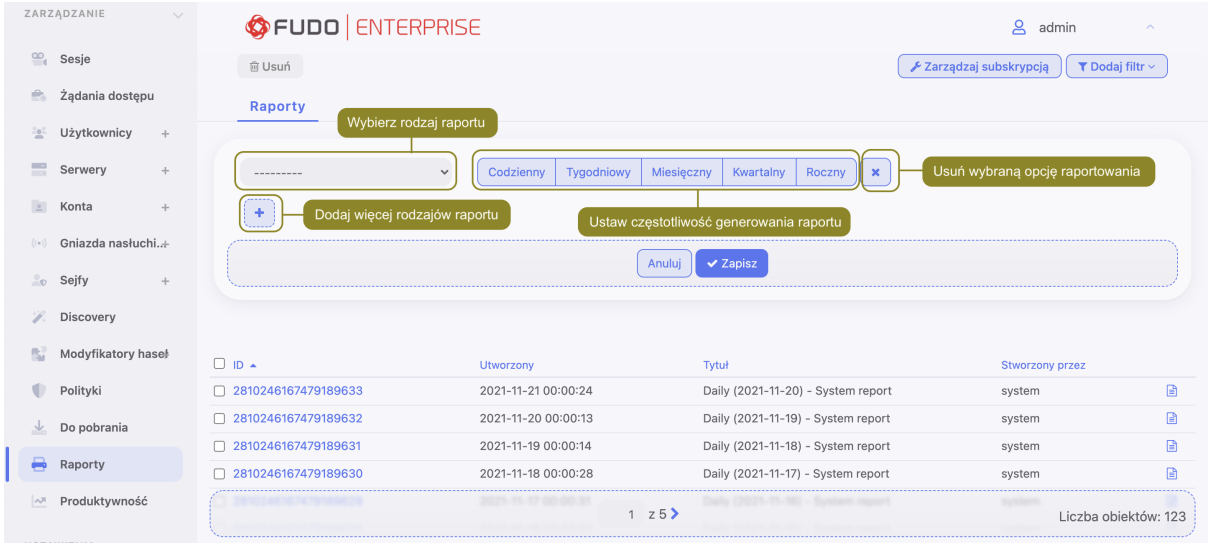
---

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*.



20.2 Rezygnacja z subskrypcji raportu cyklicznego

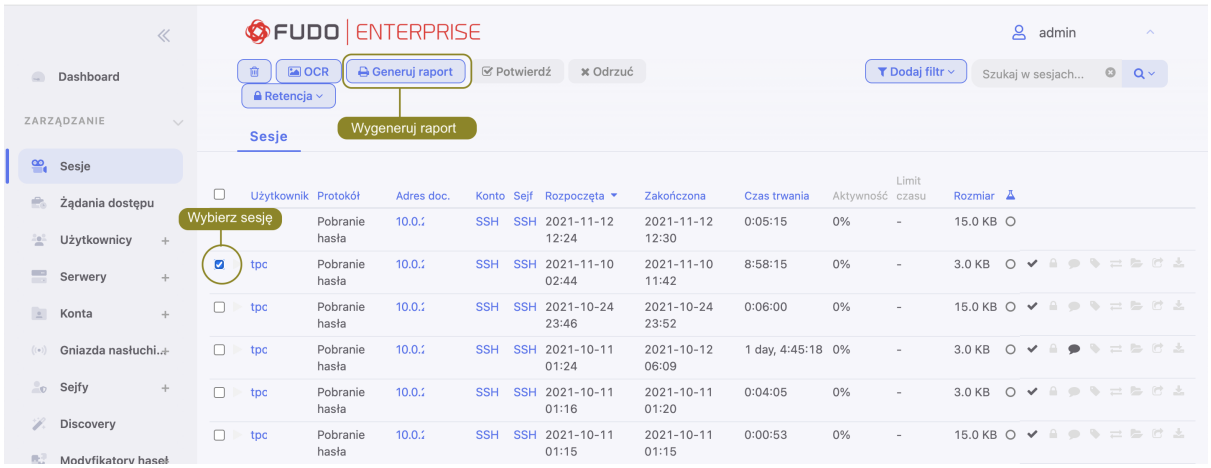
Aby zrezygnować z subskrypcji raportu cyklicznego, postępuj zgodnie z poniższą instrukcją.

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*.



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*

ROZDZIAŁ 21

Produktywność

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

21.1 Zestawienie

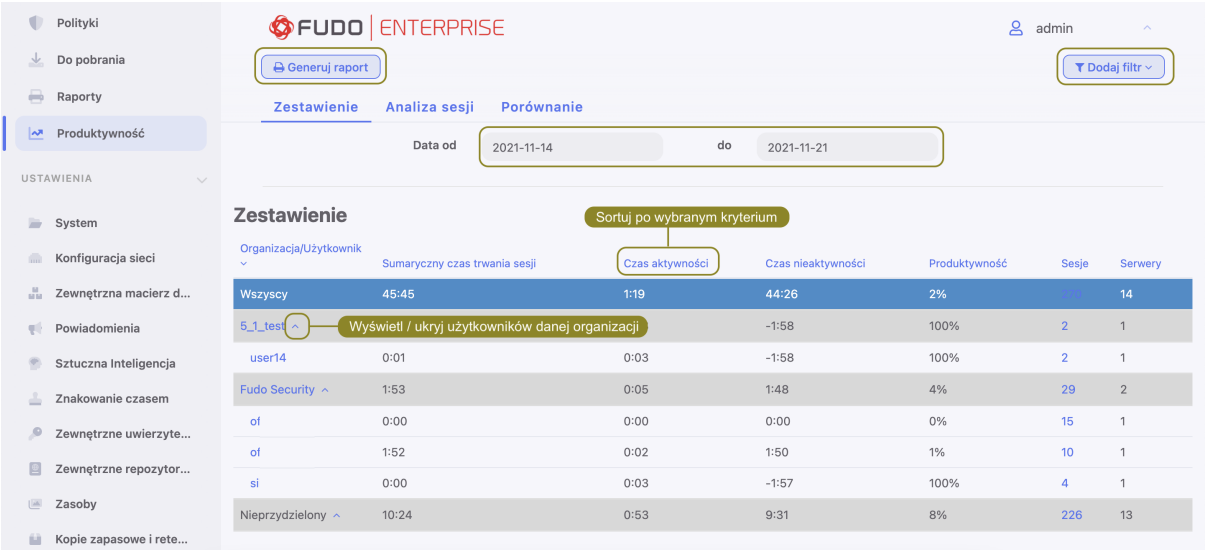
Zestawienie przedstawia dane o aktywności użytkowników i organizacji w wybranym przedziale czasu.

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*.



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*

ROZDZIAŁ 22

Administracja

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:

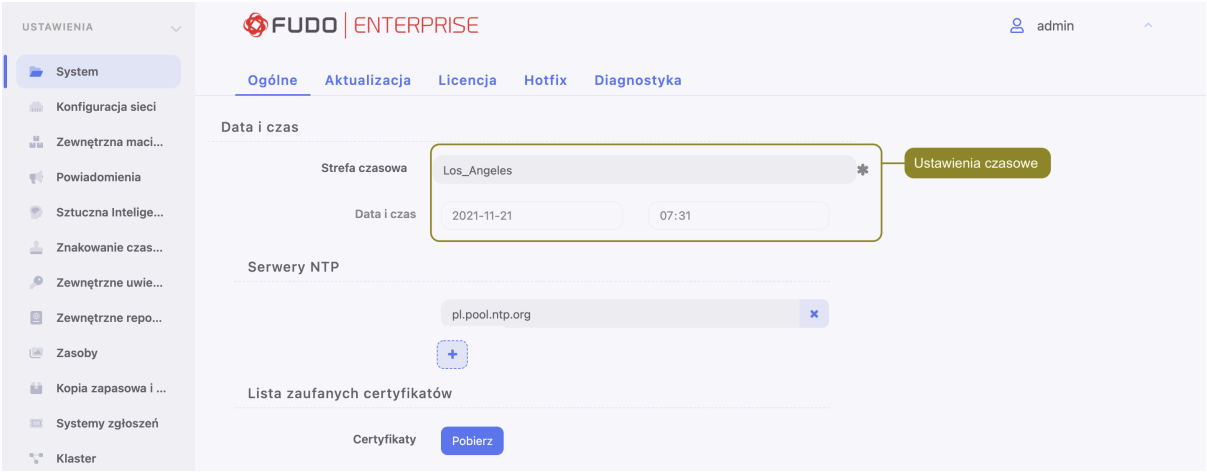
- Zaleca się, aby data i czas pobierane były z serwera NTP, będącego pewnym źródłem danych referencyjnych. Ręczna zmiana ustawień daty i czasu może spowodować nieprawidłowości w funkcjonowaniu urządzenia.
- Pobieranie czasu z serwera NTP jest wymagane w przypadku *konfiguracji klastrowych*.

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*.

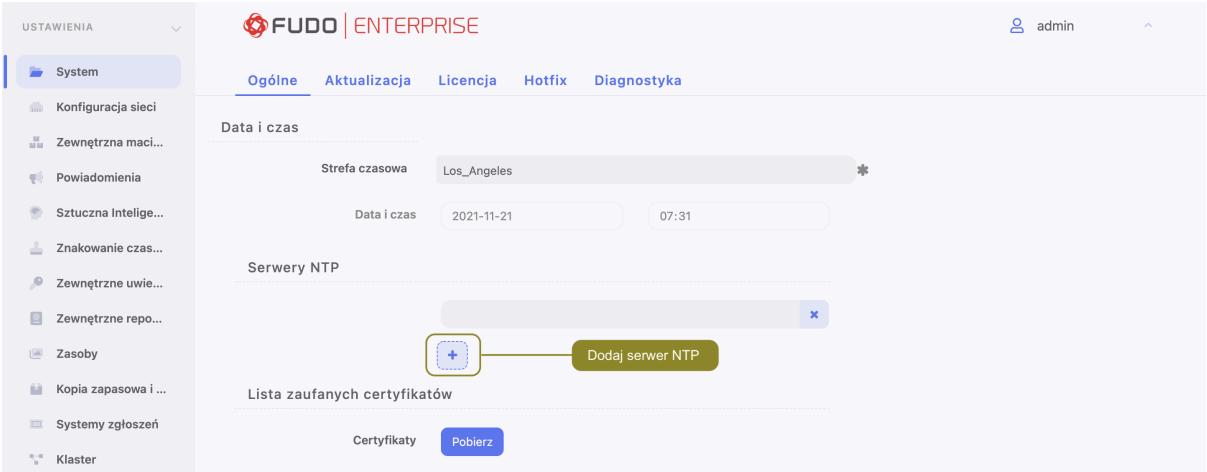
Konfiguracja serwerów czasu

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 użyktownika opcję *Uruchom ponownie*.

Modyfikowanie serwera NTP

Aby zmodyfikować serwer NTP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.

2. Wyszukaj i zmodyfikuj żądany wpis w sekcji *Serwery NTP*.
3. Kliknij *Zapisz*.
4. Wybierz z menu użyktownika opcję *Uruchom ponownie*.

Usuwanie serwera NTP

Aby usunąć serwer NTP, postępuj zgodnie z poniższą instrukcją.

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

Tematy pokrewne:

- *Znakowanie czasem*

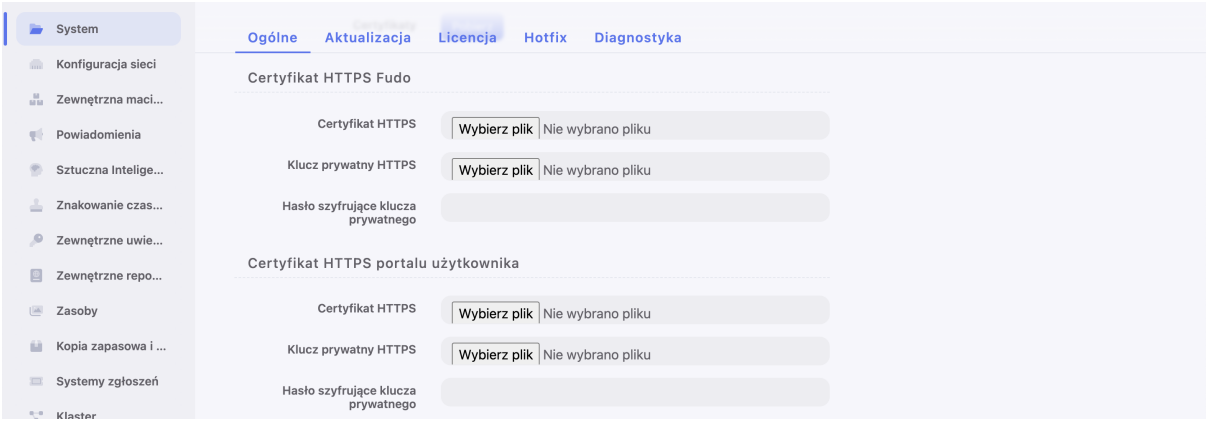
22.1.2 Certyfikaty HTTPS

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 *Przeglądaj* w polu *Klucz prywatny HTTPS* i wskaż w systemie plików definicję klucza prywatnego SSL.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Bezpieczeństwo*
- *Zarządzanie serwerami*

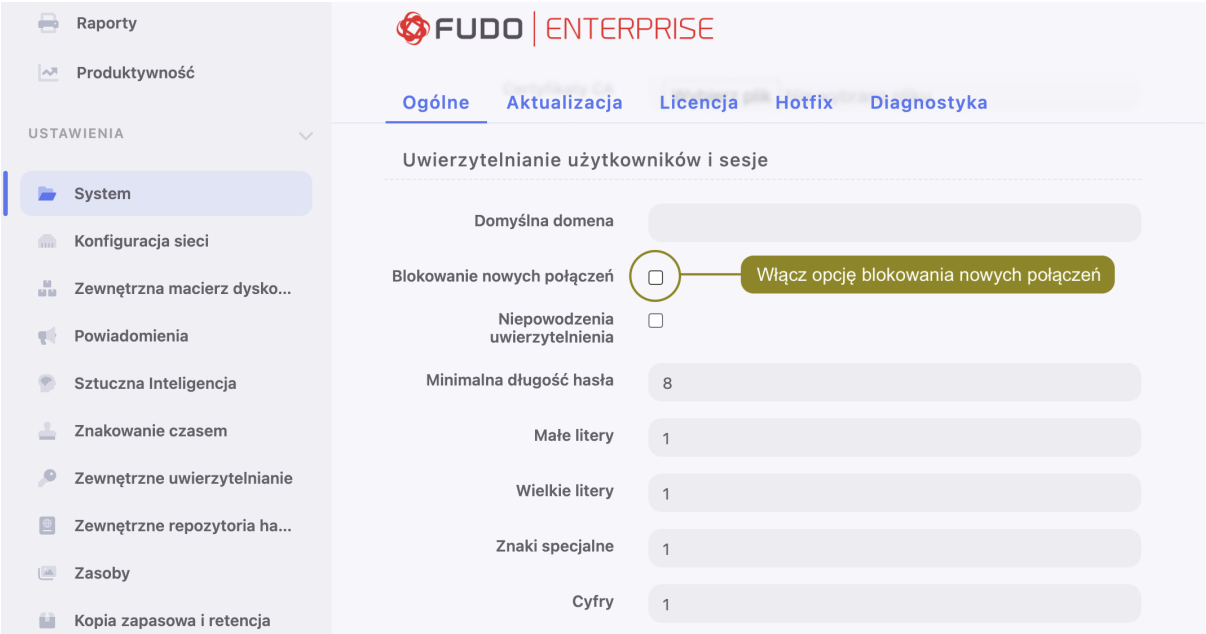
22.1.3 Blokowanie nowych połączeń

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*.



3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*

22.1.4 Dostęp SSH

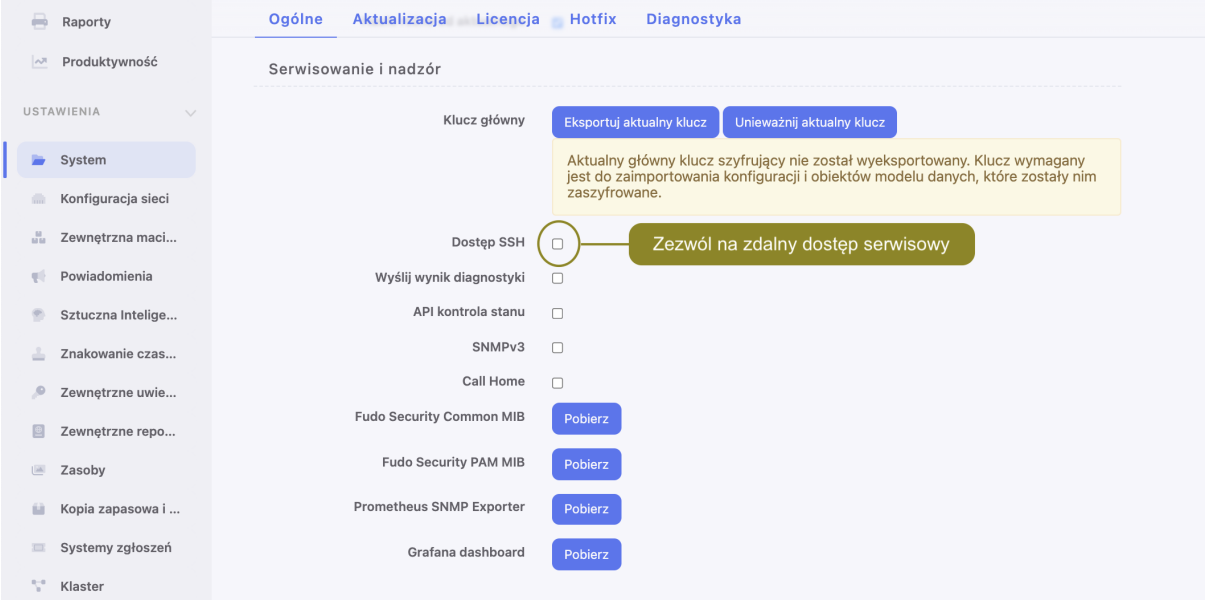
Opcja umożliwia zdalny dostęp serwisowy do Fudo Enterprise za pośrednictwem protokołu SSH.

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

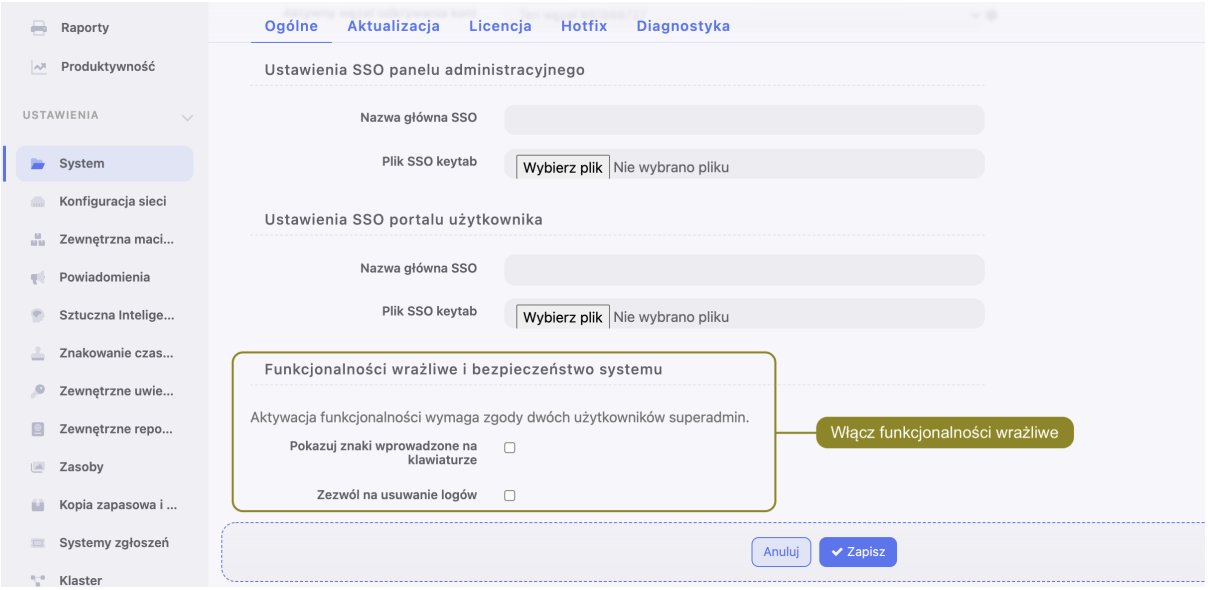
Funkcjonalności wrażliwe to zestaw opcji, których włączenie wymaga decyzji dwóch użytkowników o roli `superadmin`.

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 węźlę podrzędnym.

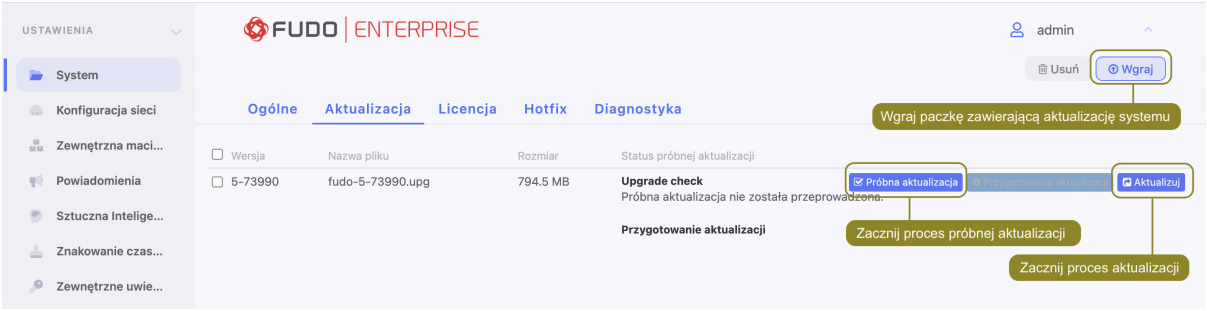
22.1.6.1 Aktualizowanie systemu

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*.

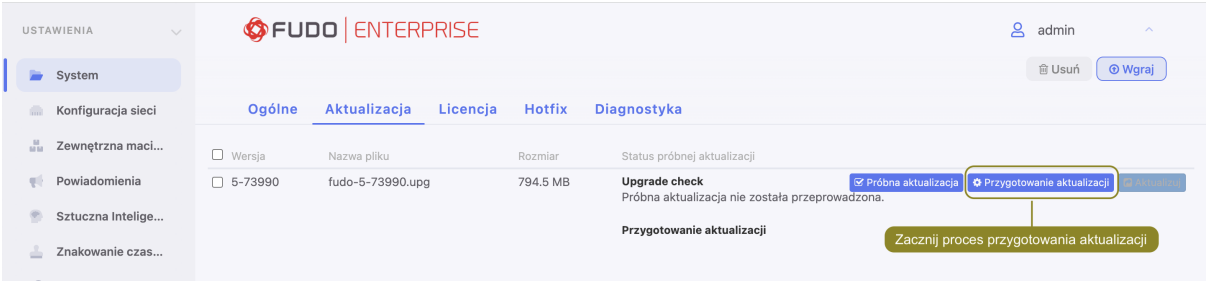
1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Aktualizacja*.
3. Kliknij *Wgraj*.
4. Wskaż plik zawierający aktualizację systemu (`.upg`).
5. Opcjonalnie, kliknij *Próbna aktualizacja* przy wybranym pliku obrazu, aby stwierdzić, czy obiekty modelu danych i bieżąca konfiguracja 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*.



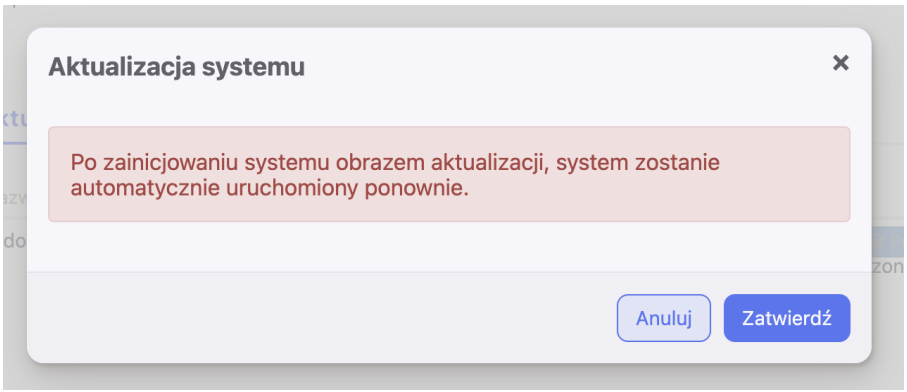
Informacja:

- 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.

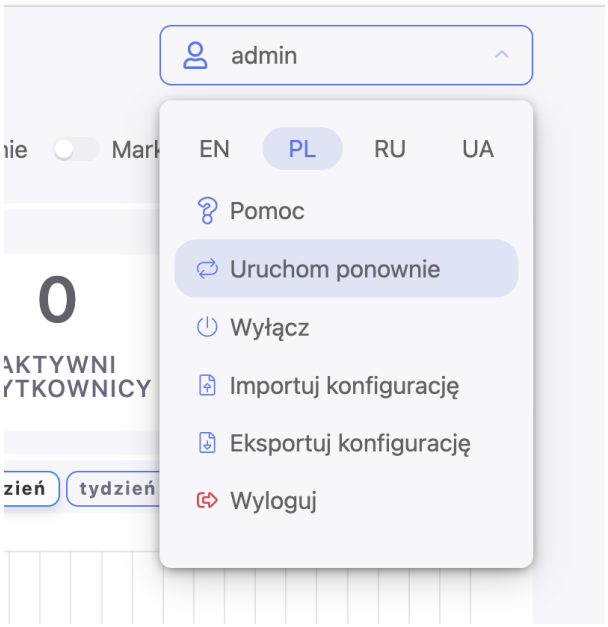
8. Kliknij *Zatwierdź*, aby wykonać aktualizację.

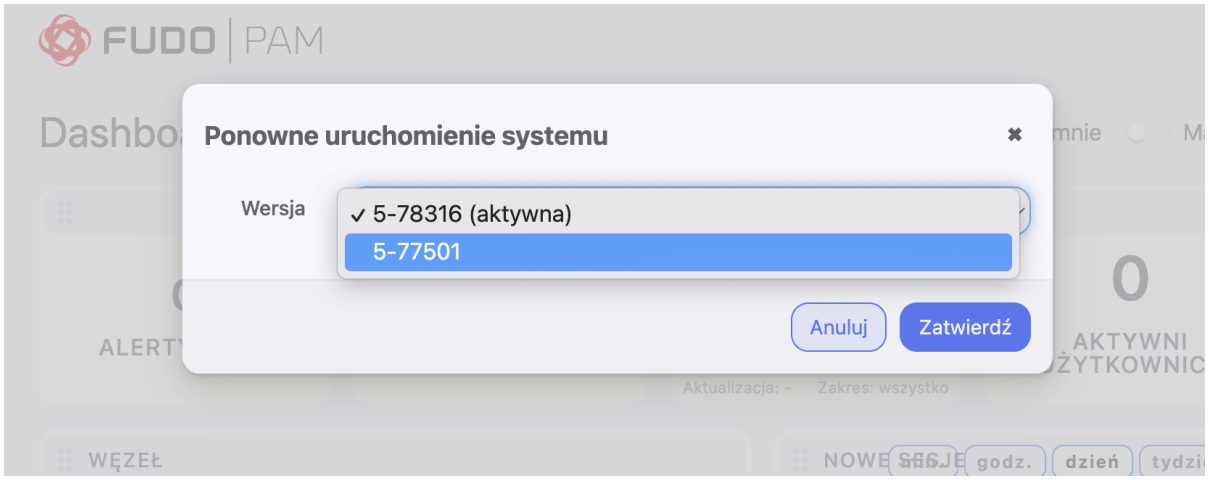


Informacja: Jeśli przed aktualizacją została włączona opcja systemowa *Blokowanie nowych połączeń*, pamiętaj żeby wyłączyć ją po ponownym uruchomieniu systemu.

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 jakiekolwiek hasła zostały zmienione podczas korzystania z nowszej wersji, przywrócenie poprzedniej wersji spowoduje utratę dostępu do wybranych systemów.

Jeśli zostanie wybrana aktywna wersja, odbędzie się ponowne uruchomienie systemu, według opisu na stronie *Ponowne uruchomienie systemu*.

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

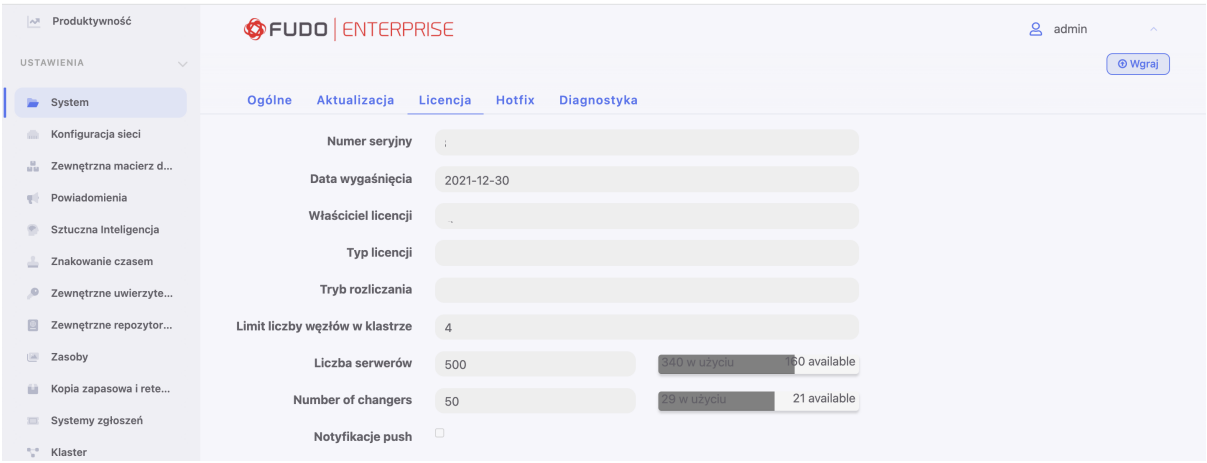
Wgrywanie licencji

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.

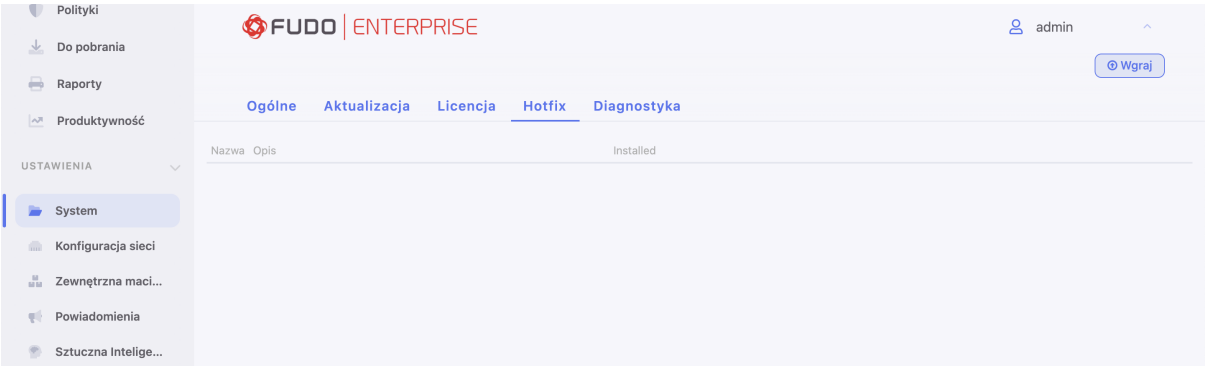
Tematy pokrewne:

- *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:

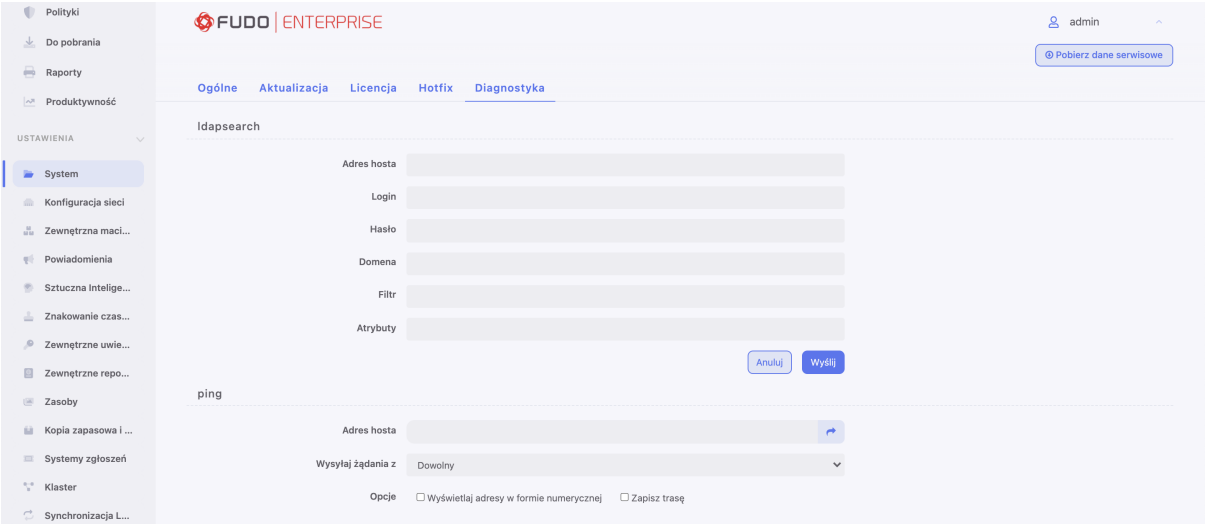
- *Aktualizacja systemu*
- *System*

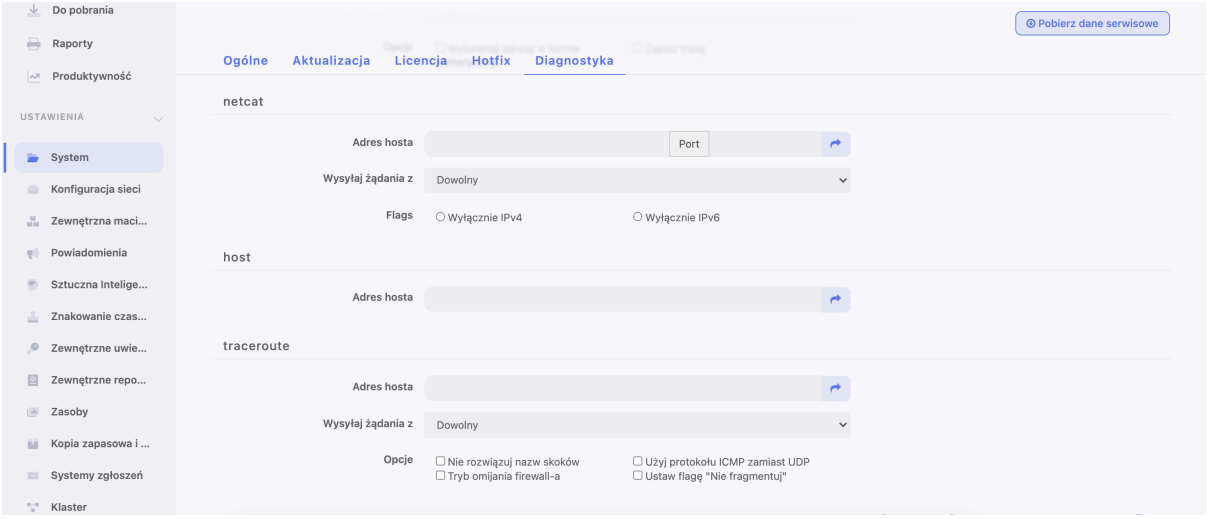
22.1.9 Diagnostyka

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 żądaną komendę, wprowadź parametry wykonania i kliknij przycisk wykonania komendy.




Do pobrania
Raporty
Produktywność
USTAWIENIA
System
Konfiguracja sieci
Zewnętrzna maci...
Powiadomienia
Sztuczna Intelige...
Znakowanie czas...
Zewnętrzne uwie...
Zewnętrzne repo...
Zasoby
Kopia zapasowa i ...
Systemy zgłoszeń
Klaster
Pobierz dane serwisowe
Ogólne
Aktualizacja
Licencja
Hotfix
Diagnostyka
netcat
Adres hosta
Port
Wysyłaj żądania z
Dowolny
Flags
Wyłącznie IPv4
Wyłącznie IPv6
host
Adres hosta
traceroute
Adres hosta
Wysyłaj żądania z
Dowolny
Opcje
Nie rozwiązuj nazw skoków
Tryb omijania firewall-a
Użyj protokołu ICMP zamiast UDP
Ustaw flagę "Nie fragmentuj"

Komenda/ parametr	Opis
LDAP search	Narzędzie umożliwia bezpośrednie wysłanie zapytania do serwera LDAP.
Adres hosta	Adres IP serwera LDAP.
Login	Login użytkownika uprawnionego do przeglądania zawartości katalogu.
Hasło	Hasło użytkownika uprawnionego do przeglądania zawartości katalogu.
Domena	Domena, w której znajdują się żądane obiekty.
Filtr	Parametr filtrowania obiektów.
Atrybuty	Atrybuty zapytania LDAP.
Ping	Ping wysyła sekwencję 10 pakietów icmp do wskazanego hosta.
Wyświetlaj adresy w formie numerycznej	Nie rozwiązuje adresu IP hosta do nazwy mnemonicznej.
Zapisz trasę	Umożliwia śledzenie trasy pakietów.
netcat	Netcat służy do nawiązywania połączeń ze zdalnym hostem na określonym numerze portu.
host	Polecenie host służy sprawdzeniu czy serwer DNS prawidłowo rozwiązuje nazwę maszyny docelowej.
traceroute	Komenda służy ustaleniu trasy, którą pokonują pakiety pomiędzy Fudo Enterprise i hostem docelowym.
Nie rozwiązuj nazw skoków	Adresy kolejnych punktów przeskoku nie będą rozwiązywane do nazw mnemonicznych.
Użyj protokołu ICMP zamiast UDP	Wymusza użycie pakietów UDP zamiast ICMP.
Tryb omijania firewall-a	Wymusza użycia niezmiennych numerów portu dla pakietów UDP i TCP. Port docelowy nie jest inkrementowany z każdym wysłanym pakietem.
Ustaw flagę „Nie fragmentuj”	Nie pozwala na fragmentację pakietów, w przypadku gdy przesyłany pakiet przekracza zdefiniowaną dla sieci wartość MTU (Maximum Transmission Unit). W przypadku przekroczenia MTU, zwrócony zostanie błąd.

Tematy pokrewne:

- *Rozwiązywanie problemów*

22.1.10 Szyfrowanie konfiguracji

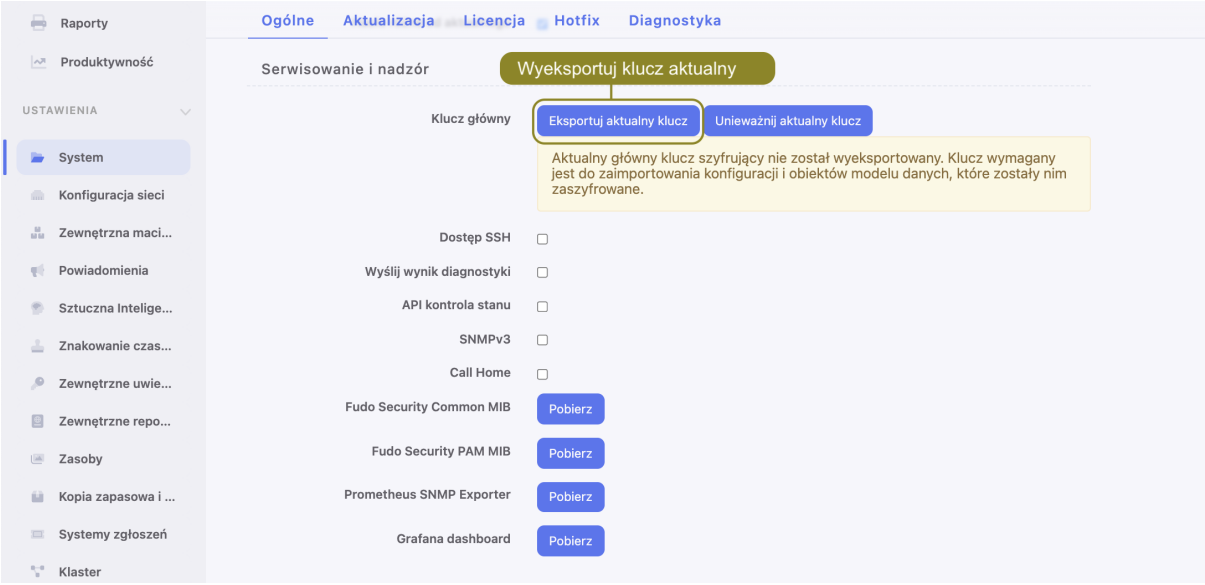
Główny klucz szyfrujący zapewnia bezpieczeństwo i poufność danych konfiguracyjnych, kopii zapasowych systemu i zewnętrznych wolumenów przechowywania danych. Klucz umożliwia również odzyskanie klucza szyfrującego wewnętrznego wolumenu danych w przypadku zaginięcia lub uszkodzenia kluczy zapisanych na 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 poskutkuje wygenerowaniem nowego klucza i ponownym zaszyfrowaniem danych.

Eksportowanie klucza głównego

1. Wybierz *Ustawienia* > *System*.
2. W sekcji *Serwisowanie i nadzór*, kliknij *Eksportuj aktualny klucz*.



3. Kliknij *Wybierz plik*, i wskaż plik z certyfikatem do zaszyfrowania klucza.

Informacja:

- Wygeneruj certyfikat i plik CSR (Certificate Signing Request) narzędziem `openssl`:

```
openssl req -newkey rsa:4096 -keyout privkey.pem -out req.pem
```

```
openssl req -nodes -newkey rsa:4096 -keyout privkey.pem -out req.pem # Do not prompt for a password.
```

- Podpisz wygenerowany plik CSR:

```
openssl x509 -req -in req.pem -signkey privkey.pem -out cert.pem
```

---

4. Kliknij *Zatwierdź* i zapisz plik z kluczem.

Unieważnienie klucza głównego

W przypadku skompromitowania *klucza głównego*, należy go unieważnić, co poskutkuje wygenerowaniem nowego klucza i ponownym zaszyfrowaniem danych.

1. Wybierz *Ustawienia* > *System*.
2. W sekcji *Serwisowanie i nadzór*, kliknij *Unieważnij aktualny klucz*.

3. Kliknij *Zatwierdź*.
4. Pamiętaj o konieczności *wyeksportowania nowego klucza*.

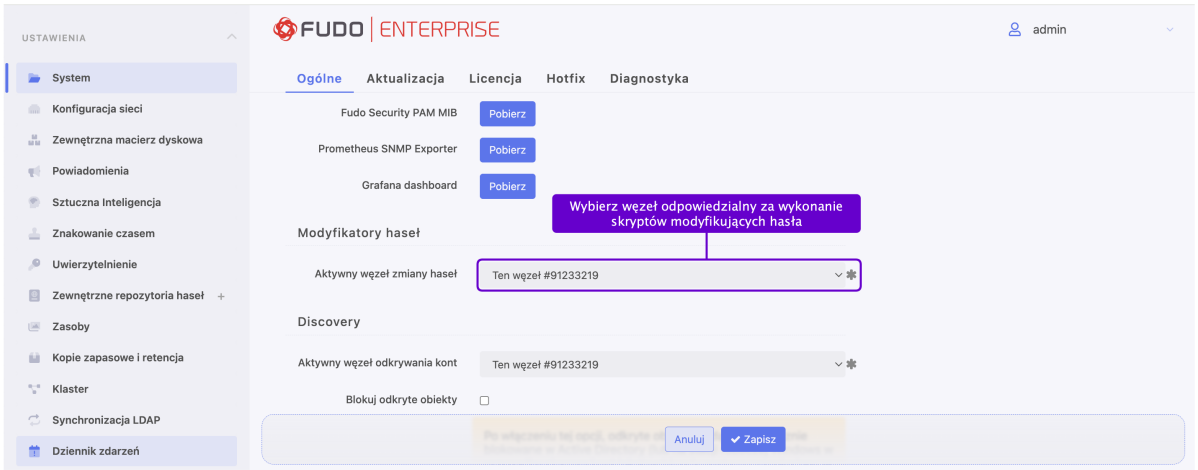
Tematy pokrewne:

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

22.1.11 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*.

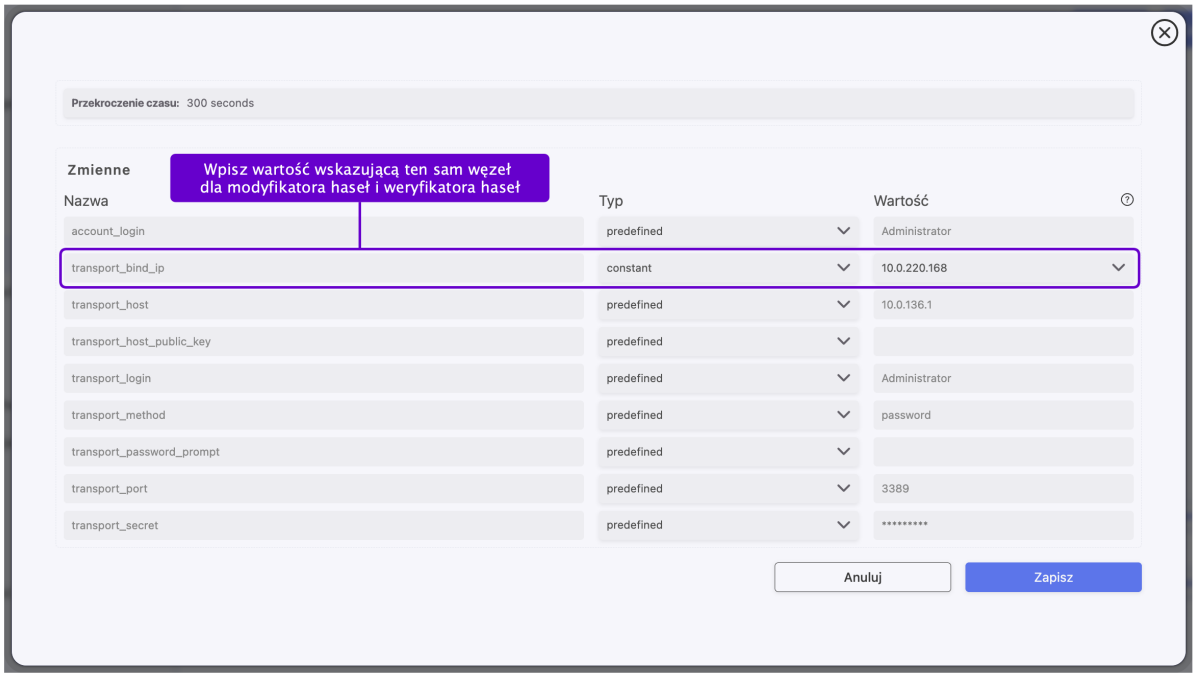
Informacja: W sytuacji, w której wskazany węzeł ulegnie awarii, zadanie zmiany haseł nie zostanie automatycznie podjęte przez inną instancję Fudo Enterprise. Automatyczna zmiana haseł wymaga zmiany przypisania aktywnego węzła lub przywrócenie działania uszkodzonej jednostki.

22.1.11.1 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 węźle, wskazanym jako *aktywny węzeł klastra dla Modyfikatorów haseł*.

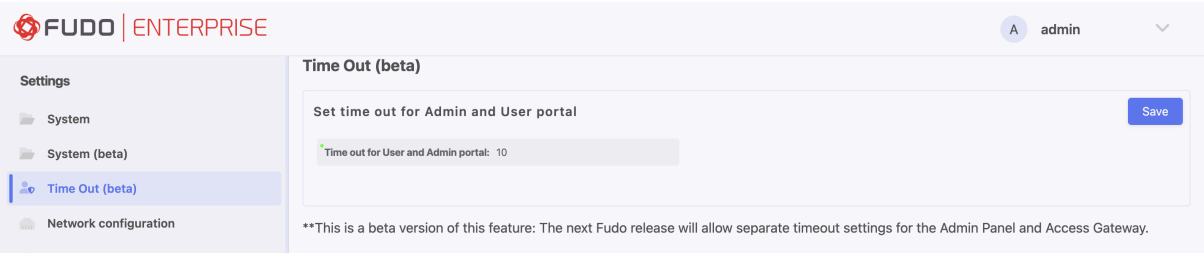
Tematy pokrewne:

- *Modyfikatory haseł*
- *Uniwersalne modyfikatory haseł*

22.2 Limit Czasu

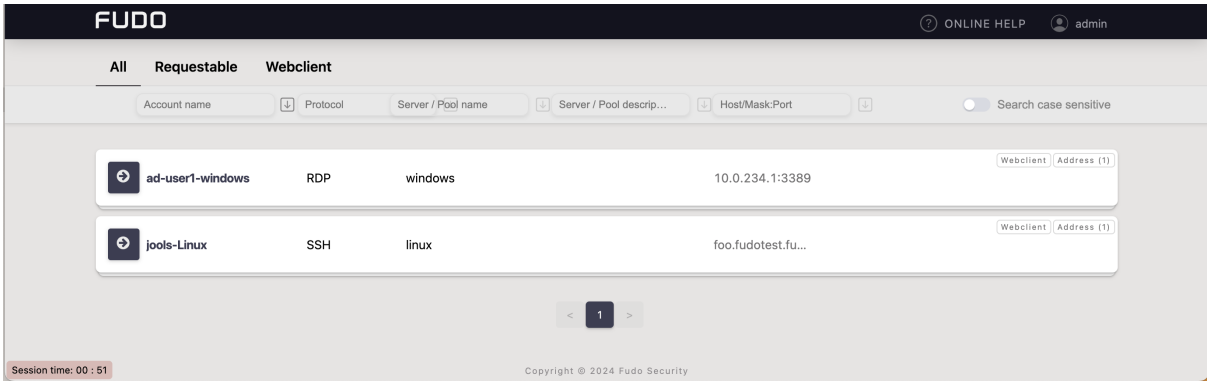
Funkcja **Limit Czasu** pozwala administratorom na ustawienie limitu czasowego nieaktywności dla Panelu Administracyjnego i Portalu Użytkownika. Funkcja ta zapewnia automatyczne wylogowanie użytkowników po określonym czasie nieaktywności, co zwiększa bezpieczeństwo systemu.

1. Przejdź do *Ustawienia > Limit Czasu*.
2. W polu *Limit czasu dla Panelu Admina i Portalu Użytkownika* wpisz czas trwania nieaktywności w minutach.
3. Kliknij *Zapisz*, aby zastosować ustawienia.



Informacja: Jest to wersja beta tej funkcji: W kolejnej wersji Fudo Enterprise zostanie wprowadzona możliwość oddzielnej konfiguracji limitów czasowych dla Panelu Administracyjnego oraz Portalu Użytkownika.

Po skonfigurowaniu ustawień limitu czasu, w Portalu Użytkownika pojawi się licznik, który będzie odmierzał czas pozostały do automatycznego wylogowania.



Powiązane tematy:

- *Dashboard: Nie wylogowuj mnie*

22.3 Konfiguracja sieci

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

22.3.1 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.

22.3.1.1 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.

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 jest **ostatnią wersją wspierającą DHCP,** które zostanie wycofane w kolejnym wydaniu.

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.

22.3.1.2 Ustawianie adresu IP z konsoli

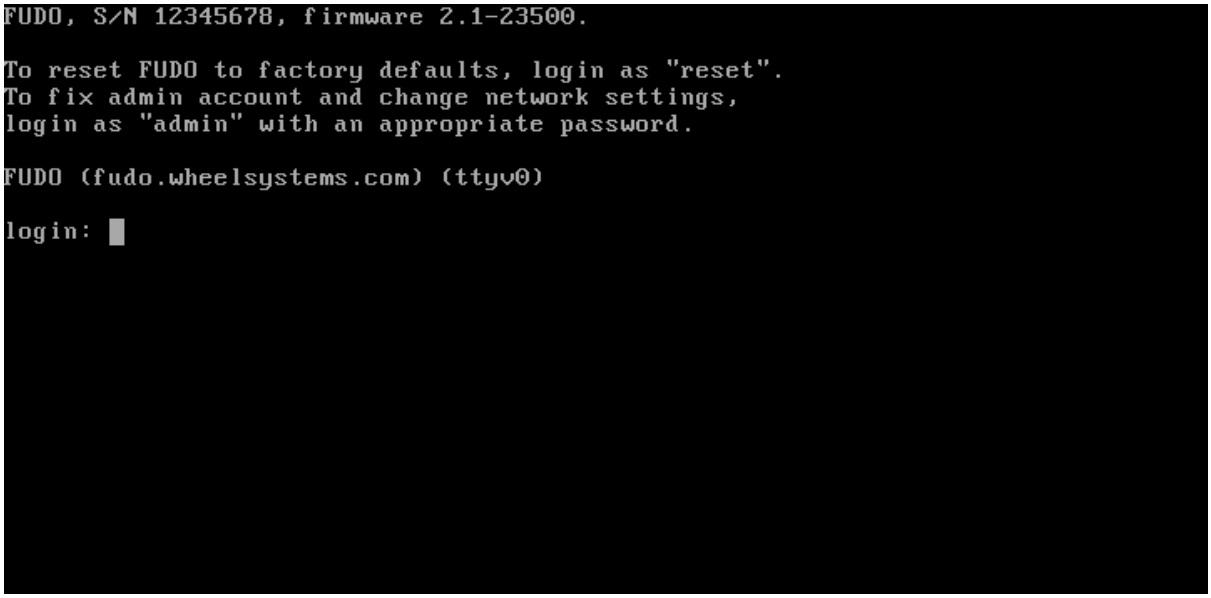
W sytuacji braku możliwości zalogowania się do zdalnego panelu administracyjnego, adres IP może zostać skonfigurowany z poziomu konsoli urządzenia.

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

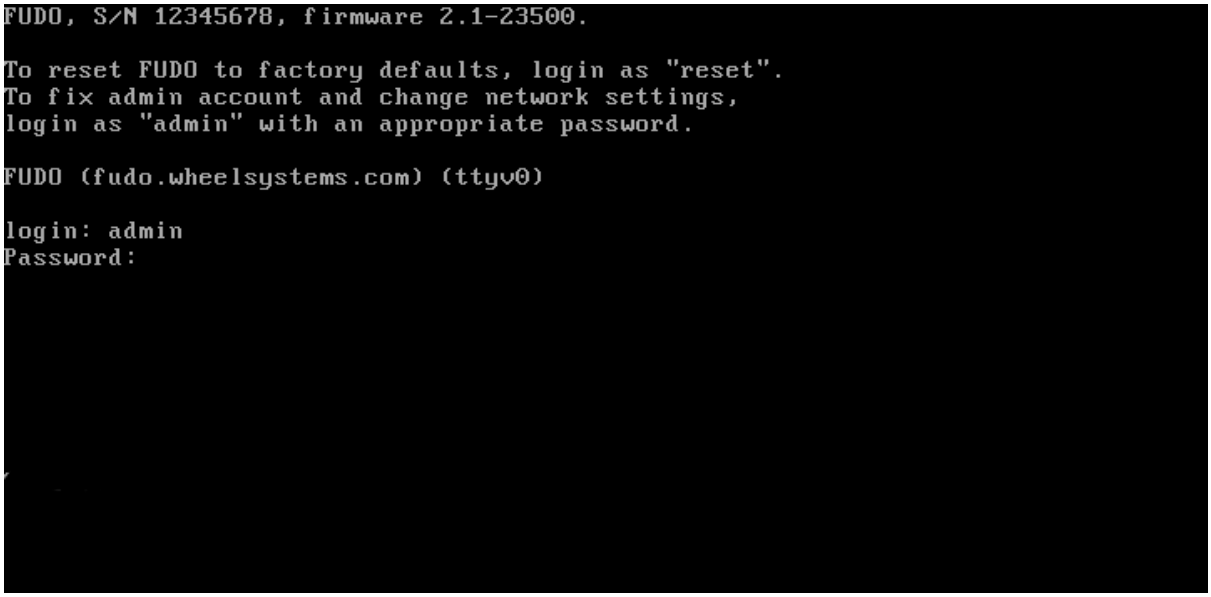
Informacja: Domyślne dane logowania:

login: admin
hasło: proxycrypto

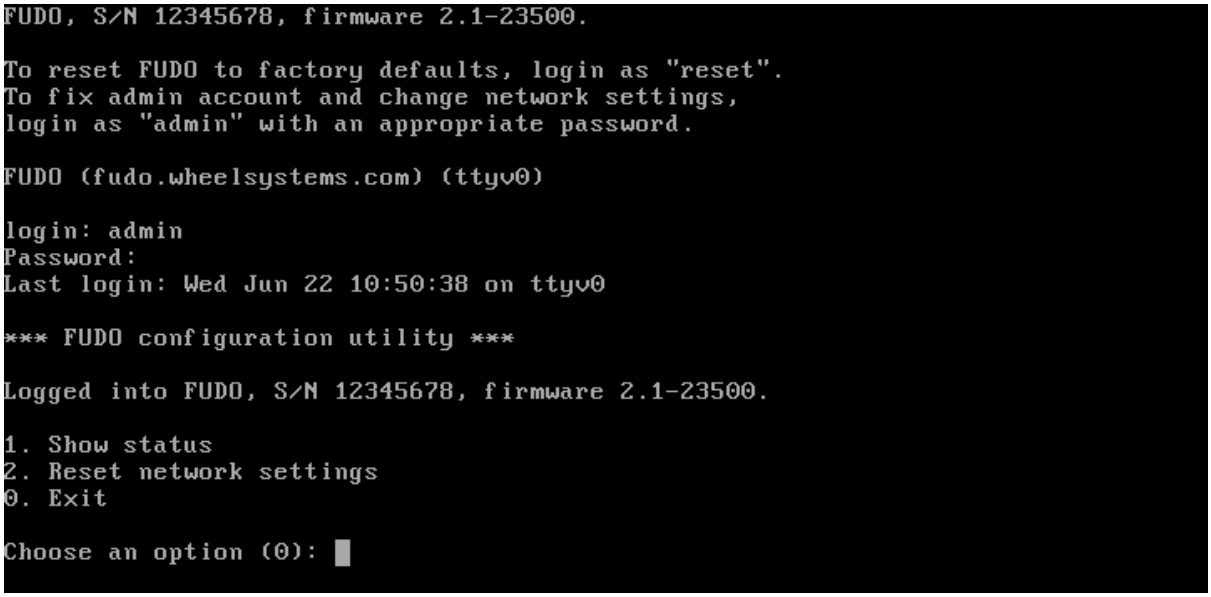
Dla wersji w chmurze domyślnym hasłem jest zazwyczaj identyfikator maszyny wirtualnej dostarczanej z Fudo Enterprise. Skontaktuj się ze sprzedawcą lub wsparciem technicznym, aby dowiedzieć się więcej.



3. Wprowadź hasło do konta administratora.



4. Wpisz 2 i naciśnij klawisz *Enter*.



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

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

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

FUDO (fudo.wheelsystems.com) (ttyv0)

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

*** FUDO configuration utility ***

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

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

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

6. Wprowadź nazwę interfejsu zarządzającego (poprzez interfejs zarządzający udostępniany jest panel administracyjny Fudo 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):
```

22.3.1.3 Konfigurowanie mostu sieciowego

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

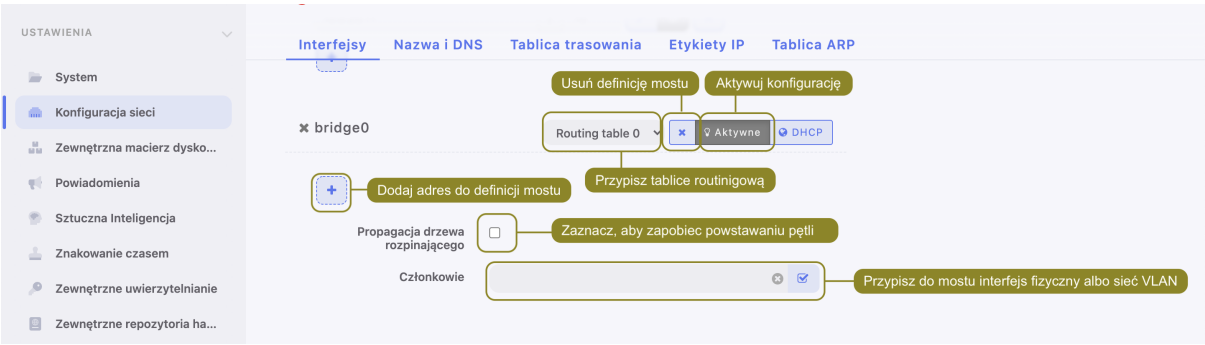
Aby stworzyć most sieciowy, postępuj zgodnie z poniższą instrukcją.

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

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

---

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



22.3.1.4 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.

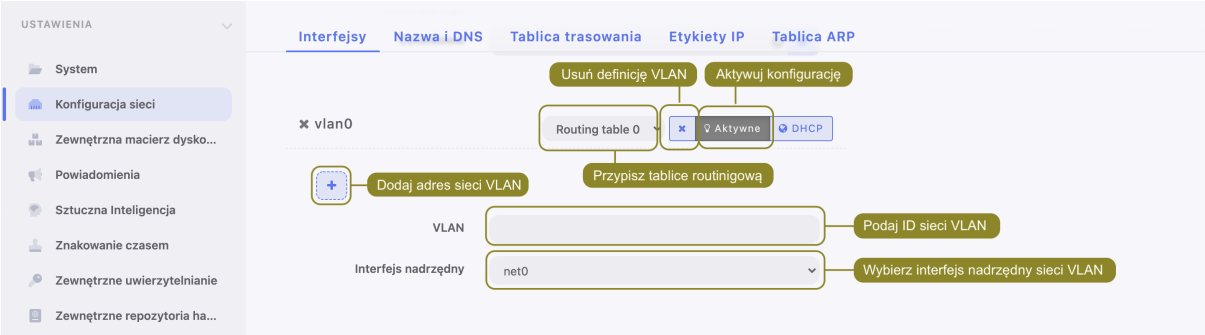
Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 jest **ostatnią wersją wspierającą DHCP,** które zostanie wycofane w kolejnym wydaniu.

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

---

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



22.3.1.5 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*

22.3.2 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.

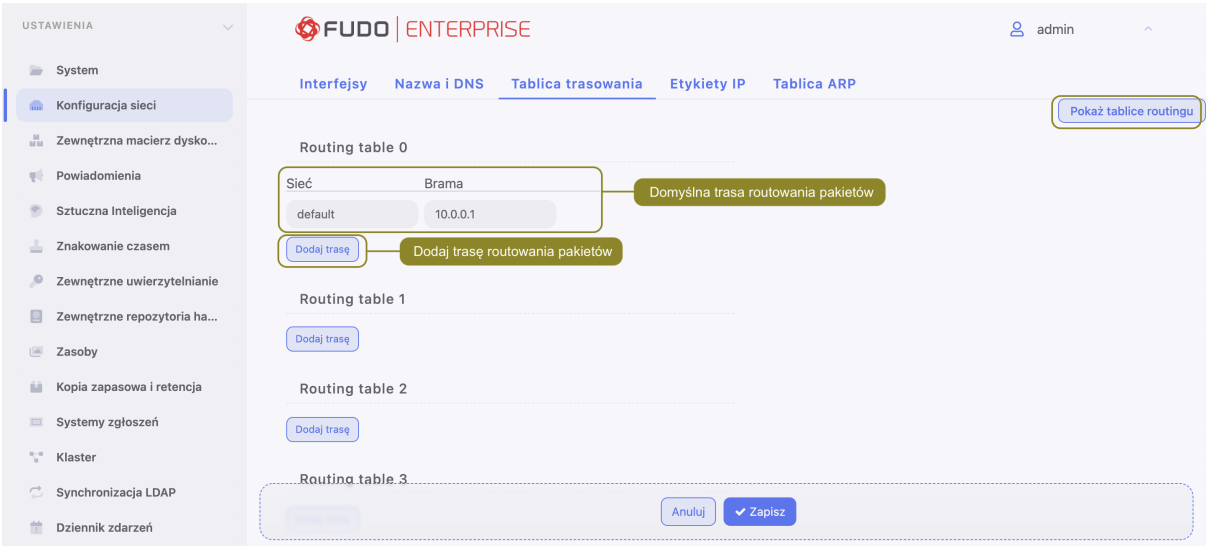
Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*
- *Uwierzytelnienie*
- *Serwery*
- *Gniazda nasłuchiwania*

22.3.3 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.

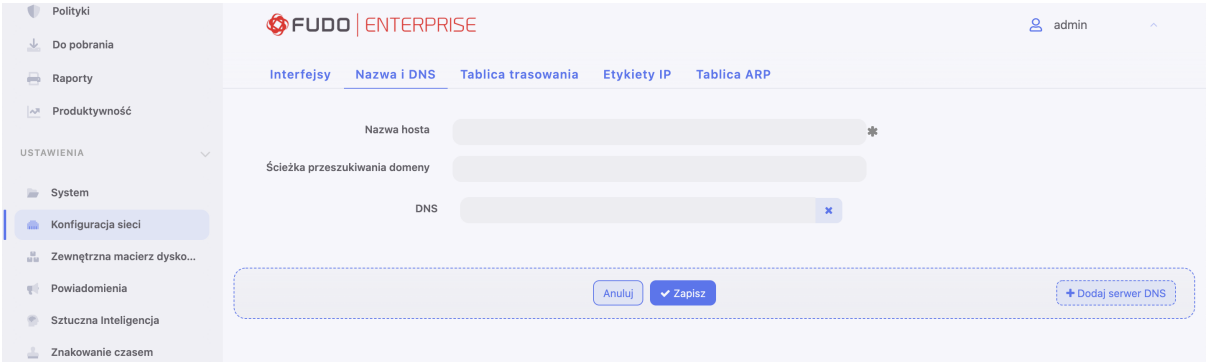
1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Tablica trasowania*.
3. Zaznacz opcję usunięcia wybranej trasy routingu i kliknij *Zapisz*.

Tematy pokrewne:

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

22.3.4 Konfiguracja DNS

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



Ścieżka domeny wyszukiwania

Domena wyszukiwania umożliwia identyfikowanie hostów na podstawie nazwy skróconej. Na przykład wskazanie domeny wyszukiwania `tech.whl` pozwala na wskazanie hosta docelowego w postaci `ftp` zamiast `ftp.tech.whl`.

Aby dodać domenę wyszukiwania, postępuj zgodnie z poniższą instrukcją.

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

2. Przejdź do zakładki *Nazwa i DNS*.
3. W polu *Ścieżka przeszukiwania domeny*, wprowadź domenę domyślną, np. `tech.whl`.

Informacja:

- Aby zdefiniować więcej niż jedną wartość, wprowadź żądane domeny oddzielając je znakiem spacji, na przykład: `tech.whl wheel.com`.
- Implementacja protokołu pozwala na zdefiniowanie do sześciu ścieżek przeszukiwania.

---

4. Kliknij *Zapisz*.

Dodawanie serwera DNS

Aby dodać serwer DNS, postępuj zgodnie z poniższą instrukcją.

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

Modyfikowanie serwera DNS

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

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

Usuwanie serwera DNS

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

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

---

1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Nazwa i DNS*.
3. Wyszukaj i kliknij opcję usunięcia wybranego wpisu.
4. Kliknij *Zapisz*.

Tematy pokrewne:

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

22.3.5 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:

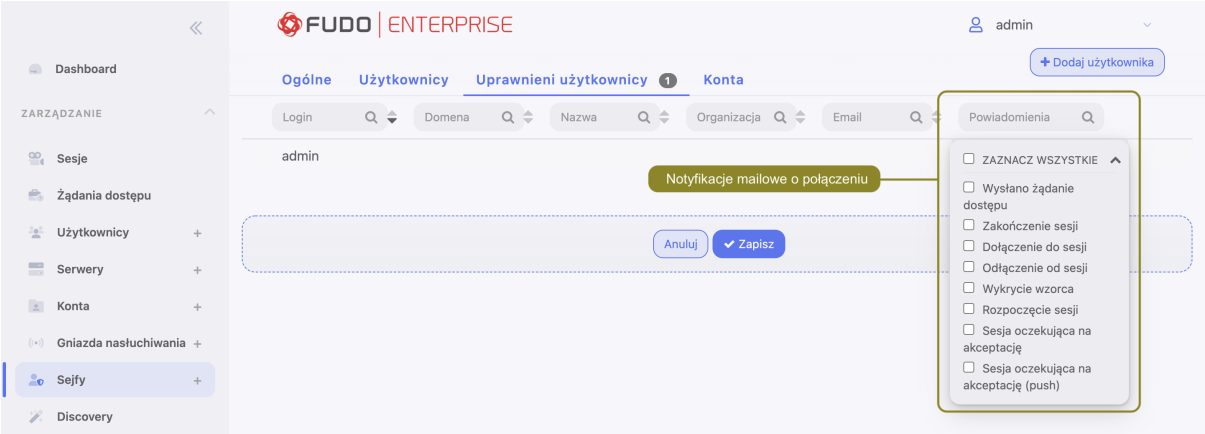
- *Konfiguracja interfejsów sieciowych*
- *Konfiguracja serwerów czasu*

22.4 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.

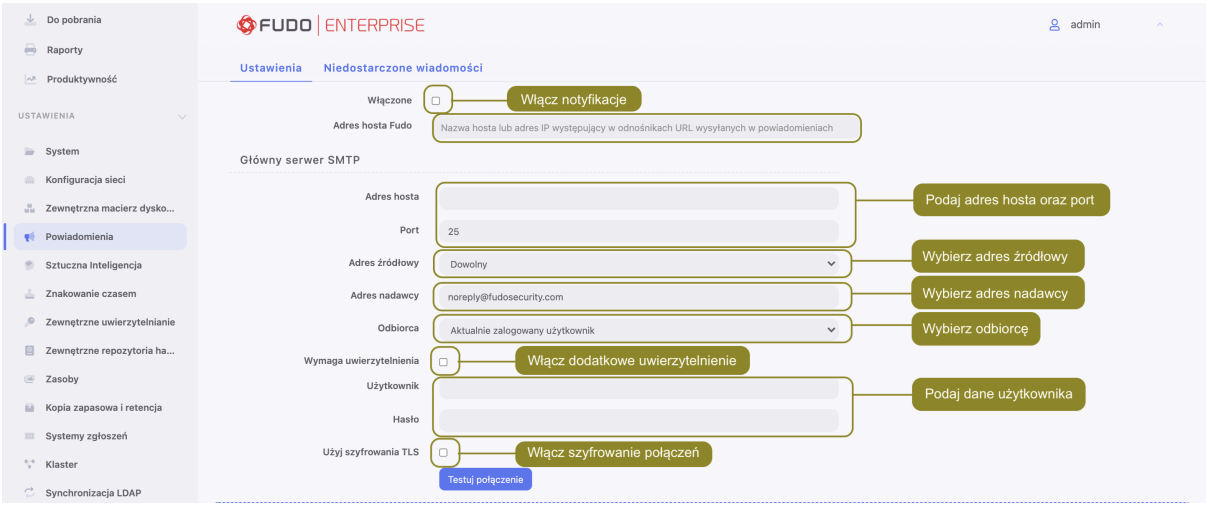
Wysyłanie powiadomień wymaga skonfigurowania serwera poczty SMTP.

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.

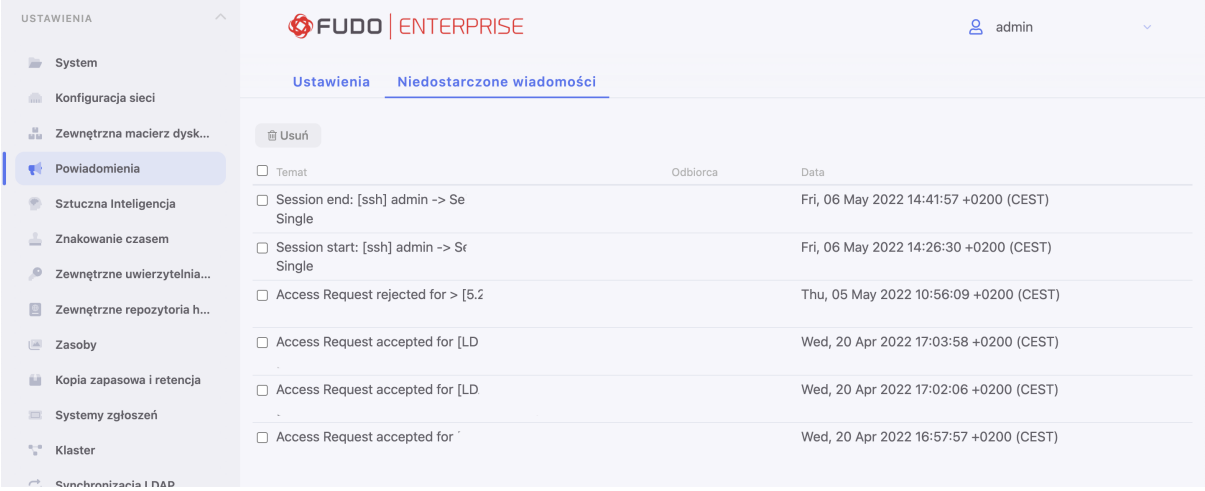


Parametr	Opis
Adres hosta	Adres serwera SMTP, na przykład `smtp.gmail.com`.
Port	Numer portu, na którym działa usługa SMTP.
Adres źródłowy	Adres IP albo adres interfejsu serwera SMTP.
Adres nadawcy	Adres email, z którego wysyłane będą powiadomienia.
Odbiorca	Adresat wiadomości testowej.
Wymaga uwierzytelnienia	Czy serwer SMTP wymaga uwierzytelniania.
Użytkownik	Nazwa użytkownika dla uwierzytelnienia usługi SMTP.
Hasło	Hasło użytkownika dla uwierzytelnienia usługi SMTP.
Użyj bezpiecznych połączeń (TLS)	Zaznacz, jeśli serwer pocztowy wykorzystuje protokół szyfrujący TLS. Dodatkowo zaznacz opcję *Użyj STARTTLS*, jeśli serwer pocztowy ma zapewnić bezpieczne połączenie.

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

5. Kliknij  w celu wgrania certyfikatu urzędu certyfikacji. Wybierz format wyświetlenia wartości SHA1 albo MD5.
6. Kliknij *Zapisz*.

Aby zobaczyć listę wiadomości, które nie zostały dostarczone do odbiorcy z jakiegoś powodu, wybierz pod-zakładkę **Niedostarczone wiadomości**. W ten sposób możesz zareagować na problem oraz go naprawić, by użytkownicy mogli dostawać powiadomienia w przyszłości.



Tematy pokrewne:

- *Konta*

22.5 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 widgecie Podejrzane sesje na Dashboard'zie. Widget 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, przekierowującym do podejrzanego segmentu sesji w playerze.

22.5.1 Konfiguracja trenera modeli

Trenowanie modeli wymaga zaangażowania zasobów obliczeniowych. Odpowiednia konfiguracja systemu pozwoli na efektywne przetwarzanie archiwum sesji, przy zachowaniu responsywności systemu w obsłudze bieżących połączeń.

Aby zmienić konfigurację trenera modeli, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Sztuczna Inteligencja*.
2. W sekcji *Trener modeli*, w polu *Maksymalna liczba procesów* określ liczbę procesów odpowiedzialnych za przetwarzanie sesji w celu zbudowania modeli.

Informacja: Wartość domyślna jest wartością optymalną, określoną na podstawie dostępnych zasobów sprzętowych. Faktyczna liczba procesów trenujących modele jest nie większa niż liczba dostępnych rdzeni procesorów.

---

3. Z listy rozwijalnej *Aktywny węzeł klastra*, wybierz węzeł odpowiedzialny za trenowanie modeli.
4. Wybierz dni tygodnia, w które będzie odbywało się trenowanie modeli.
5. Zdefiniuj czas rozpoczęcia procesu trenowania.
6. Określ przedział czasowy analizowania sesji archiwalnych.

7. W sekcji *Parametry modelu ilościowego*, w polu *Tolerancja*, określ dopuszczalne wahania liczby sesji/czasu trwania sesji.

Informacja: Parametr tolerancji wykorzystywany jest przy wyliczaniu ryzyka. Wartość tolerancji jest odejmowana od bieżącej liczby połączeń, a wyrażona w minutach, od czasu trwania pojedynczego połączenia.

---

8. W polu *Próg raportowania* zdefiniuj dopuszczalne odchylenie od spodziewanych wartości.

Informacja: Wyrażony w procentach, próg raportowania określa wartość progową przy której wyzwalany jest alarm bezpieczeństwa związany z nadzwyczaj dużą liczbą sesji lub dłuższym niż typowy czasem trwania pojedynczego połączenia.

Np. próg raportowania wyznaczony na 1% spowoduje wyzwolenie alarmu w sytuacji, w której liczba połączeń odbiegająca od wartości spodziewanej została zaobserwowania w 1% przypadków.

9. W sekcji *Analiza sesji*, w polu *Liczba procesów analizujących* określ liczbę procesów odpowiedzialnych za bieżącą analizę połączeń. Dodatkowo, z listy rozwijanej *Rejestrowanie wyników* wybierz poziom zagrożenia, który chcesz rejestrować w dzienniku zdarzeń.

Informacja: W sytuacji, w której pula dostępnych procesów analizujących zostaje wyczerpana, bieżąca analiza danych zostaje wstrzymana. Po zakończeniu sesji, dane zostają przekazane do analizy.

10. Kliknij *Zapisz*.

22.5.2 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.

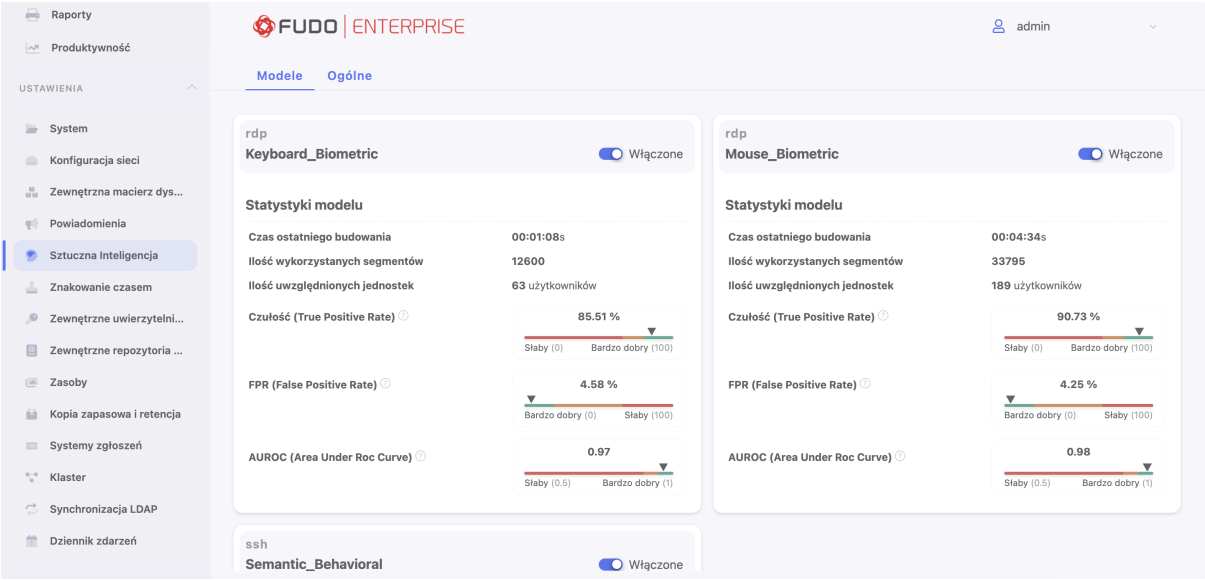
Ponieważ modele AI są oparte o protokoły (RDP oraz/lub SSH), aktywność użytkownika podczas sesji jest analizowana na podstawie funkcjonalności, które konkretny protokół umożliwia:

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*

22.6 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 *Tworzenie konta typu regular*).

Konfigurowanie usługi znakowania czasem

Informacja:

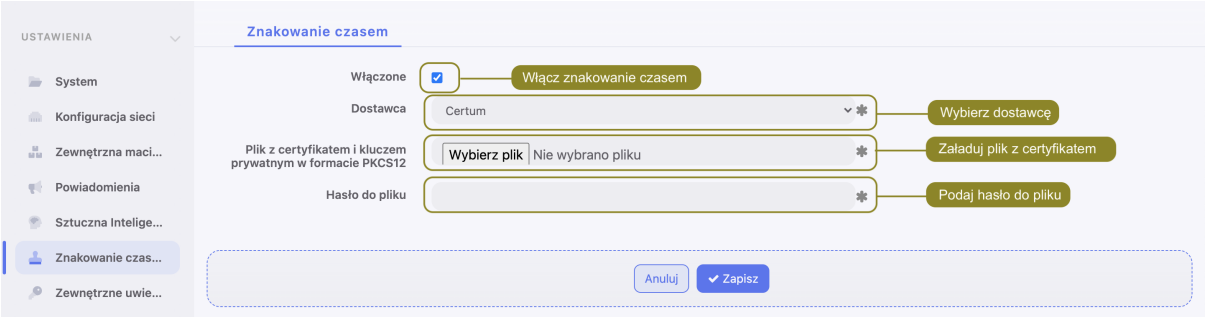
- Znacznikiem czasu zostaną opatrzone jedynie sesje, które zostały zakończone po włączeniu usługi.

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*

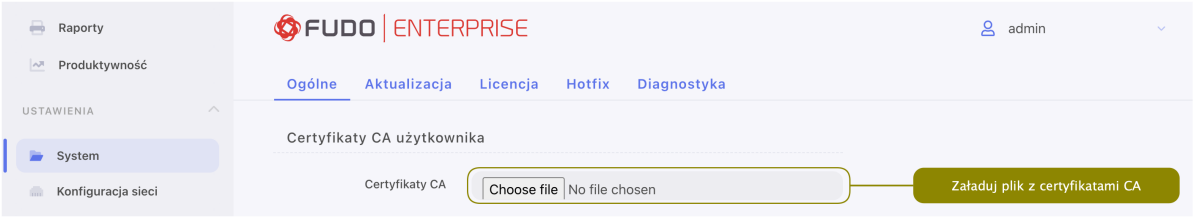
22.7 Model uwierzytelniania w oparciu o certyfikaty

Fudo Enterprise umożliwia logowanie certyfikatem do serwera docelowego. Certyfikat powinien być zgodny ze standardami PIV.

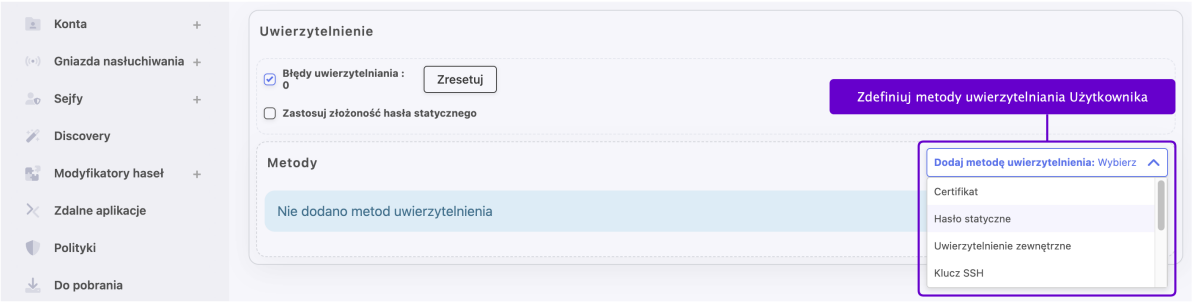
W celu konfiguracji certyfikatu jako metody uwierzytelnienia, postępuj zgodnie z instrukcją:

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.

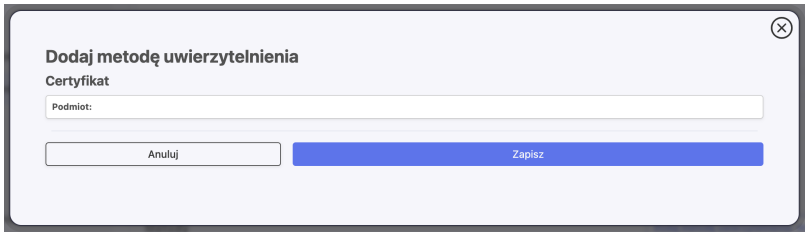


3. Kliknij *Zapisz*.
4. Wybierz *Zarządzanie* > *Użytkownicy* i edytuj użytkownika, dla którego chcesz skonfigurować metodę uwierzytelnienia `certyfikat`, lub utwórz nowego użytkownika przechodząc do menu *Zarządzanie* > *Użytkownicy* i klikając + *Dodaj użytkownika*.
5. W sekcji *Uwierzytelnienie* z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz typ *Certyfikat*.



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*

22.8 Uwierzytelnienie

Fudo Enterprise oferuje szeroki zakres metod uwierzytelniania dla weryfikacji użytkowników względem serwera docelowego. Obejmują one:

- Uwierzytelnianie zewnętrzne: *CERB*, *RADIUS*, *LDAP*, *Active Directory*
- Inne metody uwierzytelniania: *OATH*, *SMS*, *DUO*, *OpenID Connect*, *SSO*, *Kerberos*

22.8.1 Definicja serwera uwierzytelnienia zewnętrznego

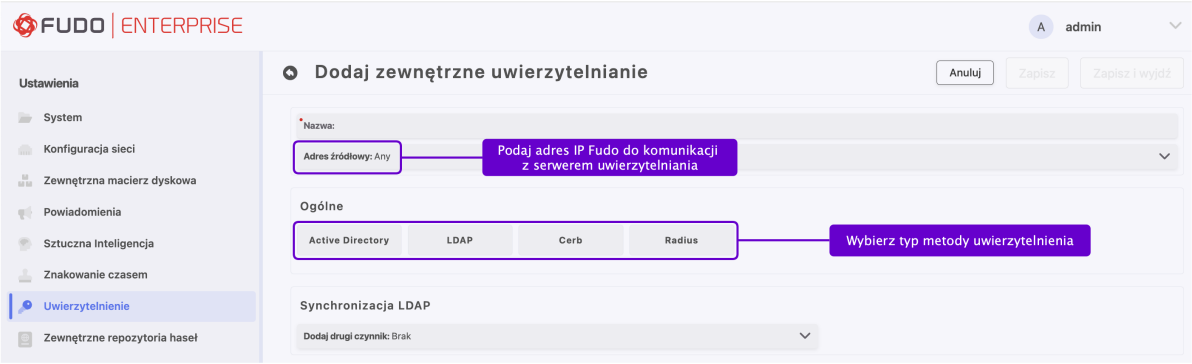
Aby dodać serwer uwierzytelnienia Active Directory, LDAP, Cerb lub Radius, postępuj zgodnie z poniższymi krokami.

1. Wybierz *Ustawienia* > *Uwierzytelnienie*.
2. Wybierz zakładkę **Uwierzytelnienie zewnętrzne**.
3. Kliknij + *Dodaj uwierzytelnienie zewnętrzne*.
4. Podaj nazwę dla tej konkretnej konfiguracji.
5. Wybierz *Bind address* - adres IP używany do wysyłania żądań do określonego hosta.

Informacja: W przypadku konfiguracji klastra wybierz **oznaczony adres IP** z listy rozwijanej *Bind address* i upewnij się, że inne węzły mają przypisane adresy IP do tej etykiety. Więcej informacji znajdziesz w temacie *Etykiety adresów IP*.

---

6. W sekcji *Ogólne* wybierz typ usługi uwierzytelnienia: `Active Directory`, `LDAP`, `CERB` lub `Radius`.



7. Podaj parametry konfiguracyjne w zależności od wybranego typu systemu uwierzytelnienia zewnętrznego.
8. Kliknij *Zapisz*.

Opisy pól i konfiguracja na podstawie wybranej metody

Active Directory

Parametr	Opis
Host	Adres IP serwera.
Port	Numer portu, na którym nasłuchuje usługa AD.
Domena Active Directory	Domena, w oparciu o którą będzie wykonywane uwierzytelnienie w serwerze Active Directory.
TLS włączony	Ta opcja jest konieczna do zaznaczenia, aby użytkownicy domenowi mogli zmieniać hasło na Portalu Użytkownika.
Certifikat serwera / Certifikat CA	Certyfikat serwera Active Directory lub certyfikat CA. Dostępne, gdy aktywowana jest opcja *TLS włączony*.
Login konta uprzywilejowanego	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.
Dodaj drugi czynnik	Dodatkowy krok weryfikacji za pomocą metod uwierzytelnienia `OATH`, `SMS` lub `DUO`.

Informacja:

- Uwierzytelnienie przy użyciu Kerberosa jest pierwszym krokiem w przypadku korzystania z metody zewnętrznego uwierzytelnienia Active Directory.
- Ta funkcjonalność jest domyślnie włączona.
- Zapoznaj się z rozdziałem *Ustawienia uwierzytelniania Kerberos*, aby dowiedzieć się, jak wyłączyć to uwierzytelnienie.
- Jeśli uwierzytelnianie w **Active Directory** zostanie pomyślnie przeprowadzone za pomocą Kerberosa, skonfigurowany certyfikat nie zostanie użyty, ponieważ jest wykorzystywany tylko wtedy, gdy wymagane jest przejście na uwierzytelnianie za pomocą LDAP.

LDAP

Parametr	Opis
Host	Adres IP serwera.
Port	Numer portu, na którym nasłuchuje usługa LDAP.
Bind DN	Miejsce w strukturze katalogowej, w której zawarte są definicje użytkowników uwierzytelnianych w usłudze LDAP. Np. `dc=example, dc=com`
TLS włączony	Ta opcja jest konieczna do zaznaczenia, aby użytkownicy domenowi mogli zmieniać hasło na Portalu Użytkownika.
Certifikat serwera / Certifikat CA	Certyfikat serwera LDAP lub certyfikat CA. Dostępne, gdy aktywowana jest opcja *TLS włączony*.
Dodaj drugi czynnik	Dodatkowy krok weryfikacji za pomocą metod uwierzytelnienia `OATH`, `SMS` lub `DUO`.

Cerb

Parametr	Opis
Host	Adres IP serwera.
Port	Numer portu, na którym nasłuchuje usługa CERB.
Service (NAS ID)	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.
Dodaj drugi czynnik	Dodatkowy krok weryfikacji za pomocą metod uwierzytelnienia `OATH`, `SMS` lub `DUO`.

Radius

Parametr	Opis
Host	Adres IP serwera.
Port	Numer portu, na którym nasłuchuje usługa RADIUS.
NAS ID	Parametr, który zostanie przekazany w atrybucie NAS-Identifier do serwera RADIUS.
Sekret	Sekret serwera RADIUS służący szyfrowaniu haseł użytkowników.
Dodaj drugi czynnik	Dodatkowy krok weryfikacji za pomocą metod uwierzytelnienia `OATH`, `SMS` lub `DUO`.

Informacja: Należy pamiętać, że podczas konfigurowania uwierzytelnienia **Radius** w Fudo Enterprise obsługiwany jest tylko **Password Authentication Protocol (PAP)**.

Ostrzeżenie: Podczas wybierania dodatkowej metody uwierzytelnienia (`OATH`, `SMS` lub `DUO`) jako *Drugiego czynnika* dla synchronizacji z *Zewnętrznym serwerem uwierzytelnienia* (AD / LDAP / CERB / RADIUS), nie wystarczy po prostu wybrać jednego z *Zewnętrznych źródeł uwierzytelnienia* w definicji użytkownika. Dodatkowo wybrana metoda uwierzytelnienia powinna być skonfigurowana w definicji użytkownika jako podstawowa metoda uwierzytelnienia. Następnie metody uwierzytelnienia użytkowników będą automatycznie synchronizowane zgodnie z ustawieniami *Zewnętrznego serwera uwierzytelnienia*.

Tematy pokrewne:

- *Metody uwierzytelnienia użytkowników i tryby*
- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*
- *Integracja z serwerem CERB*

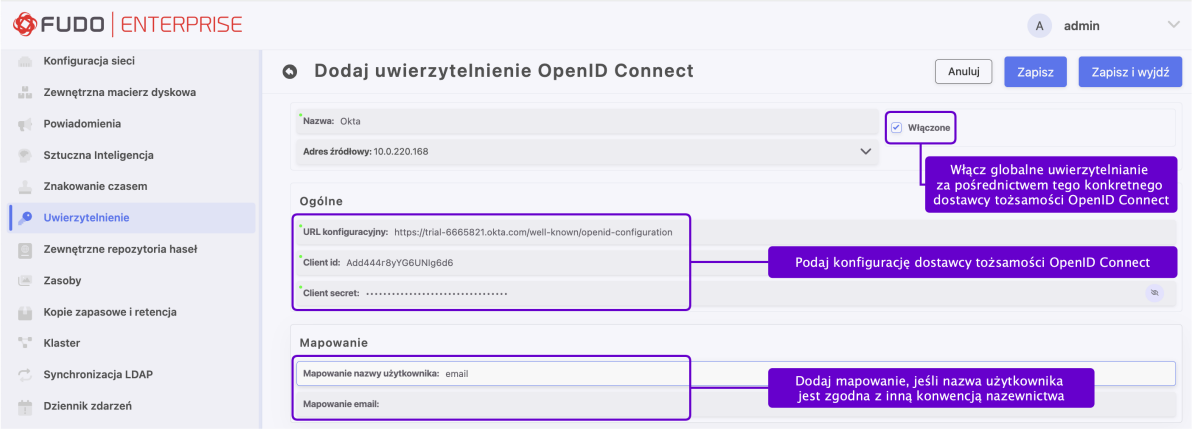
22.8.2 Definicja uwierzytelniania OpenID Connect

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 instrukcjami, aby skonfigurować metodę uwierzytelniania OpenID Connect:

1. Wybierz *Ustawienia* > *Uwierzytelnianie*.
2. Wybierz zakładkę **OpenID Connect**.
3. Kliknij *Dodaj OpenID Connect*.
4. Zaznacz opcję *Włączone*, aby globalnie włączyć uwierzytelnianie OpenID Connect.
5. Podaj Nazwę (`Azure`, `Okta` lub inny dostawca tożsamości).
6. Podaj *Bind address*.



7. W sekcji *Ogólne* wprowadź *URL konfiguracji*.

Informacja: Ten URL jest specyficzny dla każdego dostawcy tożsamości i umożliwia jego identyfikację dla poprawnej konfiguracji. Przykład *URL konfiguracji* dla Google: `https://accounts.google.com/.well-known/openid-configuration`.

---

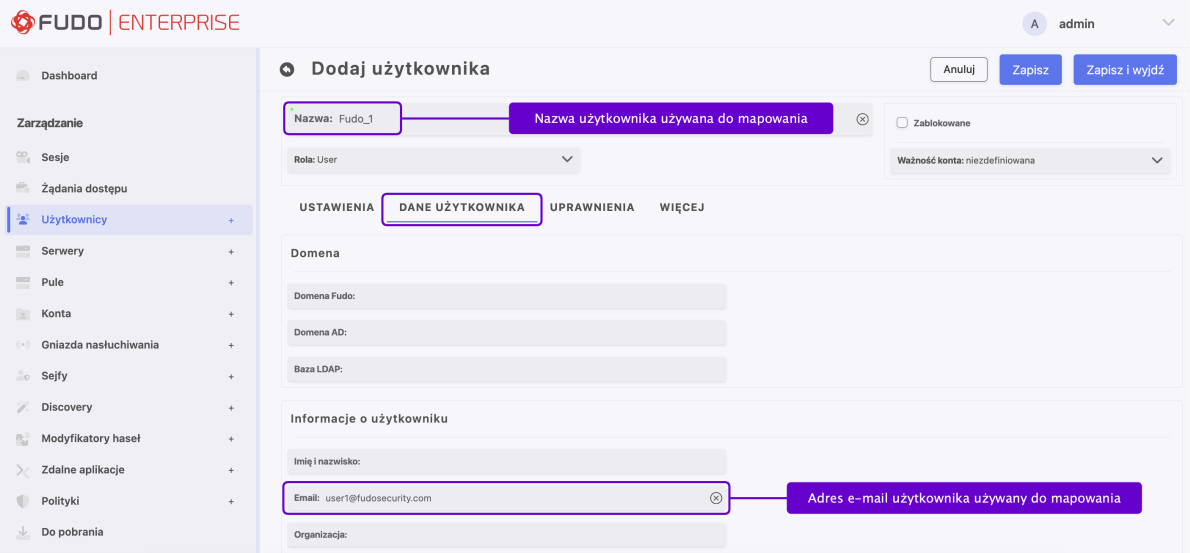
8. Podaj *Client ID* i *Client secret*. Te dane są dostępne po rejestracji na stronie wybranego dostawcy.

Informacja: Sprawdź rozdział *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)* opisujący przykład konfiguracji uwierzytelniania OpenID z Microsoft Entra.

---

9. Dodaj *Mapowanie nazwy użytkownika* oraz *Mapowanie emaila*. Te pola są przydatne w przypadku innej konwencji nazewnictwa użytkownika.

Informacja: Aby zapewnić poprawne uwierzytelnianie przy użyciu rozwiązania Okta, konieczne są szczególne konfiguracje mapowania w zależności od formatu nazwy użytkownika i obecności adresu email w konfiguracji użytkownika.



1. Nazwa użytkownika zawiera adres email:

   Scenariusz: Jeśli pole *Nazwa* w konfiguracji użytkownika zawiera adres email (np. `user1@fudosecurity.com`) a pole *Email* w zakładce *Dane użytkownika* jest puste.

   Konfiguracja: Ustaw *Mapowanie nazwy użytkownika* na `email`. To zapewnia, że adres email w nazwie użytkownika jest poprawnie rozpoznawany i używany do celów uwierzytelnienia.

2. Nazwa użytkownika z tekstem i wypełnione pole email:

   Scenariusz: Jeśli pole *Nazwa* w konfiguracji użytkownika zawiera dowolny tekst (np. `Fudo_1, user1`) a pole *Email* w zakładce *Dane użytkownika* zawiera faktyczny adres email (np. `user1@fudosecurity.com`).

   Konfiguracja: Ustaw *Mapowanie emaila* na `email`. Ta konfiguracja zapewnia, że adres email podany w polu *Email* jest używany do uwierzytelniania, nawet jeśli nazwa użytkownika jest ciągiem tekstowym bez emaila.

10. Kliknij *Zapisz*.

Informacja: Algorytm ustalania tożsamości użytkownika jest następujący:

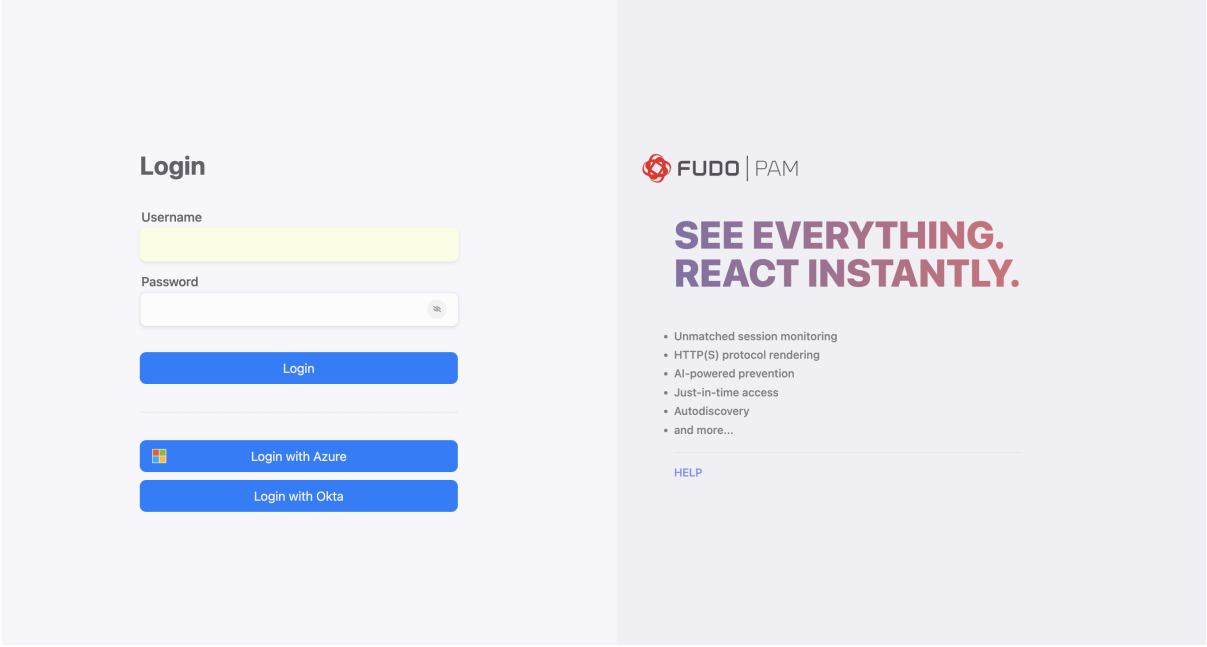
1. Użytkownik jest początkowo identyfikowany za pomocą pola `sub` od dostawcy OpenID Connect (OIDC).
2. Jeśli użytkownik nie został zidentyfikowany za pomocą pola `sub`, następnym krokiem jest sprawdzenie ustawienia *autolink* dla dostawcy OIDC. Jeśli to ustawienie jest niepoprawne, proces kończy się 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 odalezione w danych lub użytkownik nie został odnaleziony po nazwie, kolejnym krokiem jest spraw-

dzenie, 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 zdefiniowanej metody uwierzytelniania:



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*
- *Integracja z serwerem CERB*

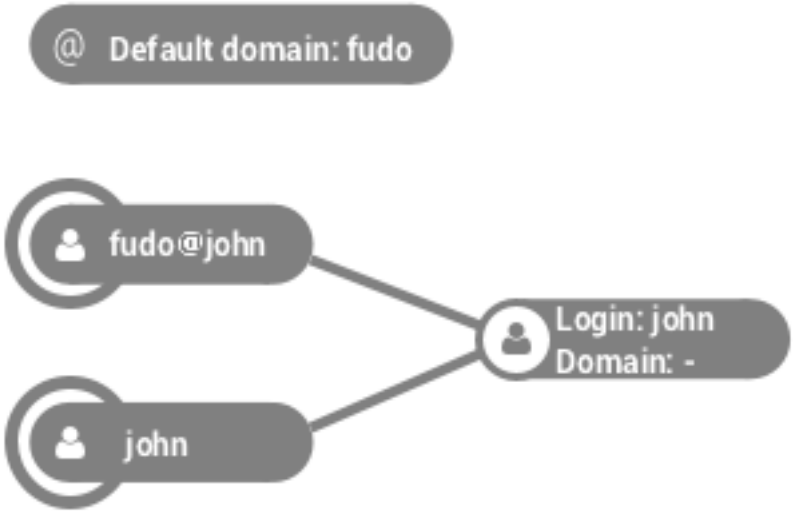
22.8.3 Global authentication settings

Zakładka *Globalne* umożliwia konfigurację domeny domyślnej, złożoności haseł oraz szeregu metod uwierzytelnienia, w tym OATH, SMS, DUO, SSO i Kerberos.

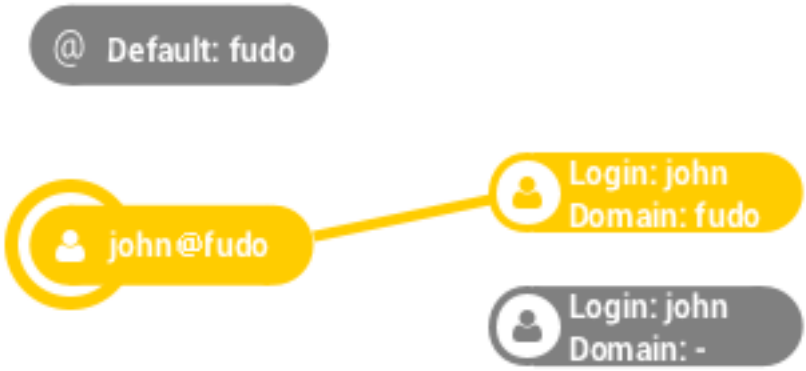
22.8.3.1 Domyślna domena

Informacja: Pamiętaj, że działanie opcji *Domena domyślna* jest ściśle powiązane z ustawieniami *Domeny Fudo* w *specyfikacji użytkownika*.

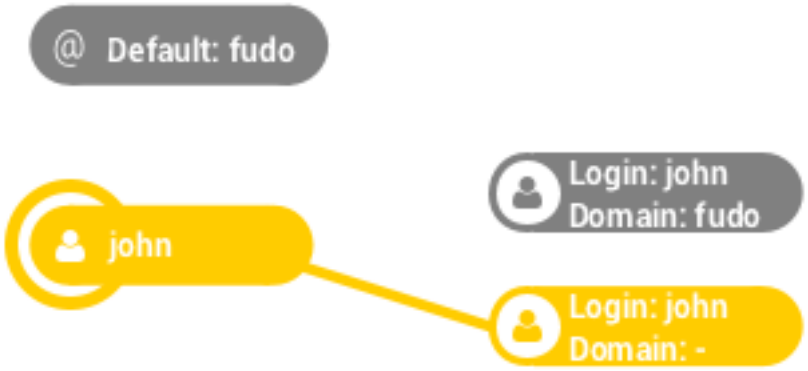
- W przypadku gdy została zdefiniowana *Domena domyślna*, a użytkownik nie ma przypisanej *Domeny Fudo*, może uwierzytelniać się podając domenę domyślną (przykład: `john@domain`) lub jej nie wskazywać (przykład: `john`).



- W sytuacji, w której istnieją dwaj użytkownicy o tym samym loginie, z których jeden ma zdefiniowaną *Domenę 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,



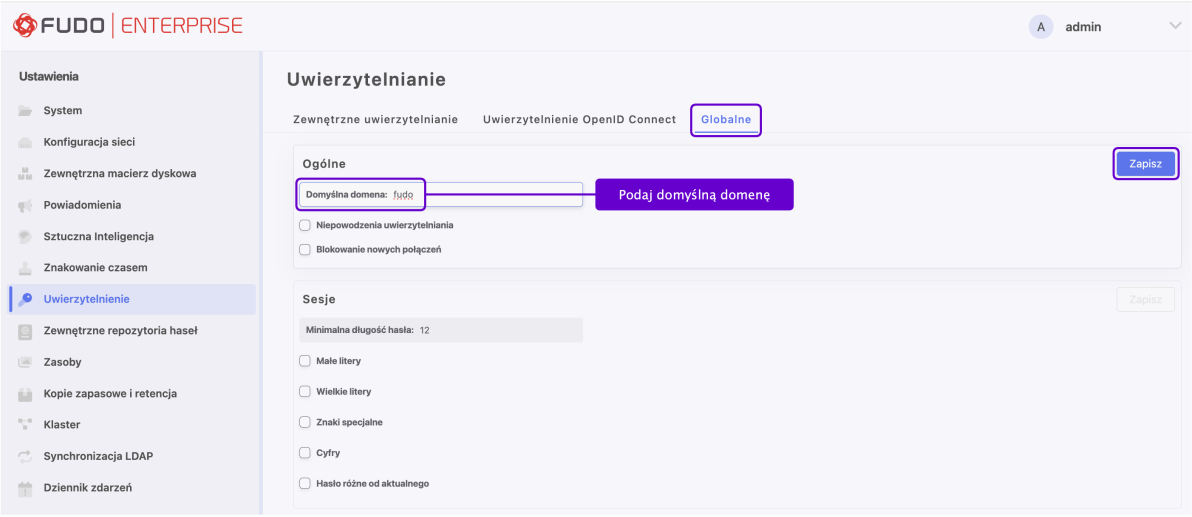
  - W przypadku, kiedy użytkownik nie poda domeny przy logowaniu, nastąpi dopasowanie użytkownika, który nie miał określonej domeny.



– 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 *Ustawienia* > *Uwierzytelnianie*.
2. Przejdź do zakładki *Globalne* i podaj domyślną domenę w sekcji *Ogólne*.
3. Kliknij *Zapisz* obok nazwy sekcji *Ogólne*.



Tematy pokrewne:

- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

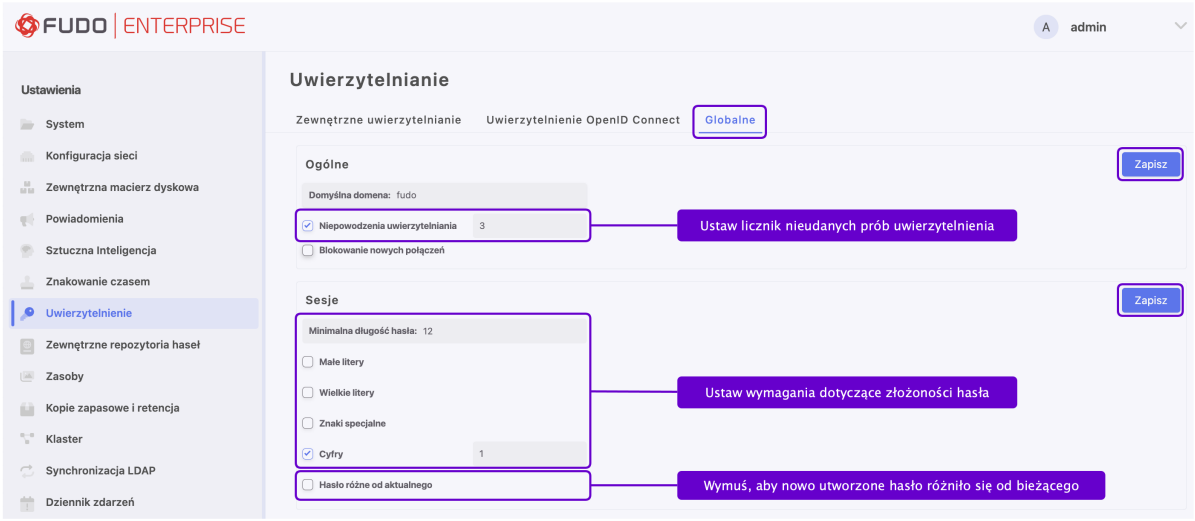
22.8.3.2 Złożoność haseł

Fudo Enterprise umożliwia definiowanie złożoności haseł, aby te były zgodne z polityką bezpieczeństwa organizacji.

Definiowanie złożoności haseł

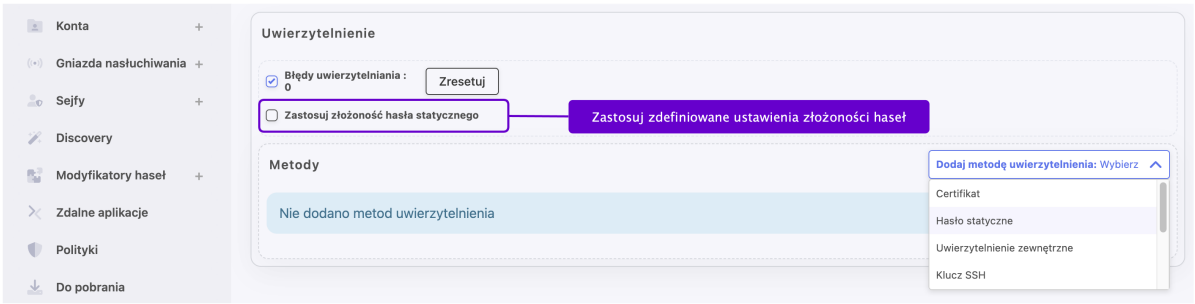
1. Wybierz *Ustawienia* > *Uwierzytelnianie*.

2. Przejdź do zakładki *Globalne* i wybierz *Niepowodzenia uwierzytelnienia*, aby ustawić licznik nieudanych logowań.
3. Przejdź do sekcji *Sesje* i ustaw kolejno zasady złożoności haseł:
   - Określ minimalną długość hasła.
   - Zaznacz *Małe litery* i określi minimalną liczbę małych liter.
   - Zaznacz *Wielkie litery* i określi minimalną liczbę wielkich liter.
   - Zaznacz *Znaki specjalne* i określi minimalną liczbę znaków specjalnych.
   - Zaznacz *Cyfry* i określi minimalną liczbę cyfr.
   - Zaznacz opcję *Hasło różne od aktualnego*, aby nowe hasło było różne od bieżącego.



4. 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*.



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*.

Tematy pokrewne:

- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

22.8.3.3 Definicja uwierzytelniania OATH

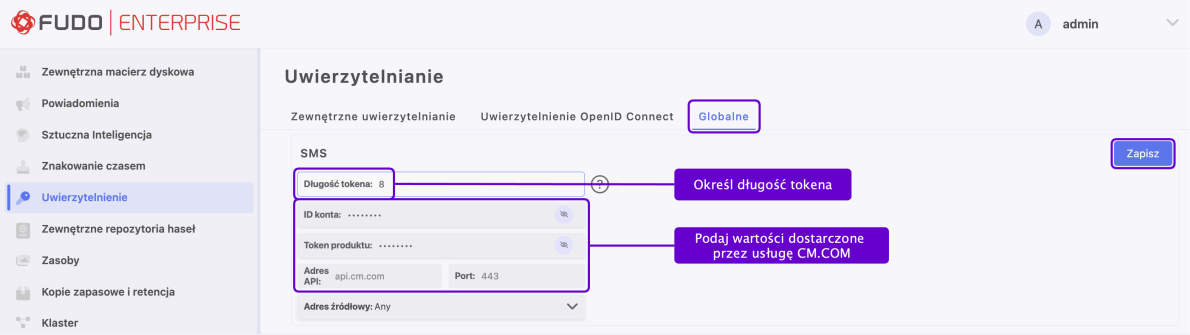
Przejdź do strony *Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator*.

Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*
- *Integracja z serwerem CERB*

22.8.3.4 Definicja uwierzytelniania SMS

1. Wybierz *Ustawienia* > *Uwierzytelnianie* > zakładka *Globalne*.
2. Przejdź do sekcji *SMS*.



3. Wprowadź *Długość tokena*.

Informacja: Długość tokena powinna mieścić się w zakresie 4-16.

---

4. Wprowadź *ID konta*.
5. Wprowadź *Token produktu*.
6. Wprowadź *Adres API* oraz *Port*.

Informacja: Wartości dla *ID konta*, *Token produktu* oraz *Adres API* są dostarczane przez usługę CM.COM. W tym celu jest wymagana rejestracja konta w tym serwisie.

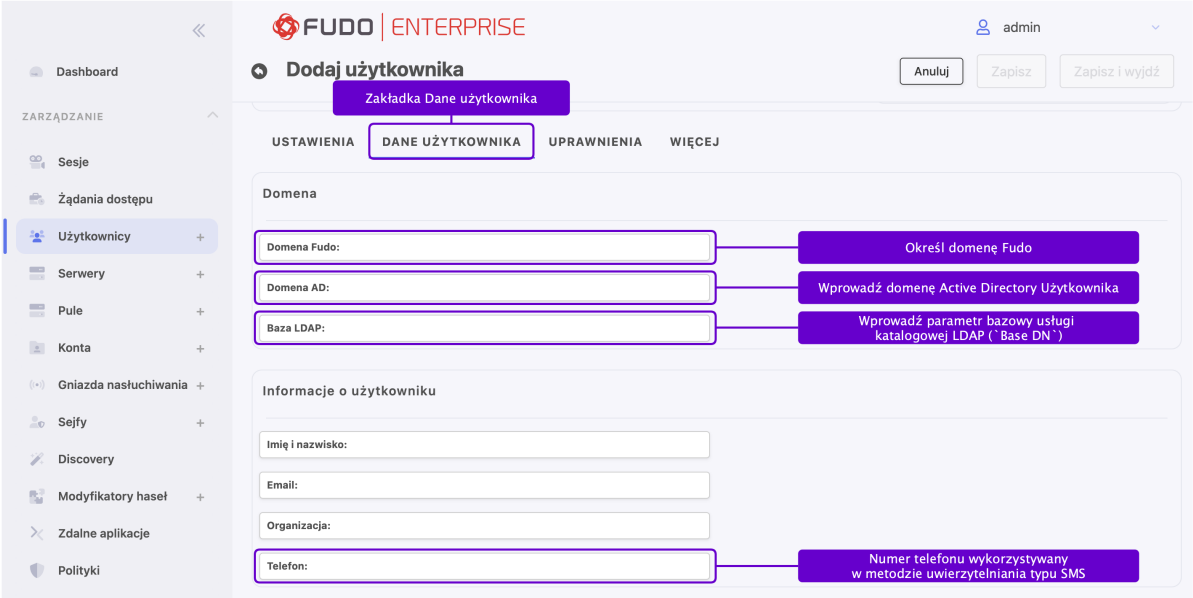
---

7. Wybierz *Adres źródłowy*.
8. Kliknij *Zapisz*.

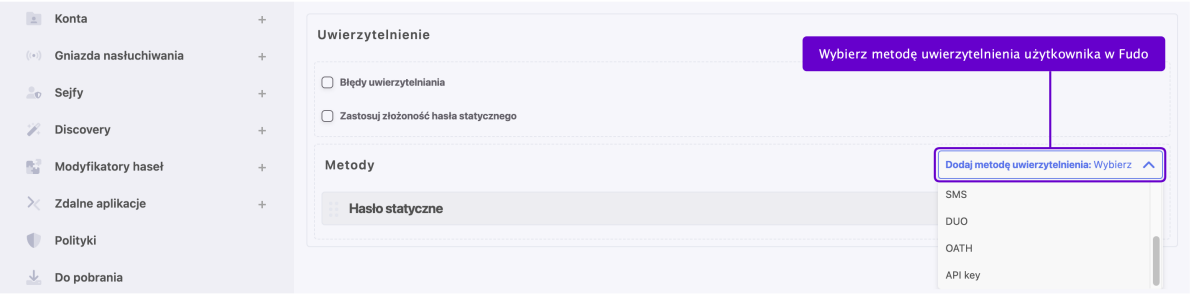
Następnie skonfiguruj metodę uwierzytelniania SMS dla użytkownika:

1. Przejdź do *Zarządzanie* > *Użytkownicy*.

2. Znajdź i wybierz użytkownika, dla którego chcesz włączyć uwierzytelnianie SMS.
3. Przejdź do zakładki *Dane użytkownika* i prowadź numer telefonu w polu *Telefon*.



4. Wróć do zakładki *Ustawienia*, przejdź do sekcji *Uwierzytelnienie* i z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz *SMS*.



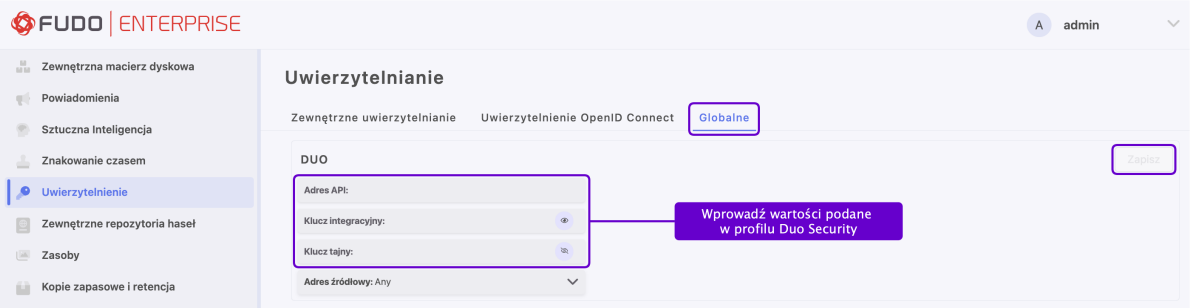
5. Jako *Pierwszy składik* wybierz `Hasło statyczne` lub `Uwierzytelnienie zewnętrzne` (AD lub LDAP).
6. Podaj hasło statyczne lub źródło zewnętrznego uwierzytelnienia.
7. Wybierz opcję *Wymagana zmiana hasła przy następnym logowaniu*, jeśli to konieczne.
8. Kliknij *Zapisz*.
9. Zaloguj się do *Portalu Użytkownika* za pomocą kodu SMS.

Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*
- *Integracja z serwerem CERB*

22.8.3.5 Definicja uwierzytelniania DUO

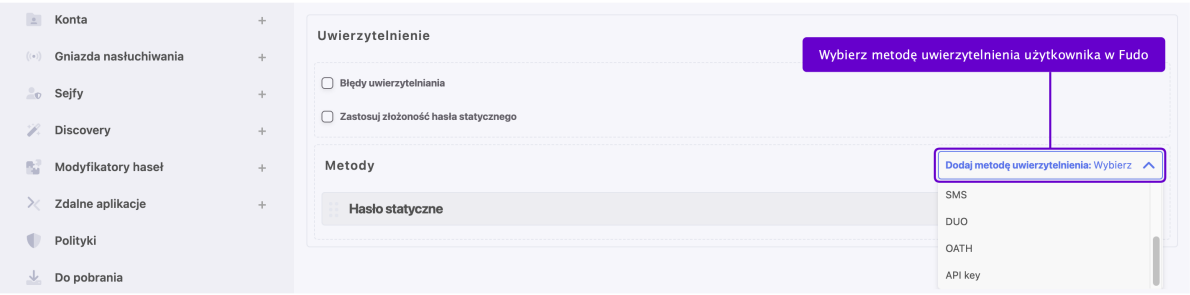
1. Pobierz i zainstaluj aplikację mobilną Duo Mobile.
2. Zarejestruj się na stronie Duo Security w celu stworzenia własnego konta.
3. Wybierz *Ustawienia* > *Uwierzytelnianie* > zakładka *Globalne*.
4. Przejdź do sekcji *DUO*.



5. Wprowadź wartości podane w profilu osobistym Duo Security: *Adres API*, *Klucz integracji* i *Tajny klucz*.
6. Wybierz *Adres źródłowy*.
7. Kliknij *Zapisz*.

Następnie skonfiguruj metodę uwierzytelniania DUO dla użytkownika:

8. Przejdź do *Zarządzanie* > *Użytkownicy*.
9. Znajdź i wybierz użytkownika, dla którego chcesz włączyć uwierzytelnianie DUO.



10. W zakładce *Ustawienia*, w sekcji *Uwierzytelnianie*, z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz *DUO*.
11. Jako *Pierwszy składik* wybierz `Hasło statyczne` lub `Uwierzytelnienie zewnętrzne` (AD lub LDAP).
12. Wprowadź *Użytkownika DUO*.
13. Wprowadź *Identyfikator użytkownika DUO*.
14. Kliknij *Zapisz*.
15. Zaloguj się do *Portalu Użytkownika* akceptując notyfikację typu push z aplikacji Duo Mobile.

Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*

- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*
- *Integracja z serwerem CERB*

22.8.3.6 Single Sign On

Single Sign On pozwala na automatyczne uwierzytelnienie użytkownika podczas logowania do systemu. Fudo Enterprise umożliwia skonfigurowanie funkcjonalności Single Sign On zarówno dla Panelu Administracyjnego, jak i Portalu Użytkownika (Access Gateway).

Informacja: Aby uzyskać bardziej szczegółowe informacje na temat konfiguracji SSO z Active Directory, zapoznaj się ze scenariuszem użycia w rozdziale *Konfiguracja Single Sign On (SSO)*.

22.8.3.6.1 Konfiguracja Fudo Enterprise dla SSO

1. Ustaw nazwę hosta Fudo Enterprise na `hostname.yourdomain.local`.
    - Wybierz *Ustawienia* > *Konfiguracja sieci*.
    - Przełącz się na zakładkę *Nazwa i DNS*.
    - Wprowadź `hostname.yourdomain.local` w polu *Nazwa hosta*.
2. Skonfiguruj serwer DNS, aby wskazywał na serwer DNS w domenie *yourdomain.local*.
    - Kliknij *Dodaj nowy*, aby zdefiniować nowy serwer DNS.
    - Wprowadź adres IP serwera DNS.
    - Kliknij *Zapisz*.
3. Dodaj użytkownika, który posiada konto w rejestrze Active Directory.
    - *Skonfiguruj synchronizację użytkowników LDAP* lub
    - *dodaj konto użytkownika ręcznie*, ze wskazaniem usługi Active Directory jako zewnętrznej metody uwierzytelnienia.

22.8.3.6.2 Konfiguracja kontrolera domeny

1. Dodaj konto użytkownika, które będzie używane przez *Portal Użytkownika* lub *Panel Administracyjny* do komunikacji z domeną *yourdomain.local*.

Informacja: Podczas dodawania konta włącz opcję *Hasło nigdy nie wygasa*.

---

2. Na serwerze DNS dodaj wpisy DNS forward oraz reverse dla adresu *hostname.yourdomain.local*.

3. Utwórz bilet Kerberos dla Fudo Enterprise wywołując następujące polecenie w konsoli Powershell lub CMD:

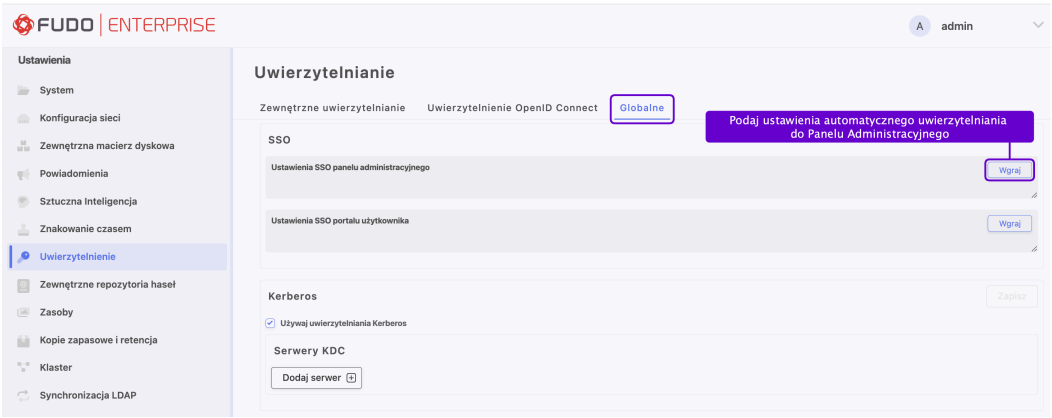
```
ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.local -mapuser
netbios_domain_name\username -pass password       - ptype KRB5_NT_PRINCIPAL -out
hostname.yourdomain.local.keytab
```

22.8.3.6.3 Single Sign On w Panelu Administracyjnym

Ostrzeżenie: Single Sign On w Panelu Administracyjnym może konfigurować tylko użytkownik o roli `superadmin`, natomiast metoda może być wykorzystywana przez użytkowników o rolach `operator`, `admin` i `superadmin`.

Aby zdefiniować parametry funkcji SSO w ustawieniach systemu, postępuj zgodnie z instrukcją:

- Wybierz *Ustawienia* > *'Uwierzytelnianie* > zakładka *Globalne*.
- W sekcji *SSO* kliknij przycisk *Prześlij* w polu *Ustawienia SSO panelu administracyjnego*, aby uzyskać dostęp do konfiguracji.



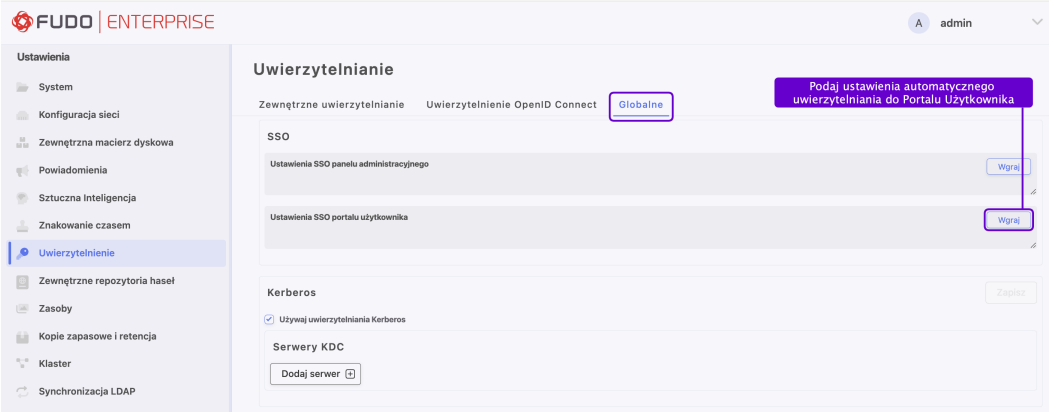
- Podaj nazwę główną SSO (principal name), która będzie zgodna z kontem użytkownika i usługą, np :`HTTP/hostname.yourdomain.local@yourdomain.local`.
- Załaduj plik `hostname.yourdomain.local.keytab` z identyfikatorem konta użytkownika w Active Directory oraz kluczami do szyfrowania i deszyfrowania żądań Kerberos.

- Kliknij *Zapisz*.

22.8.3.6.4 Single Sign On w Portalu Użytkownika

Aby zdefiniować parametry usługi SSO w ustawieniach systemu, postępuj zgodnie z instrukcjami:

- Wybierz *Ustawienia* > *'Uwierzytelnianie* > zakładka *Globalne*.
- W sekcji *SSO* kliknij przycisk Prześlij w polu *Ustawienia SSO portalu użytkownika*, aby uzyskać dostęp do konfiguracji.



- Podaj nazwę główną SSO (principal name), która będzie zgodna z kontem użytkownika i usługą, np :`HTTP/hostname.yourdomain.local@yourdomain.local`.
- Załaduj plik `hostname.yourdomain.local.keytab` z identyfikatorem konta użytkownika w Active Directory oraz kluczami do szyfrowania i deszyfrowania żądań Kerberos.

- Kliknij *Zapisz*.

Tematy pokrewne:

- *Konfiguracja Single Sign On (SSO)*
- *Dodawanie użytkownika*
- *Synchronizacja użytkowników z LDAP*

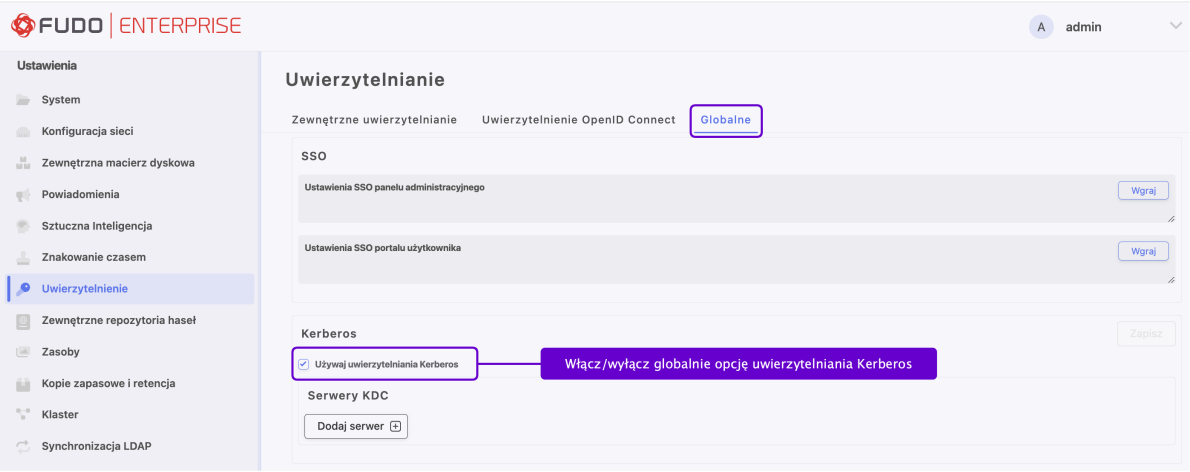
22.8.3.7 Ustawienia uwierzytelniania Kerberos

Informacja:

- Funkcjonalność ta jest domyślnie włączona, a Kerberos jest używany do uwierzytelnienia na serwerze podczas sesji RDP oraz przy metodzie zewnętrznego uwierzytelnienia Active Directory.
- Uwierzytelnienie przy użyciu Kerberosa jest pierwszym krokiem w przypadku korzystania z metody zewnętrznego uwierzytelnienia **Active Directory.**
- Jeśli uwierzytelnianie w **Active Directory** zostanie pomyślnie przeprowadzone za pomocą Kerberosa, skonfigurowany certyfikat nie zostanie użyty, ponieważ jest wykorzystywany tylko wtedy, gdy wymagane jest przejście na uwierzytelnianie za pomocą LDAP.

22.8.3.7.1 Wyłączanie uwierzytelniania Kerberos

Aby **wyłączyć** obsługę uwierzytelniania Kerberos globalnie, wybierz *Ustawienia* > *Uwierzytelnianie*, przejdź do zakładki *Globalne* i odznacz opcję *Uwierzytelnianie Kerberos włączone* w sekcji Kerberos.

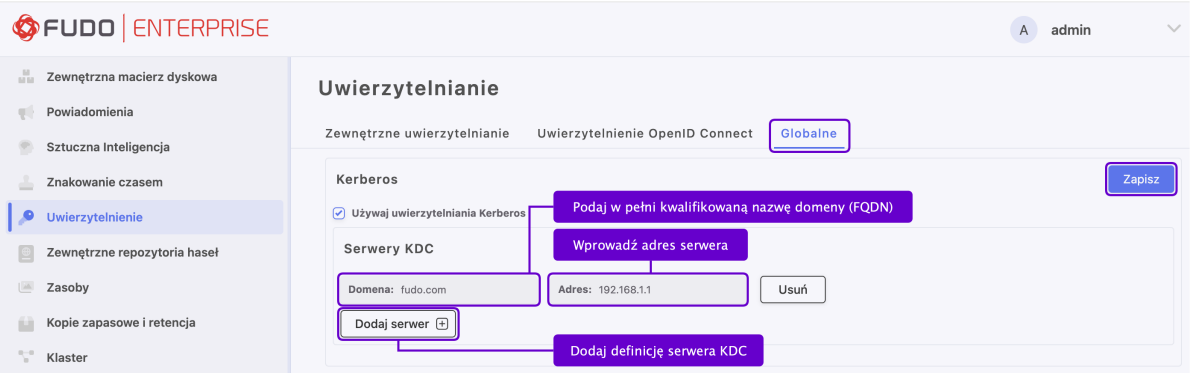


22.8.3.7.2 Dodawanie serwerów KDC

Fudo Enterprise wspiera konfigurację serwerów dystrybucji kluczy (Key Distribution Servers) oraz mapowanie domen na serwery KDC.

Aby dodać serwer KDC:

1. Wybierz *Ustawienia* > *Uwierzytelnianie* > zakładka *Globalne*.
2. Przejdź do sekcji *Kerberos*.
3. Kliknij *Dodaj serwer*.



4. Podaj pełną nazwę domeny (FQDN) w polu *Domena* (np. `fudo.com, .fudo.com`).
5. Podaj adres serwera KDC w polu *Adres* (np. `192.168.1.1, foo.bar, tcp/foo.bar, udp/192.168.1.1:88`).

Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*
- *Integracja z serwerem CERB*

22.9 Zewnętrzne repozytoria haseł

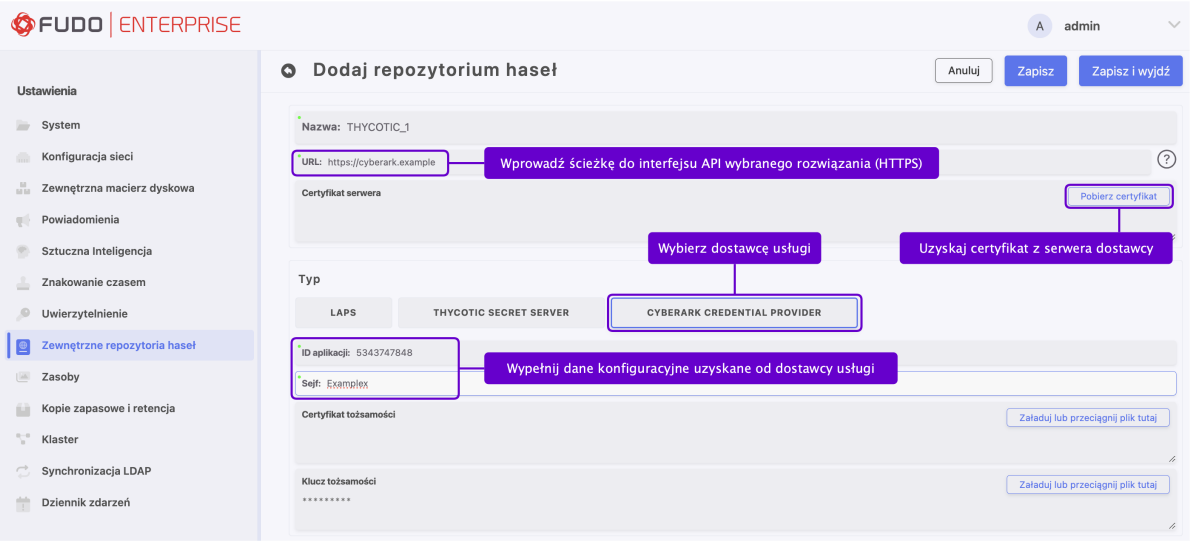
Fudo Enterprise wspiera zewnętrzne repozytoria haseł do zarządzania hasłami dostępowymi.

22.9.1 CyberArk Credential Provider

Dodawanie definicji repozytorium haseł

1. Wybierz *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij + *Dodaj repozytorium haseł*.
3. Podaj nazwę obiektu.
4. W polu *URL*, wprowadź ścieżkę do interfejsu API wybranego rozwiązania (HTTPS).
5. W polu *Certyfikat serwera* podaj certyfikat SSL lub kliknij przycisk *Pobierz certyfikat*, aby uzyskać go z serwera dostawcy.

Ostrzeżenie: Jeśli używany jest protokół HTTPS bez podania certyfikatu SSL, połączenie SSL nie będzie weryfikowane i zostanie zaakceptowane.



6. W sekcji *Typ* wybierz przycisk *CYBERARK CREDENTIAL PROVIDER*.
7. Podaj identyfikator aplikacji (*Application ID*).
8. Podaj *Sejf* (opcjonalnie). Jeśli *Sejf* nie zostanie zdefiniowany, wyszukiwanie będzie przeprowadzane 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 *Tworzenie konta typu regular*,
- `Safe` - musi zgadzać się z polem *Sejf* w utworzonym w Fudo zewnętrznym repozytorium haseł (pole opcjonalne).

---

9. W przypadku uwierzytelniania za pomocą certyfikatu klienta, należy zdefiniować pola *Certyfikat tożsamości* i *Klucz tożsamości*.

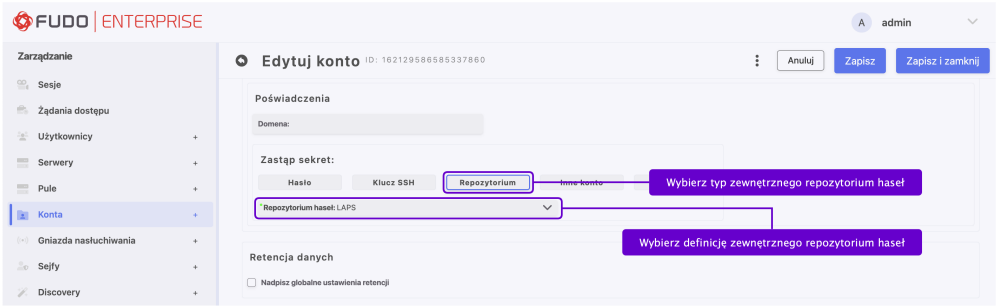
Informacja:

- Konfiguracja *Certyfikatu tożsamości* i *Klucza tożsamości* jest dostępna tylko dla serwerów typu HTTPS.
- Oba pola muszą być wypełnione przy użyciu formatu PKCS #8.
- Aby dowiedzieć się, jak wygenerować *Certyfikat tożsamości* i *Klucz tożsamości*, przejdź do następnego rozdziału.

---

10. Kliknij *Zapisz*.
11. Przypisz zewnętrzne repozytorium haseł do konta.
    - Wybierz *Zarządzanie* > *Konta*.
    - Wyszukaj i kliknij definicję konta, aby uzyskać dostęp do formularza ustawień.

- W sekcji *Dane uwierzytelniające*, w polu *Zastąp sekret*, wybierz przycisk *Repozytorium*.
- Z listy rozwijanej *Repozytorium haseł* wybierz jedno z wcześniej zdefiniowanych repozytoriów.



- Kliknij *Zapisz*.

Generowanie certyfikatu klienta 'CyberArk Credential Provider'

1. Wygeneruj losowy numer seryjny (np. 11223344556677), który będzie używany przez CyberArk do weryfikacji klienta.
2. 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
```

3. Wklej zawartość pliku *client.crt* w polu *Certyfikat tożsamości*.
4. Wklej zawartość pliku *client.key* w polu *Klucz tożsamości*.
5. 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 *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Znajdź definicję repozytorium i kliknij jej nazwę, aby edytować konfigurację.
3. Kliknij *Zapisz*.

Usuwanie definicji repozytorium haseł

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

1. Wybierz *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Znajdź definicję repozytorium, wybierz ją i kliknij przycisk *Usuń wybrane*.
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*

22.9.2 Thycotic Secret Server

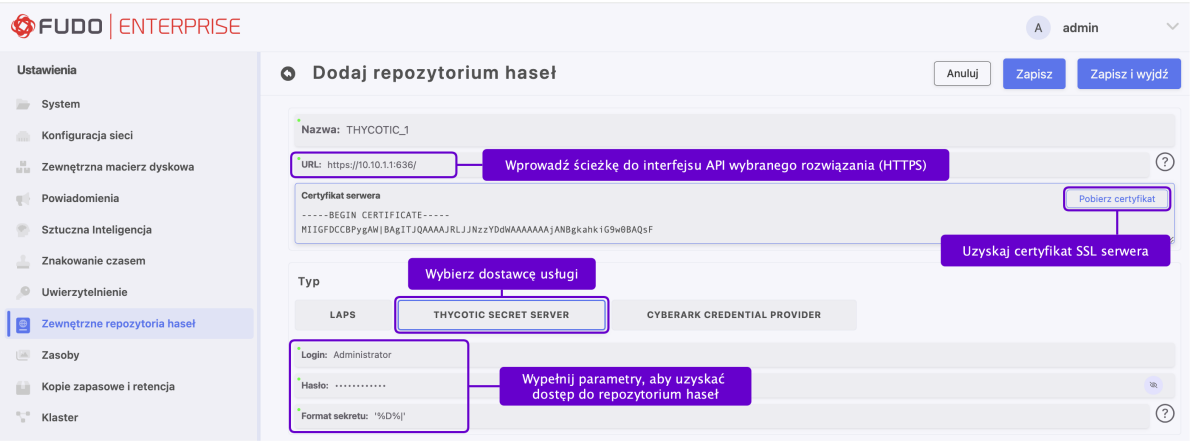
Dodawanie definicji repozytorium haseł

1. Wybierz *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj repozytorium haseł*.
3. Podaj nazwę obiektu.
4. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

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

---

5. W polu *Certyfikat serwera* podaj certyfikat SSL lub kliknij przycisk *Pobierz certyfikat*, aby uzyskać go z serwera dostawcy.



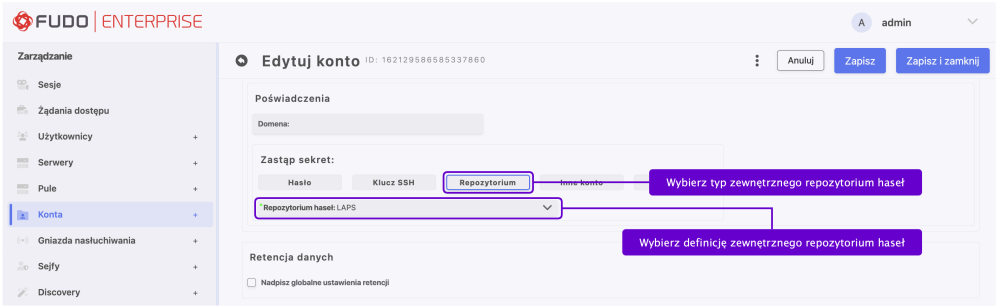
6. W sekcji *Typ* wybierz przycisk *THYCOTIC SECRET SERVER*.
7. W polu *Login* wprowadź nazwę użytkownika uprawionego do pobierania haseł.
8. W polu *Hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
9. W polu *Format sekretu* wprowadź ciąg znaków definiujący format identyfikatorów obiektów w systemie Thycotic Secret Server.

Informacja: Format sekretu można zdefiniować przy użyciu zmiennych: `%U - nazwa użytkownika, %D - domena użytkownika, %S - nazwa serwera.`, np. *«%D%U»*.

---

10. Kliknij *Zapisz*.
11. Przypisz zewnętrzne repozytorium haseł do konta.
    - Wybierz *Zarządzanie* > *Konta*.

- Wyszukaj i kliknij definicję konta, aby uzyskać dostęp do formularza ustawień.
- W sekcji *Dane uwierzytelniające*, w polu *Zastąp sekret*, wybierz przycisk *Repozytorium*.
- Z listy rozwijanej *Repozytorium haseł* wybierz jedno z wcześniej zdefiniowanych repozytoriów haseł.



- Kliknij *Zapisz*.

Modyfikowanie definicji repozytorium haseł

Aby zmodyfikować repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Znajdź definicję repozytorium i kliknij jej nazwę, aby edytować konfigurację.
3. Kliknij *Zapisz*.

Usuwanie definicji repozytorium haseł

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

1. Wybierz *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Znajdź definicję repozytorium, wybierz ją i kliknij przycisk *Usuń wybrane*.
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*

22.9.3 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 *Tworzenie 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 *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Kliknij *+ Dodaj repozytorium haseł*.
3. Podaj nazwę obiektu.
4. W polu *URL* wprowadź ścieżkę do interfejsu API wybranego rozwiązania.

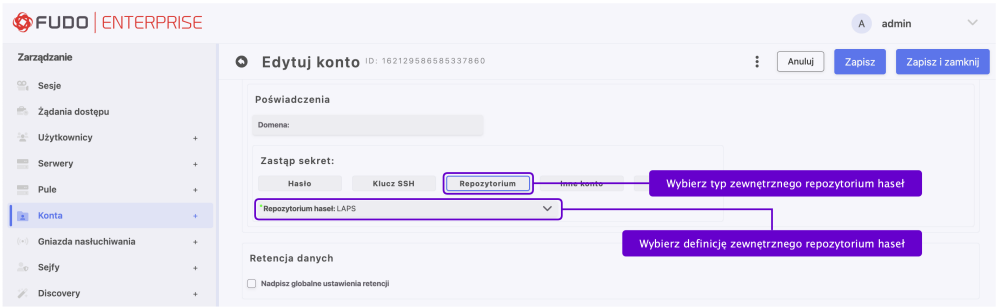
Informacja: Obsługiwany format URL to `ldaps://<server>[:<port>]/` dla połączenia przez SSL.

---

5. W polu *Certyfikat serwera* podaj certyfikat SSL lub kliknij przycisk *Pobierz certyfikat*, aby uzyskać go z serwera dostawcy.

Ostrzeżenie: W przypadku zastosowania protokołu LDAPS bez dostarczenia Certyfikatu SSL połączenie SSL zostanie zaakceptowane bez weryfikacji.

6. W sekcji *Typ* wybierz przycisk *LAPS*.
7. Podaj login użytkownika uprawnionego do dostępu do repozytorium haseł.
8. W polu *Hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
9. Podaj *Base DN* serwera AD/LDAP.
10. Kliknij *Zapisz*.
11. Przypisz zewnętrzne repozytorium haseł do konta.
    - Wybierz *Zarządzanie* > *Konta*.
    - Wyszukaj i kliknij definicję konta, aby uzyskać dostęp do formularza ustawień.
    - W sekcji *Dane uwierzytelniające*, w polu *Zastąp sekret*, wybierz przycisk *Repozytorium*.
    - Z listy rozwijanej *Repozytorium haseł* wybierz jedno z wcześniej zdefiniowanych repozytoriów haseł.



- 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 *Tworzenie konta typu regular*).

Modyfikowanie definicji repozytorium haseł

Aby zmodyfikować repozytorium haseł, postępuj zgodnie z poniższą instrukcją.

1. Wybierz *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Znajdź definicję repozytorium i kliknij jej nazwę, aby edytować konfigurację.
3. Kliknij *Zapisz*.

Usuwanie definicji repozytorium haseł

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

1. Wybierz *Ustawienia* > *Zewnętrzne repozytoria haseł*.
2. Znajdź definicję repozytorium, wybierz ją i kliknij przycisk *Usuń wybrane*.

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*

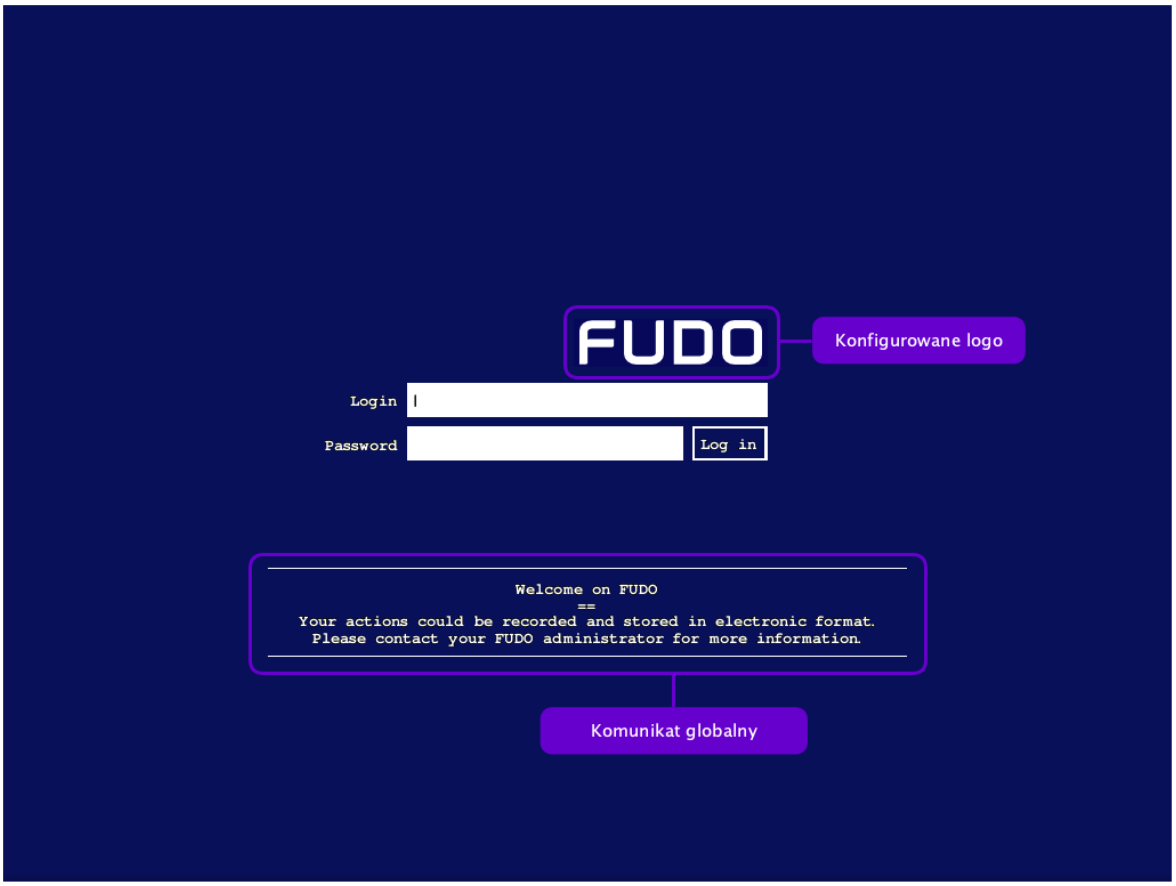
Tematy pokrewne:

- *Uwierzytelnienie*
- *Opis systemu*
- *Integracja z serwerem CERB*

22.10 Zasoby

22.10.1 Konfiguracja ekranu logowania RDP/SSH/VNC

Fudo Enterprise pozwala na dostosowanie do własnych potrzeb ekranów logowania dla połączeń RDP, SSH i VNC.



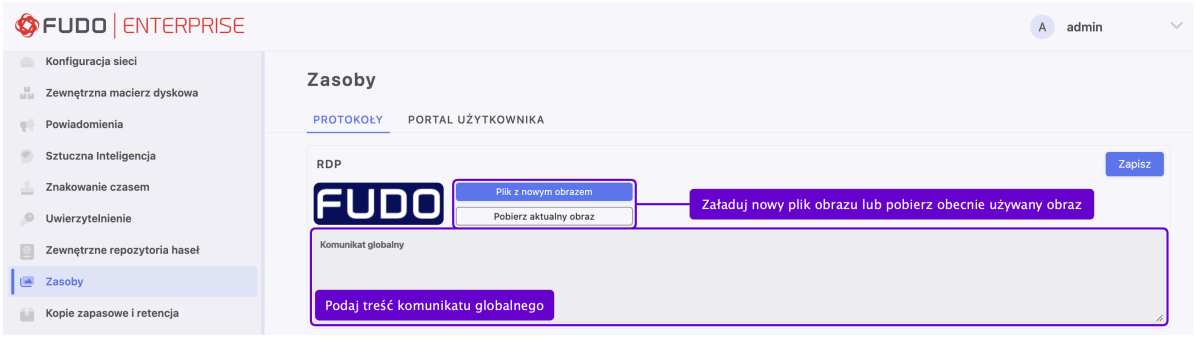
Dostosowywanie ekranu logowania RDP

1. Wybierz *Ustawienia* > *Zasoby*.
2. Wybierz zakładkę *Protokoły*.
3. W sekcji *RDP* kliknij przycisk *Prześlij nowy obraz* i wybierz pożądany obraz.

Informacja: Maksymalny rozmiar obrazu to 512 x 512 px.

4. Wprowadź tekst *Komunikatu globalnego*, który ma się pojawić jako wiadomość na ekranie logowania.

Informacja: Komunikat na ekranie logowania może mieć cztery linie, do 120 znaków.



5. Kliknij *Zapisz*.

Dostosowywanie ekranu logowania SSH

1. Wybierz *Ustawienia* > *Zasoby*.
2. Wybierz zakładkę *Protokoły*.
3. W sekcji *SSH* wprowadź tekst *Komunikatu globalnego*, który ma się pojawić jako wiadomość na ekranie logowania.

Informacja: Komunikat na ekranie logowania może mieć cztery linie, do 120 znaków.

---

4. Kliknij *Zapisz*.

Dostosowywanie ekranu logowania VNC

1. Wybierz *Ustawienia* > *Zasoby*.
2. Wybierz zakładkę *Protokoły*.
3. W sekcji *VNC* kliknij przycisk *Prześlij nowy obraz* i wybierz pożądany obraz.

Informacja: Maksymalny rozmiar obrazu to 512 x 512 px.

---

4. Wprowadź tekst *Komunikatu globalnego*, który ma się pojawić jako wiadomość na ekranie logowania.

Informacja: Komunikat na ekranie logowania może mieć cztery linie, do 120 znaków.

5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Szybki start - RDP*

22.10.2 Konfiguracja ekranu logowania *Portalu użytkownika*

Fudo Enterprise umożliwia dostosowanie informacji wyświetlanych na ekranie logowania *Portalu użytkownika*.

1. Wybierz *Ustawienia* > *Zasoby*.
2. Wybierz zakładkę *Portal użytkownika*.
3. Kliknij przycisk *Prześlij nowy obraz*, przeszukaj system plików i wybierz własne logo dla ekranu logowania *Portalu użytkownika*.

Informacja: Maksymalny rozmiar obrazu to 5 MB.

4. Wprowadź treść komunikatu wyświetlanego na ekranie logowania.

Informacja: Komunikat na ekranie logowania może mieć cztery linie, do 120 znaków.

5. Uzupełnij pole *Informacje o sprzedawcy*.

Informacja: Informacje o sprzedawcy mogą mieć pięć linii, do 70 znaków.

6. Uzupełnij dane kontaktowe do działu wsparcia technicznego.

Informacja: Informacje kontaktowe do pomocy technicznej mogą mieć pięć linii, do 70 znaków.

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.

Informacja: Możesz dostosować ten komunikat zawierając zmienne (`organization`, `phone`, `name`, `full_name`, lub `email`) zamknięte w podwójnych symbolach %%. Np. `%%email%%`.

Ostrzeżenie: Funkcja **Zajętości zasobu** jest dostępna tylko dla połączeń RDP i może być skonfigurowana podczas *Dodawanie serwera RDP*, zaznaczając opcję *Informuj o istniejącym połączeniu*.

8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Portal użytkownika*

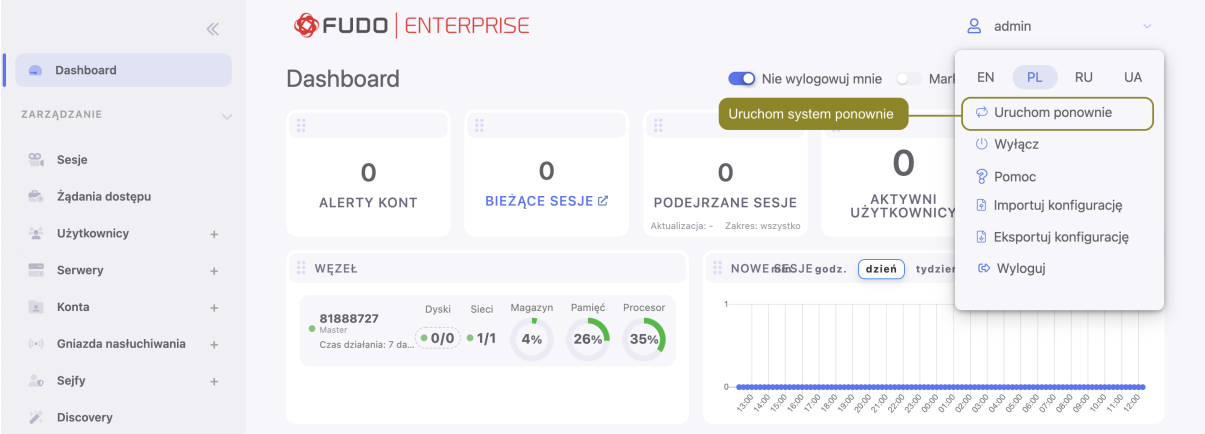
22.11 Przywracanie poprzedniej wersji systemu

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

Ostrzeżenie: Przywrócenie poprzedniej wersji spowoduje odtworzenie stanu systemu sprzed jego aktualizacji. **Dane sesji** oraz **zmiany w konfiguracji** dokonane na nowej wersji systemu zostaną utracone. Obejmuje to także **aktywność modyfikatorów haseł**. Jeśli jakiekolwiek hasła zostały zmienione podczas korzystania z nowszej wersji, przywrócenie poprzedniej wersji spowoduje utratę dostępu do wybranych systemów.

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

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



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

Informacja: Domyślnie zaznaczona jest wersja bieżąca.

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

Ostrzeżenie: Ponowne uruchomienie systemu spowoduje rozłączenie bieżących połączeń użytkowników.

Tematy pokrewne:

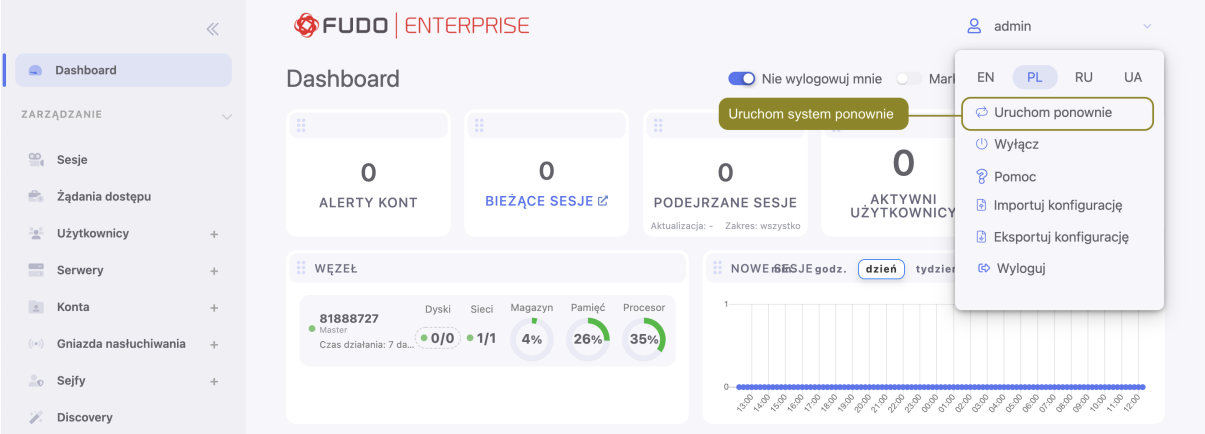
- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

22.12 Ponowne uruchomienie systemu

Ostrzeżenie: Ponowne uruchomienie systemu spowoduje rozłączenie bieżących połączeń użytkowników.

Informacja: Skorzystaj z opcji *Blokowanie nowych połączeń* sekcji *Sesja* ustawień systemowych, aby zablokować możliwość nawiązywania nowych połączeń i ograniczyć liczbę aktywnych użytkowników przed ponownym uruchomieniem systemu.

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



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

Informacja: Domyślnie zaznaczona jest wersja bieżąca.

Ostrzeżenie: Przywrócenie poprzedniej wersji spowoduje odtworzenie stanu systemu sprzed jego aktualizacji. **Dane sesji** oraz **zmiany w konfiguracji** dokonane na nowej wersji systemu zostaną utracone. Obejmuje to także **aktywność modyfikatorów haseł**. Jeśli jakiekolwiek hasła zostały zmienione podczas korzystania z nowszej wersji, przywrócenie poprzedniej wersji spowoduje utratę dostępu do wybranych systemów.

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

Tematy pokrewne:

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

22.13 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.

---

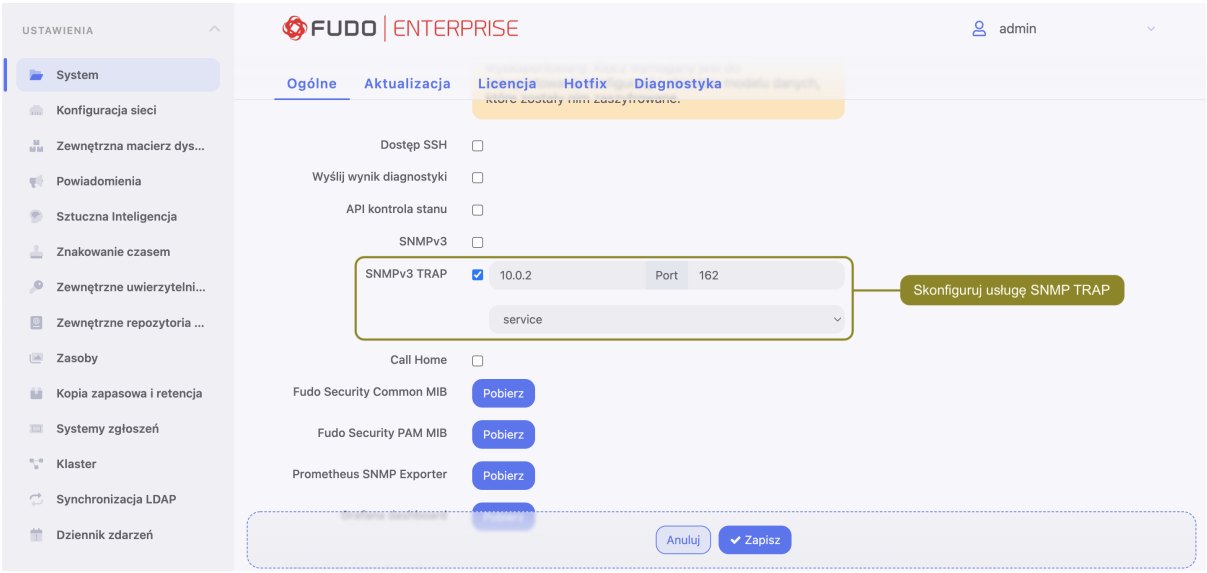
7. Przejdź do zakładki *Więcej* i w sekcji *SNMP*, zaznacz opcję *Włączone*.
8. Z listy rozwijalnej *Metoda uwierzytelnienia*, wybierz metodę *SHA* lub *MD5*.

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*.

Informacja: Przy opcji nasłuchu na *Any,* SNMP stosuje routing z domyślnej tabeli routingu `0`. Gdy ustawione jest nasłuchiwanie na określony adres IP, SNMP stosuje routing zdefiniowany na interfejsie, na którym skonfigurowany jest ten adres.

---

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

22.13.1 Odczytywanie informacji SNMP poprzez `snmpwalk`

Informacja: Odczyt danych SNMP wymaga zainstalowania pakietu *Net-SNMP 5.7.3*.

Pobieranie wszystkich informacji SNMP

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}"            -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1
```

Pobieranie wybranych informacji SNMP

```
snmpwalk -v3 -u "${SNMP_USER}" -a SHA -A "${SNMP_PASSWORD}"            -x AES -X
"${SNMP_PASSWORD}" -l authPriv "${FUDO_IP}" .1.3.6.1.4.1.24410
```

Dane SNMP	Opis
.1.3.6.1.4.1.24410.1.1.1	Status dysków (status ZFS)
.1.3.6.1.4.1.24410.1.1.2	Stan zasilaczy **Informacja:** Ta funkcja nie jest wspierana przez wszystkie urządzenia Fudo Enterprise. Skontaktuj się z działem wsparcia technicznego, aby uzyskać więcej informacji.
.1.3.6.1.4.1.24410.1.1.3	Temperatury procesora
.1.3.6.1.4.1.24410.1.1.4	Status S.M.A.R.T

22.13.2 Rozszerzenia SNMP Fudo Enterprise

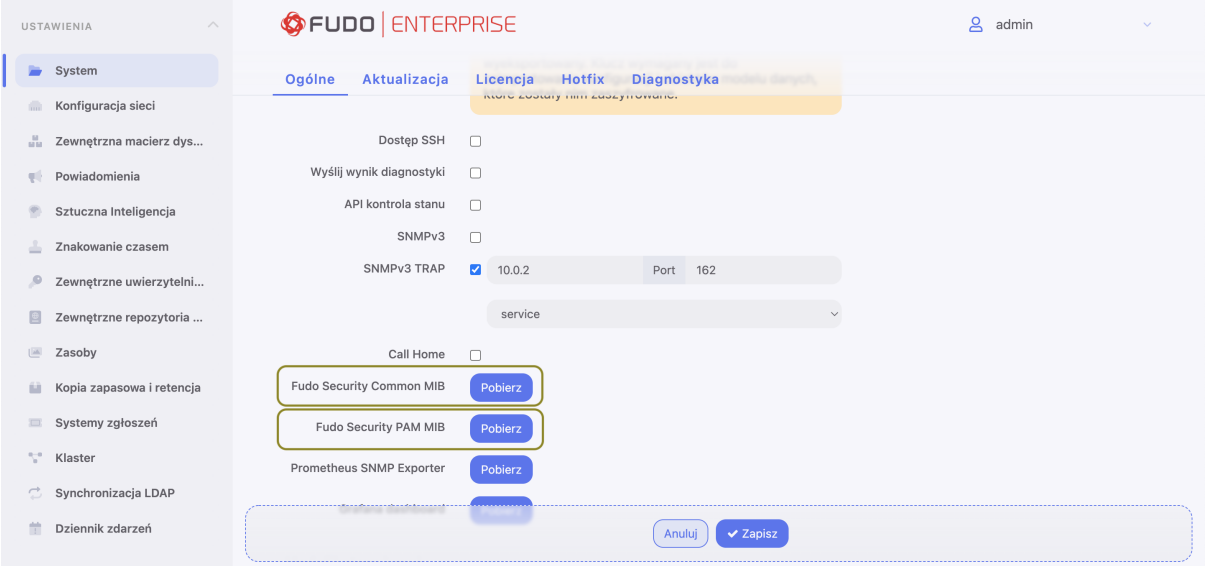
Informacje ogólne

Rozszerzenia SNMP umożliwiają monitorowanie liczby sesji SNMP, status ZFS, status zasilaczy (jeśli jest dostępny), temperaturę rdzeni procesorów, status S.M.A.R.T dysków twardych (temperatura, realokacja sektorów, stan urządzeń).

Specyfikacja pliku MIB rozszerzeń SNMP

Poniższe pliki MIB mogą zostać wczytane do managera SNMP w celu obsługi rozszerzeń specyficznych dla Fudo Enterprise.

Ostrzeżenie: W wersji 4.3 zmianie uległy nazwy plików MIB. Zamień dotychczasowe pliki MIB z nową definicją.



Tematy pokrewne:

- *Bezpieczeństwo*
- *Rozwiązywanie problemów*
- *Polityki*

22.14 Kopia zapasowa i retencja

22.14.1 Kopia zapasowa systemu

Ostrzeżenie: Kopia zapasowa systemu zawiera informacje poufne.

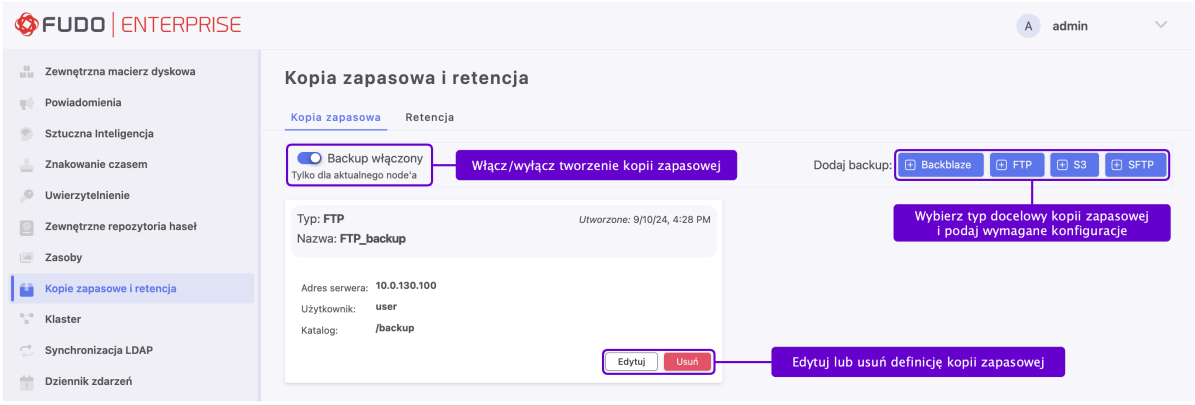
Fudo Enterprise pozwala na konfigurację wielu docelowych miejsc przechowywania kopii zapasowych. Mogą to być zewnętrzne repozytoria na S3, Backblaze, FTP lub SFTP.

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

1. Wybierz *Ustawienia* > *Kopia zapasowa i retencja*.
2. Wybierz opcję *Kopia zapasowa włączona*. Należy pamiętać, że w przypadku skonfigurowanego klastra opcja ta włącza kopię zapasową tylko dla bieżącego węzła.
3. W polu *Dodaj miejsce docelowe* kliknij przycisk typu repozytorium, aby skonfigurować docelowe miejsce przyszłej kopii zapasowej: *+Backblaze, +S3, +FTP* lub *+SFTP*.
4. Ustaw nazwę docelowego miejsca kopii zapasowej.
5. Podaj dodatkowe dane w zależności od wybranego typu połączenia:

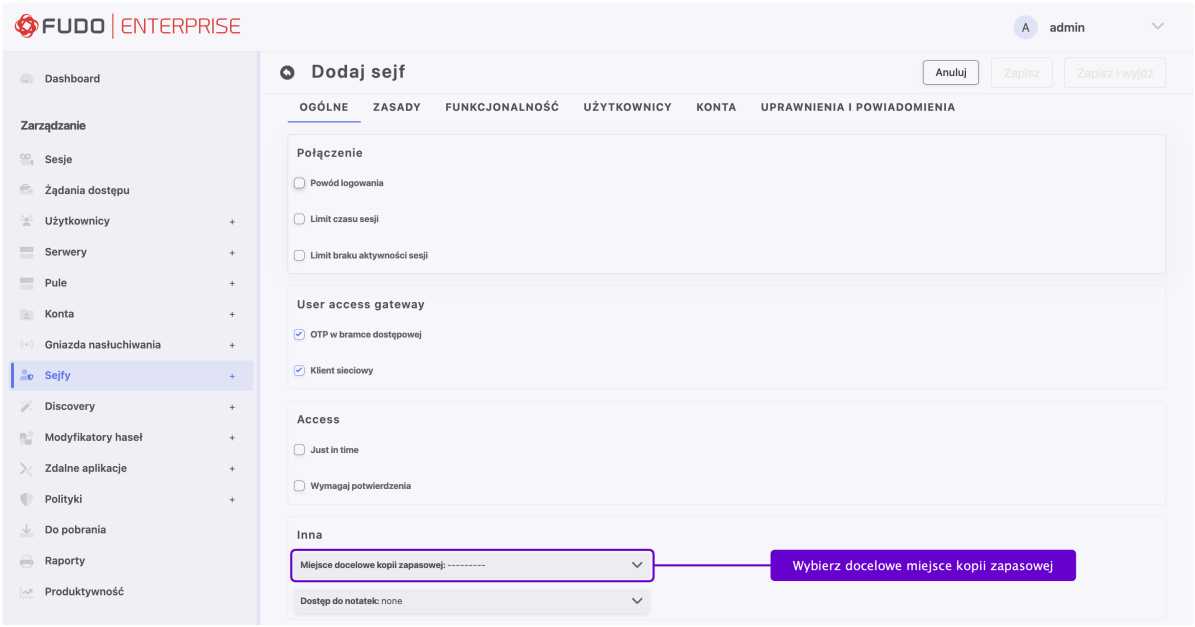
- Konfigurując miejsce docelowe kopii zapasowej w **Backblaze**, podaj: *Bucket, Katalog* i dane uwierzytelniające, takie jak *Konto* i *Klucz*.
- Dla typu kopii zapasowej **FTP** podaj: *Adres serwera (adres IP lub adres hosta), Katalog* i dane uwierzytelniające, takie jak *Nazwa użytkownika* i *Hasło*.

- W przypadku wyboru typu **S3** podaj dodatkowo: *Bucket, Katalog, Klucz dostępu, Tajny klucz dostępu, Region* i *Punkt końcowy.*
- Dla docelowego miejsca kopii zapasowej **SFTP** podaj: *Adres serwera (adres IP lub adres hosta), Nazwa użytkownika, Katalog, Klucz prywatny użytkownika, Klucz publiczny serwera* i *Numer portu.*



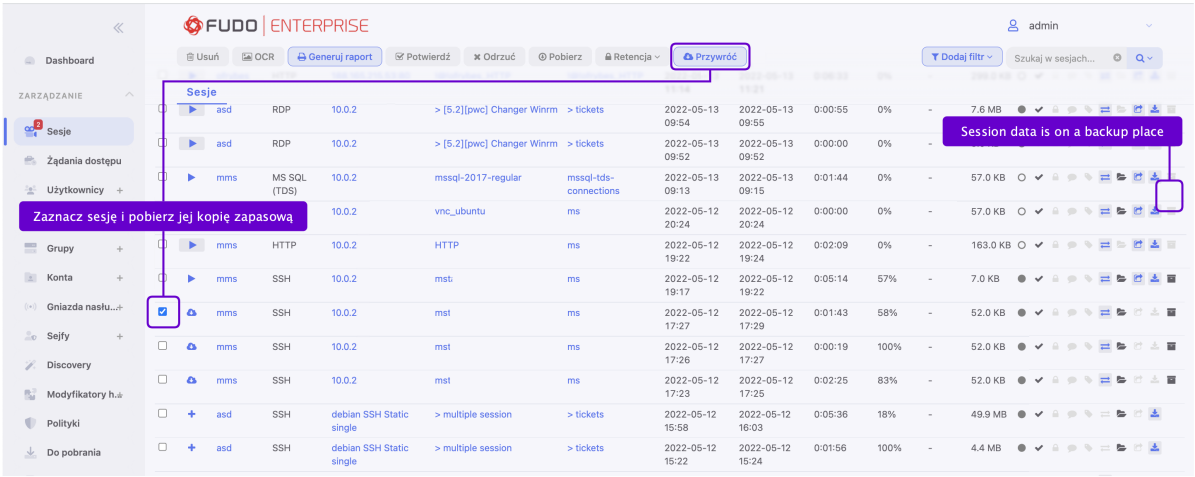
7. Kliknij *Zapisz.*

Skonfigurowane miejsce docelowe kopii zapasowej może też zostać dodane w ustawieniach Sejfu, aby dane sesji były przechowywane automatycznie.



Dane sesji, które zostały wysłane do docelowego miejsca kopii zapasowej, są oznaczone odpowiednią ikoną na liście sesji.

Jeśli sesja ma swoją kopię zapasową przechowywaną poza Fudo Enterprise, można ją pobrać z miejsca kopii zapasowej do lokalnej instancji Fudo Enterprise za pomocą opcji *Przywróć*.



Przywracanie systemu z kopii zapasowej

Usługa przywracania systemu jest świadczona przez dział wsparcia technicznego na warunkach uzgodnionych w SLA.

Tematy pokrewne:

- *Eksportowanie/importowanie konfiguracji systemu*
- *Środki bezpieczeństwa*
- *Tworzenie nowego sejfu*

22.14.2 Retencja danych

Fudo Enterprise obsługuje dwa scenariusze retencji danych w zależności od użycia pamięci zewnętrznej:

- **Dwuetapowa 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.
- **Jednoetapowa 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 *Usuwaj dane sesji* oraz w polu *Usuwaj dane sesji po* podaj liczbę dni, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.
3. W sekcji *Retencja logów*, zaznacz opcję *Usuwaj logi debug* oraz w polu *Usuwaj logi debug po* podaj liczbę dni, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.
4. W sekcji *Retencja logów - wrażliwe* podaj liczbę dni, aby dane starsze niż zdefiniowana wartość, były automatycznie usuwane.

Ostrzeżenie: Opcja *Usuwaj logi 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*

22.15 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.

22.15.1 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*.

22.15.2 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*

22.16 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.

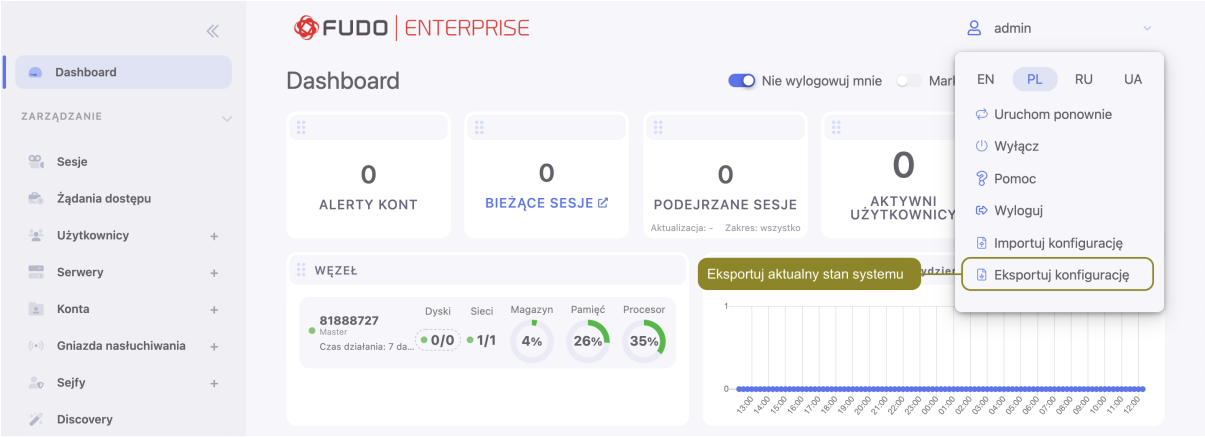
Ostrzeżenie: Wyeksportowana konfiguracja zawiera poufne informacje.

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

22.16.1 Eksportowanie konfiguracji

Aby wyeksportować konfigurację systemu, postępuj zgodnie z poniższą instrukcją.

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



22.16.2 Importowanie konfiguracji

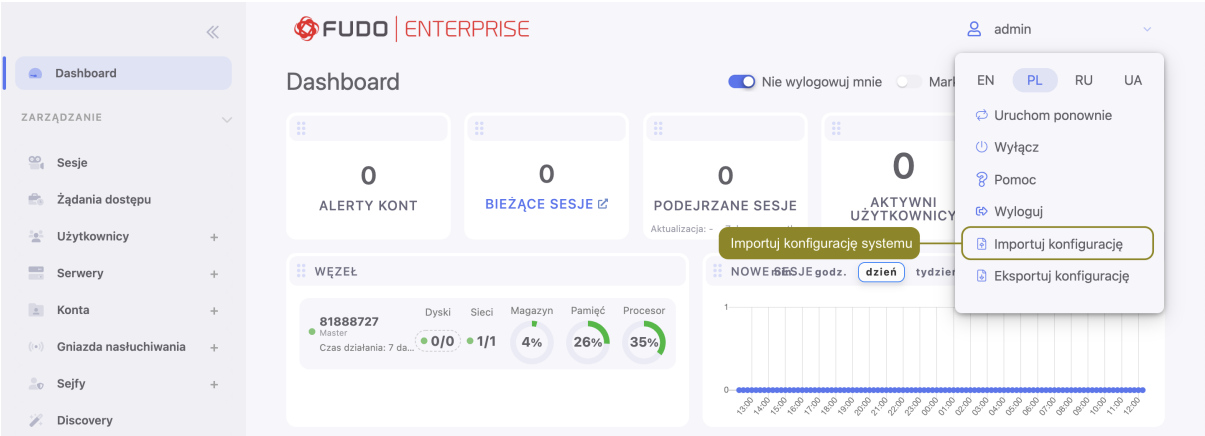
Ostrzeżenie: Zainicjowanie systemu wcześniej zapisaną konfiguracją spowoduje utratę wszystkich danych sesji.

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*

22.17 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.

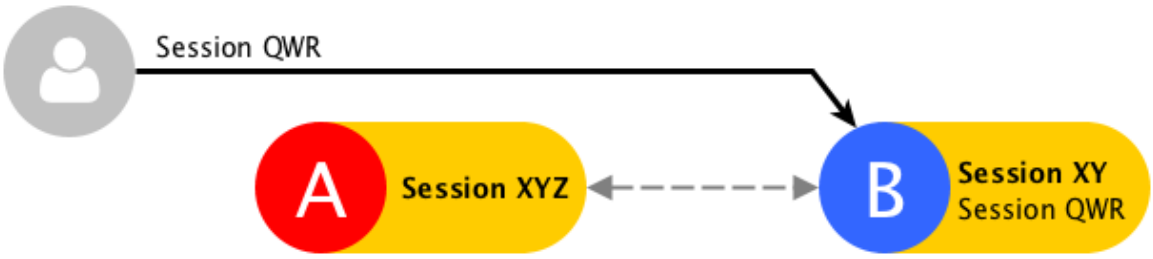
Schemat replikacji danych pomiędzy węzłami klastra jest konfigurowalny. Administrator może wybrać węzły, na które przesyłane są dane a także zdefiniować, które dane podlegają replikacji na wybraną instancję - obiekty modelu danych/sesje.

W przypadku awarii węzła, żądania dostępu do serwerów będą obsługiwane przez inny węzeł, zdeterminowany przez *priorytet grupy redundancji*.

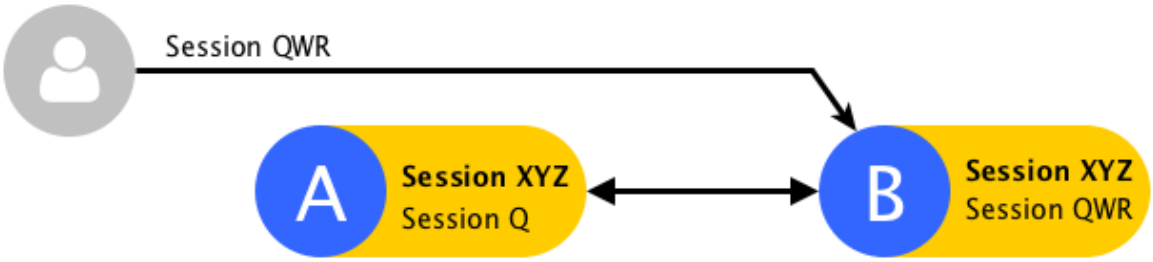
Dane bieżącej sesji są replikowane w trakcie jej trwania.

W przypadku, gdy węzeł ulegnie awarii, bieżące sesje zostaną zerwane...

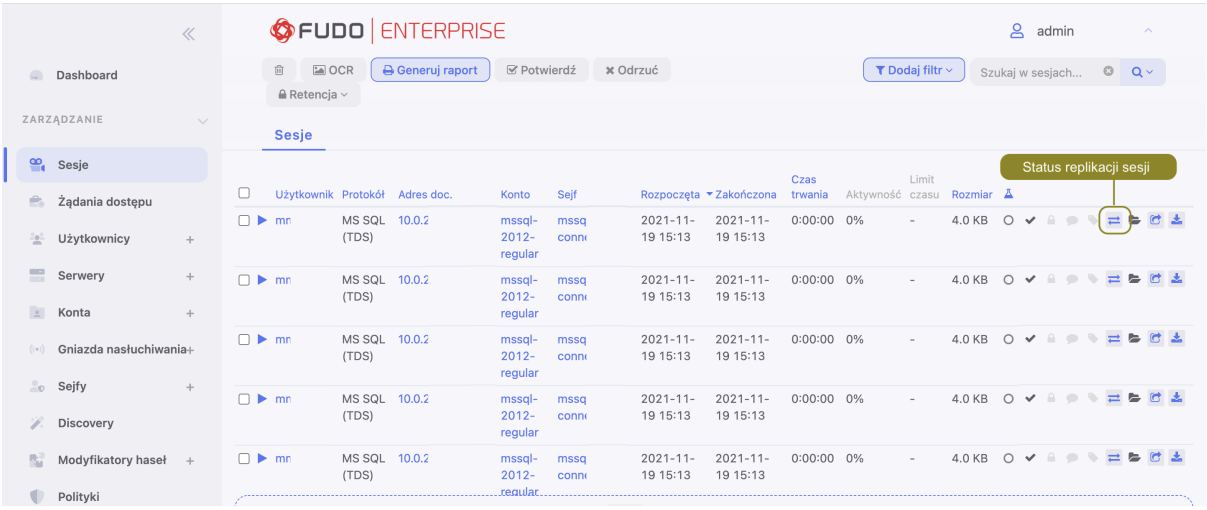
...a użytkownicy będą musieli ponownie nawiązać połączenie.



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 zsynchronizawaniu danych.



Stan replikacji danych sesji można zweryfikować klikając ikonę ⇄ na liście sesji.

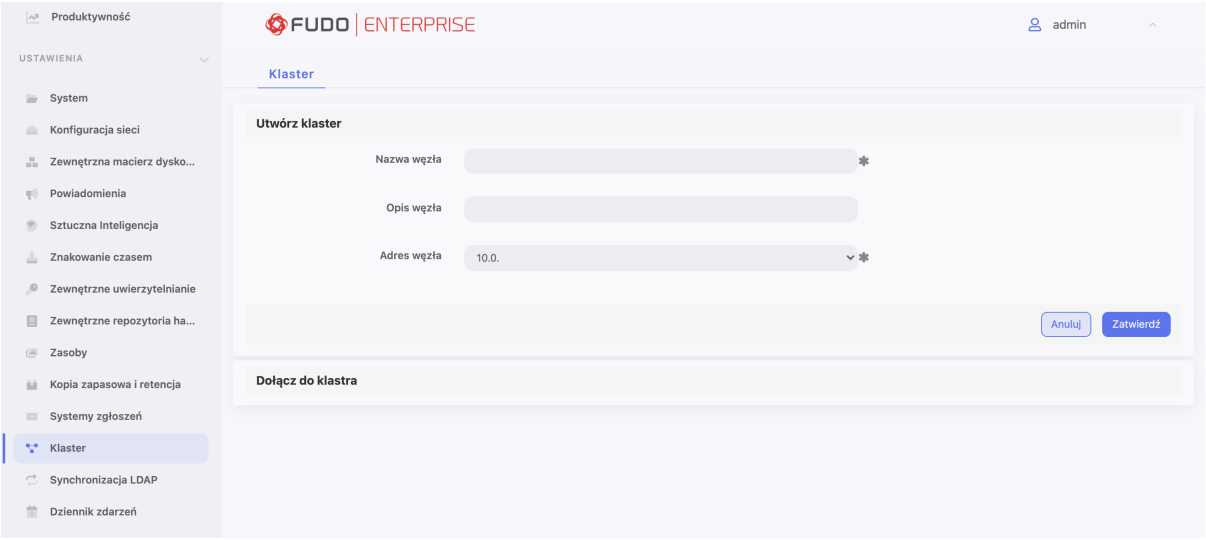


22.17.1 Inicjowanie klastra

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*

22.17.2 Zarządzanie węzłami klastra

22.17.2.1 Dodawanie węzłów klastra

Ostrzeżenie:

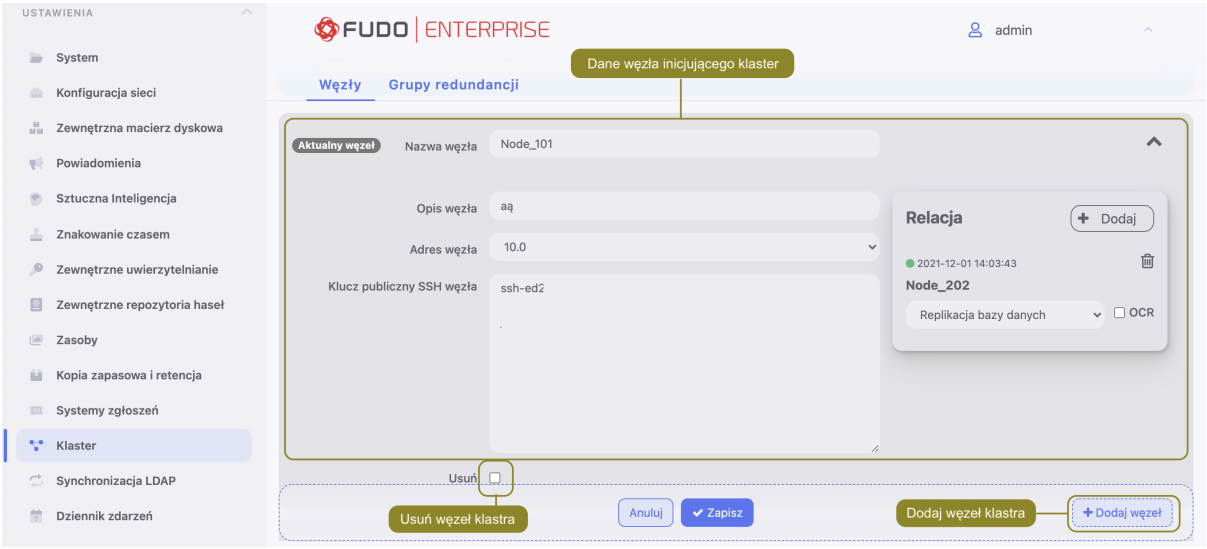
- Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i nie należy dodawać ich ręcznie na każdym z wę-

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.

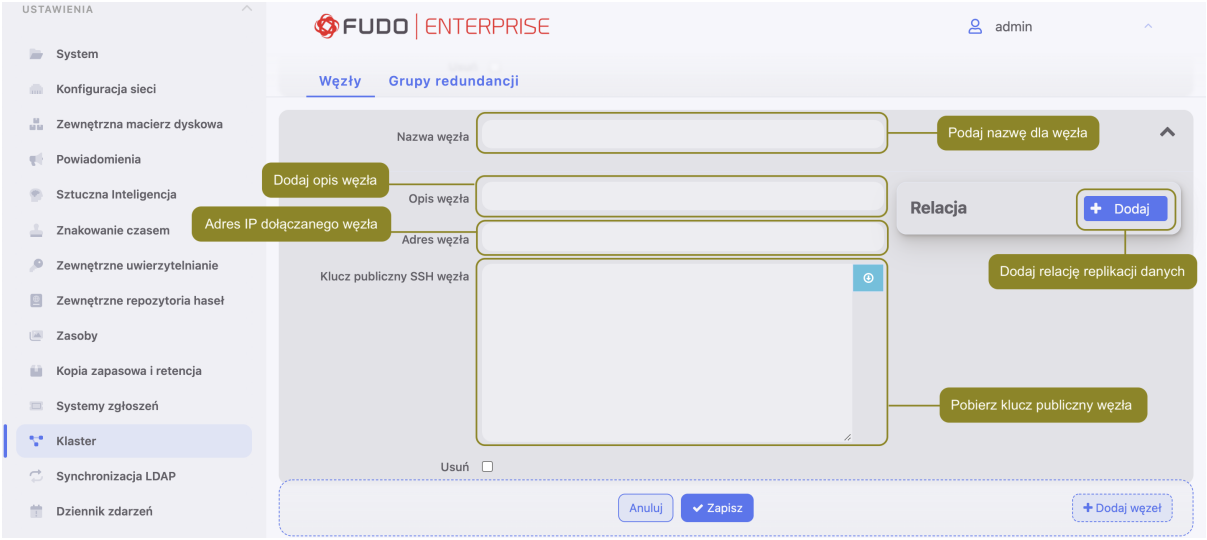
Aby dodać węzeł do klastra Fudo Enterprise, postępuj zgodnie z poniższą instrukcją.

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

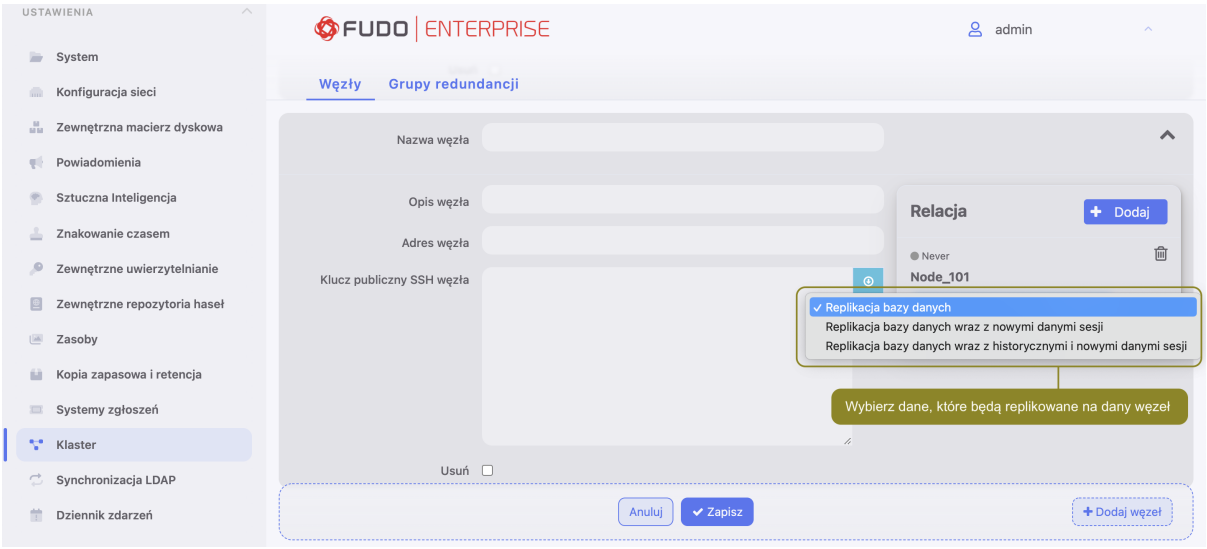


4. Wprowadź nazwę węzła oraz opis, ułatwiający identyfikację obiektu.
5. Podaj adres IP węzła dołączanego.

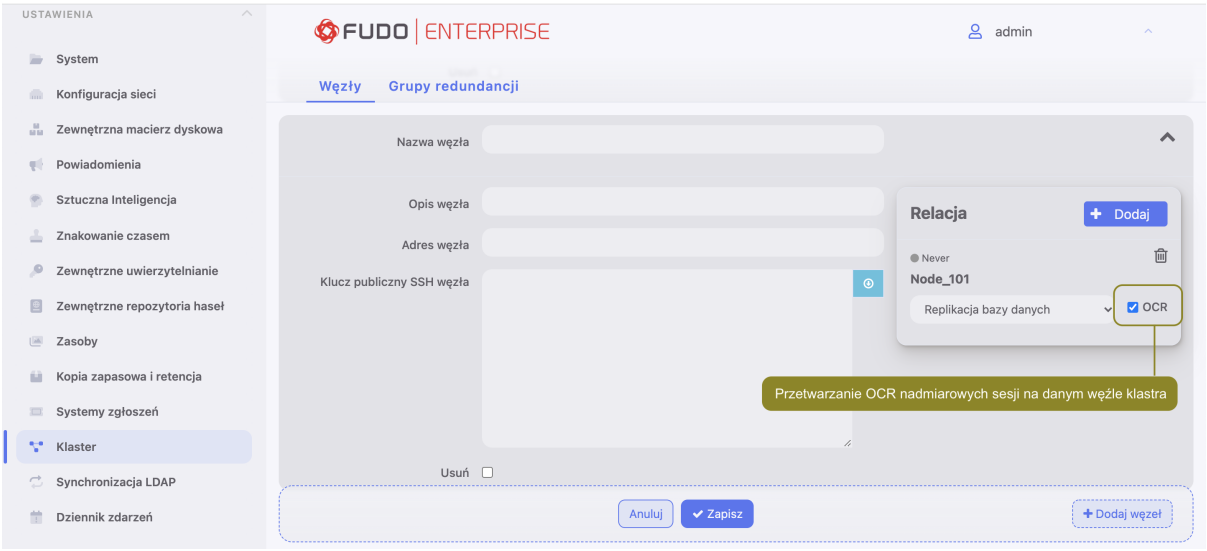
Informacja: Na wskazanym interfejsie sieciowym dołączanego węzła musi być aktywna opcja zarządzania urządzeniem. Informacje na temat konfigurowania ustawień sieciowych znajdziesz w rozdziale *Ustawienia sieci: Konfiguracja interfejsów sieciowych*.



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.

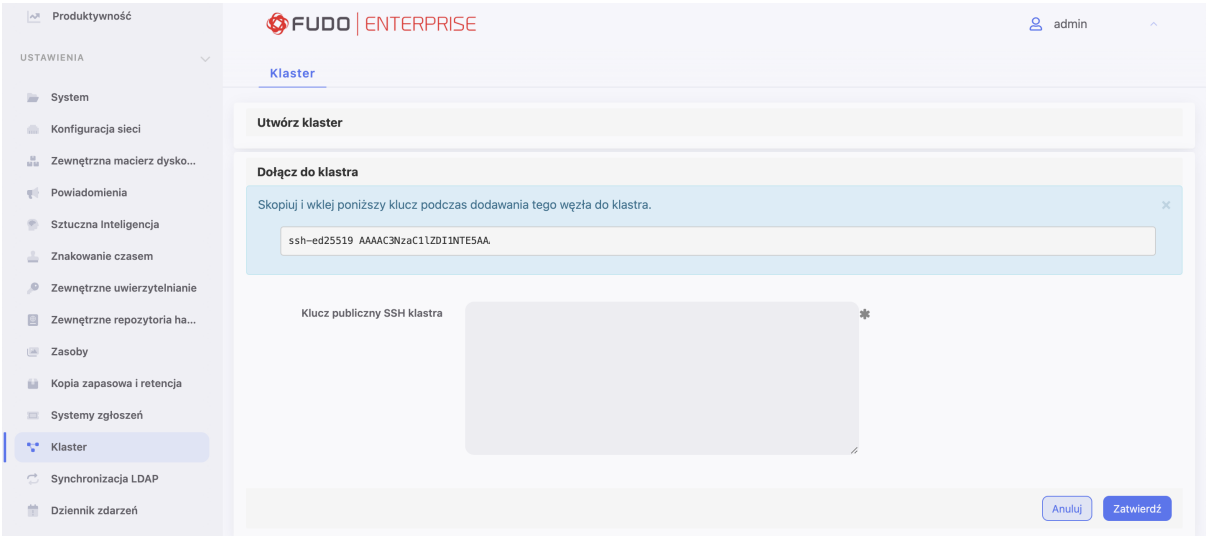


10. Zaznacz opcję *OCR*, aby wybrany węzeł przetwarzał nadwyżkę sesji graficznych.



Informacja: Każda instancja Fudo Enterprise ma ograniczoną, zdefiniowaną w licencji, liczbę procesów OCR przetwarzających sesje graficzne. Opcja *OCR* umożliwia oddelegowanie przetwarzania nadmiarowych sesji na wskazany węzeł, w sytuacji, w której liczba połączeń przekracza liczbę lokalnych procesów przetwarzających i indeksujących treść.

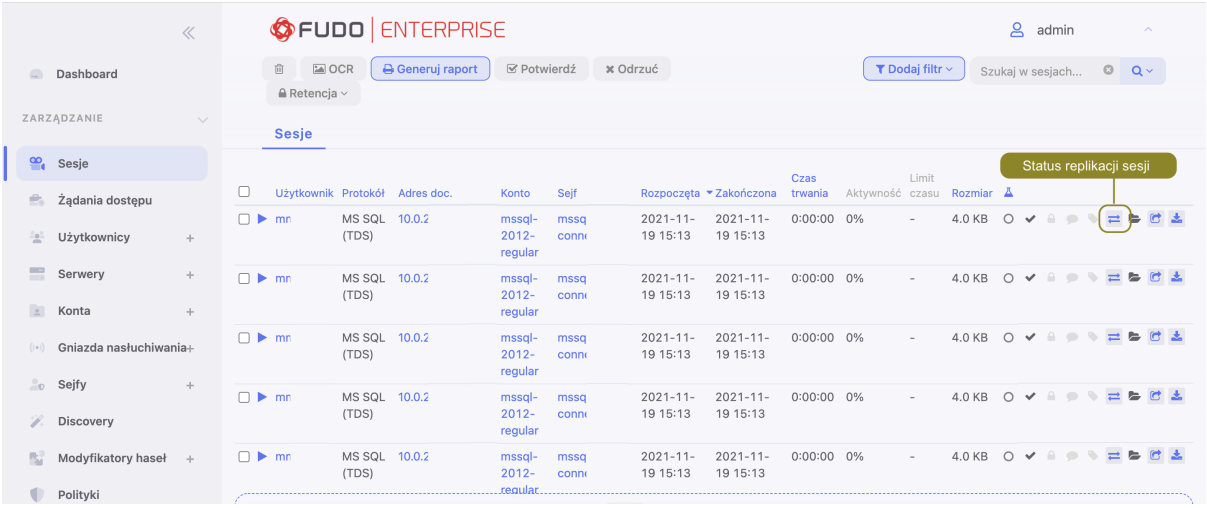
11. W sekcji *Relacje* węzła, na którym został zainicjowany klaster, kliknij przycisk *+ Dodaj*.
12. Wybierz z listy dołączany węzeł.
13. Z listy rozwijalnej, wybierz jakie dane mają podlegać replikacji na wybrany węzeł klastra.
14. Kliknij *Zapisz*.
15. Skopiuj klucz publiczny klastra.
16. Zaloguj się do panelu administracyjnego węzła dołączanego.
17. Wybierz z lewego menu *Ustawienia* > *Klaster*.
18. Wybierz opcję *Dołącz do klastra*.



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

20. Kliknij przycisk *Rozumiem konsekwencje, kontynuuj.*

Informacja: Aby sprawdzić status replikacji sesji, odszukaj połączenie na liście sesji i kliknij ikonę ⇄.



Tematy pokrewne:

- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

22.17.2.2 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 żądanego węzła.
3. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

22.17.2.3 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. Zaznaczy opcję *Usuń* przy wybranym węźle klastra i kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Edytowanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

22.17.3 Grupy redundancji

Grupy redundancji umożliwiają realizację scenariuszy niezawodnościowych. W przypadku awarii węzła pełniącego dla danej grupy redundancji rolę nadrzędną, przypisane do grupy adresy IP zostaną przejęte przez inny węzeł o najwyższym dla danej grupy priorytecie. Nadanie różnym grupom odpowiednich priorytetów na poszczególnych węzłach klastra pozwala na statyczne balansowanie obciążeniem węzłów przy zachowaniu funkcjonalności klastra niezawodnościowego.

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

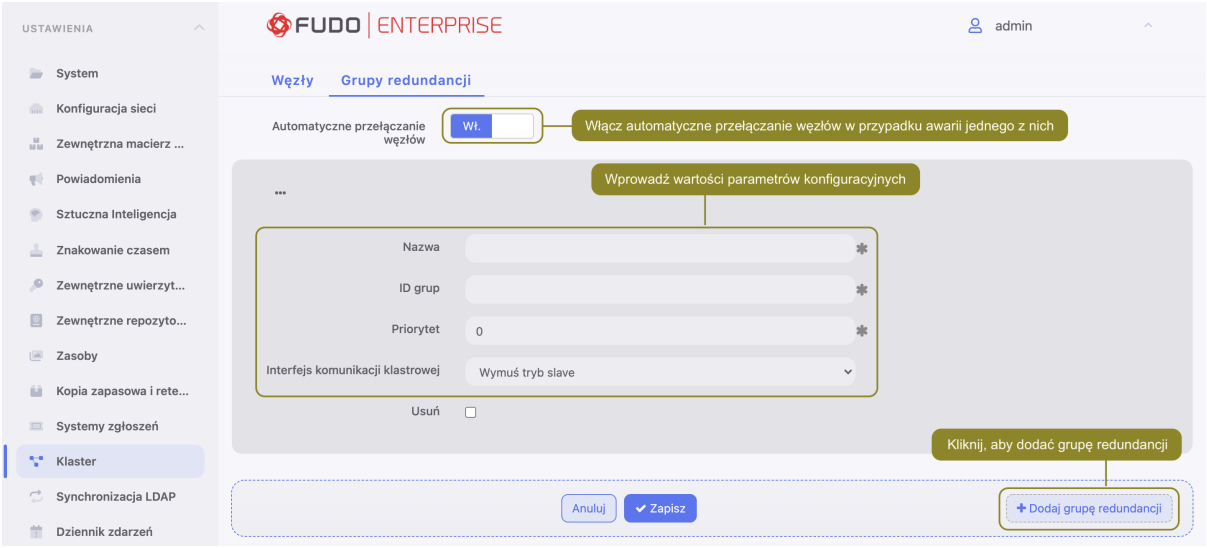
Dodawanie grup redundancji

Aby dodać grupę redundancji, postępuj zgodnie z poniższą instrukcją.

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

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

Informacja: Domyślnie, przypisanie roli *master* do węzła działa na zasadzie czasu nieokreślonego.



5. Kliknij *Zapisz*.
6. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
7. Kliknij [+], aby dodać adres IP.
8. Wprowadź adres IP i kliknij [▦], aby nadać mu atrybut klastrowy.
9. Z listy rozwijalnej wybierz wcześniej zdefiniowaną grupę redundancji.
10. Kliknij *Zapisz*.

Informacja: Klastrowy adres IP należy zdefiniować na każdym z węzłów klastra.

Edytowanie grup redundancji

Aby zmodyfikować grupę redundancji, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.

2. Przejdź do zakładki *Grupy redundancji*.
3. Zmień parametry wybranej grupy redundancji.
4. Kliknij *Zapisz*.

Usuwanie grup redundancji

Aby usunąć grupę redundancji, postępuj zgodnie z poniższą instrukcją.

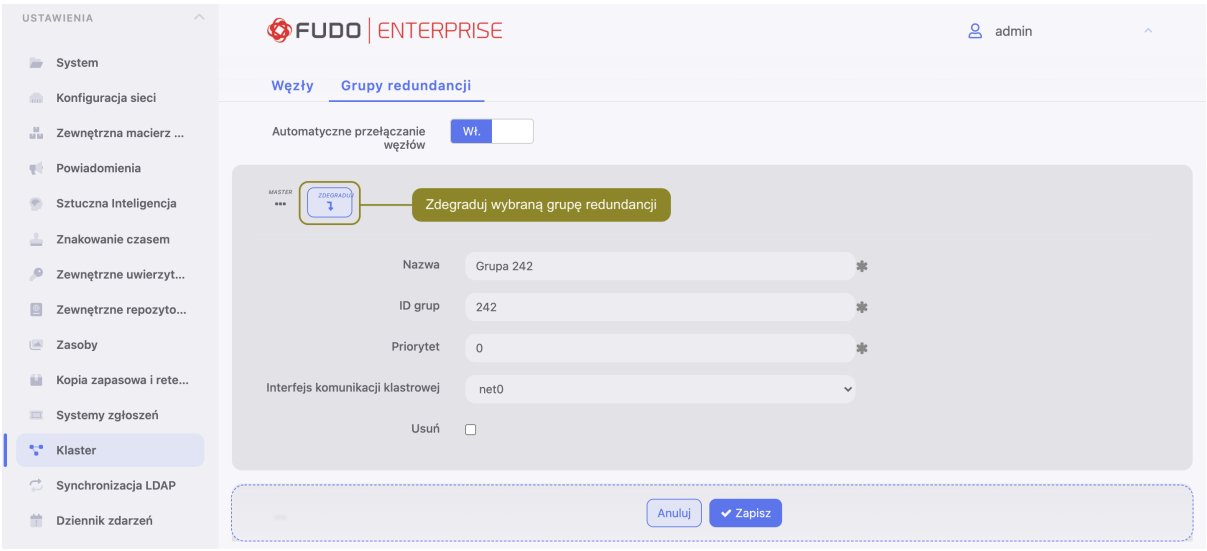
1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *Grupy redundancji*.
3. Zaznacz opcję *Usuń* przy wybranej grupie redundancji.
4. Kliknij *Zapisz*.

Degradowanie grupy redundancji

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

Aby zdegradować grupę redundancji, postępuj zgodnie z poniższą instrukcją.

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



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

Wymuszanie roli podrzędnej

Informacja: Wymuszenie roli podrzędnej spowoduje, że grupa redundancji nigdy nie przejdzie w tryb nadrzędny, niezależnie od stanu pozostałych węzłów klastra. Wymuszanie roli podrzędnej zalecane jest przed wykonywaniem prac serwisowych, aby ruch sieciowy kierowany był do pozostałych węzłów klastra. Innym przypadkiem użycia jest węzeł klastra, wdrożony w odrębnej lokalizacji, bez możliwości komunikacji z pozostałymi węzłami klastra w warstwie drugiej.

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

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

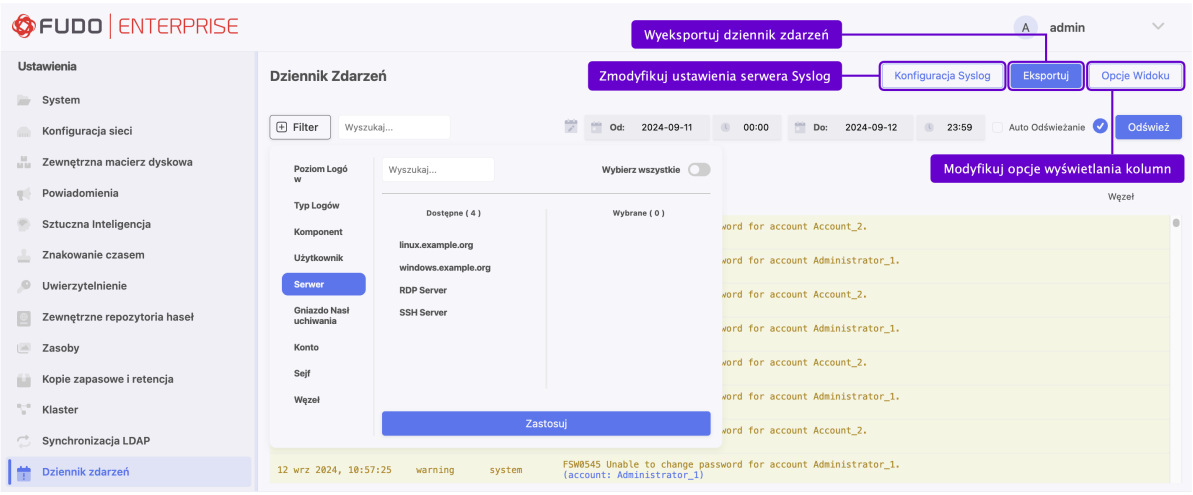
Tematy pokrewne:

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

22.18 Dziennik zdarzeń

Dziennik zdarzeń stanowi wewnętrzny zapis akcji użytkowników mających wpływ na stan systemu (logowanie użytkowników, czynności administracyjne, itp.). Przejdź do rozdziału *Komunikaty dziennika zdarzeń* aby zapoznać się z listą kluczowych komunikatów dziennika.

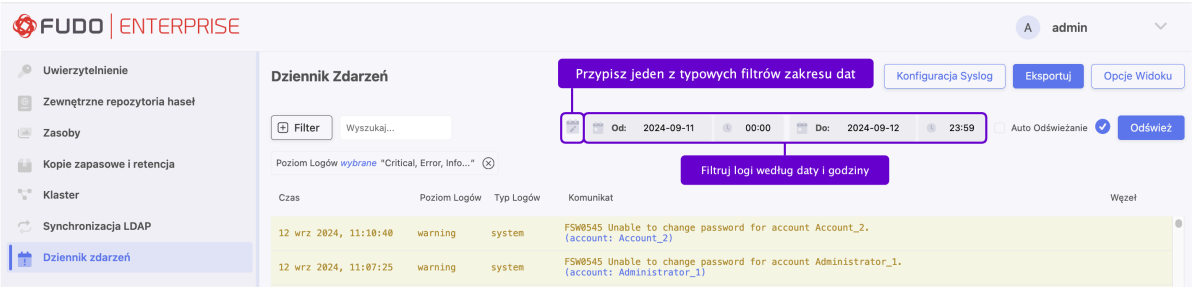
Aby wyświetlić zawartość dziennika systemowego, wybierz *Ustawienia* > *Dziennik zdarzeń*.



22.18.1 Filtrowanie logów według daty i czasu

Dzienniki można filtrować według daty i czasu bezpośrednio z paska daty znajdującego się nad listą zdarzeń. Dodatkowo dostępny jest zestaw często używanych filtrów zakresu dat, takich

jak *Dziś*, *Ostatnie 24 godziny*, *Ten tydzień*, *Ostatnia 1 godzina*, *Ostatni rok* itp., dostępnych z poziomu ikony kalendarza.



22.18.2 Zewnętrzne serwery syslog

Fudo Enterprise pozwala na przesyłanie rejestrowanych zdarzeń do zewnętrznych serwerów syslog.

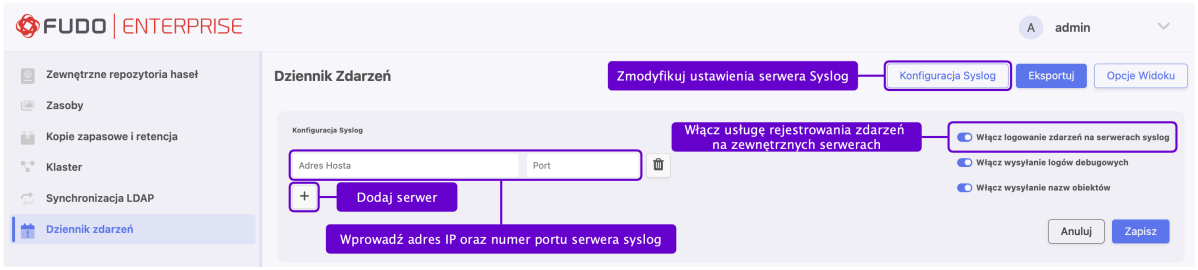
Informacja:

- 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 *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Konfiguracja syslog*, aby wyświetlić ustawienia konfiguracji serwerów syslog.
3. Wybierz opcję *Włącz logowanie zdarzeń na serwerach syslog*, aby aktywować wysyłanie dzienników do zdefiniowanych serwerów syslog.
4. Wybierz opcję *Włącz wysyłanie logów debugowych* w celu uruchomienia usługi wysłania komunikatów z treścią logów debugowych do serwera zewnętrznego.
5. Wybierz opcję *Włącz wysyłanie nazw obiektów*, aby aktywować wysyłanie nazw obiektów w wiadomościach do zdefiniowanego syslogu.
6. Wprowadź adres IP oraz numer portu serwera syslog.
7. Kliknij *Zapisz*.



Informacja:

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

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

- Przykład:

  ```
  [INFO] (fudordp) (fudo_server: 848388532111147015) (fudo_session:
  848388532111147219) (fudo_user: 848388532111147012)
  (fudo_connection:      848388532111147014) User user0 authenticated
  using password logged in from IP addres: 10.0.40.101.
  ```

- Lista komunikatów dziennika znajduje się w sekcji *Komunikaty dziennika zdarzeń*.

Modyfikowanie serwera Syslog

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

1. Wybierz *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Konfiguracja syslog*, aby wyświetlić ustawienia konfiguracji serwerów syslog.
3. Znajdź i edytuj żądaną definicję serwera syslog.
4. Kliknij *Zapisz*.

Usuwanie serwera Syslog

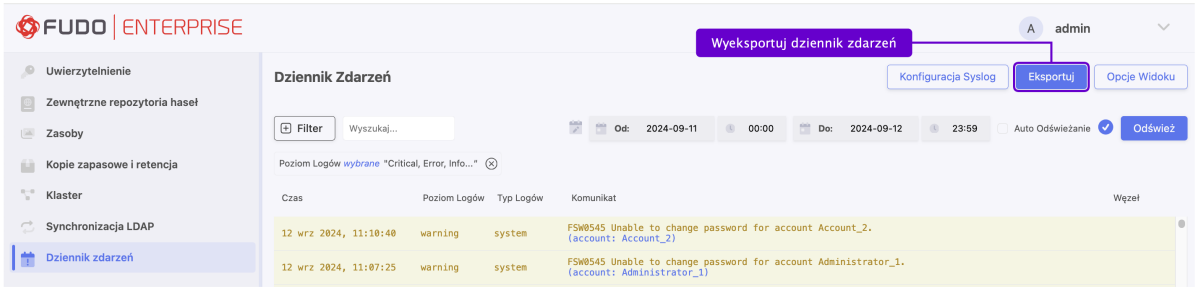
Aby usunąć serwer *Syslog*, postępuj zgodnie z poniższą instrukcją.

1. Wybierz *Ustawienia* > *Dziennik zdarzeń*.
2. Kliknij *Konfiguracja syslog*, aby wyświetlić ustawienia konfiguracji serwerów syslog.
3. Znajdź żądaną definicję serwera i kliknij ikonę i.
4. Kliknij *Zapisz*.

22.18.3 Eksportowanie dziennika zdarzeń

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

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



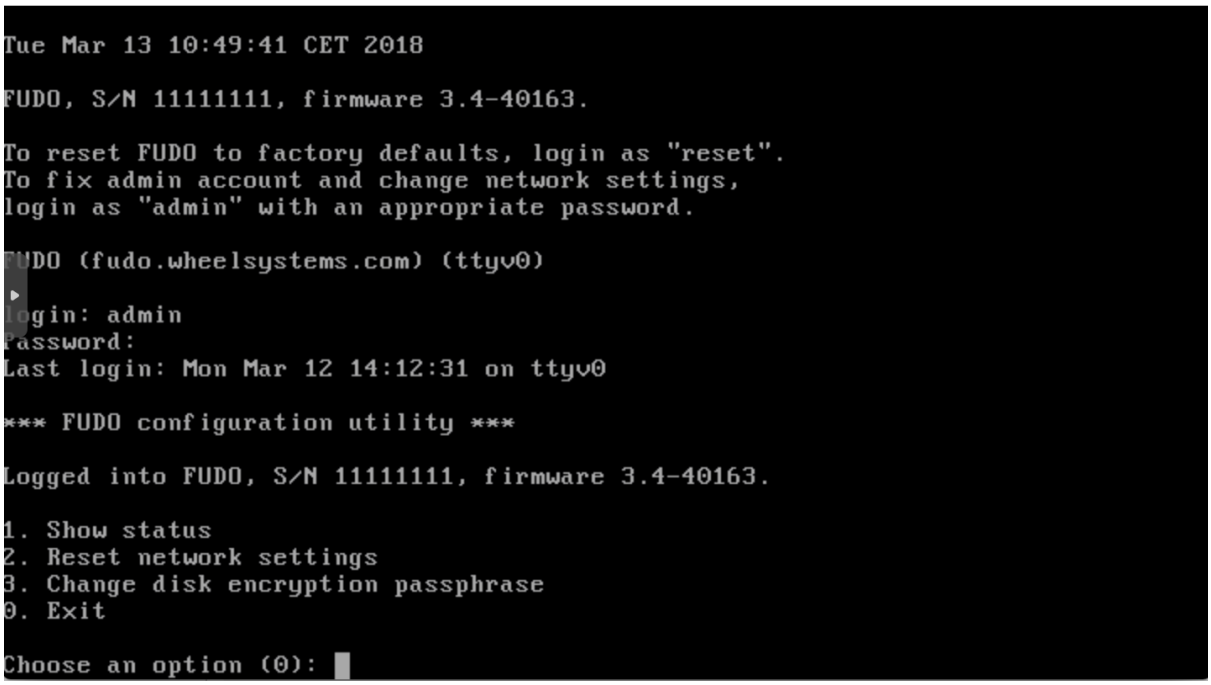
Powiązane tematy:

- *Komunikaty dziennika zdarzeń*
- *Bezpieczeństwo*
- *Zarządzanie serwerami*

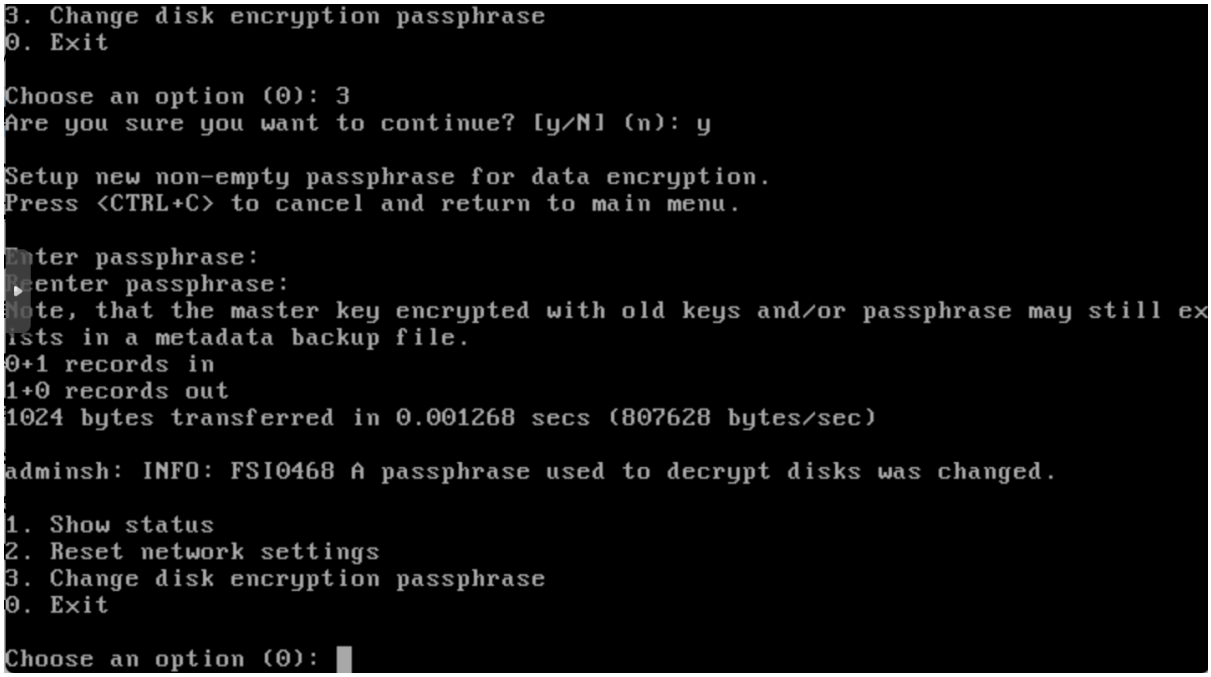
22.19 Zmiana frazy szyfrującej

W środowisku wirtualnym, dane szyfrowane są frazą szyfrującą. Aby zmienić frazę, postępuj zgodnie z poniższą instrukcją.

1. Zaloguj się do konsoli systemowej na konto z uprawnieniami *superadmin*.
2. Wpisz 3 i naciśnij klawisz *Enter*.



3. Wpisz y i naciśnij klawisz *Enter*, aby potwierdzić zmianę frazy szyfrującej.
4. Wprowadź nową frazę i zatwierdź klawiszem *Enter*.
5. Ponownie wprowadź frazę szyfrującą i zatwierdź klawiszem *Enter*.



6. Uruchom ponownie system, aby zastosować zmiany.

Tematy pokrewne:

- *Aktualizacja systemu*
- *Kopia zapasowa systemu*

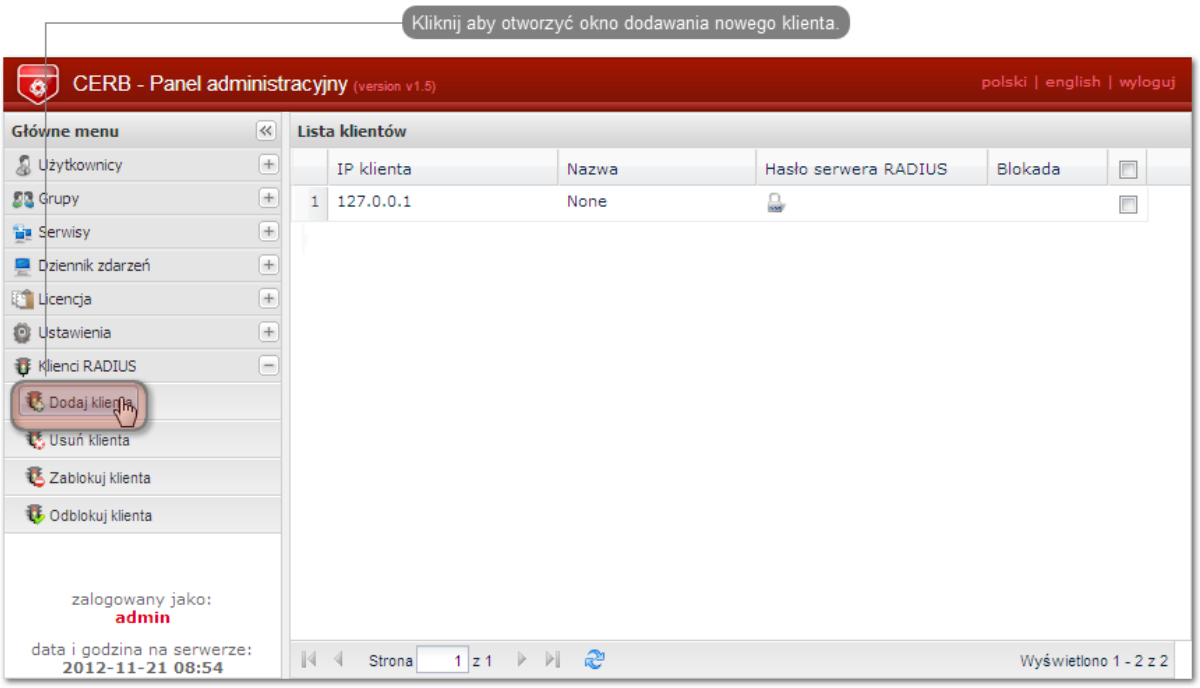
22.20 Integracja z serwerem CERB

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

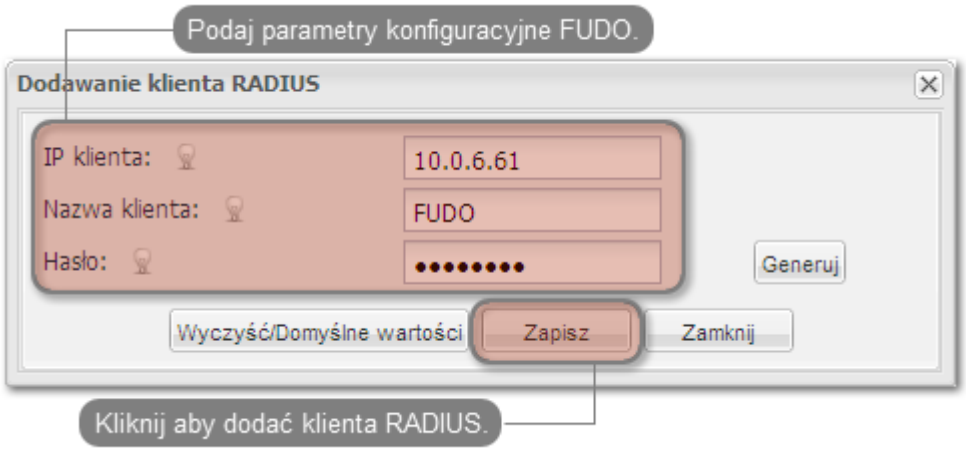
Konfiguracja serwera CERB

1. Dodanie klienta RADIUS.

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



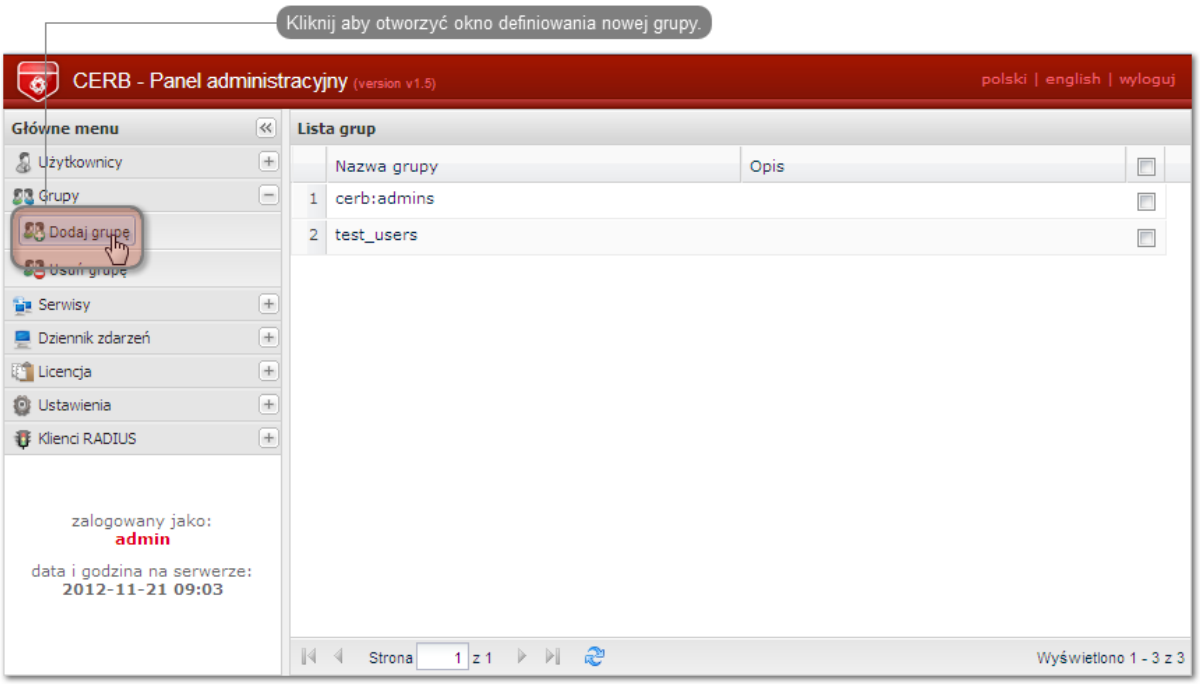
- Podaj adres IP serwera Fudo Enterprise, nazwę klienta oraz hasło i kliknij *Zapisz*.



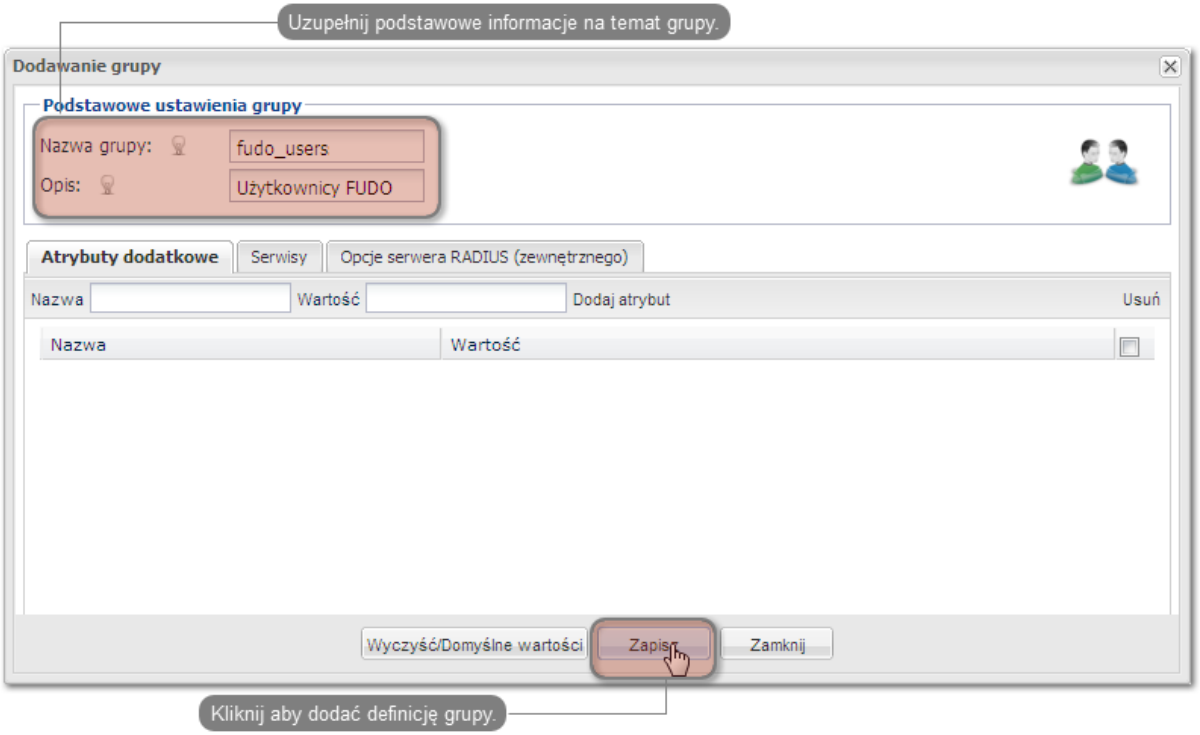
Informacja: Hasło będzie wymagane do skonfigurowania zewnętrznego serwera uwierzytelniania w panelu administracyjnym Fudo Enterprise.

2. Dodanie grupy użytkowników.

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

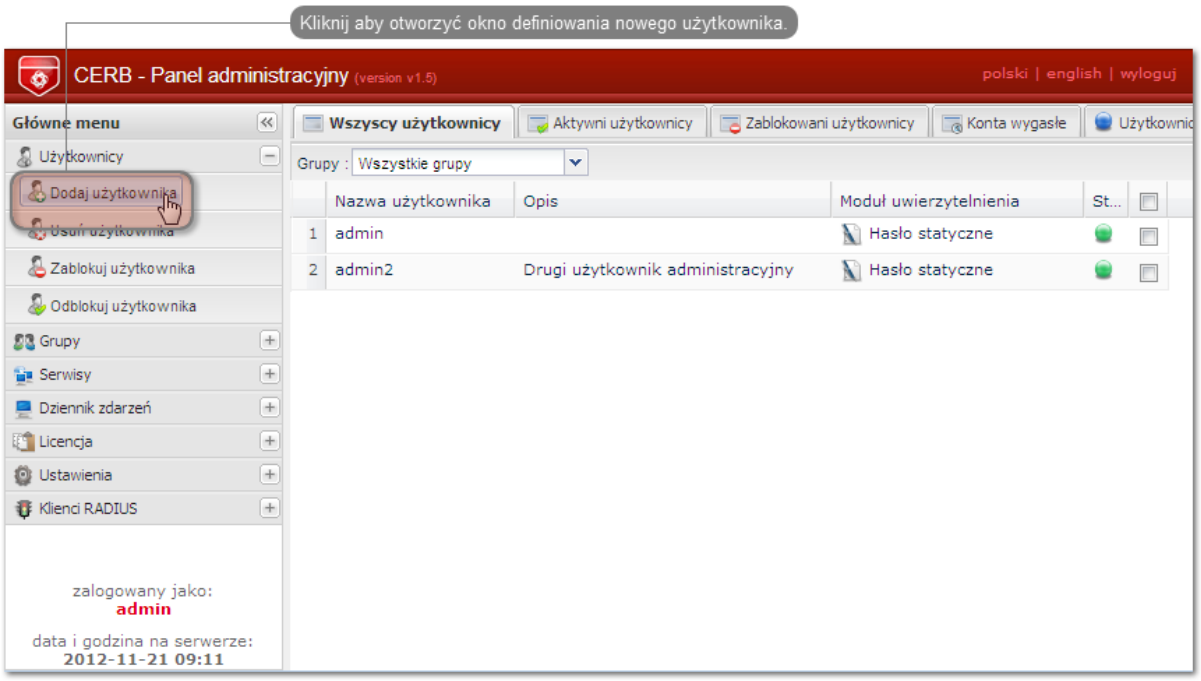


- Podaj nazwę grupy (`fudo_users`) i kliknij *Zapisz*.

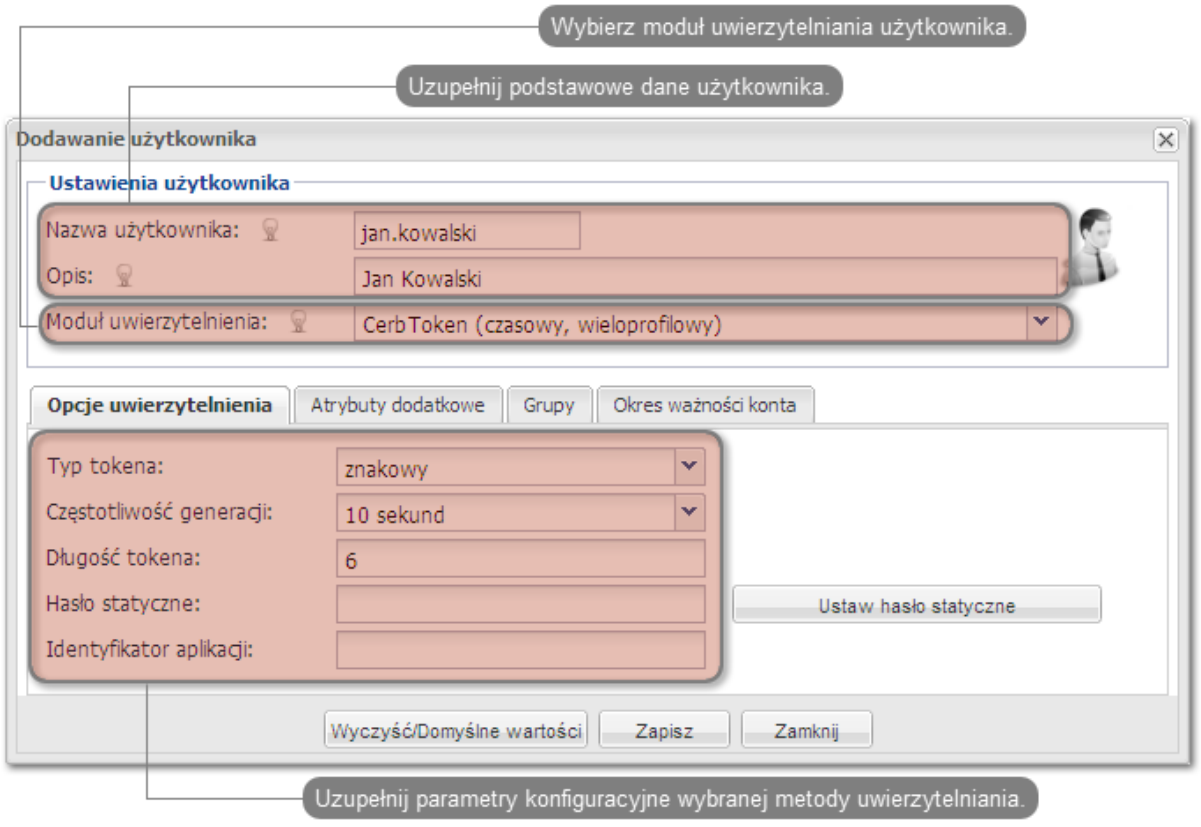


3. Dodanie użytkownika.

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

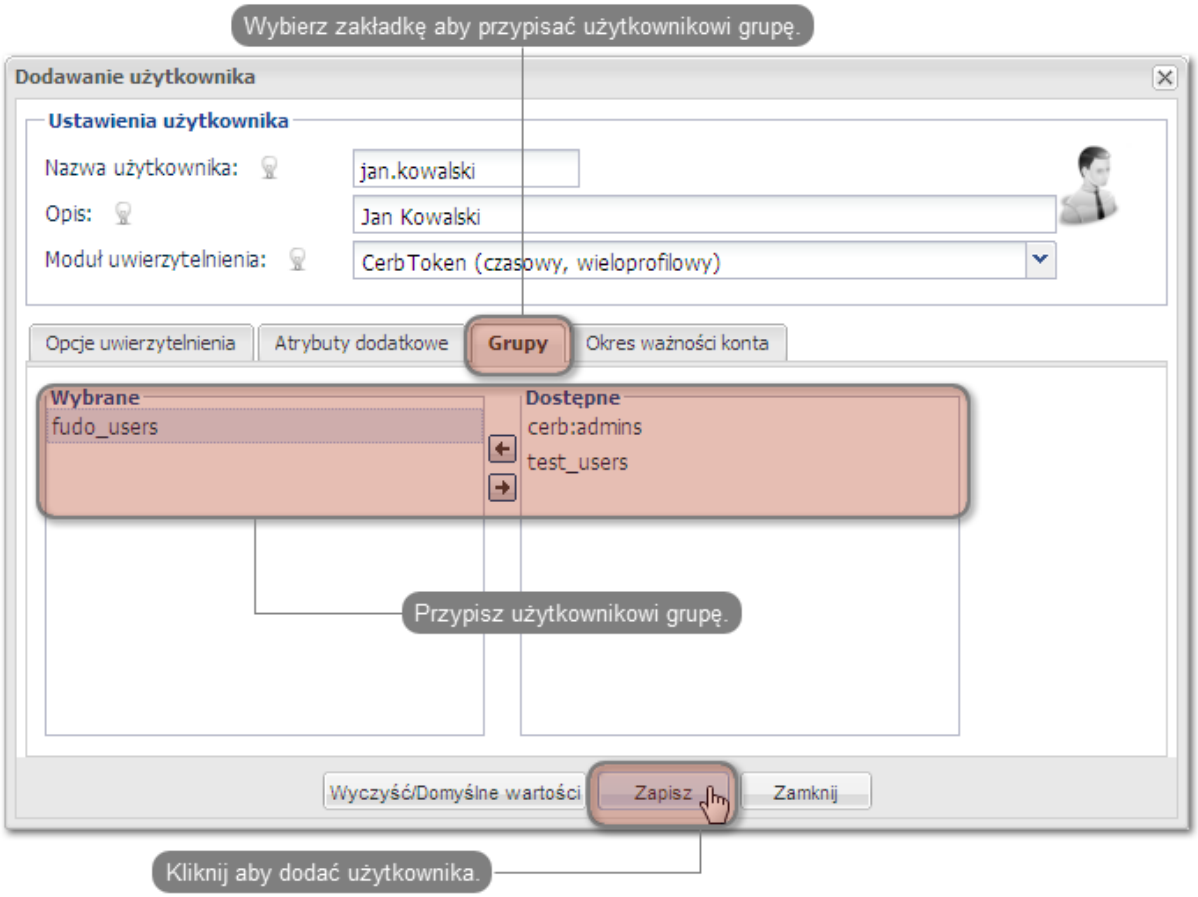


- Podaj nazwę użytkownika, opis oraz wybierz stosowny moduł uwierzytelniania (więcej informacji na temat modułów uwierzytelniania znajdziesz w dokumentacji serwera CERB).



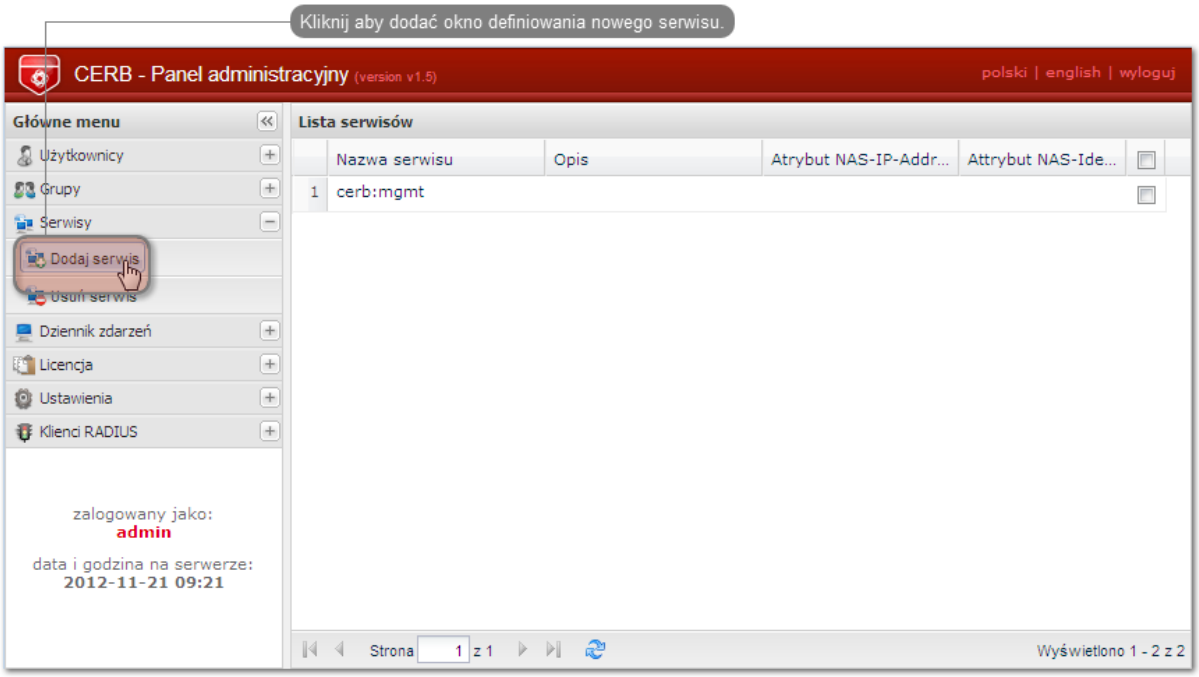
Informacja: Nazwa użytkownika wykorzystywana jest w procesie uwierzytelniania użytkowników łączących się z Fudo Enterprise.

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

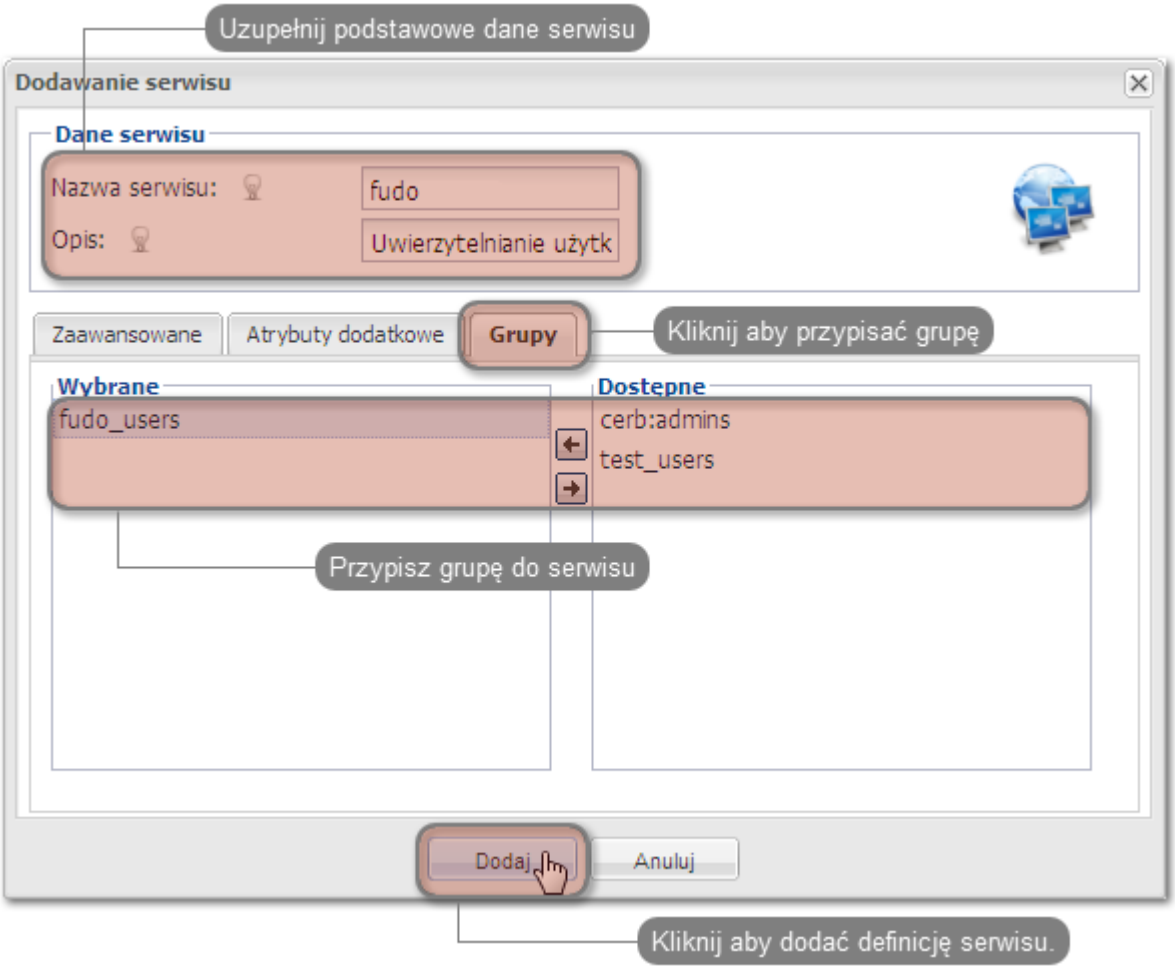


4. Skonfigurowanie serwisu.

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



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

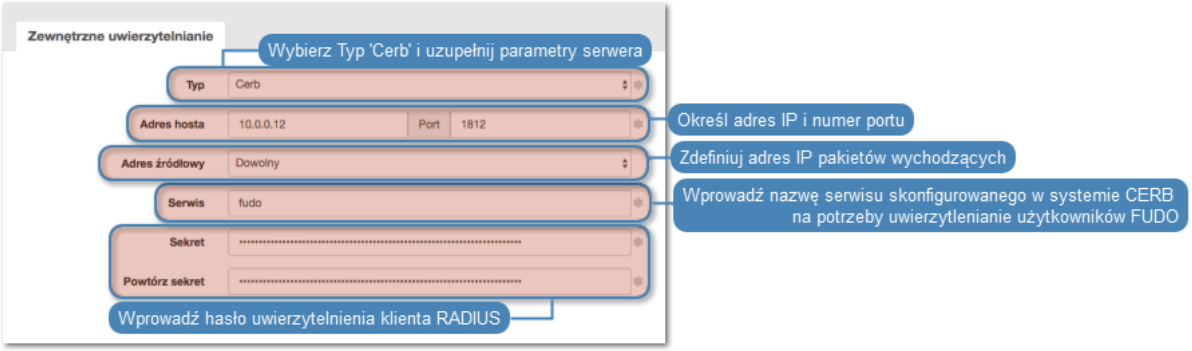


Konfiguracja serwera Fudo Enterprise

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 identyfikowana będzie usługa uwierzytelniania.

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



- Kliknij *Zapisz*.

2. Dodanie użytkownika.

- Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
- Kliknij *+ Dodaj*.
- Podaj podstawowe dane użytkownika.

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

- Przypisz użytkownikowi sejf, za pośrednictwem którego będzie mógł się łączyć do wybranych zasobów.
- W sekcji *Uwierzytelnienie*, z listy rozwijalnej *Typ*, wybierz `Zewnętrzne uwierzytelnienie` i wskaż wcześniej dodany serwer.

- Kliknij *Zapisz*.

Tematy pokrewne:

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

22.21 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.

22.21.1 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

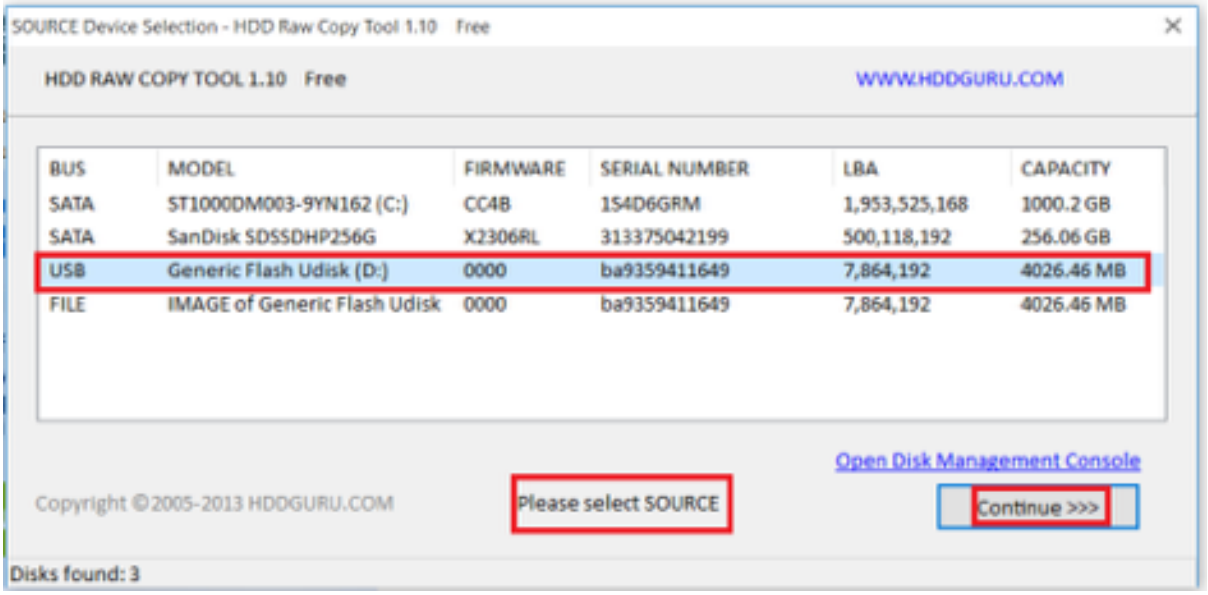
Ostrzeżenie: Po podłączeniu nośnika USB do komputera, pod żadnym pozorem nie należy wykonywać jego inicjowania/formatowania. Komunikat systemowy o braku możliwości odczytu danych należy zignorować i przystąpić do procedury tworzenia kopii zapasowej.

1. Pobierz i zainstaluj program *HDD Raw Copy Tool*.

   `http://hddguru.com/software/HDD-Raw-Copy-Tool/` (dostępna również wersja przenośna)

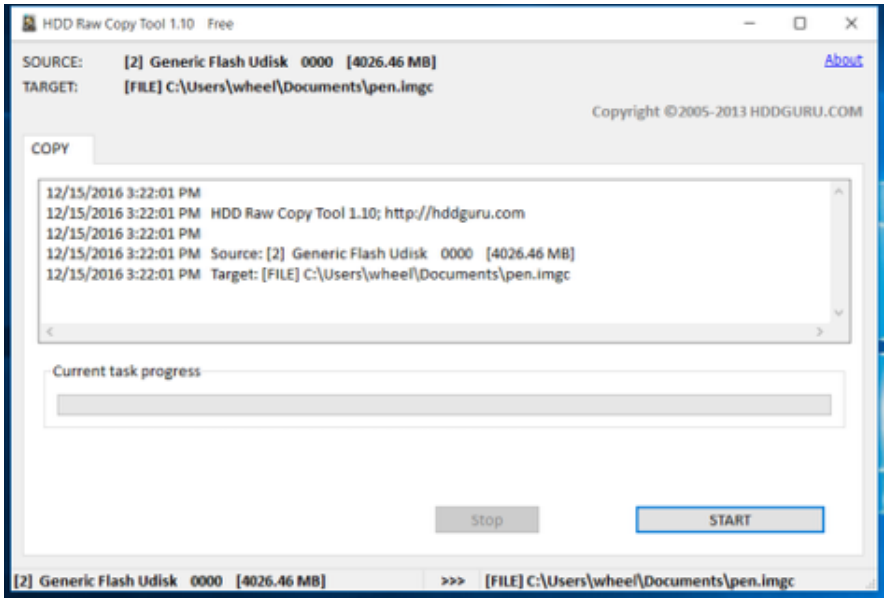
2. Uruchom program.

3. Na ekranie wyboru napędu źródłowego, zaznacz napęd USB z zapisanymi kluczami szyfrującymi i kliknij *Continue*.



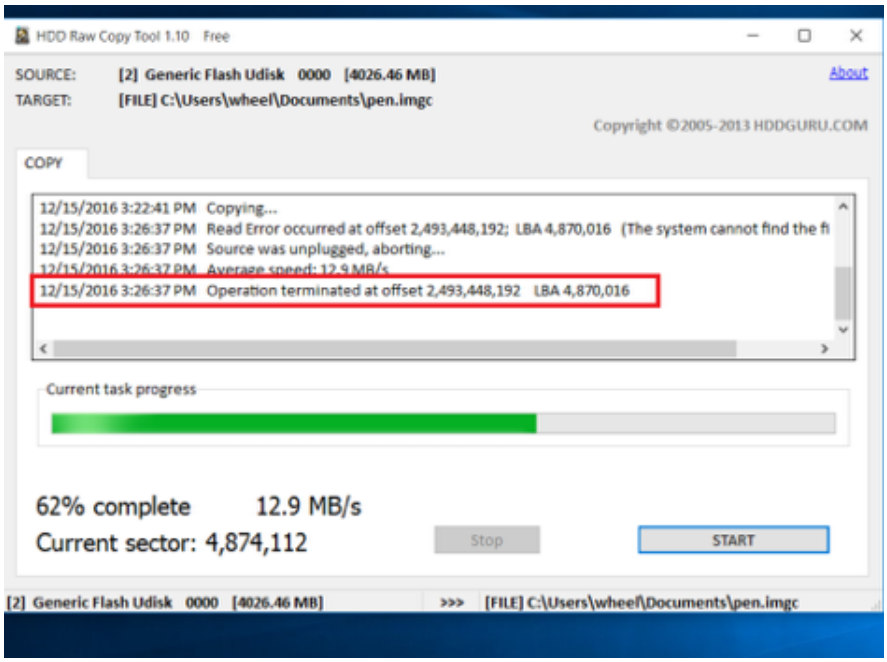
4. Kliknij dwukrotnie *FILE*, wskaż plik docelowy, w którym zapisany zostanie obraz dysku i kliknij *Continue*.

5. Kliknij *START*, aby rozpocząć procedurę kopiowania.

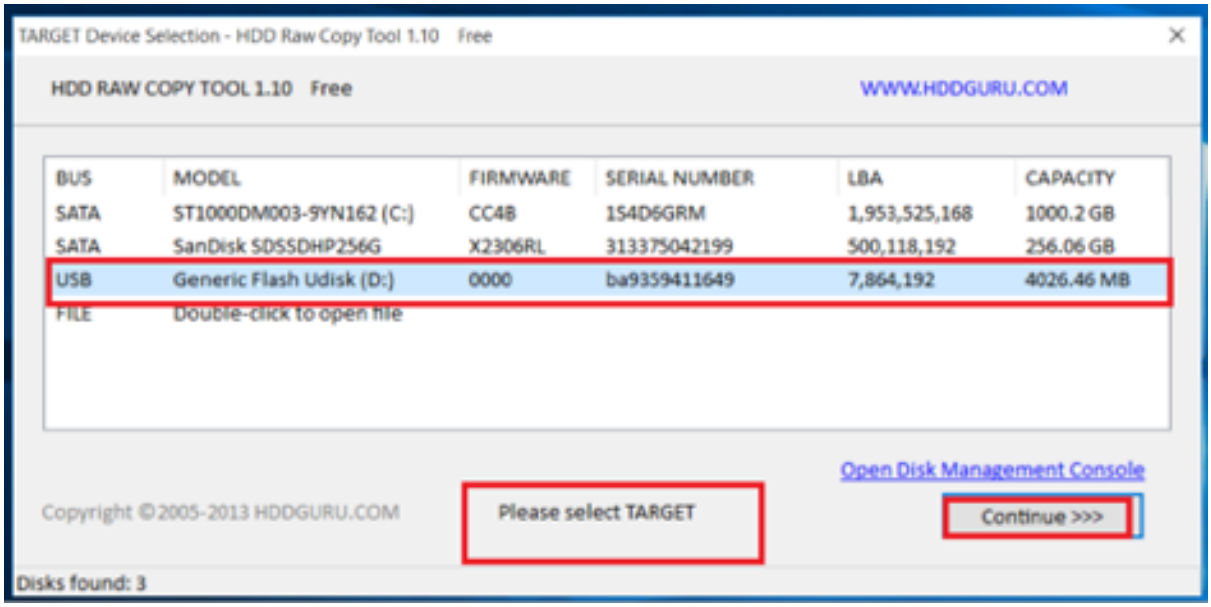


6. Z chwilą wystąpienia komunikatu

   `Operation terminated at offset...`, zamknij okno i odłącz napęd USB.

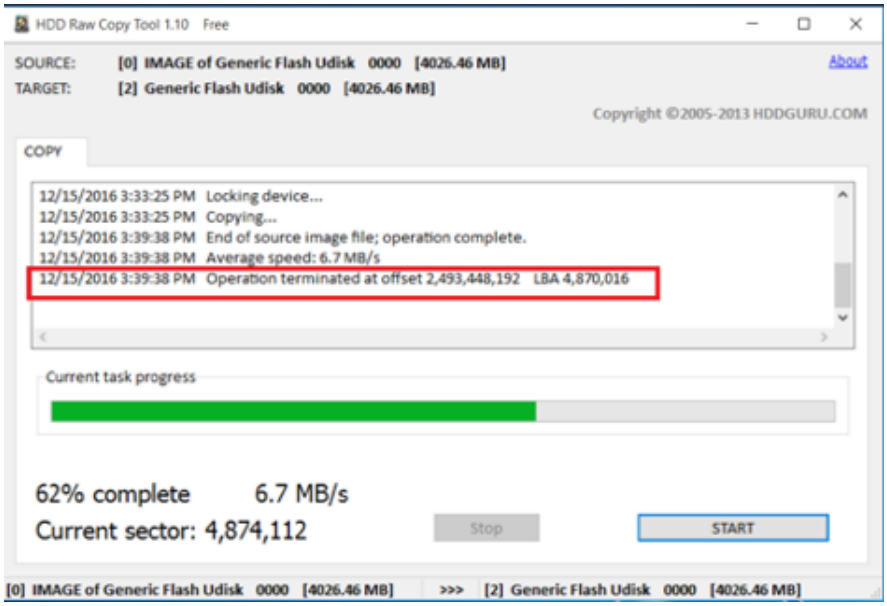


7. Podłącz nośnik pamięci flash i włącz program *HDD Raw Copy Tool*.
8. Na ekranie wyboru napędu źródłowego, zaznacz *FILE* i wskaż plik z obrazem kluczy szyfrujących.
9. Wybierz podłączony nośnik pamięci jako urządzenie docelowe i kliknij *Continue*.



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*

22.21.2 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, przejżyj i usuń sesje archiwalne, aby zwolnić miejsce.

Informacja: Więcej informacji o konfigurowaniu widgetów do wygodnego sprawdzania stanu systemu pod linkiem: *Dashboard*.

Tematy pokrewne:

- *Dziennik zdarzeń*
- *Często zadawane pytania*

22.21.3 Kontrola Stanu

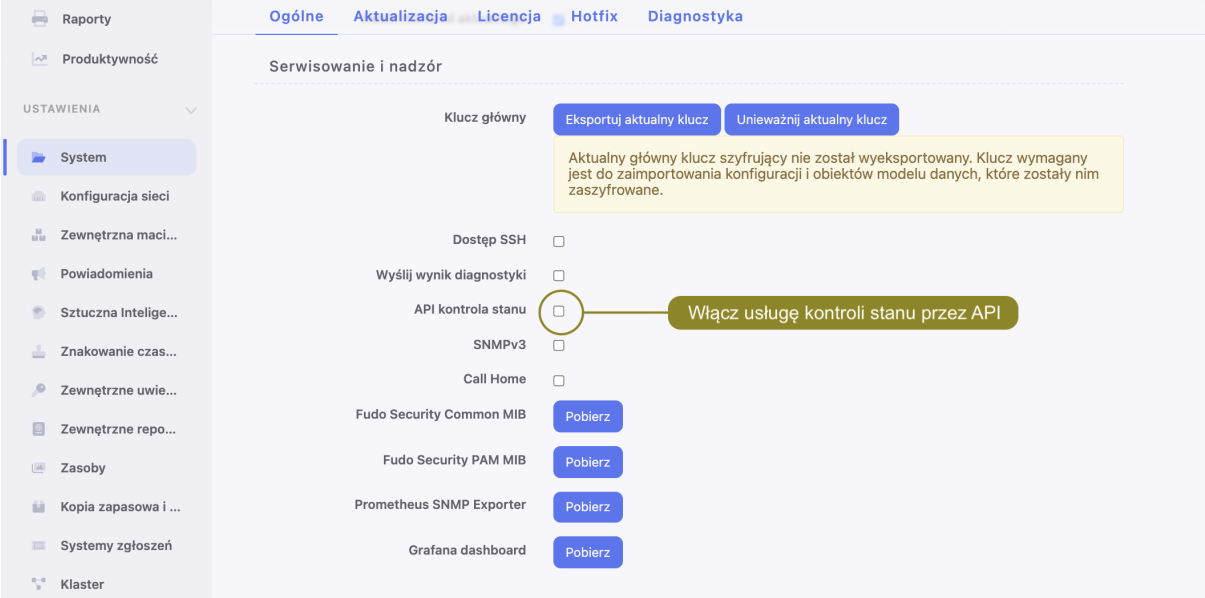
Fudo Enterprise regularnie przeprowadza kontrolę stanu najważniejszych komponentów systemu. Liczne testy systemu zapewniają stałe sprawdzenie stanu komponentu oraz wysłanie je wyników.

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.

22.21.3.1 API kontrola stanu

Funkcja API kontrola stanu jest dostępna w sekcji *Serwisowanie i nadzór* zakładki *Ustawienia* > *System*.



Dostarcza ona krótką informacje o kontroli stanu systemu Fudo 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
```

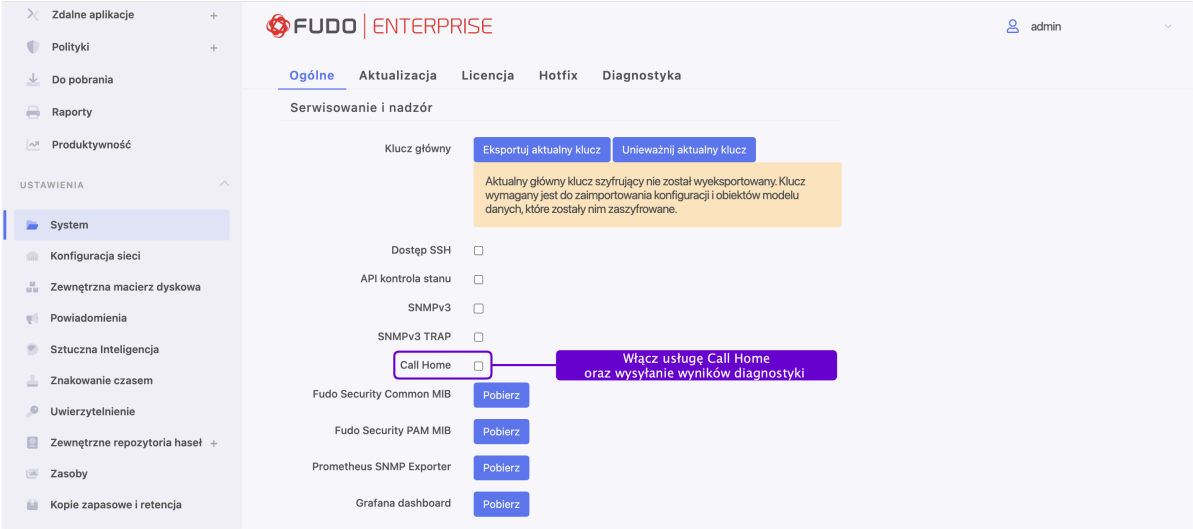
Ostrzeżenie: Opcja *API kontrola stanu* nie wymaga uwierzytelnienia. To oznacza, że każdy kto ma dostęp do TCP jest uprawniony do odczytu wyników stanu kontroli.

22.21.4 Call Home

Call Home jest usługą pozwalającą Działowi Wsparcia Technicznego Fudo na zdalne łączenie się do systemu klienta, ułatwiającą wykonywanie prac naprawczych Fudo Enterprise oraz automatyczne przesyłanie wyniki diagnostyki.

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`.



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`.

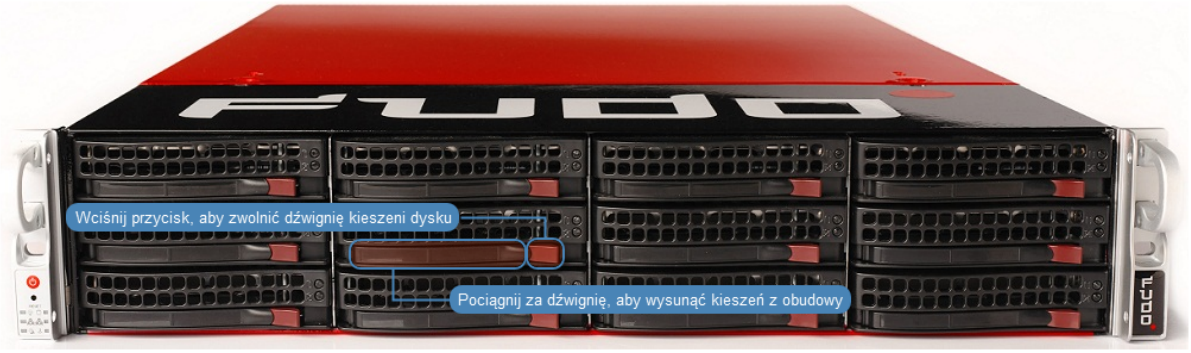
22.21.5 Wymiana dysku macierzy

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

Wymiana dysku macierzy

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

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



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

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

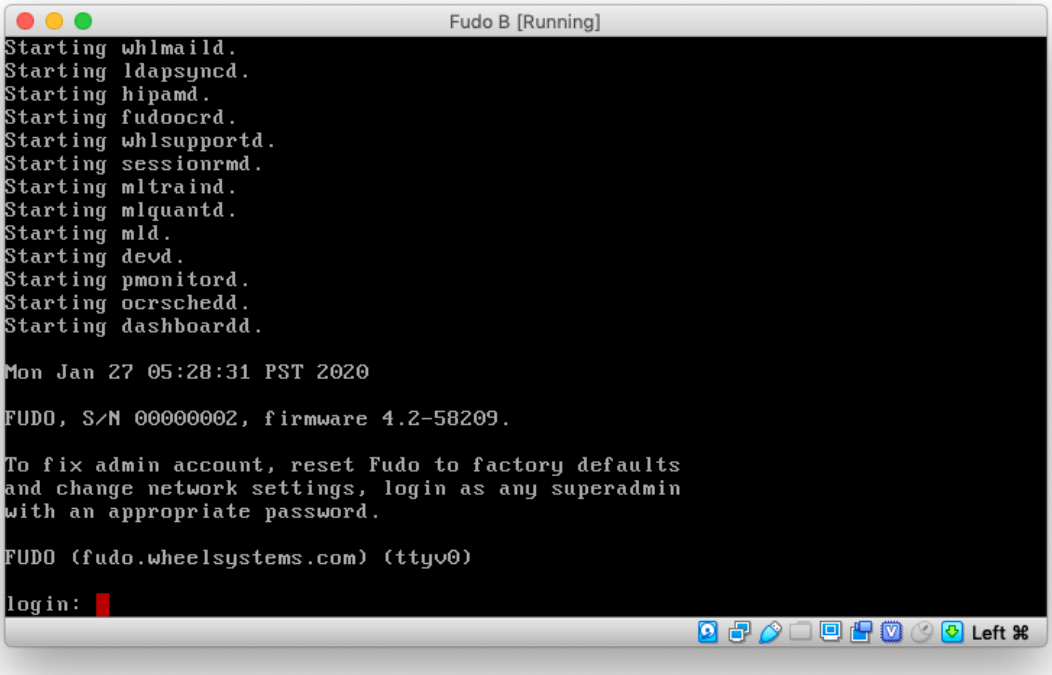
Tematy pokrewne:

- *Urządzenie*
- *Często zadawane pytania*

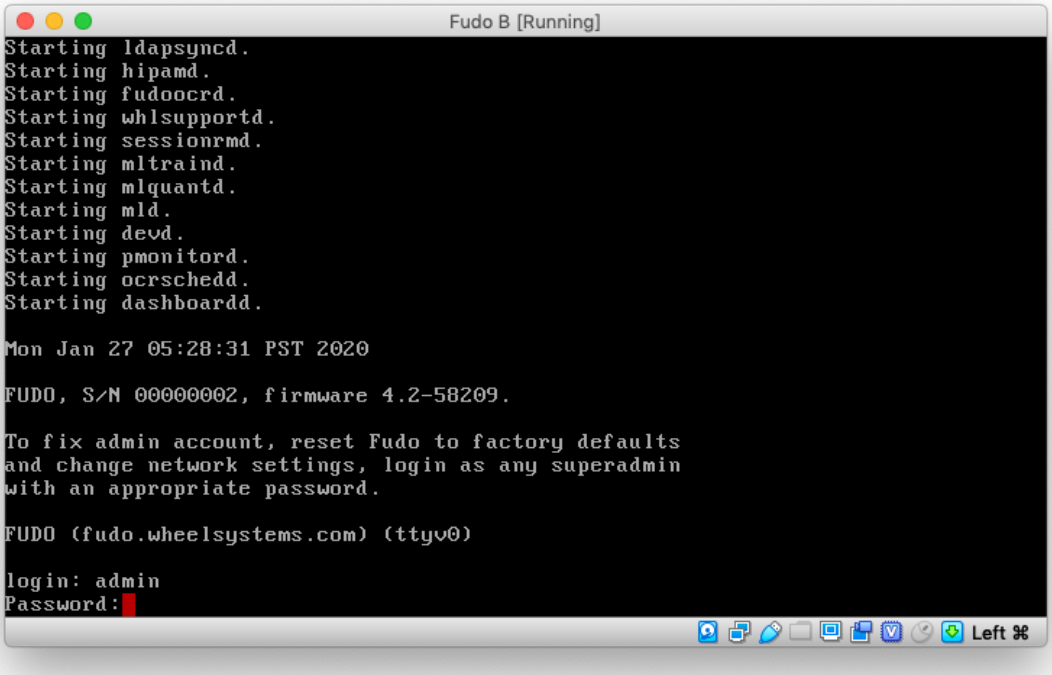
22.21.6 Przywracanie ustawień fabrycznych

Ostrzeżenie: Proces przywracania ustawień fabrycznych jest nieodwracalny i skutkuje usunięciem zarejestrowanych sesji, ustawień systemowych i zdefiniowanych obiektów. 2 pendrive'y muszą być podpięte do urządzenia, żeby proces odbył się poprawnie.

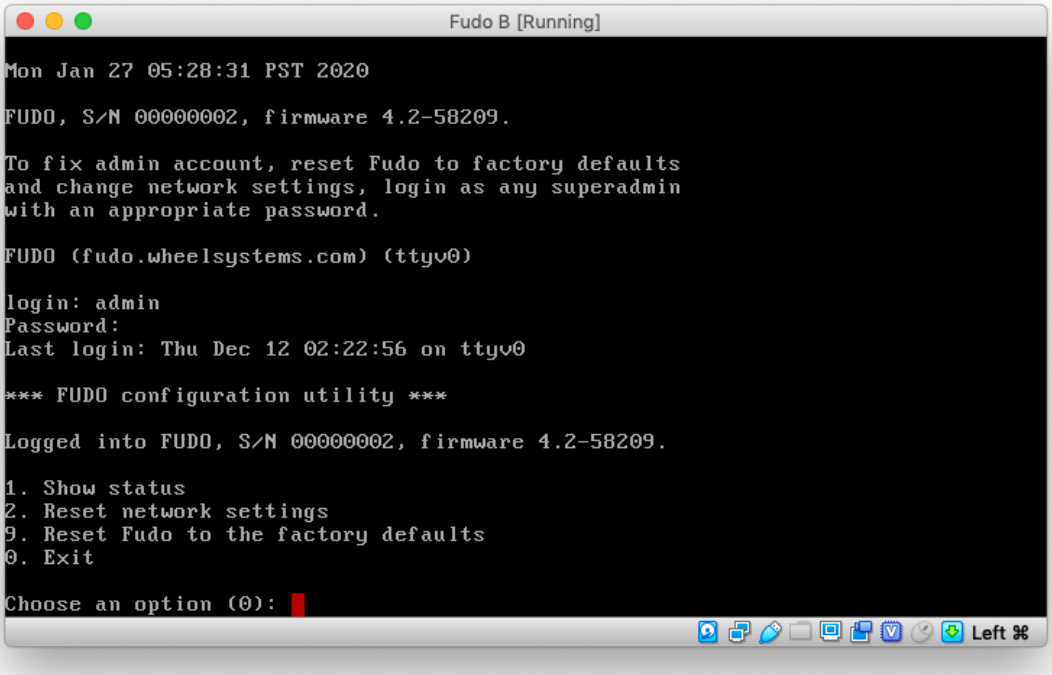
1. Uzyskaj dostęp do konsoli systemowej.
2. Wprowadź nazwę użytkownika z uprawnieniami *superadmin* i naciśnij `Enter`.



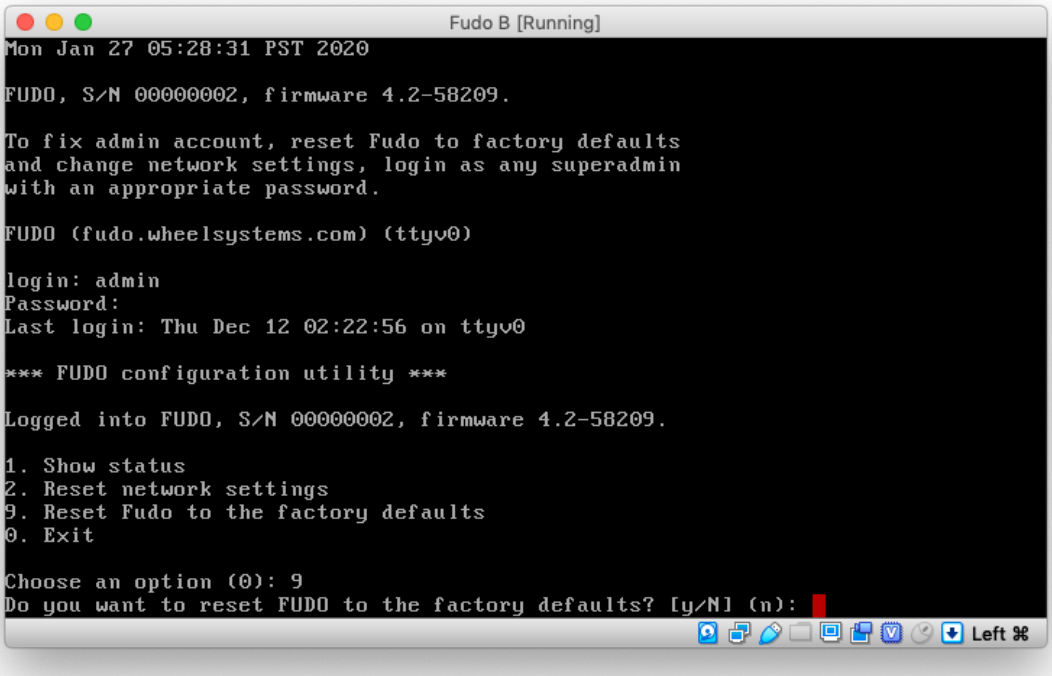
3. Wprowadź hasło i naciśnij klawisz `Enter`.



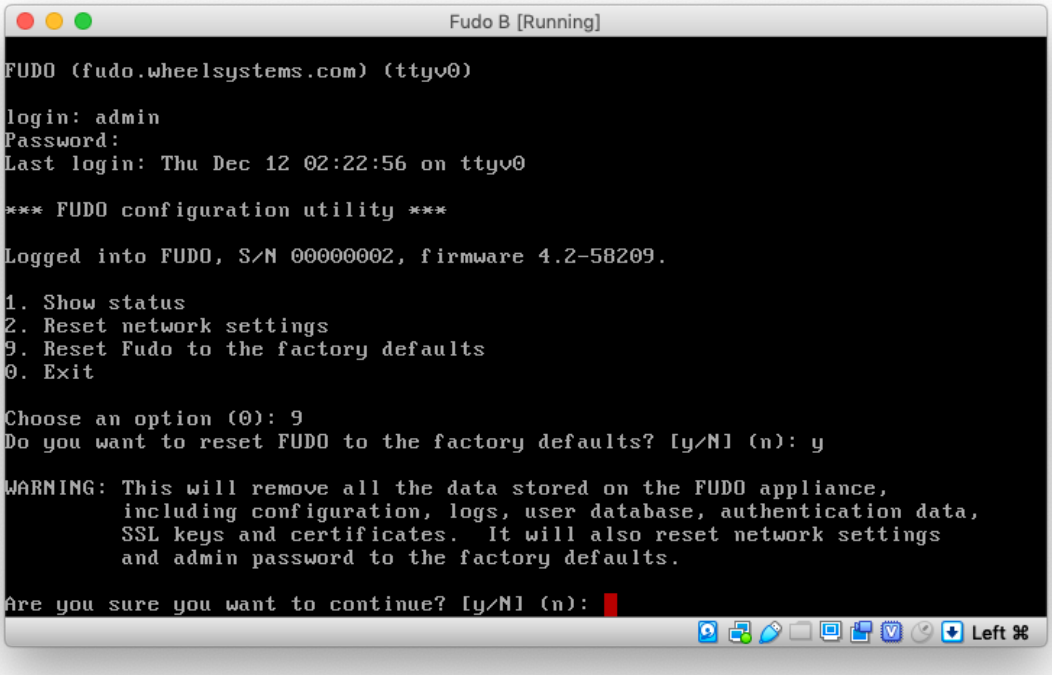
4. Wprowadź `9` i naciśnij klawisz `Enter`.



5. Wprowadź `y` i naciśnij klawisz `Enter`, aby potwierdzić wybór.



6. Wprowadź `y` i naciśnij klawisz `Enter`, aby wykonać procedurę przywrócenia ustawień fabrycznych.



Informacja: W przypadku zdawania urządzenia demonstracyjnego, należy również wyczyścić zawartość nośnika pamięci, na którym zainicjowany został klucz szyfrujący.

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*
- *Czynności serwisowe*

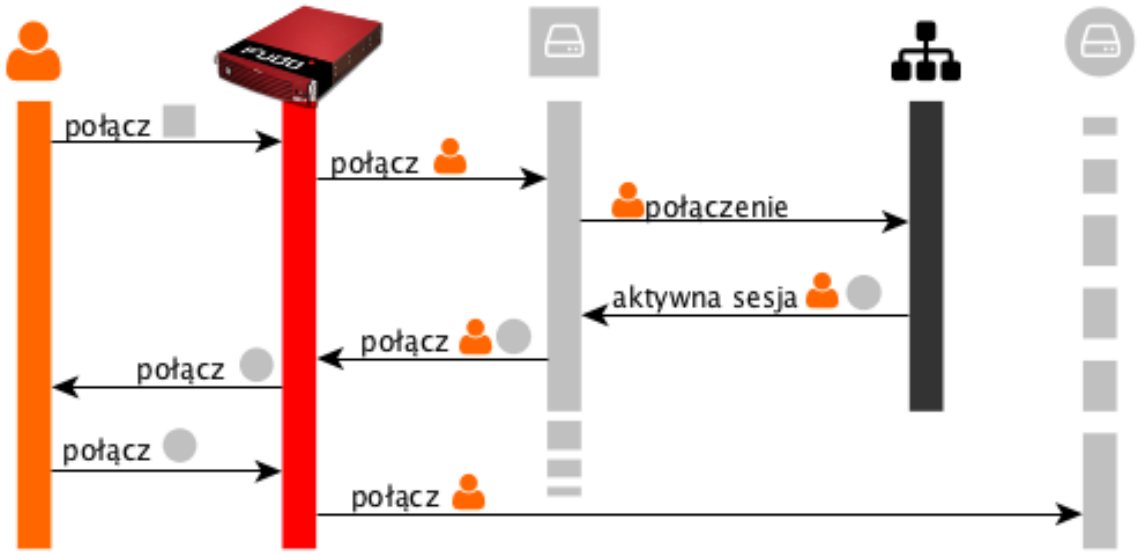
ROZDZIAŁ 23

Informacje uzupełniające

23.1 Broker połączeń RDP

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

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



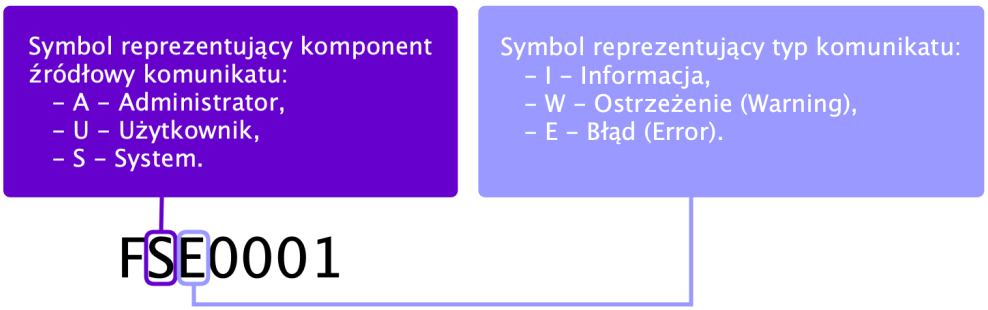
Informacja: Aby proces przekierowania użytkownika się powiódł, wskazany przez broker serwer, musi być zdefiniowany na Fudo i nasłuchiwać na domyślnym porcie RDP (3389) a użytkownik musi być uprawniony do łączenia się z tym zasobem.

Tematy pokrewne:

- *Model danych*
- *RDP*
- *Zarządzanie serwerami*
- *Konta*

23.2 Komunikaty dziennika zdarzeń

Kod komunikatu zawiera informację o typie wpisu oraz o komponencie źródłowym, którego dotyczy dana informacja.



Drugi symbol kodu wskazuje na komponent związany z logiem:

- A dla Administratora,
- U dla Użytkownika,
- S dla Systemu.

Trzeci symbol odzwierciedla typ komunikatu*:

- I dla Informacji,
- W dla Ostrzeżenia (Warning),
- E dla Błędu (Error).

Informacja: *Istnieją również typy *Critical* i *Debug*, które są przeznaczone do użytku wewnętrznego działów wsparcia oraz rozwoju. Te logi mogą zmieniać się bez ostrzeżenia i nie powinny być uznawane za wiążące przez użytkowników.

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSE0001	ERROR	SYSTEM	Internal system error.
FSE0002	ERROR	SYSTEM	Fudo certificate error.
FSE0003	ERROR	SYSTEM	Unable to change configuration settings.
FSE0004	ERROR	SYSTEM	Configuration import error.
FSE0009	ERROR	SYSTEM	Upgrade failed.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSW0011	WARNING	SYSTEM	Retention module was unable to delete session ${_sessid} from database.
FSW0012	WARNING	SYSTEM	Retention module error, session ${_sessid} skipped.
FSI0013	INFO	SYSTEM	Session ${_sessid} removed according to retention policy.
FSW0014	WARNING	SYSTEM	Retention module was unable to remove session ${_sessid}.
FSI0015	INFO	SYSTEM	Redundancy group ${_name} switched to master role.
FSW0016	WARNING	SYSTEM	Unable to send email, SMTP server not configured.
FSI0017	INFO	SYSTEM	Redundancy group ${_name} switched to slave role.
FSI0025	INFO	SYSTEM	Cluster node %s (%s) host key set to «%s».
FSI0027	INFO	SYSTEM	Cluster node %s initialized.
FSE0028	ERROR	SYSTEM	Unable to join node to cluster on %s.
FSE0031	ERROR	SYSTEM	Timestamping service communication error.
FSE0032	ERROR	SYSTEM	Unable to timestamp session.
FSE0033	ERROR	SYSTEM	Unknown timestamping service provider.
FSI0034	INFO	SYSTEM	Session ${SESSION} was timestamped.
FSI0035	INFO	SYSTEM	Email ${mailname} sent to ${admin_email}.
FSW0036	WARNING	SYSTEM	Unable to send email ${mailname} to ${admin_email} through ${account} server.
FSW0037	WARNING	SYSTEM	Output from SMTP client: ${out}.
FSI0038	INFO	SYSTEM	Saved email ${mailname} sent to ${admin_email}.
FSI0039	INFO	SYSTEM	System image version %s uploaded successfully.
FSE0040	ERROR	SYSTEM	Communication error with cluster node %s (%s): version mismatch (local: %s, remote: %s).
FSI0045	INFO	SYSTEM	Initial objects replication to cluster node %s (%s) completed.
FSE0046	ERROR	SYSTEM	There is no filter called %s.
FSW0047	WARNING	SYSTEM	Error sending notification.
FSE0048	ERROR	SYSTEM	Error authenticating user %s over RADIUS.
FUI0049	INFO	USER	User %s authenticated using password logged in from address: %s.
FUI0051	INFO	USER	User %s authenticated through %s (Host: %s, Port: %d, %s: %s) logged in from address: %s.
FUI0053	INFO	USER	User %s authenticated through LDAP (Host: %s, Port: %d) logged in from address: %s.
FUI0055	INFO	USER	User %s (domain %s) authenticated through Active Directory (Host: %s, Port: %d) logged in from address: %s.
FUE0057	ERROR	USER	Authentication method «password», required by MySQL, requested by the user %s, logging in from address %s, was not found.
FSE0061	ERROR	SYSTEM	Incorrect password repository configuration: login is empty.
FSE0062	ERROR	SYSTEM	Incorrect password repository configuration: password is empty.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSE0065	ERROR	SYSTEM	License configuration error.
FSE0066	ERROR	SYSTEM	Unable to block user %jd.
FSW0074	WARNING	SYSTEM	Connection terminated because license has expired or was not set.
FSW0075	WARNING	SYSTEM	Connection terminated because number of nodes in cluster exceeded license limit.
FSE0077	ERROR	SYSTEM	LDAP authentication error.
FSE0078	ERROR	SYSTEM	LDAP authentication error: unable to connect from %s to %s.
FUE0079	ERROR	USER	Authentication timeout after %ju key attempt%s and %ju password attempt%s.
FUE0080	ERROR	USER	Authentication timeout after %lu key attempt%s.
FUE0081	ERROR	USER	Authentication timeout after %lu password attempt%s.
FSE0082	ERROR	SYSTEM	Unable to establish connection to server %s (%s).
FSE0083	ERROR	SYSTEM	Unable to establish connection from %s to server %s (%s).
FSI0084	INFO	SYSTEM	Terminating session: %s.
FSI0085	INFO	SYSTEM	Session finished.
FUI0086	INFO	USER	User %s blocked due to connection policy violation.
FUW0087	WARNING	USER	Session has been terminated due to user %s account expiration.
FUE0089	ERROR	USER	Authentication timeout.
FSE0090	ERROR	SYSTEM	Unable to connect to the passwords repository server %s.
FSE0092	ERROR	SYSTEM	Passwords repository server %s communication error.
FSE0093	ERROR	SYSTEM	Error connecting to Thycotic server %s: incorrect URL in configuration.
FSE0094	ERROR	SYSTEM	Error connecting to Thycotic server %s: incorrect protocol specified.
FSE0095	ERROR	SYSTEM	Error fetching password from Thycotic server %s: unable to get sessid for user %s.
FSE0096	ERROR	SYSTEM	Error fetching password from Thycotic server %s.
FSE0097	ERROR	SYSTEM	Error fetching password for %s from Thycotic server %s: unable to get secretid for server %s.
FSE0098	ERROR	SYSTEM	Error fetching password for %s from Thycotic server %s: unable to get password for user %s for the %s server.
FUE0099	ERROR	USER	Connection terminated.
FUE0101	ERROR	USER	Unable to find matching HTTP connection.
FUI0102	INFO	USER	Session terminated by system administrator.
FUE0103	ERROR	USER	HTTP connection error.
FUI0104	INFO	USER	%s connection terminated.
FUI0105	INFO	USER	HTTP session inactive, terminating.
FUE0106	ERROR	USER	Authentication failed: %s.
FUW0107	WARNING	USER	Invalid inactivity timeout, falling back to %d seconds.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FUE0108	ERROR	USER	MySQL connection error.
FUI0109	INFO	USER	MySQL connection terminated.
FUE0112	ERROR	USER	RDP connection error.
FUE0113	ERROR	USER	TLS Security configured, but missing TLS private key.
FUE0115	ERROR	USER	Standard RDP Security configured, but missing private key.
FUE0116	ERROR	USER	TLS certificate verification failed.
FUE0117	ERROR	USER	RSA key verification failed.
FUI0118	INFO	USER	Successfully authenticated against server %s.
FUI0119	INFO	USER	Successfully authenticated against server %s as user %s using %s.
FUI0120	INFO	USER	Successfully authenticated against server %s as user %s within domain %s using %s.
FUI0121	INFO	USER	An anonymous user successfully authenticated against server %s.
FUI0122	INFO	USER	An anonymous user successfully authenticated against server %s as user %s.
FUI0123	INFO	USER	An anonymous user successfully authenticated against server %s as user %s within domain %s.
FUE0124	ERROR	USER	SSH connection error.
FUE0129	ERROR	USER	Failed to authenticate against server %s as user %s using %s.
FUE0130	ERROR	USER	Failed to authenticate against server %s as user %s using %s (received %s).
FUW0131	WARNING	USER	Functionality %s is not allowed.
FUE0133	ERROR	USER	MSSQL connection error.
FUE0134	ERROR	USER	TN3270 connection error.
FUE0135	ERROR	USER	Unknown TN3270 command: %02x.
FUE0136	ERROR	USER	Telnet connection error.
FSE0137	ERROR	SYSTEM	Unable to read private key.
FSE0138	ERROR	SYSTEM	Server's certificate does not match configured certificate.
FUE0139	ERROR	USER	VNC connection error.
FUE0140	ERROR	USER	Client version: %s is higher than the client integrated in Fudo: %s.
FUE0141	ERROR	USER	VNC connection error. Client answered with unsupported security type: %hhu.
FUE0142	ERROR	USER	VNC connection error. Server version: %s is lower than client version: %s.
FUI0143	INFO	USER	VNC connection closed: %s.
FUE0144	ERROR	USER	User %s failed to authorize logging in from address: %s.
FUE0146	ERROR	USER	User %s failed to authenticate logging in from address: %s.
FSE0153	ERROR	SYSTEM	Session indexing failure.
FSE0154	ERROR	SYSTEM	Session conversion failure for session %s.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0157	INFO	ADMIN	User %s %s failover configuration.
FAI0158	INFO	ADMIN	User %s added node %s.
FAI0159	INFO	ADMIN	User %s changed %s in node %s.
FAI0160	INFO	ADMIN	User %s deleted node %s.
FAI0161	INFO	ADMIN	User %s disconnected node from the cluster.
FAI0162	INFO	ADMIN	Cluster has no active nodes. Cluster will be disabled.
FAI0163	INFO	ADMIN	User %s created new cluster - %s.
FAI0164	INFO	ADMIN	User %s attached current node to cluster.
FAI0166	INFO	ADMIN	User %s restored original logo for protocol %s.
FAI0167	INFO	ADMIN	User %s changed logo for protocol %s.
FAI0168	INFO	ADMIN	User %s confirmed sensitive feature %s.
FAI0169	INFO	ADMIN	User %s removed confirmation for sensitive feature %s.
FAI0170	INFO	ADMIN	User %s changed following notifications settings: %s.
FAI0171	INFO	ADMIN	User %s enabled email notifications.
FAI0172	INFO	ADMIN	User %s disabled email notifications.
FAI0173	INFO	ADMIN	User %(username)s is upgrading Fudo.
FAI0174	INFO	ADMIN	User %(username)s upgraded Fudo.
FAI0175	INFO	ADMIN	User %(username)s uploaded new upgrade image (version: %(version)s, size: %(size)d).
FAI0176	INFO	ADMIN	User %(username)s deleted upgrade files.
FAI0177	INFO	ADMIN	User %s uploaded license file.
FAW0178	WARNING	ADMIN	User %(username)s triggered system restart.
FAW0179	WARNING	ADMIN	User %(username)s triggered system shutdown.
FAW0180	WARNING	ADMIN	User %s %s remote SSH access.
FAW0181	WARNING	ADMIN	User %(username)s changed timestamping settings.
FAW0182	WARNING	ADMIN	User %(username)s uploaded new PKCS12 file.
FAW0183	WARNING	ADMIN	User %(username)s changed timestamping provider to %(provider)s.
FAW0184	WARNING	ADMIN	User %(username)s %(action)s timestamping.
FAI0185	INFO	ADMIN	User %s imported system configuration.
FAI0186	INFO	ADMIN	User %s requested system configuration export.
FAI0187	INFO	ADMIN	User %s added NTP server %s.
FAI0188	INFO	ADMIN	User %s removed NTP server %s.
FAE0189	ERROR	ADMIN	Error saving NTP servers: „%s”.
FAI0190	INFO	ADMIN	User %(username)s changed date & time from %(old_date)s to %(new_date)s.
FAI0191	INFO	ADMIN	User %s changed timezone to %s.
FAI0192	INFO	ADMIN	User %s changed Fudo HTTPS private key and certificate.
FAI0193	INFO	ADMIN	User %s %s SSH access.
FAI0194	INFO	ADMIN	User %s requested service data.
FAI0195	INFO	ADMIN	User %s added %s to %s for %s %s.
FAI0196	INFO	ADMIN	User %s removed %s from %s for %s %s.
FAI0197	INFO	ADMIN	User %s changed %s from %s to %s for %s %s.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0198	INFO	ADMIN	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	INFO	ADMIN	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	INFO	ADMIN	User %(username)s %(new_cluster)s cluster address on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0201	INFO	ADMIN	User %(username)s %(new_management)s management on %(new_inet)s/%(new_netmask)s address on interface %(interface)s.
FAI0202	INFO	ADMIN	User %(username)s deleted IP address %(old_ip)s from interface %(interface)s.
FAI0203	INFO	ADMIN	User %(username)s %(action)s interface %(interface)s.
FAI0204	INFO	ADMIN	User %(username)s added member %(member)s to bridge %(interface)s.
FAI0205	INFO	ADMIN	User %(username)s removed member %(member)s from bridge %(interface)s.
FAI0206	INFO	ADMIN	User %(username)s enabled spanning tree propagation on bridge %(interface)s.
FAI0207	INFO	ADMIN	User %(username)s disabled spanning tree propagation on bridge %(interface)s.
FAI0208	INFO	ADMIN	User %(username)s changed VLAN %(interface)s parent interface from %(old_parent_interface)s to %(new_parent_interface)s.
FAI0209	INFO	ADMIN	User %(username)s changed VLAN %(interface)s ID from %(old_vlan)s to %(new_vlan)s.
FAI0210	INFO	ADMIN	User %s deleted interface %s.
FAI0211	INFO	ADMIN	User %s changed LDAP synchronization settings.
FAW0213	WARNING	ADMIN	LDAP error during fetching groups: %s.
FAI0214	INFO	ADMIN	User %s enforced full LDAP synchronization.
FAI0215	INFO	ADMIN	User %s disabled events logging on syslog servers.
FAI0216	INFO	ADMIN	User %s removed syslog server: %s:%s.
FAI0217	INFO	ADMIN	User %s added syslog server: %s:%s.
FAI0218	INFO	ADMIN	User %s removed syslog server %s.
FAI0219	INFO	ADMIN	User %s changed remote log dispatch settings.
FAI0220	INFO	ADMIN	User %s changed network interfaces settings.
FAI0221	INFO	ADMIN	User %s changed hostname from %s to %s.
FAI0222	INFO	ADMIN	User %s added DNS server IP address %s.
FAI0223	INFO	ADMIN	User %s removed DNS server IP address %s.
FAI0224	INFO	ADMIN	User %s added new route for network %s with gateway %s.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0225	INFO	ADMIN	User %s changed gateway for network %s from %s to %s.
FAI0226	INFO	ADMIN	User %s deleted network %s with gateway %s.
FAI0227	INFO	ADMIN	User %s (%s) terminated session.
FAI0228	INFO	ADMIN	Anonymous user from IP address %s with access rights granted by user %s joined session.
FAI0229	INFO	ADMIN	User %s from IP address %s joined session.
FAI0230	INFO	ADMIN	User %s (%s) suspended session.
FAI0231	INFO	ADMIN	User %s (%s) resumed session.
FAE0232	ERROR	ADMIN	MySQL session playback error.
FAI0233	INFO	ADMIN	Anonymous user from IP address %s accessed shared session %s with key %s.
FAI0234	INFO	ADMIN	User %s from IP address %s accessed session %s.
FAI0235	INFO	ADMIN	User %s %s comment %d for session.
FAI0236	INFO	ADMIN	User %s generated key %s with %s access.
FAI0237	INFO	ADMIN	User %s is viewing user input for session.
FAI0238	INFO	ADMIN	User %s blocked server %s.
FAI0239	INFO	ADMIN	User %s unblocked server %s.
FAI0247	INFO	ADMIN	User %s deleted server %s.
FAI0253	INFO	ADMIN	User %s deleted session.
FAI0254	INFO	ADMIN	User %s requested OCR processing for session.
FAW0255	WARNING	ADMIN	User %s tried to disable a non-exisitent sharing key for session.
FAI0256	INFO	ADMIN	User %s disabled anonymous access key %s for session.
FAI0259	INFO	ADMIN	User %s deleted download %s.
FAI0260	INFO	ADMIN	User %s downloaded file %s for session %s.
FAI0261	INFO	ADMIN	Anonymous user from IP address %s terminated shared session with key %s.
FAI0262	INFO	ADMIN	User %s terminated session.
FAI0263	INFO	ADMIN	User %s blocked user %s.
FSW0266	WARNING	SYSTEM	Failed to send email.
FSE0267	ERROR	SYSTEM	Error generating report %d: %s.
FAI0268	INFO	ADMIN	User %s deleted report „%s”.
FAI0270	INFO	ADMIN	Report {} created by user {}.
FAI0276	INFO	ADMIN	User %s unblocked user %s.
FAI0277	INFO	ADMIN	User %s deleted user %s.
FAI0279	INFO	ADMIN	User %s changed user %s.
FAI0281	INFO	ADMIN	User %s logged out from Fudo administration panel.
FUI0282	INFO	USER	User %s successfully changed his password.
FSE0283	ERROR	SYSTEM	Unable to process pattern: %s
FSW0284	WARNING	SYSTEM	Pattern %s matched on %s with priority %s in session.
FSE0285	ERROR	SYSTEM	Unable to read certificate.
FSE0286	ERROR	SYSTEM	No peer certificate received.
FUI0289	INFO	USER	MSSQL connection terminated.
FAI0299	INFO	ADMIN	User %s created server %s.
FAI0300	INFO	ADMIN	User %s changed server %s.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0303	INFO	ADMIN	User %s created user %s with role %s.
FAI0304	INFO	ADMIN	User %s modified %s for %s %s.
FUE0305	ERROR	USER	Client connection closed: encryption is not available.
FUE0306	ERROR	USER	Client connection closed.
FUE0314	ERROR	USER	Invalid pixel format.
FSE0330	ERROR	SYSTEM	Bad login field configured on LDAP server %s. Error while processing user %s.
FSI0332	INFO	SYSTEM	User %s will be blocked.
FSI0333	INFO	SYSTEM	User %s will be unblocked.
FSI0335	INFO	SYSTEM	User %s synchronized from LDAP server %s.
FSI0339	INFO	SYSTEM	User %s (%s) was removed. Reason: user was not in any of synchronized groups.
FSI0340	INFO	SYSTEM	Full synchronization from LDAP server %s started.
FSI0342	INFO	SYSTEM	User %s will be resynchronized from server %s.
FSW0344	WARNING	SYSTEM	Connecting to LDAP server error: %s.
FSI0345	INFO	SYSTEM	Successfully fetched password from %s.
FUE0346	ERROR	USER	Client sent a packet bigger than %d bytes.
FSE0348	ERROR	SYSTEM	Unable to get configuration settings.
FAI0349	INFO	ADMIN	Anonymous user from IP address %s with access rights granted by user %s left session.
FAI0350	INFO	ADMIN	User %s from IP address %s left session.
FAI0354	INFO	ADMIN	User %(username)s deleted upgrade snapshot.
FUW0356	WARNING	USER	Unsupported X11 extension: %s.
FUW0357	WARNING	USER	Server uses higher resolution than the current limit: %dx%d.
FUW0358	WARNING	USER	Server uses higher color depth than the current limit: %d bpp.
FUE0359	ERROR	USER	Server rejected X11 connection: %.*s.
FUE0360	ERROR	USER	Server requires unsupported X11 authentication: %.*s.
FSW0361	WARNING	SYSTEM	Fudo started.
FSE0362	ERROR	SYSTEM	Unable to propagate ARP.
FUE0363	ERROR	USER	User %s has no access to host %s.
FUI0364	INFO	USER	RDP server sent a redirection packet.
FUI0370	INFO	USER	User %s authenticated using OTP logged in from IP address: %s.
FUW0373	WARNING	USER	Session has been terminated due to exceeding the time window defined in a time policy for the user %s and the safe %s.
FSI0374	INFO	SYSTEM	Established %s connection from %s to %s.
FSE0376	ERROR	SYSTEM	Unable to add listener %s because %s is listening on the same IP address and port.
FSE0378	ERROR	SYSTEM	Unable to establish connection: server not found, user not found or user has no access to the server (listener: %s, user: %s).

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSE0379	ERROR	SYSTEM	Unable to establish connection: transparent server (tcp://%s) not found or cannot be reached through listener (listener: %s, user: %s).
FSE0380	ERROR	SYSTEM	Unable to authenticate user %s: server %s is blocked.
FSE0381	ERROR	SYSTEM	Unable to authenticate user %s: account not found.
FSE0382	ERROR	SYSTEM	Unable to authenticate user %s: account %s is blocked.
FSE0383	ERROR	SYSTEM	Unable to authenticate user %s%s%s: user not found.
FSE0384	ERROR	SYSTEM	Unable to authenticate user %s: user is blocked.
FSE0385	ERROR	SYSTEM	Unable to authenticate user %s: safe not found.
FSE0386	ERROR	SYSTEM	Unable to authenticate user %s: safe %s is blocked.
FSI0387	INFO	SYSTEM	Password for account %s verified successfully.
FSI0389	INFO	SYSTEM	Password for account %s changed successfully.
FAI0393	INFO	ADMIN	User %s displayed password history for account %s.
FAI0394	INFO	ADMIN	User %s displayed historical password for account %s changed at %s.
FAI0395	INFO	ADMIN	User %s displayed current password for account %s.
FAI0396	INFO	ADMIN	User %s blocked safe %s.
FAI0397	INFO	ADMIN	User %s unblocked safe %s.
FAI0398	INFO	ADMIN	User %s deleted safe %s.
FAI0399	INFO	ADMIN	User %s changed safe %s.
FAI0400	INFO	ADMIN	User %s created safe %s.
FAI0401	INFO	ADMIN	User %s blocked account %s.
FAI0402	INFO	ADMIN	User %s unblocked account %s.
FAI0403	INFO	ADMIN	User %s deleted account %s.
FAI0406	INFO	ADMIN	User %s blocked listener %s.
FAI0407	INFO	ADMIN	User %s unblocked listener %s.
FAI0408	INFO	ADMIN	User %s deleted listener %s.
FAI0411	INFO	ADMIN	User %s blocked password change policy %s.
FAI0412	INFO	ADMIN	User %s unblocked password change policy %s.
FAI0413	INFO	ADMIN	User %s deleted password change policy %s.
FAI0414	INFO	ADMIN	User %s changed password change policy %s.
FAI0415	INFO	ADMIN	User %s created password change policy %s.
FSI0416	INFO	SYSTEM	Connection between safe %s and user %s has been removed.
FSI0417	INFO	SYSTEM	Connection between safe %s and user %s has been added.
FSI0418	INFO	SYSTEM	User %s was removed from safes %s.
FSE0420	ERROR	SYSTEM	Unable to authenticate user %s against server %s.
FAI0423	INFO	ADMIN	User %s assigned account %s to safe %s.
FAI0424	INFO	ADMIN	User %s unassigned account %s from safe %s.
FAI0425	INFO	ADMIN	User %s assigned authentication method %s to user %s.
FAI0426	INFO	ADMIN	User %s unassigned authentication mathod %s from user %s.
FAI0427	INFO	ADMIN	User %s changed authentication mathod %s assigned to user %s.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0428	INFO	ADMIN	User %s assigned user %s to safe %s.
FAI0429	INFO	ADMIN	User %s unassigned user %s from safe %s.
FAI0430	INFO	ADMIN	User %s blocked password changer %s.
FAI0431	INFO	ADMIN	User %s unblocked password changer %s.
FAI0432	INFO	ADMIN	User %s deleted password changer %s.
FAI0433	INFO	ADMIN	User %s changed password changer %s.
FAI0434	INFO	ADMIN	User %s created password changer %s.
FSW0435	WARNING	SYSTEM	Password changer timed out for account %s.
FAW0438	WARNING	ADMIN	User %s authenticated using new token while the old one still exists.
FAW0439	WARNING	ADMIN	User %s authenticated using old token.
FAI0444	INFO	ADMIN	User %s created policy %s.
FAI0445	INFO	ADMIN	User %s deleted policy %s.
FAI0446	INFO	ADMIN	User %s changed policy %s.
FAI0449	INFO	ADMIN	User %s created regexp %s.
FAI0450	INFO	ADMIN	User %s deleted regexp %s.
FAI0451	INFO	ADMIN	User %s changed regexp %s.
FAI0460	INFO	ADMIN	User %s displayed current password for account %s. Reason: %s
FSE0461	ERROR	SYSTEM	Invalid data from %s LDAP server.
FAI0462	INFO	ADMIN	User {} created redundancy group {}.
FAI0463	INFO	ADMIN	User {} deleted redundancy group {}.
FUW0465	WARNING	USER	Establishing new connections has been disabled.
FSE0466	ERROR	SYSTEM	Fudo versions do not conform.
FUE0467	ERROR	USER	Client tried to authenticate using an invalid UTF-8 login.
FSI0468	INFO	SYSTEM	A passphrase used to decrypt disks was changed.
FSE0476	ERROR	SYSTEM	ZVOL with encryption key does not exist.
FAI0481	INFO	ADMIN	New OTP for user %s has been generated.
FSW0482	WARNING	SYSTEM	Unable to verify password for account %s.
FAI0487	INFO	ADMIN	User %s requested timestamping for session.
FAI0488	INFO	ADMIN	User %s requested timestamping for account.
FSI0489	INFO	SYSTEM	Label %s is not defined on this node, skipping listener %s.
FAI0490	INFO	ADMIN	User %s created external authentication %s.
FAI0491	INFO	ADMIN	User %s changed external authentication %s: %s.
FAI0492	INFO	ADMIN	User %s deleted external authentication %s.
FSE0493	ERROR	SYSTEM	Unable to establish connection to server %s (%s): label %s not defined on this node.
FSI0494	INFO	SYSTEM	Label %s not defined on this node, skipping external authentication %s.
FSE0500	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to connect to database.
FSE0502	ERROR	SYSTEM	Database error.
FSE0510	ERROR	SYSTEM	Communication error with cluster node %s (%s): initial replication failed.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAW0514	WARNING	ADMIN	User %s of role %s tried to view %s, but has insufficient privileges for this action.
FSW0522	WARNING	SYSTEM	Rollback to ${_version} failed.
FSW0523	WARNING	SYSTEM	Upgrade to ${_version} failed.
FSW0524	WARNING	SYSTEM	Rollback to ${_version} succeeded.
FSW0525	WARNING	SYSTEM	Upgrade to ${_version} succeeded.
FSE0526	ERROR	SYSTEM	Error communicating with bypass card. Error setting nextboot mode.
FSE0527	ERROR	SYSTEM	Error communicating with bypass card. Error setting bpe mode.
FSE0528	ERROR	SYSTEM	Error communicating with bypass card. Error switching card mode.
FSE0529	ERROR	SYSTEM	Error communicating with bypass card.
FAI0530	INFO	ADMIN	User %s enabled snmp.
FAI0531	INFO	ADMIN	User %s disabled snmp.
FSW0532	WARNING	SYSTEM	External storage is unavailable.
FSI0534	INFO	SYSTEM	External storage attached.
FSE0535	ERROR	SYSTEM	External storage is unavailable in this configuration.
FSW0536	WARNING	SYSTEM	External storage detached.
FAI0538	INFO	ADMIN	Set external storage connection mode to %s
FAI0539	INFO	ADMIN	Set configured WWN to %s, external storage connection mode to %s
FSW0540	WARNING	SYSTEM	Found ${cdisk} paths to fiber channel ${wwn} from ${cscbus} devices.
FSW0541	WARNING	SYSTEM	Retention module was unable to move session ${_sessid}.
FAI0542	INFO	ADMIN	User %s assigned account %s, listener %s to safe %s.
FAI0543	INFO	ADMIN	User %s unassigned account %s, listener %s from safe %s.
FSW0545	WARNING	SYSTEM	Unable to change password for account %s.
FAI0549	INFO	ADMIN	User %s approved ticket %s requesting an access for user %s to safe %s.
FAI0550	INFO	ADMIN	User %s rejected ticket %s requesting an access for user %s to safe %s.
FAI0551	INFO	ADMIN	User %(username)s added member %(member)s to lagg %(interface)s.
FAI0552	INFO	ADMIN	User %(username)s removed member %(member)s from lagg %(interface)s.
FSE0553	ERROR	SYSTEM	Unable to extract public key from CA.
FUE0554	ERROR	USER	SFTP server uses an unsupported version %u.
FSE0560	ERROR	SYSTEM	Session has not been approved nor rejected.
FAI0562	INFO	ADMIN	User %s rejected session %s. Reason: %s.
FAI0563	INFO	ADMIN	User %s rejected session %s.
FAI0564	INFO	ADMIN	User: {} tried to accept session: {} but it was accepted by:
FAI0565	INFO	ADMIN	User: {} rejected session: {}

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0566	INFO	ADMIN	User: {} tried to reject session: {} but it was accepted by:
FAI0567	INFO	ADMIN	User: {} tried to reject session: {} but it was rejected by:
FAI0568	INFO	ADMIN	User: {} accepted session: {}
FAI0569	INFO	ADMIN	User: {} tried to accept session: {} but it was rejected by:
FAI0570	INFO	ADMIN	User %s approved session %s.
FSI0571	INFO	SYSTEM	Proxy connection closed.
FSE0572	ERROR	SYSTEM	Proxy connection error.
FSE0573	ERROR	SYSTEM	Client sent an invalid token.
FSE0574	ERROR	SYSTEM	Unable to resolve hostname ${ip} to address.
FSE0575	ERROR	SYSTEM	Unable to convert raw file to pcap.
FAI0581	INFO	ADMIN	User %s changed domain search path from %s to %s.
FSE0583	ERROR	SYSTEM	LDAP authentication error: unable to connect to %s.
FAI0584	INFO	ADMIN	User %s changed data on user portal.
FAI0585	INFO	ADMIN	User %s changed User portal HTTPS private key and certificate.
FAW0586	WARNING	ADMIN	Missing safe attributes: %s
FSE0588	ERROR	SYSTEM	Failed to replicate an object to node %s (%s): %s.
FSE0589	ERROR	SYSTEM	Communication error with cluster node %s (%s): database %s transaction failure.
FSE0590	ERROR	SYSTEM	Communication error with cluster node %s: unable to establish connection.
FSE0591	ERROR	SYSTEM	Communication error with cluster node %s: unable to obtain serial number.
FSE0592	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to obtain public key.
FAI0594	INFO	ADMIN	User %s exported master key.
FUE0595	ERROR	USER	User %s authorization failed: %s.
FAI0597	INFO	ADMIN	User %s enabled failure login attempts limit.
FAI0598	INFO	ADMIN	User %s disabled failure login attempts limit.
FSI0599	INFO	SYSTEM	Fudo is successfully re-encrypted using key %s.
FUI0601	INFO	USER	VNC connection terminated.
FSW0602	WARNING	SYSTEM	Retention module was unable to fetch the current time.
FSI0603	INFO	SYSTEM	Finished full synchronization from LDAP server %s.
FAI0604	INFO	ADMIN	User %s created IP label %s.
FAI0605	INFO	ADMIN	User %s changed IP label %s.
FAI0606	INFO	ADMIN	User %s deleted IP label %s.
FAI0607	INFO	ADMIN	User %s restored original logo for portal.
FAI0608	INFO	ADMIN	User %s changed logo for portal.
FSI0609	INFO	SYSTEM	Successfully generated new master key: %s.
FAI0610	INFO	ADMIN	User %s invalidated master key.
FAI0613	INFO	ADMIN	User %s canceled timestamping for session.
FSI0614	INFO	SYSTEM	System image version %s is being processed.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSI0615	INFO	SYSTEM	System image version %s does not have preparation scripts.
FSW0616	WARNING	SYSTEM	Quantitive indicator: %s %s established %d %s sessions in past 60 minutes! It's %d more than typical at this time.
FSW0617	WARNING	SYSTEM	Anomalous session length for %s %s lasted %d seconds which is longer than %d%% of sessions for this %s.
FSE0620	ERROR	SYSTEM	Failed to expand disk ${_disk} (${_ident}).
FSI0621	INFO	SYSTEM	Disk ${_disk} (${_ident}) expanded to ${_newsize}.
FSI0622	INFO	SYSTEM	External storage expanded to ${_newsize}.
FAI0623	INFO	ADMIN	User %s enabled different password than current setting.
FAI0624	INFO	ADMIN	User %s disabled different password than current setting.
FSI0626	INFO	SYSTEM	Initial logs replication to cluster node %s (%s) completed.
FSE0633	ERROR	SYSTEM	Protocol %s doesn't support multistep authentication.
FSE0634	ERROR	SYSTEM	Authentication failed: User %s failed to authenticate using %s.
FSW0639	WARNING	SYSTEM	Data storage full, establishing connections has been disabled. Free up some storage space to re-enable the session monitoring functionality.
FUE0640	ERROR	USER	Failed to authenticate against the server as user %s using %s: %s
FSW0641	WARNING	SYSTEM	Establishing connections has been re-enabled.
FSW0642	WARNING	SYSTEM	Trying to finish all active sessions because of full filesystem.
FAI0644	INFO	ADMIN	User %s changed user portal SSO settings.
FSE0645	ERROR	SYSTEM	Communication error with cluster node %s (%s): unable to obtain time.
FSE0646	ERROR	SYSTEM	Communication error with cluster node %s (%s): time difference too large (%ds).
FUW0647	WARNING	USER	Cannot establish new connections because the capacity of the filesystem has been reached.
FSW0649	WARNING	SYSTEM	More than one server address %s.
FUE0654	ERROR	USER	Client sent an unexpected URL: %s.
FSI0658	INFO	SYSTEM	AI started training quantitative model „%s-%s".
FSE0659	ERROR	SYSTEM	AI training quantitative model „%s-%s" failed: „%s".
FSI0660	INFO	SYSTEM	AI finished training quantitative model „%s-%s".
FSE0661	ERROR	SYSTEM	AI training failed for „%s-%s".
FSI0662	INFO	SYSTEM	AI started training corpus „%s".
FSE0663	ERROR	SYSTEM	AI training corpus „%s" failed: „%s".
FSI0664	INFO	SYSTEM	AI finished training corpus „%s".
FSI0665	INFO	SYSTEM	AI started training model „%s".
FSE0666	ERROR	SYSTEM	AI training model „%s" failed: „%s".
FSI0667	INFO	SYSTEM	AI finished training model „%s". Model weight: %s

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSE0668	ERROR	SYSTEM	AI training failed for „%s”.
FSW0669	WARNING	SYSTEM	AI postponed training quantitative model „%s-%s”. Not enough training data.
FSW0670	WARNING	SYSTEM	AI postponed training corpus „%s”. Not enough training data.
FSW0671	WARNING	SYSTEM	AI postponed training model „%s”. Not enough training data.
FAI0672	INFO	ADMIN	User %s upgraded plugin %s.
FUI0673	INFO	USER	Client requested too small or too large terminal size: %dx%d. Changing to %dx%d.
FUW0674	WARNING	USER	No keys configured, skipping server authentication.
FSW0675	WARNING	SYSTEM	Unable to remove session %s on node %s.
FAI0676	INFO	ADMIN	User %s updated note for account %s.
FUI0677	INFO	USER	Portal user %s updated note for account %s.
FAI0678	INFO	ADMIN	User %s created note for account %s.
FUI0679	INFO	USER	Portal user %s created note for account %s.
FSE0681	ERROR	SYSTEM	Upgrade status could not be determined.
FSI0682	INFO	SYSTEM	Retention module will not be run during upgrade preparations.
FUW0683	WARNING	USER	Server %s accepted public key for user %s without a signature!
FUI0684	INFO	USER	User %s authenticated using SSH key logged in from address: %s.
FAI0686	INFO	ADMIN	User %s loaded new password changer %s.
FSI0688	INFO	SYSTEM	Disconnected callhome tunnel.
FSE0691	ERROR	SYSTEM	Failed to expand external storage.
FAI0692	INFO	ADMIN	User %s changed node name from %s to %s.
FUW0694	WARNING	USER	Session has been terminated: time limit exceeded (user %s, safe %s).
FUW0695	WARNING	USER	Session has been terminated: inactivity limit exceeded (user %s, safe %s).
FUI0698	INFO	USER	User %s authenticated using SMS token logged in from address: %s.
FUE0700	ERROR	USER	Unable to send one-time password to user %s: %s.
FUI0703	INFO	USER	User %s authenticated using DUO/Push logged in from address: %s.
FUE0705	ERROR	USER	Unable to send DUO/%s to user %s: %s.
FAI0706	INFO	ADMIN	User %s enabled send diagnostics setting.
FAI0707	INFO	ADMIN	User %s disabled send diagnostics setting.
FSW0708	WARNING	SYSTEM	AI Identified suspicious activity in session %s.
FSI0709	INFO	SYSTEM	AI Assessed activity in session %s with threat level %s.
FUE0710	ERROR	USER	Unable to change Active Directory password for user %s (domain %s): %s.
FUE0711	ERROR	USER	User %s OTP authentication failed: %s.
FSI0712	INFO	SYSTEM	Azure backup snapshot started.
FSI0713	INFO	SYSTEM	Azure backup snapshot finished.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSW0714	WARNING	SYSTEM	Additional space (%s) required to continue the upgrade.
FAI0715	INFO	ADMIN	User %s disabled sending debug logs to syslog server.
FUW0716	WARNING	USER	SSH connection attempt without ProxyJump.
FSE0717	ERROR	SYSTEM	Browser could not establish a connection due to exceeding a timeout of %ds.
FAI0721	INFO	ADMIN	User %s added remote application %s to server %s.
FAI0722	INFO	ADMIN	User %s removed remote application %s from server %s.
FAI0723	INFO	ADMIN	User %s changed remote application %s in server %s.
FUE0724	ERROR	USER	Too high resolution requested (%ux%u), session dropped.
FAI0729	INFO	ADMIN	User %s changed management SSO settings.
FAI0731	INFO	ADMIN	User %s %s API health check setting.
FSE0734	ERROR	SYSTEM	Unable to authenticate user %s: safe %s requires access acceptance.
FUW0735	WARNING	USER	Session has been terminated: ticket for user %s to account %s has expired.
FSI0745	INFO	SYSTEM	%zu accounts onboarded.
FSI0746	INFO	SYSTEM	%zu accounts quarantined.
FSI0747	INFO	SYSTEM	Scanner %jd/%s removed account %s.
FSI0748	INFO	SYSTEM	Scanner %jd/%s created account %s.
FSE0749	ERROR	SYSTEM	%s %s (pid %d) failed with status %d.
FSE0750	ERROR	SYSTEM	%s %s (pid %d) was terminated by signal %d.
FAI0751	INFO	ADMIN	User {} downloaded {}.
FSE0752	ERROR	SYSTEM	Client sent an invalid request.
FSI0753	INFO	SYSTEM	User %s is waiting for session approval.
FAI0754	INFO	ADMIN	User %s enabled Call Home.
FAI0755	INFO	ADMIN	User %s disabled Call Home.
FAI0756	INFO	ADMIN	User %s requested session %s from archive.
FAW0757	WARNING	ADMIN	Malformed upgrade package: %s
FSE0758	ERROR	SYSTEM	Max number of retries exceeded. Could not remove sessions %s.
FSW0759	WARNING	SYSTEM	Could not remove sessions %s.
FSI0760	INFO	SYSTEM	%s until removal retry for sessions %s.
FAE0761	ERROR	ADMIN	Failed authentication attempt from address %s.
FUI0762	INFO	USER	User %s authenticated using SSO token logged in from address: %s.
FUI0763	INFO	USER	User %s authenticated using X509 certificate logged in from address: %s.
FUE0764	ERROR	USER	User failed to authenticate using SSO token and logging in from address: %s.
FUE0765	ERROR	USER	User failed to authenticate using X509 certificate and logging in from address: %s.
FAE0766	ERROR	ADMIN	Error parsing %s file at position %s.
FAI0767	INFO	ADMIN	User %s changed password complexity settings.

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0768	INFO	ADMIN	User %s changed User CA certificates.
FAI0775	INFO	ADMIN	User %s added relation between nodes %s -> %s.
FAI0776	INFO	ADMIN	User %s removed relation between nodes %s -> %s.
FAI0777	INFO	ADMIN	User %s changed settings for relation between nodes %s -> %s.
FSW0779	WARNING	SYSTEM	Health check «%s» failed.
FAI0780	INFO	ADMIN	User %s enabled retention for session.
FAI0781	INFO	ADMIN	User %s disabled retention for session.
FAI0782	INFO	ADMIN	Interface discovery while configuring external storage: %s
FUI0783	INFO	USER	User %s authenticated using OATH/%s logged in from address: %s.
FUW0784	WARNING	USER	Functionality %s not allowed.
FAI0785	INFO	ADMIN	User %s enabled denying new connections.
FAI0786	INFO	ADMIN	User %s disabled denying new connections.
FAI0787	INFO	ADMIN	User %s changed password changer active node.
FSE0788	ERROR	SYSTEM	Unable to parse address %s.
FSE0789	ERROR	SYSTEM	Unable to find address %s.
FUE0790	ERROR	USER	User %s failed to authenticate after %d %s attempts, disconnecting.
FUE0791	ERROR	USER	User %s failed to authenticate after presenting %d keys, disconnecting.
FSW0793	WARNING	SYSTEM	DNS is slow. It took %jums to resolve %s.
FAI0796	INFO	ADMIN	User %s enabled SNMP TRAP.
FAI0797	INFO	ADMIN	User %s disabled SNMP TRAP.
FSE0798	ERROR	SYSTEM	OpenID Connect (%s) configuration error: %s.
FSE0799	ERROR	SYSTEM	OpenID Connect (%s) request failed: %s.
FSE0801	ERROR	SYSTEM	Multiple users with e-mail %s found during OpenID Connect (%s) authentication.
FUI0802	INFO	USER	User %s authenticated using OpenID Connect (%s).
FSW0803	WARNING	SYSTEM	Unable to send SNMP TRAP.
FUE0804	ERROR	USER	User's %s OATH/%s token might have been cloned (current counter: %ju, new counter: %ju).
FUI0805	INFO	USER	User %s presence confirmed during SSH authentication.
FUE0806	ERROR	USER	User %s not present during SSH authentication.
FUE0807	ERROR	USER	User's %s SSH key may have been cloned (current counter: %ju, new counter: %ju).
FUI0808	INFO	USER	Verification by the user %s confirmed during SSH authentication.
FUE0809	ERROR	USER	No verification by the user %s during SSH authentication.
FAI0810	INFO	ADMIN	User %s deleted undelivered email notifications. Recipient list: %s
FAI0811	INFO	ADMIN	User %s resent undelivered email notifications. Recipient list: %s

Kontynuacja na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSE0812	ERROR	SYSTEM	User with name %s not found during OpenID Connect (%s) authentication.
FSE0813	ERROR	SYSTEM	User's %s e-mail is not verified during OpenID Connect (%s) authentication.
FSE0814	ERROR	SYSTEM	User with neither name %s nor e-mail %s found during OpenID Connect (%s) authentication.
FAI0815	INFO	ADMIN	User %s created OpenID Connect %s.
FAI0816	INFO	ADMIN	User %s changed OpenID Connect %s: %s.
FAI0817	INFO	ADMIN	User %s deleted OpenID Connect %s.
FSW0818	WARNING	SYSTEM	The number of active users exceeds the „activeusers" limit from the license.
FSW0819	WARNING	SYSTEM	Server is not accessible through listener %s.
FSE0821	ERROR	SYSTEM	Unable to establish connection: server not found (listener: %s, user: %s, target: %s, port: %u).
FAI0822	INFO	ADMIN	User %s added KDC server %s with domain %s.
FAI0823	INFO	ADMIN	User %s removed KDC server %s with domain %s.
FAE0824	ERROR	ADMIN	Error saving KDC servers: „%s".
FSW0825	WARNING	SYSTEM	User %s not synchronized from LDAP server %s, validation error: %s.
FAI0826	INFO	ADMIN	User %s granted access to %s for %s.
FAI0827	INFO	ADMIN	User %s removed access to %s for %s.
FUE0828	ERROR	USER	Server's certificate does not match configured certificate.
FAW0832	WARNING	ADMIN	Problem with NTP server. Host: %s. Message ntpdate: %s.
FSI0835	INFO	SYSTEM	Scanner %jd/%s removed server %s.
FSI0836	INFO	SYSTEM	Scanner %jd/%s created server %s.
FSI0837	INFO	SYSTEM	%zu servers onboarded.
FSI0838	INFO	SYSTEM	%zu servers quarantined.
FSW0857	WARNING	SYSTEM	Scanner %jd/%s can not remove server %s: %s
FSE0946	ERROR	SYSTEM	OpenID Connect (%s) data is missing the sub claim.
FSE0947	ERROR	SYSTEM	User with sub %s not found during OpenID Connect (%s) authentication.
FSE0948	ERROR	SYSTEM	User's %s OpenID Connect (%s) sub claim mismatch (%s != %s).
FSI0949	INFO	SYSTEM	User %s automatically linked with sub %s for OpenID Connect %s.
FUE0953	ERROR	USER	User %s failed to authenticate, disconnecting.
FSE0962	ERROR	SYSTEM	Failed to take job from queue, error: {err}
FSE0963	ERROR	SYSTEM	Failed to parse message «{buffer}» on Unix Socket into command, err: {err}
FSE0964	ERROR	SYSTEM	Client Error handling command «{command:?}»: {err}
FSE0965	ERROR	SYSTEM	Failed to get scheduled job, error: {err}
FSE0966	ERROR	SYSTEM	Failed to queue scheduled job, error: {err}
FSE0967	ERROR	SYSTEM	Client was interrupted: {serve_result:?}

Kontynuacja na następnej stronie

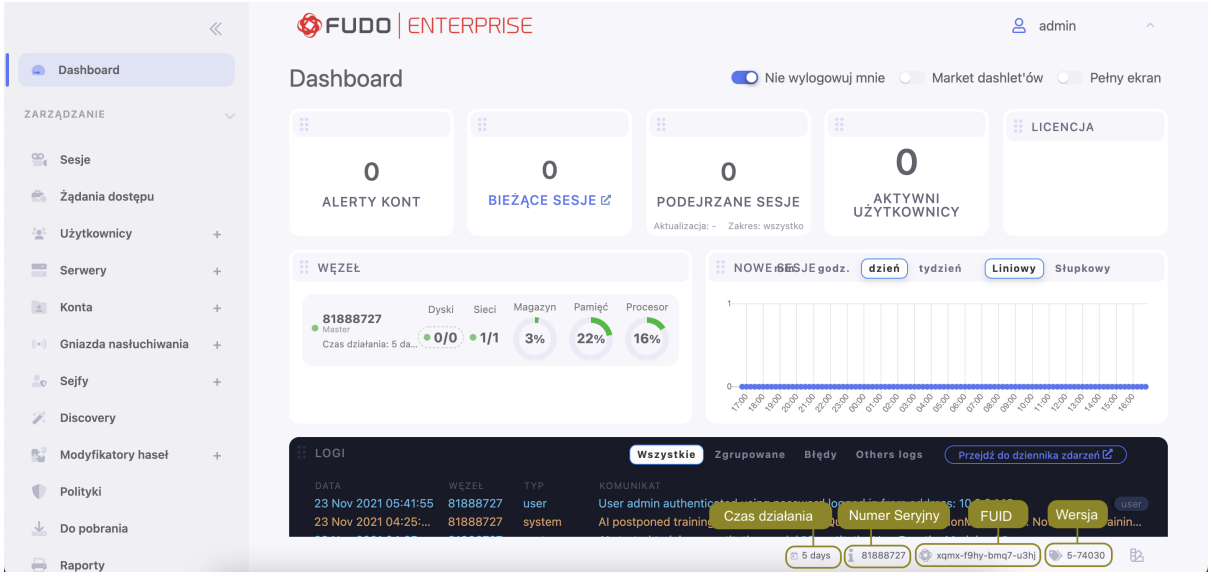
Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSE0968	ERROR	SYSTEM	Scheduler was interrupted: {serve_result:?}
FSE0969	ERROR	SYSTEM	Listener was interrupted: {serve_result:?}
FSE0970	ERROR	SYSTEM	Client connection with Unix Socket is not writeable, err: {err}
FSE0971	ERROR	SYSTEM	Failed to write response to client through Unix Socket, err: {err}
FSE0972	ERROR	SYSTEM	Job {job_id} failed with error: {err}
FSE0974	ERROR	SYSTEM	Failed to shutdown Fudo.
FSE0976	ERROR	SYSTEM	Failed to restart Fudo.
FSE0977	ERROR	SYSTEM	Failed to change Fudo version.
FSE0978	ERROR	SYSTEM	Failed to list Fudo versions.

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.



ROZDZIAŁ 24

Fudo Officer 2.0

Fudo Officer 2.0 to aplikacja mobilna wykorzystująca funkcjonalność **Just In Time**, umożliwiająca administratorom Fudo Enterprise zarządzanie żądaniami dostępu użytkowników do docelowych serwerów. Żądania mogą być akceptowane lub odrzucane przez administratorów za pośrednictwem aplikacji Fudo Officer 2.0 lub z poziomu Panelu Administracyjnego, z zakładki *Zarządzanie* > *Żądania dostępu*.

Informacja: Więcej na temat funkcji Just In Time oraz zarządzania żądaniami dostępu w Panelu Administracyjnym znajdziesz w rozdziale *Żądania dostępu*.

Informacja: Więcej na temat funkcji Just In Time oraz zarządzania żądaniami dostępu w Panelu Administracyjnym znajdziesz w rozdziale *Żądania dostępu*.

24.1 Konfiguracja

Informacja:

- Aby powiązać urządzenie mobilne, funkcja *Call Home* musi być włączona. Przejdź do *Ustawienia* > *System* i włącz ją w zakładce *Ogólne*, w sekcji *Utrzymanie i nadzór*.
- Pamiętaj, aby poprosić swojego dystrybutora Fudo Enterprise o dostęp do funkcji **Call Home**.

Aby skonfigurować Fudo Officer 2.0, pobierz aplikację ze sklepu z aplikacjami odpowiedniego dla systemu Android lub iOS i postępuj zgodnie z instrukcją:

Ostrzeżenie: Podczas procesu konfiguracji należy przyznać aplikacji Fudo Officer 2.0 dostęp do kamery oraz zezwolić na wysyłanie powiadomień.

1. Skonfiguruj Fudo Enterprise:

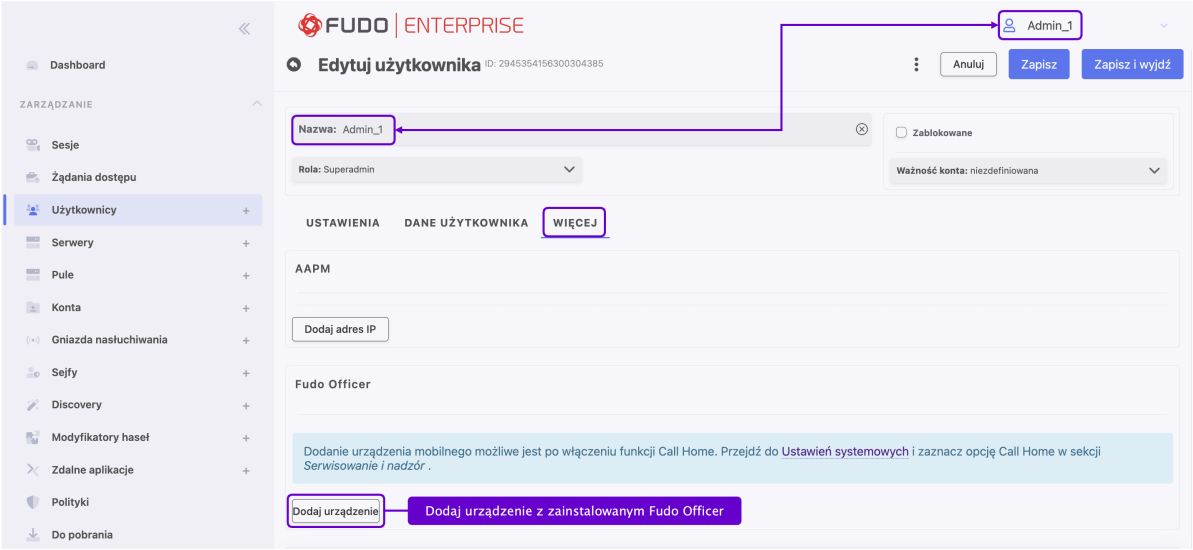
   1.1. Otwórz Panel Administracyjny Fudo Enterprise i przejdź do *Zarządzanie* > *Użytkownicy*.

   1.2 Znajdź i edytuj użytkownika, dla którego chcesz utworzyć profil w Fudo Officer 2.0.

   1.3. Przejdź do zakładki *WIĘCEJ* i kliknij przycisk *Dodaj urządzenie* w polu *Fudo Officer*, aby wygenerować kod QR.

Informacja:

- Powiązanie z Fudo Officer 2.0 można skonfigurować tylko dla użytkownika aktualnie zalogowanego do Panelu Administracyjnego.
- Tylko użytkownik z rolą *superadmin* lub *admin* może korzystać z aplikacji mobilnej Fudo Officer 2.0.



2. Otwórz aplikację Fudo Officer 2.0 na swoim urządzeniu mobilnym i wybierz *Rozpocznij*:

   2.1. Zezwól aplikacji Fudo Officer 2.0 na dostęp do kamery wymagany do skanowania kodów QR.

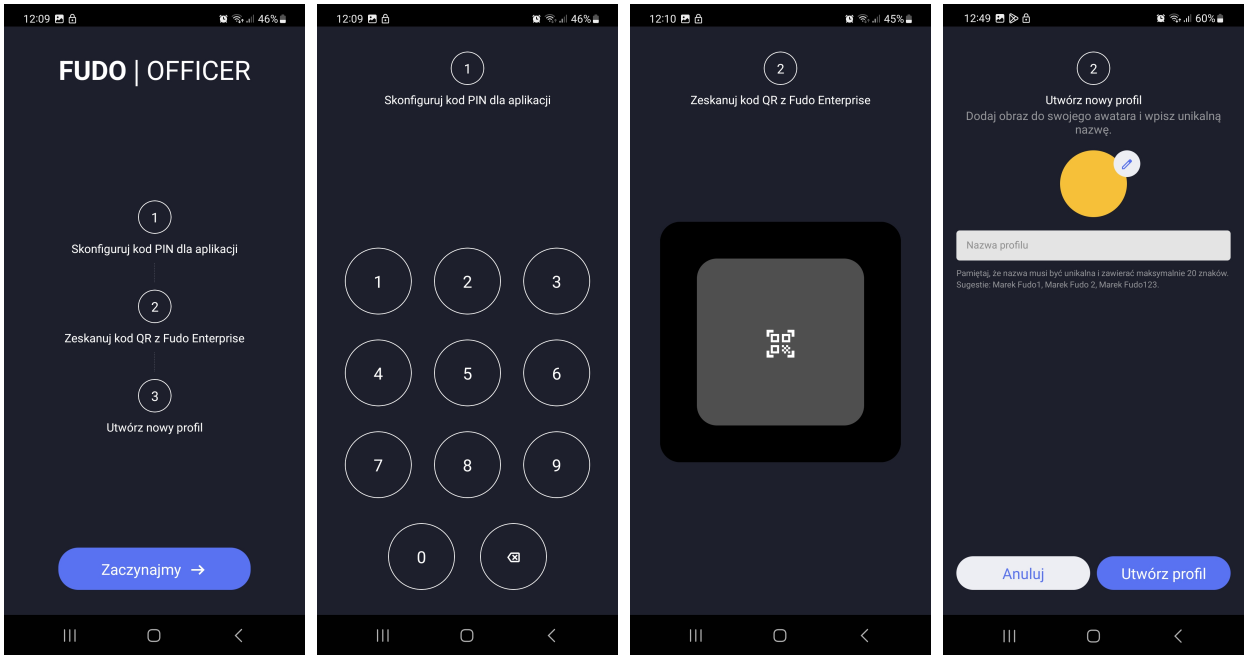
   2.2. Ustaw 6-cyfrowy kod PIN, który będzie używany do ochrony dostępu do aplikacji.

   2.2. Powtórz wprowadzony PIN, aby go potwierdzić.

   2.3. Zezwól aplikacji Fudo Officer 2.0 na wysyłanie powiadomień.

   2.4. Zeskanuj kod QR wyświetlany w Panelu Administracyjnym za pomocą swojego urządzenia mobilnego.

   2.5. Ustaw nazwę profilu i kliknij przycisk *Utwórz profil*.



Informacja: Nazwa profilu jest edytowalna.

3. Wróć do Panelu Administracyjnego Fudo Enterprise i kliknij *Zamknij* w oknie kodu QR. W sekcji *Fudo Officer* widoczne jest od teraz pole *Platforma* z nazwą powiązanego urządzenia oraz pole *Push ID* z odpowiednim ciągiem znaków.
4. Kliknij przycisk Zapisz, aby zapisać zmiany w konfiguracji użytkownika.
5. Teraz możesz zarządzać żądaniami użytkowników poprzez utworzony profil.

Powiązane tematy:

- *Zarządzanie Profilami*
- *Zarządzanie Żądaniami Sesji*
- *Fudo Officer Settings*

24.2 Zarządzanie Profilami

Profil w Fudo Officer 2.0 odpowiada obiektowi Użytkownik w Fudo Enterprise. Możesz zarządzać wieloma Profilami z poziomu jednej aplikacji Fudo Officer 2.0.

24.2.1 Dodawanie Profilów

Informacja: Pierwszy Profil jest tworzony podczas *wstępnej konfiguracji aplikacji*.

Informacja:

- Powiązanie urządzenia mobilnego możesz skonfigurować tylko dla użytkownika aktualnie zalogowanego do Panelu Administracyjnego Fudo Enterprise.
- Tylko użytkownik z rolą *superadmin* lub *admin* może korzystać z aplikacji mobilnej Fudo Officer 2.0.

Aby dodać nowy profil, wykonaj poniższe kroki:

1. Skonfiguruj Fudo Enterprise:

   1.1. Otwórz Panel Administracyjny Fudo Enterprise i przejdź do *Zarządzanie* > *Użytkownicy*.

   1.2 Znajdź i edytuj użytkownika, dla którego chcesz utworzyć profil w Fudo Officer 2.0.

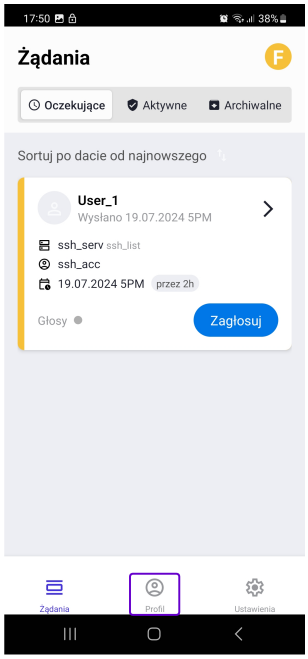
   1.3. Przejdź do zakładki *WIĘCEJ* i kliknij przycisk *Dodaj urządzenie* w polu *Fudo Officer*, aby wygenerować kod QR.

Informacja:

- Aby móc dodać urządzenie mobilne, funkcja *Call Home* musi być włączona. Przejdź do Ustawienia > System i włącz ją w zakładce *Ogólne*, w sekcji *Utrzymanie i nadzór*.
- Poproś swojego dystrybutora Fudo Enterprise o dostęp do funkcji **Call Home**.

---

2. Otwórz aplikację Fudo Officer 2.0, wybierz ikonę *Profil* na dole ekranu i kliknij przycisk + *Dodaj nowy profil*.



3. Zeskanuj kod QR wyświetlany w Panelu Administracyjnym za pomocą swojego urządzenia mobilnego.
4. Ustaw nazwę Profilu i wybierz *Utwórz profil*.

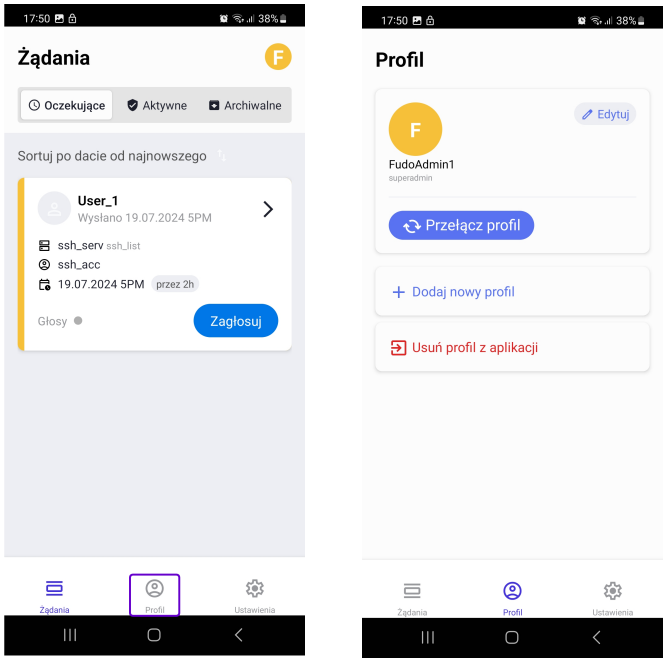
Informacja: Nazwa profilu jest edytowalna.

5. Wróć do Panelu Administracyjnego Fudo Enterprise i kliknij *Zamknij* w oknie kodu QR. Sekcja *Fudo Officer* posiada teraz pole *Platforma* z nazwą powiązanego urządzenia oraz pole *Push ID* z odpowiednim ciągiem znaków.
6. Kliknij przycisk *Zapisz*, aby zapisać zmiany w konfiguracji użytkownika.

24.2.2 Przełączanie Profilów

Możesz łatwo przełączać profile, aby zarządzać żądaniami z różnych kont użytkowników. Aby przełączać się między dostępnymi profilami, wykonaj poniższe kroki:

1. Wybierz ikonę *Profil* na dole ekranu.
2. Wybierz *Przełącz profil*, aby uzyskać dostęp do listy dostępnych profili.
3. Wybierz nazwę profilu z listy, aby go wybrać.
4. Zostaniesz automatycznie przekierowany do widoku *Żądania*, aby zarządzać żądaniami skierowanymi do tego profilu.

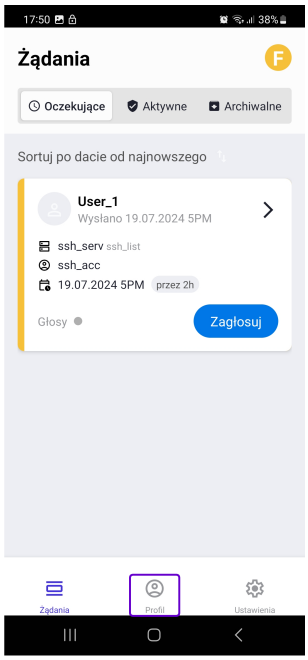


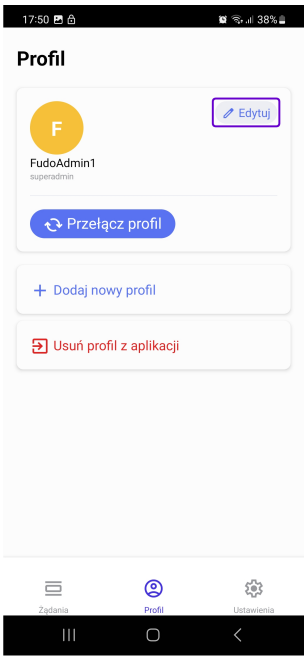
24.2.3 Edytowanie Profilu

Możesz edytować nazwę i zdjęcie profilowe aktywnego profilu:

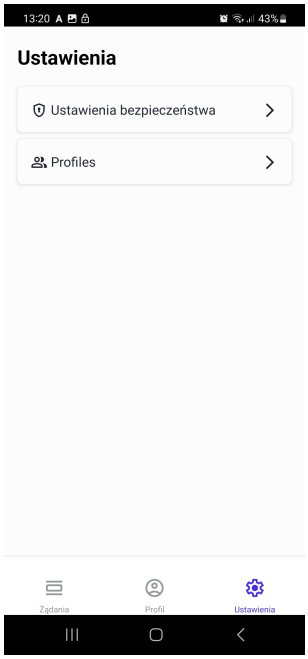
1. Wybierz ikonę *Profil* na dole ekranu.
2. Wybierz *Edytuj* obok nazwy Profilu.
3. Wprowadź nową nazwę Profilu.
4. Edytuj avatar, wybierając ikonę ołówka obok niego i przesyłając żądane zdjęcie z pamięci urządzenia.

5. Wybierz *Zapisz*, aby zapisać zmiany.





Informacja: Możesz również przełączać profile w ustawieniach aplikacji. Wystarczy wybrać ikonę koła zębatego w prawym dolnym rogu ekranu i wybrać *Profile*.

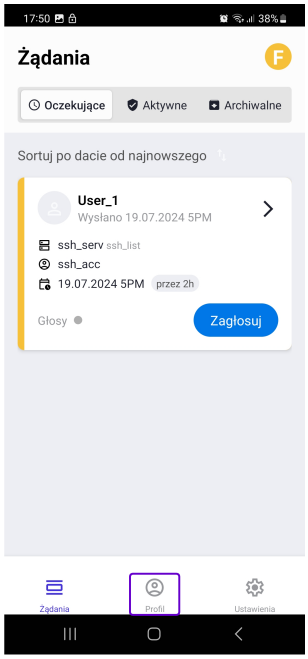


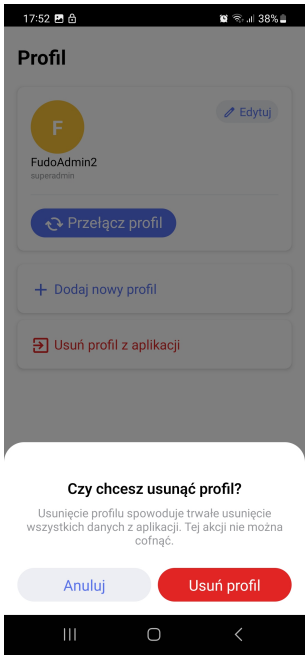
Informacja: Aby zmienić PIN, przejdź do sekcji *Zmiana kodu PIN*.

24.2.4 Usuwanie Profilu

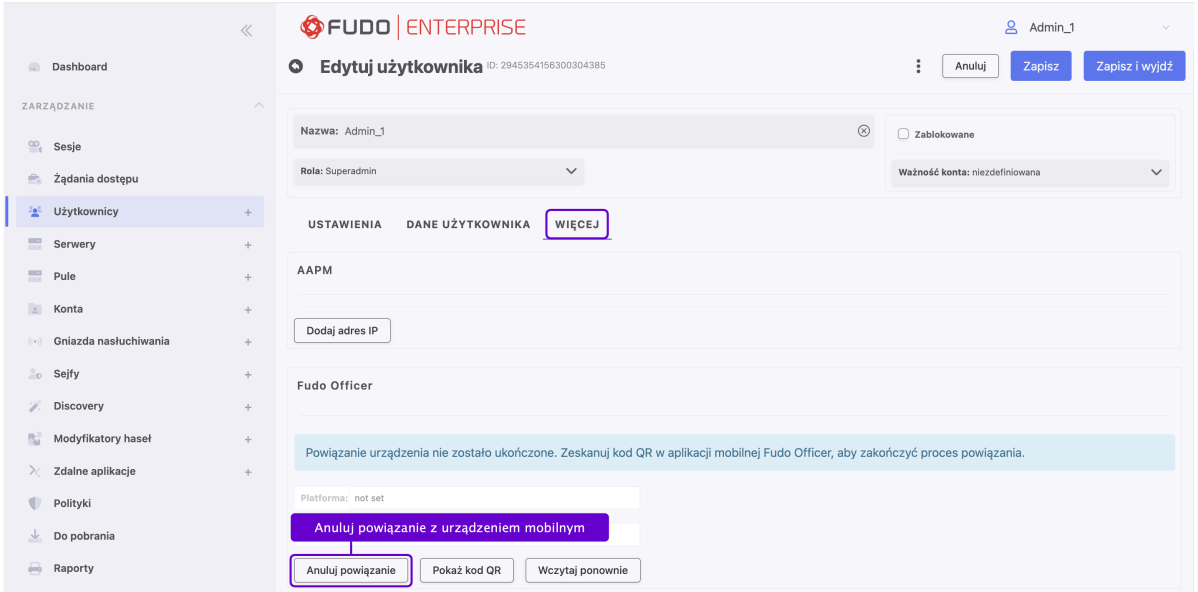
Aby usunąć profil z Fudo Officer 2.0, najpierw musisz przełączyć się na ten profil:

1. Wybierz ikonę *Profil* na dole ekranu.
2. Wybierz *Przełącz profil*, aby uzyskać dostęp do listy dostępnych profili.
3. Wybierz nazwę profilu z listy, aby go wybrać.
4. Ponownie wybierz ikonę *Profil* na dole ekranu.
5. Wybierz *Usuń profil z aplikacji*.
6. Wybierz *Usuń profil*, aby potwierdzić.





Informacja: Upewnij się, że odłączyłeś również urządzenie w konfiguracji użytkownika w Panelu Administracyjnym Fudo Enterprise.



Powiązane tematy:

- *Zarządzanie Żądaniami Sesji*
- *Fudo Officer Settings*

24.3 Zarządzanie Żądaniami Sesji

Istnieją trzy rodzaje żądań: oczekujące, aktywne i archiwalne.

Informacja: Żeby obsługiwać żądania dostępu, opcja *Just In Time*, oraz opcja *Sesja oczekująca na zatwierdzenie (push)* dla powiadomień push musi być włączona w danym sejfie.

24.3.1 Żądania Oczekujące

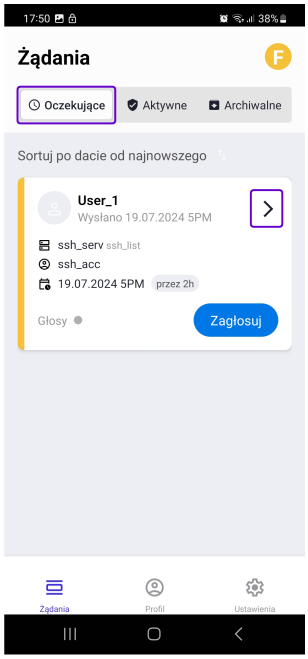
Zakładka **Oczekujące** pokazuje listę żądań oczekujących na decyzję od aktualnego profilu użytkownika.

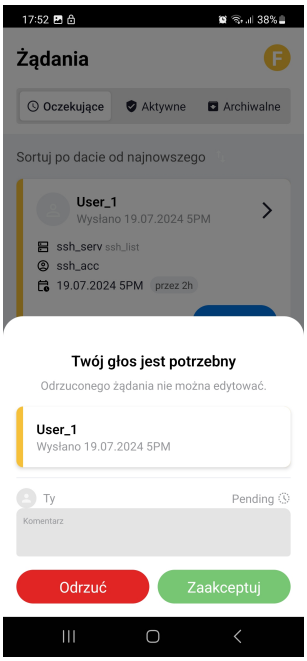
Informacja:

- Dostępne są dwa rodzaje żądań do wysłania przez użytkownika: *natychmiastowe* i *zaplanowane*. Szczegółowe informacje na ten temat znajdziesz w rozdziale *Żądania dostępu*.
- Aby dowiedzieć się, jak użytkownicy mogą wysyłać żądania, zapoznaj się z sekcją Połączenie przez żądanie o dostęp w dokumentacji Portalu Użytkownika.

Aby głosować za zatwierdzeniem lub odrzuceniem żądania, wykonaj poniższe kroki:

1. Otwórz Fudo Officer 2.0 i podaj kod PIN. Zostaniesz automatycznie przekierowany do zakładki **Oczekujące**.
2. Stuknij strzałkę obok nazwy użytkownika, aby rozwinąć szczegóły żądania.
3. Alternatywnie, wybierz przycisk *Zagłosuj*, aby zatwierdzić lub odrzucić żądanie bezpośrednio z tej zakładki.
4. W przypadku odrzucenia wymagany jest komentarz do decyzji.
5. Wybierz przycisk *Akceptuj* lub *Odrzuć*.





Informacja:

- Zatwierdzone żądania można znaleźć w zakładce **Aktywne**.
- Odrzucone żądania można znaleźć w zakładce **Archiwalne**.

Informacja:

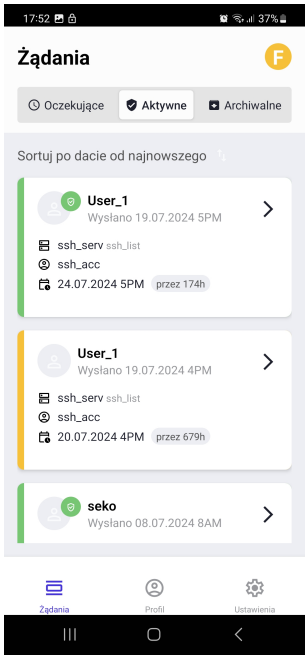
- Użytkownicy, którzy wysłali żądanie za pośrednictwem Portalu Użytkownika i mają skonfigurowany adres e-mail w Panelu Administracyjnym, otrzymają wiadomość, gdy ich żądanie zostanie zaakceptowane lub odrzucone.

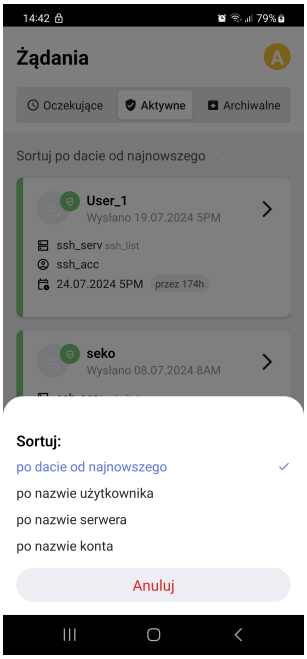
24.3.2 Żądania Aktywne

Zakładka **Aktywne** wyświetla listę dwóch rodzajów żądań:

- Żądania, które zostały zaakceptowane przez wymaganą liczbę głosujących (oznaczone na zielono).
- Żądania oczekujące na głosy innych administratorów (oznaczone na żółto).

Żądania można sortować według *daty, użytkownika, nazwy serwera lub nazwy konta.*



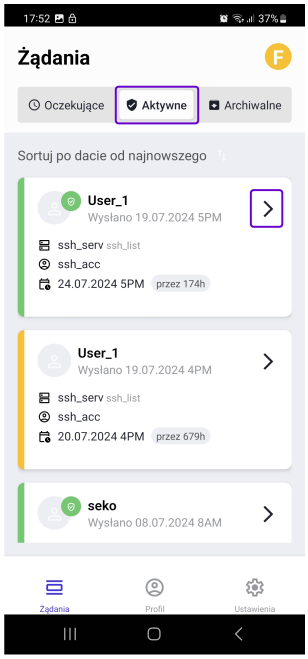


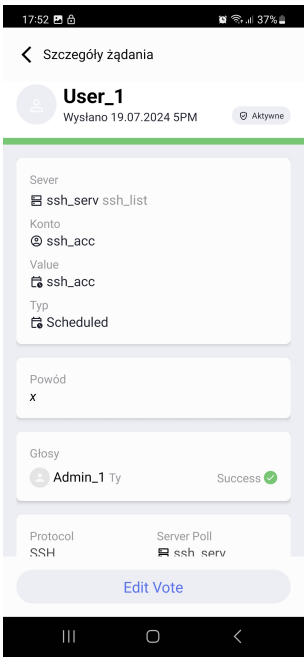
24.3.3 Cofnięcie Żądania

Głosy oddane na zatwierdzone i aktywne żądania można cofnąć, na przykład w przypadku wykrycia nadużycia. Opcja ta jest też przydatna, gdy użytkownik zakończył pracę wcześniej niż przewidywano, ale jego żądanie jest nadal ważne.

Aby cofnąć zatwierdzone i aktywne żądania, wykonaj poniższe kroki:

1. Otwórz Fudo Officer 2.0 i podaj kod PIN.
2. Wybierz zakładkę **Aktywne**.
3. Wybierz strzałkę obok nazwy użytkownika, aby rozwinąć szczegóły żądania.
4. Wybierz przycisk *Edytuj głos* na dole ekranu żądania.
5. W polu **Komentarz** podaj powód cofnięcia (wymagane).
6. Wybierz przycisk *Odrzuć*, aby cofnąć żądanie.

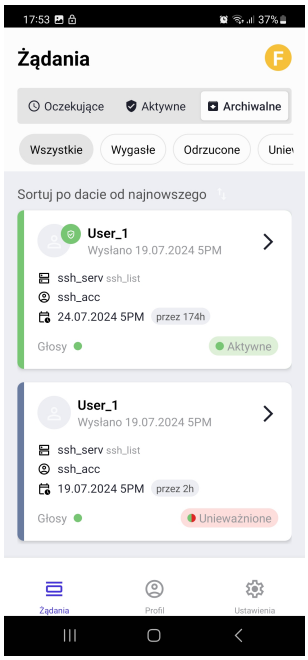




Informacja: Jeśli zaakceptowałeś żądanie, które nadal oczekuje na głosy innych administratorów, przycisk *Odrzuć* będzie dostępny bezpośrednio na ekranie żądania.

24.3.4 Żądania Archiwalne

Historia przetworzonych żądań jest dostępna w zakładce **Archiwalne**. Żądania archiwalne można sortować według statusów *wygasłe, odrzucone, cofnięte* i *zatwierdzone*.



Powiązane tematy:

- *Fudo Officer Settings*

24.4 Ustawienia

Aby uzyskać dostęp do ustawień aplikacji, wybierz ikonę koła zębatego w prawym dolnym rogu ekranu.

24.4.1 Uwierzytelnianie biometryczne

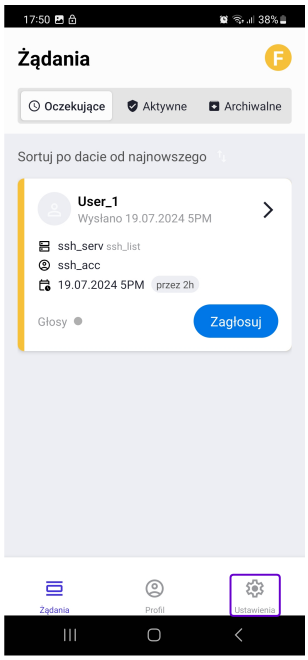
Aby włączyć opcję uwierzytelniania biometrycznego:

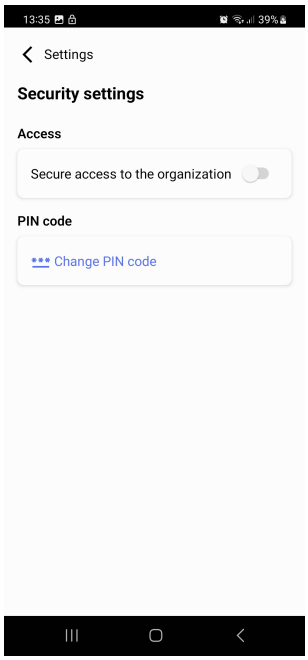
1. Wybierz ikonę koła zębatego w prawym dolnym rogu ekranu.
2. Wybierz *Ustawienia bezpieczeństwa*.
3. Wybierz opcję *Włącz uwierzytelnianie biometrią*.
4. Zeskanuj odcisk palca, aby zakończyć procedurę.

Informacja: Po włączeniu opcji uwierzytelnianie biometryczne zostanie ustawione jako metoda domyślna podczas uruchamiania aplikacji.

24.4.2 Zmiana kodu PIN

1. Wybierz ikonę koła zębatego w prawym dolnym rogu ekranu.
2. Wybierz *Ustawienia bezpieczeństwa*.
3. Wybierz *Zmień kod PIN*.





4. Podaj nowy 6-cyfrowy kod PIN.
5. Powtórz podany 6-cyfrowy kod PIN, aby potwierdzić zmianę.

24.4.3 Język

Język aplikacji jest ustawiany zgodnie z ustawieniami języka telefonu.

Powiązane tematy:

- *Zarządzanie Żądaniami Sesji*

ROZDZIAŁ 25

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 5.5

Fudo Enterprise 5.5 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, możesza wykorzystać znajdujące się w nim narzędzia *pip* oraz *easy_ install*. W takim przypadku, należy dodatkowo ustawić ścieżkę do bibliotek współdzielonych i uruchomić `virtualenv` wskazując interpreter w parametrze `-p`:

```
    LD_LIBRARY_PATH=/opt/python-3.6/lib
/opt/python-3.6/bin/pip install virtualenv requests
/opt/python-3.6/bin/virtualenv -p /opt/python-3.6/bin/python deps
```

W celu aktywacji środowiska, wykonaj komendę

```
source deps/bin/activate
```

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 5.5

Fudo Enterprise 5.5 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 katalog nadrzędny `fudopv/` do ścieżki wyszukiwania Pythona. Wykonaj polecenie `export PYTHONPATH=~/parent`, gdzie `"~/parent"` to ścieżka do katalogu, w którym znajduje się `fudopv/`.
5. Uruchom `source deps/bin/activate`.
6. Z poziomu katalogu `parent/` uruchom `python -m fudopv`.

Tematy pokrewne:

- *Uruchamianie fudopv*
- *Kompilowanie narzędzia fudopv*

25.3 Uruchamianie *fudopv*

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 jest ostatnią wersją obsługującą *Application to Application Password Manager*. Funkcjonalność modułu *AAPM* zostanie zastąpiona APIv2 w kolejnym wydaniu.

Parametry wywołania

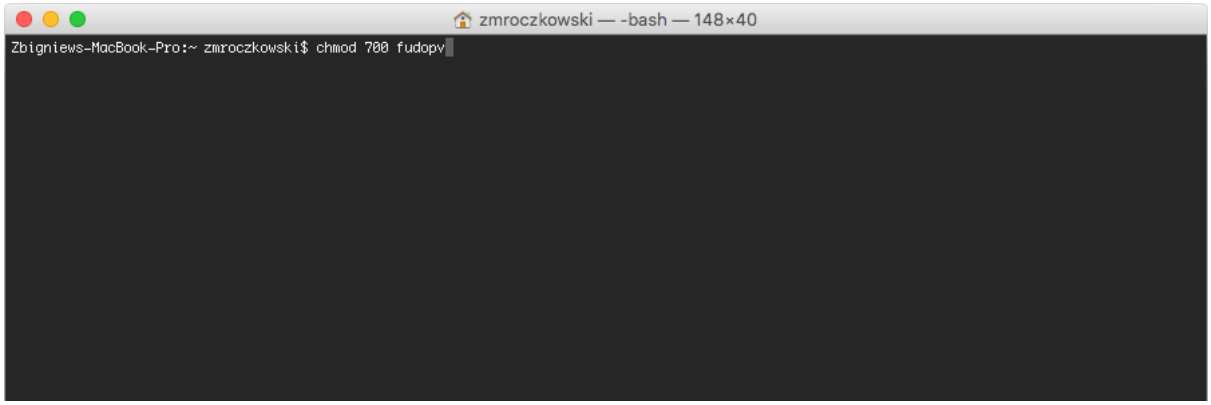
Podczas pracy z *fudopv* używany jest następujący format poleceń:

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

Poniższa tabela przedstawia listę opcji dostępnych dla polecenia `fudopv`.

Komenda/opcja/parametr	Opis
Komendy	
`getcert`	Pobierz certyfikat SSL *Portalu Użytkownika*.
`getpass` <typ> <nazwa_konta>	Pobierz hasło do wybranego konta. typ: • `direct` - połączenie bezpośrednie, niemonitorowane; • `fudo` - połączenie monitorowane przez moduł PSM
Opcje dla typu fudo	
`-s <adres>, --server-address <adres>`	Adres serwera, do którego będzie łączyć się konto.
`-p <port>, --port <port>`	Port serwera, do którego będzie łączyć się konto
Opcje ogólne	
`-c <ścieżka>, --cfg <ścieżka>`	Użyj pliku konfiguracyjnego znajdującego się we wskazanej lokalizacji.
`-h, --help`	Wyświetl listę opcji i parametrów wywołania skryptu.

1. Skrypt `fudopv` umieść na serwerze i nadaj mu prawa wykonywalności.



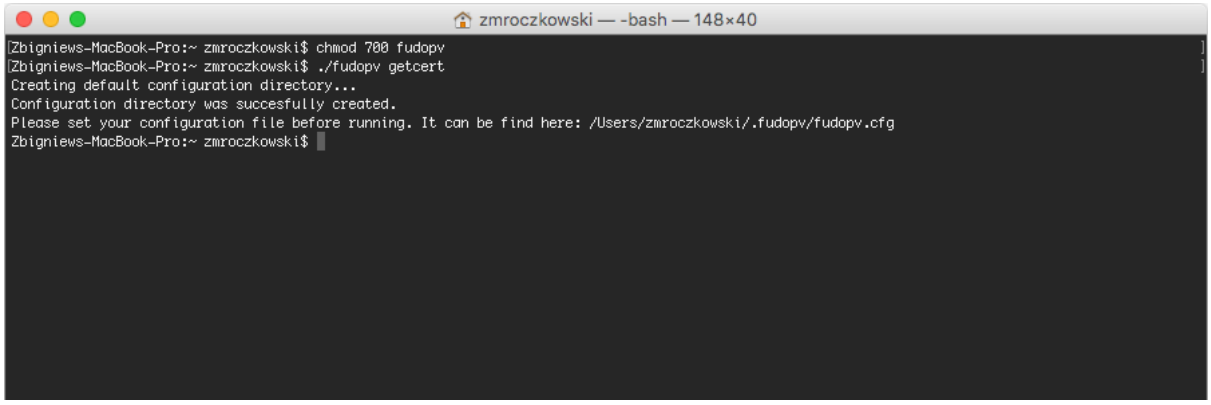
2. Zaloguj się do panelu administracyjnego Fudo Enterprise.
3. Stwórz konto użytkownika o roli *User*, uwierzytelnianego hasłem statycznym.

Informacja:

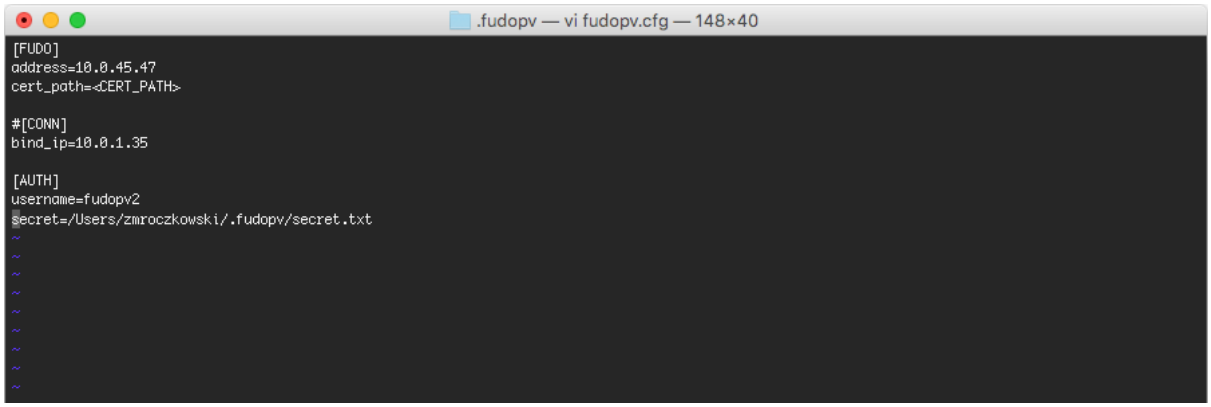
- Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
- Kliknij *+Dodaj użytkownika*.
- Wprowadź nazwę użytkownika.
- Określ termin ważności konta.
- Z listy rozwijalnej *Rola*, wybierz *User*.
- Przypisz użytkownikowi sejf i kliknij obiekt, aby wywołać jego właściwości.
- Zaznacz opcję *Pokaż hasło*.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



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



Sekcja	Opis
`[FUDO]`	
`address`	Adres IP *Portalu Użytkownika*.
`cert_path`	Ścieżka pliku z certyfikatem SSL Portalu Użytkownika.

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

`[AUTH]`	
`username`	Nazwa obiektu użytkownika zdefiniowanego w kroku 3.
`secret`	Lokalizacja pliku z hasłem statycznym.

Informacja:

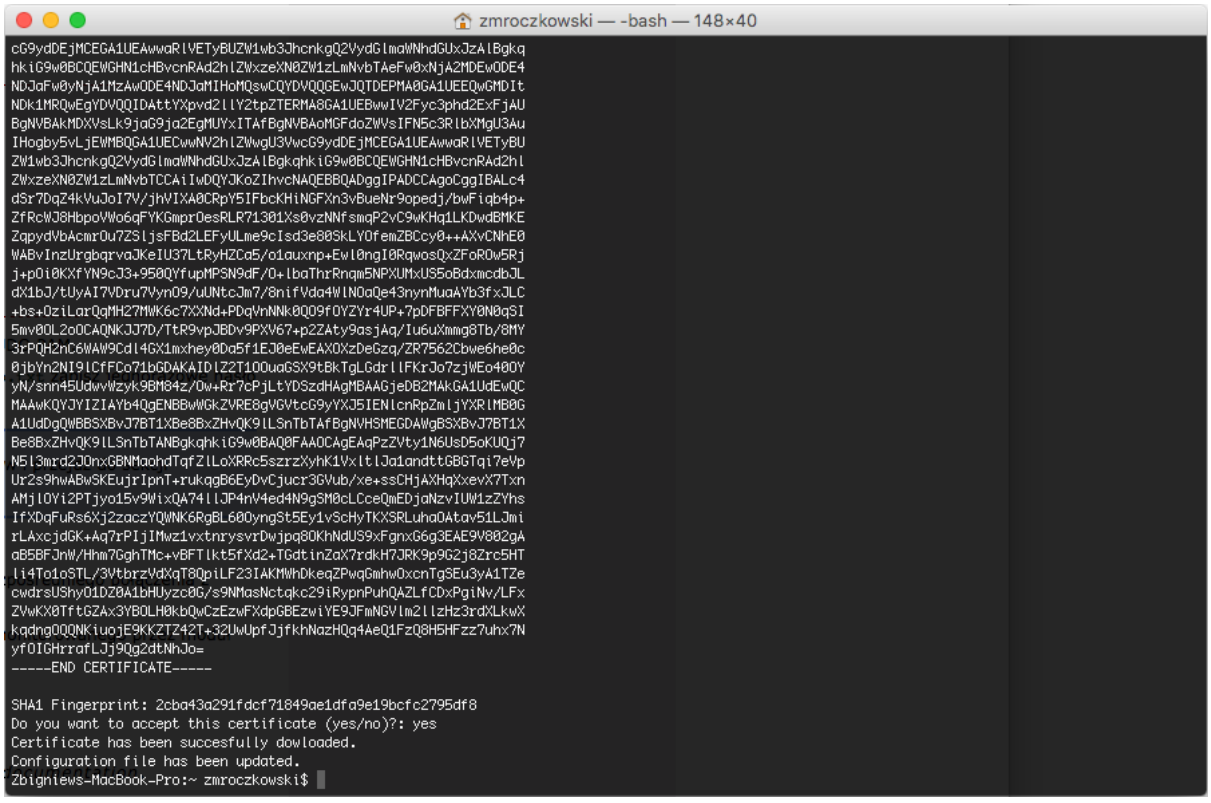
- W sekcji `[FUDO]`, w linii `address`, wprowadź adres IP Portalu Użytkownika.

- Linię `cert_path` pozostaw bez zmian, zostanie ona uzupełniona automatycznie przy okazji poprawnego wykonania komendy `fudopv getcert`.
- Jeśli dla użytkownika skonfigurowana została możliwość wysyłania zapytań do API z określonego adresu IP, w sekcji `[CONN]`, odkomentuj linię `bind_ip` i wprowadź adres IP serwera, na którym wykonywany jest skrypt `fudopv`.
- W sekcji `[AUTH]`, w linii `username`, uzupełnij nazwę konta obiektu użytkownik, stworzonego w kroku 3.

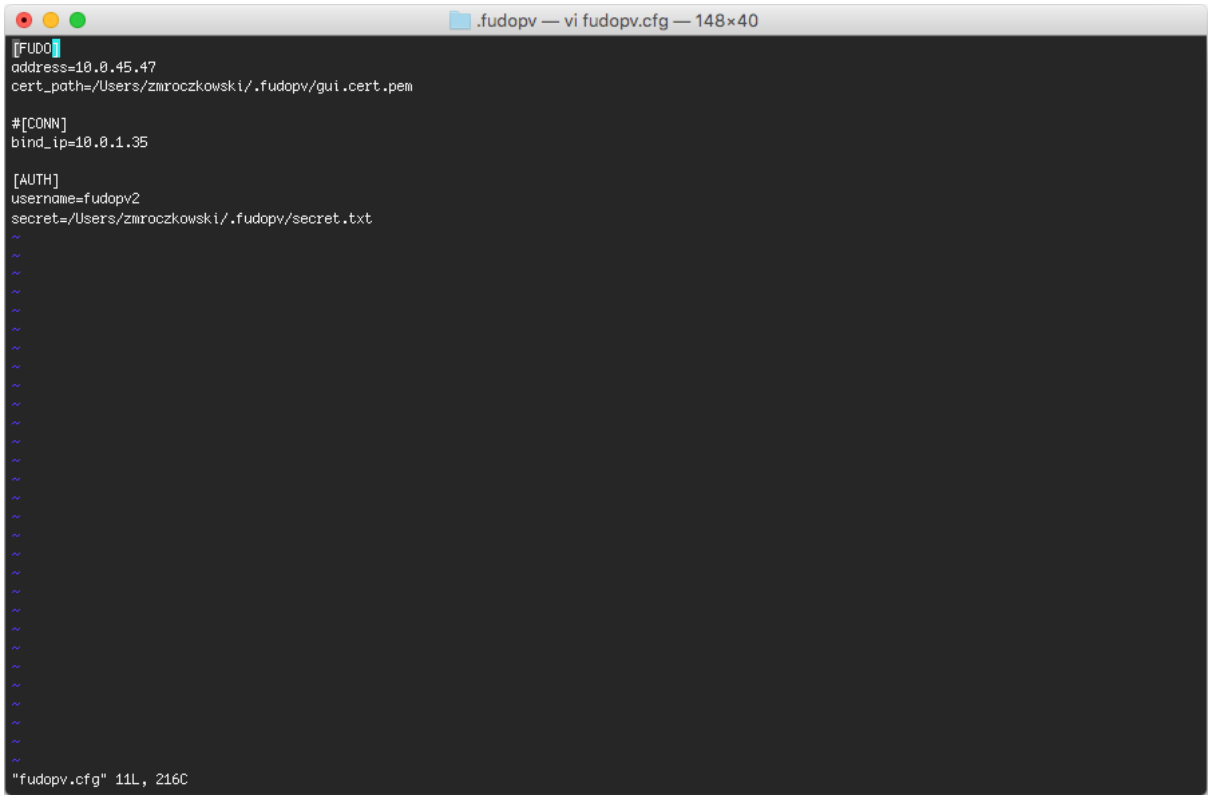
Na przykład:

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

[CONN]
bind_ip=10.0.0.8.11

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

6. Wykonaj komendę `fudopv getcert`, aby pobrać certyfikat Portalu Użytkownika.

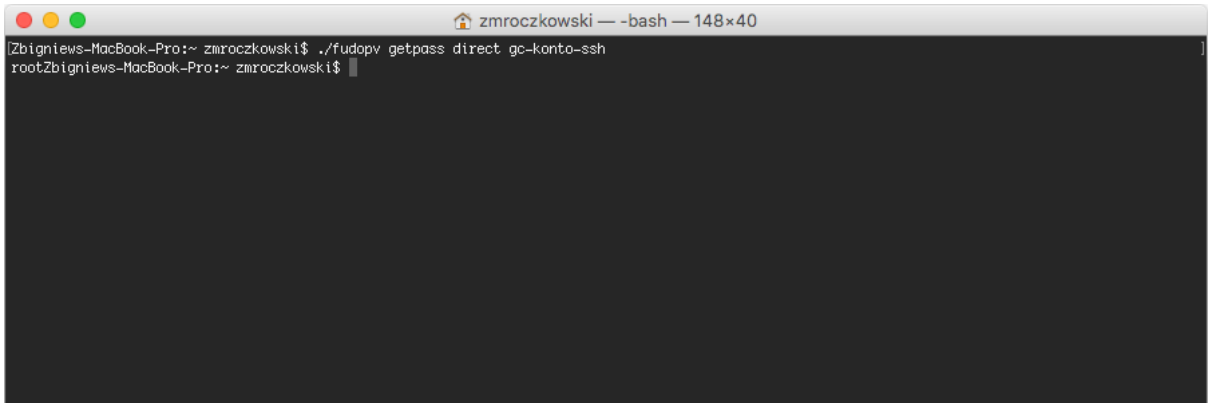


Informacja: Po prawidłowym wykonaniu komendy, ścieżka certyfikatu w pliku konfiguracyjnym zostanie automatycznie uzupełniona.

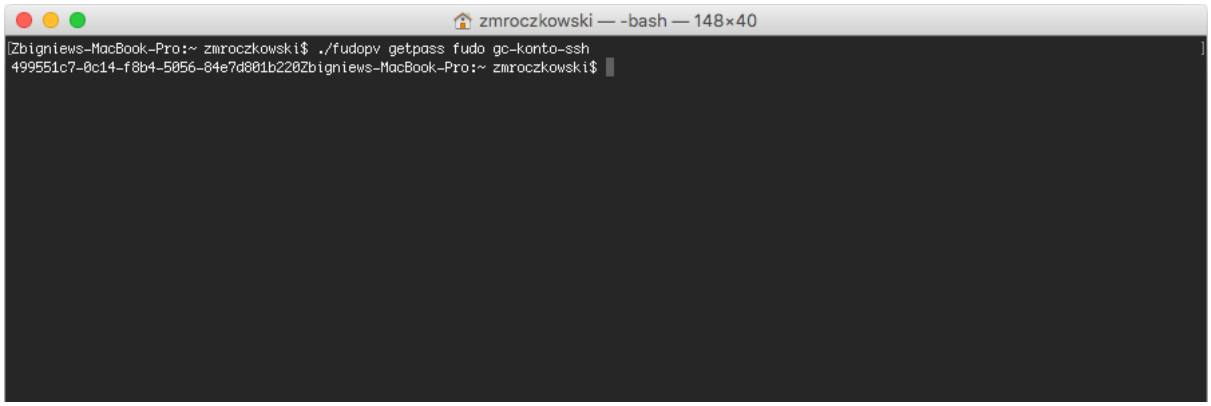


7. W pliku `secret.txt` zapisz hasło konta użytkownika.
8. Wykonaj komendę:

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



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



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

Tematy pokrewne:

- *Kompilowanie narzędzia fudopv*
- *Model danych*
- *Opis systemu*
- *Konfigurowanie modyfikatora haseł Unix poprzez SSH*

25.4 Sposoby uwierzytelnienia

Funkcja zdeprecjonowana od wersji 5.5

Fudo Enterprise 5.5 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

Statyczne hasło użytkownika, przechowywane w pliku `secret.txt`.

- -> url: https://FUDO/api/portal/login
- -> method: POST
- -> `{"username": "USER", "password": "SECRET"}`
- <- status:
  - 200, OK
    - <- `{"sessionid": "SESSIONID"}`
  - 401, UNAUTHORIZED
  - <- *Nie dotyczy.*

Tematy pokrewne:

- *Uruchamianie fudopv*
- *Kompilowanie narzędzia fudopv*

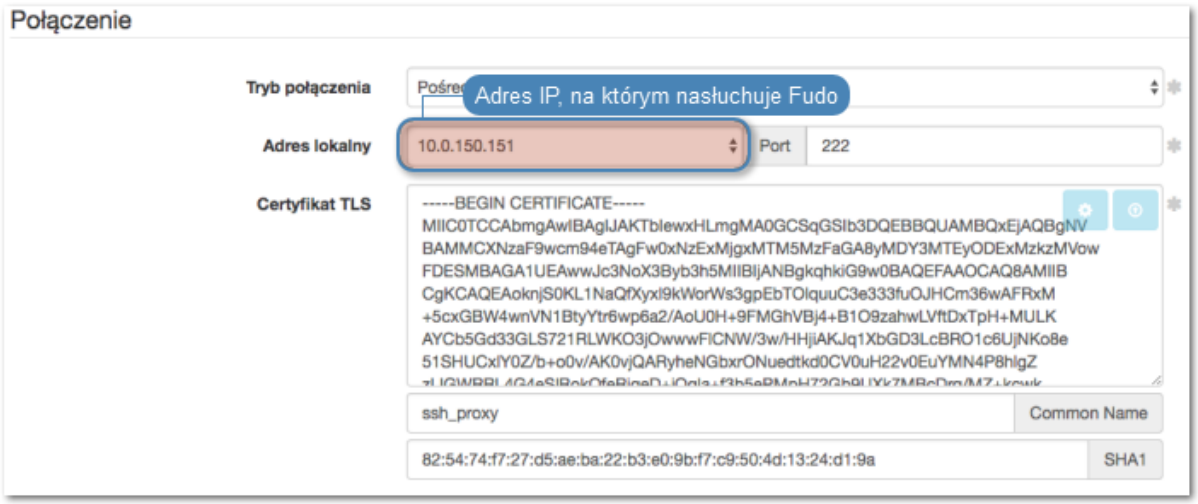
ROZDZIAŁ 26

Aplikacje klienckie

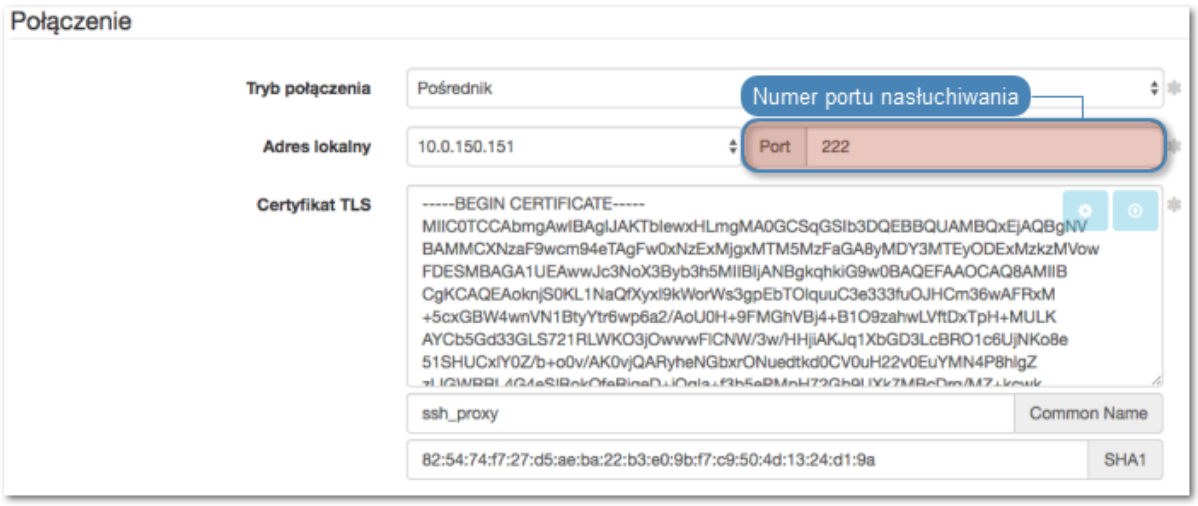
26.1 PuTTY

Połączenie *SSH* z serwerem monitorowanym poprzez gniazdo nasłuchiwania w trybie *proxy*.

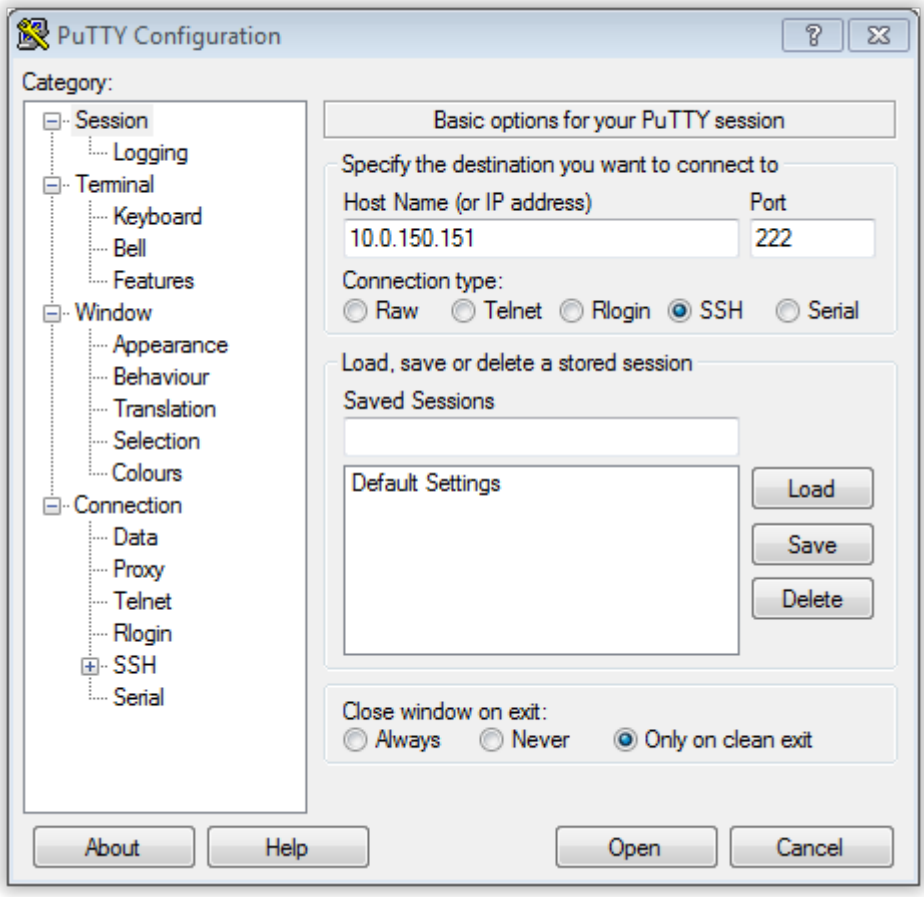
1. Pobierz i uruchom PuTTY.
2. W polu *Host Name (or IP address)* wprowadź adres IP zdefiniowany w sekcji *Połączenie*, w parametrze *Adres lokalny* gniazda nasłuchiwania.



3. Wprowadź numer portu zgodnie z definicją w obiekcie.

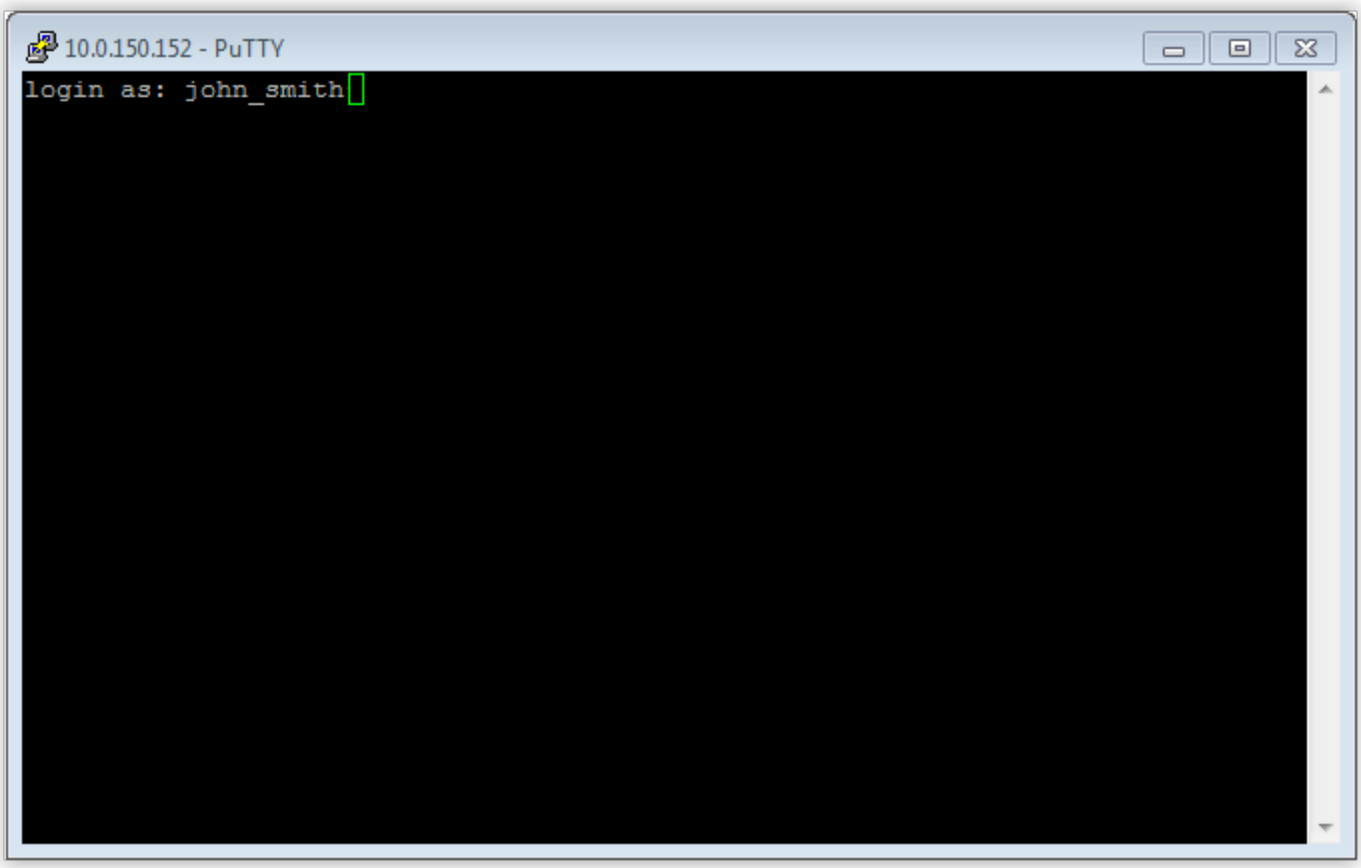


4. W polu wyboru typu połączenia (*Connection type*), wybierz `SSH`.



5. Kliknij *Open*.

6. Wprowadź nazwę użytkownika wraz z nazwą konta, na serwerze docelowym.



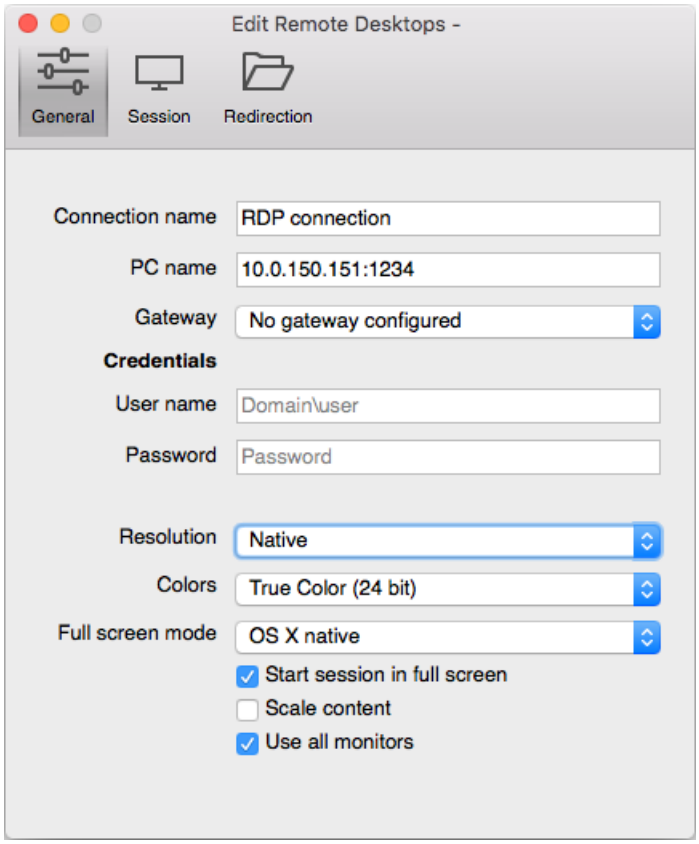
6. Wprowadź hasło użytkownika.

Tematy pokrewne:

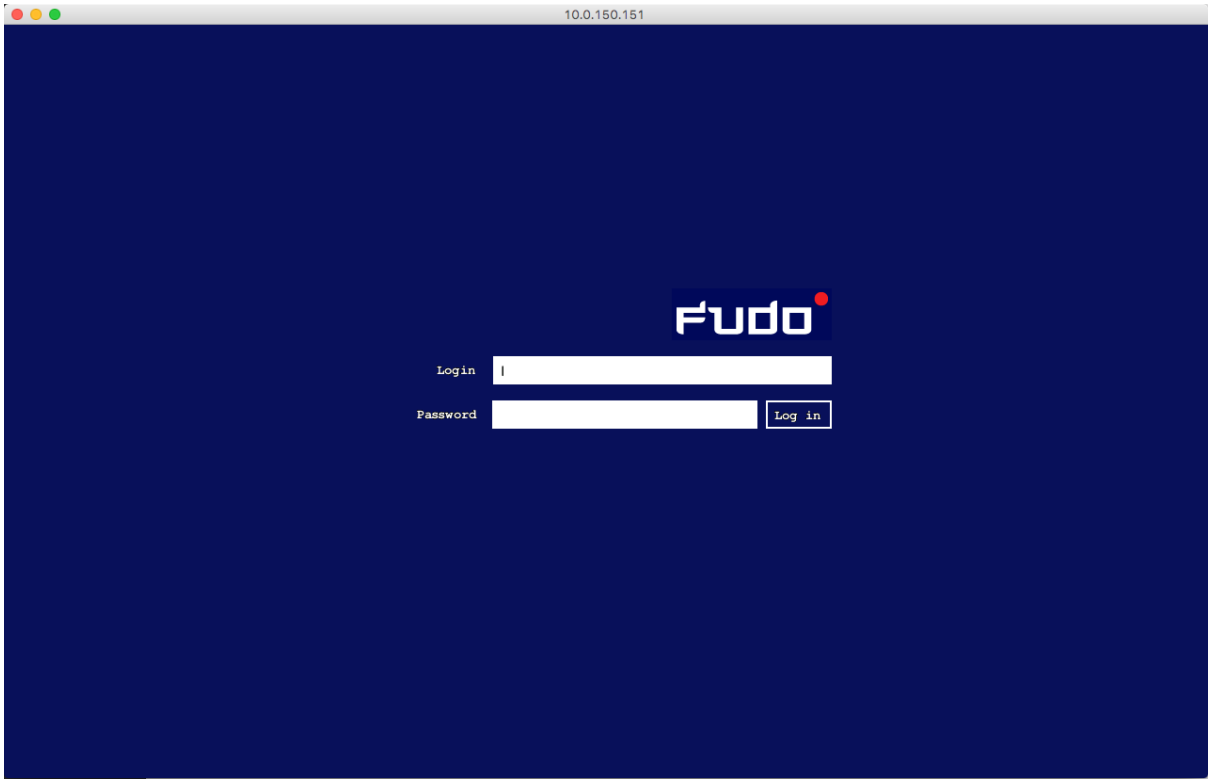
- *SSH*

26.2 Microsoft Remote Desktop

1. Uruchom klienta połączeń RDP.
2. W polu *PC name*, wprowadź adres IP oraz numer portu zdefiniowany w gnieździe nasłuchiwania.

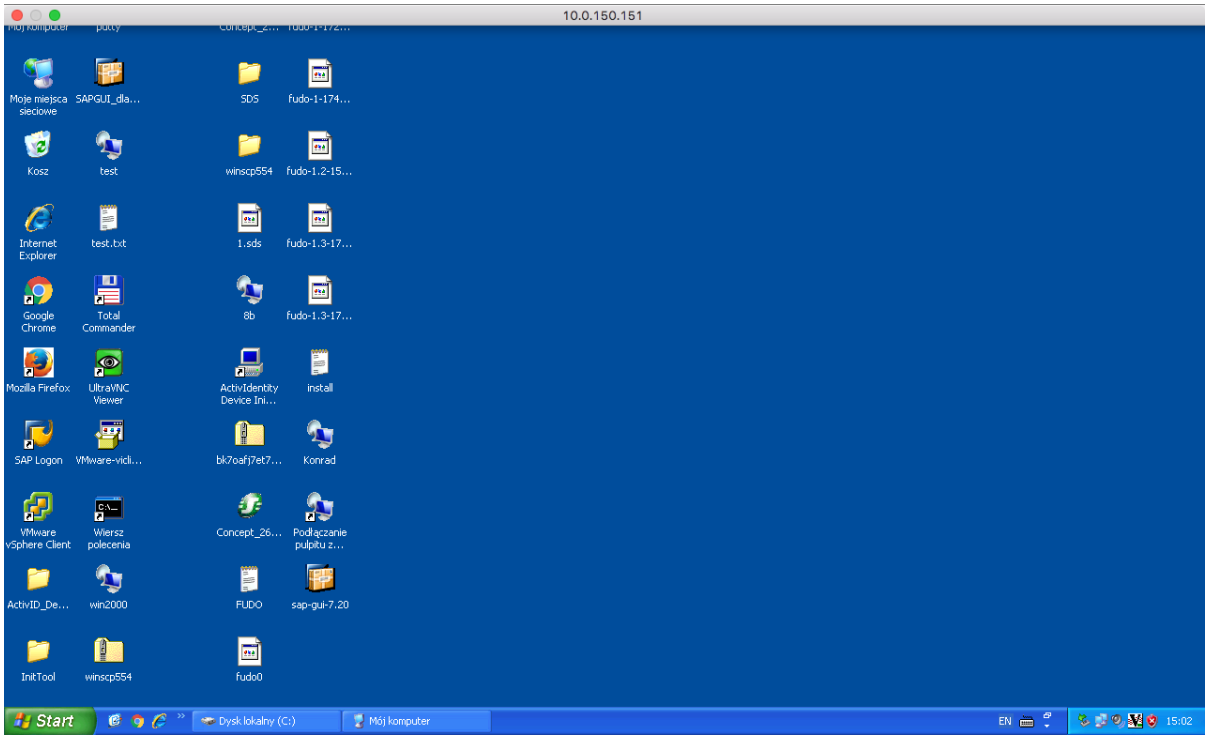


3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter].



Informacja: Fudo Enterprise pozwala na zastosowanie własnych ekranów logowania, braku dostępu i zakończenia sesji dla połączeń RDP i VNC. Więcej informacji na temat konfigurowania

własnych ekranów dla połączeń graficznych, znajdziesz w sekcji *Zasoby*.

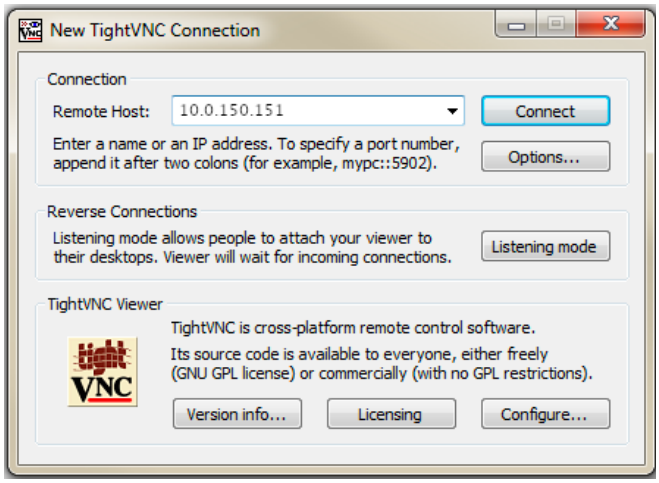


Tematy pokrewne:

- *RDP*

26.3 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*).



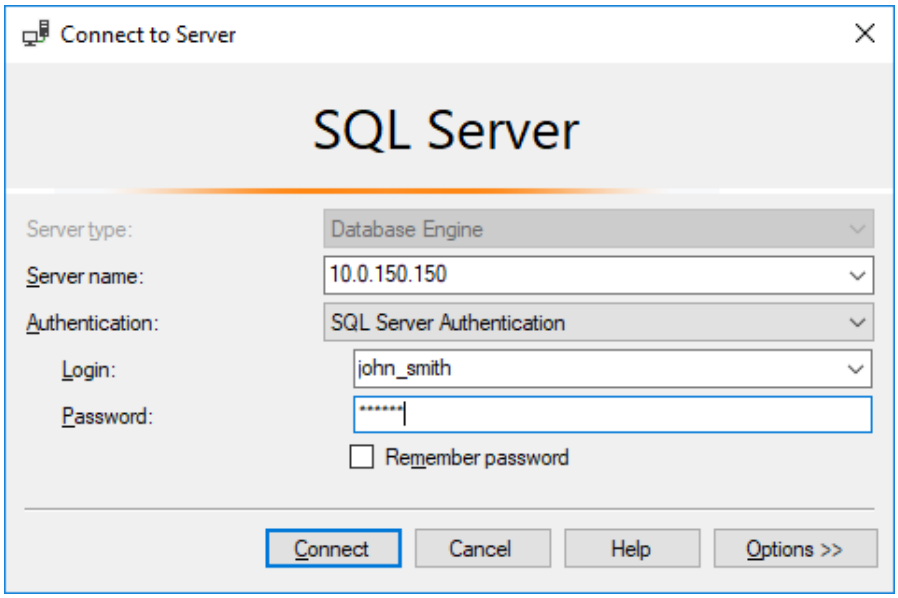
2. Wprowadź nazwę użytkownika, hasło i zatwierdź klawiszem enter.

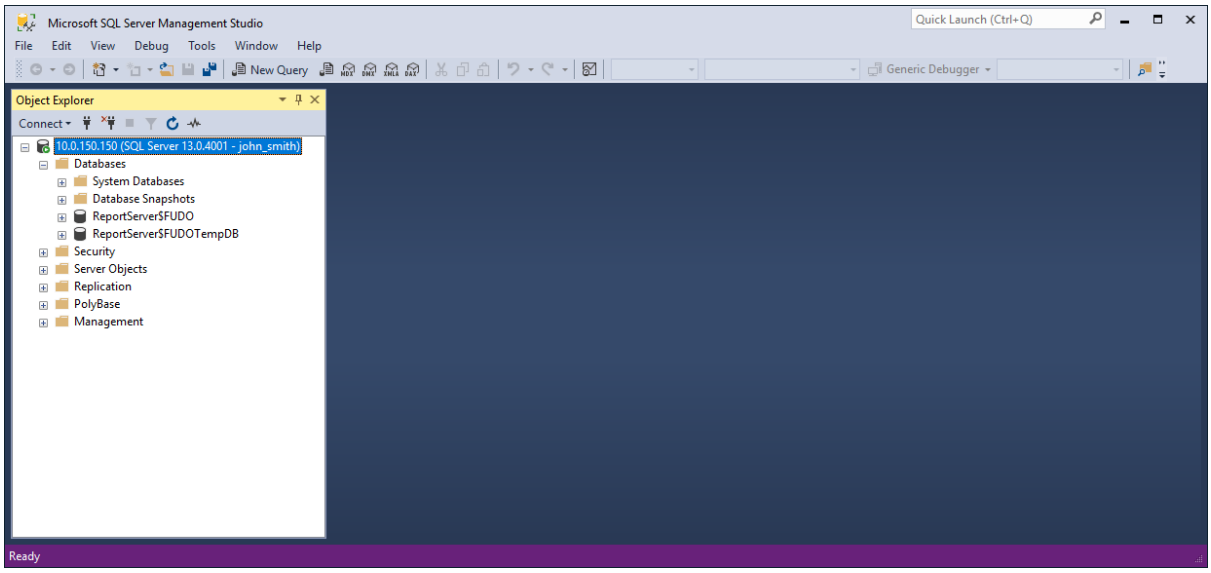
Tematy pokrewne:

- *Szybki start*

26.4 SQL Server Management Studio

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





Tematy pokrewne:

- *MS SQL*

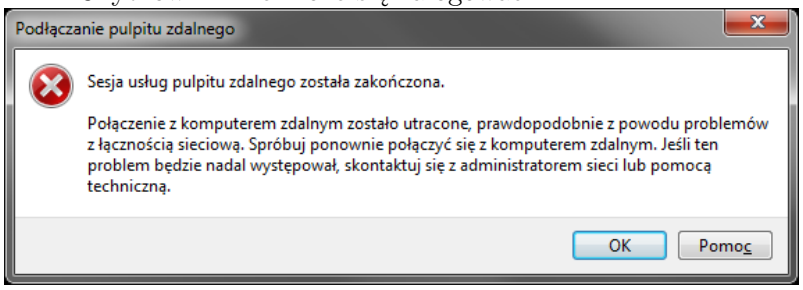
ROZDZIAŁ 27

Rozwiązywanie problemów

27.1 Uruchamianie Fudo Enterprise

Problem	Objawy i opis rozwiązania
Fudo Enterprise nie uruchamia się	• Sprawdź czy oba zasilacze są podłączone do instalacji elektrycznej 230V. Brak odpowiedniego podłączenia komunikowany jest sygnałem dźwiękowym. • Upewnij się czy podłączony został klucz szyfrujący. Brak klucza komunikowany jest sygnałem dźwiękowym. • W przypadku gdy problem wynika z nieudanej próby aktualizacji systemu, odczekaj kilka minut, podczas których urządzenie wykryje problem i uruchomi się ponownie przywracając poprzednią wersję systemu.

27.2 Połączenia z serwerami

Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem	**Objawy:** • Użytkownik nie może się zalogować.  • Wpis w dzienniku zdarzeń: *Authentication failed: Invalid username kowalski or password.*
	Rozwiązanie: • Sprawdź czy definicja użytkownika istnieje w systemie Fudo 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
	Objawy: Komunikat klienta: *Cannot establish new connection because the capacity of the filesystem has been reached.*
	Przyczyna: Zajętość przestrzeni przechowywania przekroczyła 90%.
	Rozwiązanie: Zwolnij miejsce na dane usuwając archiwalne sesje. Więcej informacji znajdziesz w rozdziale *Usuwanie sesji*.

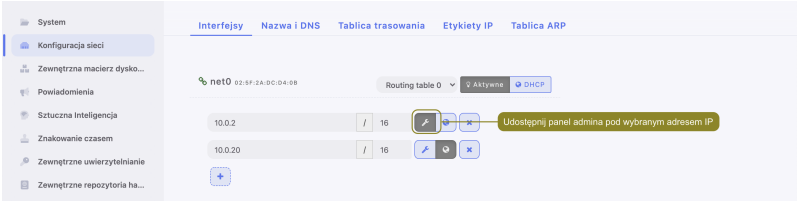
Problem	Objawy i opis rozwiązania
Przy próbie logowania nie wszyscy użytkownicy widzą ekran logowania Fudo Enterprise (standardowy, z szarym tłem).	**Przyczyna:** • Zapisane poświadczenia w skrócie RDP skutkują ukryciem ekranu Fudo Enterprise i bezpośrednim zalogowaniem do serwera docelowego. • Zapisane 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.
	Objawy: • Komunikat klienta: *Connection closed by remote host.* • Wpis w dzienniku zdarzeń: *Failed to authenticate against the server as user root using password.*
	Przyczyna: niepoprawne dane logowania do serwera docelowego.
	Rozwiązanie: zmień dane logowania w konfiguracji obiektu serwera.
	Objawy: • Komunikat klienta RDP: *Connection refused.* • Komunikat klienta SSH: *ssh: connect to host 10.0.1.111 port 10011: Connection refused*
	Przyczyna: serwer jest zablokowany.
	Rozwiązanie: odblokuj serwer w panelu administracyjnym Fudo Enterprise.

Problem	Objawy i opis rozwiązania
Połączenie jest zrywane	**Objawy:** • Użytkownik próbuje się połączyć z serwerem przez Fudo Enterprise, po wpisaniu nazwy użytkownika i hasła sesja od razu się zrywa. • Komunikat w dzienniku zdarzeń: *TLS certificate verification failed.*
	Rozwiązanie:
	Pobierz nowy certyfikat serwera docelowego w sekcji *Host docelowy.*
	
	Objawy: • Po wpisaniu nazwy użytkownika i hasła następuje zerwanie połączenia. • Wpis w dzienniku zdarzeń: *RDP connection error.*
	Rozwiązanie: sprawdź czy w zakładce *General* we właściwościach TCP-Rdp, opcja *Encryption level* nie jest ustawiona na *FIPS Compliant.*
Brak połączenia z serwerem	**Objawy:** • Nie można zalogować się do serwera, komunikat *User user0 not allowed to connect to server.* • w dzienniku zdarzeń wpis: *Authentication failed: User user0 not allowed to connect to server.*
	Przyczyna: użytkownik nie jest dodany do połączenia.
	Rozwiązanie: dodaj użytkownika do odpowiedniego obiektu połączenia.

Problem	Objawy i opis rozwiązania
	Objawy: • Po wpisaniu nazwy użytkownika i hasła następuje jakby zamrożenie ekranu logowania. • Wpis w dzienniku zdarzeń *Terminating session: User user0 (id=8483885321111147010) is blocked.*
	Przyczyna: użytkownik jest zablokowany w Fudo Enterprise.
	Rozwiązanie: odblokuj użytkownika.
Użytkownik musi logować się dwukrotnie	**Objawy:** użytkownik łącząc się poprzez protokół RDP wpisuje login i hasło po czym po chwili jest proszony o ponowne wprowadzenie danych autoryzujących.
	Przyczyna: serwer stanowi część infrastruktury zarządzanej przez broker połączeń, który wykrył istniejącą aktywną sesję użytkownika na innym serwerze.
	Objawy: użytkownik nawiązując połączenie SSH wprowadza dane logowania po czym ponownie proszony jest o ich podanie.
	Przyczyna: w obiekcie *połączenie* włączone są opcje zastępowania loginu i hasła, ale te pola ich definicji pozostawione są puste, co skutkuje podwójnym uwierzytelnieniem - w pierwszej kolejności przed Fudo, w drugiej przed serwerem docelowym.
Nie można nawiązać połączenia z serwerem RDP	**Objawy:** • użytkownik nawiązując połączenie RDP zostaje rozłączony chwilę po uwierzytelnieniu. • w dzienniku zdarzeń wpis: *RDP server 10.0.0.:33890 has to listen on the default RDP port in order to redirect sessions.*
	Przyczyna: serwer docelowy, na który następuje przekierowanie, nie nasłuchuje na porcie 3389.
	Rozwiązanie: skonfiguruj serwer docelowy tak, by oczekiwał na połączenia użytkowników na porcie 3389.
	Objawy: • w dzienniku zdarzeń wpis: *User user0 has no access to host 192.168.0.1:3389*
	Przyczyna: broker stwierdza, że użytkownik ma aktywną sesję na innym serwerze i inicjuje przekierowanie, ale docelowy serwer nie jest skonfigurowany na Fudo Enterprise lub użytkownik nie jest uprawniony do nawiązywania połączeń z wybranym zasobem.
	Rozwiązanie: • Upewnij się, że obiekt serwera jest dodany do Fudo. • Dodaj użytkownika do odpowiedniego *sejfu*.

Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem Telnet5250 poprzez aplikację PC5250 w wersji 20091005 S oraz 20111019 S	**Objawy:** próba nawiązania połączenia kończy się niepowodzeniem.
	Przyczyna: w przypadku wymienionych wersji aplikacji klienckiej, konieczne jest skonfigurowanie ruchu TCP na portach 449, 8470 i 8476, celem poprawnego zestawienia połączenia.
	Rozwiązanie: • Dodaj serwer Telnet TN5250, z domyślnym numerem portu, tj. 23. • Dodaj trzy obiekty typu serwer o protokole *TCP* i numerach portów odpowiednio 449, 8470 i 8476. • Dodaj gniazdo nasłuchiwania *TN5250*, w trybie *Pośrednik*, z domyślnym numerem portu. • Dodaj trzy gniazda nasłuchiwania *TCP*, w trybie *Pośrednik*, z numerami portów odpowiednio 449, 8470 i 8476. • Dodaj konto typu *regular*, określ parametry uwierzytelnienia i przypisz do głównej definicji serwera TN5250. • Dodaj trzy konta typu *anonymous* przypisując do kolejnych serwerów pomocniczych. • Dodaj sejf i przypisz konta wraz z odpowiadającymi gniazdami nasłuchiwania.

27.3 Logowanie do panelu administracyjnego

Problem	Objawi i opis rozwiązania
Nie można zalogować się do panelu administracyjnego	• Zweryfikuj czy wprowadzony adres Fudo Enterprise jest poprawny. • Ustaw adres IP Fudo Enterprise z poziomu konsoli, postępując zgodnie z instrukcją w rozdziale *Konfiguracja interfejsów sieciowych* w dokumentacji systemu Fudo Enterprise. • Upewnij się, że adres IP ma włączoną funkcję zarządzania Fudo Enterprise. 

27.4 Odtwarzanie sesji

Problem	Objawy i opis rozwiązania
Nie można odtworzyć wyeksportowanego materiału	**Przyczyna:** brak odpowiednich kodeków wideo.
	Rozwiązanie: zweryfikuj czy masz zainstalowane odpowiednie oprogramowanie.
Użytkownik administrator nie widzi sesji	**Objawy:** na liście sesji nie ma spodziewanych pozycji.
	Przyczyna: brak stosownych uprawnień.
	Rozwiązanie: nadaj użytkownikowi uprawnienia do określonego obiektu połączenia, serwera oraz użytkownika.
Nie można odtworzyć sesji w odtwarzaczu	**Objawy:** komunikat: `Nie można odnaleźć danych sesji.`
	Przyczyna: połączenie miało miejsce przy wyłączonej opcji rejestrowania sesji.
	Rozwiązanie: włącz opcję rejestrowania sesji, aby w przyszłości mieć możliwość odtworzenia materiału.

27.5 Konfiguracja klastrowa

Problem	Objawy i opis rozwiązania
Obiekty nie replikują się na drugi węzeł	**Objawy:** Obiekty utworzone na jednym węźlę, nie pojawiają się automatycznie na pozostałych węzłach klastra. **Rozwiązanie:** Skontaktuj się z działem wspracia technicznego.

27.6 Znakowanie czasem

Problem	Objawy i opis rozwiązania
Sesje nie są znakowane znacznikiem czasu	**Objawy:** • Komunikat w dzienniku zdarzeń: *Timestamping service communication error.*
	Przyczyna: brak komunikacji z serwerem usługi znakowania czasem.
	Rozwiązanie: Upewnij się, że serwer usługi znakowania czasem jest osiągalny przez system Fudo. • adres IP serwera znakowania czasem PWPW: 193.178.164.5 • adres serwera znakowania czasem KIR: http://www.ts.kir.com.pl/HttpTspServer
	Objawy: • Komunikat w dzienniku zdarzeń: *Unable to timestamp session.* • Brak ikony przy wybranej sesji.
	Przyczyna: Problem z funkcjonowaniem usługi znakowania czasem.
	Rozwiązanie: Zweryfikuj poprawność *konfiguracji usługi znakowania czasem*.

27.7 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*.

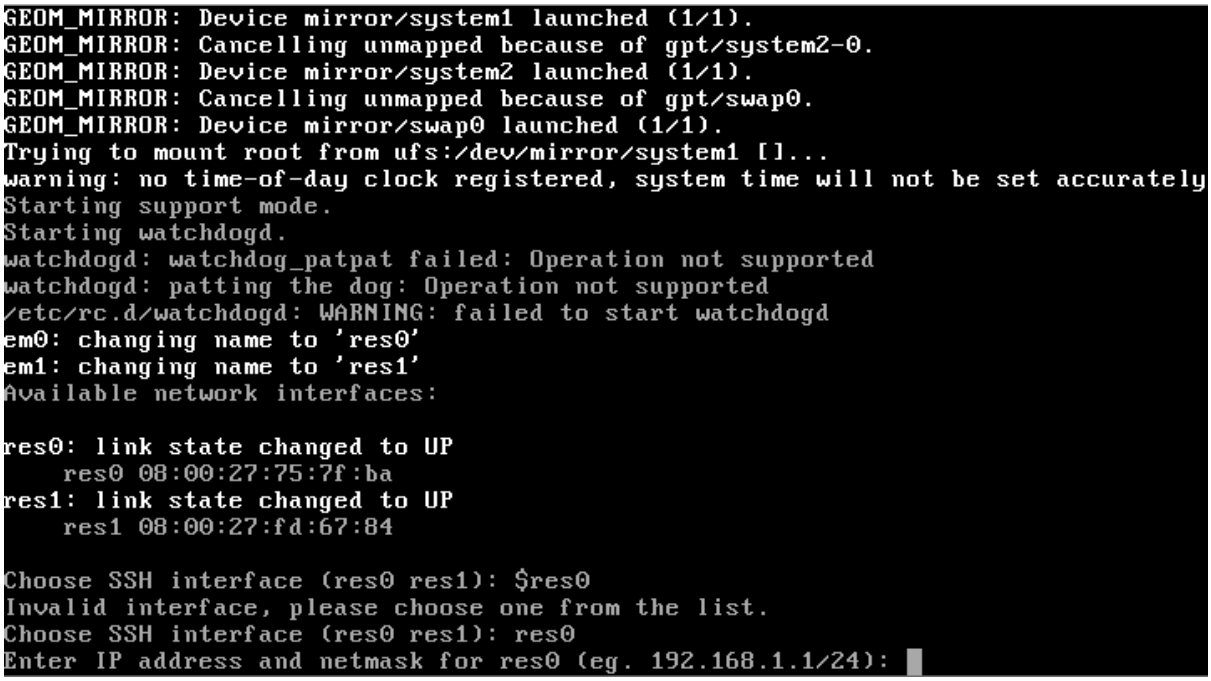
3. Wprowadź nazwę interfejsu sieciowego.

Informacja: W trybie serwisowym, nazwy interfejsów sieciowych przyjmują nazwę `res*`.

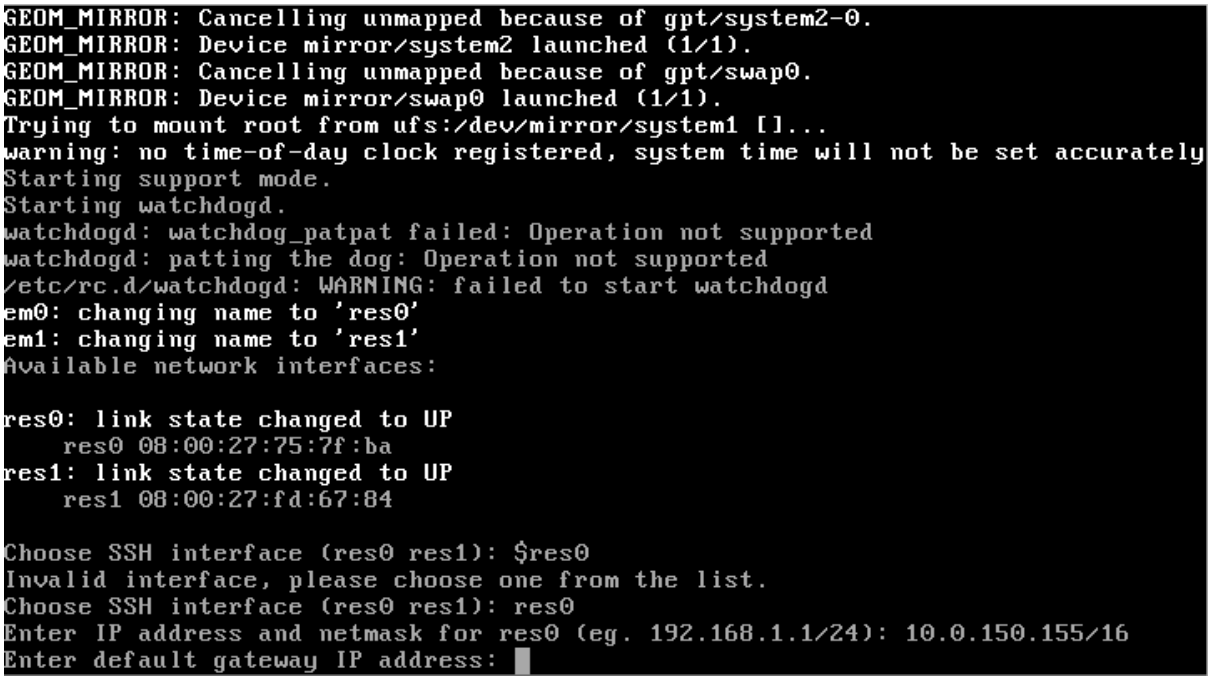
```
GEOM_MIRROR: Cancelling unmapped because of gpt/system0-0.
GEOM_MIRROR: Device mirror/system0 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system1-0.
GEOM_MIRROR: Device mirror/system1 launched (1/1).
GEOM_MIRROR: Cancelling unmapped because of gpt/system2-0.
GEOM_MIRROR: Device 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 []...
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.



5. Wprowadź adres IP bramy i zatwierdź klawiszem `[Enter]`, aby umożliwić nawiązanie zdalnego połączenia z Fudo Enterprise.



Informacja:

- Odcisk palca pozwala na weryfikację, że połączenie zostało nawiązane z właściwym systemem.

```
warning: no time-of-day clock registered, system time will not be set accurately
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
em0: changing name to 'res0'
em1: changing name to 'res1'
Available network interfaces:

res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address: 10.0.0.1
res0: link state changed to DOWN
add net default: gateway 10.0.0.1
SSH Fingerprint: SHA256:dgu2Ec8deFWPZkIxJk6EV9loggwm+OKXERsW+2PQBSY
res0: link state changed to UP
```

6. Po zakończeniu prac serwisowych, użyj kombinacji klawiszy `[Ctrl]` + `C`, aby zerwać połączenie i zresetować interfejs sieciowy.

```
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $res0
Invalid interface, please choose one from the list.
Choose SSH interface (res0 res1): res0
Enter IP address and netmask for res0 (eg. 192.168.1.1/24): 10.0.150.155/16
Enter default gateway IP address: 10.0.0.1
res0: link state changed to DOWN
add net default: gateway 10.0.0.1
SSH Fingerprint: SHA256:dgu2Ec8deFWPZkIxJk6EV9loggwm+OKXERsW+2PQBSY
res0: link state changed to UP
^CDec 21 13:31:56 init: single user shell terminated, restarting
Starting support mode.
Starting watchdogd.
watchdogd: watchdog_patpat failed: Operation not supported
watchdogd: patting the dog: Operation not supported
/etc/rc.d/watchdogd: WARNING: failed to start watchdogd
ifconfig: ioctl SIOCSIFNAME (set name): File exists
ifconfig: ioctl SIOCSIFNAME (set name): File exists
Available network interfaces:

    res0 08:00:27:75:7f:ba
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1):
```

Tematy pokrewne:

- *Konfiguracja ustawień sieciowych*
- *Czynności serwisowe*

ROZDZIAŁ 28

Przypadki użycia

28.1 Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator

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

Informacja: Do konfiguracji dwuskładnikowego uwierzytelnienia OATH w Fudo Enterprise można również rozważyć użycie alternatywnych aplikacji, takich jak Microsoft Authenticator.

28.1.1 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

Kontynuacja na następnej stronie

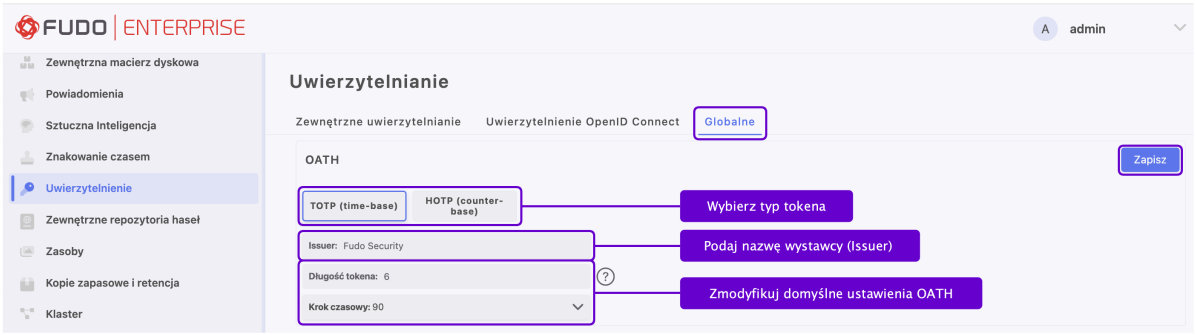
Tabela 1 – kontynuacja poprzedniej strony

Platforma / Protokół	Tryb Challenge-Response	Hasło + Wygenerowany kod
Telnet 5250	nie dostępne	dostępne
Telnet	nie dostępne	dostępne
MS SQL(TDS)	nie dostępne	nie dostępne
HTTP/S	nie dostępne	nie dostępne
TCP	nie dostępne	nie dostępne
MySQL	nie dostępne	nie dostępne
X11	nie dostępne	nie dostępne
Modbus	nie dostępne	nie dostępne

28.1.2 Konfiguracja domyślnych wartości OATH

Aby skonfigurować domyślne ustawienia dla metody uwierzytelniania OATH, postępuj zgodnie z instrukcją:

1. Wybierz *Ustawienia* > *Uwierzytelnianie* > zakładka *Globalne*.
2. Przejdź do sekcji *OATH* i wybierz typ tokena: `TOTP (czasowy)` lub `HOTP (licznikowy)`.
3. Wypełnij pole *Wydawca*.
4. Wypełnij pole *Długość tokena*.
5. Wprowadź *Krok czasu*, jeśli wybrany typ tokena to `TOTP (czasowy)`.
6. Kliknij *Zapisz* obok nazwy sekcji *OATH*.



28.1.3 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.
3. Przejdź do sekcji *Uwierzytelnianie* i wybierz typ `OATH` z listy rozwijanej *Dodaj metodę uwierzytelniania*.

4. Wybierz *Pierwszy składnik*: `Hasło` lub `Zewnętrzne uwierzytelnienie`.

Jeśli zostało wybrane `Hasło`:

- 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.

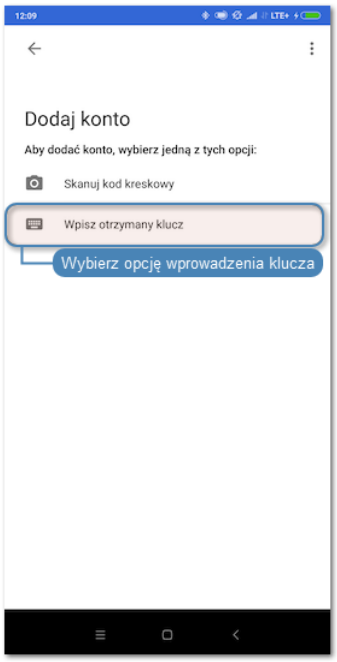
Informacja: Opcja *Zainicjowany* służy do inicjalizacji użytkownika za pomocą kodu QR. Przy podanym haśle albo wybranym źródle zewnętrznego uwierzytelnienia jako *Pierwszego składnika* części statycznej, kod QR wyświetla się użytkownikowi podczas jego pierwszego połączenia. W przypadku pomyślnego pierwszego uwierzytelnienia, opcja Zainicjowany jest zaznaczana i nabywa stanu nieedytowalnego.

---

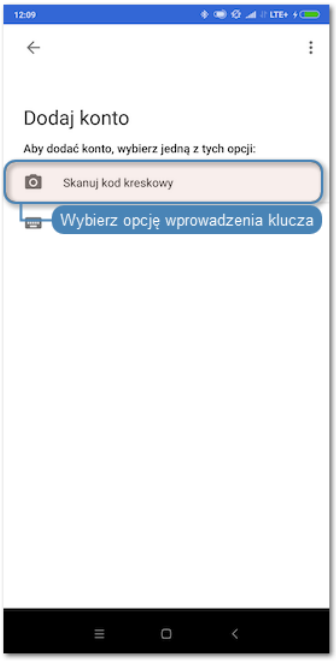
5. Kliknij *Zapisz.*
6. Uruchom aplikację *Google Authenticator* i dodaj konto ręcznie lub skanując kod QR.

Ręczne wprowadzenie danych	Kod QR

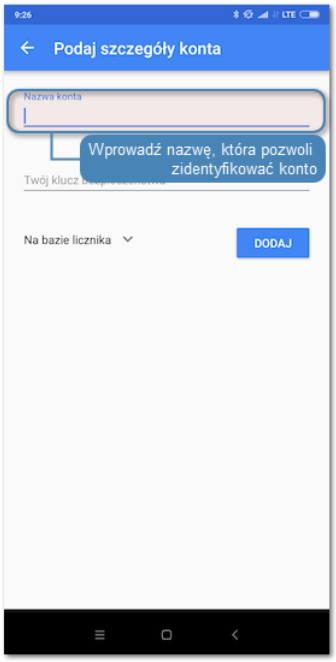
- Na ekranie dodawania konta, wybierz *Wpisz otrzymany klucz*.



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

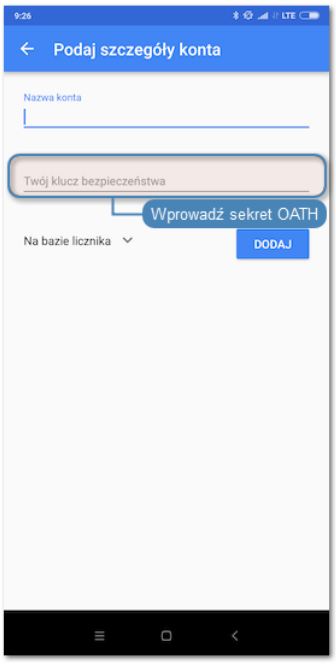
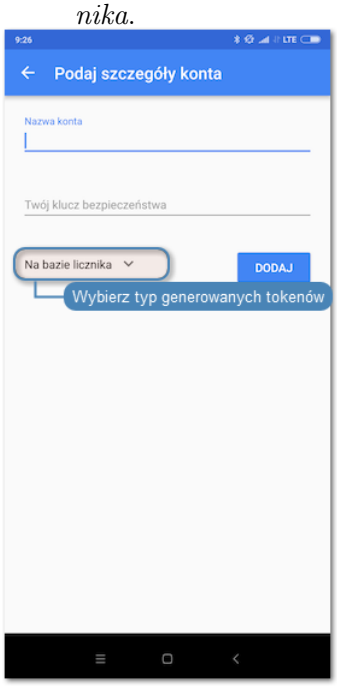


- Nadaj nazwę konta.



Kontynuacja na następnej stronie

Tabela 2 – kontynuacja poprzedniej strony

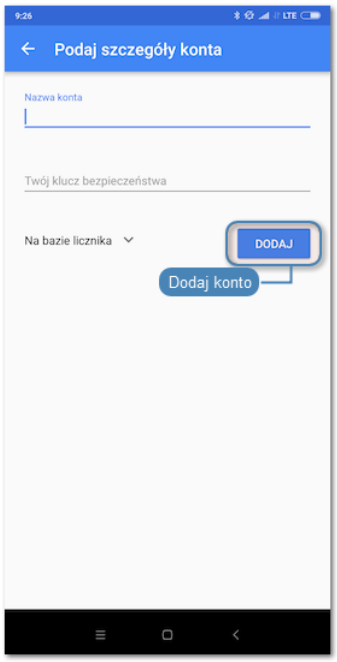
Ręczne wprowadzenie danych	Kod QR
• W polu *Twój klucz bezpieczeństwa*, wprowadź sekret z formularza konfiguracji metody uwierzytelnienia OATH. 	
• Z listy rozwijalnej wybierz *Na bazie licznika*. 	

Kontynuacja na następnej stronie

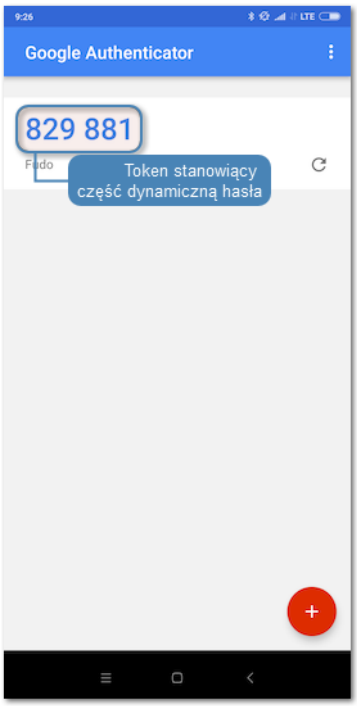
Tabela 2 – kontynuacja poprzedniej strony

Ręczne wprowadzenie danych	Kod QR

- Wybierz DODAJ.



7. W procesie uwierzytelnienia, ciąg hasła składa się ze statycznego hasła zdefiniowanego w metodzie uwierzytelniania i dynamicznej części wygenerowanej przez, np. `password829881`.



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*

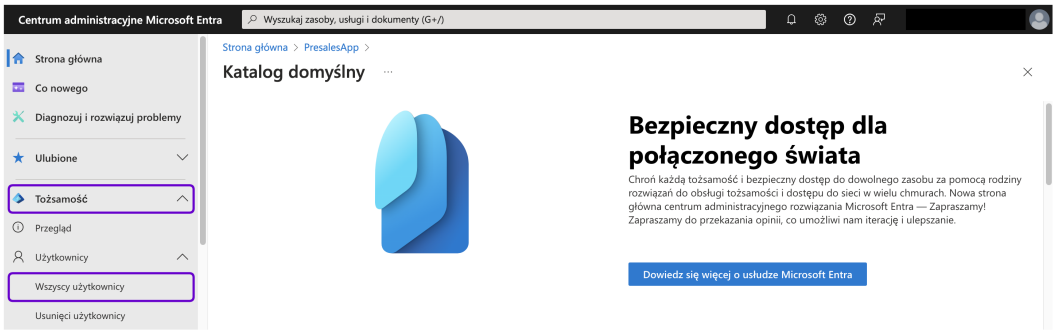
28.2 Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)

Aby skonfigurować metodę uwierzytelnienia OpenID Connect z Microsoft Entra, postępuj zgodnie z poniższymi krokami.

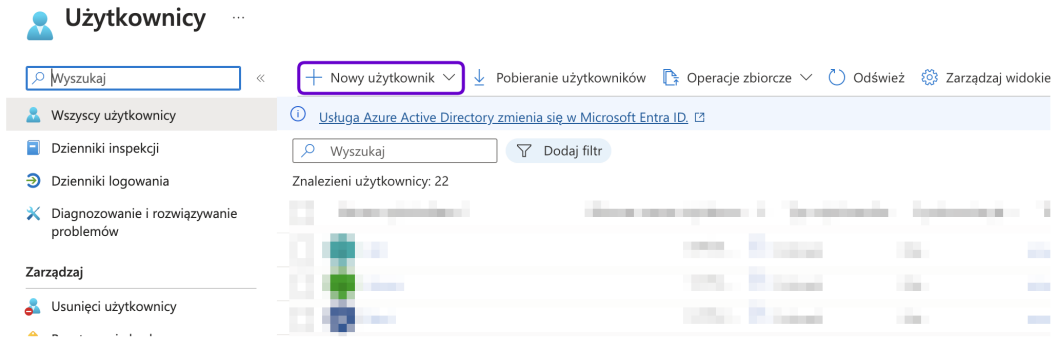
Informacja: Jest to ogólna instrukcja, mająca na celu przybliżenie procesu konfigurowania metody uwierzytelnienia OpenID Connect w Fudo Enterprise. Niektóre szczegóły mogą się różnić w zależności od posiadanej wersji oraz konfiguracji Microsoft Entra. Szczegółową instrukcję znajdziesz w dokumentacji Microsoft Entra.

Tworzenie użytkownika w Microsoft Entra ID:

1. Przejdź do panelu administratora Microsoft Entra i zaloguj się przy użyciu swoich danych uwierzytelniających Microsoft Entra.
2. Z lewego menu wybierz *Tożsamość* > *Użytkownicy* > *Wszyscy użytkownicy*.



3. Kliknij przycisk + *Nowy użytkownik* i z listy rozwijanej wybierz opcję *Utwórz nowego użytkownika*.



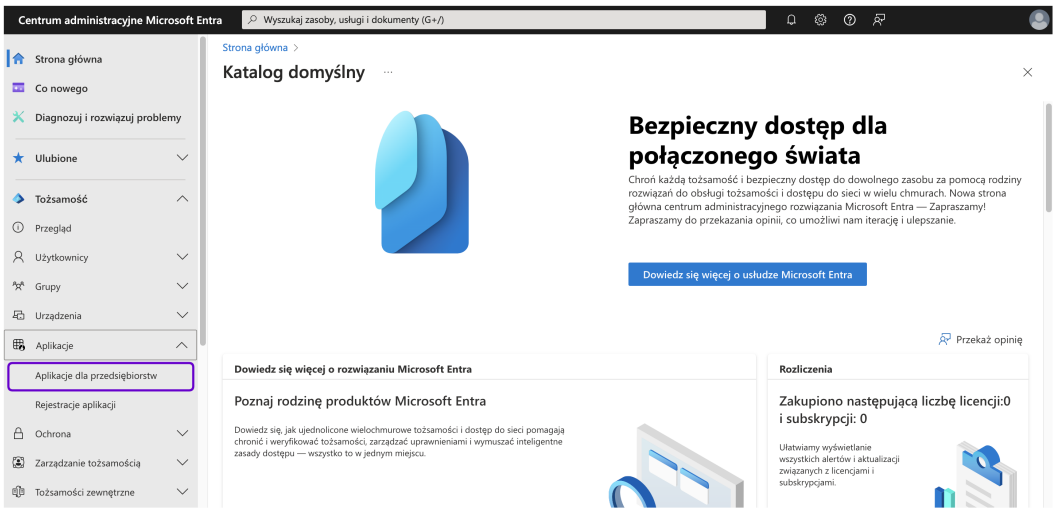
4. W polu *Nazwa główna użytkownika* wprowadź nazwę użytkownika konta. Na przykład: `user1@fudosecurity.com`.
5. W polu *Nazwa wyświetlana* podaj nazwę użytkownika konta.
6. Wprowadź hasło w polu *Hasło* lub kliknij opcję *Automatyczne generowanie hasła*, aby wygenerować hasło.
7. Wybierz opcję *Konto włączone*.
8. W zakładce *Właściwości*, w sekcji menu *Informacje kontaktowe*, w polu *E-mail* podaj adres e-mail. Na przykład: `user1@fudosecurity.com`.

9. Wprowadź pozostałe parametry wymagane dla użytkownika w zakładkach *Właściwości* i *Przypisania*.

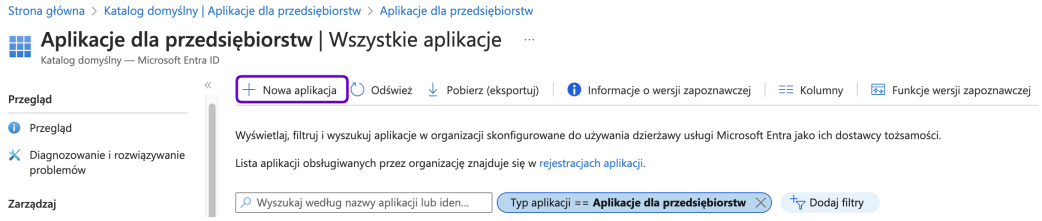
10. Kliknij *Utwórz*.

Rejestracja Fudo w Microsoft Entra ID:

1. Z lewego menu wybierz *Tożsamość* > *Aplikacje* > *Aplikacje dla przedsiębiorstw*.



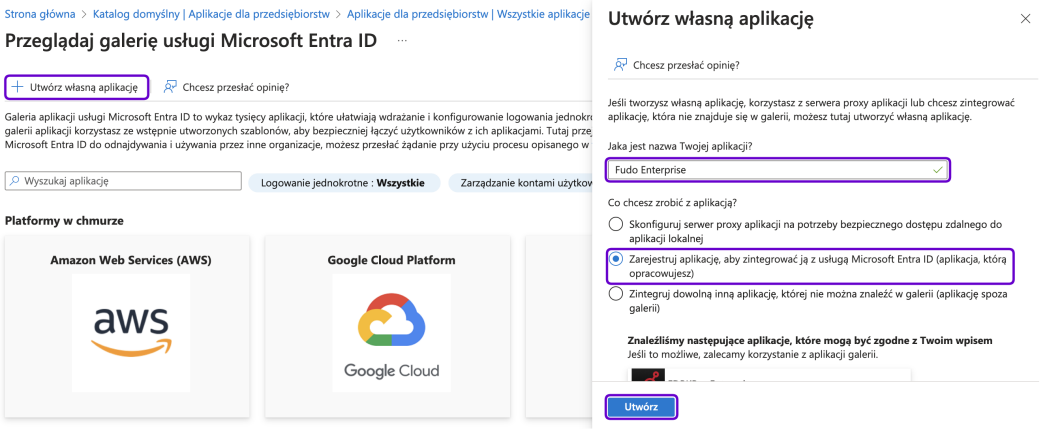
2. Kliknij przycisk + *Nowa aplikacja*, aby utworzyć nową aplikację.



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*.

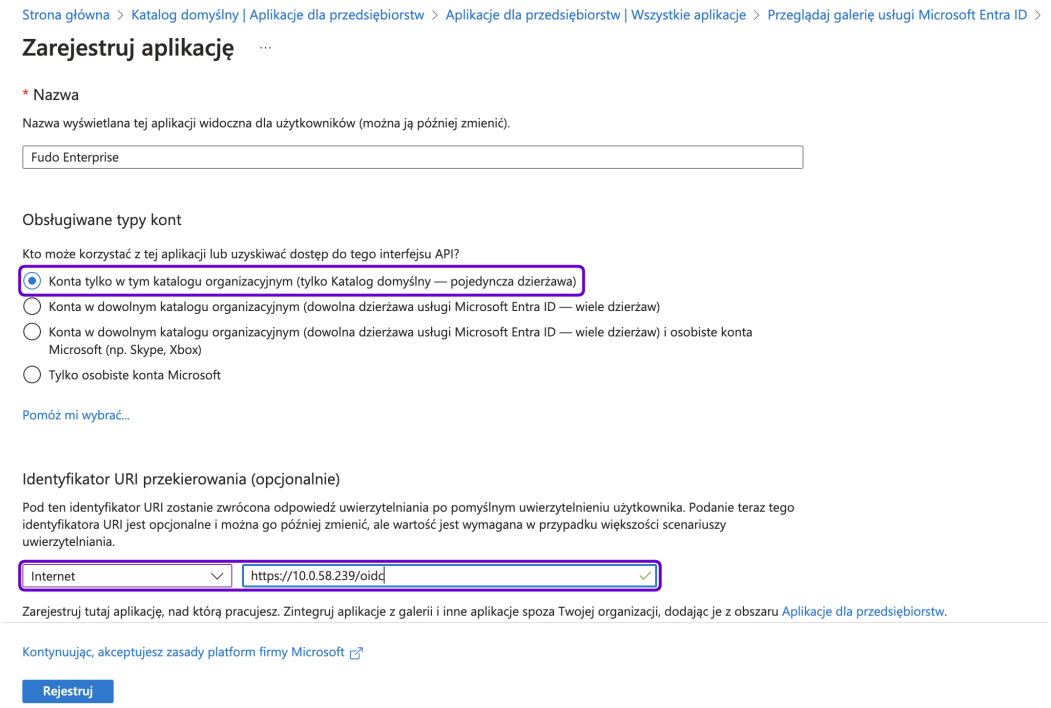


6. Na kolejnej stronie, w sekcji menu *Obsługiwane typy kont*, wybierz opcję *Konta*

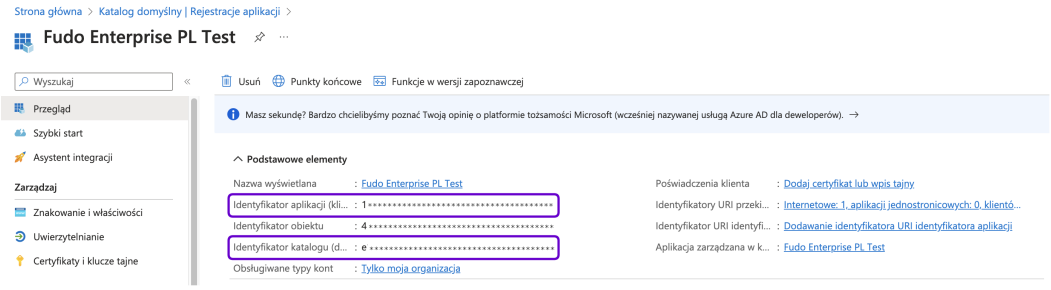
tylko w tym katalogu organizacyjnym (tylko Katalog domyślny — pojedyncza dzierżawa).

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*.

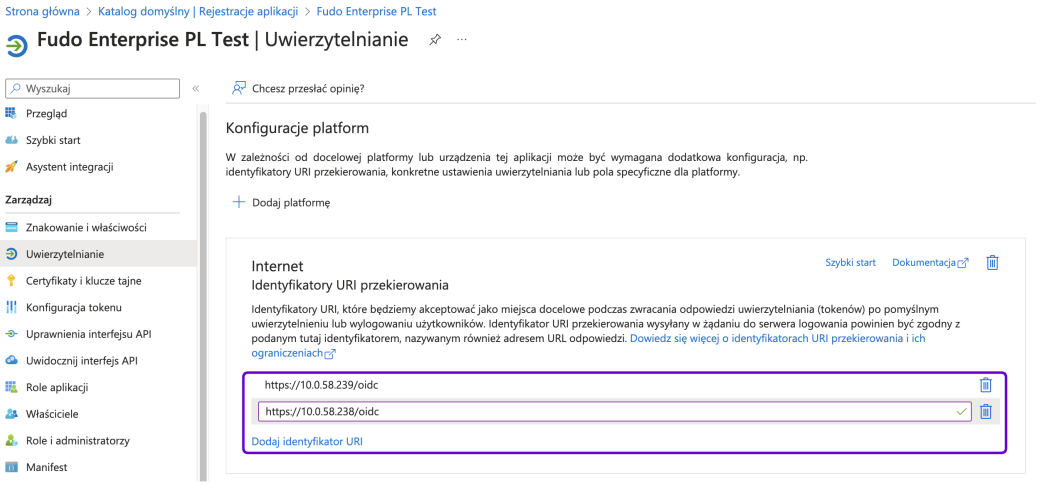


8. Kliknij *Rejestruj*, aby utworzyć aplikację.
9. Z lewego menu wybierz *Tożsamość* > *Aplikacje* > *Rejestracje aplikacji*.
10. Przejdź do zakładki *Wszystkie aplikacje*, znajdź utworzoną aplikację na liście aplikacji i kliknij na nazwę, aby edytować jej parametry. Zapisz *Identyfikator aplikacji (klienta)* i *Identyfikator katalogu (dzierżawcy)*, ponieważ będziesz ich potrzebować na późniejszym etapie konfiguracji.

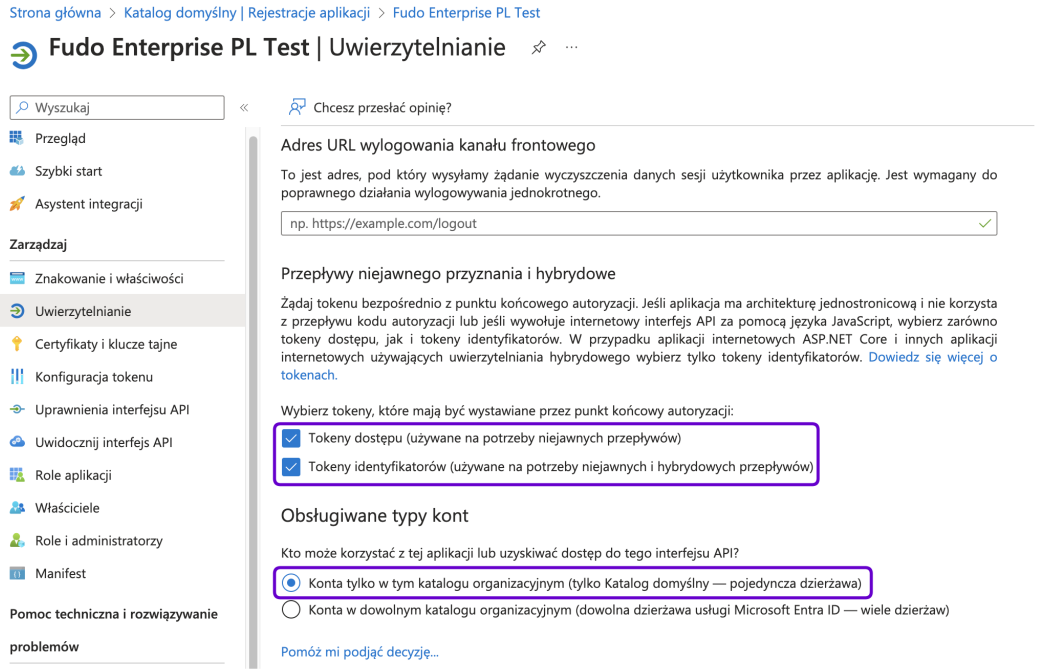


Konfiguracja ustawień uwierzytelnienia:

1. Wróć do głównego menu *Microsoft Entra ID* i z sekcji menu *Zarządzaj* wybierz *Rejestracje aplikacji*.
2. Znajdź utworzoną aplikację na liście aplikacji i kliknij na nazwę, aby edytować jej parametry.
3. W sekcji menu *Zarządzaj* wybierz *Uwierzytelnianie*.
4. 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`.



5. W sekcji menu *Przepływy niejawnego przyznania i hybrydowe* zaznacz opcje *Tokeny dostępu* i *Tokeny identyfikatorów*.



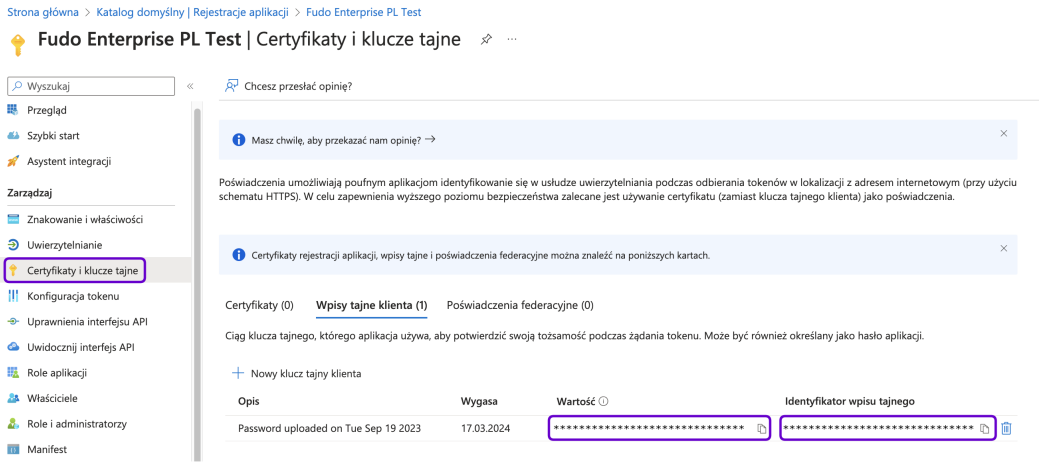
6. W sekcji menu *Blokada właściwości wystąpienia aplikacji* kliknij *Konfiguruj* i w prawym oknie dialogowym wyłącz opcję *Włącz blokadę właściwości*. Kliknij *Zapisz*, aby zamknąć okno dialogowe.

7. Kliknij *Zapisz*, aby zapisać ustawienia uwierzytelnienia.

Generowanie sekretu klienta:

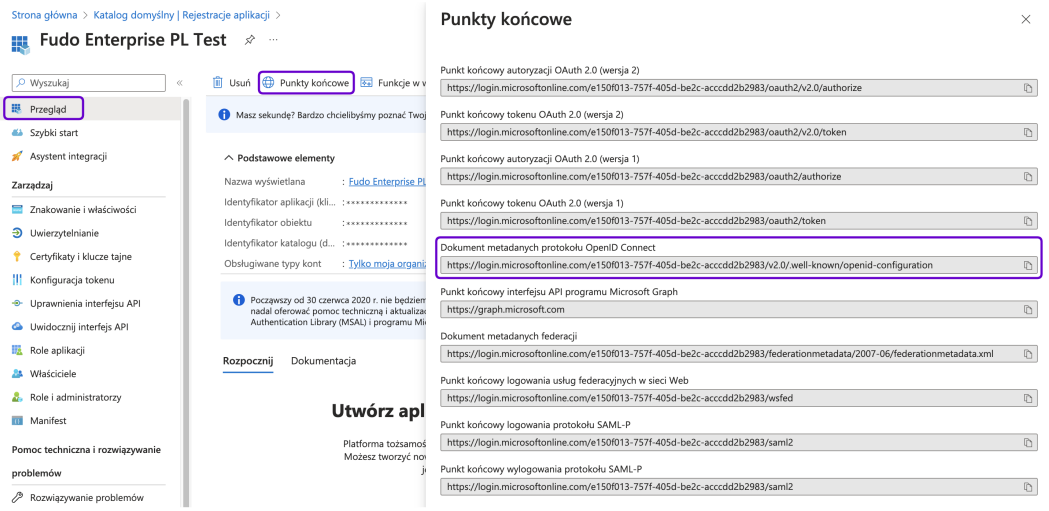
1. W ustawieniach aplikacji na portalu Azure przejdź do sekcji *Certyfikaty i klucze tajne*.
2. W zakładce *Wpisy tajne klienta* wybierz *+ Nowy klucz tajny klienta*.
3. Podaj opis, wybierz pożądany okres ważności i kliknij *Dodaj*.

Ostrzeżenie: Zapisz *Identyfikator wpisu tajnego* oraz *Wartość* wygenerowanego sekretu, ponieważ będziesz ich potrzebować do konfiguracji Fudo Enterprise. Po zapisaniu wartość sekretu nie będzie widoczna.



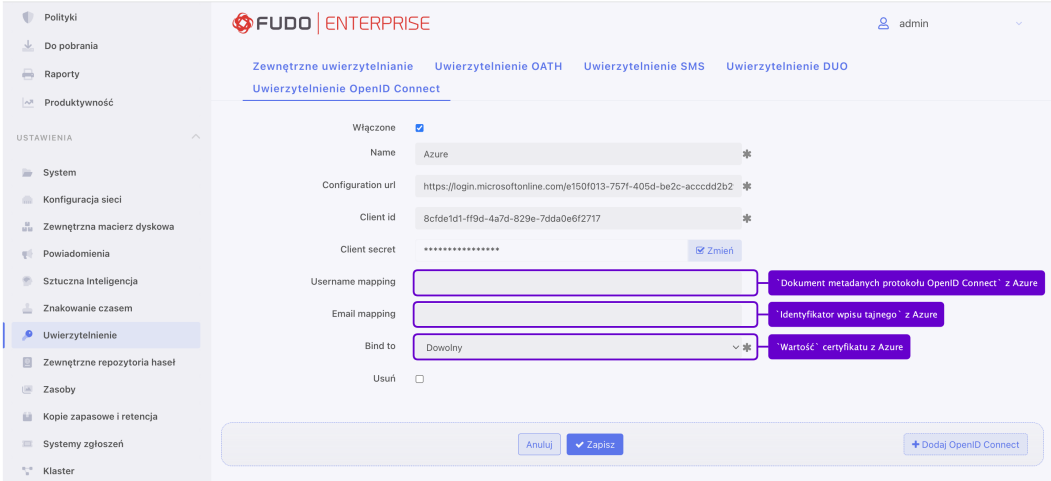
Pobieranie adresu URL konfiguracji OpenID Connect:

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.



Konfiguracja metody uwierzytelniania OpenID Connect w Fudo:

1. Przejdź do Panelu Administracyjnego Fudo Enterprise.
2. Wybierz *Ustawienia* > *Uwierzytelnienie*.
3. Wybierz zakładkę **Uwierzytelnienie OpenID Connect**.
4. Kliknij *Dodaj uwierzytelnienie OpenID Connect*.
5. Zaznacz opcję *Włączone*, aby włączyć globalnie uwierzytelnienie przy użyciu OpenID Connect.
6. Podaj nazwę (np. *Azure*).
7. Ustaw *Adres źródłowy* na *Dowolny*.
8. Wprowadź *URL konfiguracyjny* (*Dokument metadanych protokołu OpenID Connect* z Azure).
9. Podaj *Client ID* (*Identyfikator wpisu tajnego* z Azure).
10. Wprowadź *Client secret* (wartość certyfikatu, czyli *Wartość* z Azure).

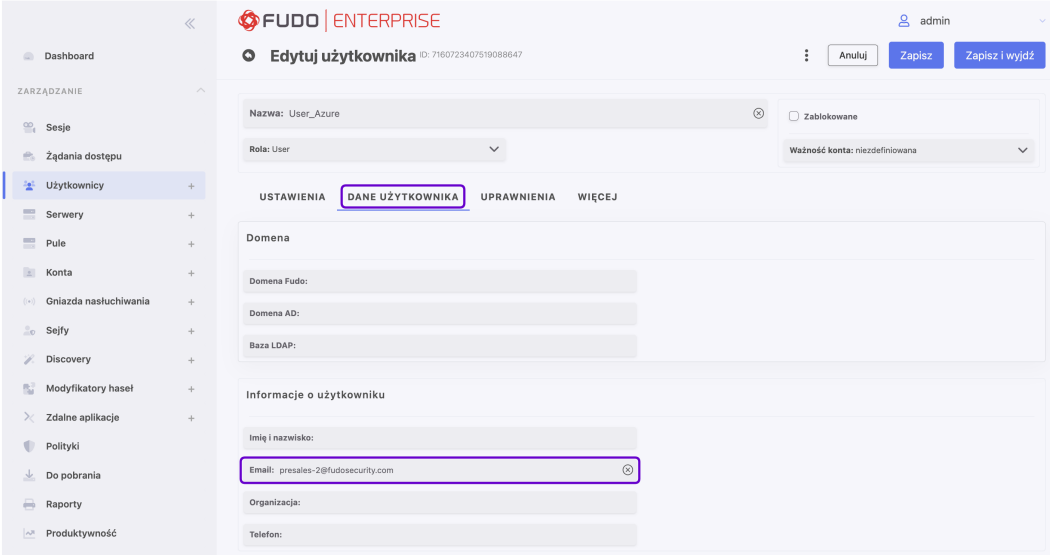


11. Dodaj *Mapowanie nazwy użytkownika* i *Mapowanie email* (opcjonalne). Te pola są przydatne, gdy nazwa użytkownika ma przyjętą inną konwencję nazewnictwa.
12. Kliknij *Zapisz*.

Informacja: Aby dowiedzieć się więcej o algorytmie używanym do określenia tożsamości użytkownika, odwiedź sekcję *Definicja uwierzytelniania OpenID Connect*.

Tworzenie użytkownika w Fudo:

1. Wybierz *Zarządzaj* > *Użytkownicy*, a następnie kliknij + *Dodaj użytkownika*.
2. Wprowadź nazwę użytkownika.
3. W zakładce *Dane użytkownika*, w sekcji menu *Informacje o użytkowniku*, w polu *Email* wprowadź adres e-mail używany podczas tworzenia użytkownika w Azure - w tym przypadku `user1@fudosecurity.com`.

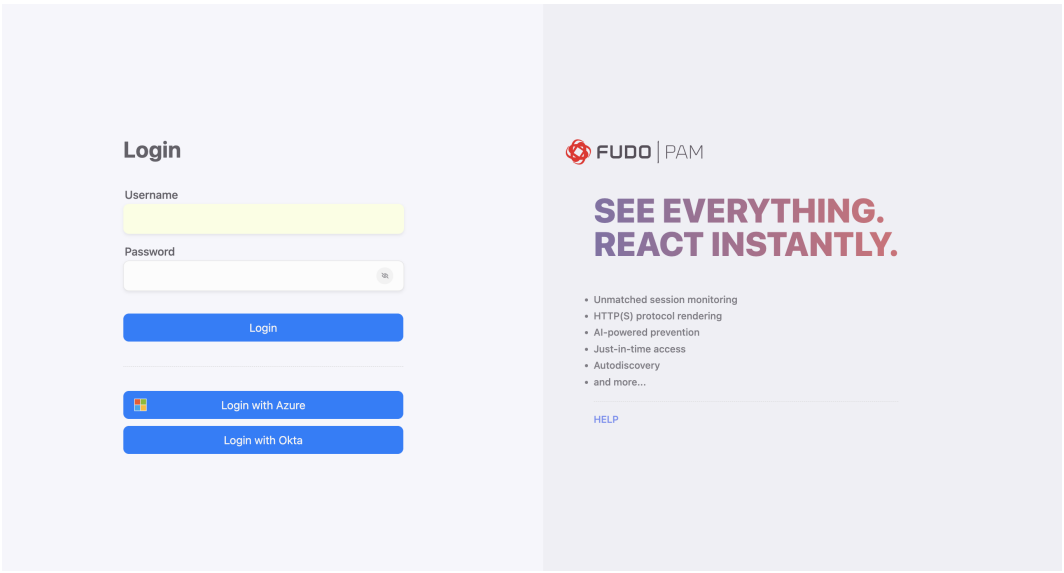


4. Wypełnij resztę parametrów zgodnie z Twoimi wymaganiami.
5. Kliknij *Zapisz*.

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*

28.3 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 domenie;
- 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.

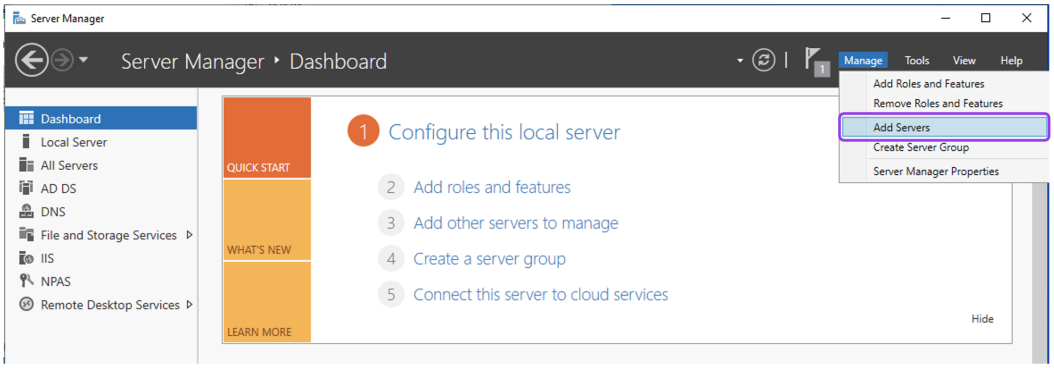
Aby skonfigurować i używać usługi Remote Desktop Services (RDS) wraz z Fudo Enterprise, postępuj zgodnie z poniższą instrukcją.

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.

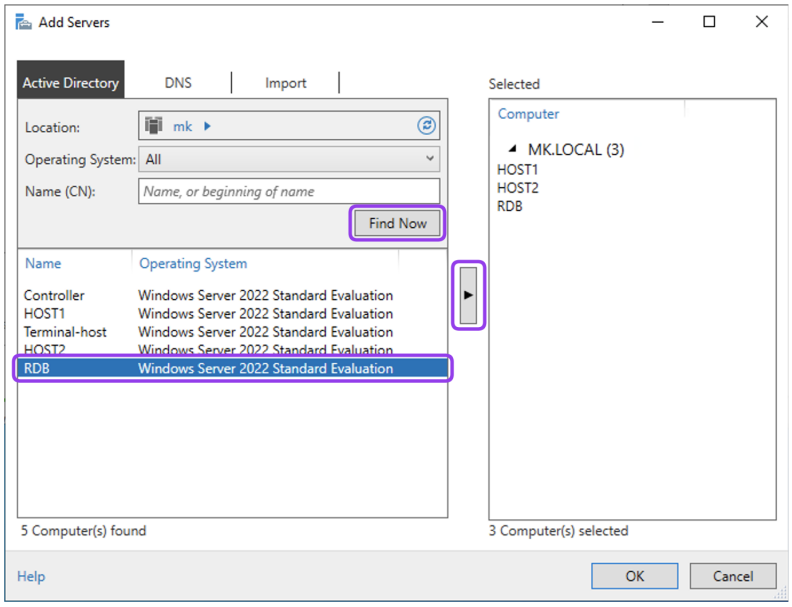
28.3.1 Konfiguracja usługi Remote Desktop Services (RDS)

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*.

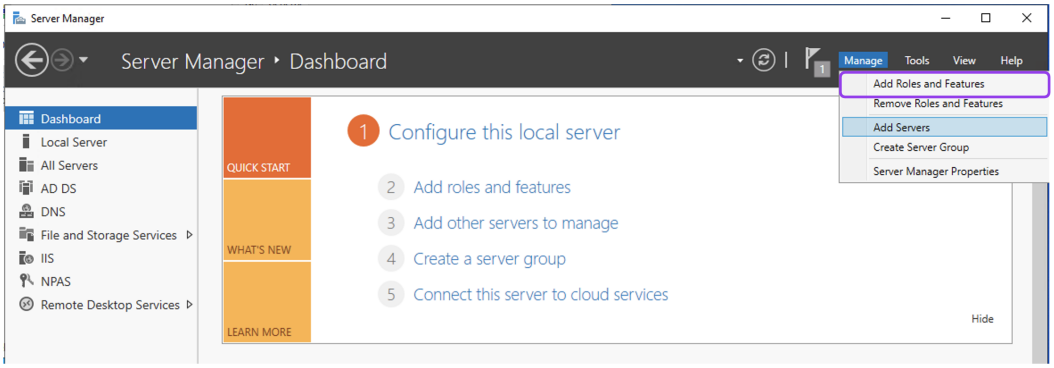


4. Kliknij *Find Now*.
5. Dodaj wszystkie serwery, które zamierzasz użyć w RDS, klikając na każdy serwer w konfiguracji. Kliknij *OK*. W tym przypadku dodajemy 3 serwery: `HOST1`, `HOST2`, i `RDB`, który będzie pełnił rolę *Brokera*.

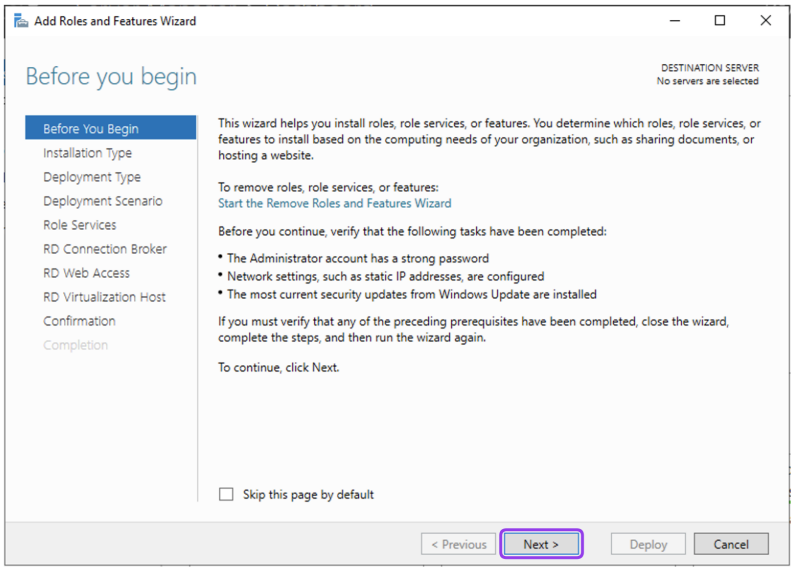


Dodaj komponenty usługi Remote Desktop Services:

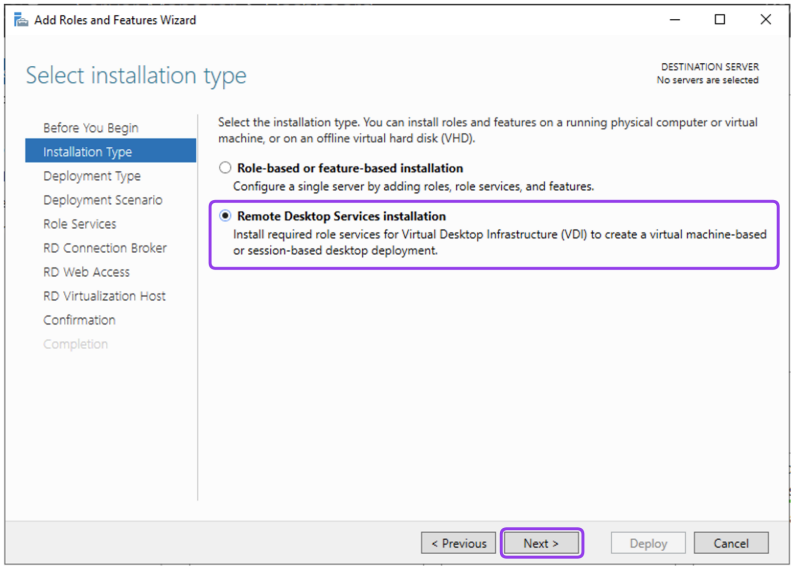
1. Kliknij przycisk *Manage* w prawym górnym rogu okna, aby rozwinięcia listę menu, a następnie wybierz *Add Roleas and Features*.



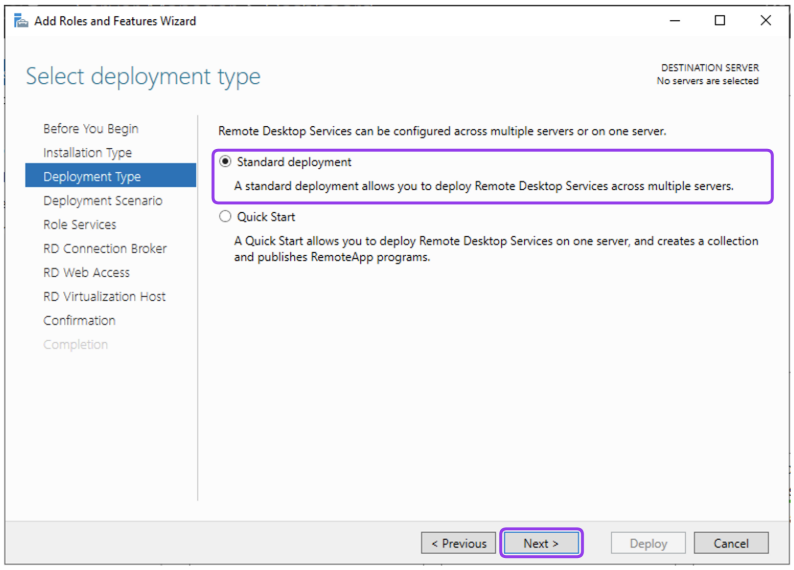
2. Na karcie *Before You Begin* kliknij *Next*, aby kontynuować.



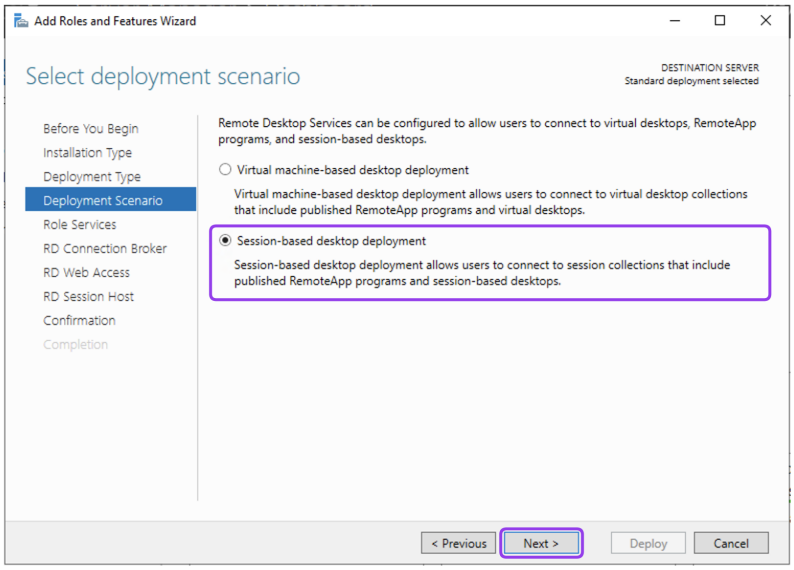
3. Na karcie *Installation Type* wybierz *Remote Desktop Services installation* i kliknij *Next*, aby kontynuować.



4. Na karcie *Deployment Type* wybierz *Standard Deployment*, aby uzyskać bardziej szczegółowe instrukcje dotyczące instalacji usługi Remote Desktop Services. Kliknij *Next*, aby kontynuować.

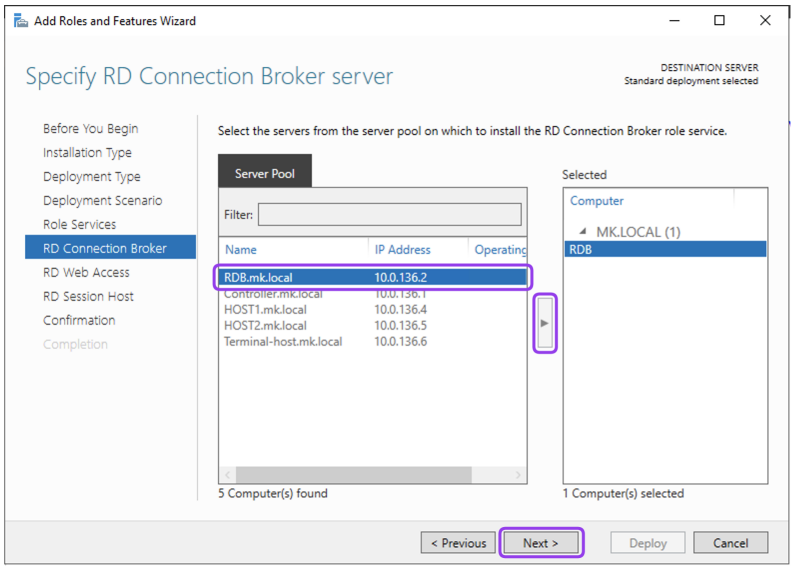


5. Na karcie *Deployment Scenario* wybierz *Session-based desktop deployment*. Kliknij *Next*, aby kontynuować.

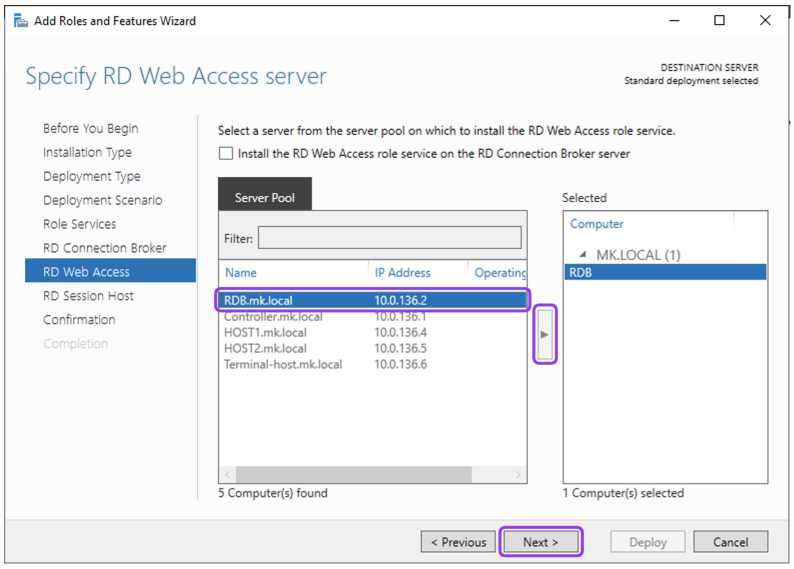


6. Na karcie *Role Services* sprawdź usługi, które zostaną zainstalowane. Kliknij *Next*, aby kontynuować.

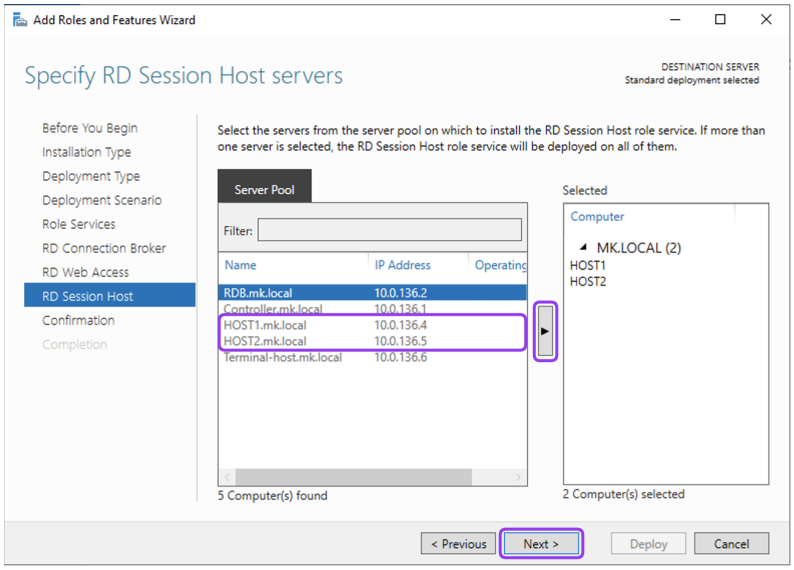
7. Na karcie *RD Connection Broker* wybierz odpowiedni serwer, na którym zostanie zainstalowana usługa roli Brokera. W tym przykładzie wybrano serwer `RDB`. Kliknij *Next*, aby kontynuować.



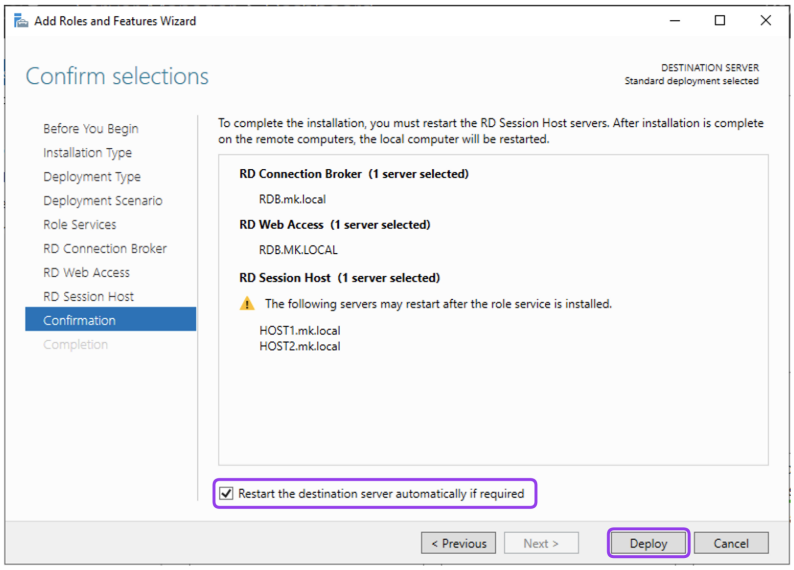
8. Na karcie *RD Web Access* wybierz odpowiedni serwer, na którym chcesz zainstalować rolę usługi RD Web Access. W tym przykładzie wybrano również serwer `RDB`. Kliknij *Next*, aby kontynuować.



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.



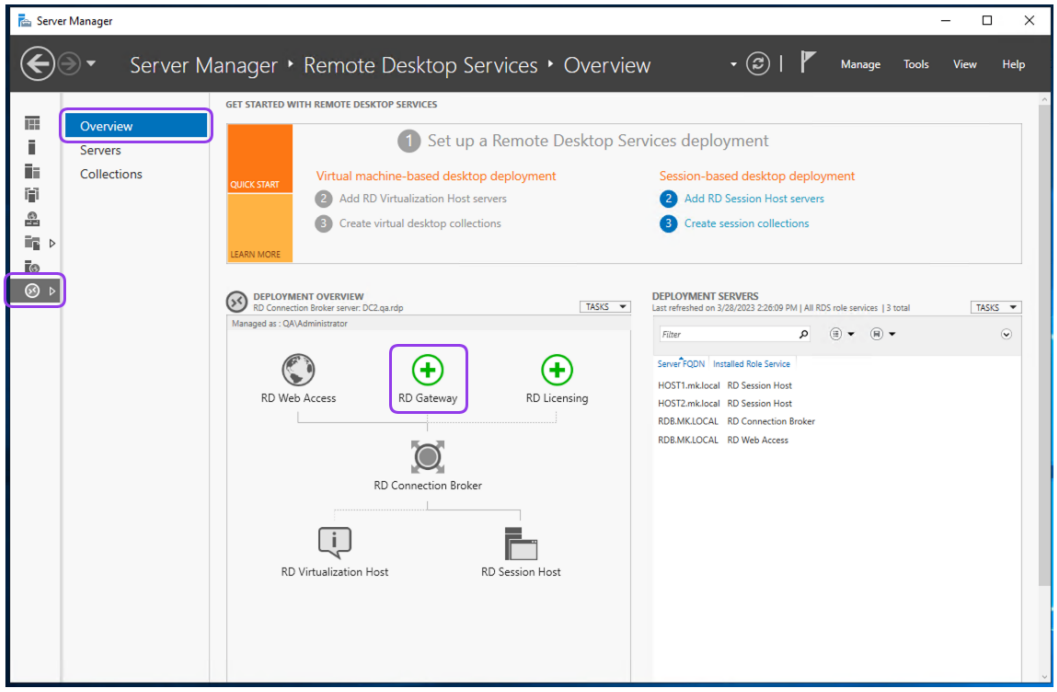
10. Na karcie *Confirmation* zaznacz *Restart the destination server automatically if required*, a następnie kliknij *Deploy*.



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`.

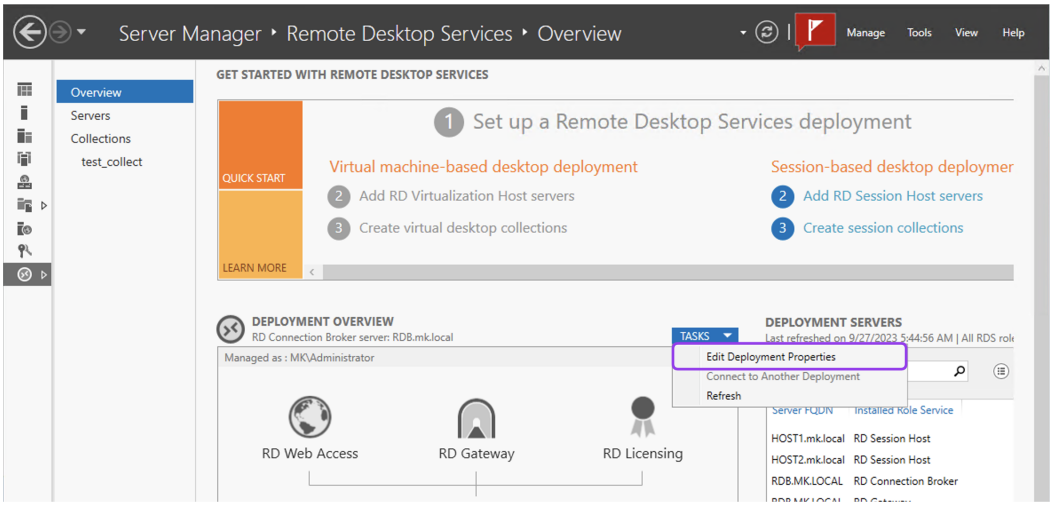


3. Kliknij *Next*.
4. Wprowadź nazwę certyfikatu SSL dla serwera RD Gateway, używając zewnętrznej, w pełni kwalifikowanej nazwy DNS (FQDN) serwera RD Gateway. Przykład, `cert.mk.local`.

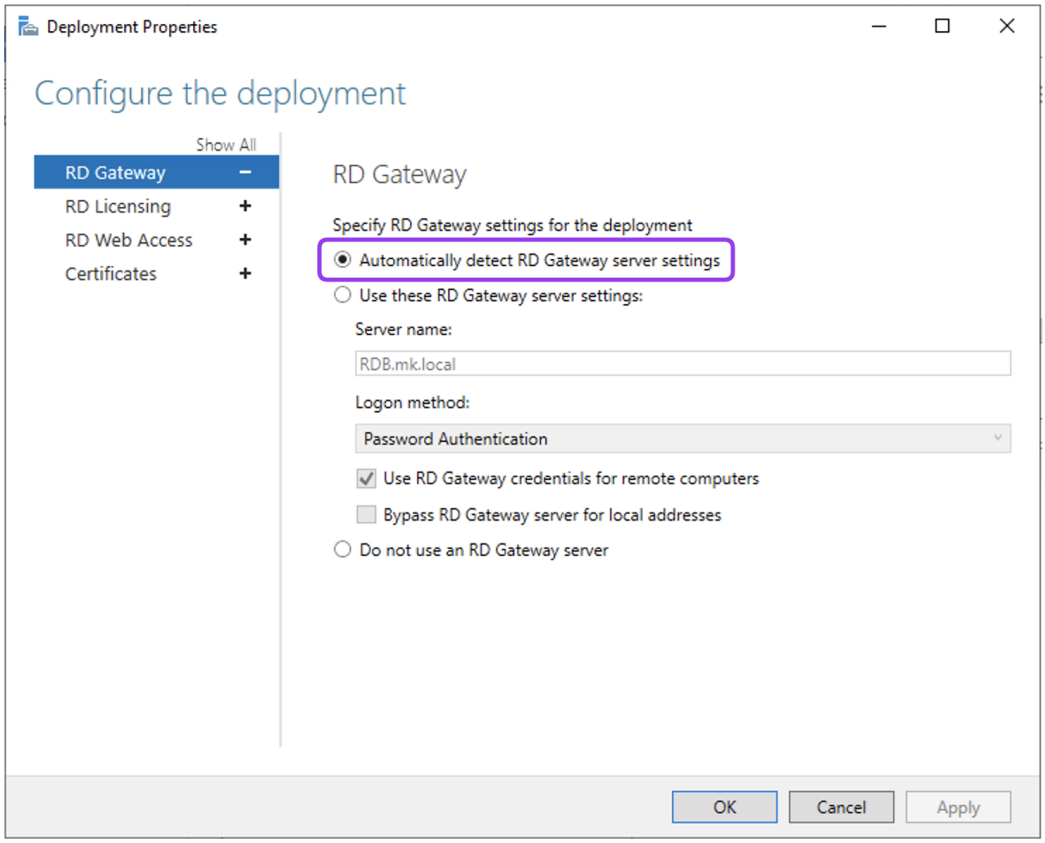
5. Kliknij *Next*, a następnie *Add*.
6. Poczekaj, aż usługa roli zostanie wdrożona, i kliknij *Close*.

Konfiguracja właściwości RD Gateway i RD Licensing:

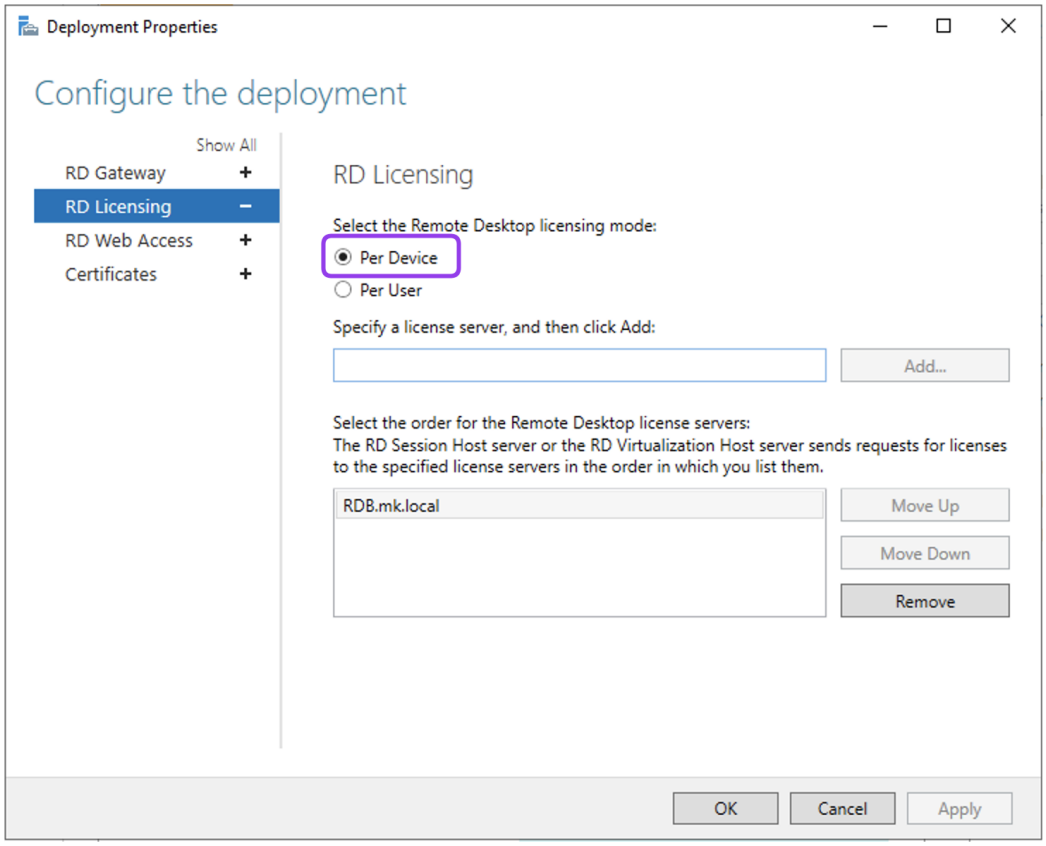
1. Wróć do karty *Overview*, kliknij *Tasks* i z listy rozwijanej wybierz *Edit Deployment Properties*.



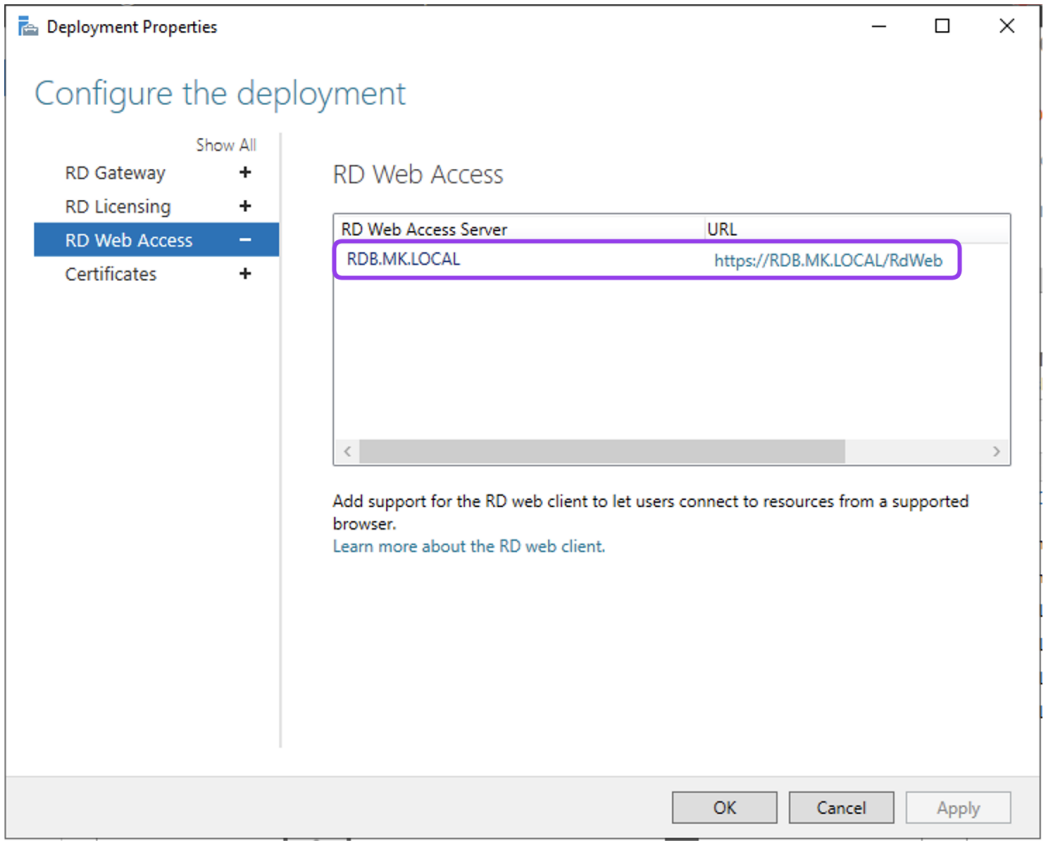
2. Na karcie *RD Gateway* wybierz opcję *Automatically detect RD Gateway server settings* i kliknij *Apply*.



3. Rozwiń kartę *RD Licensing* i wybierz *Per Device*. Kliknij *Apply*.

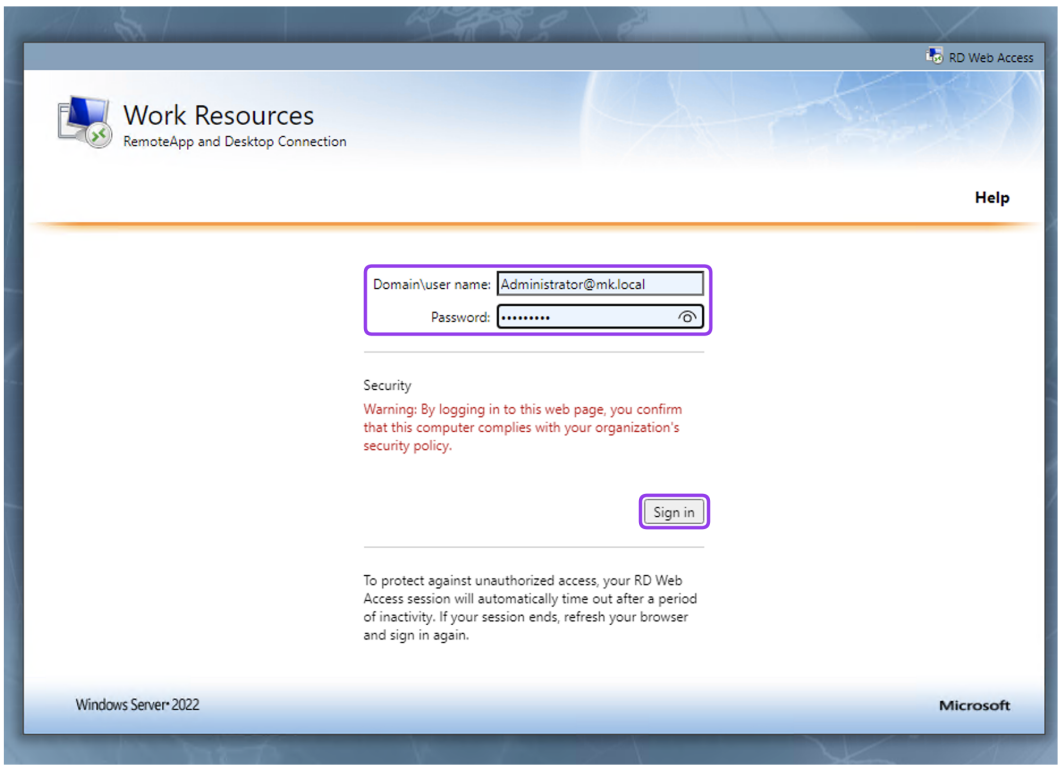


4. Rozwiń kartę «RD Web Access», aby sprawdzić adres URL dla RD Web Access IIS. Domyślnie jest zainstalowana pod adresem `/RdWeb`.



5. Kliknij na wyświetlony adres URL, aby zweryfikować logowanie do RD Web Access za pomocą konta administratora.

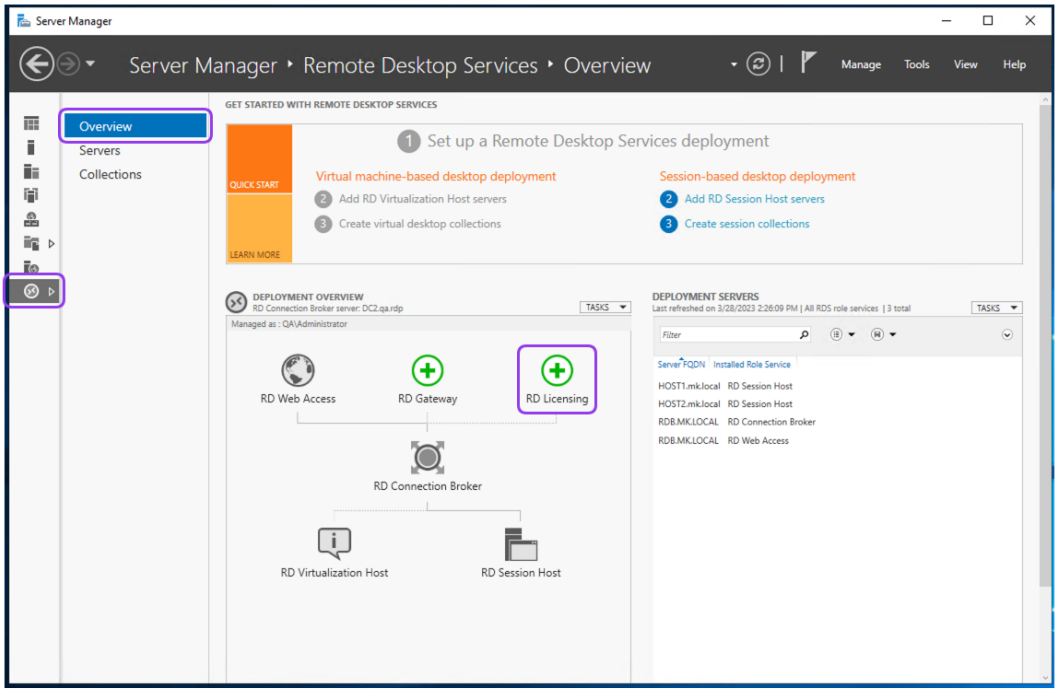
Informacja: Podczas logowania użyj domeny w polu *nazwa użytkownika*. Na przykład, `Administrator@mk.local`.



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:

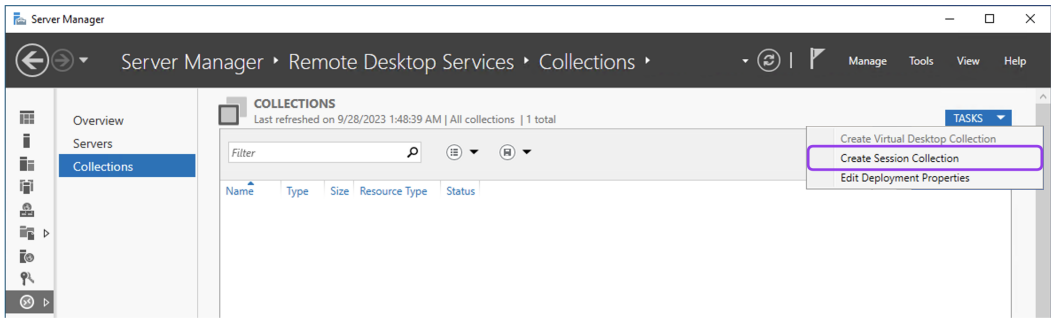
1. Kliknij przycisk *+ RD Licensing* na karcie *Overview* w sekcji *Remote Desktop Services*.



2. Wybierz maszynę wirtualną, na której zostanie zainstalowany serwer licencji RD. W tym przykładzie wybrano serwer `RDB`. Kliknij *Next*, a następnie *Add*.
3. Poczekaj, aż usługa roli zostanie wdrożona i kliknij *Close*.

Utwórz kolekcję:

1. Przejdź do karty *Collections* w sekcji *Remote Desktop Services*, kliknij *Tasks* i z listy rozwijanej wybierz *Create Session Collection*.



2. Na karcie *Before You Begin* kliknij *Next*.
3. Na karcie *Collection Name* podaj opisową nazwę kolekcji. W tym przykładzie użyto nazwy `test-collection`. Kliknij *Next*, aby kontynuować.

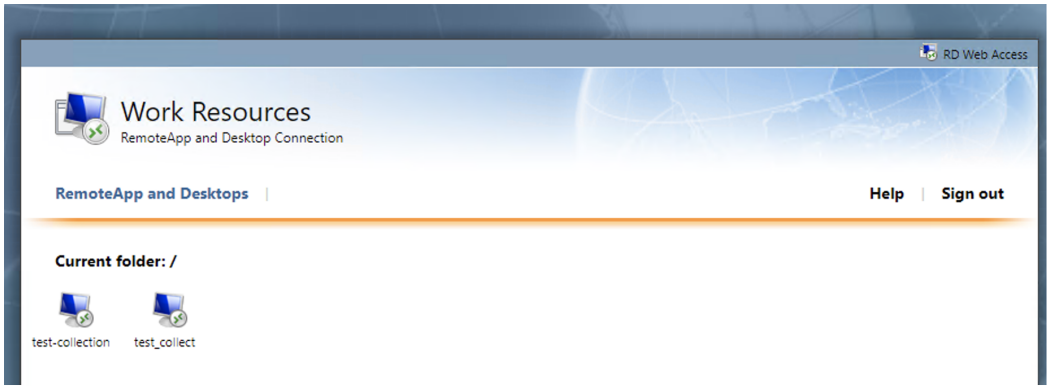
Informacja: Ta nazwa będzie wyświetlana pod ikoną w interfejsie Web Access.

4. Na karcie *RD Session Host* wybierz serwery do dodania do tej kolekcji. W tym przykładzie wybrano serwery `HOST1` i `HOST2`.
5. 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.

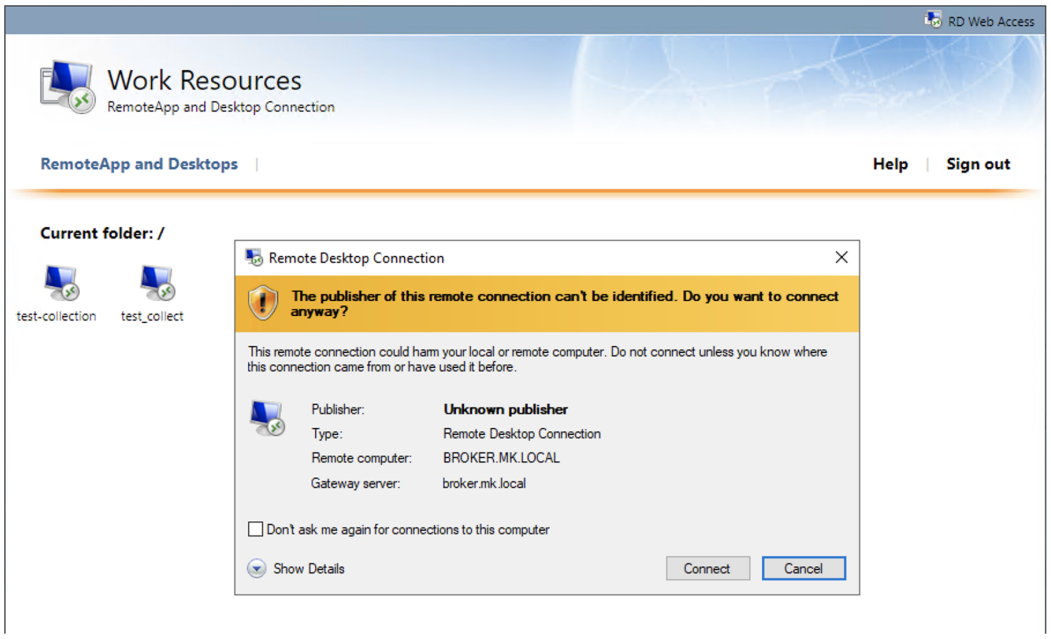
6. Na karcie *User Profile Disks* wybierz opcję *Enable User Profile Disks* i określ ustawienia, jeśli jest to konieczne. Możesz również pozostawić tę opcję wyłączoną.
7. Na karcie *Confirmation* przejrzyj wszystkie informacje, a następnie kliknij «Create».
8. Poczekaj, aż kolekcja zostanie utworzona. Kliknij *Close*.

Test połączenia:

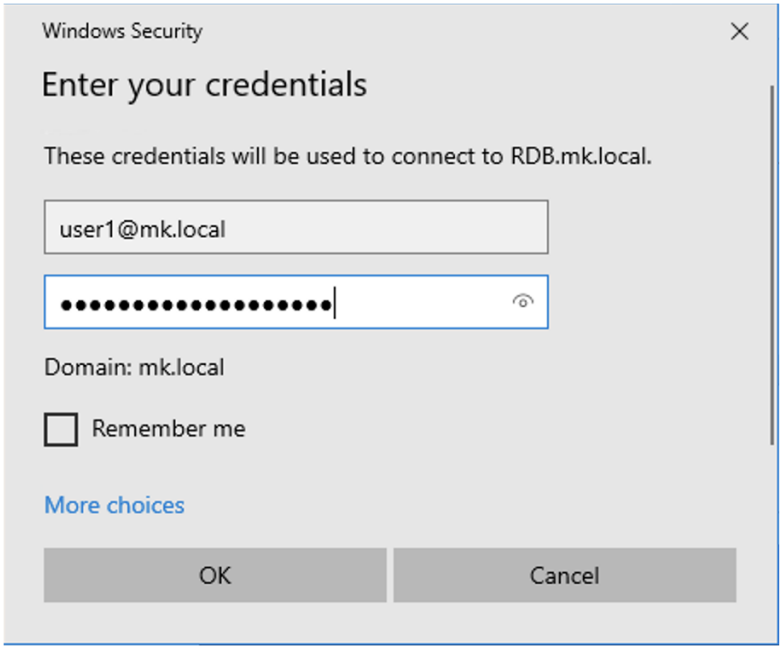
1. Otwórz zapisany wcześniej adres URL dla RD Web Access (np. `https://rdb.mk.local/RDWeb/`).
2. Wprowadź prawidłową nazwę użytkownika i hasło, a następnie kliknij *Sign in*. Możesz użyć konta administratora domeny do logowania, na przykład `Administrator@mk.local`.
3. Po zalogowaniu zostanie przedstawiona 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.

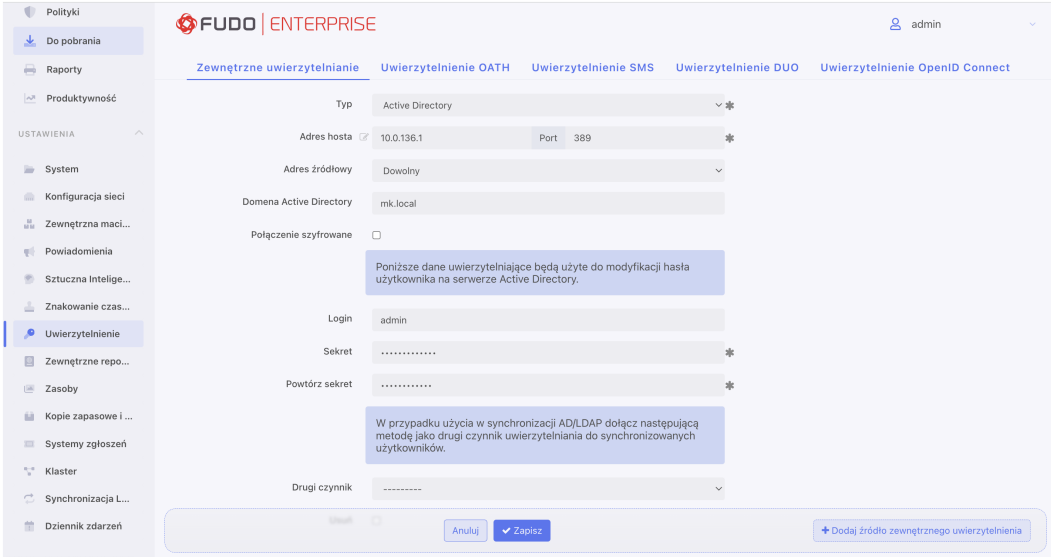
28.3.2 Konfiguracja Fudo Enterprise

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*.
2. Wpisz nazwę użytkownika odpowiadającą wybranemu kontu użytkownika w Active Directory (np. `user1`).
3. W karcie *Ustawienia*, w sekcji *Sejfy*, wybierz *portal*.
4. Kliknij *Zapisz*.
5. Przejdź do sekcji *Uwierzytelnienie* i z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz *Uwierzytelnienie zewnętrzne*.
6. Wybierz metodę Active Directory utworzoną w poprzednich krokach i kliknij *Zapisz*.
7. W razie potrzeby uzupełnij pozostałe parametry zgodnie z wymaganiami swojej specyficznej konfiguracji. Po więcej szczegółów przejdź do sekcji *Dodawanie użytkownika*.
8. 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*.

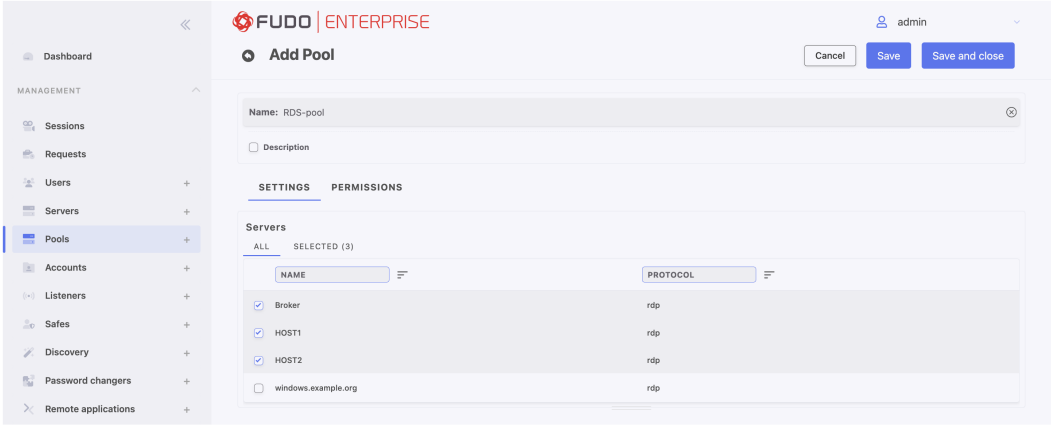
6. W sekcji *Adres źródłowy* wybierz `IPv4` i wprowadź adres IP serwera wybranego podczas konfiguracji RDS dla roli RD Broker (w naszym przykładzie serwer `RDB` z adresem IP `10.0.136.2`).
7. Kliknij *Zapisz i zamknij*.

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:

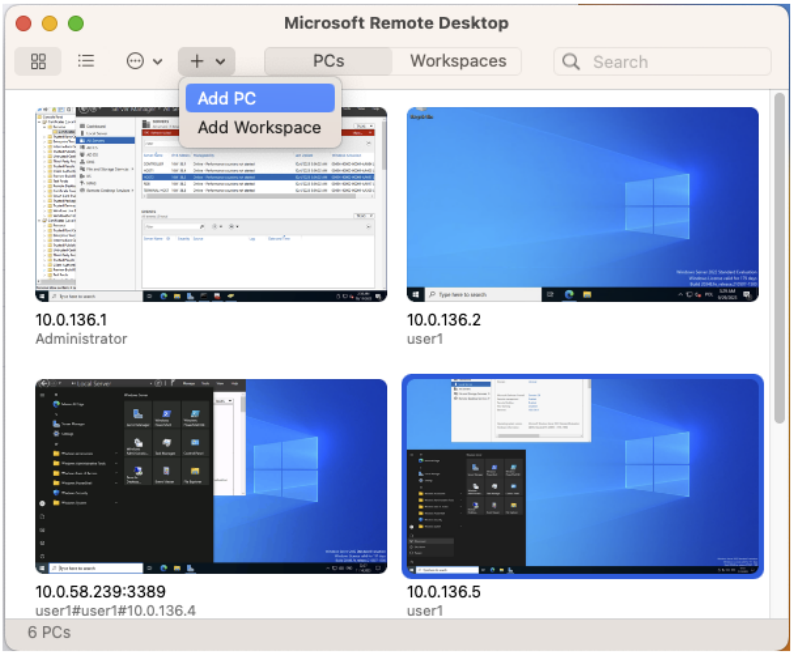
> **Ostrzeżenie:** Podczas nawiązywania połączeń za pomocą Remote Desktop Services zalecane jest korzystanie z opcji *Native client*. *Web client* nie obsługuje tego typu połączeń.

1. Zaloguj się do «Portalu 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`.

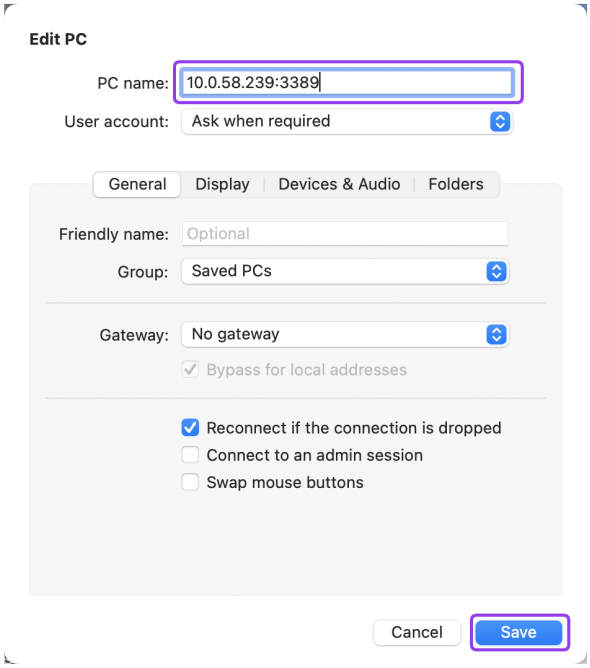
Przekierowanie połączenia przez Fudo w natywnym kliencie RDP:

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.

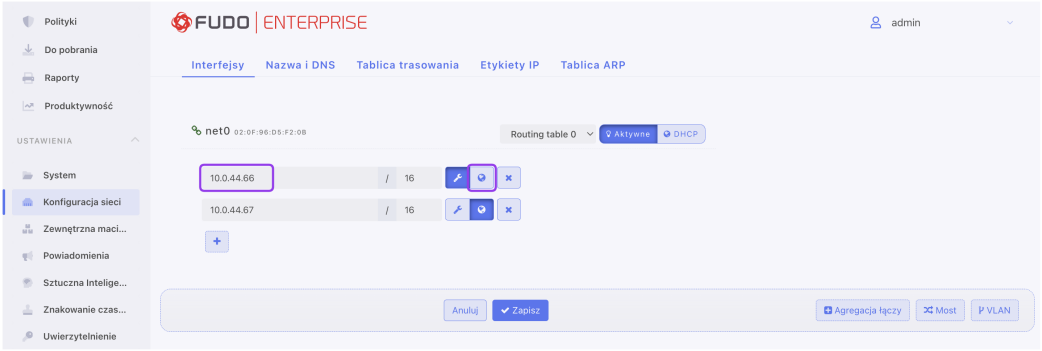
3. Na przykładzie Microsoft Remote Desktop, kliknij ikonę plus w górnej części okna i wybierz *Dodaj komputer*.



4. W polu *Nazwa komputera* wprowadź adres IP Portalu Użytkownika Fudo Enterprise wraz z numerem portu i kliknij *Dodaj*.



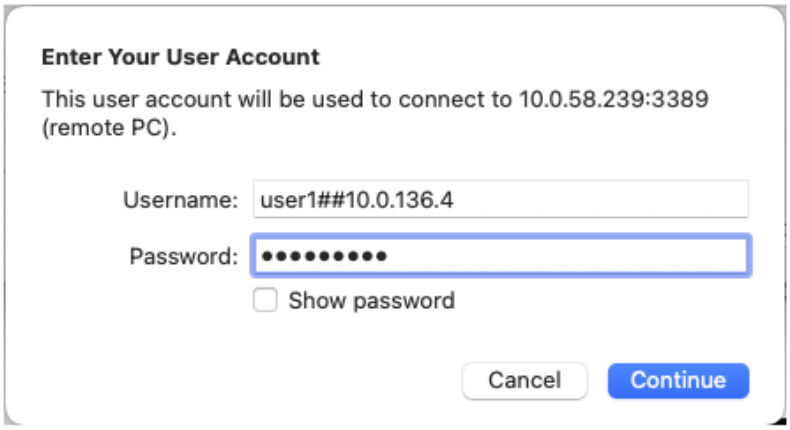
Informacja: Adres IP Portalu Użytkownika znajdziesz w zakładce *Ustawienia* > *Konfiguracja sieci*.



5. Połącz się z dodanym komputerem, podając w polu *Nazwa użytkownika* ciąg logowania dla połączeń bastion oraz hasło w polu *Hasło*.

Informacja:

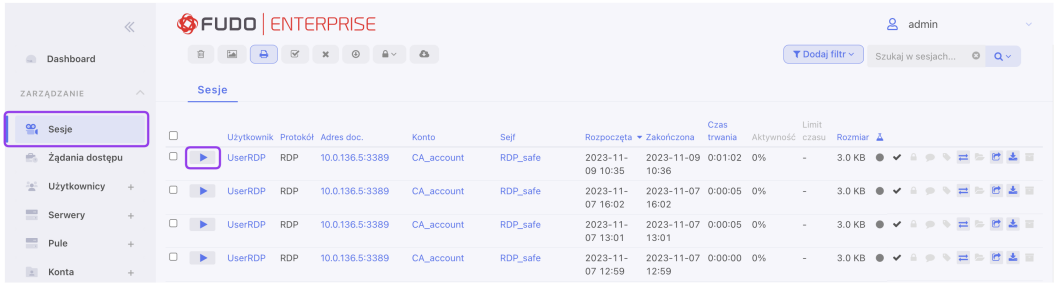
- Użyj następującego wzoru dla ciągu logowania bastion: nazwa użytkownika # login konta na docelowym serwerze # adres docelowego serwera (np. `user1#user1#10.0.136.4`).
- Można pominąć login konta, jeśli jest taki sam jak nazwa użytkownika, np. `user1##10.0.136.4`

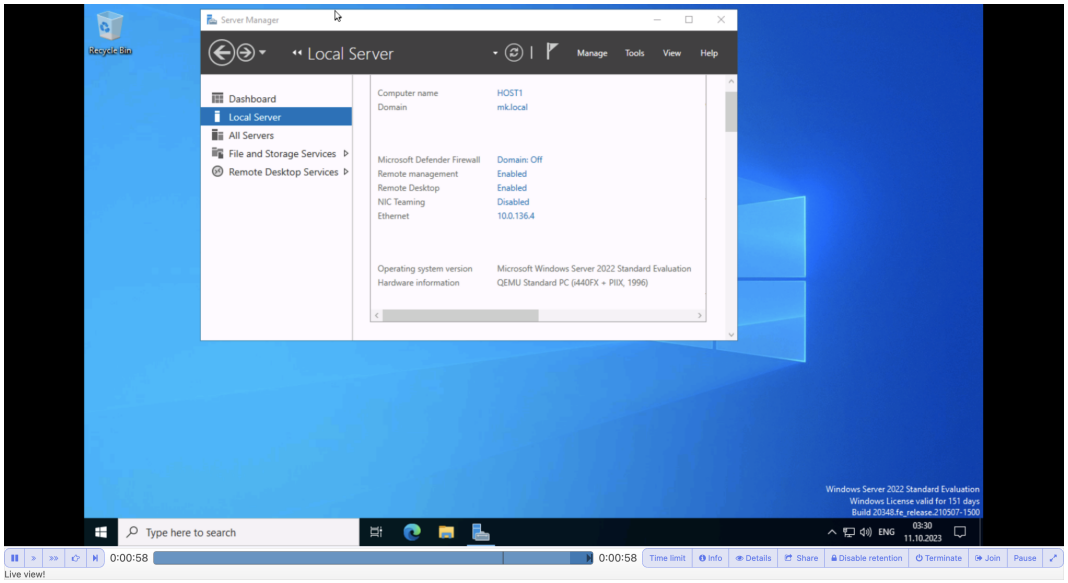


6. Klient RDP nawiąże połączenie z jednym z serwerów z kolekcji RDS.

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.





Tematy pokrewne:

- *RDP w trybie bastionu*
- *Uwierzytelnienie*
- *Integracja z serwerem CERB*

28.4 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.

28.4.1 Lokalizacja certyfikatu dla protokołu RDP w Windows Server

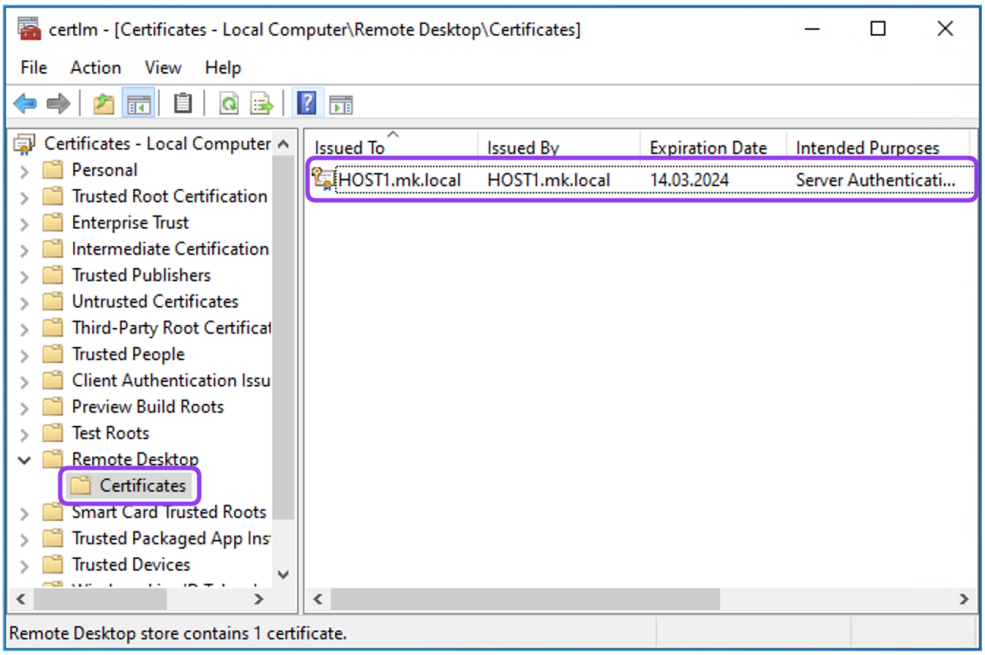
Postępuj zgodnie z jednym z poniższych scenariuszy, aby zlokalizować certyfikat pobrany przez Fudo Enterprise z Windows Server podczas tworzenia serwera RDP.

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`.

2. Wyświetli się okno Menedżera certyfikatów dla lokalnego urządzenia.
3. 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.

1. 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
```

2. W odpowiedzi otrzymasz certyfikat, z którego możesz wyodrębnienić numer seryjny, wpisując poniższe polecenie i podając otrzymaną zawartość certyfikatu:

```
c x509 -noout -serial

-----BEGIN CERTIFICATE-----
MIIChbdygdu656sdf65ac55mpn1PmpBK/
↪7OWFeh+xjANBgkqhkiG9w0BAQsFADAZ
MRcwFQYDVQQDEw5IT1NUMS5tay5sb2NhbDAeFw0yMzA5MTMxNzA2NTRaFw0yNDAz
MTQxNzA2NTRaMBkxFzAVcas7c6c6sh83uydtLm1rLmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ngYkoMa4dgLgGl1+G+m2UEAIH/
↪6ttyQep5u
tUYkxKeuqpn9AWnYP8To1fornJN387ddhcy76d7jchc8Q093RWVb2cMKKjgOAW9w
qLFW+WrLEUPY8hYvsCFYgFH3HOHhKLEoWBN5qHH7vjIiW3RbOY7xeGb9x0FWItQX
mbF6sucGdlH+OsjepxMLPVh3Qpb2WQ18kSQGyS1ocbJxOWST9sH4MQkRVFL3rkxN
```

(ciąg dalszy na następnej stronie)

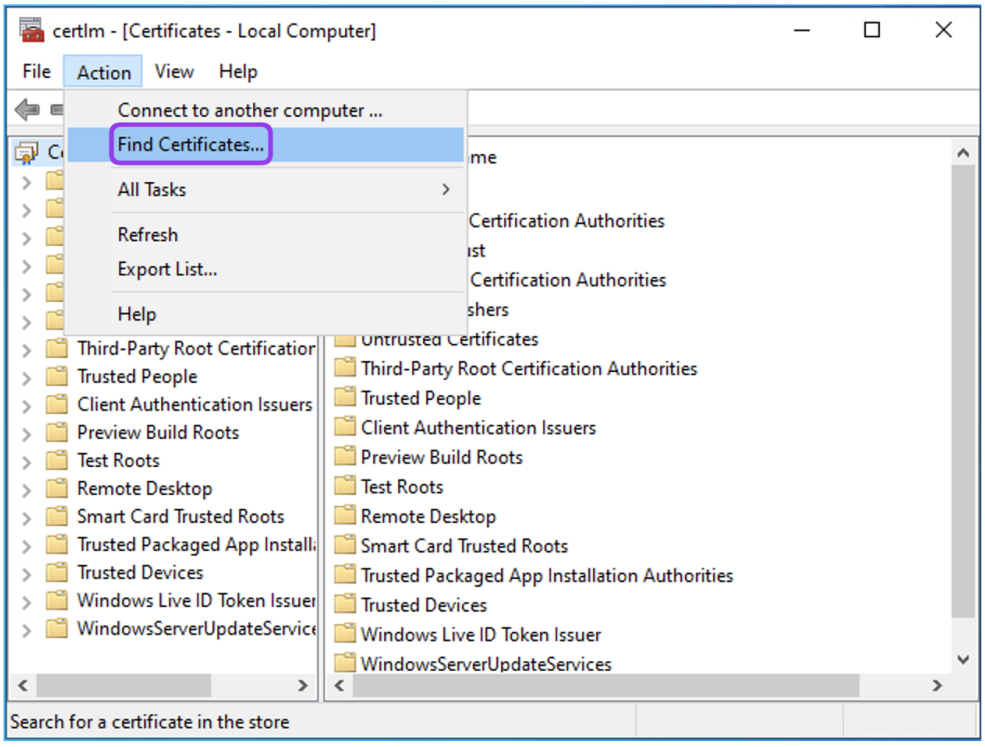
(kontynuacja poprzedniej strony)

```
f7/
↪qdJcdM6sFxEJTdp30CITRfbORXacl84bStjW2MJzvJRqr94xDHonRdIM9tUka
O6LVJQY6qiEpMVE8MpSDAfoZ+HeyVWt+2EfXlfWE4hiMJP1DoQIDAQABoyQwIjAT
BgNVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQAD
ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
↪Tnrrn2
7pr0jLnCjUq9rxHC6jfMR0U2PT4qrMHvGD1nUwZdHuZPavPLFHh/
↪rYHZpizoS+9W
ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
↪Tnrrn2
xyXjeYdX8/U9EdgrXOLGX9U74rfGQTrQxZyjuYlGxxqop/
↪y2V3n+3NnNzY+ehW1G
ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
↪Tnrrn2
ZUvdUnqtdH+0DdAWBo4P1dv0nL8=
-----END CERTIFICATE-----
```

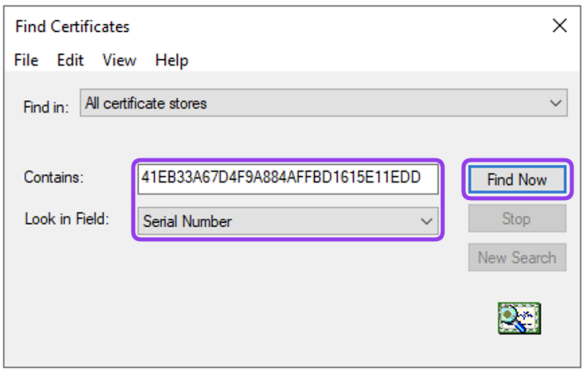
3. W odpowiedzi wyodrębniony zostanie numer seryjny, który możesz wykorzystać do wyszukania certyfikatu w Menedżerze certyfikatów.

```
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*.

28.4.2 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.

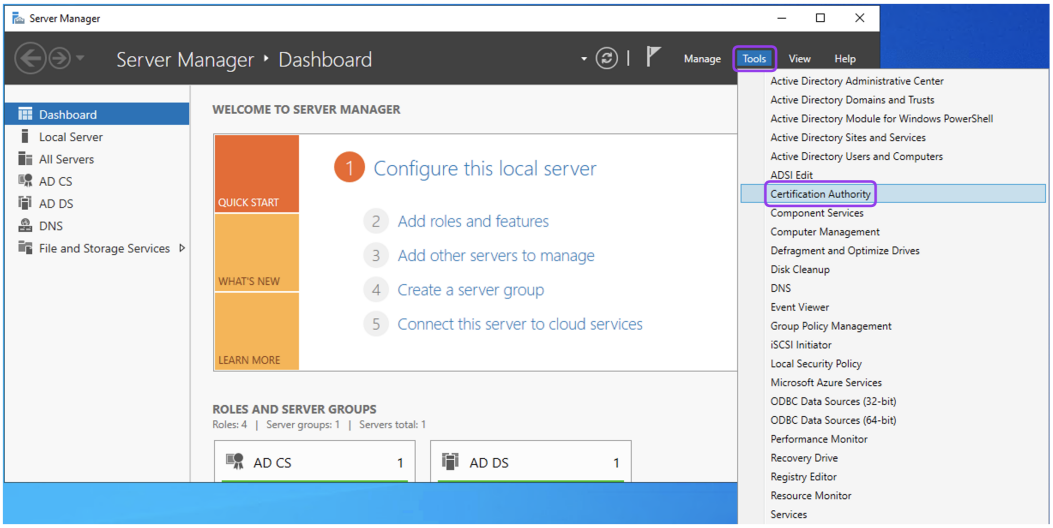
Instalacja Certificate Authority w Windows Server:

Aby zainstalować *Certificate Authority* w Windows Server, postępuj zgodnie z instrukcją Windows Server.

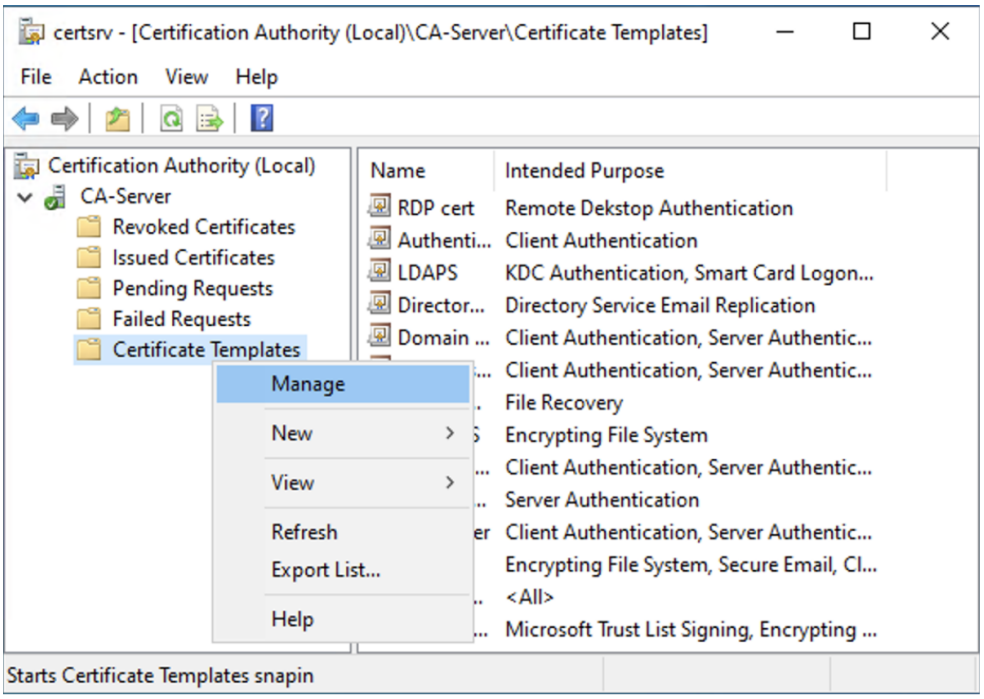
Informacja: W procedurze opisanej poniżej wykorzystano opcję *Enterprise CA*.

Tworzenie szablonu dla certyfikatu RDP:

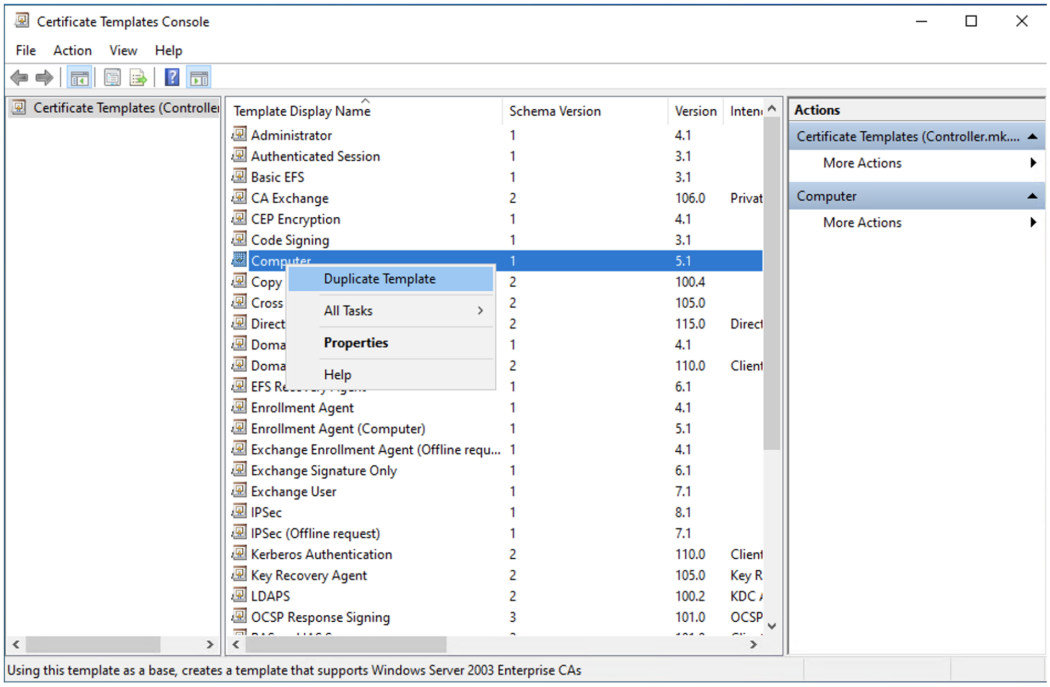
1. Otwórz *Certificate Authority* z poziomu narzędzia *Server Manager*, klikając *Tools* > *Certification Authority* w prawym górnym rogu okna.



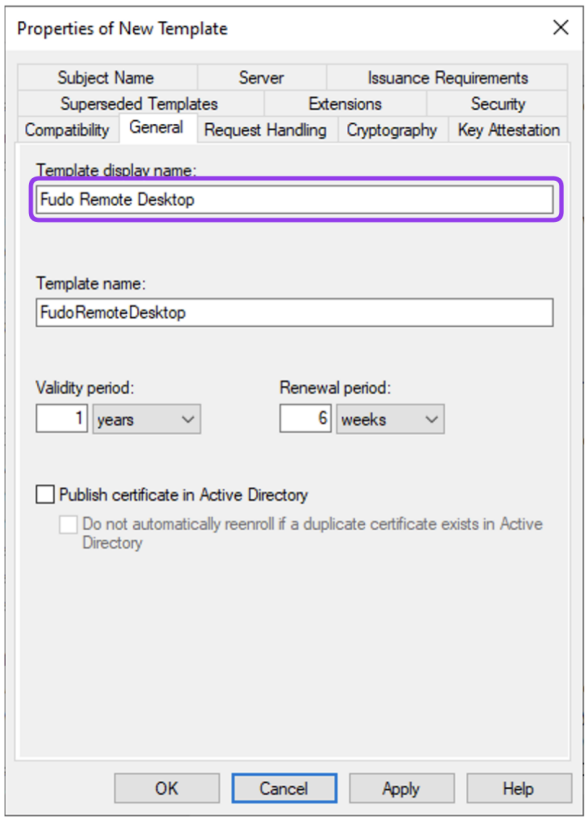
2. Kliknij prawym przyciskiem myszy na *Certificate Templates* i wybierz *Manage*.



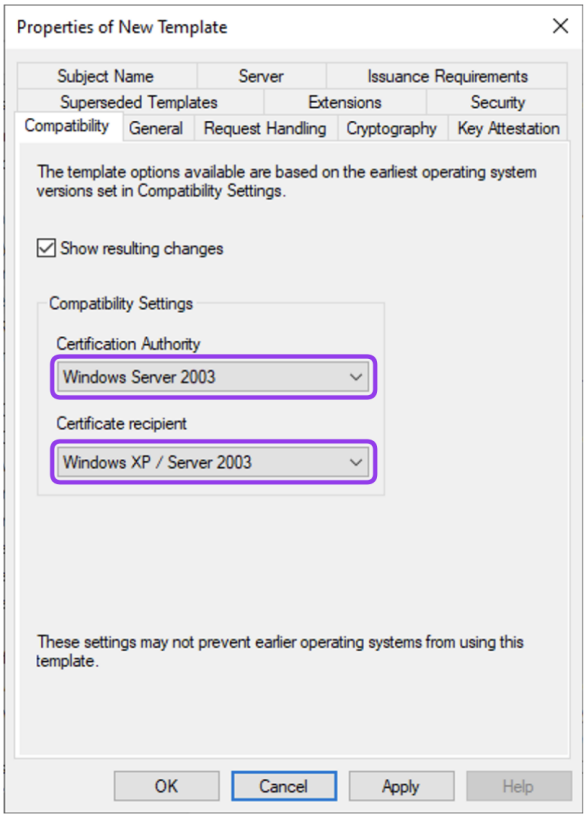
3. Znajdź szablon *Computer*, kliknij na nim prawym przyciskiem myszy i wybierz *Duplicate Template*.



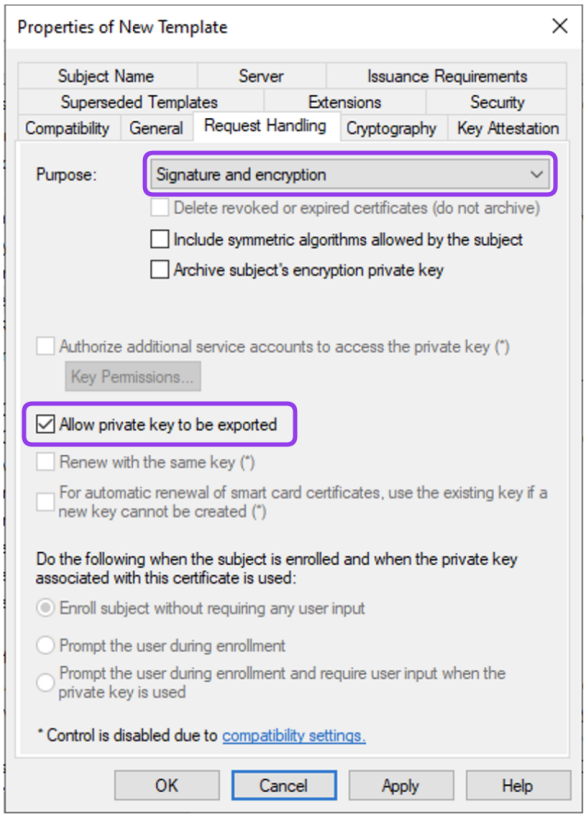
4. W zakładce *General*, wprowadź nazwę dla nowego szablonu oraz określ okres ważności i odnawiania według potrzeb.

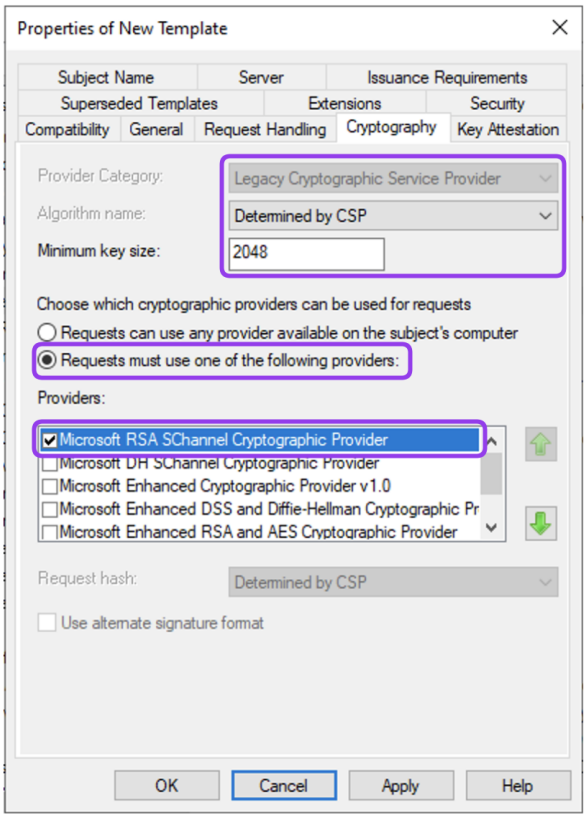


5. W zakładce *Compatibility*, z listy rozwijanej *Certification Authority* wybierz *Windows Server 2003*, natomiast z listy rozwijanej *Certificate recipient* wybierz *Windows XP/Server 2003*.

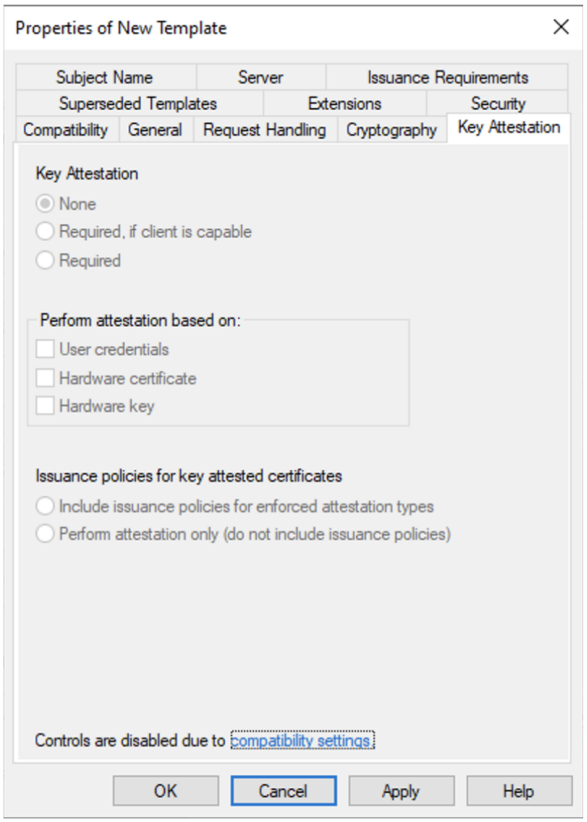


6. W zakładce *Request Handling*, ustaw *Purpose* na *Signature and encryption* i zaznacz opcję *Allow private key to be exported*.

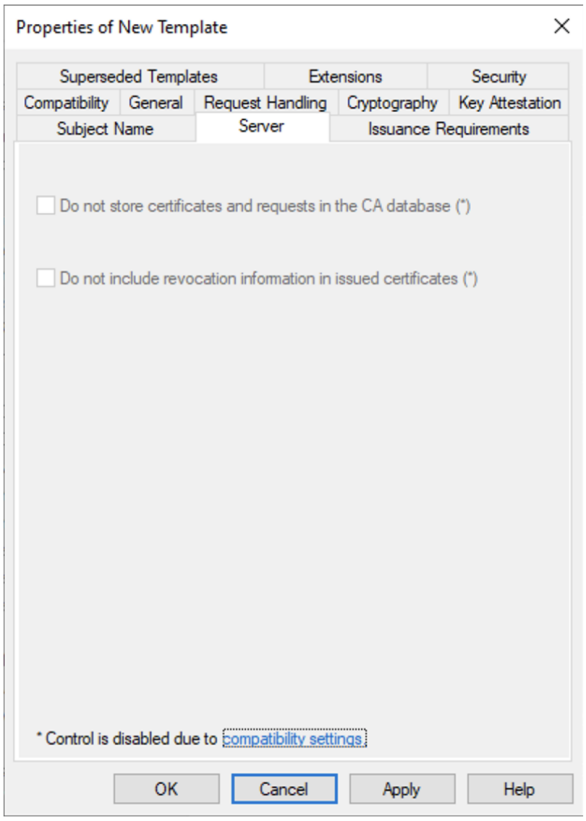




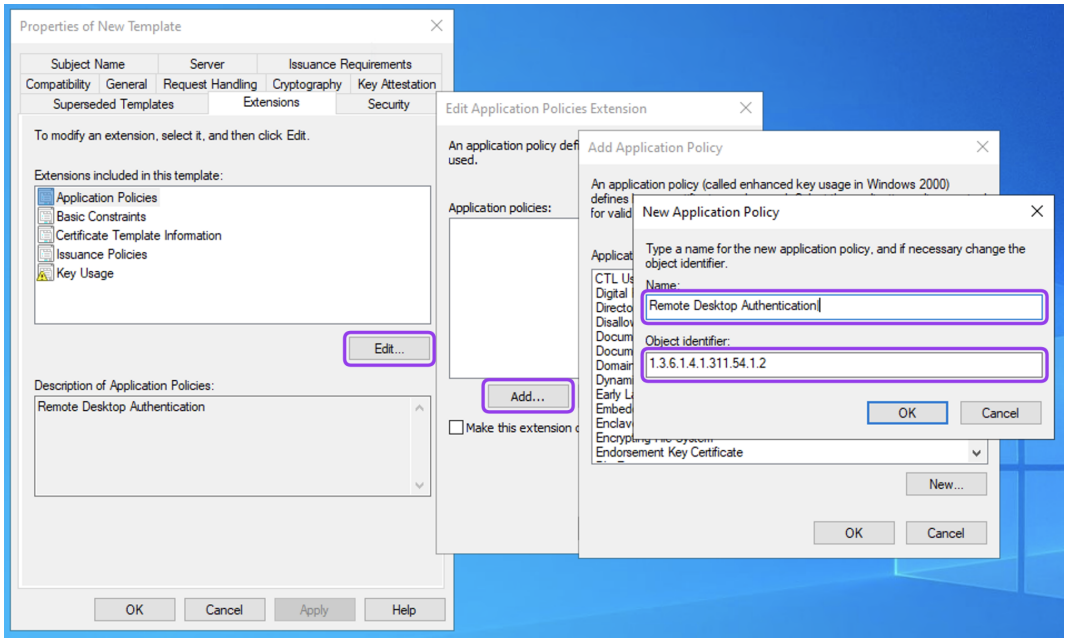
8. W zakładce *Key Attestation* pozostaw ustawienia domyślne.



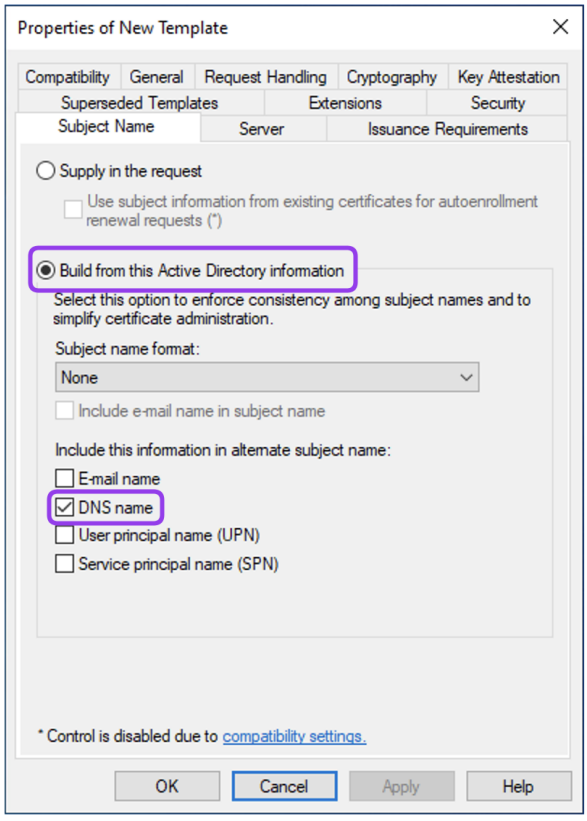
9. W zakładce *Server* pozostaw ustawienia domyślne.



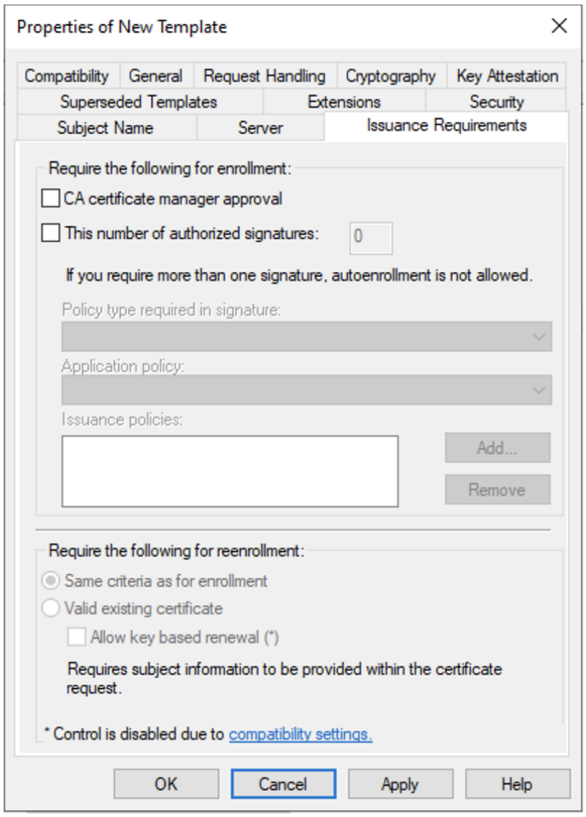
10. W zakładce *Security* dodaj komputery i grupy, które mają być uprawnione do używania tego szablonu. Sprawdź, czy grupa lub użytkownik, którego używasz, ma włączone uprawnienia *Read*, *Write* i *Enroll*. Jest to konieczne do żądania certyfikatu przy użyciu tego szablonu w następnych krokach.
11. 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*.

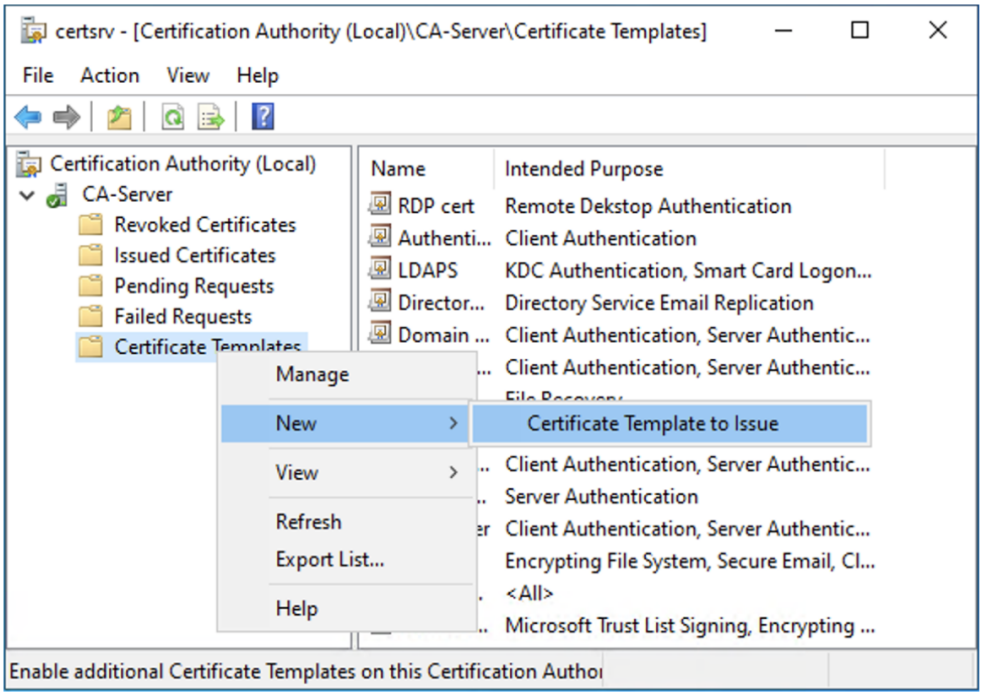


17. W zakładce *Issuance Requirements*, pozostaw ustawienia domyślne.

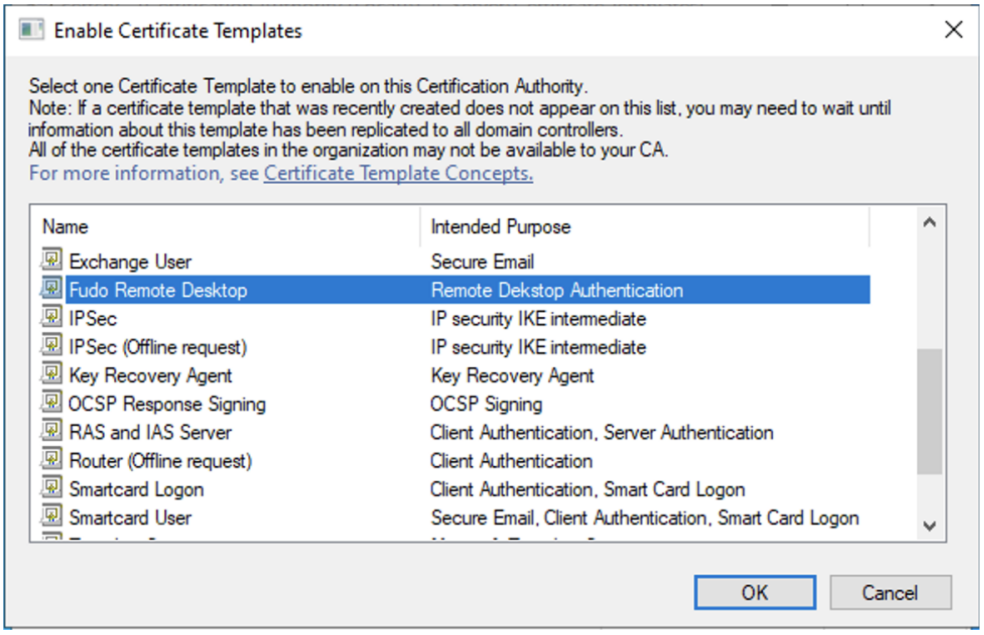


18. Kliknij *OK*, aby zapisać utworzony szablon. Zamknij *Certificate Templates Console*.

19. Wróć do okna *Certification Authority*, kliknij prawym przyciskiem myszy na *Certificate Templates* i wybierz *New* > *Certificate Template to Issue*.

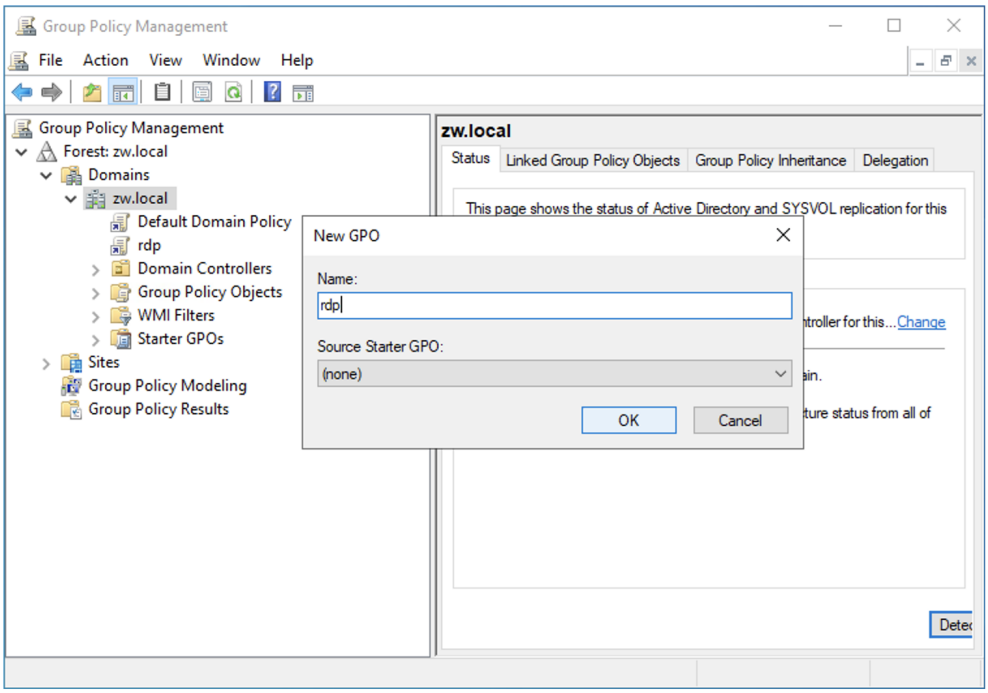


20. Wybierz utworzony szablon i kliknij *OK*.



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*.

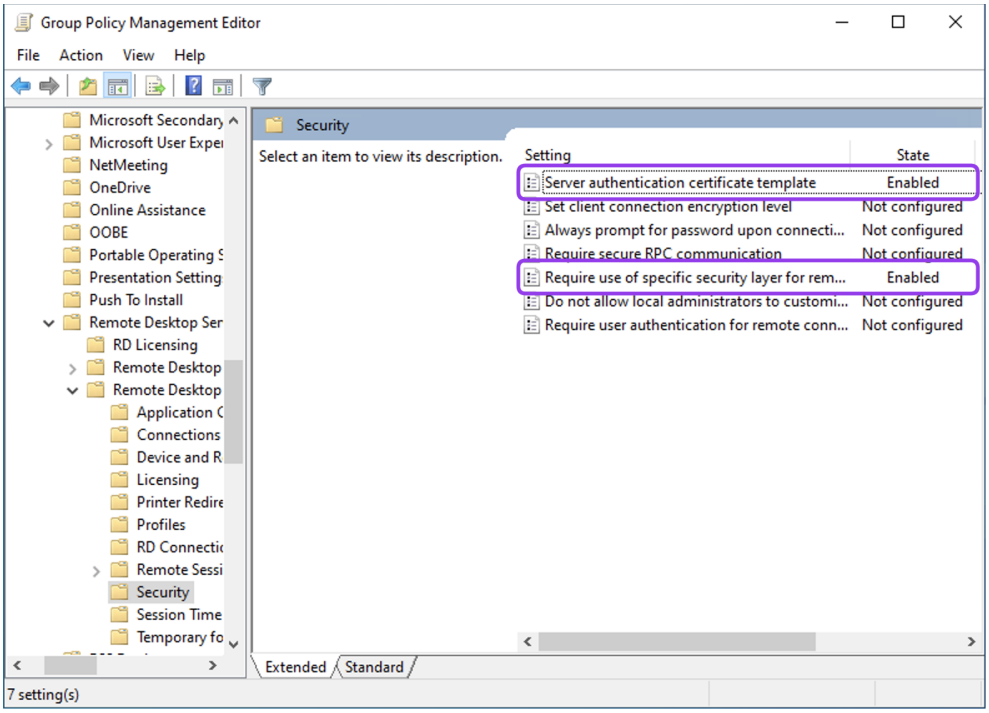


5. Kliknij prawym przyciskiem myszy na nazwę utworzonego *GPO* i wybierz

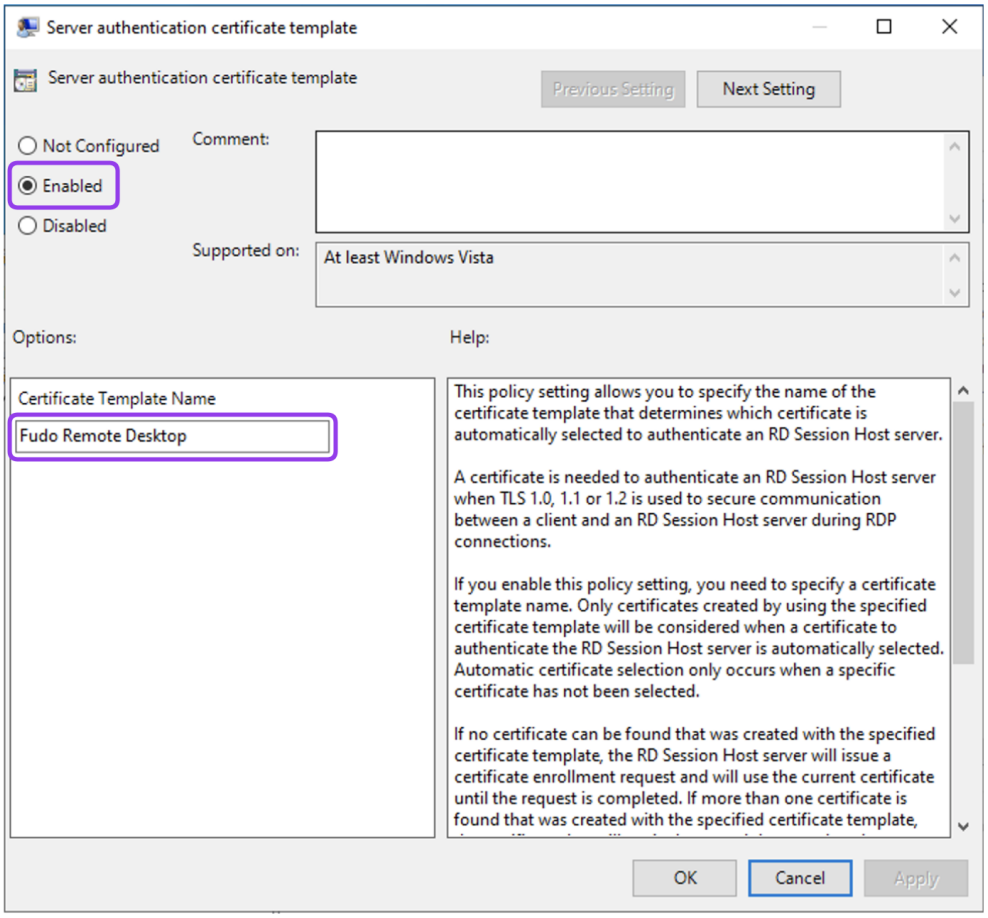
Edit....

6. W *Group Policy Management Editor* przejdź do *Computer Configuration* > *Policies* > *Administrative Templates* > *Windows Components* > *Remote Desktop Services* > *Remote Desktop Session Host* > *Security*.

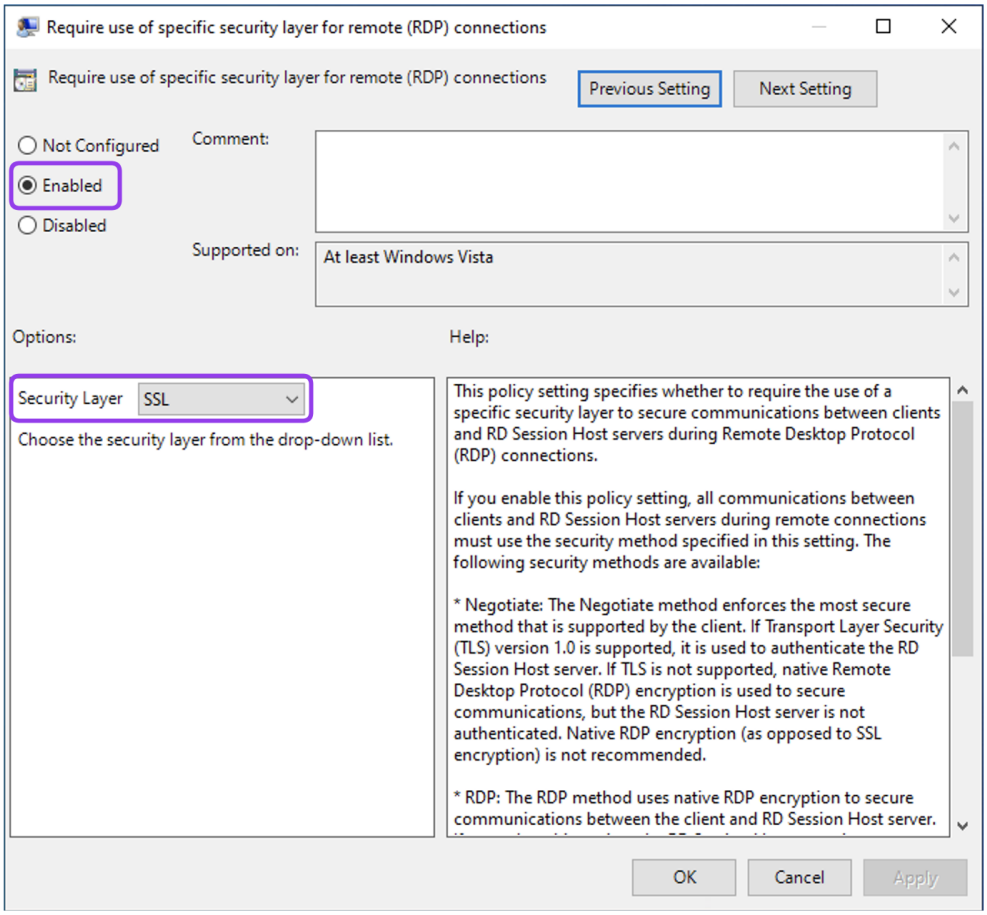
7. Kliknij dwukrotnie na *Server authentication certificate template*, aby edytować to ustawienie.



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*.

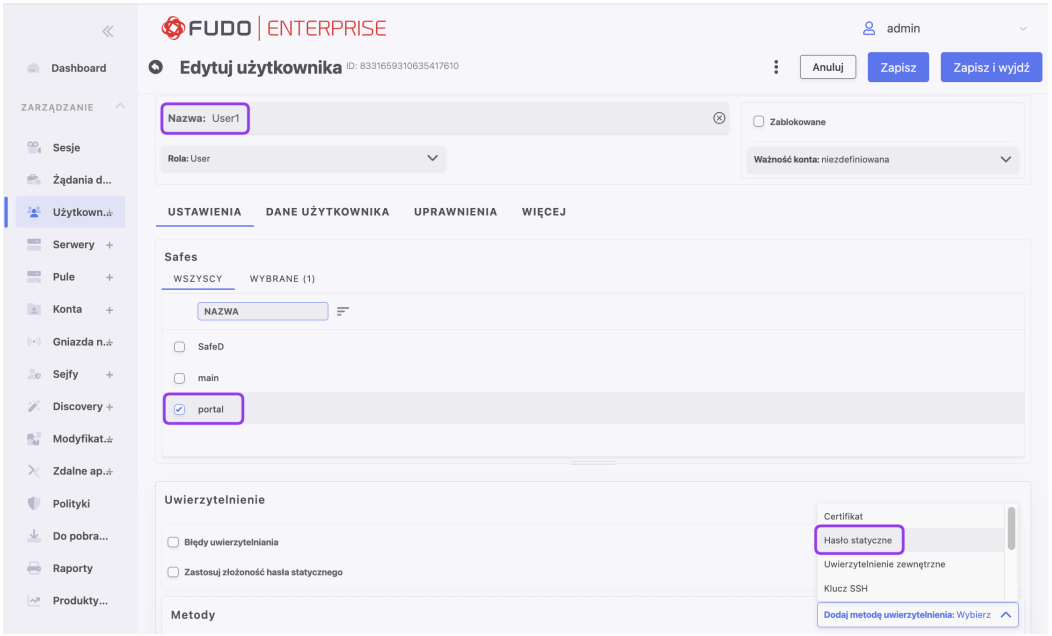
Eksport certyfikatu CA:

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*.

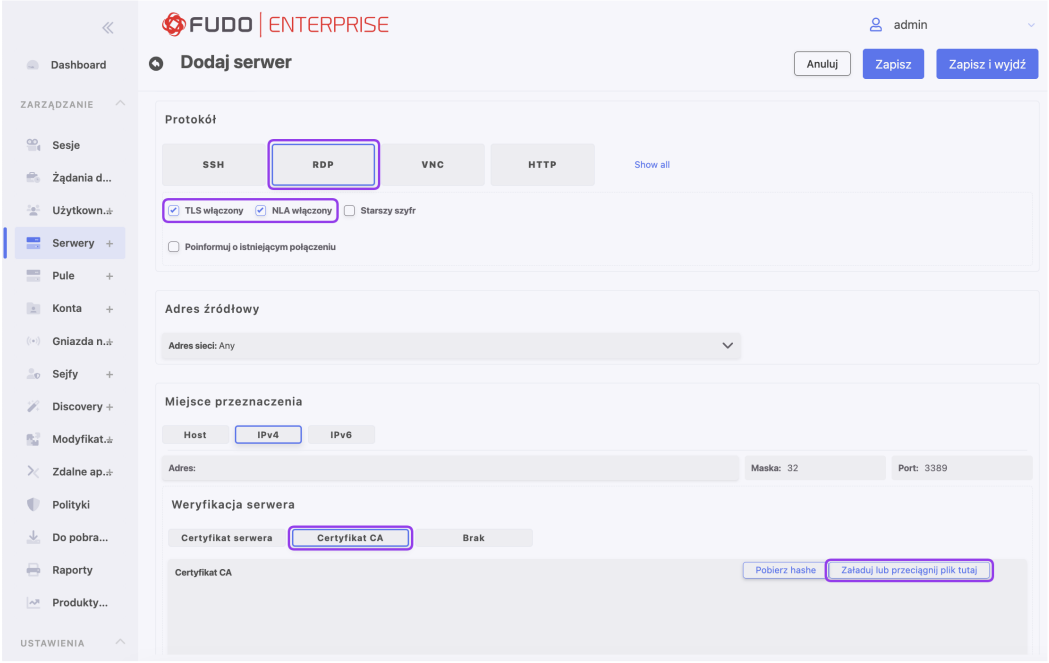


6. Wprowadź hasło i kliknij *Zapisz*.
8. Uzupełnij pozostałe parametry według własnych wymagań (jeśli wymagane). W tym celu możesz zapoznać się z treścią rozdziału *Dodawanie użytkownika*.
9. Kliknij *Zapisz i zamknij*.

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.



8. Kliknij *Zapisz i zamknij*.

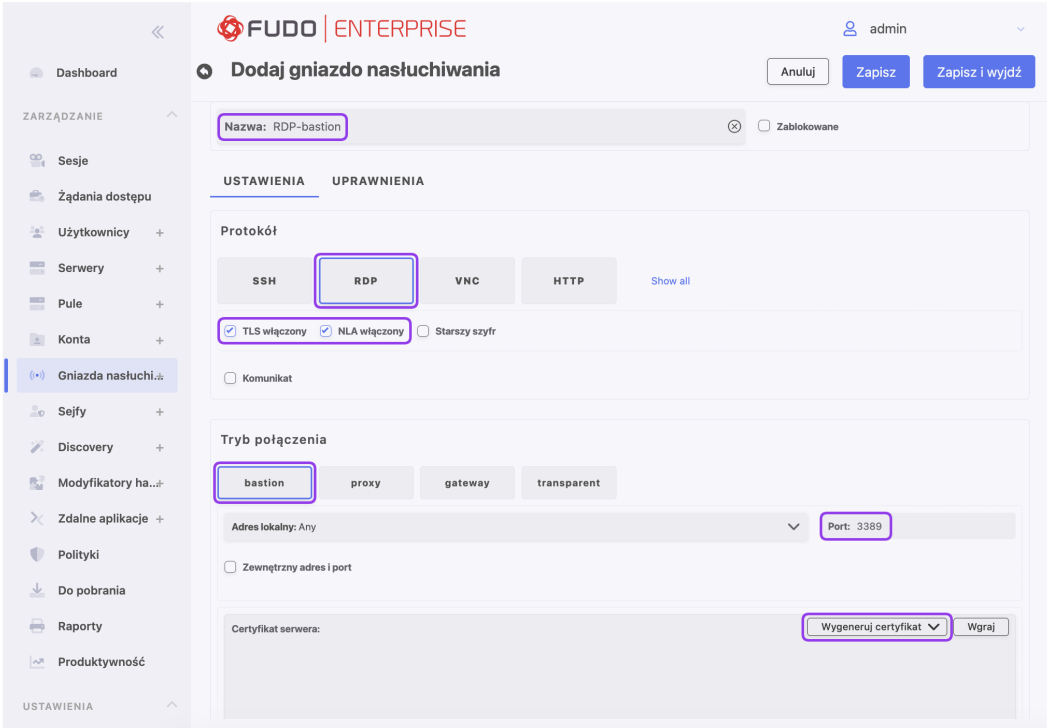
Konfiguracja konta:

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 *Zastąp 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`).

3. Przejdź do zakładki *Uprawnienia* i dodaj użytkowników upoważnionych 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 bezpieczeństwa.
7. W sekcji *Tryb połączenia* wybierz *bastion*.
8. Ustaw *Adres lokalny* na `Any` i port `3389`.
9. 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).



10. Kliknij *Zapisz i zamknij*.

Konfiguracja Sejfu:

1. Wybierz *Zarządzanie* > *Sejfy* i kliknij *+ Dodaj*.
2. Wprowadź nazwę obiektu (np. `SafeRDP`).
3. Wybierz opcję *Klient Webowy*, aby umożliwić nawiązanie sesji w przeglądarce.
4. 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.

5. Wybierz zakładkę **Konta**, aby dodać konta dostępne przez ten sejf.

- **Kliknij «+ Dodaj konto», a następnie kliknij ikonę [+] obok `CA-account`, które zostało utwo**

  – Kliknij «ok», aby zamknąć okno.

  – Kliknij ikonę edycji, aby przypisać do konta gniazdo nasłuchiwania.

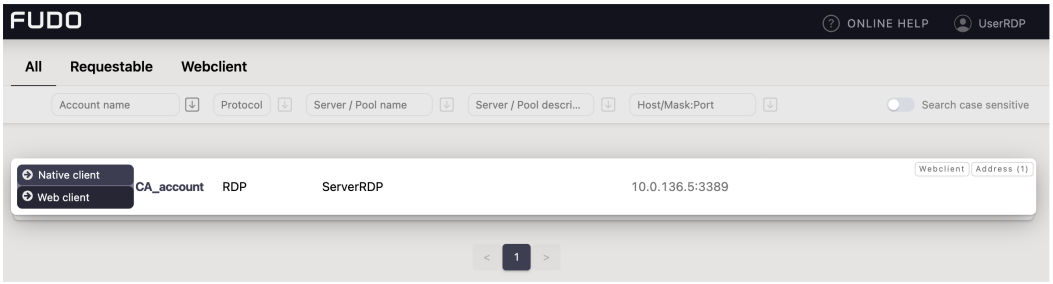
  – Kliknij ikonę [+], aby dodać gniazdo nasłuchiwania `RDP-bastion` utworzone w poprzednich krokach.

  – 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*

28.5 Konfiguracja Single Sign On (SSO)

Przed rozpoczęciem procedury sprawdź następujące wymagania:

- Wszystkie serwery z systemem Windows Server 2019 lub 2022 są połączone w domenie;
- Istnieje skonfigurowany na serwerze Windows kontroler domeny z grupą użytkowników AD.

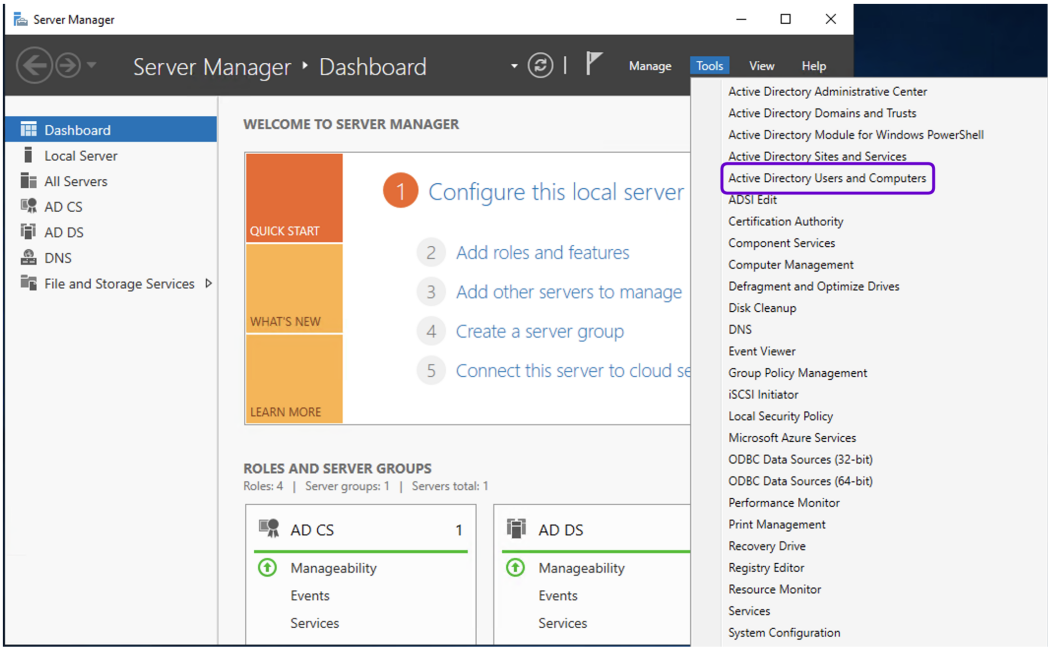
Aby skonfigurować i używać usługi Single Sign On (SSO) wraz z Fudo Enterprise, postępuj zgodnie z poniższą instrukcją.

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.

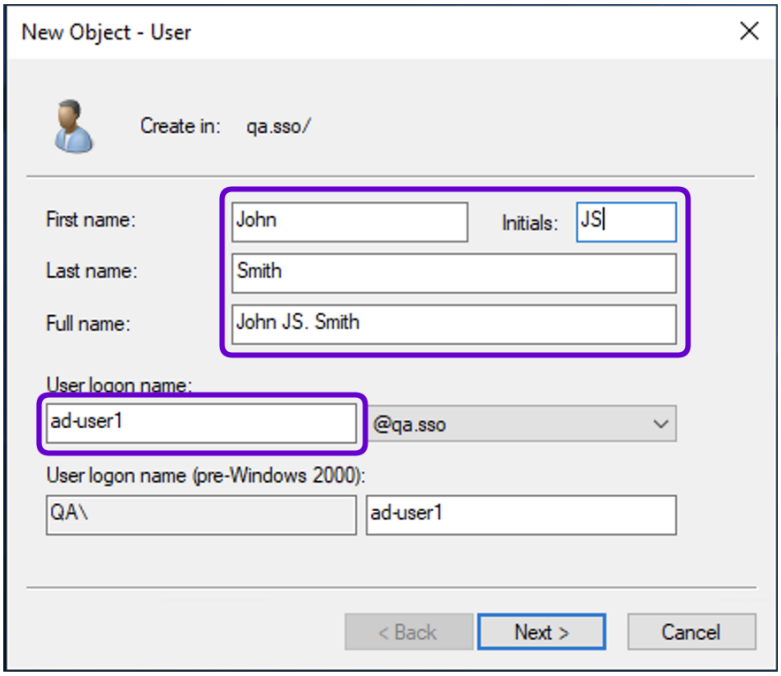
28.5.1 Konfiguracja SSO na Windows Server 2019

Dodaj użytkownika:

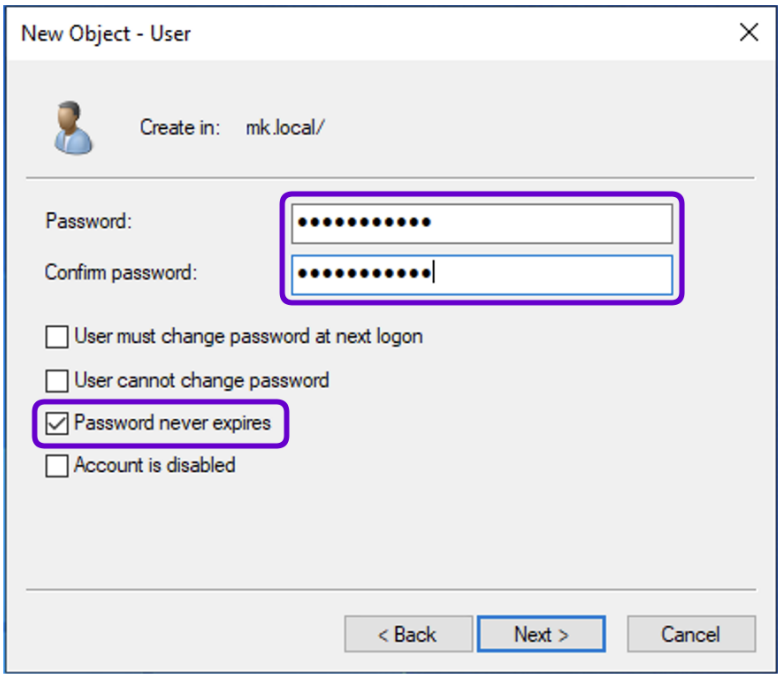
1. Zaloguj się na serwerze, na którym chcesz skonfigurować SSO, używając konta administratora.
2. Uruchom aplikację *Server Manager*.
3. Kliknij przycisk *Tools* w prawym górnym rogu okna, aby rozwinąć listę menu i wybierz *Active Directory Users and Computers*.



4. W oknie menedżera rozwiń katalogi domeny, ewentualnie grupy użytkowników i kliknij prawym przyciskiem myszy na katalog *Users* .
5. Wybierz *New* > *User*.
6. Utwórz użytkownika, który będzie używał SSO do logowania się do Fudo Enterprise. W tym przykładzie będzie to `User logon name: ad-user1`).

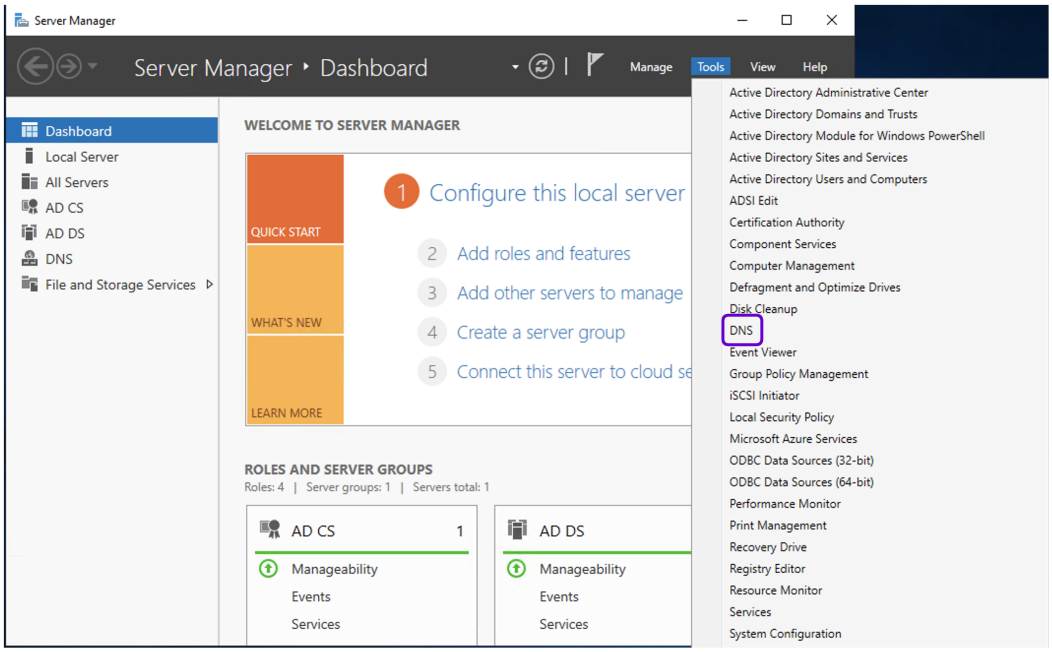


7. Kliknij *Next*.
8. Podaj hasło dla utworzonego użytkownika (np. `PaSSwOrD`) i wybierz opcję *Hasło nigdy nie wygasa*.
9. Kliknij *Next* i *Finish*.

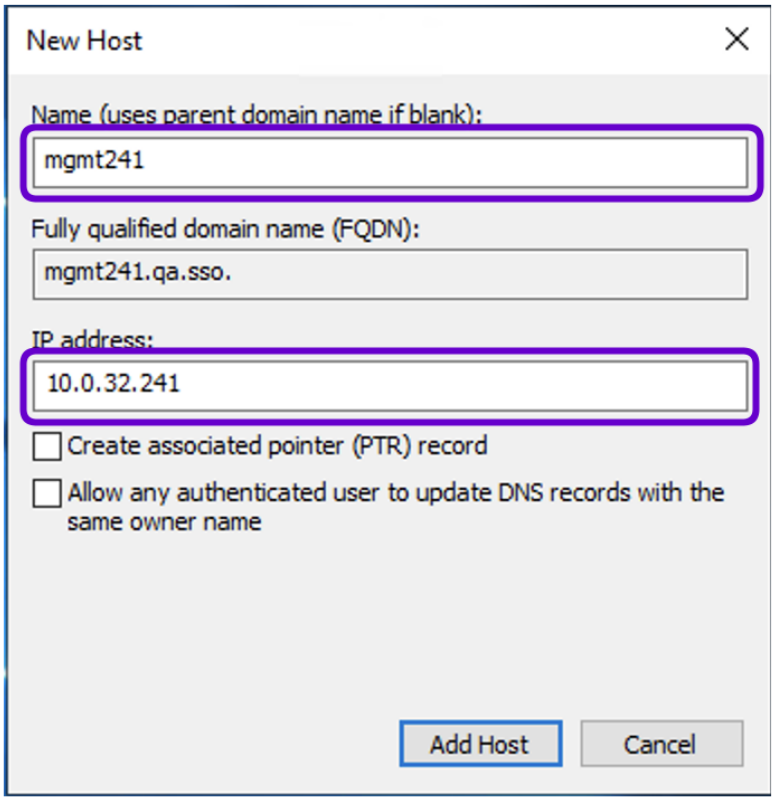


Konfiguracja wpisów DNS:

1. Uruchom aplikację *Server Manager*.
2. Kliknij przycisk *Tools* w prawym górnym rogu okna, aby rozwinąć listę menu i wybierz *DNS*.

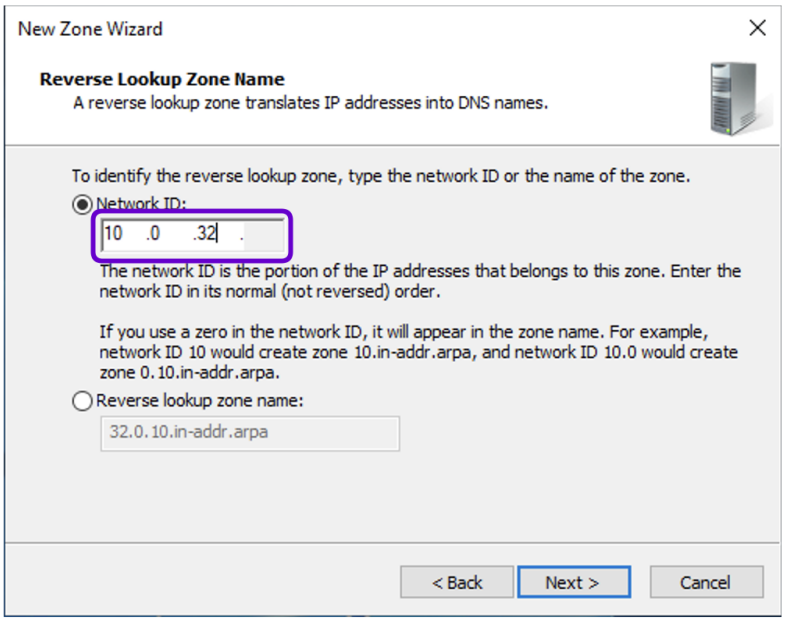


3. Przejdź do *Forward Lookup Zones*, kliknij prawym przyciskiem myszy na nazwę domeny i wybierz *New Host.*
4. Podaj *Nazwę* i *Adres IP* Panelu Administracyjnego Fudo Enterprise (np: `mgmt241.qa.sso, 10.0.32.241`).
5. Kliknij *Add Host.*

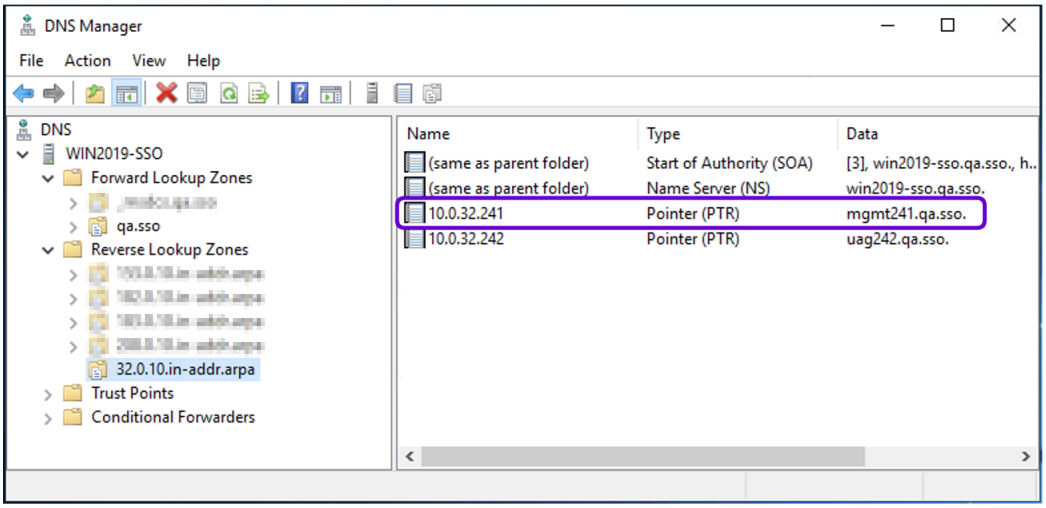


6. Kliknij prawym przyciskiem myszy na *Reverse Lookup Zone* i wybierz *New Zone.*

7. Kliknij *Next.*
8. Wybierz opcję *Primary zone* i kliknij *Next.*
9. Wybierz opcję *To all DNS servers running on domain controllers in this domain:* i kliknij *Next.*
10. Wybierz opcję *IPV4 Reverse Lookup Zone* i kliknij *Next.*
11. W polu *Network ID* wpisz początek zakresu podsieci dla swojej sieci (np. `10.0.32`) i kliknij *Next.*



12. Wybierz opcję aktualizacji (np. *Allow only secure dynamic updates*) i kliknij *Next.*
13. Kliknij *Finish.*
14. Kliknij prawym przyciskiem myszy na utworzoną strefę `32.0.10.in-addr.arpa` i wybierz *New Pointer (PTR).*
15. Podaj adres IP hosta oraz nazwę hosta Panelu Administracyjnego (np: `10.0.32.241` i `mgmt241.qa.sso`).



Utwórz bilet Kerberos:

1. Uruchom poniższe polecenie w konsoli Powershell lub CMD:

   ```
   ktpass -princ HTTP/hostname.yourdomain.local@yourdomain.local
   -mapuser netbios_domain_name\username -pass password -ptype
   KRB5_NT_PRINCIPAL -out hostname.yourdomain.local.keytab
   ```

   - Przykład:

   ```
   ktpass -princ HTTP/mgmt241.qa.sso@QA.SSO -mapuser QA\ad-user1 -pass
   PaSSwOrD -ptype KRB5_NT_PRINCIPAL -out mgmt241.qa.sso.keytab
   ```

2. Skopiuj utworzony plik na stację roboczą użytkownika, na której będziesz konfigurować Fudo Enterprise.

28.5.2 Konfiguracja Fudo Enterprise

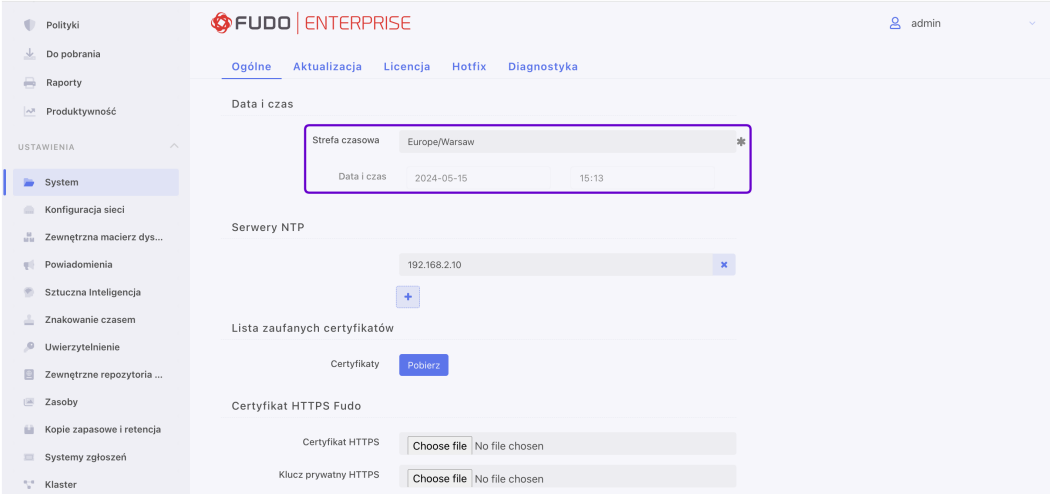
Informacja: Ten przypadek użycia opisuje, jak skonfigurować Fudo Enterprise przy użyciu metody zewnętrznego uwierzytelnienia Active Directory. Należy pamiętać, że można dostosować uwierzytelnienie użytkowników za pomocą innej metody obsługiwanej przez Fudo Enterprise, aby dopasować ją do swoich specyficznych wymagań, metod typowo stosowanych w środowisku i scenariuszy pracy.

Konfiguracja SSO:

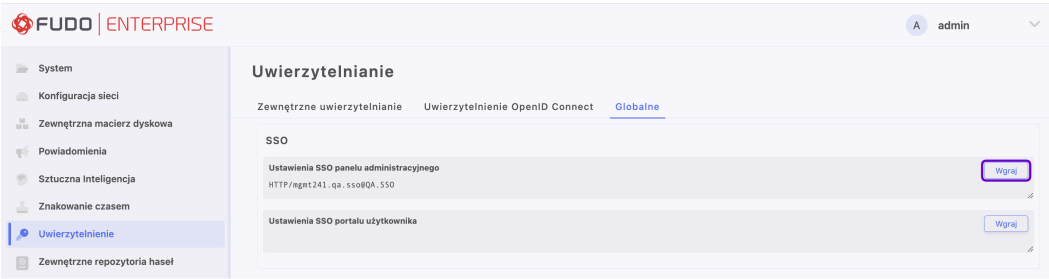
Aby zdefiniować parametry usługi SSO w Fudo Enterprise, wykonaj następujące kroki:

1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise używając danych uwierzytelniających użytkownika z rolą `superadmin`.
2. Wybierz *Ustawienia* > *Uwierzytelnianie*.
3. W sekcji *Data i czas* sprawdź, czy wybrana strefa czasowa jest zgodna z konfiguracją strefy czasowej klienta Windows.

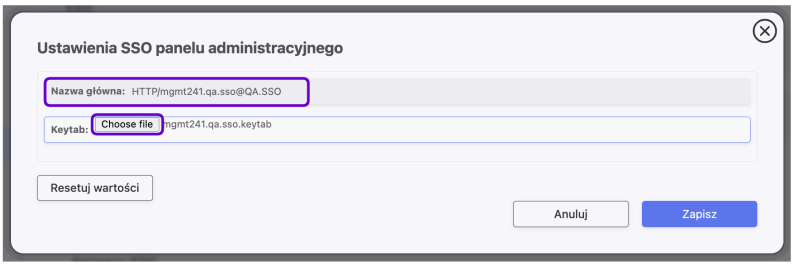
Ostrzeżenie: Strefa czasowa Fudo Enterprise musi być zgodna z konfiguracją strefy czasowej klienta Windows.



4. Wybierz *Ustawienia* > *Uwierzytelnianie*.
5. Przejdź do zakładki *Globalne*.
6. W sekcji *SSO* kliknij przycisk *Prześlij* obok pola *Ustawienia SSO panelu administracyjnego*.



7. W polu *Nazwa główna* podaj identyfikator usługi, który będzie parował konto użytkownika z instancją usługi (np. `HTTP/mgmt241.qa.sso@QA.SSO`).
8. W polu *Keytab* prześlij plik keytab zawierający ID użytkownika i klucze szyfrowania używane do szyfrowania i deszyfrowania biletów Kerberos (wygenerowany w poprzednich krokach plik `mgmt241.qa.sso.keytab`).



9. Kliknij *Zapisz*.

Informacja: Możesz również skonfigurować SSO dla Portalu Użytkownika, przesy-

łając odpowiednio skonfigurowany plik keytab w polu *Ustawienia SSO portalu użytkownika*. Pamiętaj, że podczas etapu konfigurowania środowiska Windows należy użyć adresu IP przydzielonego dla Portalu Użytkownika.

Konfiguracja DNS:

1. Przejdź do *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Nazwa i DNS*.
3. W polu *Nazwa hosta* wpisz nazwę w podanym formacie: `hostname.yourdomain.local` (np. `mgmt241.qa.sso`).
4. Skonfiguruj serwer DNS tak, aby wskazywał na serwer DNS w domenie `yourdomain.local` (w tym przykładzie użyjemy adresu IP kontrolera domeny):
    - Kliknij *Dodaj serwer DNS*, aby zdefiniować nowy serwer DNS.
    - Wpisz adres IP serwera DNS (np. `10.0.242.100`).
    - Kliknij *Zapisz*.

Konfiguracja metody zewnętrznego uwierzytelnienia:

1. Zaloguj się do Panelu Administratora Fudo Enterprise.
2. Wybierz *Ustawienia* > *Uwierzytelnienie*.
3. W karcie **Zewnętrzne uwierzytelnianie** kliknij *Dodaj zewnętrzne uwierzytelnianie*.
4. W polu *Nazwa* wpisz nazwę dla tworzonej konfiguracji.
5. Ustaw *Adres źródłowy* na *Dowolny*.
6. W polu *Ogólne* wybierz *Active Directory*.
7. W polu *Host* podaj adres IP kontrolera domeny (np. `10.0.242.100`).
8. Pozostaw domyślny numer portu: `389`.
9. Podaj nazwę domeny, która będzie używana do uwierzytelnienia użytkowników w Active Directory (np. `qa.sso`).
9. W polach *Login użytkownika uprzywilejowanego* i *Sekret* podaj dane logowania uprzywilejowanego konta używanego do dostępu do kontrolera domeny.
10. Kliknij *Zapisz*.

Utwórz użytkownika w Fudo:

> **Ostrzeżenie:** Konfiguracja **Single Sign On** jest dostępna tylko dla użytkowników z rolą `superadmin`, i może być używana przez użytkowników z rolami `operator`, `admin`, i `superadmin`.

1. Wybierz *Zarządzanie* > *Użytkownicy* i kliknij + *Dodaj użytkownika*.
2. Wpisz nazwę użytkownika odpowiadającą wybranemu kontu użytkownika w Active Directory (np. `ad-user1`).
3. Wybierz rolę `Admin`.

4. W karcie *Ustawienia*, w sekcji *Sejfy*, wybierz *main,* aby przyznać użytkownikowi prawa dostępu do Panelu Administracyjnego.
5. 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. Przejdź do zakładki *Dane użytkownika* i w polach *Domena Fudo* i *Domena AD* wpisz nazwę domeny skonfigurowanej na serwerze *Active Directory*. W tym przykładzie będzie to `qa.sso`.

Informacja: Zarówno *Domena Fudo,* jak i *Domena AD* powinny odpowiadać nazwie domeny podanej w bilecie Kerberos.

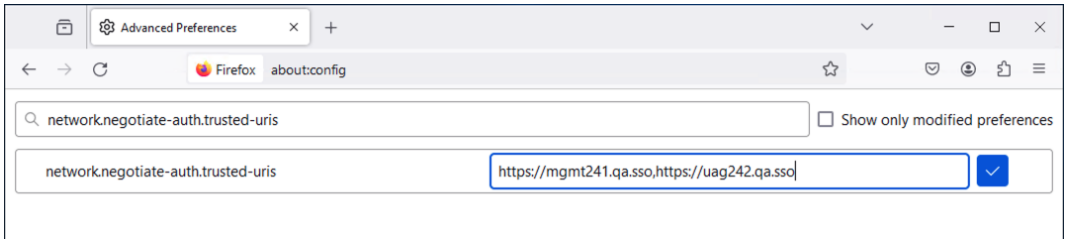
---

9. W razie potrzeby uzupełnij pozostałe parametry zgodnie z wymaganiami swojej specyficznej konfiguracji. Po więcej szczegółów przejdź do sekcji *Dodawanie użytkownika*.
9. Kliknij *Zapisz i zamknij*.

28.5.3 Konfiguracja i sprawdzenie stacji roboczej użytkownika - klienta Windows 2010

Konfiguracja przeglądarki Firefox:

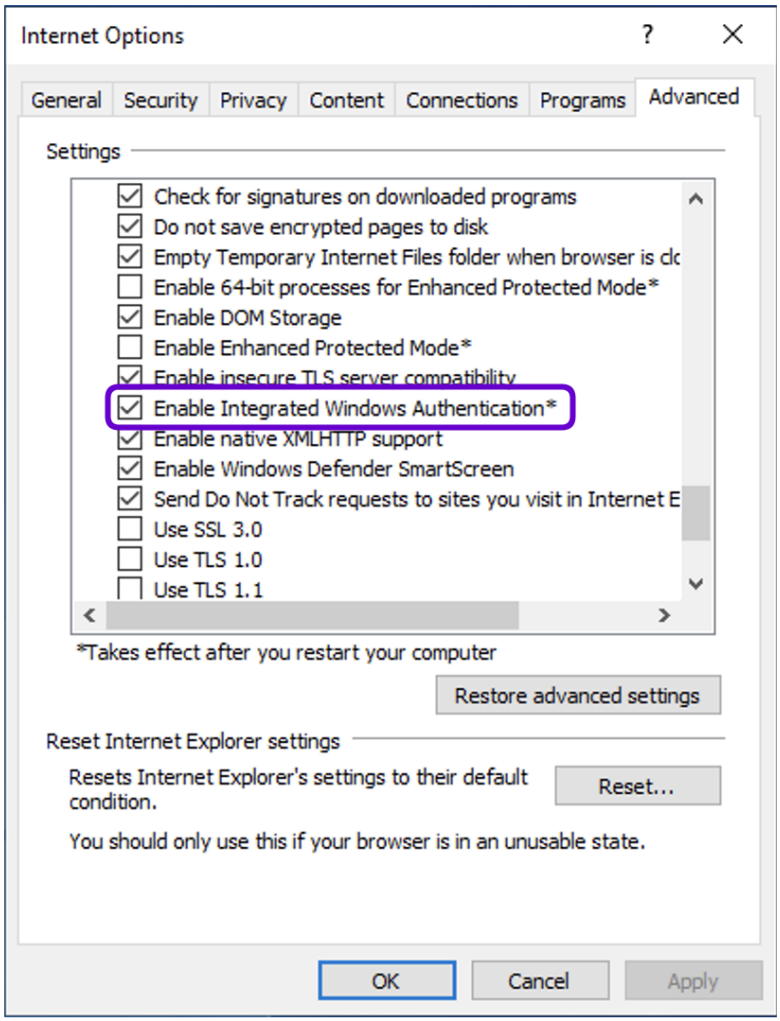
1. Zaloguj się na klienta Windows używając konta `ad-user1`.
2. Otwórz przeglądarkę *Firefox,* wpisz `about:config` w pasku adresu i wciśnij *Enter*.
3. Kliknij opcję *Akceptuj ryzyko i kontynuuj,* aby potwierdzić wyświetlony komunikat ostrzegawczy.
4. W pasku wyszukiwania na górze wpisz `network.negotiate-auth.trusted-uris`.
5. Kliknij dwukrotnie na `network.negotiate-auth.trusted-uris` i wprowadź wybrany FQDN (Pełna Nazwa Kwalifikowana Domeny) wraz z protokołem, rozdzielając wpisy przecinkiem (np: `https://mgmt241.qa.sso,https://uag242.qa.sso)`.
6. Naciśnij *Enter,*, aby zapisać zmiany.



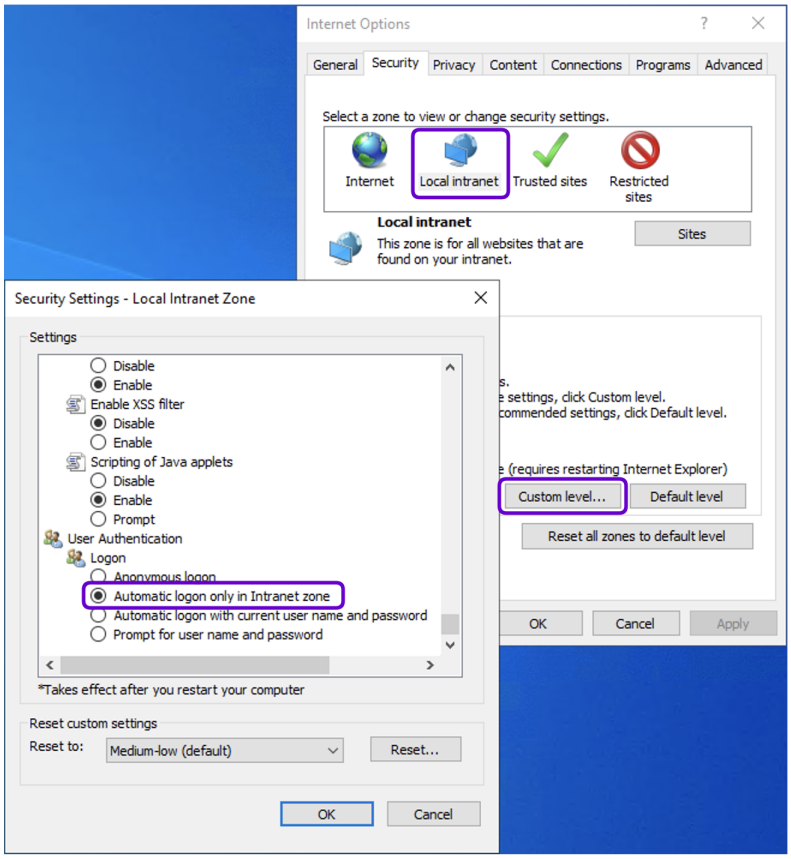
7. Następnie w pasku wyszukiwania wpisz `network.automatic-ntlm-auth.trusted-uris`.
8. Kliknij dwukrotnie na `network.automatic-ntlm-auth.trusted-uris` i wprowadź wybrany FQDN (Pełna Nazwa Kwalifikowana Domeny) wraz z protokołem, rozdzielając wpisy przecinkiem (np: `https://mgmt241.qa.sso,https://uag242.qa.sso`).
9. Naciśnij *Enter*, aby zapisać zmiany.
10. Uruchom ponownie przeglądarkę.

Konfiguracja przeglądarki Internet Explorer:

1. Przejdź do *Narzędzia* > *Opcje internetowe* > *Zaawansowane*.
2. W zakładce *Zaawansowane* i sekcji *Zabezpieczenia* zaznacz *Włącz zintegrowane uwierzytelnianie Windows*.



3. W zakładce *Zabezpieczenia* wybierz *Intranet lokalny*.
4. Kliknij *Poziom niestandardowy*.
5. W sekcji *Uwierzytelnianie użytkownika/Logowanie* wybierz *Automatyczne logowanie tylko w strefie Intranet*.



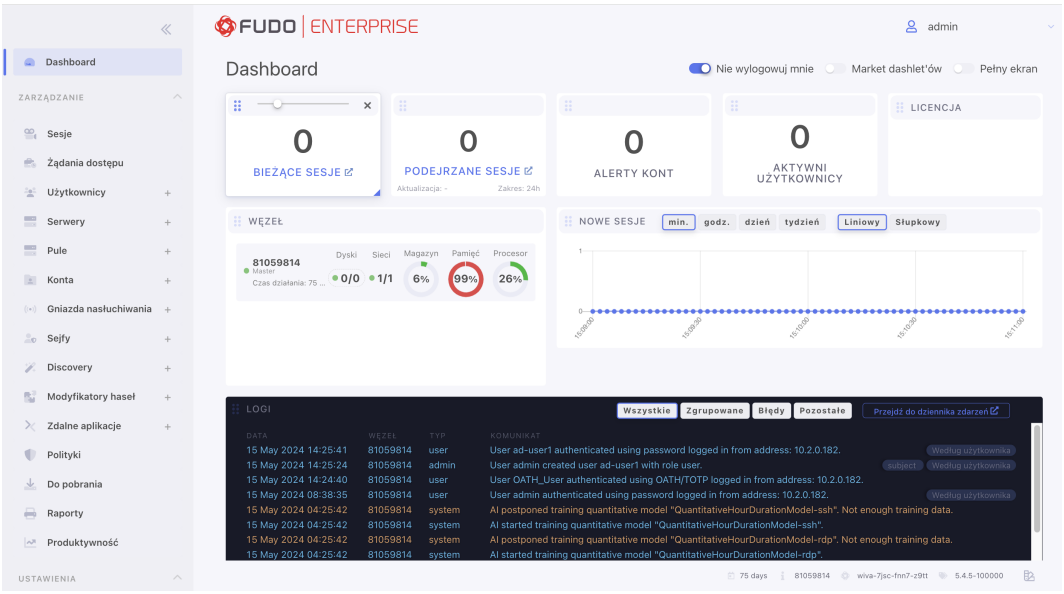
6. Kliknij *OK*.
7. Kliknij *Witryny* i zaznacz wszystkie pola wyboru.‘
8. Kliknij *Zaawansowane* i dodaj stronę usługi Remedy SSO do strefy lokalnej (w naszym przykładzie to `https://mgmt241.qa.sso`).
9. Kliknij *Dodaj*.
10. Kliknij *OK* we wszystkich oknach dialogowych.
11. Uruchom ponownie przeglądarkę.

Konfiguracja przeglądarki Chrome:

Google Chrome obsługuje uwierzytelnianie Kerberos. Po skonfigurowaniu Internet Explorera nie są potrzebne dodatkowe ustawienia dla Google Chrome, ponieważ korzysta on z konfiguracji Internet Explorera.

Logowanie do Panelu Administracyjnego za pomocą SSO:

1. Otwórz przeglądarkę *Firefox* i w pasku adresu wpisz wcześniej zdefiniowany FQDN (w naszym przykładzie to `https://mgmt241.qa.sso`).
2. Jeśli proces konfiguracji SSO przebiegł prawidłowo, w oknie przeglądarki pojawi się pulpit Panelu Administracyjnego Fudo Enterprise.



Tematy pokrewne:

- *Single Sign On*
- *Uwierzytelnienie*

ROZDZIAŁ 29

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 nieuprawionego dostępu do monitorowanych serwerów?

6. Czy możliwe jest ukrycie ekranu logowania podczas nawiązywania połączeń RDP?

7. Dlaczego lista użytkowników we właściwościach połączenia jest niekompletna?

8. Dlaczego użytkownik usunięty z serwera LDAP/AD w dalszym ciągu widoczny jest na Fudo 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 muszę nagrać, aby zobaczyć wyniki?

14. Mamy 20 kont i 20 użytkowników w firmie - ile czasu zajmie zauważenie różnic w zachowaniu użytkowników?

15. Jeśli łączę się do różnych serwerów, czy Fudo tworzy osobny model dla każdego z nich?

16. Jeśli przekażę swoje dane logowania innej osobie, czy sztuczna inteligencja stwierdzi, że zalogował się ktoś inny i przerwie połączenie?

17. Ikonka statusu sesji jest stale żółta - co to oznacza?

18. Pięciu użytkowników korzysta z tego samego konta do nawiązywania połączeń - czy system będzie w stanie stwierdzić kto i kiedy łączył się z serwerem?

19. W jaki sposób system będzie w stanie stwierdzić, że to ktoś inny zalogował się do systemu, skoro wszyscy wykonujemy te same komendy?

20. Dlaczego moje sesje nie są analizowane?

1. Jaka jest maksymalna ilość nagranych sesji na Fudo 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 upłynięciu 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 przypadki eksportu do formatu video, rozmiar wynikowy pliku zależy od wybranego kodowania strumienia video oraz wybranej rozdzielczości nagrania.

4. W jaki sposób użytkownicy mogą ukrywać swoje działania na serwerach, do których mają skonfigurowane połączenia na Fudo 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 muszę nagrać, aby zobaczyć wyniki?

Modele są trenowane zgodnie z ustawieniami terminarza w konfiguracji *Sztucznej inteligencji*.

- W przypadku modelu SSH, wytrenowanie modelu wymaga minimum 65 sesji (każda musi zawierać co najmniej 25 unikatowych komend) oraz 5 unikatowych predyktorów (np. użytkowników). Uzyskanie optymalnych wyników wymaga 300 sesji dla każdego predyktora i 10 unikatowych predyktorów.
- Dla modelu RDP, minimum konieczne do wytrenowania modelu, to 5 godzin nagrań dla pojedynczego predyktora. Optymalne wyniki uzyskuje się przy 30 godzinach nagrań i 10 unikatowych predyktorach.

14. Mamy 20 kont i 20 użytkowników w firmie - ile czasu zajmie zauważenie różnic w zachowaniu użytkowników?

Czas jest ściśle uzależniony od dostępności zarejestrowanych sesji. Jeśli jest wystarczająca ilość danych do zbudowania modelu, system będzie w stanie wykryć zmiany w zachowaniu użytkowników w jeden dzień po nagraniu pierwszej sesji dla danego predyktora (użytkownika).

- W przypadku modelu SSH, wytrenowanie modelu wymaga minimum 65 sesji (każda musi zawierać co najmniej 25 unikatowych komend) oraz 5 unikatowych predyktorów (np. użytkowników). Uzyskanie optymalnych wyników wymaga 300 sesji dla każdego predyktora i 10 unikatowych predyktorów.
- Dla modelu RDP, minimum konieczne do wytrenowania modelu, to 5 godzin nagrań dla pojedynczego predyktora. Opymalne wyniki uzyskuje się przy 30 godzinach nagrań i 10 unikatowych predyktorach.

15. Jeśli łączę się do różnych serwerów, czy Fudo tworzy osobny model dla każdego z nich?

Fudo 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*.

ROZDZIAŁ 30

Słownik pojęć

AAPM Moduł AAPM (Application to Application Password Manager) umożliwiający bezpieczną wymianę haseł pomiędzy aplikacjami.

Active Directory Usługa uwierzytelniania i autoryzacji użytkowników w domenie Windows.

AD Active Directory - usługa uwierzytelnienia i autoryzacji użytkowników w domenie Windows.

ARP Address Resolution Protocol - protokół mapujący adresy warstwy trzeciej (adresy IP) na fizyczne adresy warstwy łącza danych (adresy MAC).

Azure Microsoft Azure - platforma chmurowa firmy Microsoft, udostępniająca mechanizmy pozwalające przetwarzać oraz składować dane.

broker połączeń RDP Mechanizm zarządzania sesjami dostępowymi do maszyn będących częścią farmy serwerów.

CERB Kompleksowe rozwiązanie uwierzytelniania i autoryzacji użytkowników, wspierające metody uwierzytelniania tj. token mobilny (aplikacja na telefon komórkowy), hasło statyczne, hasła jednorazowe SMS.

certyfikat CA Certyfikat urzędu certyfikacji.

Czułość Czułość (ang. True Positive Rate) - to procent wszystkich złośliwych (malicious) sesji rozpoznanych przez model jako podejrzane (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.

Kerberos Protokół uwierzytelniania sieciowego wykorzystujący kryptografię klucza symetrycznego do zapewnienia bezpiecznej weryfikacji tożsamości w aplikacjach klient-serwer.

Klucz publiczny Metoda uwierzytelniania, w której tożsamość użytkownika ustalana jest na podstawie pary kluczy - prywatny (będący tylko w posiadaniu użytkownika) i publiczny (udostępniany innym podmiotom).

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

LDAP Lightweight Directory Access Protocol - protokół dostępu i zarządzania rozproszonymi usługami katalogowymi w sieciach IP.

modyfikator haseł Narzędzie służące do zmiany hasła do konta na monitorowanym serwerze.

notacja CIDR Skrócona notacja adresów sieciowych, w której adres IP zapisywany jest zgodnie z notacją IPv4, a maska podawana jest w postaci liczby wiodących cyfr «1» w zapisie bitowym (192.168.1.1 - 255.255.255.0; 192.168.1.1/24).

OATH Open Authentication - otwarty standard bezpiecznego, dwuskładnikowego uwierzytlenienia użytkowników i urządzeń.

OCR Optical Character Recognition - przetwarzanie obrazów pod kątem identyfikacji i indeksacji tekstów.

Odcisk Palca Fingerprint - ciąg znaków będący działaniem funkcji skrótu na danych wejściowych, pozwalający jednoznacznie stwierdzić, czy dane nie zostały zmienione.

Okta Okta - to narzędzie klasy enterprise do zarządzania dostępami oraz tożsamościami cyfrowymi pracowników.

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.

SSO Jest to proces uwierzytelniania użytkownika, który pozwala na dostęp do wielu aplikacji za pomocą jednego zestawu danych logowania, zwiększając wygodę i bezpieczeństwo poprzez redukcję potrzeby posiadania wielu haseł.

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.

Indeks

A

AAPM, **570**
Active Directory, **570**
AD, **570**
administracja
    aktualizacja systemu, 339
    import/eksport konfiguracji, 412
    pierwsze uruchomienie, 40
    ponowne uruchomienie, 402
    przywracanie poprzedniej wersji, 401
API
    użytkownicy, 127
ARP, **570**
Azure, **570**

B

blokowanie
    serwery, 166
broker połączeń RDP, **570**
broker połączeń RDP, 446

C

CERB, **570**
certyfikat CA, **570**
Czułość, **570**

D

DHCP, **570**
DNS, **570**
DNS
    konfiguracja, 362
dodawanie
    serwery, 149
DoS (*Denial of Service*), **570**
dostęp SSH, **570**
DUO, **570**

E

Efficiency Analyzer/Productivity Analyzer, **571**

F

FPR, **571**
fudopv, **571**

G

gniazda nasłuchiwania
    HTTP, 210
    konfiguracja, 198
    Modbus, 215
    MS SQL, 221
    MySQL, 217
    RDP, 203
    SSH, 200
    TCP, 219
    Telnet, 223
    Telnet 3270, 226
    Telnet 5250, 229
    VNC, 207
gniazdo nasłuchiwania, **571**
grupa redundancji, **571**

H

Hasło statyczne, **571**
heartbeat, **571**
hot-swap, **571**
HTTP
    gniazda nasłuchiwania, 210
    protokoły, 8
    protokół, 8
    serwery, 149

I

import
    serwery, 164

K

Kerberos, **571**

Klucz publiczny, **571**
konfiguracja
    AI, 367
    gniazda nasłuchiwania, 198
    model danych, 31
    powiadomienia, 364
    serwery, 149
    synchronizacja użytkowników, 144
    ustawienia sieciowe, 351, 360
    użytkownicy, 125
konto, **571**

L

LDAP, **571**

M

Modbus
    gniazda nasłuchiwania, 215
    protokoły, 9
    protokół, 9
    serwery, 151
model danych
    serwer, 31
    użytkownik, 31
modyfikator haseł, **571**
modyfikowanie
    serwery, 166
MS SQL
    gniazda nasłuchiwania, 221
    serwery, 152
MS SQL (*TDS*)
    protokoły, 10
    protokół, 10
MySQL
    gniazda nasłuchiwania, 217
    protokoły, 10
    protokół, 10
    serwery, 154

N

notacja CIDR, **571**

O

OATH, **571**
OCR, **571**
odblokowanie
    serwery, 167
Odcisk Palca, **571**
Okta, **571**
OpenID Connect, **571**

P

polityka, **572**
polityka czasowa, **572**
Prawdopodobieństwa zagrożenia, **572**
protocol
    secret, 21
protocols
    secret, 21
protokoły
    HTTP, 8
    Modbus, 9
    MS SQL (*TDS*), 10
    MySQL, 10
    RDP, 11
    SSH, 14
    TCP, 21
    Telnet, 19
    Telnet 3270, 18
    Telnet 5250, 19
    VNC, 20
    X11, 21
protokół
    HTTP, 8
    Modbus, 9
    MS SQL (*TDS*), 10
    MySQL, 10
    RDP, 11
    SSH, 14
    TCP, 21
    Telnet, 19
    Telnet 3270, 18
    Telnet 5250, 19
    VNC, 20
    X11, 21
PSM (*Privileged Session Management*), **572**

R

RADIUS, **572**
RDP, **572**
RDP
    gniazda nasłuchiwania, 203
    protokoły, 11
    protokół, 11
    serwery, 155
repozytorium haseł, **572**
retencja, **572**

S

scenariusze wdrożenia
    bastion, 25
    brama, 24

most, 22
pośrednik, 25
wymuszony routing, 23
secret
protocol, 21
protocols, 21
sejf, **572**
sejf anonimowy, **572**
serwer, **572**
Serwery, **572**
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, 296
dołączanie do trwającej sesji, 308
eksportowanie, 314
filtrowanie, 298
komentowanie, 311
odtwarzanie i podgląd, 300
SMS, **572**
SSH, **572**
SSH
gniazda nasłuchiwania, 200
protokoły, 14
protokół, 14
ssh
serwery, 156
SSO, **572**
synchronizacja użytkowników, 144
konfiguracja, 144
Syslog, **572**

T

TCP
gniazda nasłuchiwania, 219
protokoły, 21
protokół, 21
serwery, 163
Telnet
gniazda nasłuchiwania, 223
protokoły, 19
protokół, 19
serwery, 158
Telnet 3270
gniazda nasłuchiwania, 226
protokoły, 18
protokół, 18
serwery, 159
Telnet 5250
gniazda nasłuchiwania, 229
protokoły, 19
protokół, 19
serwery, 161
tryb połączenia
transparentny, 24

U

ustawienia sieciowe
ARP, 364
etykiety adresów IP, 360
konfiguracja interfejsów, 351
serwery DNS, 362
trasa routingu, 361
usuwanie
serwery, 167
użytkownicy, 125
API, 127
konfiguracja, 125
prawa dostępu, 127, 142
role, 127, 142
użytkownik, **572**

V

VLAN, **572**
VNC, **572**
VNC
gniazda nasłuchiwania, 207
protokoły, 20
protokół, 20
serwery, 162

W

WWN, **572**

X

X11
protokoły, 21

protokół, 21

Z

zewnętrzny serwer uwierzytelnienia, **573**
znacznik czasu, **573**