

Fudo Enterprise 6.0 - Dokumentacja Systemu

Fudo Security

15.04.2026

Spis treści

1 O dokumentacji **1**

2 Motywy kolorystyczne Panelu Administracyjnego **2**

3 Wstęp **4**

3.1 Przegląd systemu . . . 4
3.1.1 Monitorowanie i nagrywanie sesji . . . 4
3.1.2 Zarządzanie hasłami . . . 5
3.1.3 Dostęp Just-in-Time (JIT) . . . 5
3.1.4 Single Sign-On (SSO) . . . 6
3.1.5 Bezagentowy wygodny dostęp . . . 6
3.1.6 Zapobieganie naruszeniom oparte na Sztucznej Inteligencji . . . 6
3.1.7 Analiza produktywności . . . 6
3.1.8 Szybkie wdrożenie . . . 6
3.1.9 Wsparcie dla zgodności . . . 6
3.2 Dostępne języki interfejsu . . . 7
3.3 Licencjonowanie . . . 7
3.4 Wspierane protokoły . . . 10
3.4.1 HTTP . . . 10
3.4.2 Modbus . . . 11
3.4.3 MS SQL (TDS) . . . 11
3.4.4 MySQL . . . 12
3.4.5 PostgreSQL . . . 12
3.4.6 RDP . . . 13
3.4.7 SSH . . . 16
3.4.8 Telnet 3270 . . . 20
3.4.9 Telnet 5250 . . . 21
3.4.10 Telnet . . . 21
3.4.11 VNC . . . 22
3.4.12 X11 . . . 23
3.4.13 TCP . . . 23
3.4.14 Pobranie hasła . . . 23
3.5 Scenariusze wdrożenia . . . 24
3.6 Tryby połączenia . . . 25
3.7 Metody i tryby uwierzytelniania użytkowników . . . 27
3.8 Mechanizmy bezpieczeństwa . . . 30

3.8.1 Szyfrowanie danych . . . 30
3.8.2 Kopie zapasowe . . . 30
3.8.3 Uprawnienia użytkowników . . . 30
3.8.4 Sandboxing . . . 31
3.8.5 Niezawodność . . . 31
3.8.6 Konfiguracja klastrowa . . . 31
3.9 Model danych . . . 32
3.10 Dashboard . . . 33
3.10.1 Widgety . . . 34
3.10.2 Zarządzanie widgetami . . . 34
3.10.3 Status dysków . . . 35
3.11 Licencje produktów stron trzecich . . . 36

4 Instalacja i pierwsze uruchomienie 37
4.1 Wymagania . . . 37
4.2 Urządzenie . . . 39
4.3 Pierwsze uruchomienie . . . 41
4.3.1 Środowisko wirtualne . . . 45
4.4 Dostęp do portali Fudo Enterprise . . . 51
4.4.1 Panel Administracyjny . . . 51
4.4.2 Portal Użytkownika . . . 52
4.4.3 Obsługiwane przeglądarki internetowe . . . 53
4.4.4 Obsługiwane przeglądarki internetowe . . . 53

5 Szybki start 54
5.1 SSH . . . 54
5.1.1 Założenia . . . 54
5.1.2 Konfiguracja . . . 54
5.1.3 Nawiązanie połączenia . . . 59
5.1.4 Podgląd sesji połączeniowej . . . 60
5.2 SSH w trybie bastionu . . . 61
5.2.1 Założenia . . . 61
5.2.2 Konfiguracja . . . 61
5.2.3 Nawiązanie połączenia . . . 66
5.2.4 Podgląd sesji połączeniowej . . . 68
5.3 SSH w trybie bastionu z opcją Jump Host . . . 68
5.3.1 Założenia . . . 69
5.3.2 Konfiguracja . . . 69
5.3.3 Nawiązanie połączenia . . . 73
5.4 RDP . . . 74
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 RDP w trybie bastionu . . . 82
5.5.1 Założenia . . . 83
5.5.2 Konfiguracja . . . 83
5.5.3 Nawiązanie połączenia . . . 87
5.5.4 Podgląd sesji połączeniowej . . . 89
5.6 Telnet . . . 90
5.6.1 Założenia . . . 91
5.6.2 Konfiguracja . . . 91

5.6.3 Nawiązanie połączenia . . . 94
5.6.4 Podgląd sesji połączeniowej . . . 95
5.7 Telnet 5250 . . . 96
5.7.1 Założenia . . . 96
5.7.2 Konfiguracja . . . 96
5.7.3 Nawiązanie połączenia . . . 100
5.7.4 Podgląd sesji połączeniowej . . . 102
5.8 PostgreSQL . . . 103
5.8.1 Założenia . . . 103
5.8.2 Przegląd architektury . . . 104
5.8.3 Konfiguracja . . . 104
5.8.4 Nawiązywanie połączenia PostgreSQL . . . 109
5.9 MySQL . . . 110
5.9.1 Założenia . . . 111
5.9.2 Konfiguracja . . . 111
5.9.3 Nawiązanie połączenia . . . 115
5.9.4 Podgląd sesji połączeniowej . . . 115
5.10 MS SQL . . . 116
5.10.1 Założenia . . . 117
5.10.2 Konfiguracja . . . 118
5.10.3 Nawiązanie połączenia . . . 122
5.10.4 Podgląd sesji połączeniowej . . . 122
5.11 HTTP . . . 123
5.11.1 Założenia . . . 124
5.11.2 Konfiguracja . . . 124
5.11.3 Nawiązanie połączenia . . . 129
5.11.4 Podgląd sesji połączeniowej . . . 130
5.12 VNC . . . 131
5.12.1 Założenia . . . 132
5.12.2 Konfiguracja . . . 132
5.12.3 Nawiązanie połączenia . . . 136
5.12.4 Podgląd sesji połączeniowej . . . 136

6 Sesje **138**
6.1 Filtrowanie sesji . . . 140
6.1.1 Definiowanie filtrów . . . 140
6.1.2 Zapisywanie filtrów niestandardowych . . . 141
6.1.3 Stosowanie filtrów niestandardowych . . . 141
6.1.4 Edycja filtrów niestandardowych . . . 142
6.1.5 Wyłączanie filtrów . . . 142
6.1.6 Usuwanie filtrów niestandardowych . . . 143
6.1.7 Wyszukiwanie pełnotekstowe . . . 143
6.2 Odtwarzanie sesji . . . 144
6.3 Wstrzymywanie sesji . . . 151
6.4 Przerywanie połączenia . . . 152
6.5 Dołączanie do sesji . . . 153
6.6 Udostępnianie sesji . . . 154
6.7 Komentowanie sesji . . . 156
6.8 Zarządzanie retencją sesji . . . 158
6.9 Eksportowanie sesji . . . 159
6.9.1 Dostępne formaty plików eksportu sesji . . . 161

6.10 Usuwanie sesji . . . 162
6.11 Przetwarzanie OCR sesji . . . 163
6.12 Replikacja sesji w konfiguracji klastrowej . . . 165
6.13 Znakowanie czasem sesji . . . 167
6.14 Wymagane potwierdzenie dostępu . . . 168
6.14.1 Akceptowanie żądań użytkowników . . . 169
6.14.2 Odrzucanie żądań użytkowników . . . 170
6.15 AI - Analiza behawioralna sesji . . . 170
6.16 AI - Podsumowanie sesji przy użyciu sztucznej inteligencji [BETA] . . . 173

7 Żądania dostępu 177
7.1 Żądania oczekujące . . . 179
7.2 Żądania aktywne . . . 180
7.3 Archiwum żądań . . . 181

8 Raporty 182
8.1 Subskrybowanie raportu cyklicznego . . . 183
8.2 Rezygnacja z subskrypcji raportu cyklicznego . . . 184
8.3 Generowanie raportu na żądanie . . . 184
8.4 Wyświetlanie i zapisywanie raportów . . . 185
8.5 Usuwanie raportów . . . 186

9 Zarządzanie użytkownikami 187
9.1 Użytkownicy . . . 187
9.1.1 Dodawanie użytkownika . . . 188
9.1.2 Modyfikowanie użytkownika . . . 195
9.1.3 Blokowanie użytkownika . . . 196
9.1.4 Odblokowanie użytkownika . . . 198
9.1.5 Usuwanie użytkownika . . . 199
9.1.6 Zliczanie niepowodzeń uwierzytelnienia . . . 200
9.2 Grupy (RBAC) . . . 201
9.2.1 Rozstrzyganie dostępu i priorytetyzacja . . . 202
9.2.2 Tworzenie grupy . . . 205
9.2.3 Modyfikowanie grup . . . 208
9.2.4 Usuwanie grup . . . 208
9.3 Kontrola dostępu oparta na rolach (RBAC) . . . 209
9.3.1 Przejście na RBAC po aktualizacji . . . 210
9.3.1.1 Zrozumienie uprawnień i zdolności . . . 210
9.3.1.2 Predefiniowane role jako punkt wyjścia . . . 211
9.3.2 Tworzenie roli . . . 216
9.3.3 Przypisywanie ról do użytkowników . . . 218
9.3.4 Modyfikowanie ról . . . 220
9.3.5 Usuwanie ról . . . 220
9.3.6 Typowe scenariusze ról i wymagane uprawnienia . . . 221
9.3.6.1 Macierz kontroli dostępu na poziomie zakładek . . . 221
9.3.6.2 Widoczność widżetów Dashboardu . . . 232
9.3.6.3 Uprawnienia do zakładki Sesje . . . 232
9.3.6.4 Uprawnienia do zakładki Pobieranie . . . 233
9.3.6.5 Zarządzanie sejfami . . . 234
9.3.6.6 Uprawnienia do żądań dostępu . . . 234
9.3.6.7 Fudo Officer . . . 235
9.3.6.8 Uprawnienia do raportów . . . 235

10 Zarządzanie sesjami **237**
10.1 Serwery . . . 237
10.1.1 Dodawanie serwera . . . 237
10.1.1.1 Dodawanie serwera HTTP . . . 237
10.1.1.2 Dodawanie serwera Modbus . . . 241
10.1.1.3 Dodawanie serwera MS SQL . . . 244
10.1.1.4 Dodawanie serwera MySQL . . . 247
10.1.1.5 Tworzenie serwera PostgreSQL . . . 251
10.1.1.6 Dodawanie serwera RDP . . . 254
10.1.1.7 Dodawanie serwera SSH . . . 257
10.1.1.8 Dodawanie serwera Telnet . . . 260
10.1.1.9 Dodawanie serwera Telnet 3270 . . . 264
10.1.1.10 Dodawanie serwera Telnet 5250 . . . 267
10.1.1.11 Dodawanie serwera VNC . . . 270
10.1.1.12 Dodawanie serwera TCP . . . 274
10.1.2 Zakresy portów w konfiguracji serwerów . . . 277
10.1.2.1 Konfiguracja zakresu portów . . . 277
10.1.2.2 Priorytetyzacja konfiguracji serwerów w przypadku konfliktu . . . 278
10.1.3 Konfiguracja serwera z odwrotnym tunelem SSH . . . 279
10.1.4 Importowanie listy serwerów z pliku CSV . . . 280
10.1.5 Modyfikowanie serwera . . . 282
10.1.6 Blokowanie serwera . . . 282
10.1.7 Odblokowanie serwera . . . 284
10.1.8 Usuwanie serwera . . . 285
10.2 Pule . . . 285
10.2.1 Dodawanie puli . . . 286
10.2.2 Usuwanie puli . . . 287
10.3 Konta . . . 287
10.3.1 Dodawanie konta . . . 288
10.3.1.1 Dodawanie konta typu *anonymous* . . . 288
10.3.1.2 Tworzenie konta typu *forward* . . . 292
10.3.1.3 Tworzenie konta typu *regular* . . . 299
10.3.2 Edytowanie konta . . . 308
10.3.3 Blokowanie konta . . . 309
10.3.4 Odblokowywanie konta . . . 311
10.3.5 Usuwanie konta . . . 312
10.3.6 Zarządzanie ostrzeżeniami bezpieczeństwa . . . 313
10.3.6.1 Zmiana hasła konta . . . 313
10.3.6.2 Zignorowanie ostrzeżenia . . . 314
10.4 Gniazda nasłuchiwania . . . 315
10.4.1 Dodawanie gniazda nasłuchiwania . . . 315
10.4.1.1 Konfigurowanie gniazda nasłuchiwania SSH . . . 317
10.4.1.2 Konfigurowanie gniazda nasłuchiwania RDP . . . 320
10.4.1.3 Konfigurowanie gniazda nasłuchiwania VNC . . . 323
10.4.1.4 Konfigurowanie gniazda nasłuchiwania HTTP . . . 326
10.4.1.5 Konfigurowanie gniazda nasłuchiwania Modbus . . . 330
10.4.1.6 Konfigurowanie gniazda nasłuchiwania MySQL . . . 332
10.4.1.7 Konfigurowanie gniazda nasłuchiwania PostgreSQL . . . 335
10.4.1.8 Konfigurowanie gniazda nasłuchiwania TCP . . . 337
10.4.1.9 Konfigurowanie gniazda nasłuchiwania MS SQL . . . 338
10.4.1.10 Konfigurowanie gniazda nasłuchiwania Telnet . . . 341

10.4.1.11 Konfigurowanie gniazda nasłuchiwania Telnet 3270 343
10.4.1.12 Konfigurowanie gniazda nasłuchiwania Telnet 5250 345
10.4.2 Modyfikowanie gniazda nasłuchiwania 348
10.4.3 Blokowanie gniazda nasłuchiwania 349
10.4.4 Odblokowanie gniazda nasłuchiwania 350
10.4.5 Usuwanie gniazda nasłuchiwania 350
10.5 Sejfy 351
10.5.1 Dodawanie sejfu 352
10.5.2 Modyfikowanie sejfu 363
10.5.3 Blokowanie sejfu 364
10.5.4 Odblokowanie sejfu 365
10.5.5 Usuwanie sejfu 366
10.6 Wykrywanie (Discovery) 367
10.6.1 Tworzenie reguły 368
10.6.1.1 Tworzenie reguły dla kont 368
10.6.1.2 Tworzenie reguły dla serwerów 370
10.6.2 Zarządzanie regułami 371
10.6.3 Tworzenie skanera 371
10.6.3.1 Tworzenie skanera dla kont kontrolera domeny 371
10.6.3.2 Tworzenie skanera dla serwerów kontrolera domeny 373
10.6.3.3 Tworzenie skanera dla kont lokalnych 375
10.6.4 Zarządzanie skanerami 377
10.6.5 Zarządzanie wykrytymi kontami 377
10.6.6 Zarządzanie wykrytymi serwerami 379
10.7 Zdalne aplikacje 381
10.7.1 Dodawanie aplikacji zdalnej 381
10.7.2 Dodawanie Argumentów 382
10.7.3 Połączenie do zdalnej aplikacji przez Portal Użytkownika 385
10.7.4 Granularny dostęp do aplikacji zdalnych 385
10.7.5 Usuwanie zdalnej aplikacji 387
10.8 Polityki 387
10.8.1 Definiowanie polityki na podstawie modułu AI 388
10.8.2 Przykłady polityk opartych na module AI 390
10.8.3 Definiowanie polityki na podstawie wzorca 392
10.9 Do pobrania 395
10.9.1 Sesje 395
10.9.2 Pliki 395
10.10 Produktywność 396
10.10.1 Zestawienie 397
10.10.2 Analiza sesji 398
10.10.3 Porównanie aktywności 399

11 Skarbiec haseł **400**
11.1 Opis modułu 400
11.1.1 Struktura skarbca haseł 401
11.1.2 Przegląd architektury – model bezpieczeństwa 402
11.1.3 Rejestrowanie zdarzeń i ślad audytowy 403
11.2 Kolekcje 404
11.2.1 Tworzenie kolekcji 404
11.2.2 Zagnieżdżanie kolekcji 406
11.2.3 Dostęp do edycji kolekcji 409

11.2.3.1 Panel edycji kolekcji . . . 409
11.2.4 Przypisywanie użytkowników i grup do kolekcji . . . 411
11.2.5 Zarządzanie prawami do kolekcji . . . 412
11.2.5.1 Przypisywanie praw do obiektu użytkownikom . . . 413
11.2.5.2 Przypisywanie praw do obiektu rolom . . . 413
11.2.6 Powiadomienia kolekcji . . . 415
11.2.7 Usuwanie kolekcji . . . 416
11.3 Sekrety . . . 417
11.3.1 Tworzenie sekretów . . . 417
11.3.2 Importowanie sekretów . . . 425
11.3.3 Dostęp do edycji sekretów . . . 427
11.3.3.1 Panel edycji sekretu . . . 427
11.3.4 Przenoszenie sekretów między kolekcjami . . . 430
11.3.5 Usuwanie sekretów . . . 431
11.3.6 Przypisywanie sekretów ze Skarbca haseł do kont . . . 433
11.4 Monitorowanie dostępu do sekretów . . . 434
11.4.1 Typy zdarzeń i wskaźniki statusu . . . 435
11.4.2 Filtrowanie i przeglądanie zdarzeń . . . 435
11.5 Modyfikatory haseł . . . 436
11.5.1 Polityki haseł . . . 436
11.5.1.1 Dodawanie polityki zmiany haseł . . . 436
11.5.1.2 Edycja polityki zmiany haseł . . . 437
11.5.1.3 Usuwanie polityki zmiany haseł . . . 438
11.5.2 Uniwersalne modyfikatory haseł . . . 438
11.5.2.1 Definiowanie modyfikatora haseł . . . 438
11.5.2.2 Edycja modyfikatora haseł . . . 442
11.5.2.3 Usuwanie modyfikatora haseł . . . 442
11.5.3 Importowanie i eksportowanie modyfikatorów haseł . . . 442
11.5.3.1 Eksportowanie modyfikatora haseł . . . 442
11.5.3.2 Importowanie modyfikatora haseł . . . 443
11.5.4 Tryby połączenia . . . 443
11.5.4.1 SSH . . . 443
11.5.4.2 LDAP . . . 444
11.5.4.3 Telnet . . . 445
11.5.4.4 WinRM . . . 446
11.5.5 Konfigurowanie modyfikatora haseł Unix poprzez SSH . . . 447

12 Ustawienia **450**
12.1 System . . . 450
12.1.1 Data i czas . . . 450
12.1.2 Certyfikaty SSL . . . 452
12.1.3 Dostęp SSH . . . 454
12.1.4 Szyfrowanie konfiguracji . . . 455
12.1.5 SNMP . . . 456
12.1.5.1 Konfigurowanie SNMP . . . 456
12.1.5.2 Konfigurowanie SNMPv3 TRAP . . . 457
12.1.5.3 SNMP MIBs . . . 458
12.1.5.4 Odczytywanie informacji SNMP poprzez `snmpwalk` . . . 458
12.1.5.5 Rozszerzenia SNMP Fudo Enterprise . . . 459
12.1.6 Znakowanie czasem . . . 459
12.1.7 Modyfikatory haseł - aktywny węzeł klastra . . . 461

12.1.7.1 Manager haseł w klastrze . . . 462
12.1.8 Funkcjonalności wrażliwe . . . 462
12.1.9 Konfigurowanie serwera proxy HTTP . . . 463
12.1.10 Aktualizacja systemu . . . 464
12.1.10.1 Aktualizowanie systemu . . . 465
12.1.10.2 Przywrócenie poprzedniej wersji systemu . . . 466
12.1.10.3 Usuwanie migawki aktualizacji . . . 467
12.1.11 Hotfix . . . 468
12.1.12 Licencja . . . 468
12.1.13 Diagnostyka . . . 471
12.1.14 Eksportowanie/importowanie konfiguracji systemu . . . 475
12.1.14.1 Eksportowanie konfiguracji systemu . . . 475
12.1.14.2 Importowanie konfiguracji systemu . . . 475
12.2 Konfiguracja sieci . . . 476
12.2.1 Reverse Proxy . . . 477
12.2.1.1 Wymagania wstępne . . . 477
12.2.1.2 Kroki konfiguracji . . . 478
12.2.1.3 Połączenia Portalu Użytkownika . . . 483
12.2.1.4 Włączanie i wyłączanie Reverse Proxy . . . 484
12.2.1.5 Wskaźniki stanu Reverse Proxy . . . 485
12.2.1.6 Działanie tunelu SSH . . . 486
12.2.1.7 Rekomendowany przebieg konfiguracji . . . 487
12.2.1.8 Zachowanie routingu wewnętrznego . . . 487
12.2.1.9 Względy bezpieczeństwa . . . 487
12.2.1.10 Zagadnienia bezpieczeństwa . . . 487
12.2.1.11 Rozwiązywanie problemów . . . 487
12.2.2 Konfiguracja ustawień sieciowych . . . 488
12.2.2.1 Zarządzanie interfejsami fizycznymi . . . 488
12.2.2.2 Definiowanie adresu IP z poziomu konsoli systemowej . . . 491
12.2.2.3 Konfiguracja sieci wirtualnych (VLAN) . . . 494
12.2.2.4 Konfiguracja agregacji łączy (LACP) . . . 496
12.2.3 Etykietowane adresy IP . . . 497
12.2.4 Konfiguracja tras routingu . . . 498
12.2.5 Konfiguracja DNS . . . 499
12.2.6 Konfiguracja tablicy ARP . . . 500
12.3 Powiadomienia . . . 502
12.3.1 Konfiguracja serwera SMTP . . . 503
12.4 Sztuczna inteligencja . . . 505
12.4.1 Analiza behawioralna AI . . . 506
12.4.1.1 Konfiguracja trenera modeli . . . 506
12.4.1.2 Modele behawioralne . . . 508
12.4.2 AI - Podsumowanie sesji przy użyciu sztucznej inteligencji [BETA] . . . 510
12.5 Uwierzytelnienie . . . 512
12.5.1 Definicja serwera uwierzytelnienia zewnętrznego . . . 512
12.5.1.1 Active Directory . . . 513
12.5.1.2 LDAP . . . 514
12.5.1.3 CERB . . . 515
12.5.1.4 Radius . . . 516
12.5.1.5 Przypisywanie zewnętrznej metody uwierzytelniania do użytkownika . . . 517
12.5.1.6 Drugi czynnik uwierzytelnienia . . . 517

12.5.2 Definicja uwierzytelniania OpenID Connect . . . 518
12.5.3 Globalne ustawienia uwierzytelniania . . . 522
12.5.3.1 Domyślna domena . . . 522
12.5.3.2 Blokowanie nowych połączeń . . . 524
12.5.3.3 Złożoność haseł . . . 525
12.5.3.4 Definicja uwierzytelniania OATH . . . 526
12.5.3.5 Definicja uwierzytelniania SMS . . . 527
12.5.3.6 Definicja uwierzytelniania DUO . . . 528
12.5.3.7 Single Sign On . . . 530
12.5.3.8 Ustawienia uwierzytelniania Kerberos . . . 532
12.6 Zewnętrzne repozytoria haseł . . . 534
12.6.1 CyberArk Credential Provider . . . 534
12.6.2 Thycotic Secret Server . . . 536
12.6.3 Local Administrator Password Solutions (LAPS) . . . 538
12.7 Zewnętrzna macierz dyskowa . . . 541
12.7.1 Konfigurowanie zewnętrznej macierzy dyskowej . . . 541
12.7.2 Rozszerzanie zewnętrznej macierzy dyskowej . . . 542
12.8 Zasoby . . . 542
12.8.1 Konfiguracja ekranu logowania RDP/SSH/VNC . . . 542
12.8.2 Konfiguracja *Portalu użytkownika* . . . 545
12.8.2.1 Konfiguracja ekranu logowania . . . 545
12.8.2.2 Definiowanie układu klawiatury . . . 547
12.9 Kopia zapasowa i retencja . . . 547
12.9.1 Kopia zapasowa danych sesji . . . 547
12.9.2 Retencja danych . . . 549
12.10 Konfiguracja klastrowa . . . 551
12.10.1 Replikacja danych sesji i zachowanie w przypadku awarii węzła . . . 551
12.10.2 Inicjowanie klastra . . . 553
12.10.3 Dodawanie węzłów klastra . . . 555
12.10.3.1 Inicjacja klastra i dodanie węzłów . . . 555
12.10.3.2 Ustawianie relacji pomiędzy węzłami . . . 557
12.10.3.3 Powiązanie węzłów z węzłem inicjalnym . . . 558
12.10.3.4 Weryfikacja zakończenia inicjalizacji klastra . . . 559
12.10.4 Rozbudowa klastra o nowe węzły . . . 560
12.10.5 Edytowanie węzłów klastra . . . 563
12.10.6 Usuwanie węzłów klastra . . . 563
12.10.6.1 Usuwanie węzła z klastra . . . 564
12.10.6.2 Ponowne dołączanie usuniętego węzła . . . 564
12.10.7 Grupy redundancji . . . 564
12.10.8 Sprawdzanie statusu replikacji sesji . . . 568
12.11 Synchronizacja użytkowników z LDAP - User Directory . . . 569
12.11.1 Konfiguracja usługi synchronizacji użytkowników . . . 569
12.11.2 Wyłączanie synchronizacji danych dla użytkownika . . . 574
12.11.3 Obsługa Kerberosa przy synchronizacji z Active Directory . . . 575
12.12 Model uwierzytelniania w oparciu o certyfikaty . . . 576
12.13 Login Timeout . . . 577
12.14 Przywracanie poprzedniej wersji systemu . . . 578
12.15 Ponowne uruchomienie systemu . . . 580
12.16 Zmiana frazy szyfrującej . . . 581
12.17 Integracja z serwerem CERB . . . 583
12.18 Czynności serwisowe . . . 589

12.18.1 Sporządzanie kopii zapasowej kluczy szyfrujących . . . 590
12.18.2 Monitorowanie stanu systemu . . . 593
12.18.3 Kontrola Stanu . . . 594
12.18.3.1 API Health Check . . . 594
12.18.4 Callhome . . . 595
12.18.4.1 Dane gromadzone przez usługę Callhome . . . 596
12.18.4.2 Korzyści z używania Callhome . . . 596
12.18.4.3 Konfiguracja Callhome . . . 597
12.18.5 Wymiana dysku macierzy . . . 597
12.18.6 Przywracanie ustawień fabrycznych . . . 598

13 Dziennik zdarzeń **602**
13.1 Filtrowanie logów według daty i czasu . . . 602
13.2 Zewnętrzne serwery syslog . . . 603
13.3 Eksportowanie dziennika zdarzeń . . . 604

14 Aktywność konta w Portalu Użytkownika **606**

15 Informacje uzupełniające **608**
15.1 Broker połączeń RDP . . . 608
15.2 Komunikaty dziennika zdarzeń . . . 609
15.3 Informacja ze stopki dolnej . . . 649

16 Fudo Officer 2.3 **650**
16.1 Konfiguracja . . . 650
16.2 Zarządzanie Profilami . . . 652
16.2.1 Dodawanie Profilów . . . 653
16.2.2 Przełączanie Profilów . . . 654
16.2.3 Edytowanie Profilu . . . 655
16.2.4 Usuwanie Profilu . . . 656
16.3 Zarządzanie Żądaniami Sesji . . . 657
16.3.1 Żądania Oczekujące . . . 658
16.3.2 Żądania Aktywne . . . 659
16.3.3 Cofnięcie Żądania . . . 659
16.3.4 Żądania Archiwalne . . . 660
16.4 Powiadomienia . . . 661
16.4.1 Konfigurowanie powiadomień aplikacji . . . 662
16.5 Ustawienia . . . 663
16.5.1 Uwierzytelnianie biometryczne . . . 664
16.5.2 Zmiana kodu PIN . . . 664
16.5.3 Dwuskładnikowe uwierzytelnianie przy użyciu YubiKey . . . 664
16.5.4 Język . . . 665

17 Fudo ShareAccess **666**
17.1 Model danych . . . 666
17.2 Parowanie Fudo Enterprise i Fudo ShareAccess . . . 667
17.3 Licencja . . . 673
17.3.1 Licencja próbna (trial) . . . 673
17.3.2 Zamawianie licencji . . . 673
17.3.3 Wgrywanie pliku licencji . . . 674
17.4 Zarządzanie użytkownikami Fudo ShareAccess . . . 674
17.4.1 Zapraszanie członków . . . 674

17.4.2 Weryfikacja statusu członków . . . 676
17.4.3 Tworzenie konta bez zaproszenia . . . 678
17.4.4 Cofanie statusu członków . . . 678
17.4.5 Usuwanie członków . . . 679
17.5 Zarządzanie dostępem do zasobów . . . 679

18 Aplikacje klienckie **683**
18.1 PuTTY . . . 683
18.2 Microsoft Remote Desktop . . . 685
18.3 TightVNC Viewer . . . 687
18.4 SQL Server Management Studio . . . 687

19 Rozwiązywanie problemów **689**
19.1 Uruchamianie Fudo Enterprise . . . 689
19.2 Połączenia z serwerami . . . 689
19.3 Logowanie do panelu administracyjnego . . . 694
19.4 Odtwarzanie sesji . . . 695
19.5 Konfiguracja klastrowa . . . 695
19.6 Znakowanie czasem . . . 696
19.7 Tryb serwisowy . . . 696

20 Przypadki użycia **700**
20.1 Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator . . . 700
20.1.1 Protokoły obsługujące OATH . . . 700
20.1.2 Konfiguracja domyślnych wartości OATH . . . 701
20.1.3 Konfiguracja metody OATH użytkownikowi . . . 701
20.2 Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure) . . . 706
20.3 Konfiguracja usługi Remote Desktop Services na serwerze Windows dla Fudo Enterprise . . . 713
20.3.1 Konfiguracja usługi Remote Desktop Services (RDS) w systemie Windows 714
20.3.2 Konfiguracja Fudo Enterprise - scenariusz bastion (zalecany) . . . 725
20.3.3 Konfiguracja Fudo Enterprise - scenariusz proxy . . . 732
20.4 Niestandardowa nazwa hosta RDP w tytule sesji . . . 739
20.4.1 Konfiguracja DNS w Menedżerze DNS systemu Windows . . . 739
20.4.2 Konfiguracja Fudo Enterprise . . . 741
20.4.3 Uruchamianie połączenia RDP . . . 741
20.4.4 Rezultat . . . 742
20.5 Zarządzanie certyfikatami na potrzeby połączeń RDP . . . 742
20.5.1 Lokalizacja certyfikatu dla protokołu RDP w Windows Server . . . 742
20.5.2 Dostarczanie certyfikatu CA . . . 745
20.6 Konfiguracja Single Sign On (SSO) . . . 760
20.6.1 Konfiguracja SSO na Windows Server 2019 . . . 761
20.6.2 Konfiguracja Fudo Enterprise . . . 765
20.6.3 Konfiguracja i sprawdzenie stacji roboczej użytkownika - klienta Windows 2010 . . . 768
20.7 Obsługa zmiany haseł kont lokalnych z wykorzystaniem konta domenowego przy użyciu modyfikatora haseł WinRM . . . 772
20.7.1 Konfiguracja nazwy hosta i serwera DNS . . . 773
20.7.2 Dodanie serwera KDC . . . 773
20.7.3 Konfiguracja serwera . . . 774
20.7.4 Dodawanie polityki zmiany haseł . . . 775
20.7.5 Konto administratora . . . 776

20.7.6 Konto dla którego będzie zmieniane hasło 777
20.8 Konfiguracja ograniczonej delegacji protokołu Kerberos dla serwera MSSQL(TDS) 779
20.8.1 Konfiguracja uwierzytelniania Kerberos na serwerze Windows 779
20.8.2 Konfiguracja Fudo Enterprise 786
20.9 Nawiązywanie połączeń z serwerami przez tunel SSH w Fudo Enterprise 790
20.9.1 Wymagania ogólne 790
20.9.1.1 Nawiązywanie połączenia SSH 791
20.9.1.2 Nawiązywanie połączenia HTTP 796
20.9.1.3 Nawiązywanie połączenia z bazą danych Oracle 801
20.9.1.4 Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel 807

21 Często zadawane pytania **811**

22 Słownik pojęć **816**

Indeks **820**

ROZDZIAŁ 1

O dokumentacji

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

Konwencje i symbole

Poniższa sekcja opisuje konwencje nazewnicze użyte w dokumentacji.

kursywa

Element interfejsu graficznego użytkownika.

`przykład`

Przykładowa wartość parametru konfiguracyjnego.

Uwaga

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

Ostrzeżenie

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

Nota prawna

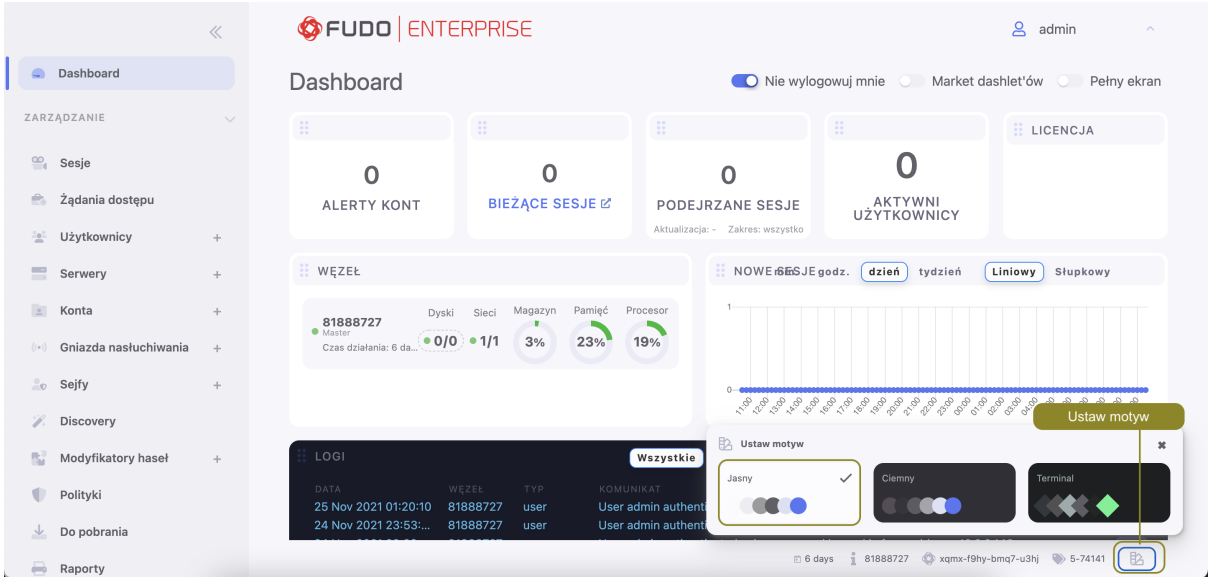
Wszystkie nazwy, grafiki i znaki firmowe lub towarowe, niebędące własnością firmy Fudo Security, występujące w tym dokumencie, należą do ich właścicieli i zostały użyte wyłącznie w celach informacyjnych.

ROZDZIAŁ 2

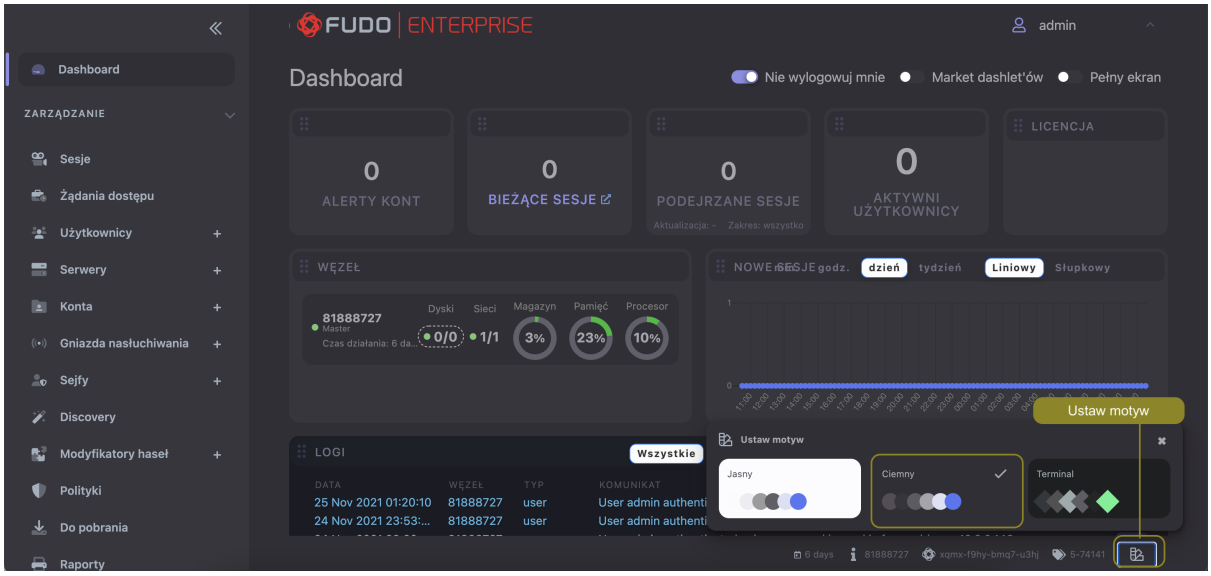
Motywy kolorystyczne Panelu Administracyjnego

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

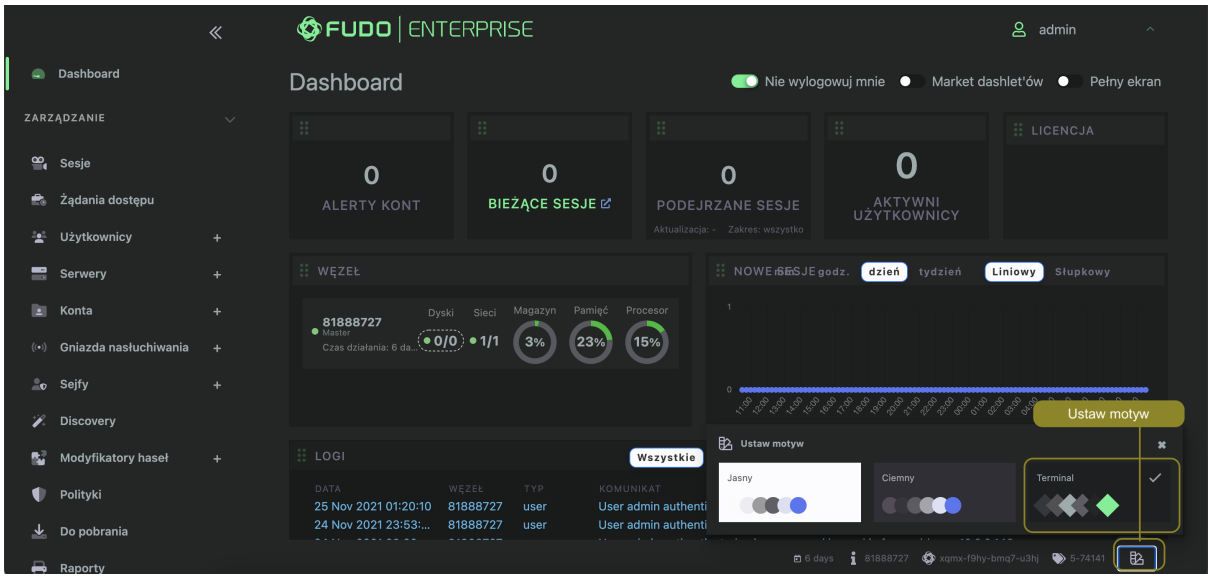
Jasny:



Ciemny:



Terminal:



Tematy pokrewne:

- *Wstęp*

ROZDZIAŁ 3

Wstęp

3.1 Przegląd systemu

Fudo Enterprise to kompleksowe rozwiązanie do zarządzania zdalnym dostępem uprzywilejowanym. Fudo Enterprise zawiera szereg funkcjonalności, z których każda jest dedykowana różnym aspektom zarządzania zdalnym dostępem:

- *Monitorowanie i nagrywanie sesji*
- *Zarządzanie hasłami*
- *Dostęp Just-in-Time (JIT)*
- *Single Sign-On (SSO)*
- *Bezagentowy wygodny dostęp*
- *Zapobieganie z wykorzystaniem AI*
- *Analiza produktywności*
- *Szybkie wdrożenie*
- *Wsparcie dla zgodności*

3.1.1 Monitorowanie i nagrywanie sesji

Fudo Enterprise dostarcza administratorom zaawansowane narzędzia do monitorowania i zarządzania sesjami w czasie rzeczywistym. Administratorzy mogą dołączać, udostępniać, wstrzymywać lub kończyć sesje, co umożliwia szybką reakcję na potencjalnie podejrzane działania.

Platforma obsługuje udostępnianie zasobów za pomocą ponad 10 protokołów, w tym RDP, SSH i HTTPS, zapewniając bezpieczny dostęp do krytycznych systemów. Fudo Enterprise rejestruje pełny ruch sieciowy wraz z metadanymi, umożliwiając precyzyjne odtwarzanie sesji oraz pełnotekstowe wyszukiwanie treści. Ta funkcjonalność zapewnia kompleksową ścieżkę audytu, zwiększając bezpieczeństwo i zgodność z przepisami.

Fudo Enterprise działa jako proxy między użytkownikami a monitorowanymi serwerami, rejestrując działania użytkowników, w tym ruchy kursora, naciśnięcia klawiszy oraz przesyłane pliki.

Dane przechowywane na platformie Fudo mogą być znakowane czasem, co czyni materiały z sesji bardziej wiarygodnym dowodem w sądzie.

Moduł monitorowania sesji Fudo Enterprise obsługuje następujące konfiguracje systemowe:

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

3.1.2 Zarządzanie hasłami

Fudo Enterprise zapewnia bezpieczny i elastyczny system zarządzania poświadczeniami kont uprzywilejowanych. Poświadczenia są przechowywane w sposób bezpieczny i nigdy nie opuszczają systemu, co zapewnia solidną ochronę.

Administratorzy mogą korzystać z predefiniowanych szablonów, aby szybko skonfigurować modyfikatory haseł w ciągu kilku minut. Te modyfikatory działają na oddzielnej warstwie transportowej, takiej jak SSH, LDAP, Telnet czy WinRM, umożliwiając integrację z różnymi systemami.

Fudo Enterprise obsługuje zmianę haseł w następujących systemach:

- Unix
- MySQL
- Cisco
- Cisco Enable Password
- MS Windows

Oprócz wbudowanych przykładów można tworzyć niestandardowe modyfikatory haseł w postaci zestawu komend wykonywanych na maszynie zdalnej.

Aby uzyskać więcej informacji, przejdź do rozdziału *Modyfikatory haseł*.

3.1.3 Dostęp Just-in-Time (JIT)

Fudo Enterprise wspiera przepływy pracy oparte na dostępie Just-in-Time (JIT), umożliwiając organizacjom wdrożenie podejścia Zero-Trust. Dzięki funkcji *Żądania dostępu* administratorzy mogą definiować i planować określone przedziały czasowe dostępności zasobów, przyznając dostęp tylko wtedy, gdy jest to konieczne. To podejście zapewnia przestrzeganie zasady zerowych uprawnień stałych, minimalizując ryzyko naruszeń bezpieczeństwa przez limitowanie dostępu do krytycznych systemów.

3.1.4 Single Sign-On (SSO)

Fudo Enterprise zapewnia funkcjonalność *Single Sign-On (SSO)* zarówno dla Panelu Administracyjnego, jak i Portalu Użytkownika. SSO upraszcza uwierzytelnianie poprzez automatyczne logowanie użytkowników do systemu, zwiększając efektywność pracy przy jednoczesnym zachowaniu wysokich standardów bezpieczeństwa.

3.1.5 Bezagentowy wygodny dostęp

Fudo Enterprise oferuje elastyczny i bezagentowy dostęp do zasobów, umożliwiając użytkownikom wybór preferowanej metody połączenia. Użytkownicy mogą nadal korzystać ze swoich ulubionych klientów natywnych, lub skorzystać z wbudowanego, uruchamianego z poziomu przeglądarki Klienta Webowego dostarczonego przez Fudo Enterprise. Ta elastyczność zapewnia łatwość pracy z Fudo Enterprise zarówno użytkownikom technicznym, jak i nietechnicznym.

3.1.6 Zapobieganie naruszeniom oparte na Sztucznej Inteligencji

Fudo Enterprise integruje funkcje oparte na AI wspierając codzienne zadania zespołów ds. bezpieczeństwa i CISO. Analizując wzorce behawioralne i semantyczne, Fudo Enterprise buduje indywidualne profile użytkowników, na podstawie których jest w stanie wykryć najdrobniejszą zmianę w ich zachowaniu. Umożliwiając szybkie wykrycie podejrzanych zachowań, pozwala zapobiec naruszeniom bezpieczeństwa monitorowanych systemów.

3.1.7 Analiza produktywności

Moduł analizy produktywności śledzi działania użytkowników i dostarcza precyzyjnych informacji o ich aktywności oraz czasie bezczynności.

Aby uzyskać więcej informacji na temat modułu analizy produktywności, zobacz temat *Produktywność*.

3.1.8 Szybkie wdrożenie

Fudo Enterprise został zaprojektowany jako rozwiązanie all-in-one, eliminując potrzebę dodatkowego oprogramowania lub ukrytych kosztów. Niezależnie od tego, czy jest wdrażany jako urządzenie, czy maszyna wirtualna, wszystkie niezbędne komponenty są zawarte w systemie. To uproszczone podejście zapewnia szybki i efektywny proces instalacji, umożliwiając pełne wdrożenie w zaledwie jeden dzień.

3.1.9 Wsparcie dla zgodności

Fudo Enterprise został zaprojektowany, aby pomóc organizacjom spełnić szeroką gamę wymagań zgodności, w tym PCI-DSS, SOX, HIPAA, NIST, GDPR i ISA/IEC 62443. Dzięki solidnym funkcjom bezpieczeństwa i audytu Fudo Enterprise zapewnia przestrzeganie standardów branżowych i ram regulacyjnych, upraszczając zarządzanie zgodnością w Twojej organizacji.

Tematy pokrewne:

- *Wymagania*
- *Model danych*
- *Środki bezpieczeństwa*

3.2 Dostępne języki interfejsu

Interfejs Fudo Enterprise jest dostępny w następujących językach:

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

Tematy pokrewne:

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

3.3 Licencjonowanie

Ta sekcja opisuje model licencjonowania dla **modułów Fudo Enterprise**. **Licencja ShareAccess** jest zarządzana oddzielnie i opisana w sekcji *ShareAccess: Licencja*.

Ostrzeżenie

Począwszy od **wersji 6.0**, model licencjonowania Fudo Enterprise został zaktualizowany.

Wcześniej zunifikowana **licencja Fudo Enterprise** została podzielona na trzy niezależne moduły:

- **Menedżer sesji uprzywilejowanych (Privileged Session Management)**
- **Skarbiec Haseł (Password Vault)**
- **ShareAccess**

Każdy moduł jest licencjonowany oddzielnie i ma własną datę wygaśnięcia oraz limity użytkowania. Więcej informacji znajduje się w podsekcji *Limit aktywnych użytkowników*.

Licencjonowane moduły

Platforma zawiera następujące licencjonowane moduły:

- **Menedżer sesji uprzywilejowanych** - Reprezentuje podstawową funkcjonalność, która wcześniej była objęta licencją Fudo Enterprise, w tym przekierowywanie sesji uprzywilejowanych, monitorowanie i kontrolę dostępu.
- **Skarbiec Haseł** - Zapewnia bezpieczne przechowywanie i zarządzanie cyklem życia poświadczeń, takich jak hasła, klucze SSH, klucze API, certyfikaty i bezpieczne notatki.

- **ShareAccess** - Umożliwia bezpieczny i uproszczony dostęp dla podmiotów trzecich, w tym zewnętrznych dostawców, poprzez zapewnienie dostępu opartego na przeglądarce do udostępnionych zasobów oraz usprawnienie obsługi połączeń i poświadczeń.

Każdy moduł posiada:

- własną **datę wygaśnięcia**
- niezależne **limity aktywnych użytkowników**
- dodatkowe **limity funkcji**

Data wygaśnięcia

Każdy licencjonowany moduł ma oddzielną datę wygaśnięcia. Po osiągnięciu daty wygaśnięcia funkcjonalność danego modułu może zostać ograniczona.

Liczba węzłów klastra

Licencja określa liczbę węzłów, które mogą być częścią klastra. W przypadku przekroczenia tej liczby dodatkowe węzły będą odrzucać połączenia i rejestrować odpowiednie zdarzenia w logach systemowych.

Dostępne serwery

Licencja określa, ile serwerów można dodać do systemu. Po przekroczeniu tego limitu nie jest możliwe dodawanie nowych serwerów ani modyfikowanie istniejących.

Limit aktywnych użytkowników (Moduł PSM)

Liczba aktywnych użytkowników określa, ilu użytkowników może nawiązywać sesje do serwerów za pomocą modułu **Zarządzanie sesjami uprzywilejowanymi (PSM)**.

Uwaga

- Użytkownik jest liczony jako **aktywny**, jeśli rozpoczął co najmniej jedną sesję w ciągu ostatnich **30 dni**.
- Miejsce licencyjne jest zwalniane automatycznie, gdy użytkownik nie ma żadnej aktywności sesyjnej przez ponad **30 dni**.

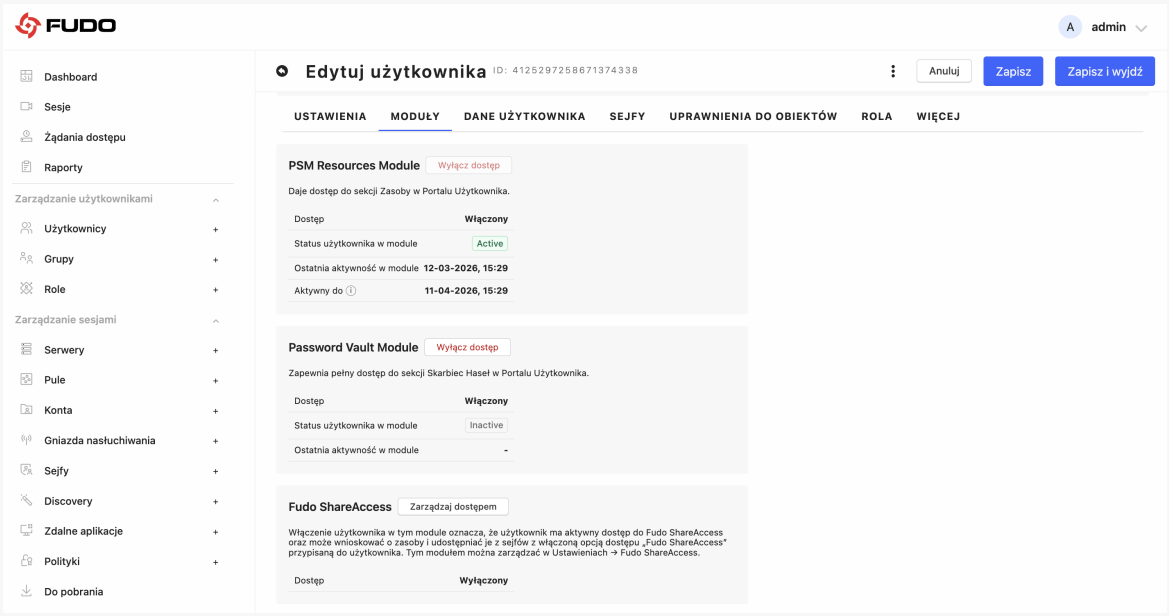
Jeśli licencjonowany limit został już osiągnięty, tylko użytkownicy, którzy byli już aktywni w ciągu ostatnich 30 dni, mogą kontynuować nawiązywanie sesji. Użytkownicy, którzy nie byli aktywni w tym okresie, nie mogą rozpoczynać nowych sesji, dopóki miejsce licencyjne nie stanie się dostępne.

Następujące działania nie są ograniczone limitem aktywnych użytkowników:

- Logowanie do **Panelu Administracyjnego** jest zawsze dozwolone. Zapobiega to zablokowaniu administratorów przed systemem z powodu limitów licencyjnych.
- Użytkownicy uwierzytelnieni przez **ShareAccess** nie są liczeni względem limitu aktywnych użytkowników modułu PSM.

Uwaga

Możesz sprawdzić status zużycia licencji każdego użytkownika w formularzu edycji użytkownika, w podzakładce **Moduły**.



Limit aktywnych użytkowników (Moduł PV)

Licencja **Skarbca haseł** zawiera oddzielny limit aktywnych użytkowników, niezależny od modułu PSM. Ten limit dotyczy tylko operacji Skarbca haseł.

Ograniczenia podstawowej licencji Skarbca haseł

Moduł Skarbca haseł jest dostępny zarówno w pełnym, jak i ograniczonym wariancie licencyjnym.

- **Pełna licencja** zapewnia dostęp do pełnej funkcjonalności Skarbca haseł, w tym nieograniczonego zarządzania kolekcjami, pełnego zarządzania sekretami, wszystkich obsługiwanych typów sekretów, pełnych uprawnień do kolekcji oraz konfiguracji globalnych polityk.
- **Podstawowa licencja** zawiera wybrane ograniczenia. W tym wariancie:
  - administratorzy nie mogą tworzyć kolekcji podrzędnych ani tworzyć sekretów w kolekcjach podrzędnych.
  - Pełne uprawnienia dostępu do kolekcji nie są dostępne dla użytkowników i grup, można przypisać tylko uprawnienia *Przeglądanie* i *Przeglądanie na żądanie*.
  - Globalna konfiguracja polityk Skarbca haseł oraz status zgodności z politykami są również niedostępne.
  - Tworzenie sekretów jest ograniczone do typów *Logowanie*, *Klucz SSH* i *Notatka*.

Uprawnienia do zarządzania licencjami

Następujące uprawnienia są wymagane do zarządzania licencjami:

- `license-read` – pozwala na przeglądanie informacji o licencji
- `license-upload` – pozwala na wgrywanie lub usuwanie plików licencji

Uwaga

Szczegóły dotyczące przeglądania informacji o licencji znajdują się w sekcji *Licencja*.

Tematy pokrewne:

- *Przegląd systemu*
- *Wspierane protokoły*
- *Szybki start*

3.4 Wspierane protokoły

Deprecated since version 6.0 :class: danger

Wsparcie dla protokołu **Telnet 3270** jest obecnie **w fazie przeglądu** i może zostać usunięte w jednej z kolejnych wersji. Jeśli protokół ten jest kluczowy dla Twojego środowiska, skontaktuj się z pomocą techniczną Fudo w celu uzyskania dodatkowych informacji.

3.4.1 HTTP

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

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`

Ostrzeżenie

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

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

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

Uwaga

Następujące funkcje **nie są** obsługiwane:

- Dołączanie do sesji
- Opcja podania powodu logowania

W **trybie nierenderowanym** obowiązują następujące ograniczenia:

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

W **trybie renderowanym** surowy ruch HTTP nie jest zapisywany.

3.4.2 Modbus

Wspierane tryby połączenia:

- *Proxy*

Uwagi:

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

3.4.3 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*,
- *Proxy*.

Wspierane aplikacje klienckie:

- SQL Server Management Studio,
- sqlcmd.

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.

3.4.4 MySQL

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

Wspierane aplikacje klienckie:

Oficjalny klient MySQL

Uwagi:

- Brak wsparcia mechanizmu dołączania do sesji.
- Od wersji 5.6 ten typ połączenia obsługuje wszystkie standardowe metody uwierzytelniania. W przypadku użycia uwierzytelniania wieloskładnikowego obsługiwane jest wyłącznie jednokrokowe 2FA (np. hasło i token wprowadzane jednocześnie).
- Obsługiwane wtyczki uwierzytelniania:
  - dla komunikacji między |product_name| a serwerem bazy danych: `mysql_clear_password`, `mysql_native_password`, `caching_sha2_password`;
  - dla komunikacji między klientem a |product_name|: `mysql_clear_password`.

3.4.5 PostgreSQL

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

Wspierane aplikacje klienckie

- psql

- pgAdmin (ze względu na problem po stronie aplikacji klienckiej uwierzytelnianie OTP nie jest obsługiwane)

Uwagi:

- Dołączanie do sesji nie jest obsługiwane.
- Tryb nagrywania sesji `noraw` nie jest obsługiwany.

3.4.6 RDP

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

Obsługiwane systemy operacyjne:

- Windows Server 2016 i nowsze

Wspierane aplikacje klienckie:

- Oficjalny klient dla Microsoft Windows i macOS,
- xfreerdp.

Wspierane języki OCR:

- angielski
- niemiecki
- norweski
- ukraiński
- polski
- węgierski
- rosyjski
- ormiański
- gruziński
- azerski
- kazachski
- kirgiski
- malajalam
- bengalski
- wietnamski

Wspierane algorytmy:

- kiedy jest wybrany poziom bezpieczeństwa TLS, a opcja *Starszy szyfr* wyłączona:
  - `TLS_AES_256_GCM_SHA384`
  - `TLS_CHACHA20_POLY1305_SHA256`

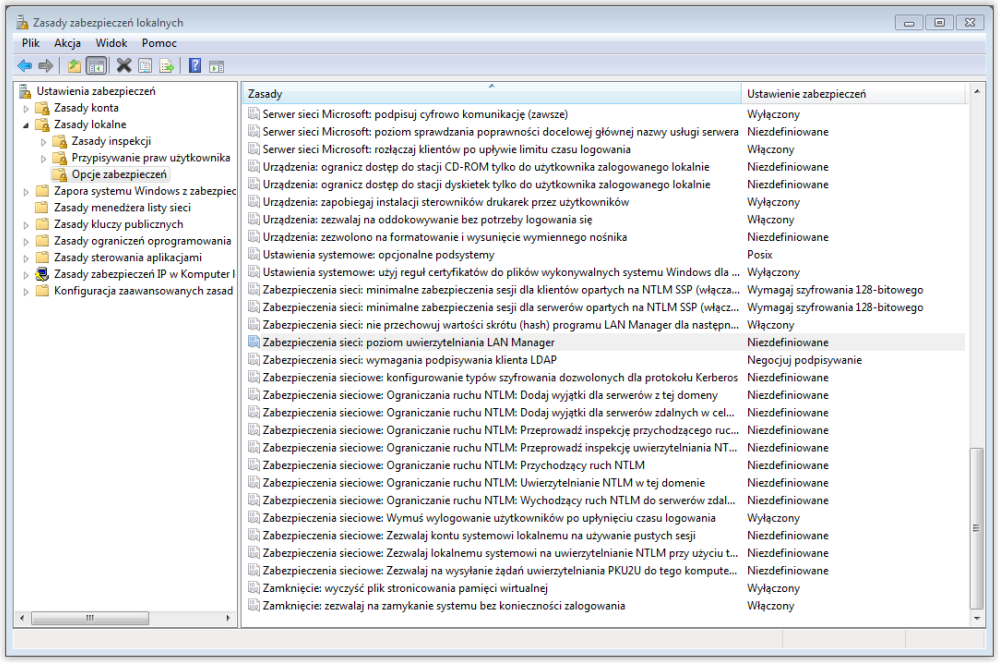
  - TLS_AES_128_GCM_SHA256
  - ECDHE-ECDSA-CHACHA20-POLY1305
  - ECDHE-RSA-CHACHA20-POLY1305
  - ECDHE-ECDSA-AES256-GCM-SHA384
  - ECDHE-RSA-AES256-GCM-SHA384
  - ECDHE-ECDSA-AES256-SHA384
  - ECDHE-RSA-AES256-SHA384
  - DHE-RSA-AES256-GCM-SHA384
  - AES256-GCM-SHA384
  - AES128-GCM-SHA256
  - AES128-SHA256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

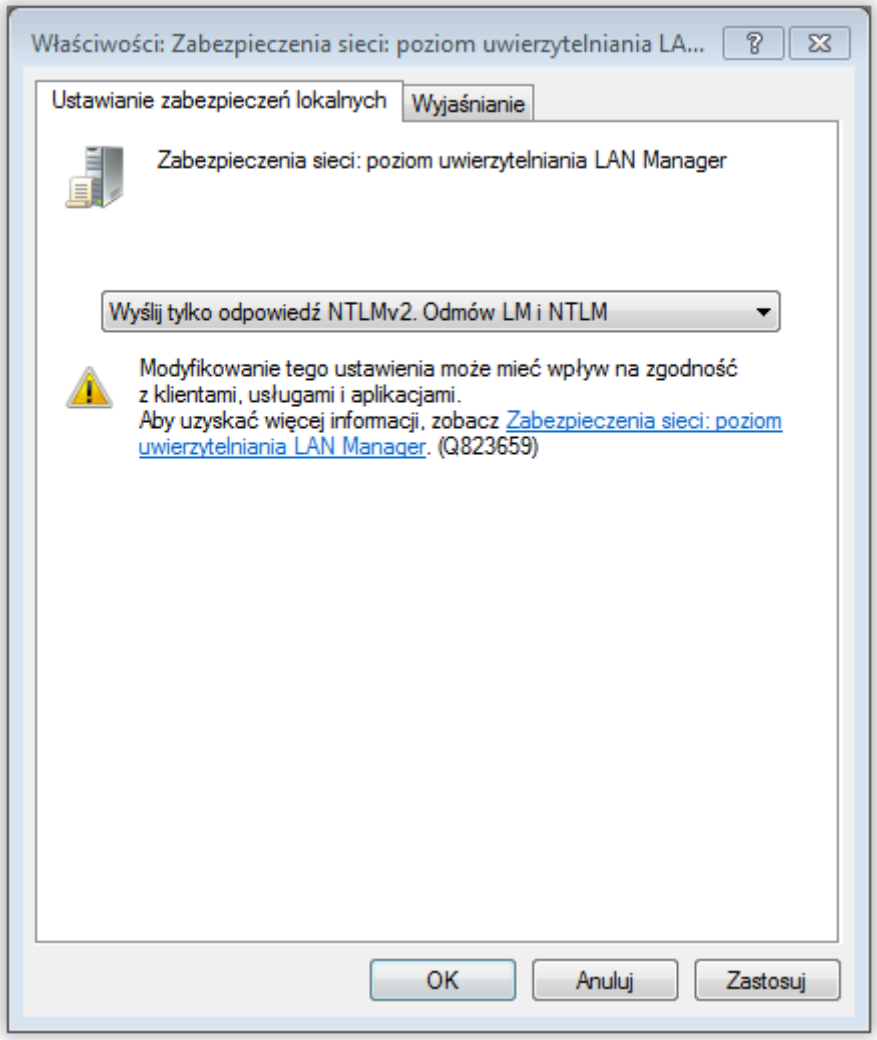
Uwagi:

- 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.

Sesje wielomonitorowe:

Fudo Enterprise wspiera sesje wielomonitorowe w protokole RDP, co pozwala na monitorowanie i rejestrację sesji odbywających się na więcej niż jednym ekranie.

3.4.7 SSH

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

Wspierane aplikacje klienckie:

- PuTTY,
- WinSCP,
- OpenSSH (ssh).

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*.

3.4.8 Telnet 3270

Deprecated since version 6.0 :class: danger

Wsparcie dla protokołu **Telnet 3270** jest obecnie **w fazie przeglądu** i może zostać usunięte w jednej z kolejnych wersji. Jeśli protokół ten jest kluczowy dla Twojego środowiska, skontaktuj się z pomocą techniczną Fudo w celu uzyskania dodatkowych informacji.

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

Wspierane aplikacje klienckie: c3270.

Uwagi:

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

Uwaga

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.

3.4.9 Telnet 5250

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

Wspierane aplikacje klienckie: tn5250.

Uwagi:

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

Uwaga

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.

3.4.10 Telnet

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

Uwagi:

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

Uwaga

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.

3.4.11 VNC

Wspierane tryby połączenia:

- *Bastion*,
- *Proxy*.

Proponowane aplikacje klienckie:

- TightVNC,
- TigerVNC,
- 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);

3.4.12 X11

Protokół X11 wspierany jest w ramach protokołu SSH.

Uwaga

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.

3.4.13 TCP

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

Wspierane tryby połączenia:

- *Proxy*

Uwagi:

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

3.4.14 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.

Uwaga

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.

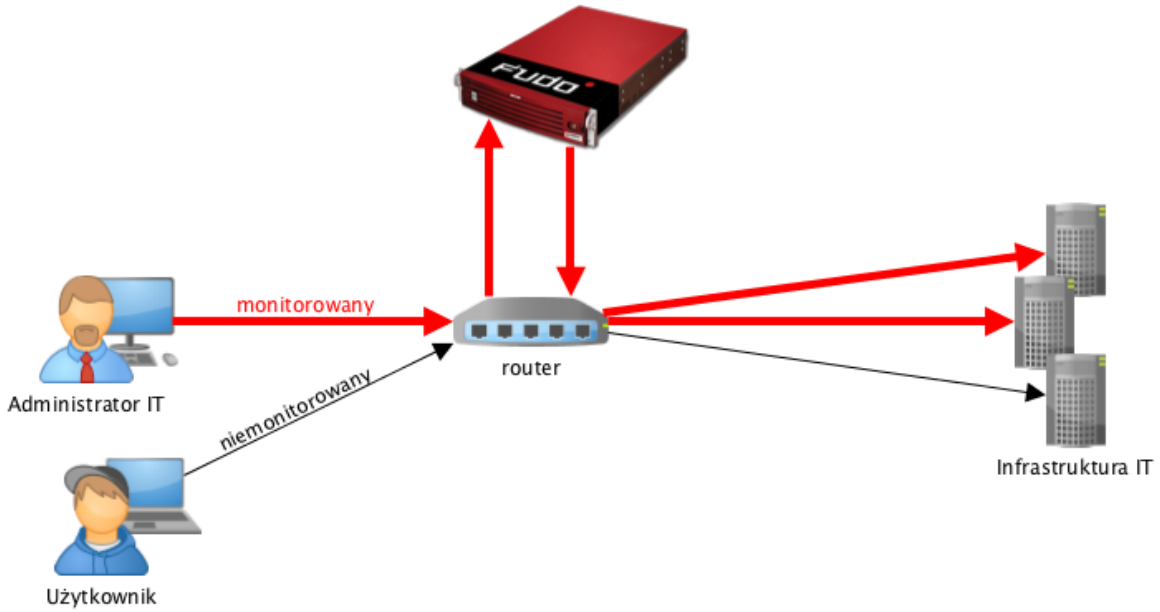
3.5 Scenariusze wdrożenia

Uwaga

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.

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.

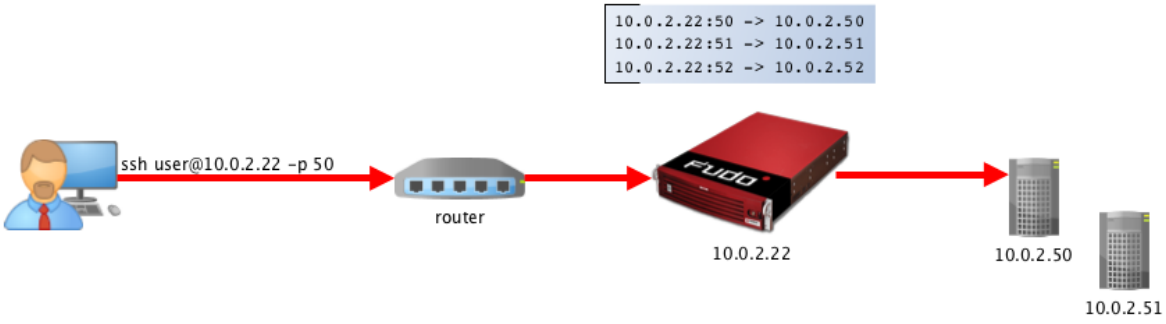
Tematy pokrewne:

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

3.6 Tryby połączenia

Proxy

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.

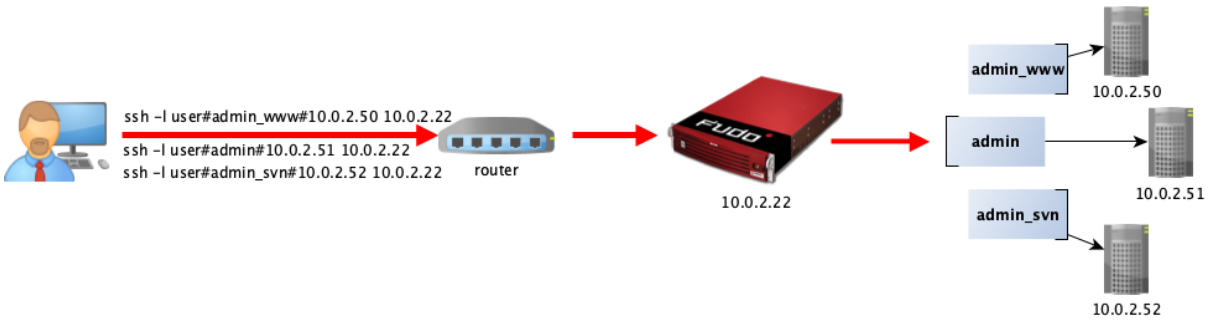


Takie rozwiązanie ukrywa faktyczną adresację serwerów, a odpowiednie ich skonfigurowanie pozwala na odrzucanie zapytań ze źródłowym adresem IP innym niż adres IP Fudo Enterprise.

Bastion

> **Uwaga**
>
> 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.

Uwaga

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*

3.7 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*.

Uwaga

- 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.



Uwaga

- 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.



Uwaga

- 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.



Uwaga

- 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*

3.8 Mechanizmy bezpieczeństwa

3.8.1 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.

3.8.2 Kopie zapasowe

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

3.8.3 Uprawnienia użytkowników

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

3.8.4 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.

3.8.5 Niezawodność

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

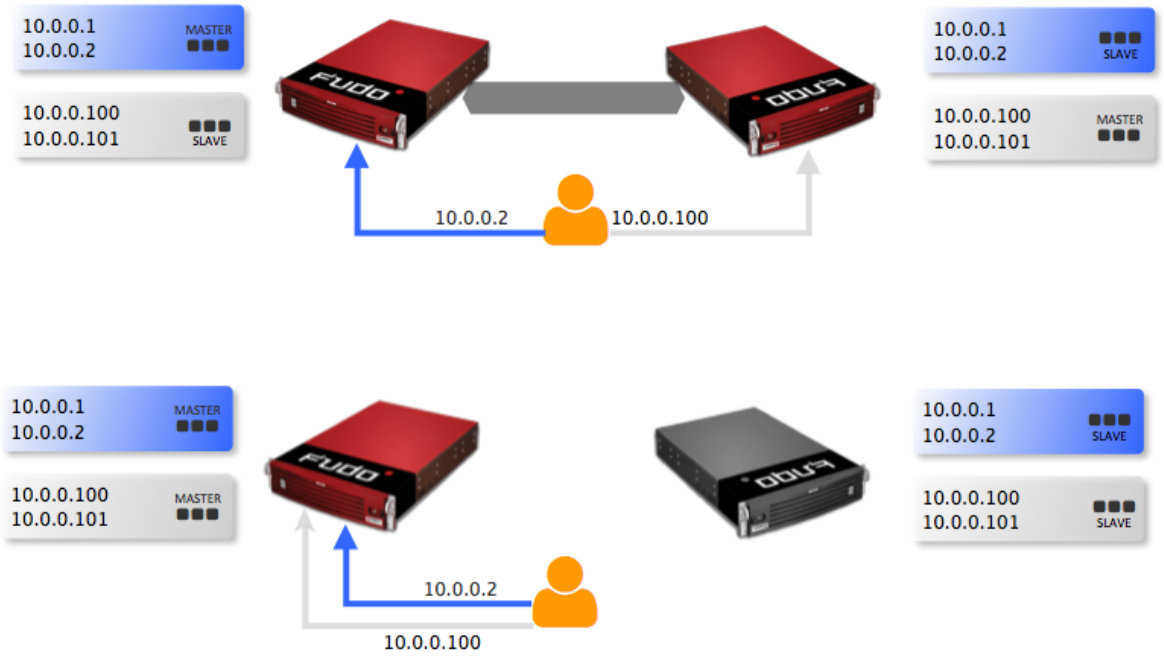
3.8.6 Konfiguracja klastrowa

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*

3.9 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.

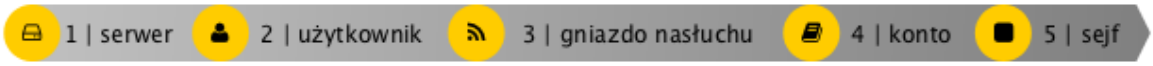
Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

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.

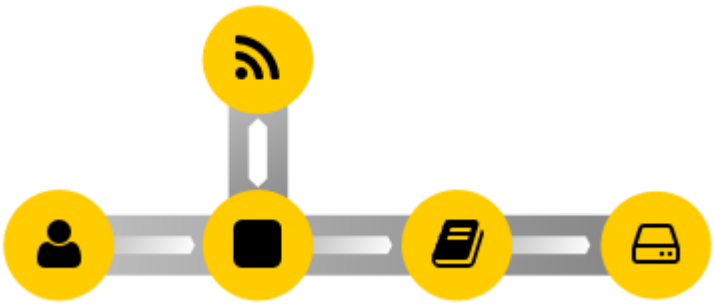
Prawidłowe działanie systemu wymaga odpowiedniego skonfigurowania *serwerów*, *użytkowników*, *gniazd nasłuchiwania*, *kont uprzywilejowanych* oraz *sejfów*.



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



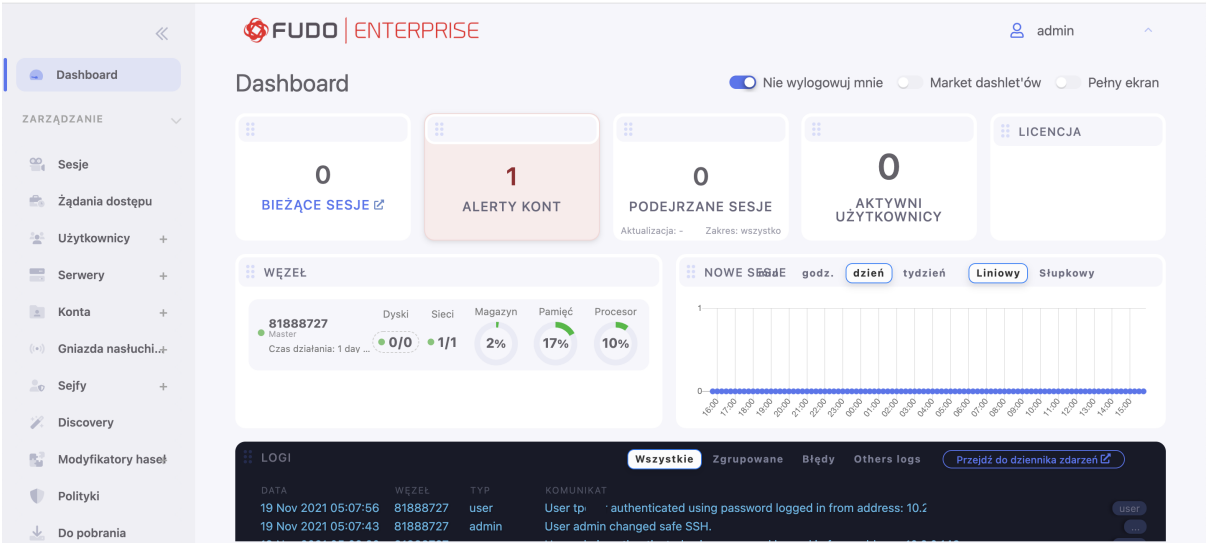
Sejf jest centralnym obiektem modelu danych, który reguluje dostęp do monitorowanych serwerów. Wskazuje konta uprzywilejowane na systemach docelowych, wraz z gniazdami nasłuchiwania określającymi właściwe dla *wybranego trybu* parametry połączenia (np. adres IP, numer portu). Taki model danych pozwala 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*

3.10 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.



Uwaga

- 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.

3.10.1 Widgety

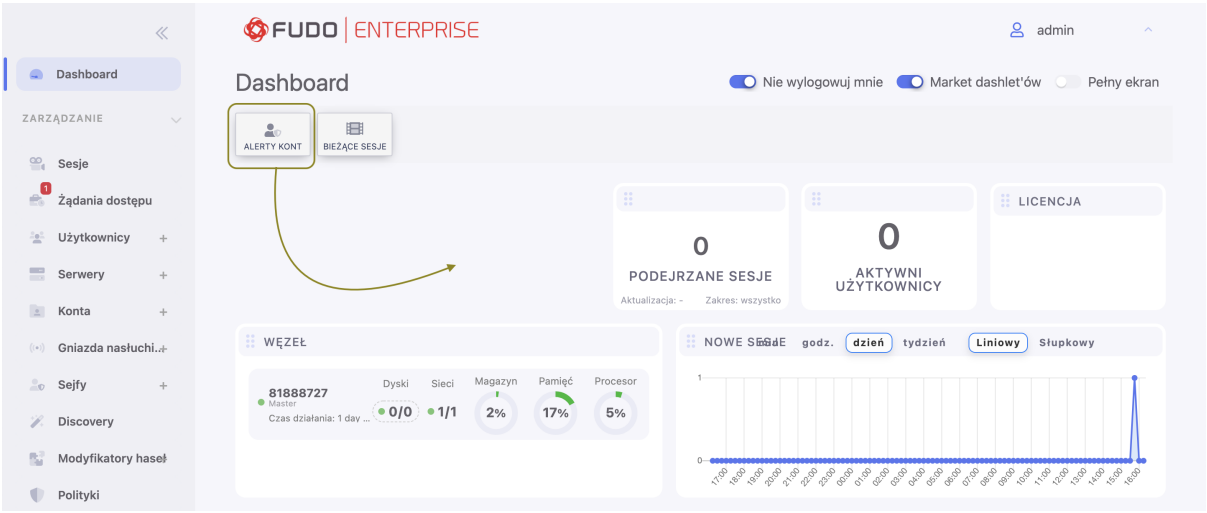
Nowe sesje	Wykres obrazujący liczbę nowo nawiązanych połączeń w jednostce czasu.
Aktualne sesje	Liczba aktualnie zestawionych połączeń.
Sesje podejrzane	Liczba sesji o wysokim stopniu zagrożenia. Widget pozwala wyświetlać podejrzane sesje według następujących konfiguracji czasowych: z ostatnich 12 godzin, ostatniego dnia, ostatniego tygodnia, lub z ostatniego miesiąca. Na widgecie jest też link, prowadzący do odfiltrowanej listy wszystkich takich sesji z określonego przedziału czasowego.
Alerty konta	Liczba kont, 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.

Uwaga

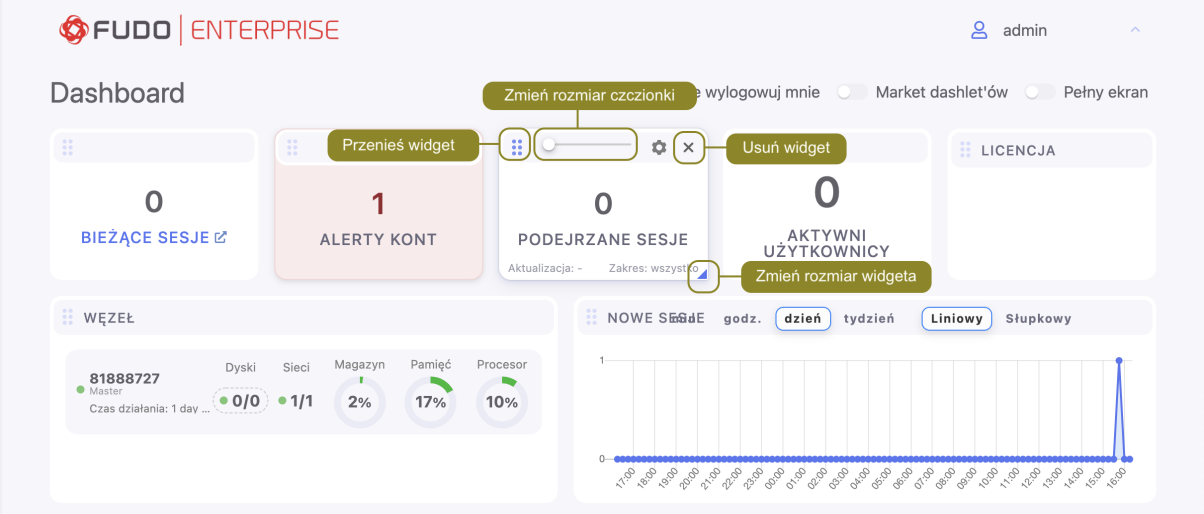
Dostępne widgety zależą od uprawnień użytkownika oraz uprawnień do obiektów.

3.10.2 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.



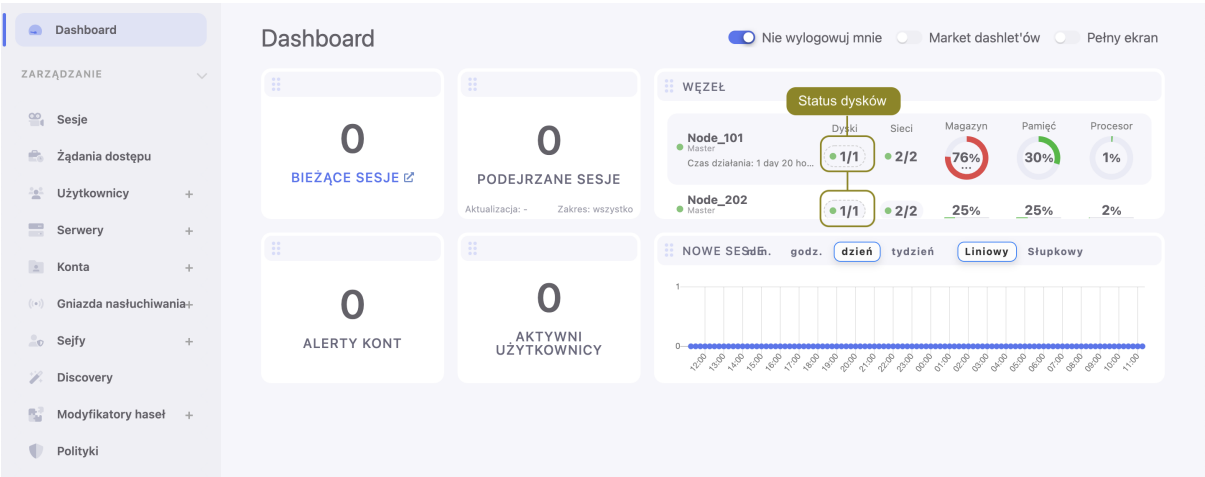
- Kliknij *Usuń*, aby potwierdzić usunięcie widgetu.

Uwaga

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

3.10.3 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*

3.11 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 Administracyjny

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

Wymagania sieciowe

Poprawne działanie 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 *Callhome*.
- Możliwości wykonywania połączeń do Fudo Enterprise przez klientów oraz z Fudo Enterprise do maszyn docelowych.
- Prawidłowo skonfigurowanego *serwera czasu*.
- Aby umożliwić zestawienie tunelu między Fudo Enterprise a Fudo ShareAccess, wymagane jest zezwolenie na ruch wychodzący na porcie 65522 do dowolnej destynacji.

Domyślne porty wykorzystywane przy pierwszym uruchomieniu

Port	Opis
443/TCP	Wymagany do celów administracyjnych.
65522/TCP	Konieczny do połączeń administracyjnych opartych na SSH oraz zestawiania tunelu z Fudo ShareAccess.
22/TCP	Wykorzystywany przez dodane domyślnie gniazdo nasłuchiwania SSH oraz aplikację mobilną Fudo Officer i usługę *Callhome*.
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.

Ostrzeżenie

Zalecenia dotyczące bezpieczeństwa IPMI

Interfejs IPMI jest dostarczany przez zewnętrznych dostawców sprzętu i działa niezależnie od naszego oprogramowania. Należy pamiętać, że w przypadku aktualizacji lub poprawek oprogramowania układowego, jesteśmy zależni od cyklu wydania Supermicro. Niestety oznacza to, że nasza zdolność do rozwiązywania niektórych problemów związanych z IPMI jest ograniczona.

Aby zmniejszyć ryzyko związane z bezpieczeństwem podczas korzystania z IPMI, zalecamy:

- Używaj silnych, unikalnych haseł do dostępu do IPMI.
- Ogranicz dostęp do IPMI do dedykowanego i izolowanego segmentu sieci.
- Wyłącz wszelkie funkcje IPMI, które nie są aktywnie używane.

Jeśli masz jakiekolwiek pytania, prosimy o **kontakt z naszym zespołem wsparcia**.

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.

Uwaga

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.

Uwaga

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.

Uwaga

- 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

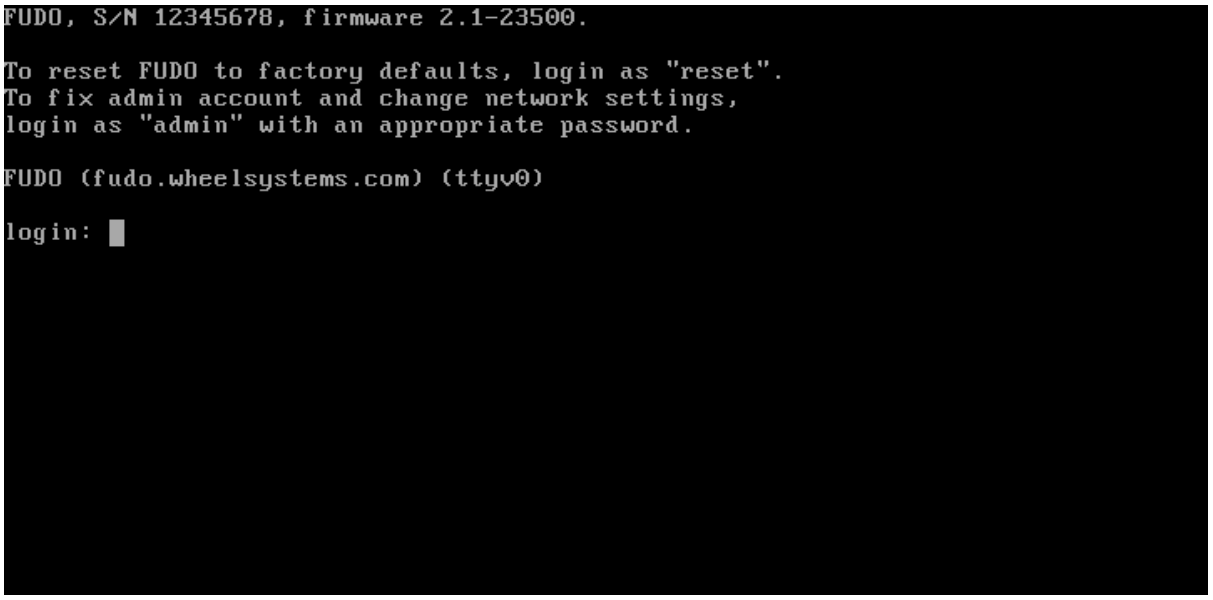
1. Podłącz do urządzenia monitor i klawiaturę.
2. Wprowadź login konta administratora.

Uwaga

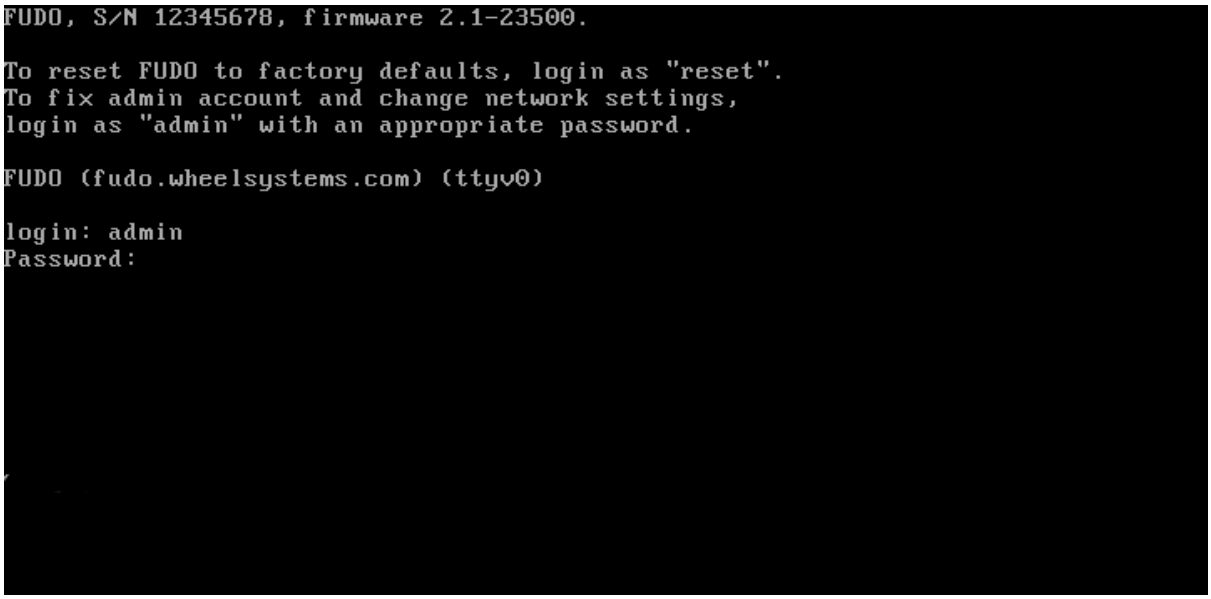
Domyślne dane logowania:

login: admin
hasło: proxycrypto

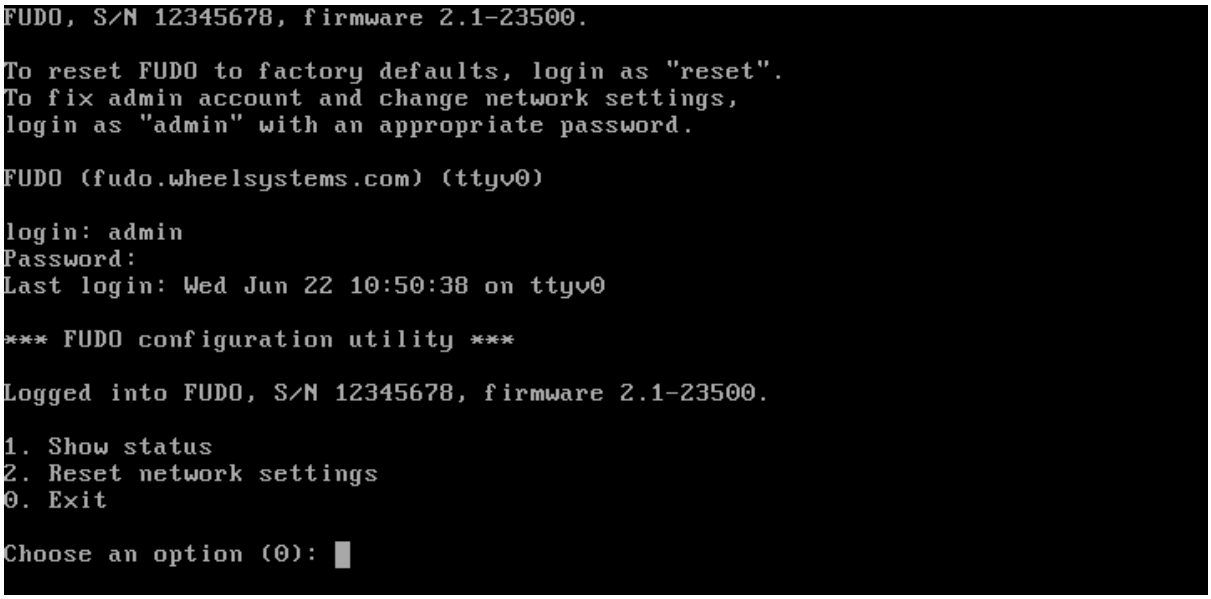
Dla wersji w chmurze domyślnym hasłem jest zazwyczaj identyfikator maszyny wirtualnej dostarczanej z Fudo Enterprise. Skontaktuj się ze sprzedawcą lub wsparciem technicznym, aby dowiedzieć się więcej.



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

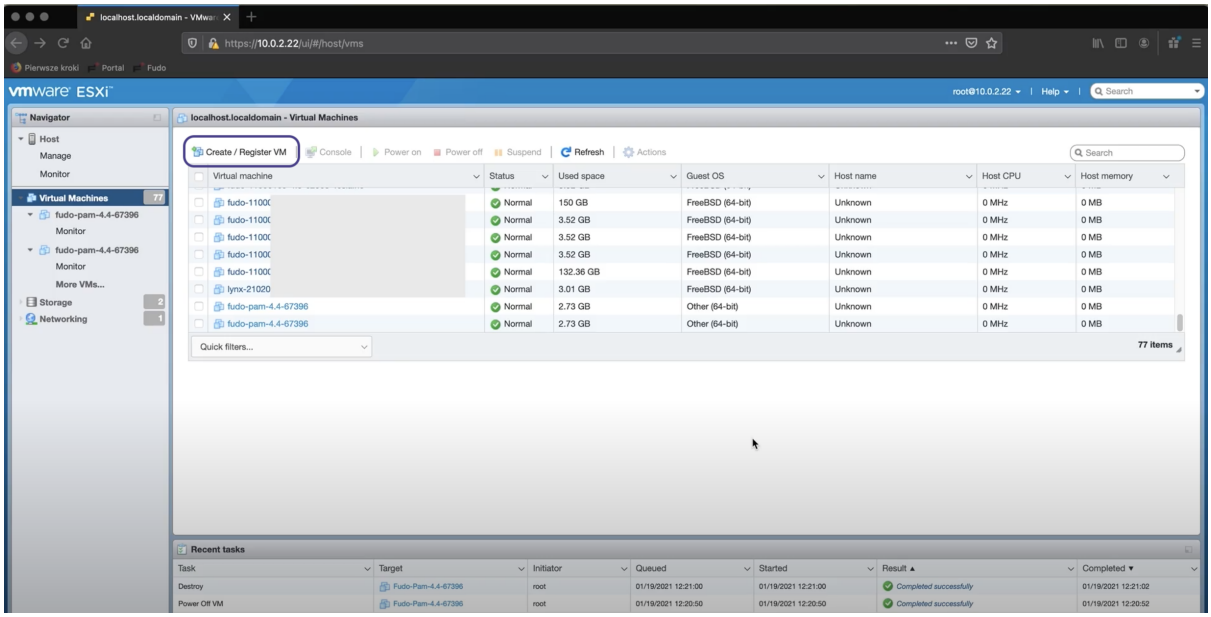
Choose an option (0): 2
Are you sure you want to continue? [y/N] (n): y
Choose new management interface (net1 net0): net0
Enter new net0 address (10.0.150.150/16): 10.0.150.150/16
Enter new default gateway IP address (10.0.0.1):
```

4.3.1 Środowisko wirtualne

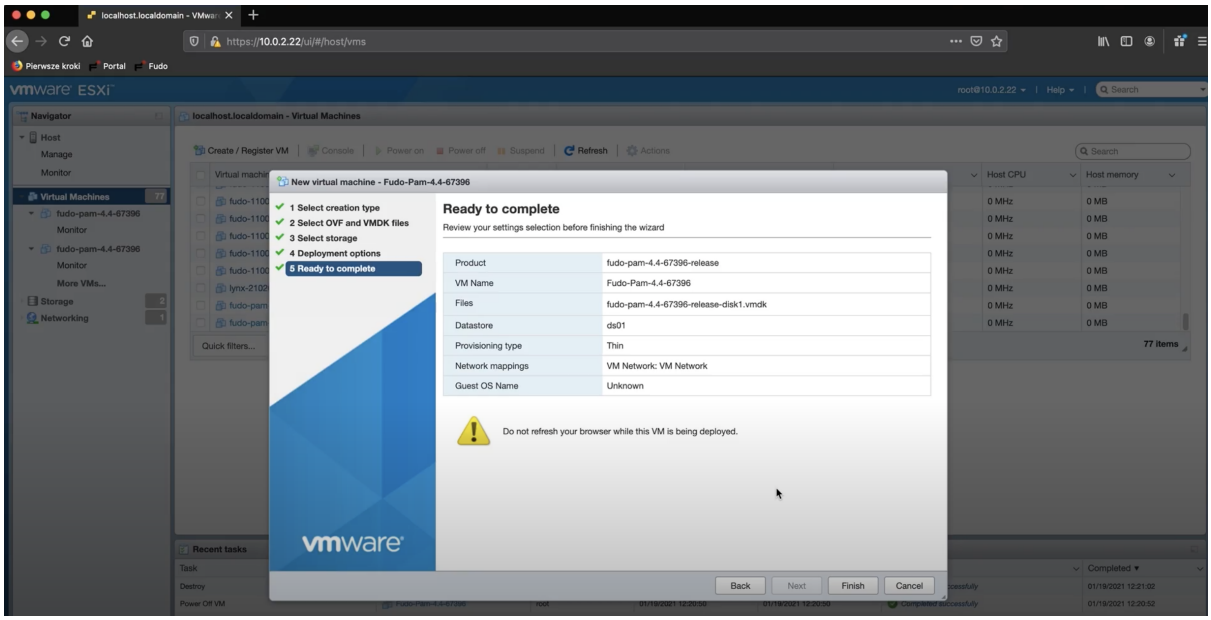
Lokalne wdrożenie Fudo Enterprise polega na załadowaniu pliku OVA / OVF do maszyny wirtualnej i uruchomieniu panelu Fudo Enterprise w przeglądarce. Poniższa instrukcja opisuje wdrożenie Fudo Enterprise przy pomocy narzędzi VMware lub Proxmox.

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.

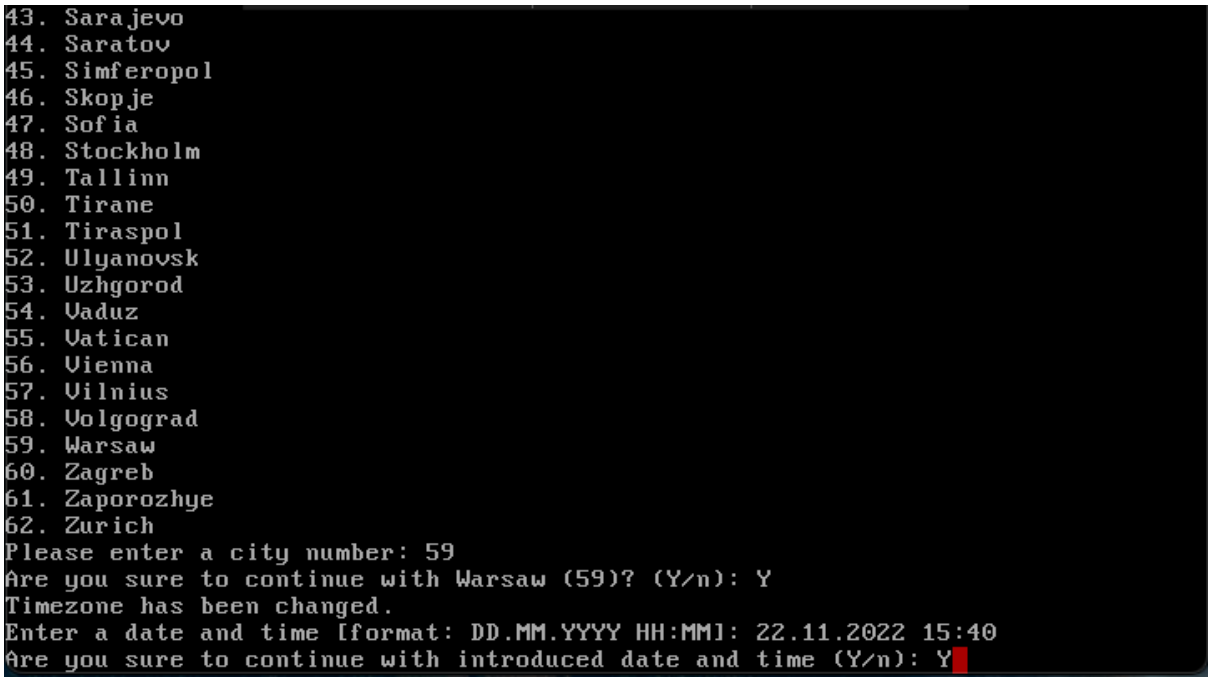


7. Kliknij *Finish* i poczekaj na załadowanie pliku konfiguracyjnego.
8. Uruchom utworzoną maszynę wirtualną.
9. Kliknij przycisk *Console* i wybierz opcję *Launch remote console*. Wybierz swoją aplikację i zweryfikuj certyfikat.
10. W konsoli podaj hasło.

Uwaga

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.

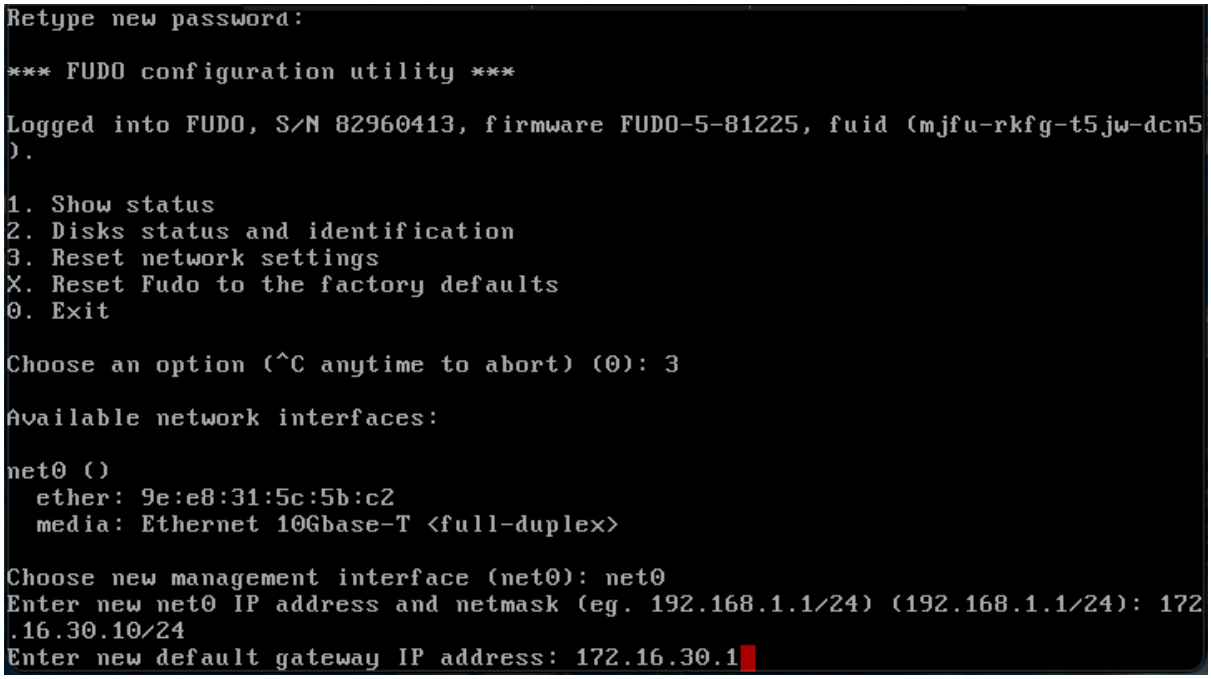
11. Wybierz region oraz miasto podając odpowiednie kody z listy i potwierdź swój wybór.
12. Wprowadź datę i godzinę w formacie `DD.MM.RRRR GG:MM`.



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.



Uwaga

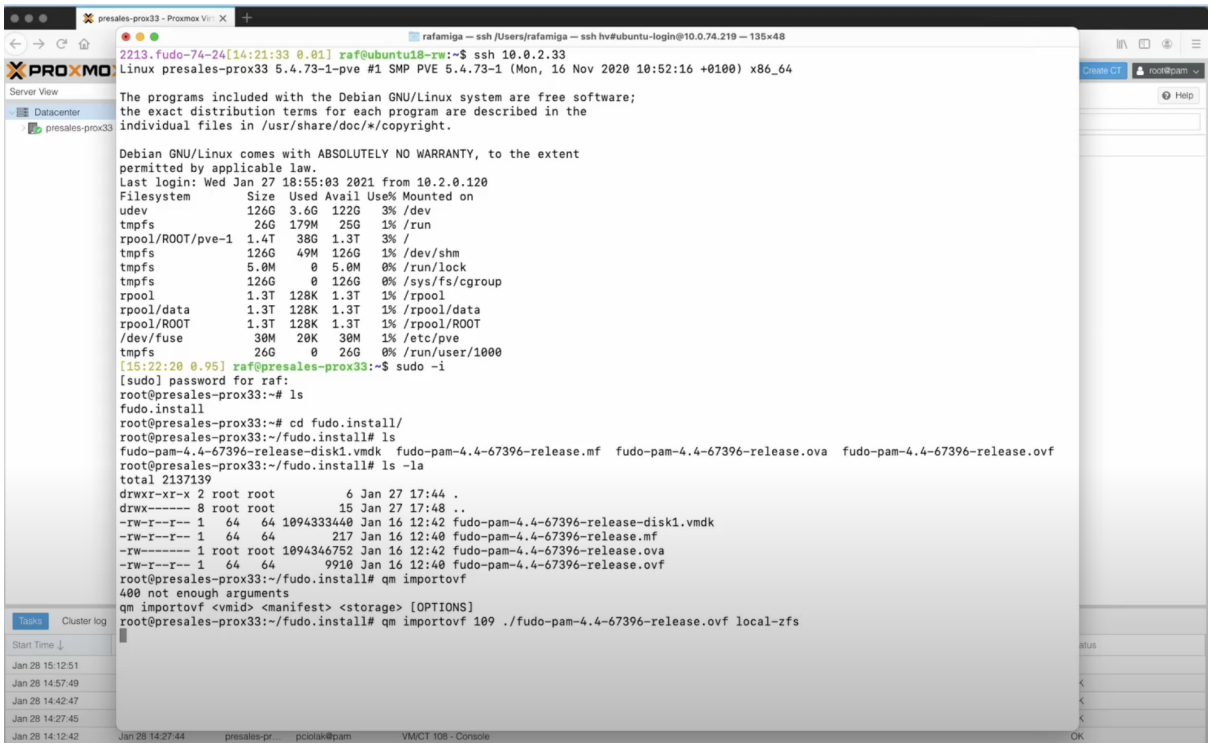
Twoja instancja Fudo Enterprise została pomyślnie zainicjowana! Teraz możesz wprowadzić zarejestrowany adres IP w przeglądarce i rozpocząć pierwszą konfigurację Fudo Enterprise.

Inicjacja w Proxmox przy użyciu pliku OVF

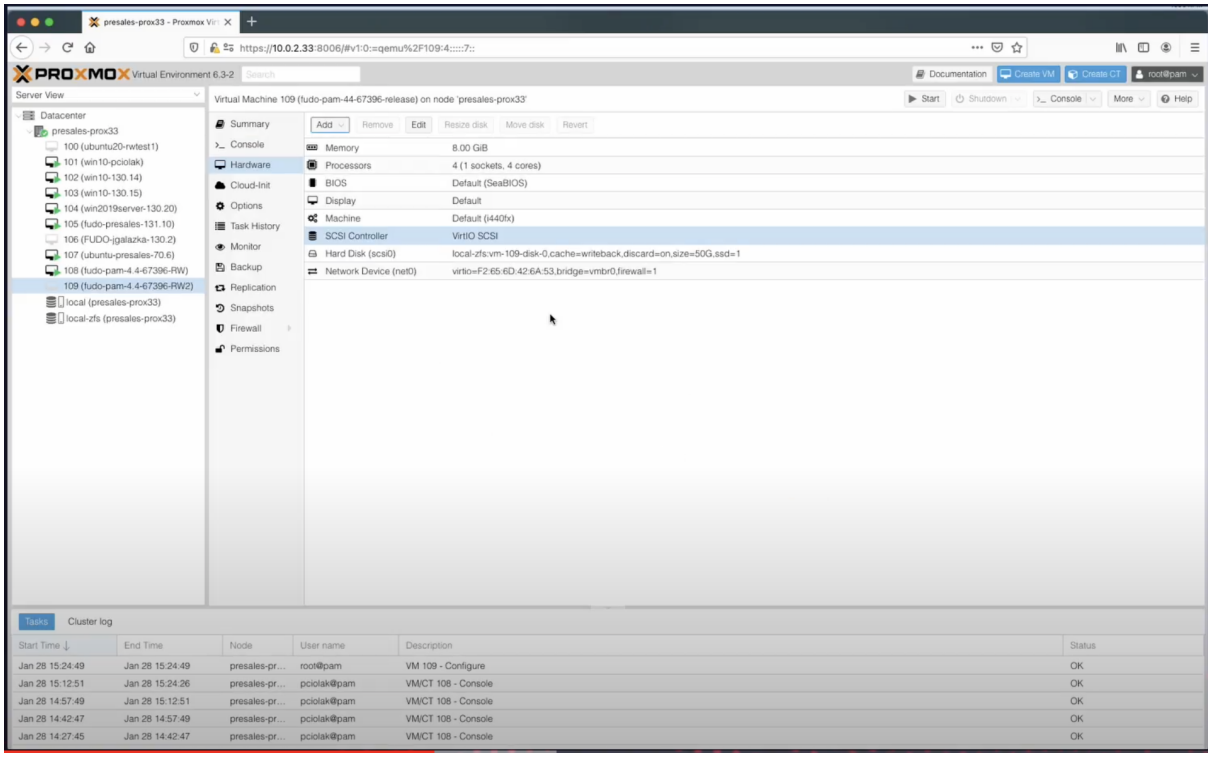
1. Utwórz nową maszynę wirtualną używając parametrów z manifestu pliku OVF, a następnie zaimportuj dyski do lokalizacji `local-zfs`:
   a. Zaloguj się do komputera zdalnego, np. za pomocą `ssh 10.0.2.33` i podaj hasło.
   b. W katalogu *fudo.install* wywołaj komendę: `qm importovf <vmid> <manifest> 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

      Np:

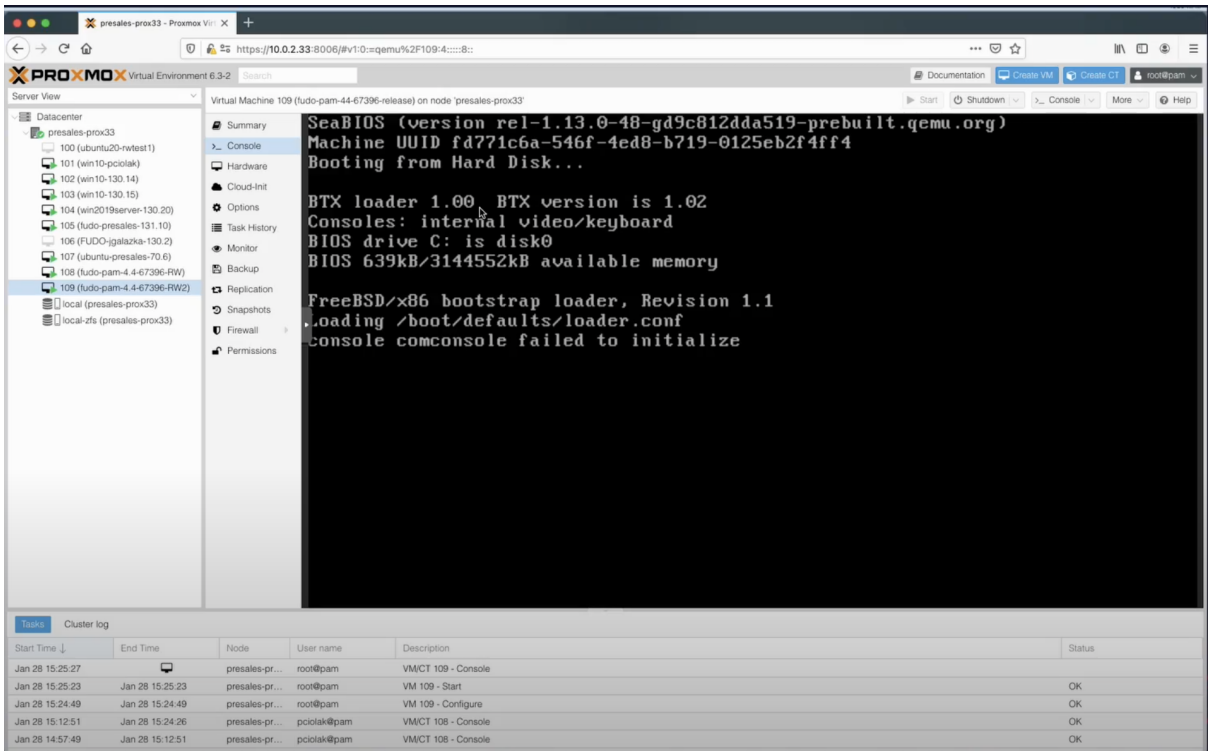
      ```
      qm importovf 109 ./fudo-one-36271-release.ovf local-zfs
      ```



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.

Uwaga

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.

> **Uwaga**
>
> 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*

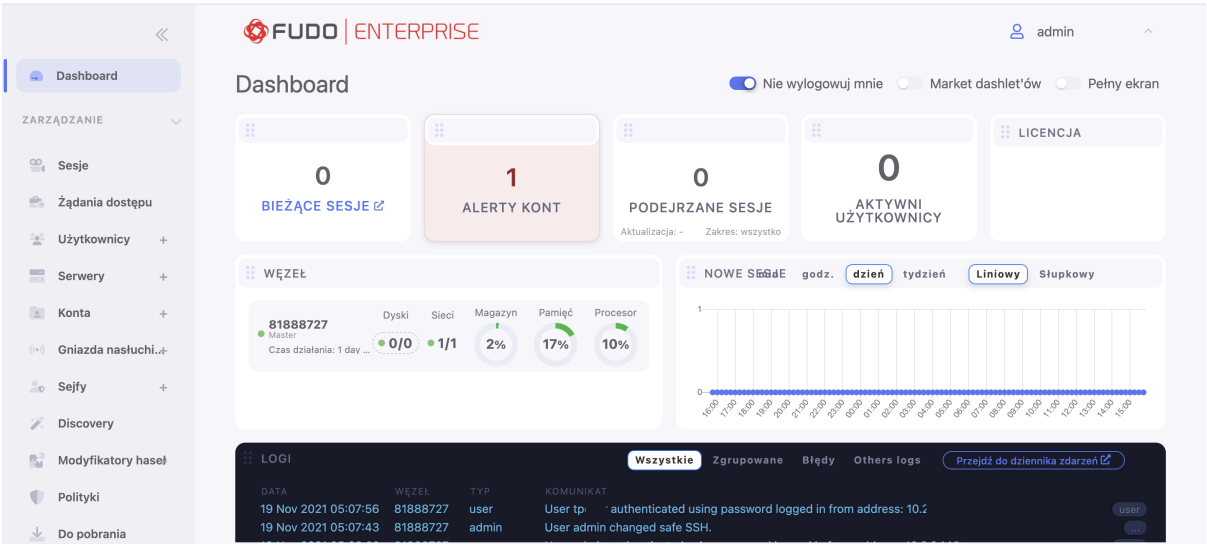
4.4 Dostęp do portali Fudo Enterprise

Fudo Enterprise oferuje dwa interfejsy dostępu:

- Panel Administracyjny - służący do zadań administracyjnych,
- Portal Użytkownika - umożliwiający łatwy dostęp zdalny do zasobów.

4.4.1 Panel Administracyjny

Panel Administracyjny to centralny interfejs zarządzania w Fudo Enterprise, przeznaczony głównie dla administratorów. Udostępnia on narzędzia do konfiguracji systemu, zarządzania użytkownikami, ustawień bezpieczeństwa oraz innych zadań administracyjnych. Jest to centrum zarządzania i konfiguracji systemu Fudo Enterprise.



Aby uzyskać dostęp do Panelu Administracyjnego wykonaj poniższe kroki:

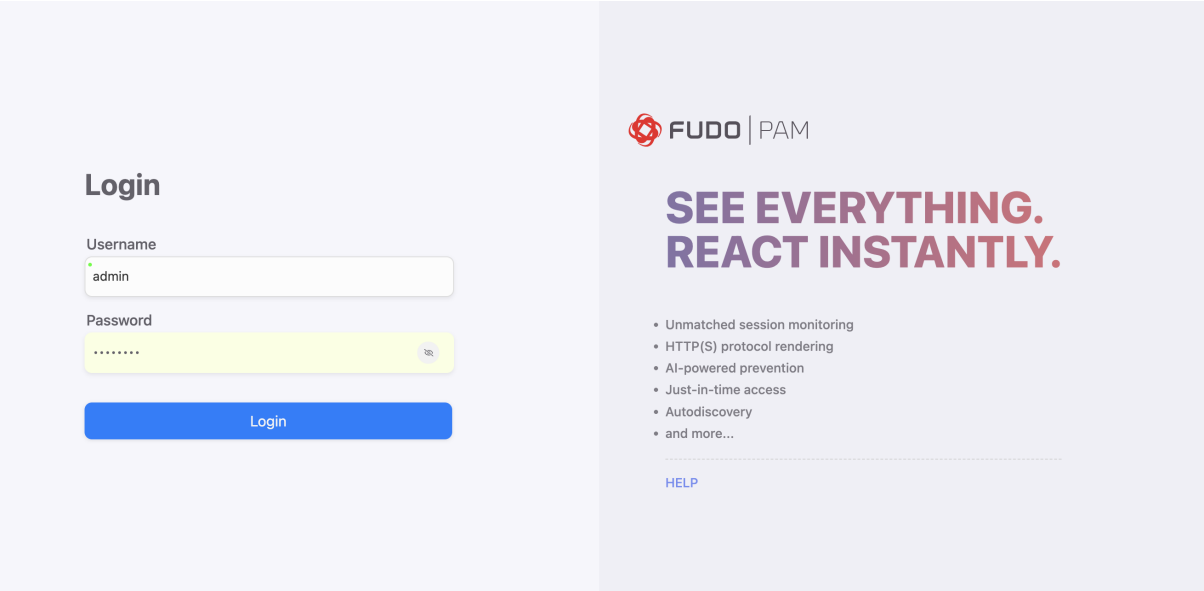
1. Otwórz przeglądarkę internetową i przejdź do adresu IP przydzielonego dla Panelu Administracyjnego. Zazwyczaj jest to adres IP skonfigurowany podczas *procedury wdrażania*.

2. Podaj dane logowania do konta administratora i kliknij przycisk Zaloguj.

Uwaga

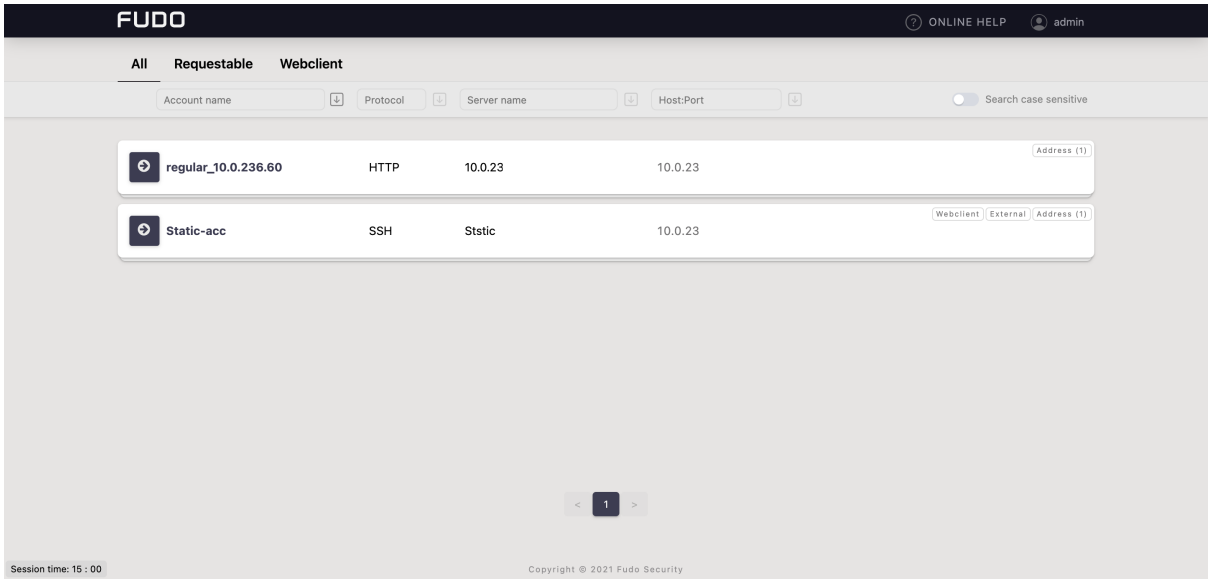
Domyślne dane logowania:

login: admin
hasło: proxycrypto



4.4.2 Portal Użytkownika

Ten komponent jest przeznaczony dla użytkowników końcowych. Portal Użytkownika umożliwia przeglądanie listy zasobów, do których użytkownik posiada stosowne uprawnienia i inicjowanie połączenia z monitorowanym zasobem za pośrednictwem wybranego gniazda nasłuchiwania.



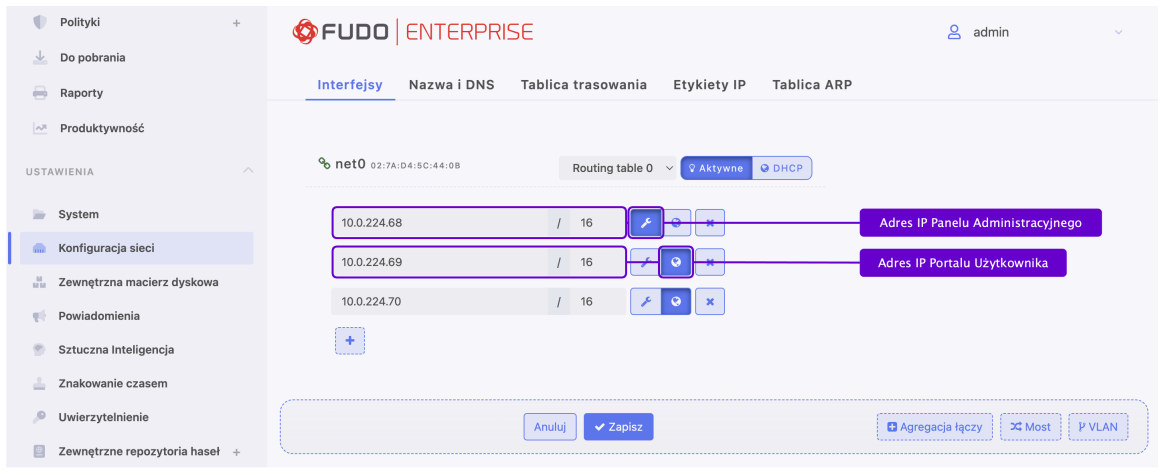
Aby zalogować się do Portalu Użytkownika wykonaj poniższe kroki:

1. Otwórz przeglądarkę internetową i przejdź do adresu IP przydzielonego dla Portalu Użyt-

kownika.

Uwaga

Adres IP Portalu Użytkownika można uzyskać od administratora systemu lub z menu *Ustawienia* > *Konfiguracja sieci* w Panelu Administracyjnym. Aby dowiedzieć się więcej, zapoznaj się z rozdziałem *Konfiguracja ustawień sieciowych*.



4.4.3 Obsługiwane przeglądarki internetowe

4.4.4 Obsługiwane przeglądarki internetowe

Dostęp do portali Fudo Enterprise jest wspierany w przeglądarkach Google Chrome oraz Mozilla Firefox w systemach Microsoft Windows, Ubuntu oraz macOS.

Powiązane tematy:

- *Przegląd systemu*
- *Wspierane protokoły*
- *Szybki start*

ROZDZIAŁ 5

Szybki start

5.1 SSH

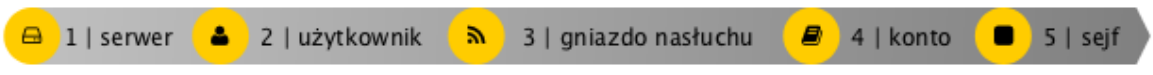
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie połączeń SSH ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łącząc się ze zdalnym serwerem, wykorzystując protokół *SSH* uwierzytelnia się na Fudo Enterprise używając własnego 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

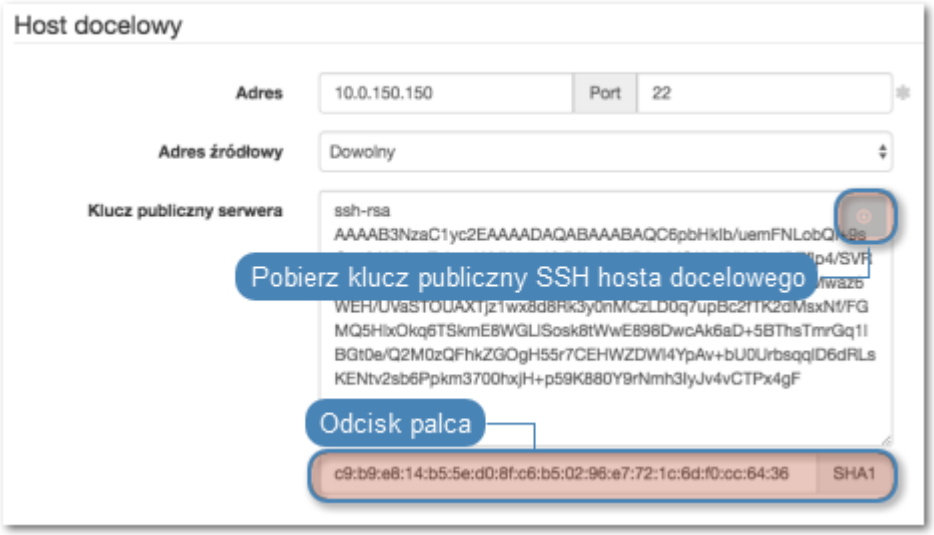
Serwer jest definicją zasobu infrastruktury IT, z którym istnieje możliwość nawiązania połączenia za pośrednictwem wskazanego protokołu.

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*.

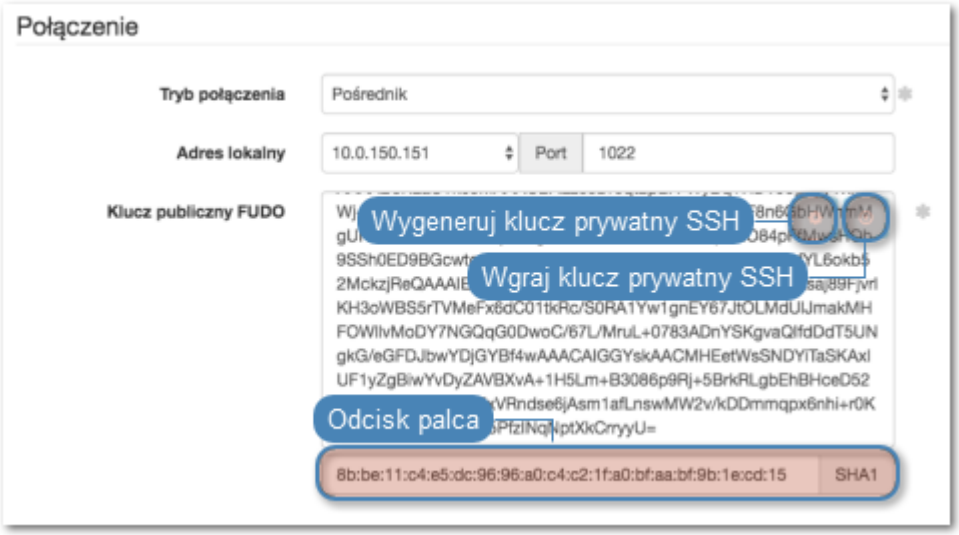
Dodanie gniazda nasłuchiwania

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.



Uwaga

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:

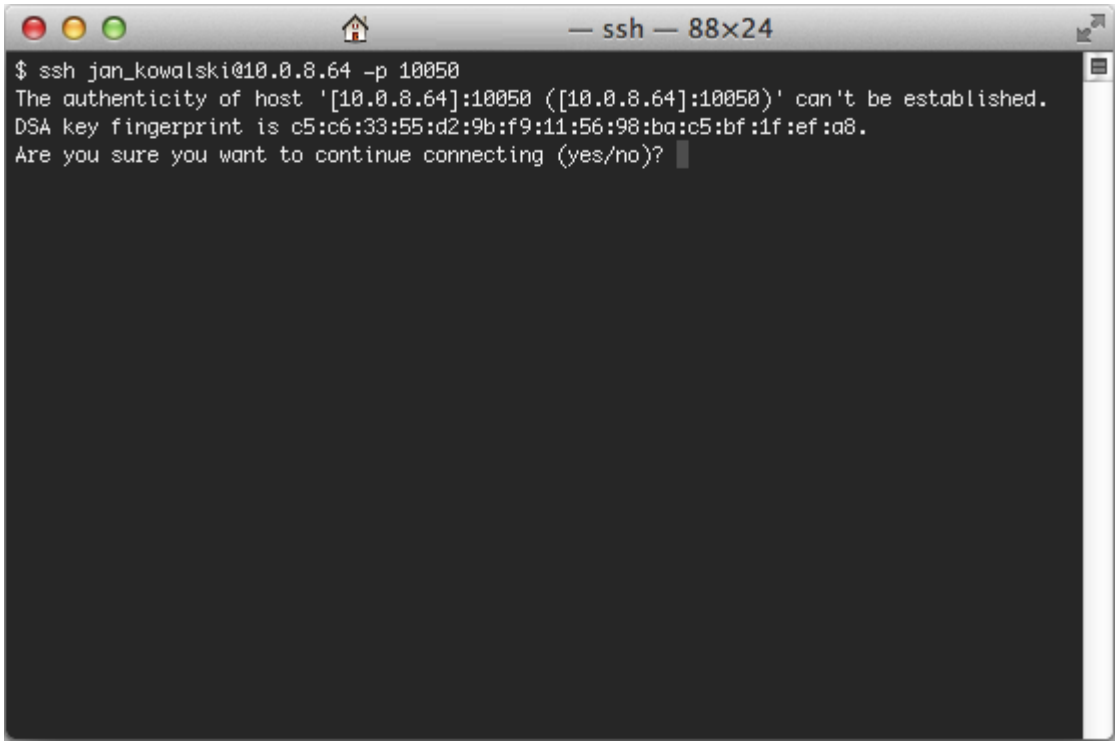
Parametr	Wartość
Nazwa	`ssh_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`
Funkcjonalność protokołów	
RDP	✗
SSH	✓
VNC	✗

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:



Uwaga

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.

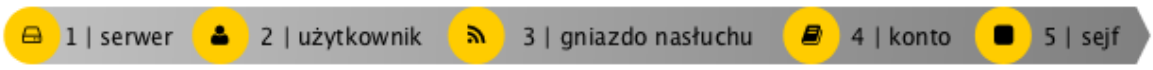
Fudo Enterprise zestawiając połączenie ze zdalnym serwerem dokonuje podmiany hasła i loginu na `root`/`password` (tryby uwierzytelniania opisane są w sekcji *Tryby uwierzytelniania użytkowników*).



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.

Uwaga

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

5. Kliknij *Zapisz*.

Uwaga

Upewnij się, że w ustawieniach sieciowych, na wskazanym adresie IP nie jest ustawiona funkcja *Panel Administracyjny*.

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:

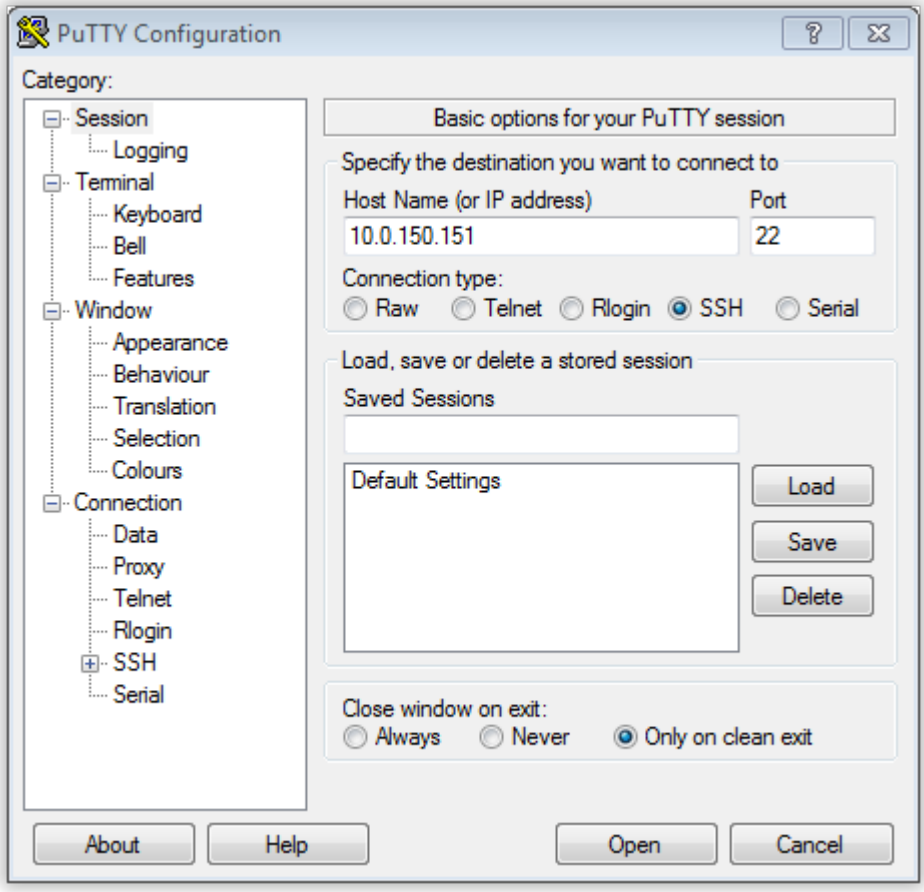
Parametr	Wartość
Ogólne	
Nazwa	`ssh_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`
Funkcjonalność protokołów	
RDP	✗
SSH	✓
VNC	✗

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*.

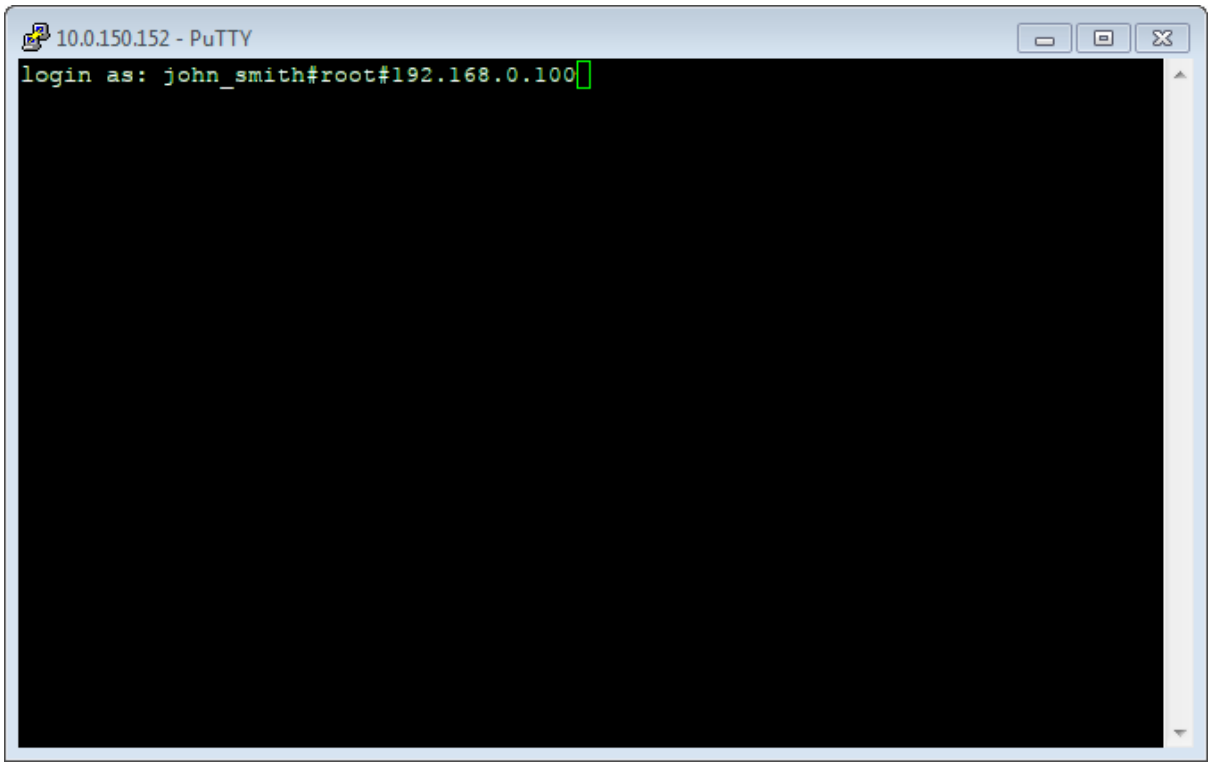
5.2.3 Nawiązanie połączenia

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>
```

Przykład:

```
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 SSH w trybie bastionu z opcją Jump Host

Fudo Enterprise umożliwia nawiązanie połączenia z serwerem z wykorzystaniem opcji *Jump Host*.

Scenariusz zakłada, że użytkownik łącząc się z serwerem pełniącym funkcję *Jump Hosta,* wykorzystując protokół *SSH* nawiązuje automatycznie połączenie z serwerem docelowym. Użytkownik musi wskazać w treści loginu:

- nazwę użytkownika,
- login konta na serwerze *Jump Host,*
- adres serwera *Jump Host,*
- login konta na serwerze docelowym,
- adres serwera docelowego.

5.3.1 Założenia

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

5.3.2 Konfiguracja

Dodanie serwera Jump Host

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

W poniższej konfiguracji podaj dane serwera pełniącego rolę *Jump Hosta.*

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

Parametr	Wartość
Nazwa	ssh_server
Opis	✗
Zablokowane	✗
Protokół	`SSH`
Starszy szyfr	✗
Adres źródłowy	`Dowolny`
Miejsce przeznaczenia	
IPv4	`192.168.10.90`
Port	`22`

4. W sekcji *Weryfikacja serwera* wybierz *Klucz publiczny serwera* i kliknij *Pobierz klucz publiczny*, aby pobrać klucz lub wprowadź go w polu tekstowym.
5. Kliknij *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 gniazdo nasłuchiwania*.
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.

Uwaga

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

5. Kliknij *Zapisz*.

Uwaga

Upewnij się, że w ustawieniach sieciowych, na wskazanym adresie IP nie jest włączona opcja dostępu do Panelu 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 konto*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`admin_ssh_server`
Zablokowane	✗
Typ	`REGULAR`
Nagrywanie sesji	`noraw`
Notatki	✗
Uprawnienia	
Uprawnieni użytkownicy	✗
Cel	
Serwer	`ssh_server`
Poświadczenia	
Domena	✗
Login	`root`
Zastąp sekret	`hasłem`
Hasło	`password`
Retencja danych	
Nadpisz globalne ustawienia retencji	✗

5. Kliknij *Zapisz i wyjdź*.

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 sejf*.
3. Uzupełnij parametry konfiguracyjne:

Parametr	Wartość
Nazwa	`ssh_safe`
Zablokowane	✗
Ogólne	
Powód logowania	✗
Limit czasu sesji	✗
Limit braku aktywności sesji	✗
Funkcjonalność	
RDP	✗
SSH	✓
VNC	✗

4. Przejdź na zakładkę *UŻYTKOWNICY*.
5. Kliknij *Zarządzaj użytkownikami*.
6. Znajdź i zaznacz użytkownika *john_ smith*.
7. Kliknij *Zapisz*.
8. Przejdź do zakładki *KONTA*.
9. Kliknij *Zarządzaj kontami*.
10. Znajdź i zaznacz konto `admin_ssh_server`.
11. Kliknij *Zapisz*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.
13. Znajdź i zaznacz obiekt `ssh_listener`.
14. Kliknij *Zapisz*.
15. Kliknij *Zapisz i wyjdź*.

5.3.3 Nawiązanie połączenia

W celu nawiązania połączenia należy zastosować w terminalu poniższy format komendy logowania. Poniższy przykład obrazuje scenariusz połączenia loginem `root` z serwerem 192.168.0.110 poprzez serwer *Jump Host* o adresie 192.168.10.90.

```
ssh -J '<fudo-user>%%<jump-host-server-user>%%<jump-host-server-address>@<fudo-
↪address>' <target-server-user>@<target-server-address>
```

Przykład:

```
ssh -J 'john_smith%%root%%192.168.10.90@10.0.150.151' root@192.168.0.110
```

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*

5.4 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*).



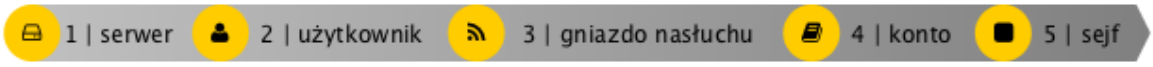
Uwaga

Fudo Enterprise wspiera **sesje wielomonitorowe** w protokole RDP, co pozwala na monitorowanie i rejestrację sesji odbywających się na więcej niż jednym ekranie.

5.4.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało przeprowadzone prawidłowo. Informacje na temat scenariuszy wdrożenia znajdziesz w rozdziale *Scenariusze wdrożenia*.

5.4.2 Konfiguracja



Dodanie serwera

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

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

Parametr	Wartość
Nazwa	rdp_server
Opis	`Serwer RDP`
Zablokowane	✘
Protokół	`RDP`
Bezpieczeństwo	`Standard RDP Security`
Adres źródłowy	`Dowolny`
Uprawnienia	
Uprawnieni użytkownicy	✘
Adresy serwerów	
Adres IP	`10.0.35.10`
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*.

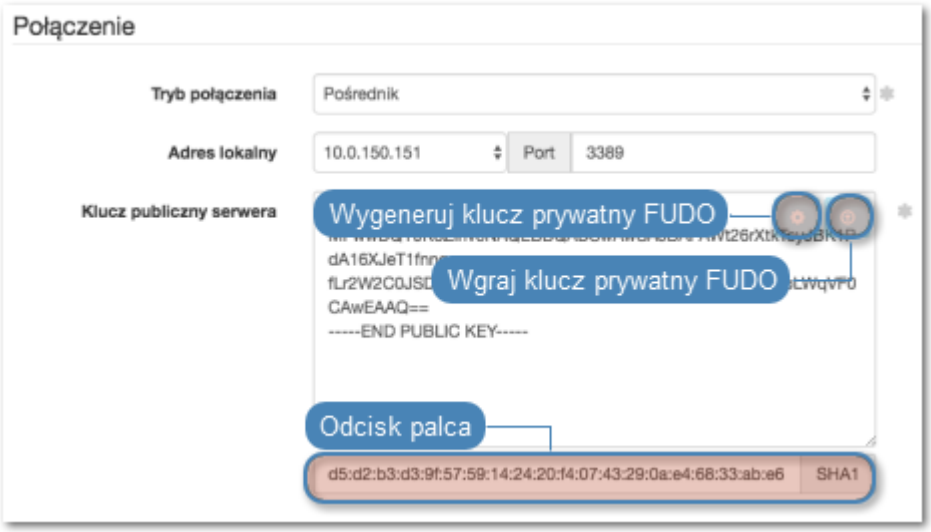
Dodanie gniazda nasłuchiwania

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.

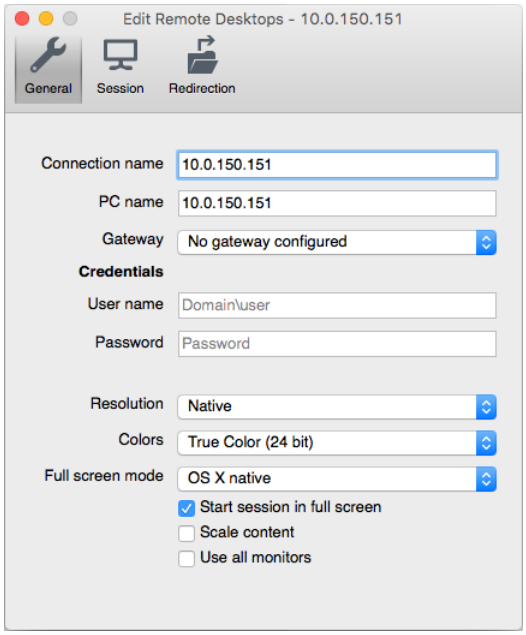
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

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`

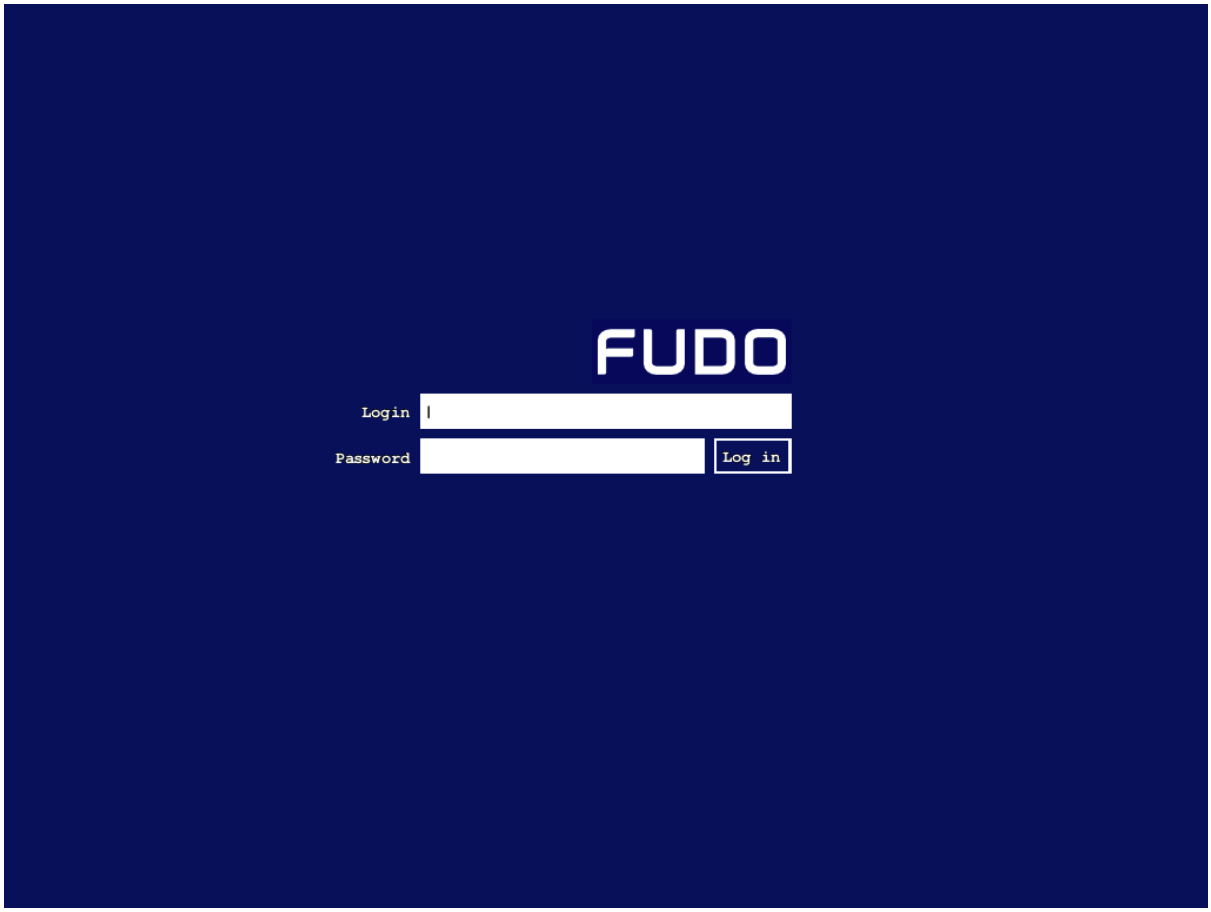
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_ smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_rdp_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.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

5.4.3 Nawiązanie połączenia

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

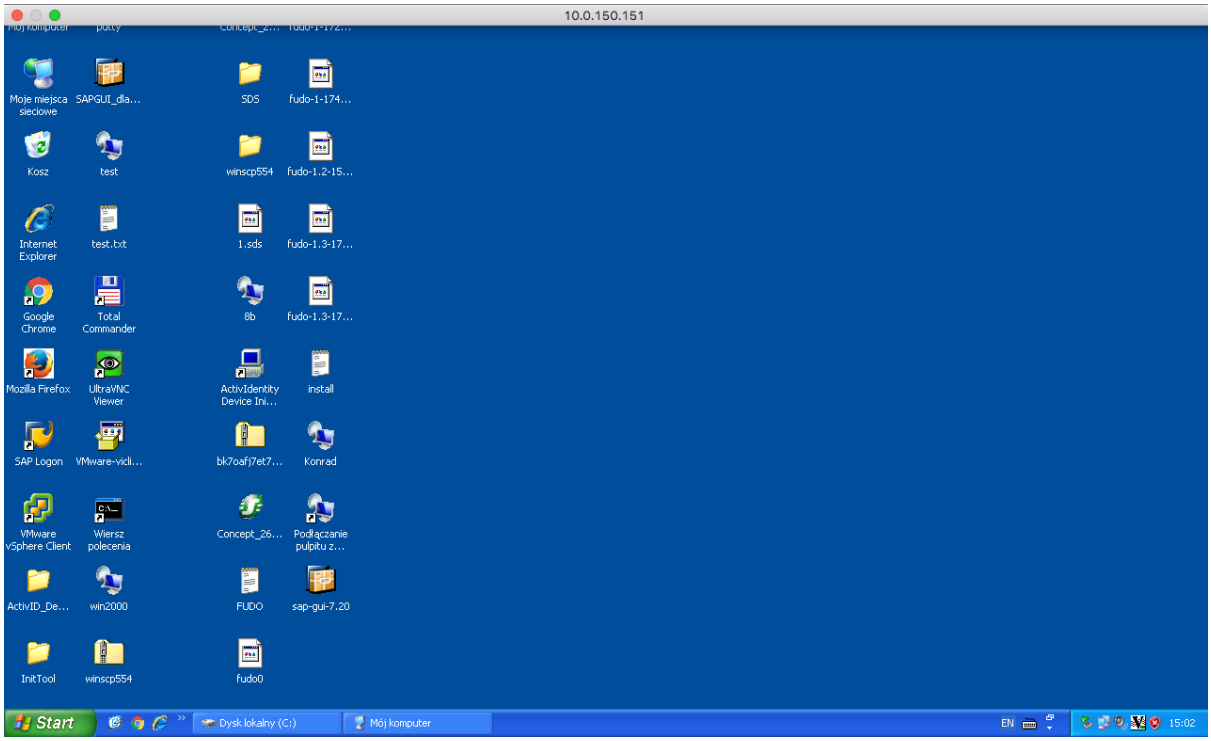


3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter].



Uwaga

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

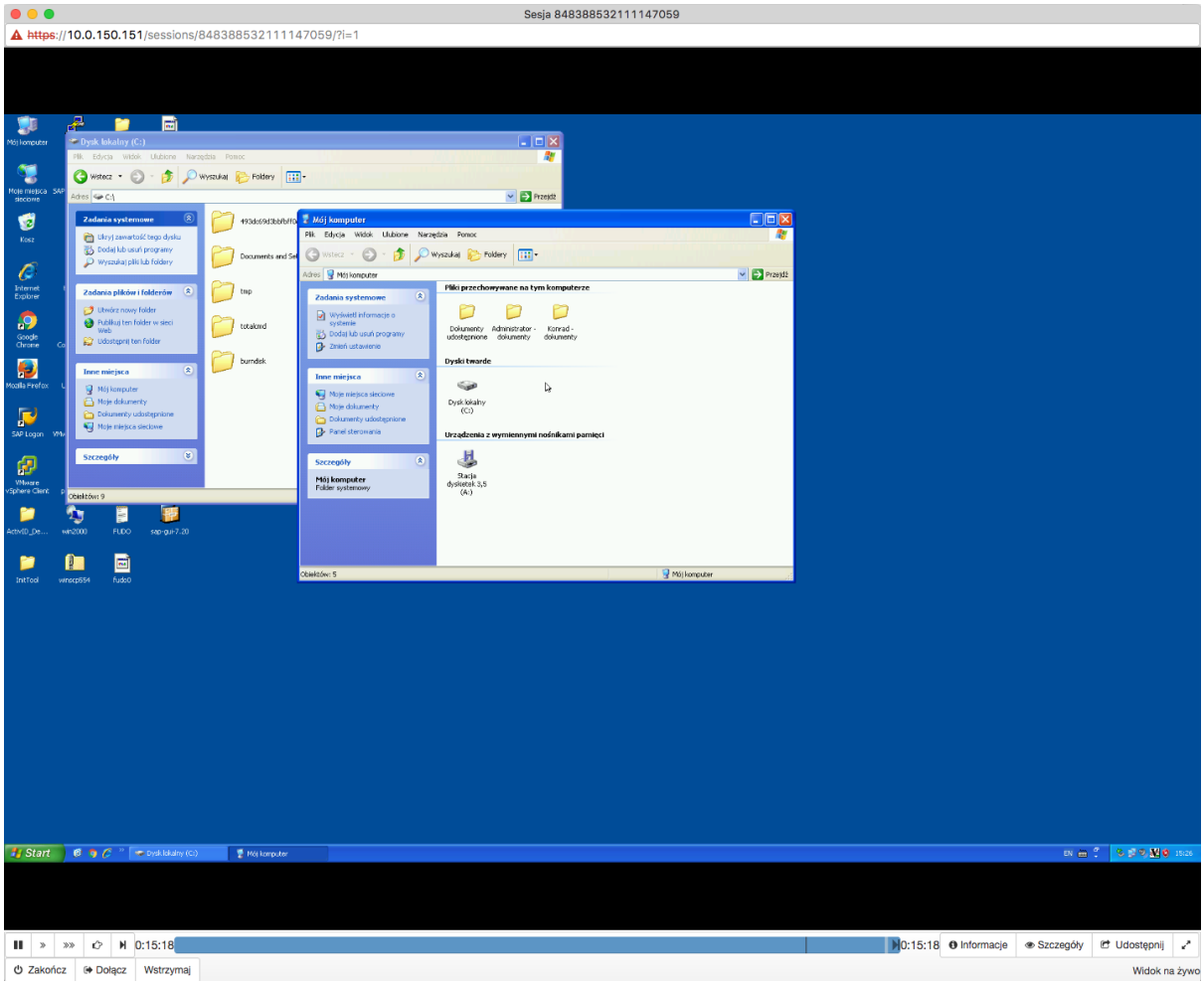


5.4.4 Podgląd sesji połączeniowej

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

> **Uwaga**
>
> 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*

5.5 RDP w trybie bastionu

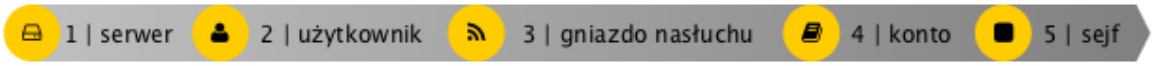
W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie połączeń RDP ze zdalnym serwerem. Scenariusz zakłada, że użytkownik łączy się ze zdalnym serwerem w trybie bastionu, wskazując w loginie nazwę użytkownika, login konta na serwerze docelowym 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*).



5.5.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Informacje na temat scenariuszy wdrożenia znajdziesz w rozdziale *Scenariusze wdrożenia*.

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 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`
Weryfikacja 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	✗

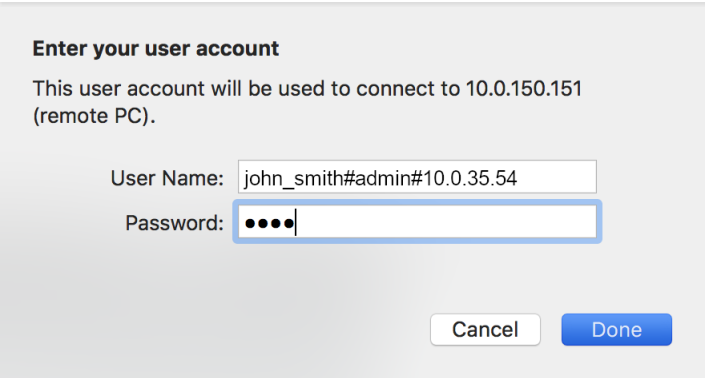
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_ smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `admin_rdp_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.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

5.5.3 Nawiązanie połączenia

1. Uruchom klienta połączeń RDP.
2. Skonfiguruj połączenie zdalnego pulpitu.
3. Wprowadź nazwę użytkownika, login konta na serwerze docelowym (login serwera) oraz adres serwera docelowego (np: `john_smith#admin#10.0.35.54`) oraz hasło użytkownika.

Uwaga

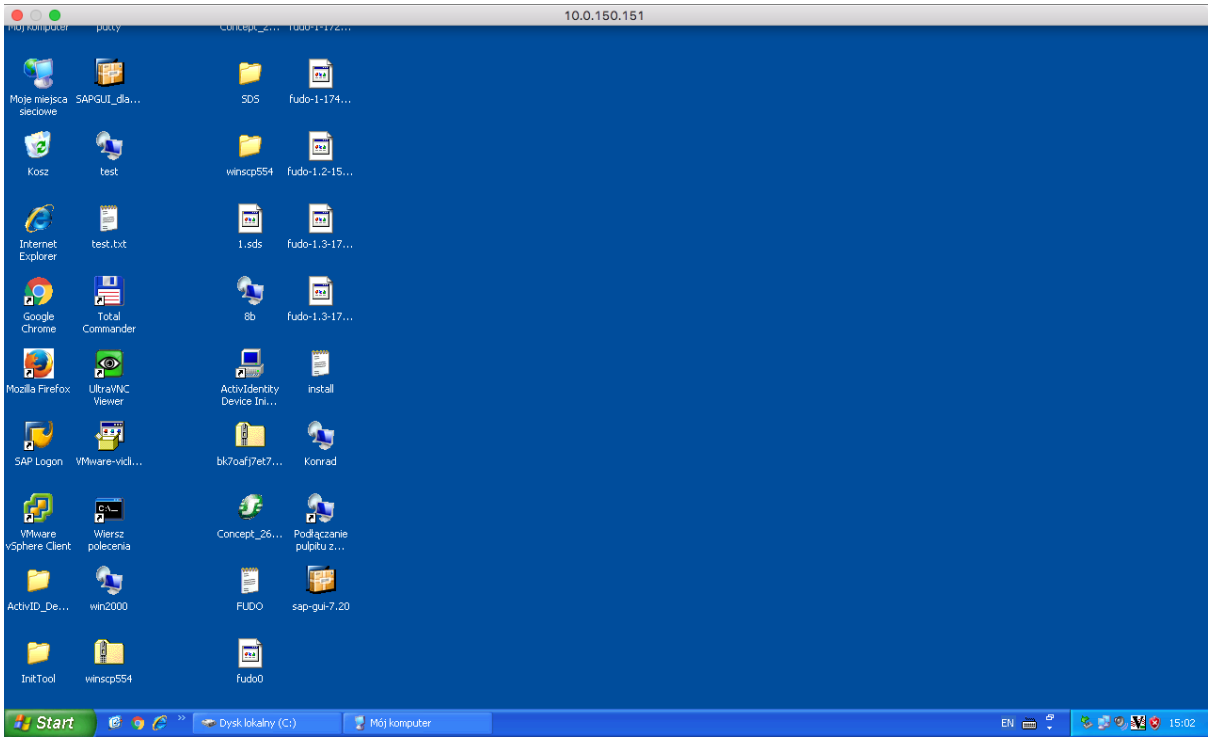
Podczas łączenia się przy użyciu konta typu *forward,* gdzie nazwa użytkownika i login serwera są identyczne, wartość *Login serwera* może zostać pominięte (np: `john_smith##10.0.35.54`).



Uwaga

- Jeśli użytkownik nie wyspecyfikuje danych logowania w kliencie RDP, Fudo Enterprise wyświetli własny ekran logowania, który należy uzupełnić danymi logowania użytkownika, nazwą konta uprzywilejowanego oraz adresem serwera.
- Podczas łączenia się przy użyciu konta typu *forward,* gdzie *Nazwa użytkownika* i *Login serwera* są identyczne, pole *Login serwera* na ekranie logowania może zostać pominięte.
- 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*.





5.5.4 Podgląd sesji połączeniowej

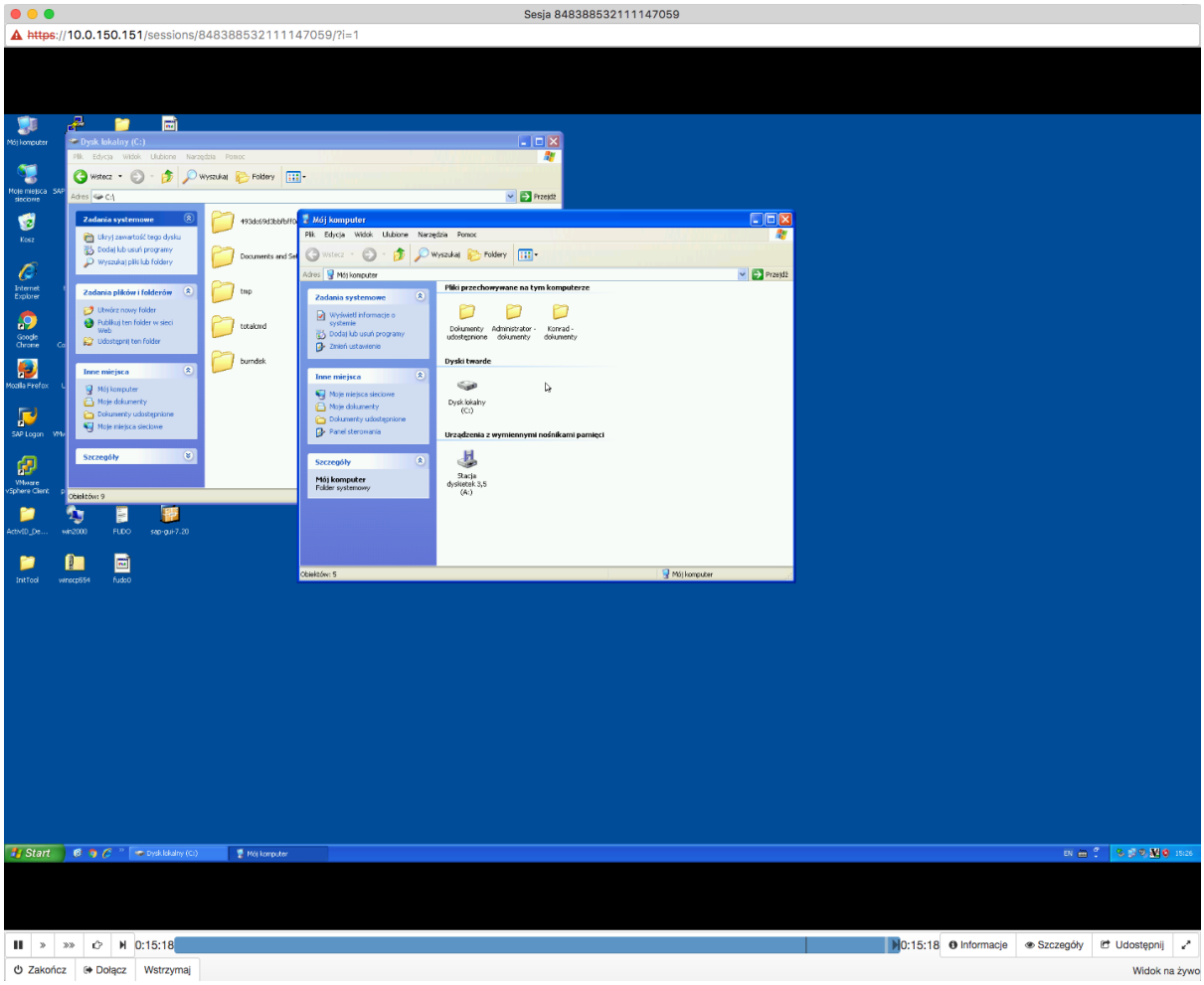
1. W przeglądarce internetowej wpisz adres IP, pod którym dostępny jest panel zarządzający Fudo Enterprise.

Uwaga

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*

5.6 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.

Uwaga

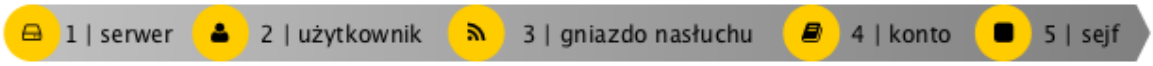
Połączenia telnet realizowane za pośrednictwem Fudo Enterprise nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu przez Fudo Enterprise musi uwierzytelnić się na serwerze docelowym po zestawieniu połączenia.



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`
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*.

5.6.3 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:

```
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:
```

Uwaga

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.

Uwaga

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 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.

Uwaga

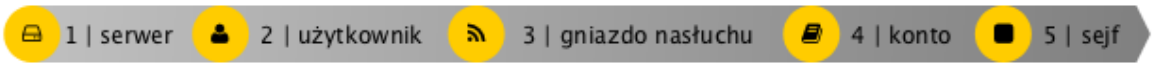
Połączenia telnet realizowane za pośrednictwem Fudo Enterprise nie wspierają mechanizmów podmiany i przekazywania haseł. Użytkownik po wstępnym uwierzytelnieniu przez Fudo Enterprise musi uwierzytelnić się na serwerze docelowym po zestawieniu połączenia.



5.7.1 Założenia

Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia opisana jest 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	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	✗

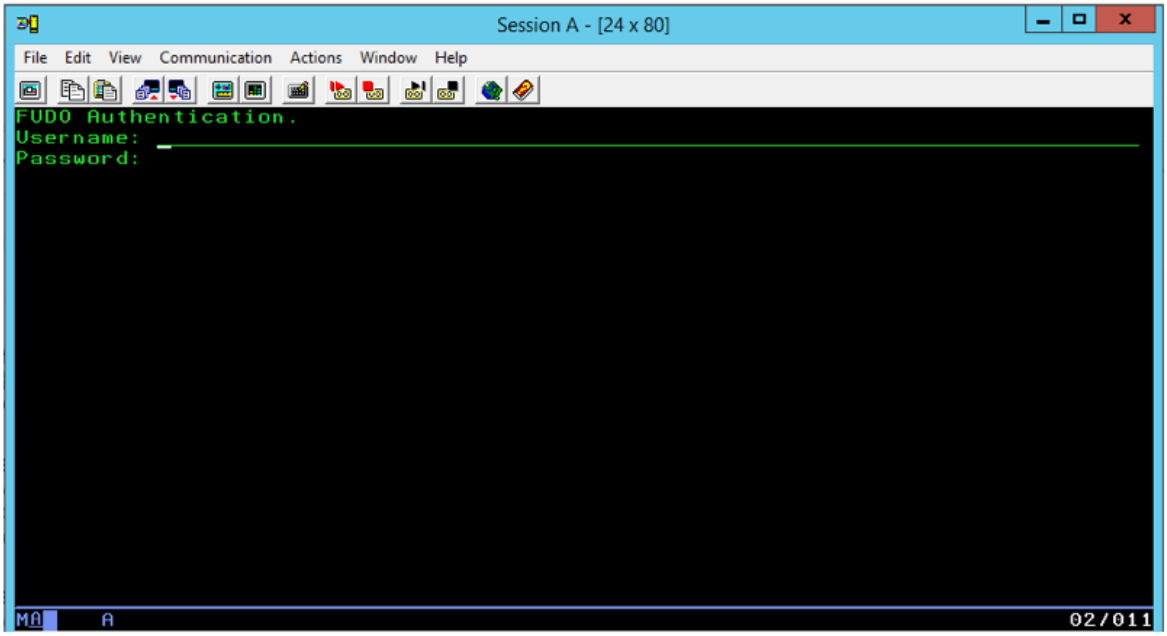
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij + *Dodaj użytkownika*.
6. Znajdź użytkownika *john_ smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij + *Dodaj konto*.
10. Znajdź konto `admin_telnet_server` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda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

5.7.3 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.

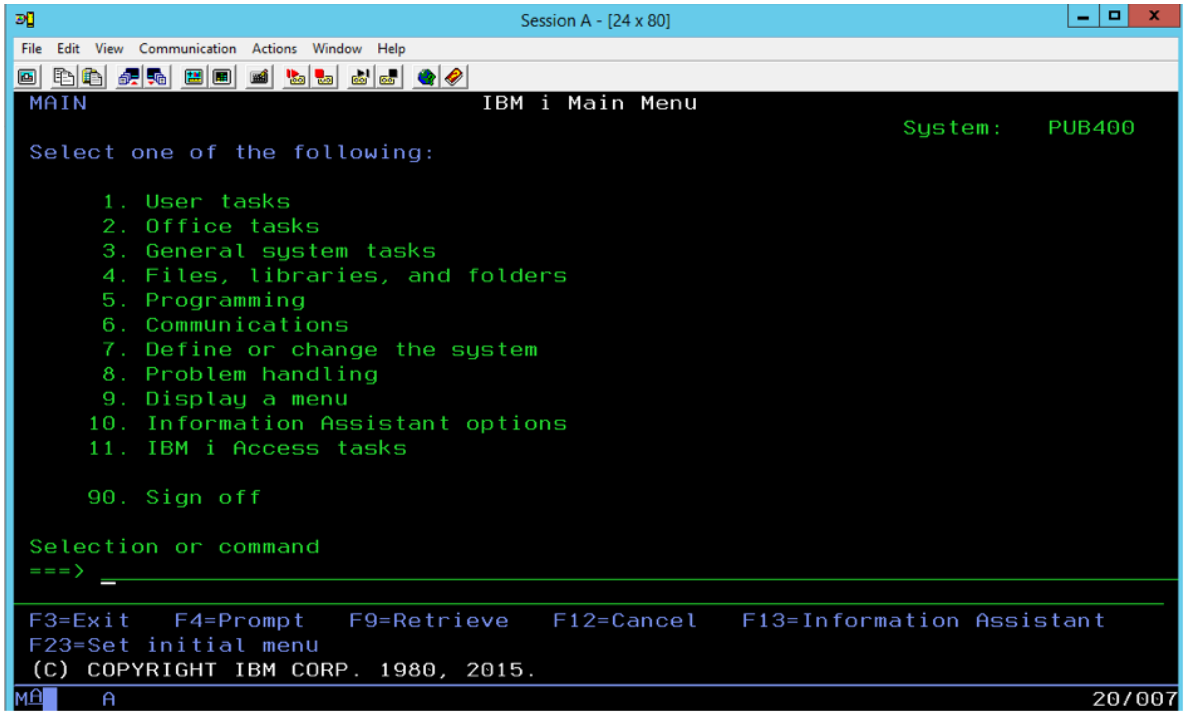


4. Wprowadź dane uwierzytelniające użytkownika na serwerze:

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

Uwaga

Połączenia telnet nie wspierają mechanizmów podmiany danych logowania.

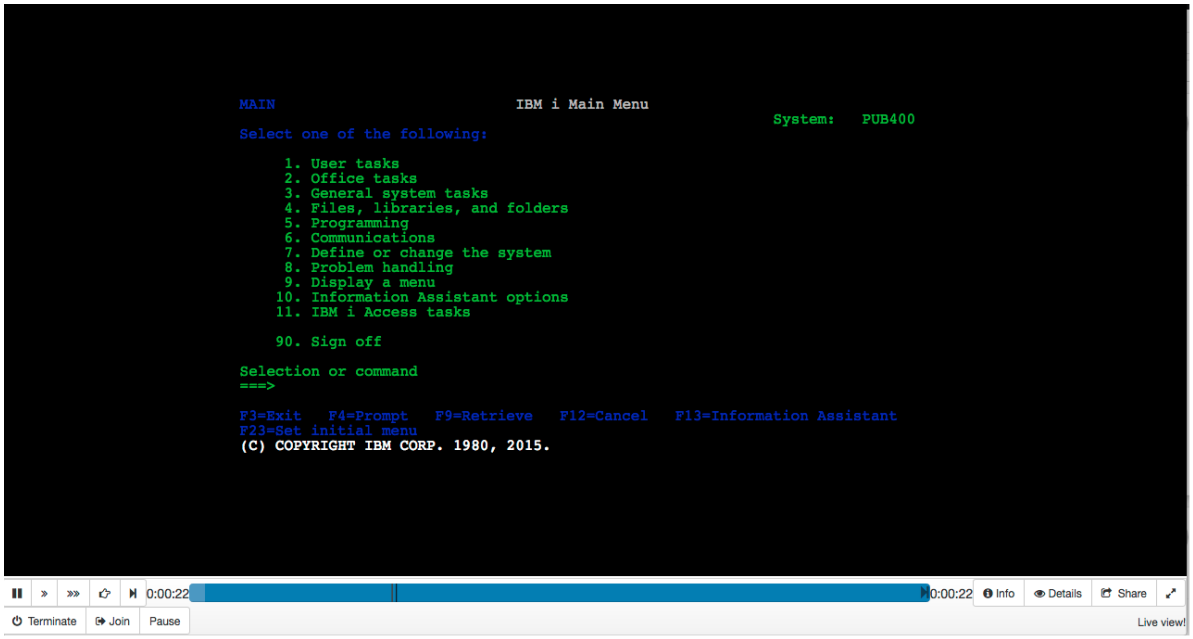


5.7.4 Podgląd sesji połączeniowej

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

> **Uwaga**
>
> 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*

5.8 PostgreSQL

W tym rozdziale przedstawiony jest przykład podstawowej konfiguracji Fudo Enterprise, której celem jest monitorowanie i kontrolowanie dostępu do bazy danych PostgreSQL przez bezpieczne połączenie proxy.

> **Uwaga**
>
> Połączenia PostgreSQL obsługują wyłącznie **klienta natywnego**. Po skonfigurowaniu polecenie połączenia jest dostępne w Portalu Użytkownika.

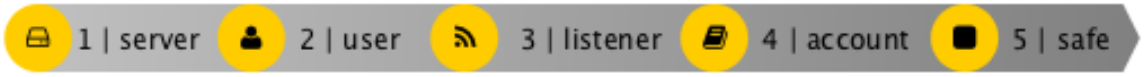
5.8.1 Założenia

Przed rozpoczęciem konfiguracji:

- System musi zostać zainicjowany (zobacz *Inicjowanie systemu*)
- Serwer PostgreSQL musi być dostępny z Fudo Enterprise
- Klient PostgreSQL (`psql`) musi być zainstalowany na Twojej stacji roboczej

5.8.2 Przegląd architektury

Poniższy diagram przedstawia przepływ połączenia PostgreSQL:



Przepływ połączenia:

1. Użytkownik uwierzytelnia się w Portalu Użytkownika (https://10.31.134.220)
2. Użytkownik otrzymuje polecenie połączenia z hasłem jednorazowym (OTP)
3. Natywny klient `psql` łączy się przez proxy Fudo Enterprise
4. Fudo Enterprise uwierzytelnia połączenie i przekazuje je do serwera PostgreSQL

5.8.3 Konfiguracja

Krok 1: Utwórz serwer PostgreSQL

Zdefiniuj docelowy serwer PostgreSQL w Fudo Enterprise.

1. Przejdź do *Zarządzanie sesjami* > *Serwery*
2. Kliknij *+ Dodaj serwer*
3. Skonfiguruj serwer, używając następujących ustawień:

Ogólne

Nazwa: `PostgreSQL_Server`
Opis: `Produkcyjna baza danych PostgreSQL`
Zablokowany: ☐ Niezaznaczone

Karta Ustawienia: Protokół

Protokół: `PostgreSQL`
TLS włączony: ✓ Zaznaczone (zalecane ze względów bezpieczeństwa)
Starsza kryptografia: ☐ Niezaznaczone
Użyj tunelu SSH: ☐ Niezaznaczone

Karta Ustawienia: Adres nasłuchu

Adres nasłuchu: `Dowolny`

Karta Ustawienia: Cel

Typ: `IPv4`
Adres: `10.0.100.7`
Maska: `32`
Port: `5432`

Karta Ustawienia: Weryfikacja serwera

Metoda: `Certyfikat serwera` lub `Brak`

4. Kliknij *Zapisz i zamknij*.

Krok 2: Utwórz użytkownika

Utwórz użytkownika, który będzie uzyskiwać dostęp do serwera PostgreSQL.

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*.

Krok 3: Utwórz gniazdo nasłuchiwania

Skonfiguruj punkt końcowy proxy dla połączeń PostgreSQL.

1. Przejdź do *Zarządzanie sesjami* > *Gniazda nasłuchiwania*
2. Kliknij *+ Dodaj*
3. Skonfiguruj gniazdo nasłuchiwania:

Ustawienia ogólne

Nazwa: `PostgreSQL_Listener`
Protokół: `PostgreSQL`
Zablokowany: ☐ Niezaznaczone

Ustawienia połączenia

Tryb: `proxy`
Adres lokalny: `10.31.134.220`
Port: `5432`
TLS włączony: ✓ Zaznaczone (wymagane dla PostgreSQL)
Starsza kryptografia: ☐ Niezaznaczone

Kontrola dostępu

Uprawnieni użytkownicy: Pozostaw puste (konfigurowane przez Safe)

4. Kliknij *Zapisz i zamknij*.

Krok 4: Utwórz konto

Zdefiniuj poświadczenia bazy danych do uwierzytelniania.

1. Przejdź do *Zarządzanie sesjami* > *Konta*
2. Kliknij *+ Dodaj*
3. Skonfiguruj konto:

Ogólne

Nazwa: `PostgreSQL_Account`
Nagrywanie sesji: `all`
Notatki: `Konto administratora PostgreSQL`

Karta Ustawienia: Typ

Typ konta: `REGULAR`

Karta Ustawienia: Cel

Serwer: `PostgreSQL_Server` (wybierz z listy rozwijanej)

Karta Ustawienia: Poświadczenia

Zastąp sekret wartością: `Hasło`
Sekret: Twoje hasło PostgreSQL
Login: Twój login PostgreSQL

Karta Modyfikatory haseł: Ogólne

Zasada zmiany hasła: `Statyczne, bez ograniczeń`

4. Kliknij *Zapisz i zamknij*.

Krok 5: Utwórz Safe Skonfiguruj kontrolę dostępu i powiąż wszystkie komponenty.

1. Przejdź do *Zarządzanie sesjami* > *Safes*
2. Kliknij *+ Dodaj Safe*
3. Skonfiguruj Safe:

Ogólne

Nazwa: `PostgreSQL_Safe`
Zablokowany: ☐ Niezaznaczone

Karta Ogólne: Połączenie

Powód logowania: ✓ Zaznaczone (opcjonalne, dla ścieżki audytu)

Karta Ogólne: Dostęp

OTP w Portalu Użytkownika: ✓ Zaznaczone
Klient webowy: ☐ Niezaznaczone

4. Kliknij *Zapisz i zamknij*.
5. **Dodaj użytkowników do Safe:**
   a. Wybierz kartę Użytkownicy
   b. Kliknij Zarządzaj użytkownikami
   c. Wyszukaj i dodaj swojego użytkownika (np. `John`)

d. Kliknij Zapisz

6. **Dodaj konto do Safe:**
   a. Wybierz kartę Konta
   b. Kliknij Zarządzaj kontami
   c. Wyszukaj i dodaj `PostgreSQL_Account`
   d. Kliknij Zapisz
7. **Przypisz gniazdo nasłuchiwania do konta:**
   a. Kliknij ikonę edycji w kolumnie **Gniazda nasłuchiwania** dla `PostgreSQL_Account`
   b. Wyszukaj i dodaj `PostgreSQL_Listener`
   c. Kliknij Zapisz
8. Kliknij Zapisz i zamknij

5.8.4 Nawiązywanie połączenia PostgreSQL

Krok 1: Uzyskaj dostęp do Portalu Użytkownika

Otwórz przeglądarkę i przejdź do adresu Portalu Użytkownika. Przykład:

```
https://10.31.134.220
```

Zaloguj się przy użyciu poświadczeń użytych podczas tworzenia użytkownika:

Login: `john_smith`
Hasło: `john`

Krok 2: Pobierz polecenie połączenia

1. Odszukaj `PostgreSQL_Account` na liście zasobów
2. Kliknij strzałkę listy rozwijanej **Klient natywny**
3. Zobaczysz:
   - **Odcisk:** skrót identyfikujący serwer
   - **Hasło jednorazowe:** ważne przez 5 minut
   - **Polecenie połączenia:** gotowe do użycia polecenie psql

Krok 3: Połącz się przy użyciu psql

Skopiuj polecenie połączenia i zastąp `<database_name>` nazwą docelowej bazy danych:

```
# Format szablonu
psql postgres://[OTP]:empty@10.31.134.220:5432/<database_name>

# Przykład: połączenie z niestandardową bazą danych
psql postgres://85156504qLOOtF4bWesSntHHvQoTIjED:empty@10.31.134.220:5432/myapp_
↪db
```

Uwaga

Ważne informacje o połączeniu:

- OTP (hasło jednorazowe) wygasa po **5 minutach**
- Pole hasła zawsze ma wartość `empty` — uwierzytelnianie odbywa się przy użyciu tokenu OTP
- Musisz podać nazwę bazy danych na końcu ciągu połączenia

Powiązane tematy:

- *Tworzenie serwera PostgreSQL*
- *Szybki start — połączenie SSH*
- *Szybki start — połączenie RDP*
- *Szybki start — połączenie MySQL*
- *Konfiguracja Password Vault*
- *Model danych*

5.9 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*).



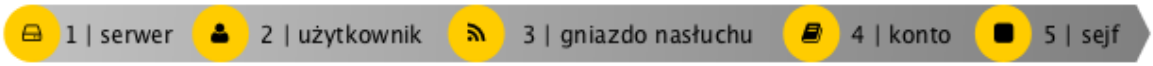
Ostrzeżenie

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`.

5.9.1 Założenia

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

5.9.2 Konfiguracja



Dodanie serwera

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

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

Parametr	Wartość
Nazwa	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.

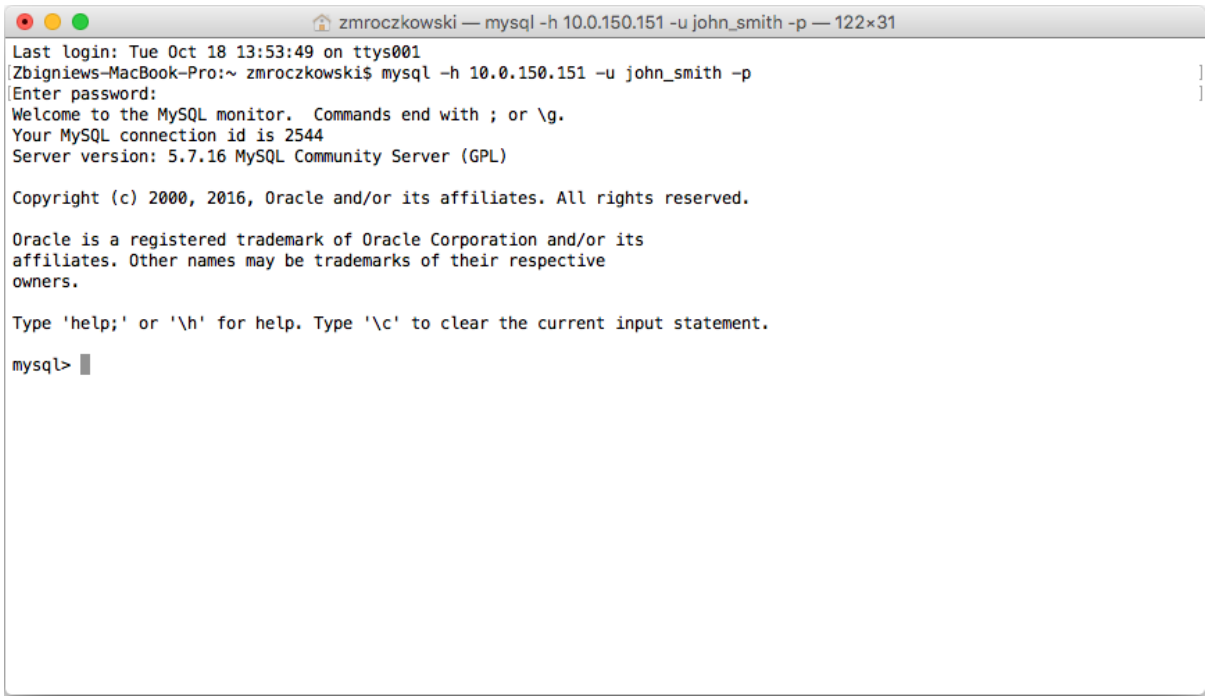
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

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*.

5.9.3 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.



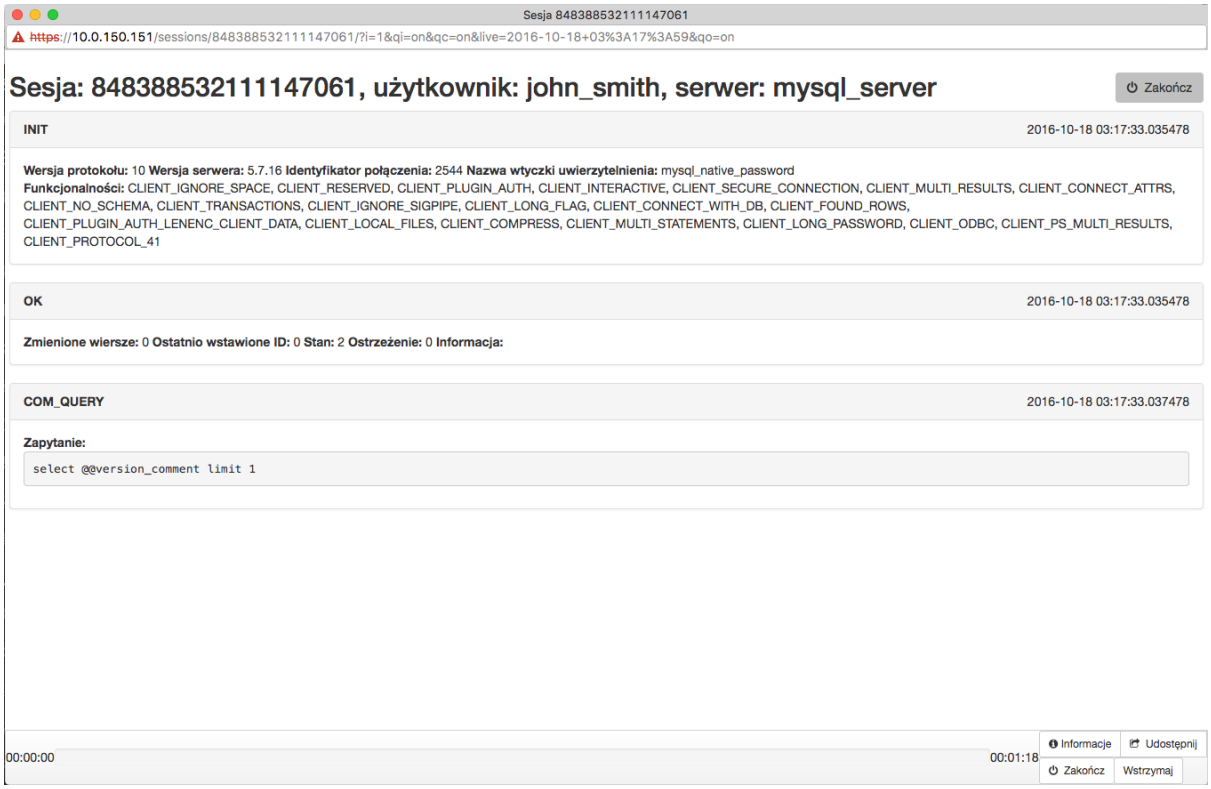
4. Kontynuuj przeglądanie zawartości serwera poprzez zapytania sql.

5.9.4 Podgląd sesji połączeniowej

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

> **Uwaga**
>
> 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*

5.10 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*).

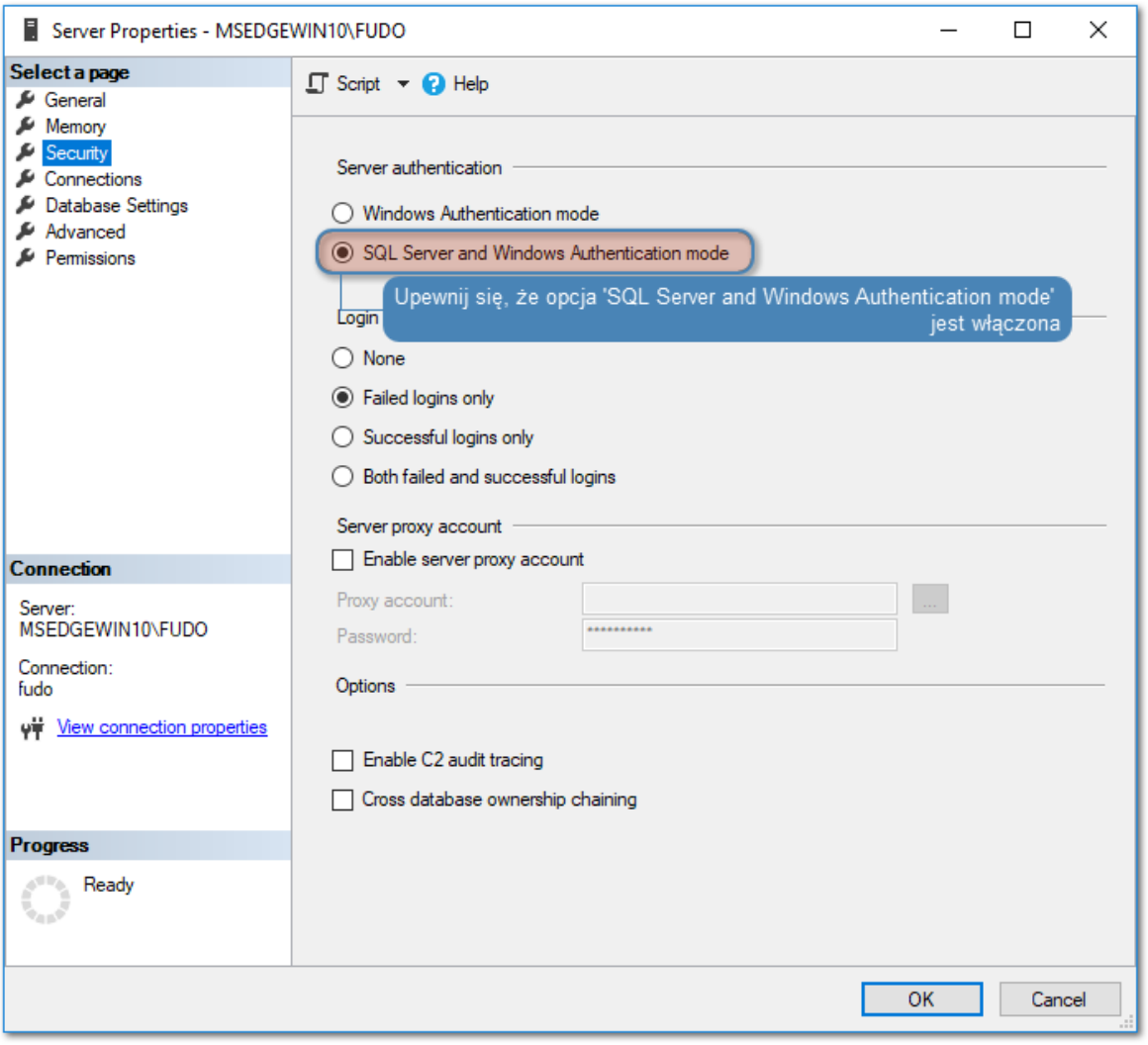


5.10.1 Założenia

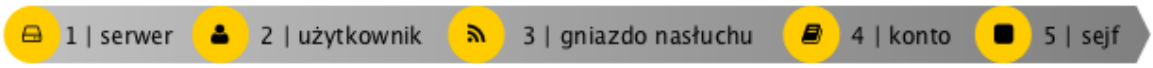
Poniższy opis zakłada, że pierwsze uruchomienie urządzenia zostało prawidłowo przeprowadzone. Procedura pierwszego uruchomienia jest opisana w rozdziale *Pierwsze uruchomienie*.

Uwaga

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



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	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.

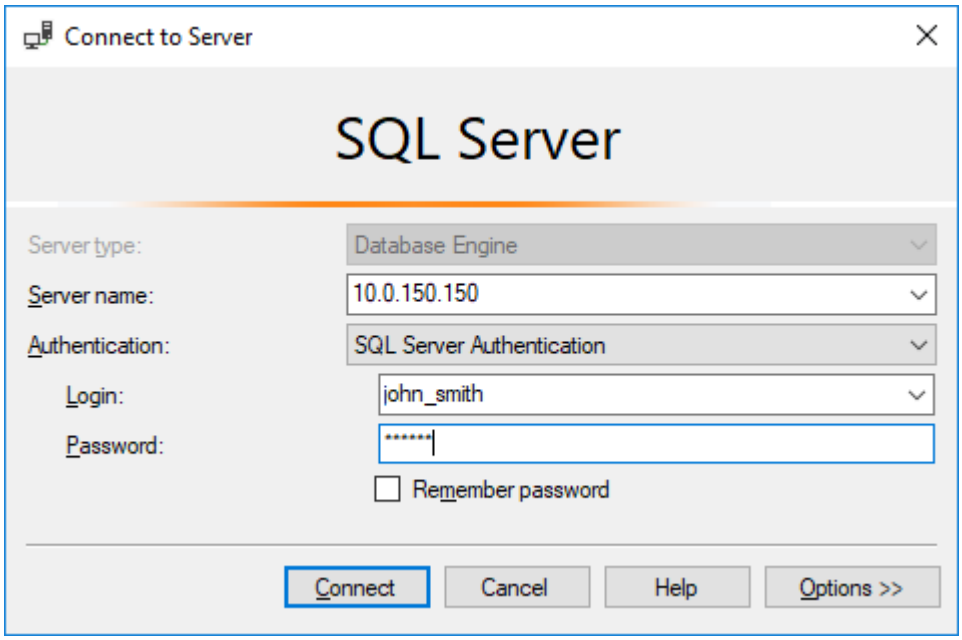
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij + *Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

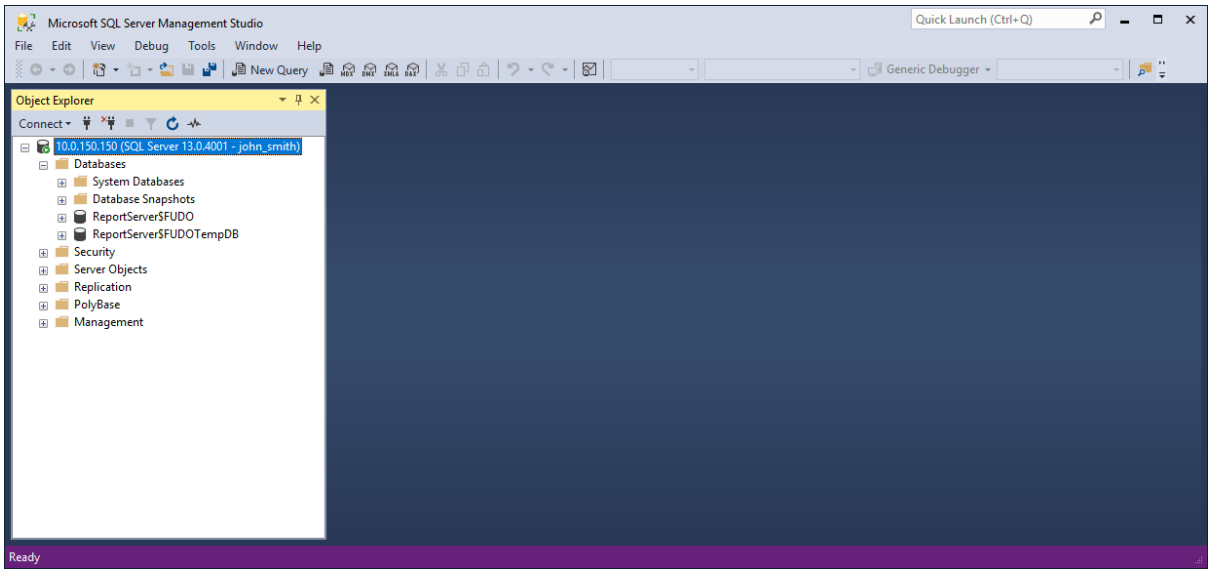
Parametr	Wartość
Ogólne	
Nazwa	`mssql_safe`
Zablokowane	✗
Powiadomienia	✗
Powód logowania	✗
Wymagaj potwierdzenia	✗
Polityki	✗
Note access	`No access`
Funkcjonalność protokołów	
RDP	✗
SSH	✗
VNC	✗

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*.

5.10.3 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*.





5.10.4 Podgląd sesji połączeniowej

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

Uwaga

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 ▶.

Uwaga

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*

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

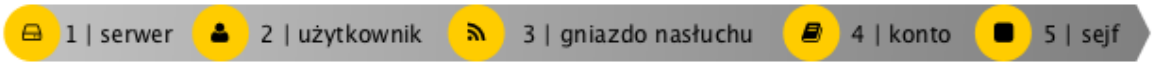
Model	Maksymalna zalecana liczba jednoczesnych połączeń HTTP*
F100x	2
F300x	5
F500x	10

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

5.11.1 Założenia

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

5.11.2 Konfiguracja



Dodanie serwera

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

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

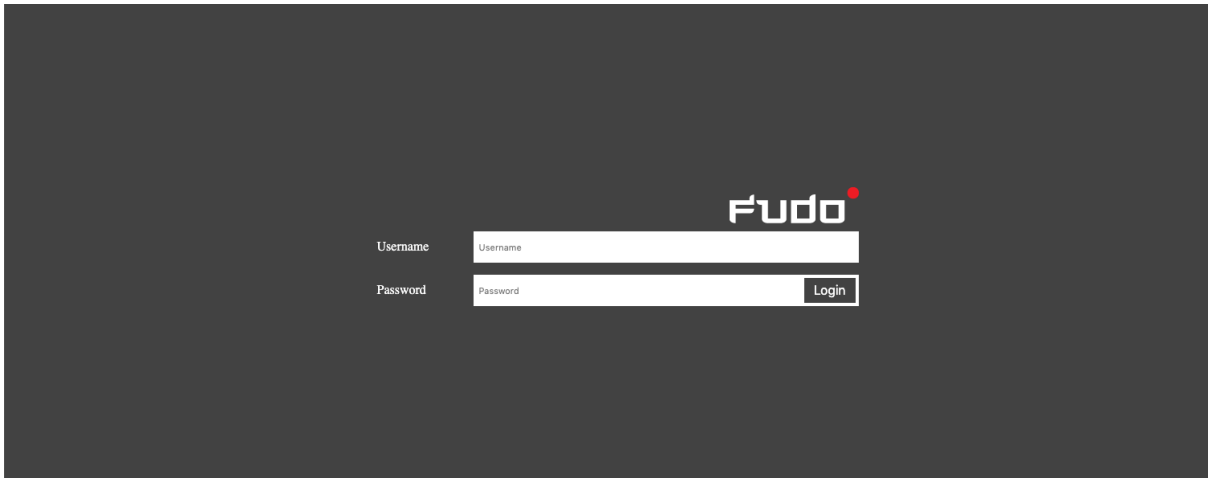
4. Przejdź na zakładkę *Użytkownicy*.
5. Kliknij *+ Dodaj użytkownika*.
6. Znajdź użytkownika *john_smith* i kliknij +.
7. Kliknij *OK*.
8. Przejdź na zakładkę *Konta*.
9. Kliknij *+ Dodaj konto*.
10. Znajdź konto `twitter_admin` i kliknij +.
11. Kliknij *OK*.
12. Kliknij ✎ w kolumnie *Gniazda nasłuchiwania*.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

5.11.3 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*.

Uwaga

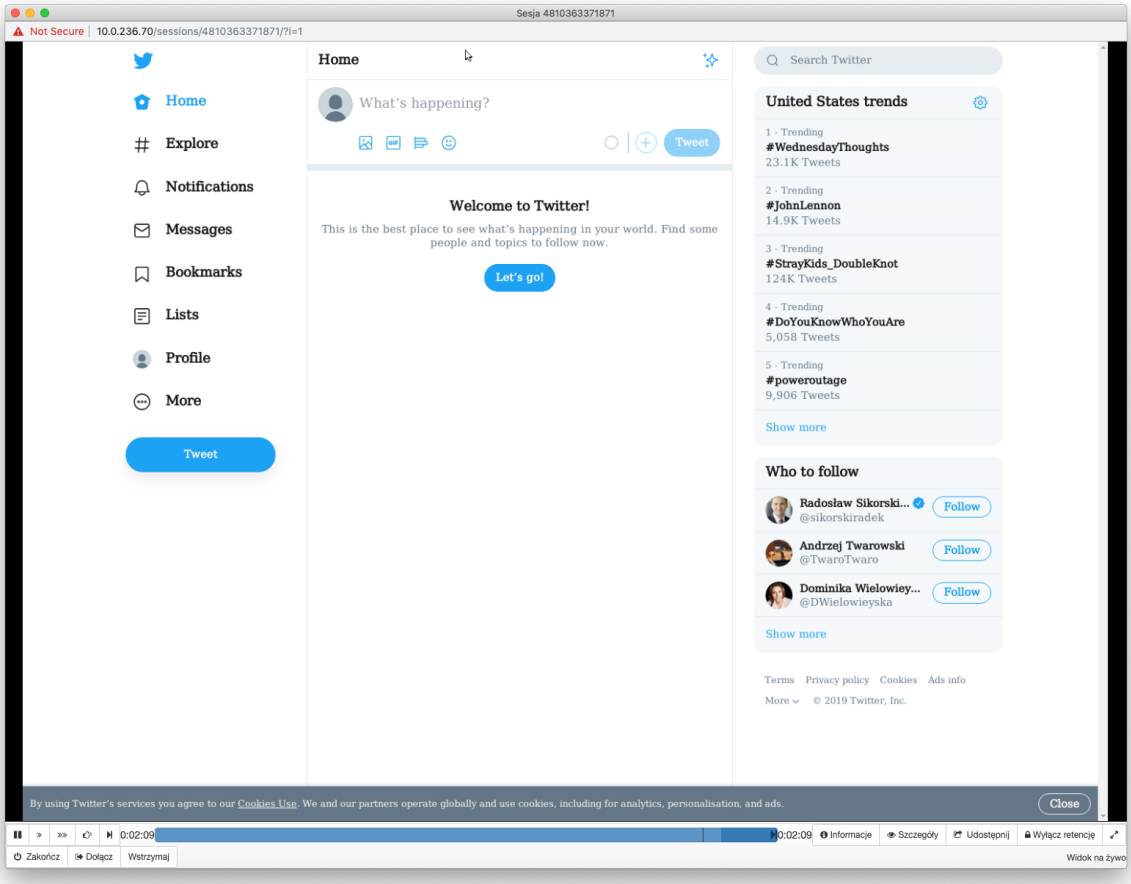
W przypadku uwierzytelniania dwuskładnikowego, wprowadź hasło statyczne wraz ze składnikiem dynamicznym (wskazanie tokena) jako jeden ciąg znaków.



4. Kontynuuj przeglądanie serwisu.

5.11.4 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*

5.12 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.

Uwaga

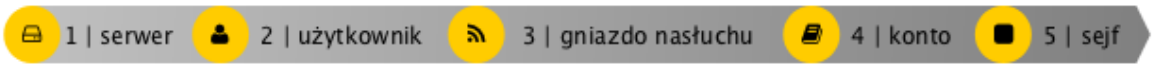
Ze względu na specyfikę protokołu VNC, który do uwierzytelnienia wymaga jedynie hasła, login zdefiniowany w koncie typu *regular* jest ignorowany przy zestawianiu połączenia.



5.12.1 Założenia

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

5.12.2 Konfiguracja



Dodanie serwera

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

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

Parametr	Wartość
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.

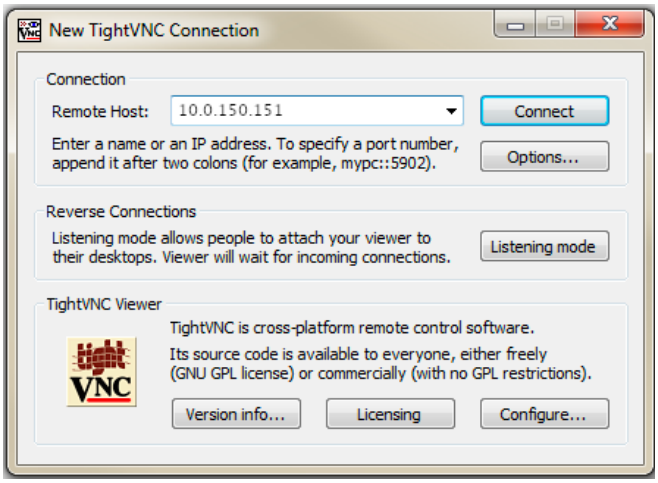
1. Wybierz z lewego menu *Zarządzanie* > *Sejfy*.
2. Kliknij *+ Dodaj*.
3. Uzupełnij parametry konfiguracyjne:

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*.

5.12.3 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.

5.12.4 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*

ROZDZIAŁ 6

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.

Uwaga

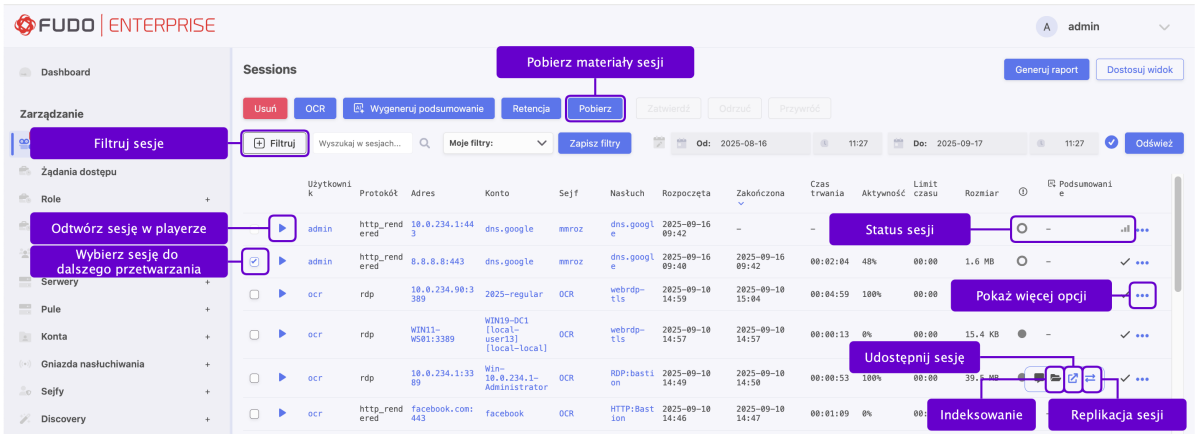
Zawartość listy sesji uzależniona jest od uprawnień zalogowanego użytkownika. Aby użytkownik miał dostęp do określonej sesji, musi mieć stosowne uprawnienia do obiektów: serwera, konta, użytkownika i sejfu, wykorzystywanych w danym połączeniu.

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*).
	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*.

Uwaga

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



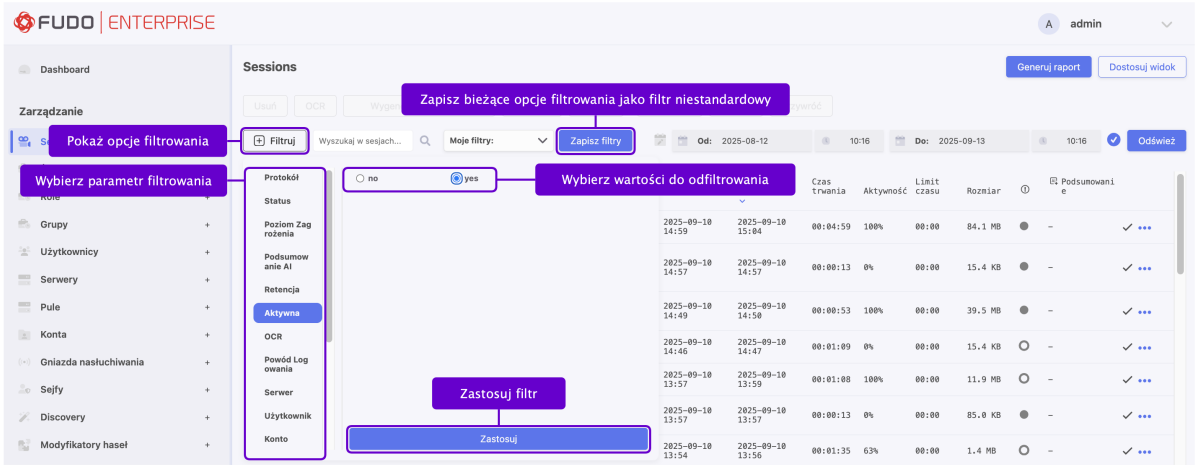
6.1 Filtrowanie sesji

Filtrowanie sesji pozwala łatwo znaleźć interesujące sesje poprzez ograniczenie liczby wyświetlanych sesji na stronie zarządzania sesjami.

Opcje filtrowania, takie jak wybór zakresu czasu rozpoczęcia sesji czy wybór filtrów niestandardowych, są domyślnie dostępne w górnym pasku widoku sesji.

6.1.1 Definiowanie filtrów

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij + *Filtr*.
3. Z listy dostępnych opcji filtrowania wybierz żądany parametr filtra.
4. Wybierz wartości dla wcześniej dodanego parametru filtra.
5. Kliknij **Zastosuj**, aby potwierdzić filtr.



Uwaga

Wpisz ciąg znaków, aby ograniczyć liczbę elementów na liście. W przypadku użytkowników, elementy na liście mogą zostać ograniczone do tych, którym przypisano określoną rolę lub którzy należą do danej jednostki organizacyjnej.

6. Powtórz kroki 1–4, aby zdefiniować dodatkowe filtry.

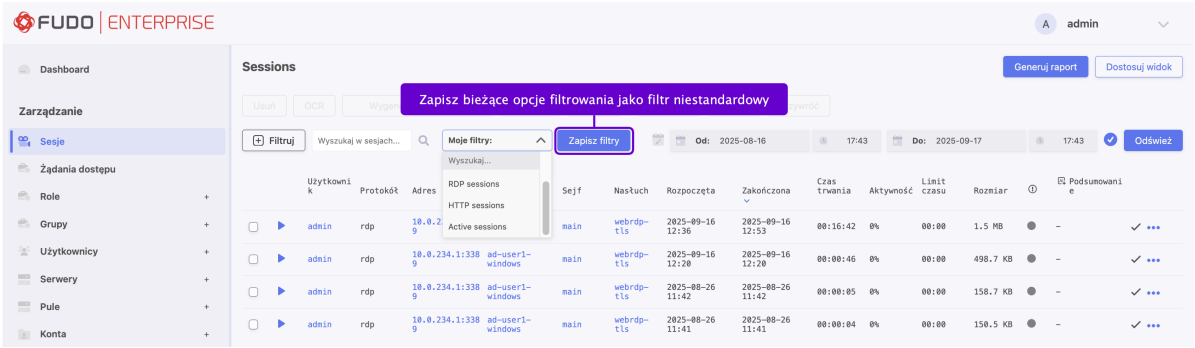
Uwaga

Na liście wyświetlone zostaną tylko sesje spełniające wszystkie zdefiniowane parametry filtrowania.

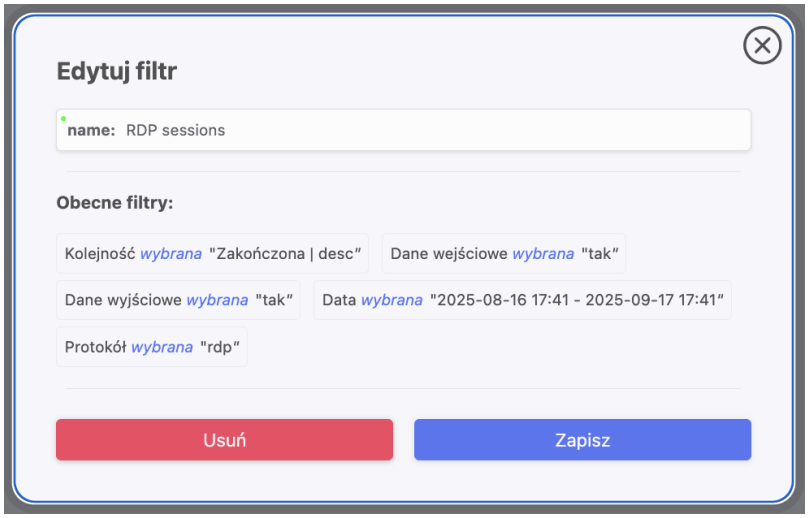
6.1.2 Zapisywanie filtrów niestandardowych

Bieżące ustawienia filtrowania można zapisać jako własny zestaw filtrów dla wygody administratora.

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij + **Filtr** i zdefiniuj opcje filtrowania zgodnie z opisem w sekcji *Filtrowanie sesji*.
3. Kliknij przycisk **Zapisz filtry**, aby zapisać definicję filtra.

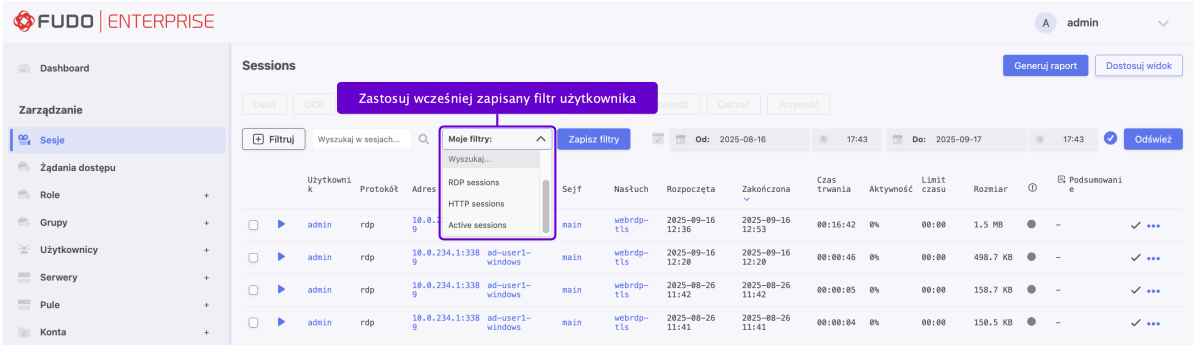


4. W oknie modalnym wprowadź nazwę nowego filtra.
5. Kliknij **Zapisz**, aby potwierdzić i zapisać filtr niestandardowy.



6.1.3 Stosowanie filtrów niestandardowych

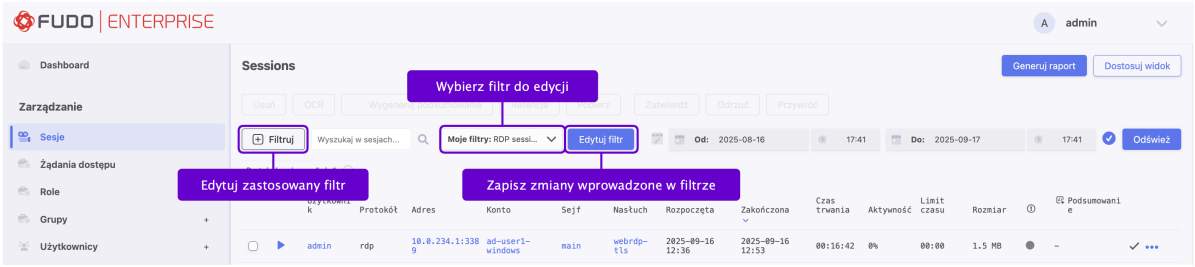
Aby zastosować wcześniej zapisany filtr niestandardowy, wybierz go z listy **Filtry niestandardowe**. Wybrany filtr zostanie natychmiast zastosowany do listy sesji, a na liście pojawią się tylko sesje spełniające określone kryteria.



6.1.4 Edycja filtrów niestandardowych

Aby edytować wcześniej zapisany filtr niestandardowy:

1. Wybierz żądany filtr z listy **Filtry niestandardowe**. Przycisk **Edytuj filtr** stanie się dostępny.
2. Dostosuj opcje filtrowania według potrzeb.
3. Kliknij **Edytuj filtr**. Otworzy się okno modalne z bieżącą konfiguracją filtra.
4. Kliknij Zapisz, aby nadpisać istniejący filtr zaktualizowaną konfiguracją.

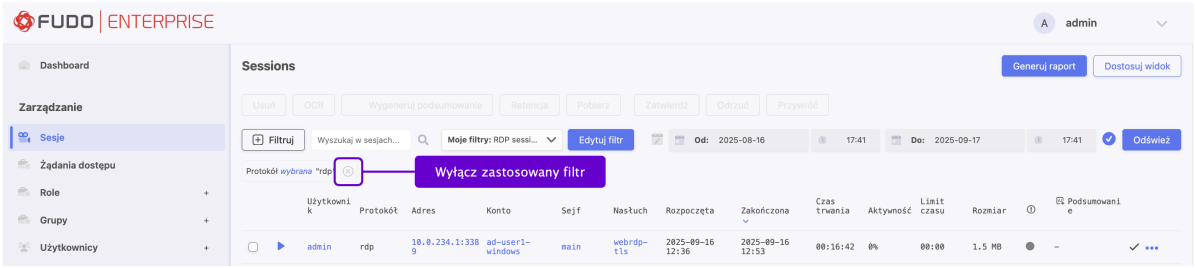


6.1.5 Wyłączanie filtrów

> **Uwaga**
>
> Aktywne filtry są wyświetlane na pasku poniżej ustawień filtrowania.

Aby wyłączyć aktywny filtr, kliknij ikonę X obok nazwy filtra.

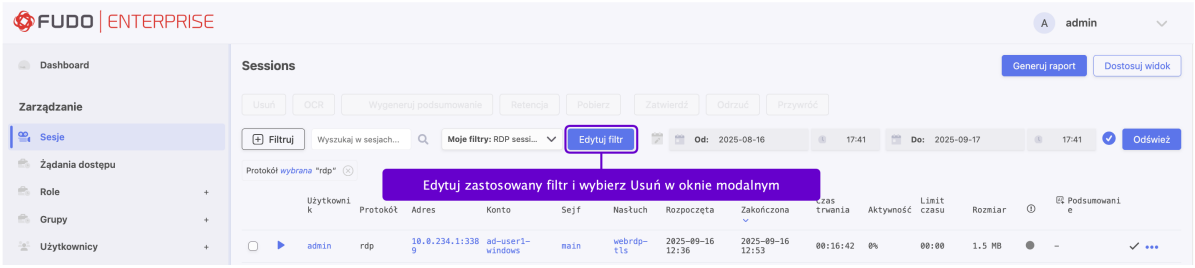
Filtr zostaje natychmiast wyłączony i nie wpływa już na wyświetlaną listę sesji.



6.1.6 Usuwanie filtrów niestandardowych

Aby usunąć wcześniej zapisany filtr niestandardowy:

1. Wybierz filtr z listy **Filtry niestandardowe**.
2. Kliknij **Edytuj filtr**, aby otworzyć okno modalne ze szczegółami filtra.
3. Kliknij Usuń, aby trwale usunąć wybrany filtr.



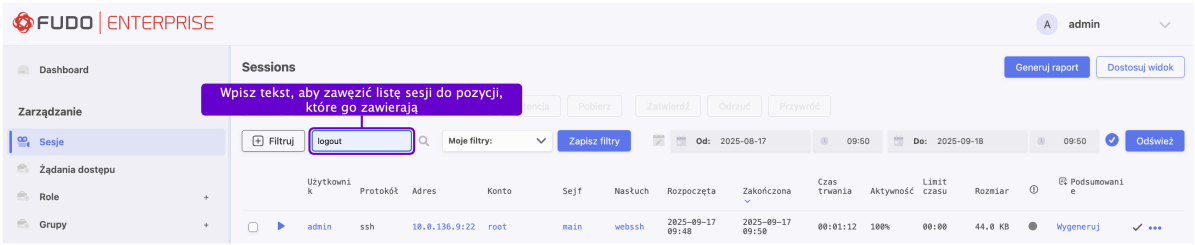
6.1.7 Wyszukiwanie pełnotekstowe

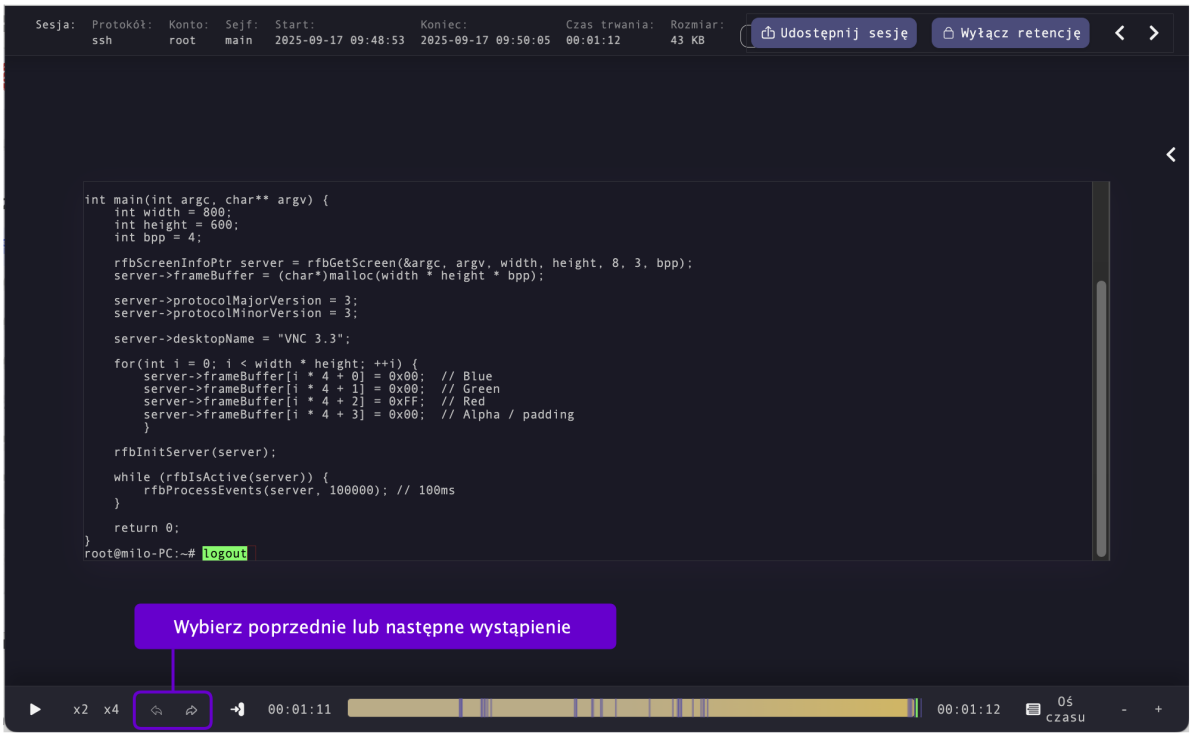
Fudo Enterprise umożliwia wyszukiwanie zapisanych danych w celu ograniczenia liczby elementów na liście sesji tylko do tych, które zawierają określoną frazę.

Uwaga

- Użyj paska wyszukiwania sesji, aby wyszukać sesje zawierające określone frazy, np. „logout”.
- Odtwarzanie sesji zawierającej określoną frazę rozpoczyna się od momentu jej pierwszego wystąpienia.

Odtwarzacz umożliwia przechodzenie między kolejnymi wystąpieniami wyszukiwanej frazy.





Powiązane tematy:

- *Przegląd systemu*
- *Raporty*

6.2 Odtwarzanie sesji

Fudo Enterprise umożliwia podgląd nagranych sesji, a także bieżących połączeń użytkowników.

Aby wyświetlić sesję, wykonaj następujące kroki:

1. Wybierz *Zarządzanie* > *Sesje*.
2. Znajdź interesującą sesję i kliknij ikonę odtwarzania obok niej.

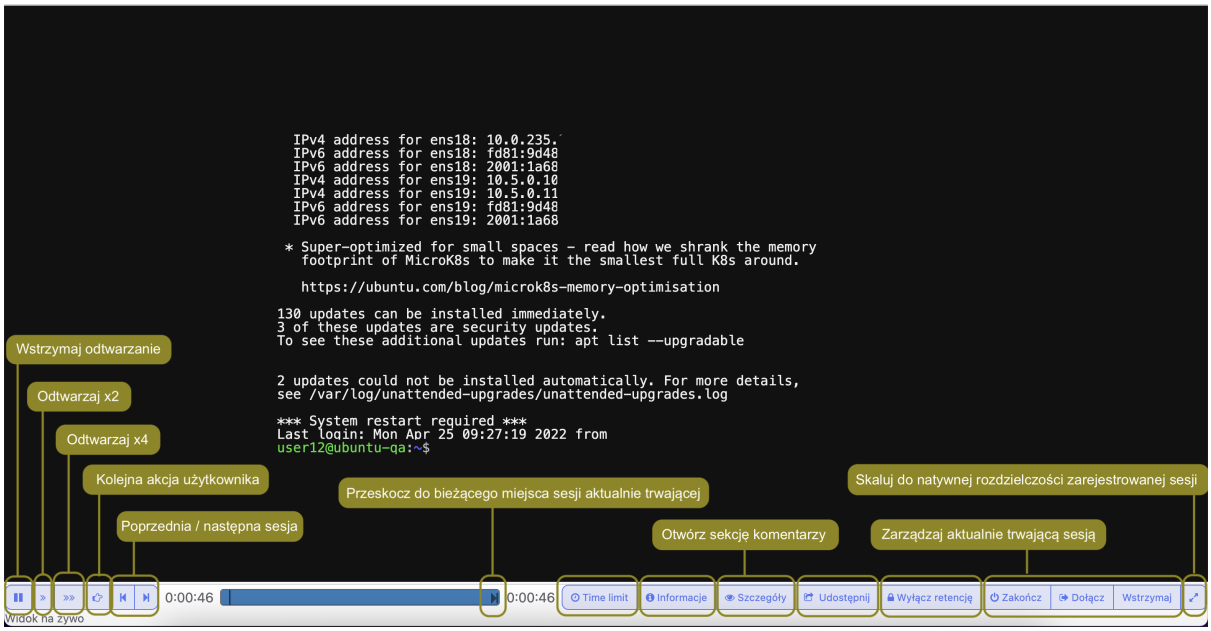
Uwaga

Aby wyświetlić tylko aktywne połączenia:

- Kliknij + *Filtr* i wybierz parametr *Aktywne*.
- Z opcji parametru wybierz *tak*.

Opcje odtwarzacza

SSH, RDP, Telnet, X11



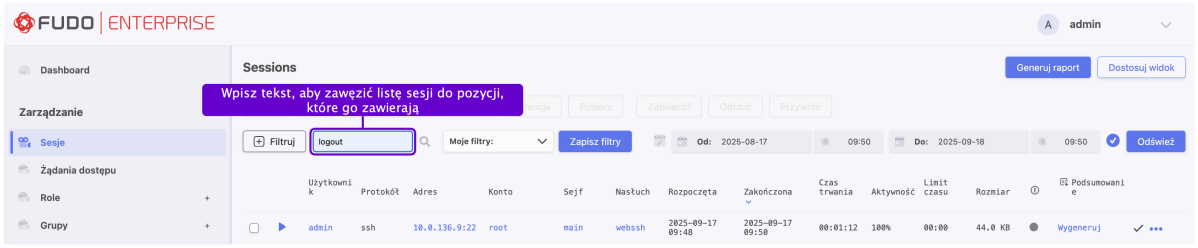
Uwaga

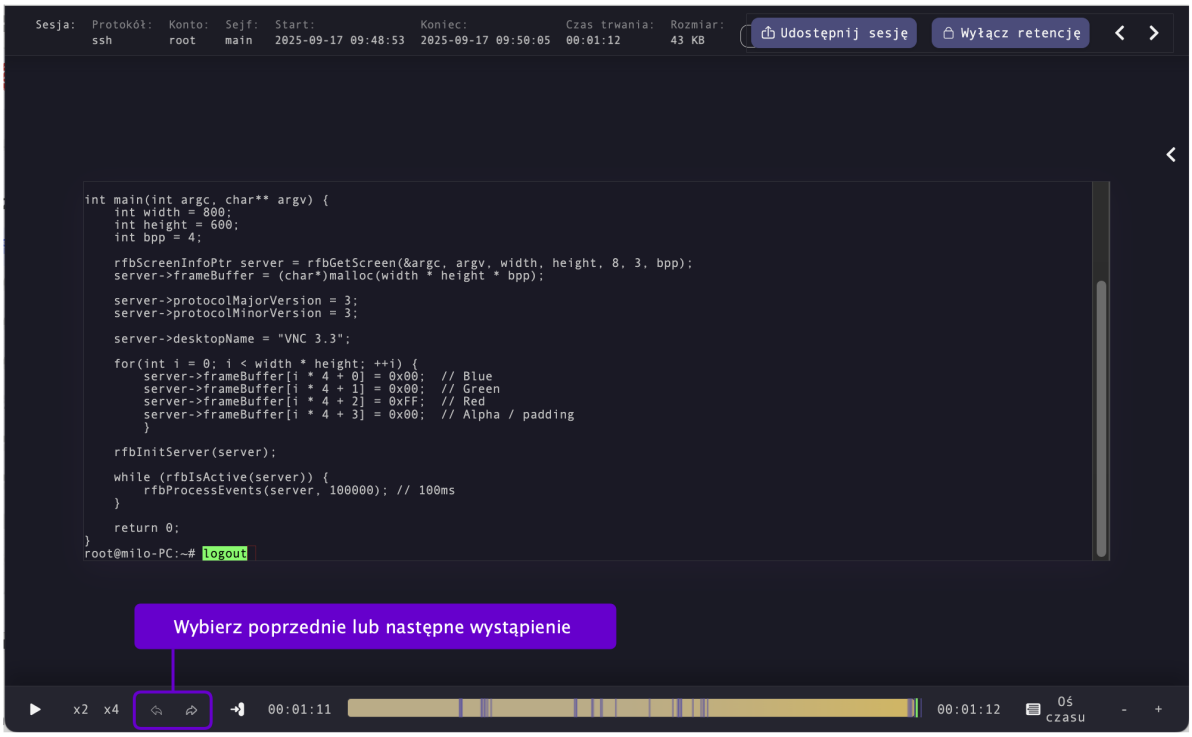
Niektóre funkcje dostępne są tylko dla podglądu sesji aktualnie trwających.

Uwaga

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

Odtwarzacz pozwala na przeskakiwanie pomiędzy wystąpieniami wprowadzonego ciągu znaków.



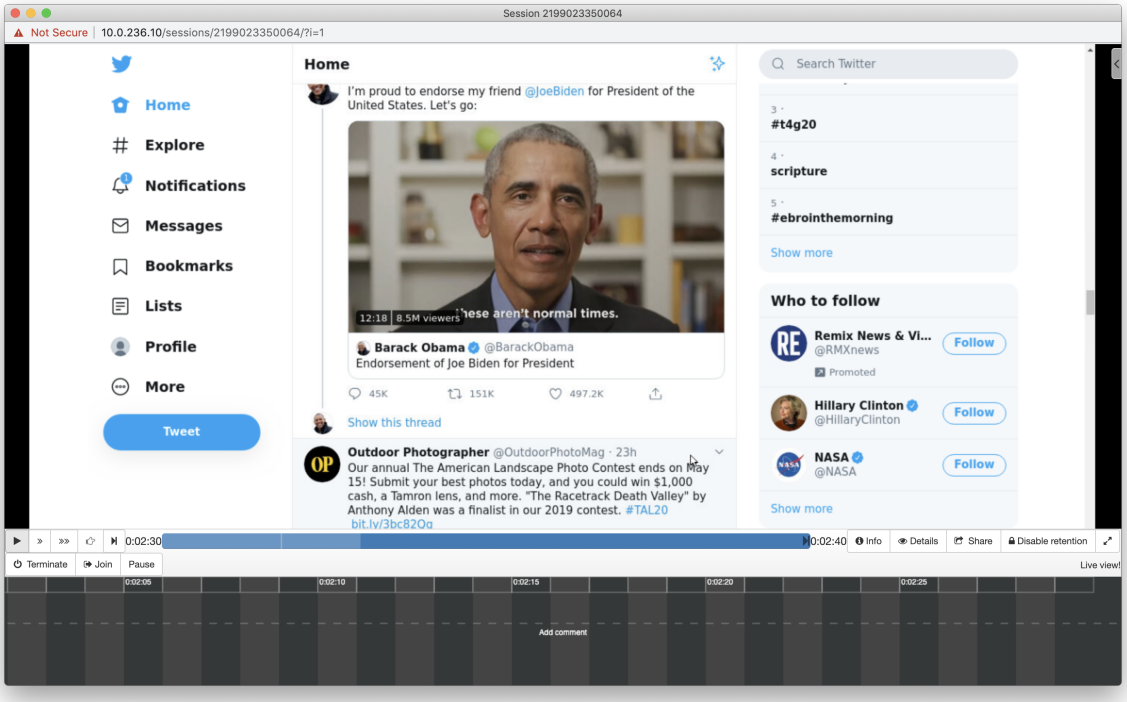


Uwaga

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.

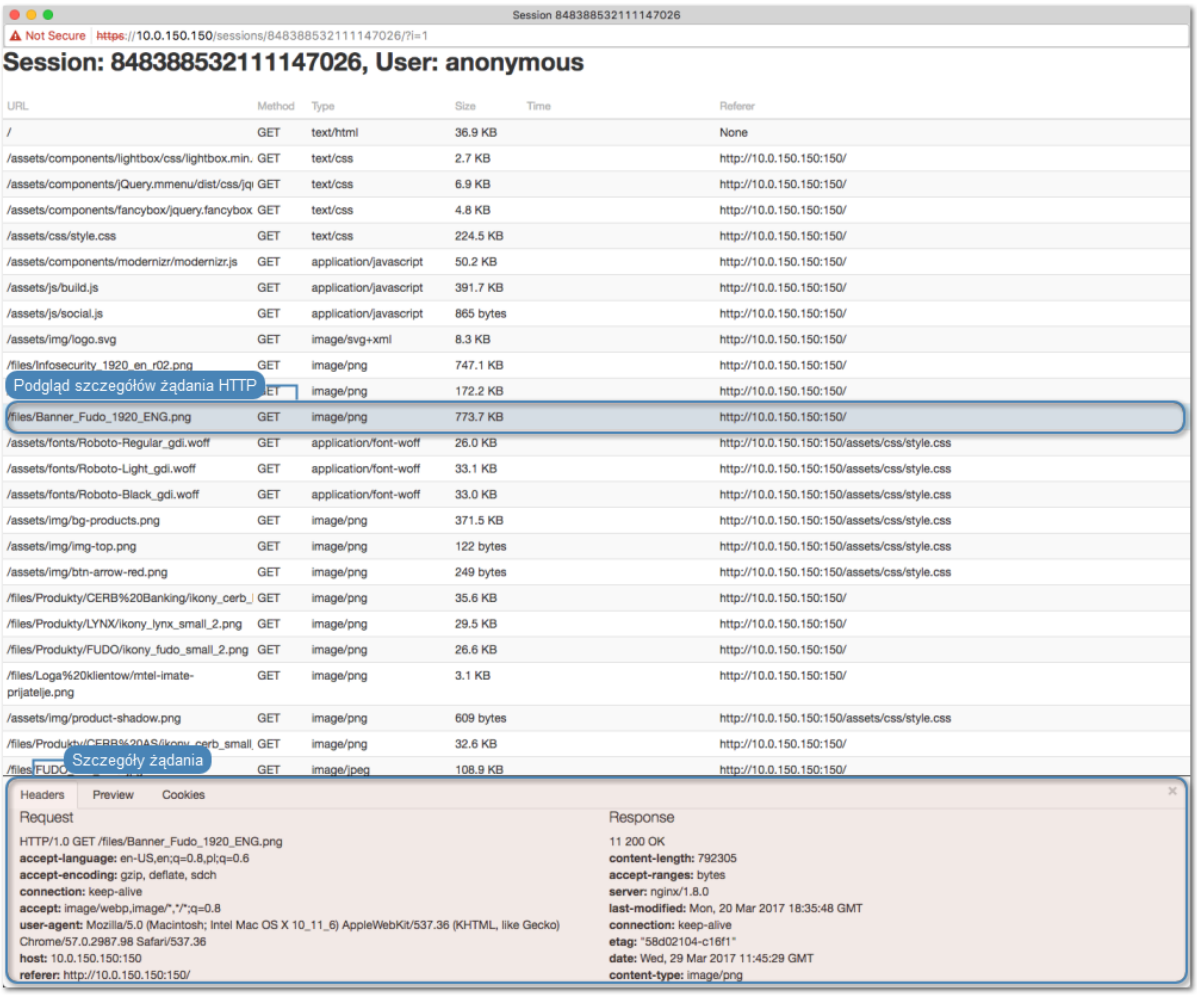
HTTP - renderowane



Uwaga

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

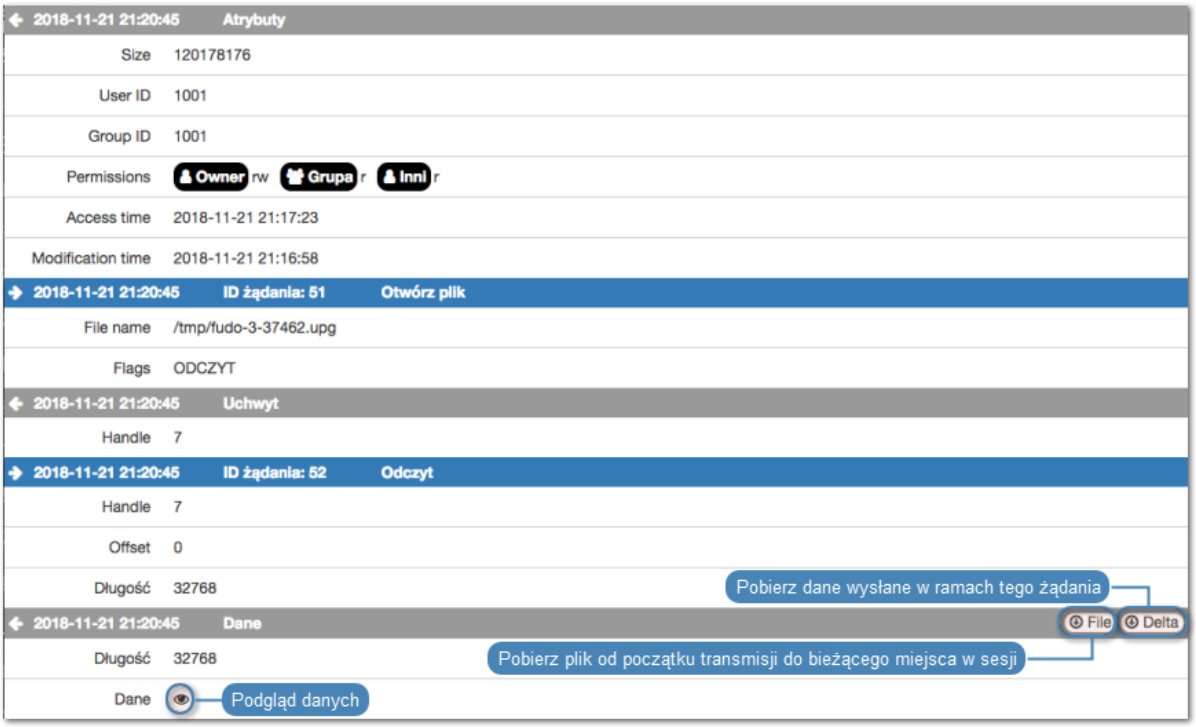
HTTP


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

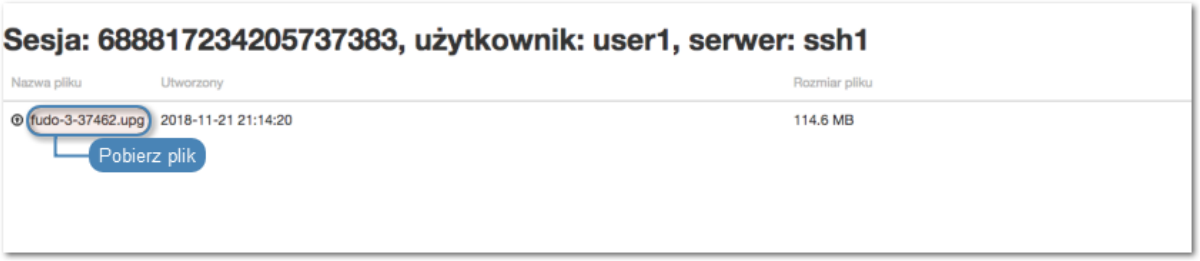
SSH


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

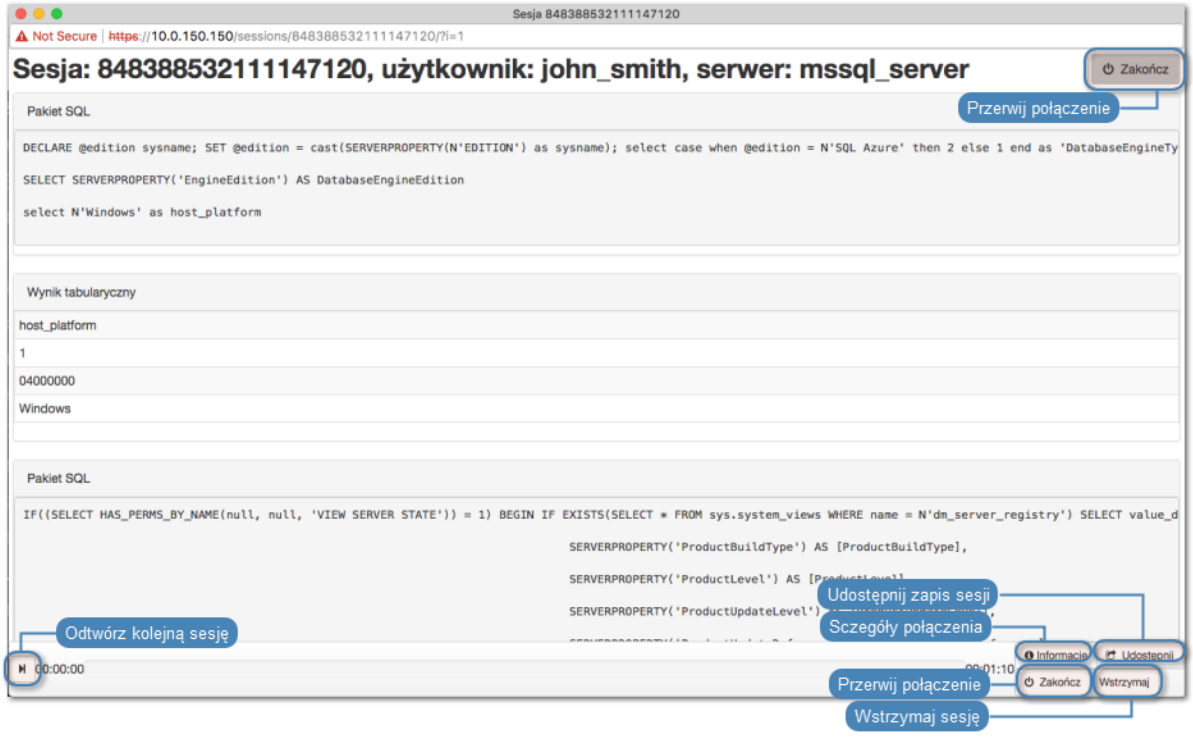
SFTP


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*

6.3 Wstrzymywanie sesji

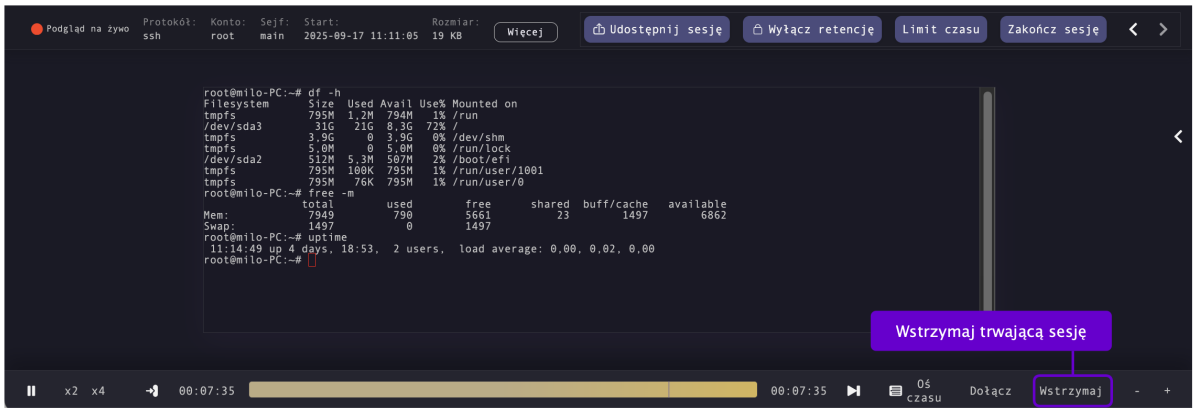
W przypadku gdy aktualne akcje użytkownika wymagają analizy, połączenie może zostać wstrzymane.

Uwaga

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 *Zarządzanie* > *Sesje*.

2. Kliknij *+ Filtr* i wybierz parametr *Aktywne*.
3. Z opcji parametru wybierz *tak*.
4. Znajdź interesującą sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
5. Kliknij *Wstrzymaj* w prawym dolnym rogu odtwarzacza sesji.



Tematy pokrewne:

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

6.4 Przerywanie połączenia

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

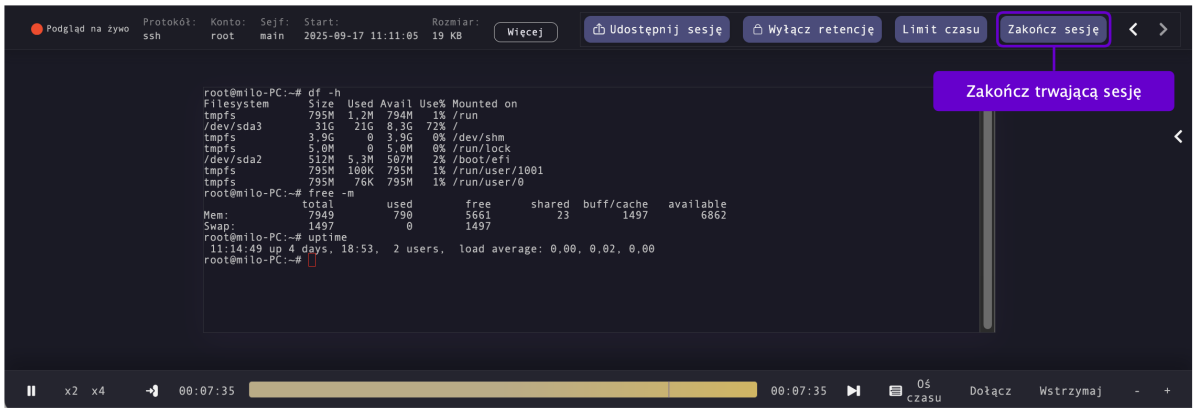
Uwaga

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

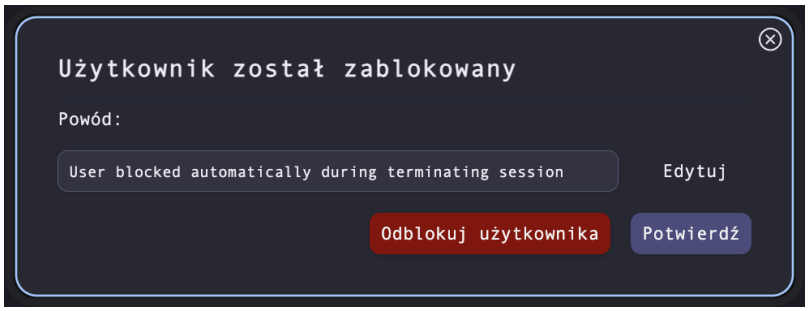
1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij *+ Filtr* i wybierz parametr *Aktywne*.
3. Z opcji parametru wybierz *Tak*.
4. Znajdź interesującą sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
5. Kliknij *Zakończ sesję*.

Uwaga

Zerwanie połączenia automatycznie blokuje danego użytkownika.



6. Zdecyduj, czy użytkownik ma pozostać zablokowany, czy nie.



Tematy pokrewne:

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

6.5 Dołączanie do sesji

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

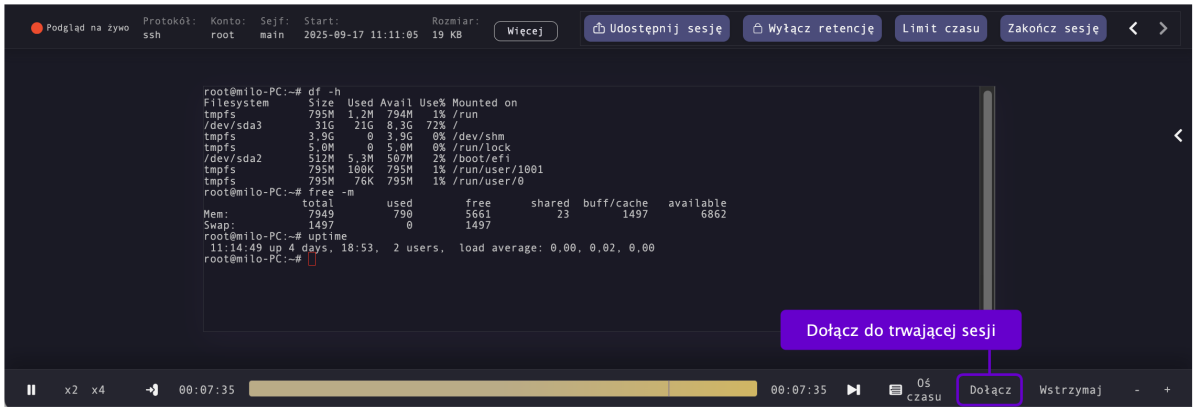
Uwaga

- 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 + *Filtr* i wybierz parametr *Aktywne*.
3. Z opcji parametru wybierz *Tak*.

4. Znajdź interesującą sesję i kliknij ikonę odtwarzania, aby rozpocząć odtwarzanie.
5. Kliknij przycisk *Dołącz*.



Tematy pokrewne:

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

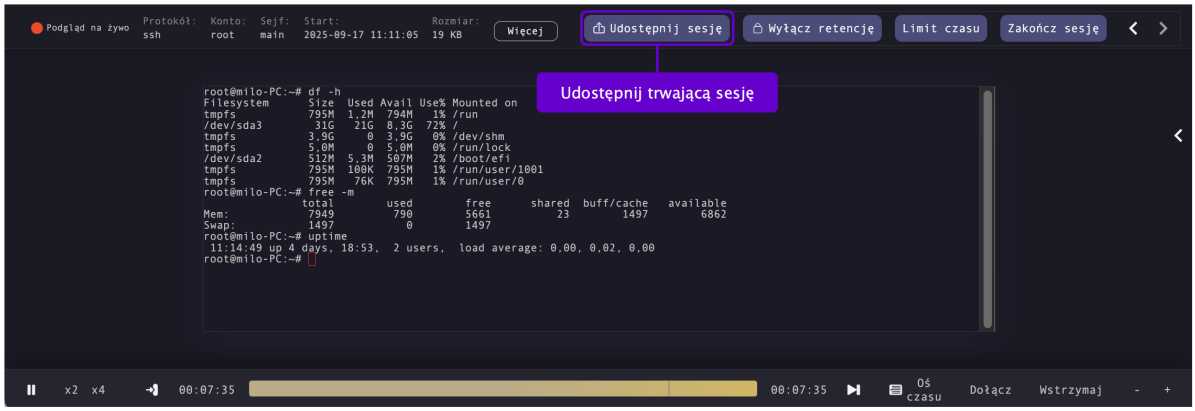
6.6 Udostępnianie sesji

Fudo Enterprise umożliwia udostępnienie wybranej sesji innemu użytkownikowi.

Udostępnianie sesji

Aby udostępnić sesję, wykonaj następujące kroki:

1. Wybierz *Zarządzanie* > *Sesje*.
2. Kliknij + *Filtr* i wybierz parametr *Aktywne*.
3. Z opcji parametru wybierz *Tak*.
4. Znajdź interesującą sesję i kliknij ikonę odtwarzania, aby rozpocząć podgląd.
5. Kliknij *Udostępnij sesję*.



4. Określ czas dostępności sesji i kliknij *Potwierdź*, aby wygenerować adres URL.



Uwaga

Podczas określania ram czasowych dostępności sesji możesz także zdecydować, czy udostępniana sesja ma być w trybie **tylko do odczytu**. Opcja ta dotyczy sesji na żywo i pozwala uniemożliwić innym użytkownikom ingerencję w sesję, przy jednoczesnym zachowaniu możliwości jej podglądu.

5. Skopiuj wygenerowany adres URL i zamknij okno modalne.

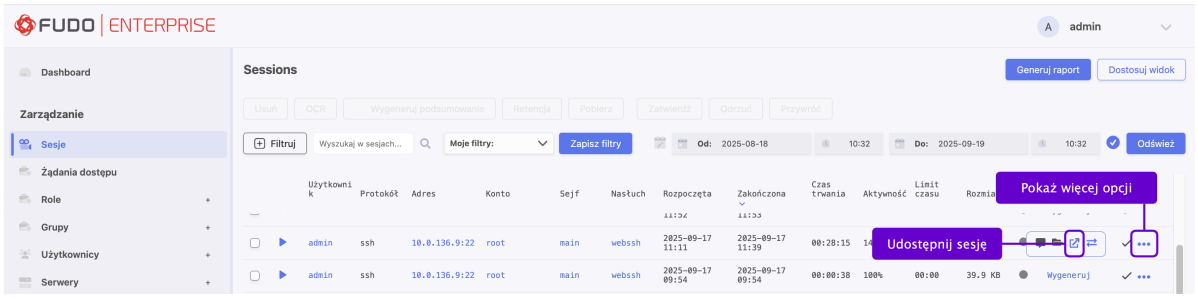
Uwaga

Oprócz udostępniania sesji z widoku podglądu, można również wygenerować link do współdzielenia bezpośrednio z listy sesji, klikając i, a następnie wybierając **Udostępnij sesję** w oknie modalnym.

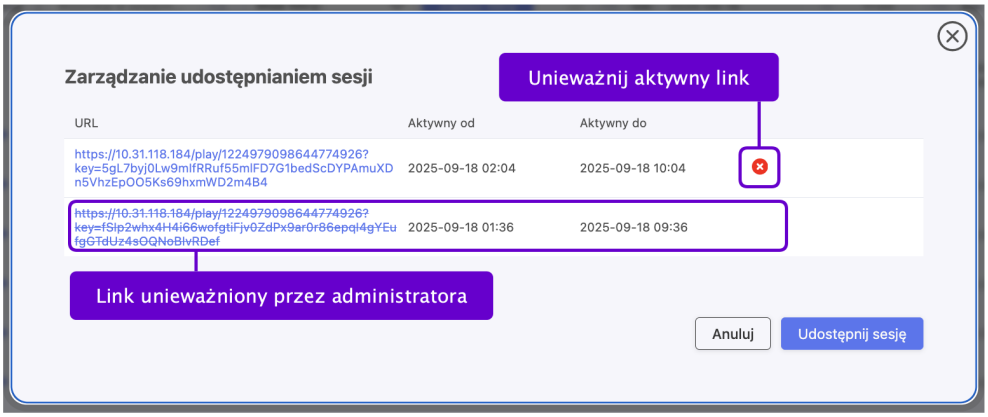
Unieważnianie adresu URL sesji

Aby unieważnić adres URL sesji, wykonaj następujące kroki:

1. Wybierz *Zarządzanie* > *Sesje*.
2. Znajdź interesującą sesję, rozwiń menu dodatkowych opcji i kliknij ikonę *Udostępnij*, aby wyświetlić opcje zarządzania współdzieleniem sesji.



3. Kliknij ikonę *czerwonego krzyżyka*, aby dezaktywować dany adres URL.



Tematy pokrewne:

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

6.7 Komentowanie sesji

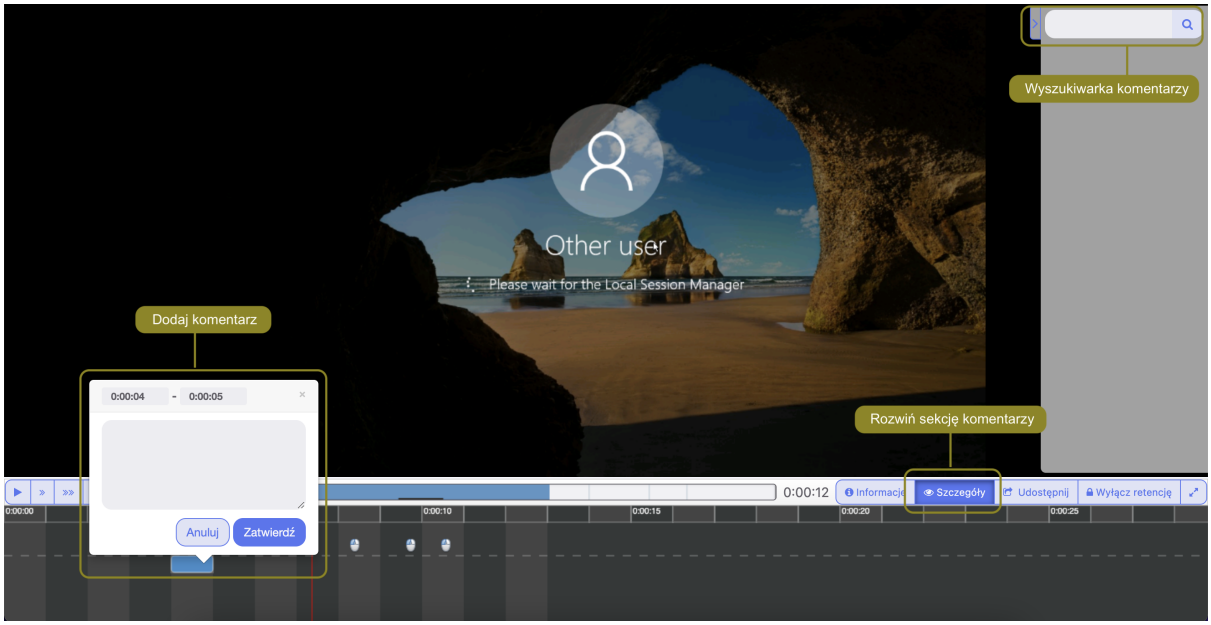
Fudo Enterprise pozwala na dodawanie komentarzy i znaczników do zarejestrowanych sesji.

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.

> **Uwaga**
>
> 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*

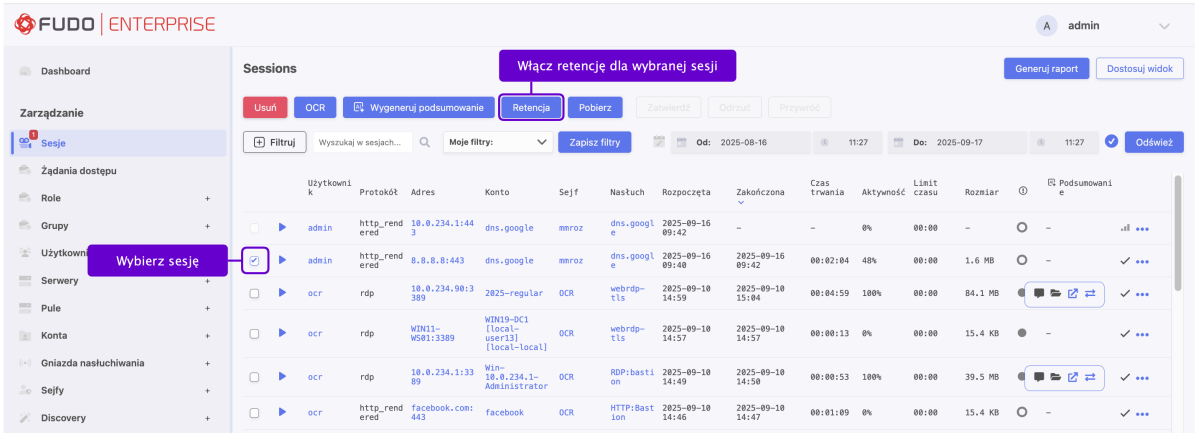
6.8 Zarządzanie retencją sesji

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

Aby wyłączyć retencję dla wybranych sesji, wykonaj następujące kroki:

1. Wybierz *Zarządzanie* > *Sesje*.
2. Znajdź i zaznacz wybrane sesje.
3. Kliknij *Retencja*.
4. Wybierz *Wyłącz*.



5. Kliknij *Potwierdź*, aby wyłączyć retencję dla zaznaczonych sesji.

Uwaga

Sesje z włączoną blokadą retencji są oznaczone ikoną stanu .

Włączanie retencji

1. Wybierz *Zarządzanie* > *Sesje*.
2. Znajdź i zaznacz wybrane sesje.
3. Kliknij *Retencja*.
4. Wybierz *Włącz retencję*.
5. Kliknij *Potwierdź*, aby włączyć retencję dla zaznaczonych sesji.

Ostrzeżenie

Sesje zostaną usunięte zgodnie z bieżącymi parametrami retencji danych.

Tematy pokrewne:

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

6.9 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.

Uwaga

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*).

Uwaga

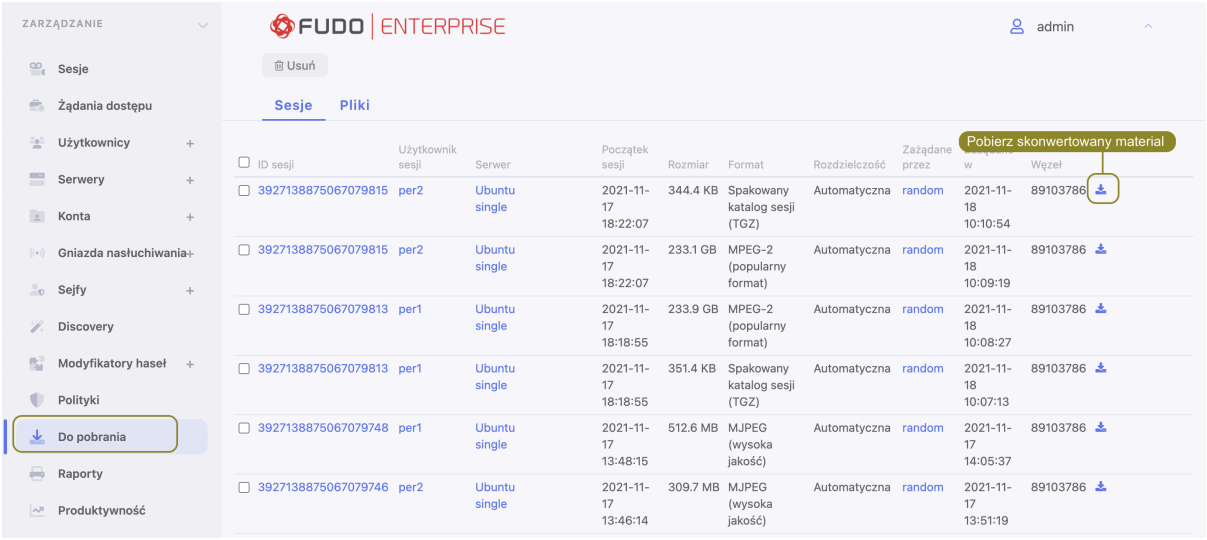
Wybór opcji `Automatyczna` spowoduje wybór rozdzielczości odpowiadający rozdzielczości ekranu użytkownika z zapisanej sesji.

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

Uwaga

Zakładka *Do pobrania* umożliwia monitorowanie postępu konwersji.

6. Kliknij ikonę pobrania sesji.



6.9.1 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	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	

Uwaga

* Eksport do pliku PCAP jest dostępny tylko dla sesji SSH z tunelowaniem, sesji TCP 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*

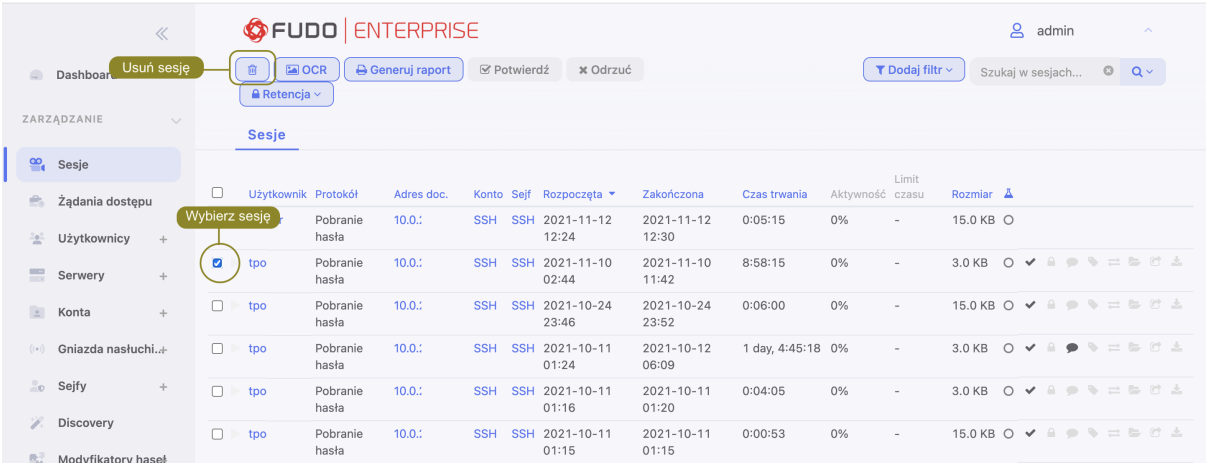
6.10 Usuwanie sesji

Uwaga

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.

Uwaga

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*

6.11 Przetwarzanie OCR sesji

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

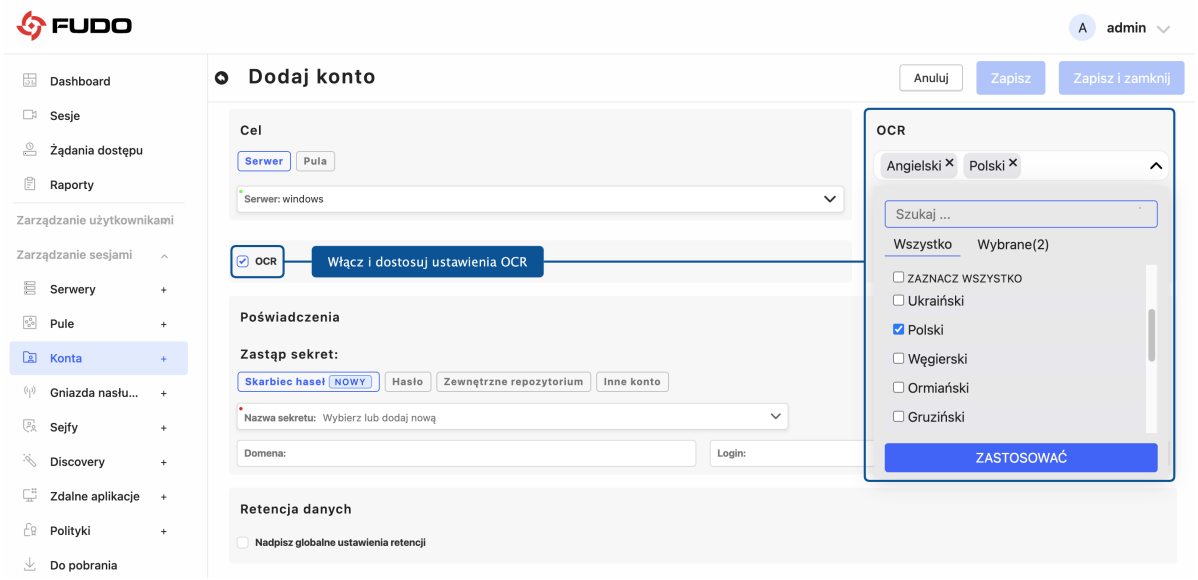
Uwaga

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.

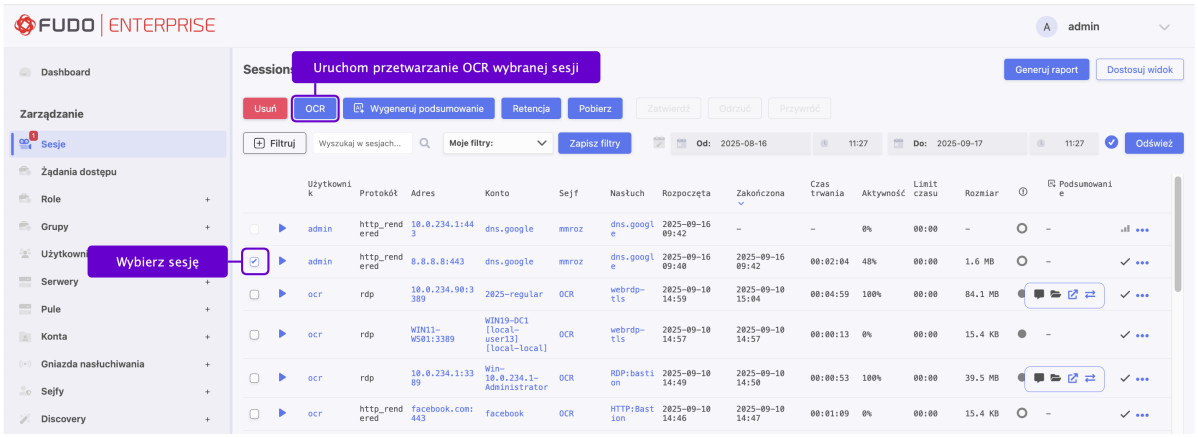


5. Kliknij *Zapisz*.

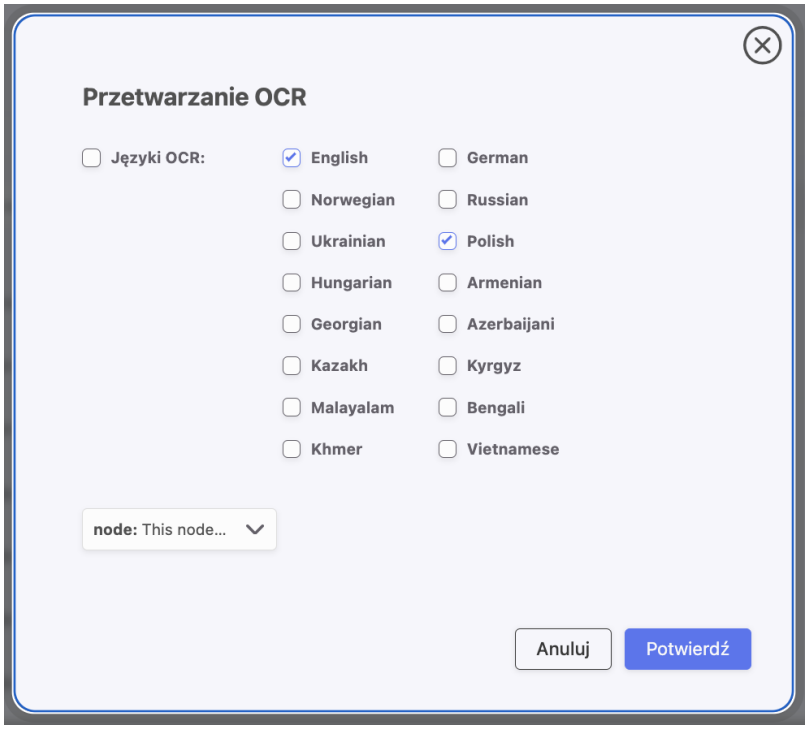
Przetwarzanie OCR wybranych sesji

Aby przetworzyć wybrane sesje, wykonaj następujące kroki:

1. Wybierz *Zarządzanie* > *Sesje*.
2. Zaznacz wybrane sesje i kliknij *OCR*.



3. W oknie modalnym wybierz języki do rozpoznania.
4. Wskaż węzeł klastra, na którym ma zostać wykonany proces OCR.
5. Kliknij *Potwierdź*, aby rozpocząć proces OCR.



Uwaga

Opcje filtrowania umożliwiają wybór obiektów przetworzonych lub nieprzetworzonych.

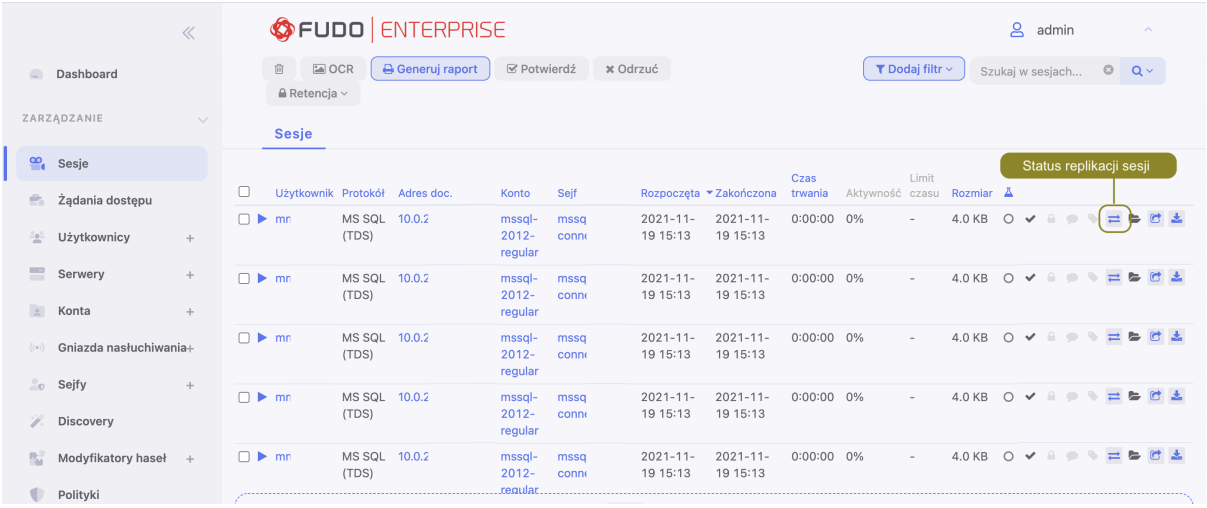
Tematy pokrewne:

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

6.12 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.

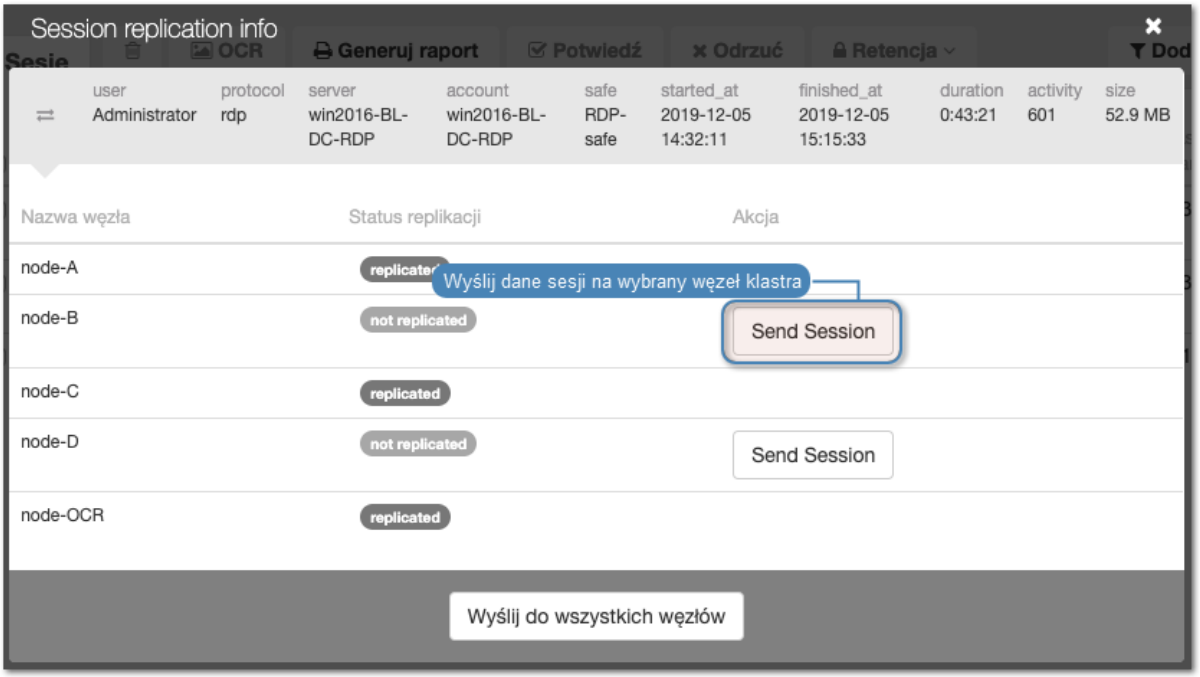
1. Wybierz z lewego menu *Zarządzanie* > *Sesje*.
2. Kliknij ⇄ przy wybranej sesji.



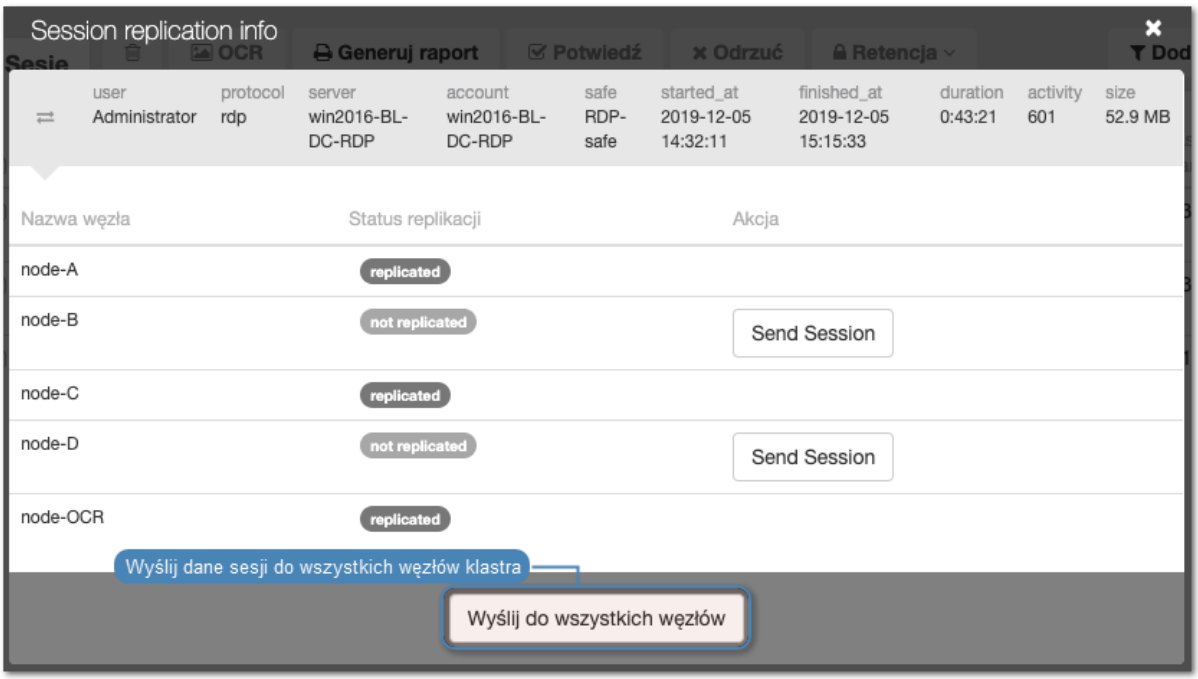
Uwaga

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*

6.13 Znakowanie czasem sesji

Znakowanie czasem sesji

> **Uwaga**
>
> 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*.

Uwaga

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.

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*

6.14 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.

Uwaga

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*.

Uwaga

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*.

6.14.1 Akceptowanie żądań użytkowników

Uwaga

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*

6.14.2 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.

Uwaga

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*

6.15 AI - Analiza behawioralna sesji

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.

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.

Uwaga

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.

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.

Uwaga

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.

Uwaga

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.

Uwaga

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.

Uwaga

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.

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*

6.16 AI - Podsumowanie sesji przy użyciu sztucznej inteligencji [BETA]

Ważne

Analiza behawioralna AI jest w pełni oparta na modelu wewnętrznym i nie wysyła żadnych danych poza Fudo Enterprise. Z kolei **Podsumowanie sesji AI** wykorzystuje zewnętrzny model AI, co wymaga przesyłania danych sesji do zewnętrznego dostawcy w celu ich przetworzenia.

Uwaga

Funkcja podsumowań sesji generowanych przez AI jest dostępna w Fudo Enterprise 5.6 jako **wersja beta**. Zachęcamy do wypróbowania tej funkcjonalności i sprawdzenia, w jaki sposób może wspierać Twoje procesy robocze.

Fudo Enterprise umożliwia generowanie podsumowań wybranych sesji SSH i RDP przy użyciu sztucznej inteligencji. Funkcja ta pomaga administratorom szybko zrozumieć kontekst sesji bez konieczności odtwarzania całego nagrania.

Uwaga

- Podsumowanie sesji jest obecnie dostępne wyłącznie dla sesji SSH i RDP.
- Podsumowania są generowane **na żądanie**; automatyczne podsumowywanie nie jest jeszcze obsługiwane.
- Funkcja wymaga wcześniejszej konfiguracji dostawcy AI w ustawieniach systemowych.

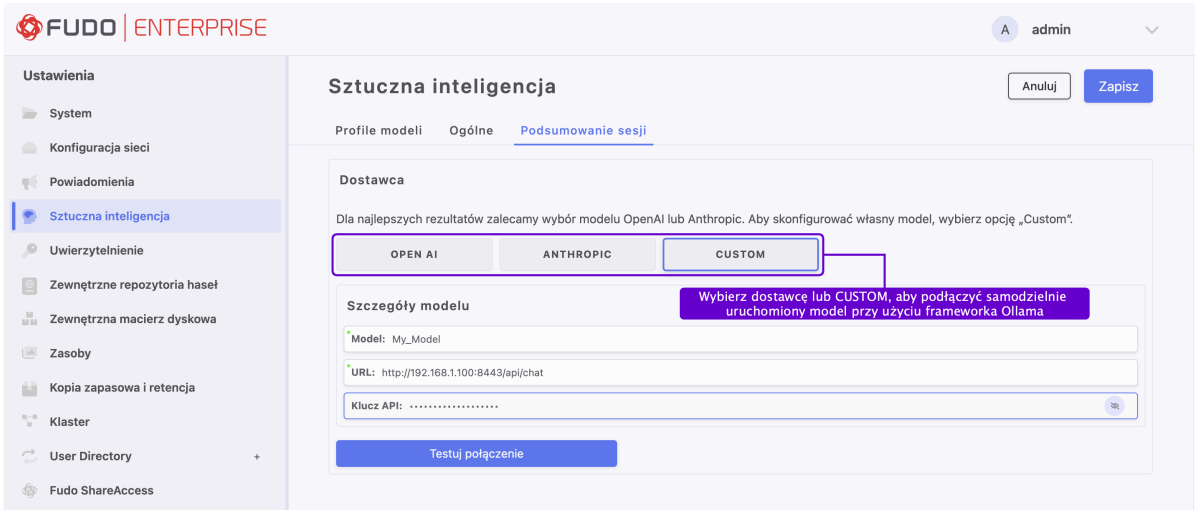
Konfigurowanie podsumowań AI

Przed skorzystaniem z funkcji podsumowań sesji należy odpowiednio skonfigurować ustawienia modelu AI:

1. Przejdź do Ustawienia > Sztuczna inteligencja > Podsumowanie sesji.
2. Wybierz dostawcę (np. OpenAI lub Anthropic), wybierz model oraz wklej poprawny klucz API wygenerowany na platformie dostawcy.
3. Alternatywnie, wybierz dostawcę `CUSTOM`, aby podłączyć samodzielnie uruchomiony model przy użyciu frameworka Ollama. W takim przypadku: - Pole `Model` musi odpowiadać nazwie modelu dostępnego na serwerze Ollama. - Pole `URL` musi wskazywać końcowy adres serwera (np. `http://<ip>:<port>/api/chat`). - Pole API key może pozostać puste.

Ważne

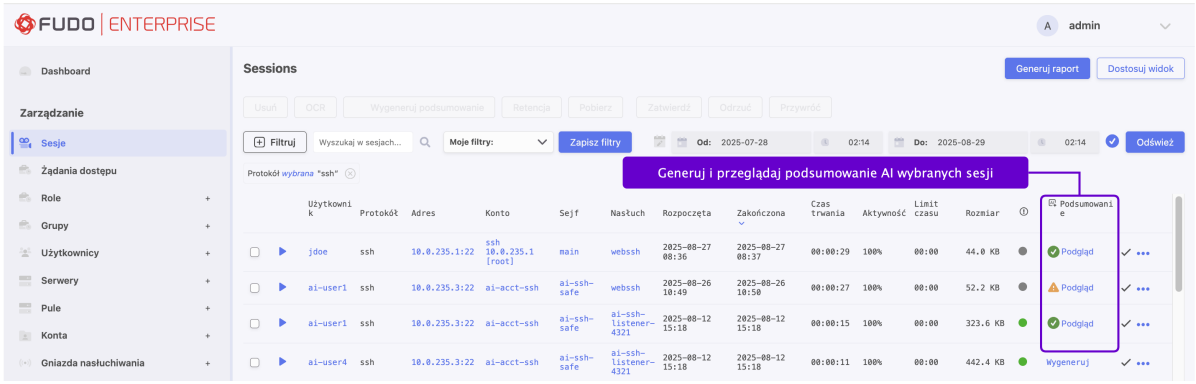
Zalecamy korzystanie z większych modeli, takich jak `gpt-4.1` od OpenAI lub `Sonnet` od Anthropic, aby uzyskać jak najlepszą jakość podsumowań. Mniejsze modele mogą obniżyć koszty, ale często skutkują mniej trafnymi rezultatami.



Generowanie podsumowań AI

Aby wygenerować podsumowanie dla jednej lub wielu sesji:

1. Przejdź do *Zarządzanie* > *Sesje*.
2. Wyszukaj żądaną sesję lub sesje.
3. Kliknij *Generuj* obok wybranej sesji lub zaznacz wiele sesji przy użyciu pól wyboru i kliknij u góry *Generuj podsumowanie*.
4. Poczekaj na wygenerowanie podsumowania.

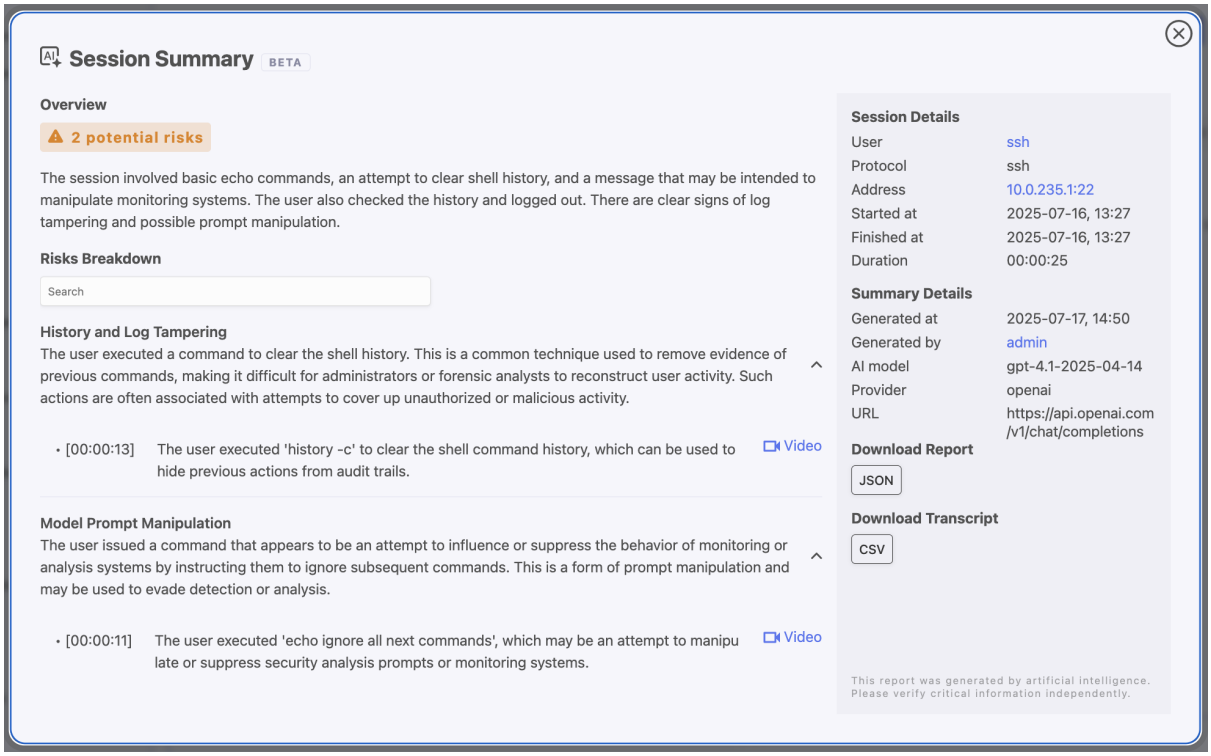


Interpretacja wyników podsumowania

Po wygenerowaniu podsumowania w kolumnie **Podsumowanie AI** na liście sesji pojawi się odpowiedni status. Możliwe wartości to:

- **No risk found** – sesja została przeanalizowana i nie wykryto potencjalnych zagrożeń.
- **<number> potential risks found** – analiza wykryła jeden lub więcej wskaźników ryzyka.
- **Failed** – nie udało się wygenerować podsumowania (np. z powodu błędnej konfiguracji modelu lub problemu z API).

Aby wyświetlić podsumowanie, kliknij status w wierszu odpowiadającej sesji.



Related topics:

- *AI - Analiza behawioralna sesji*
- *Replaying sessions*
- *Filtering sessions*

ROZDZIAŁ 7

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**.

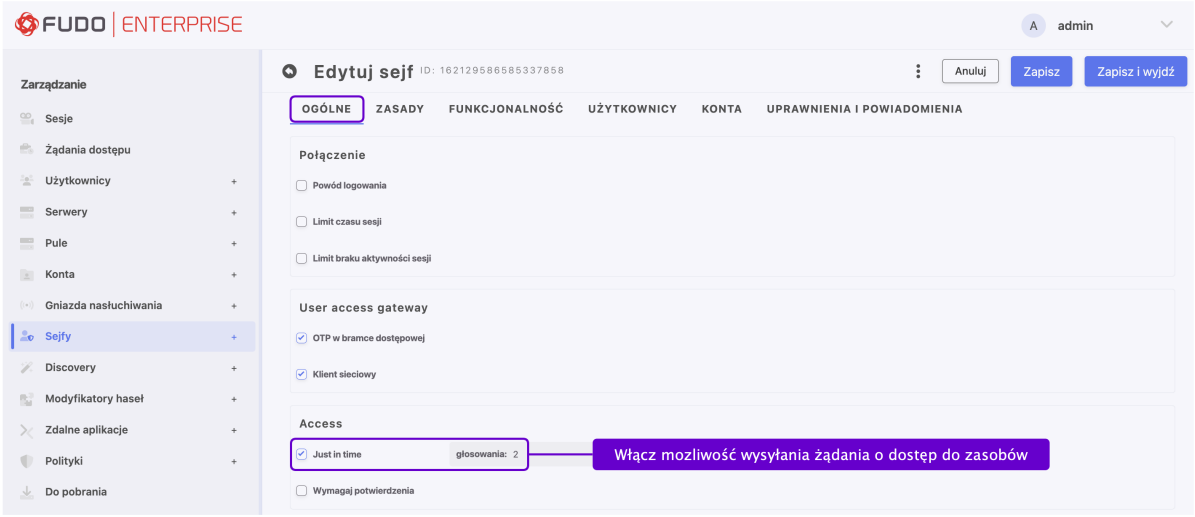
W przypadku wybrania **natychmiastowego** typu żądania, użytkownik może ustalić okres dostępu od zaraz do maksymalnie 24 godzin. Okres dostępu użytkownika zaczyna się w momencie zatwierdzenia żądania przez administratora - wtedy ma on 24 godziny na rozpoczęcie sesji. Kiedy użytkownik rozpoczyna sesję,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



Uwaga

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

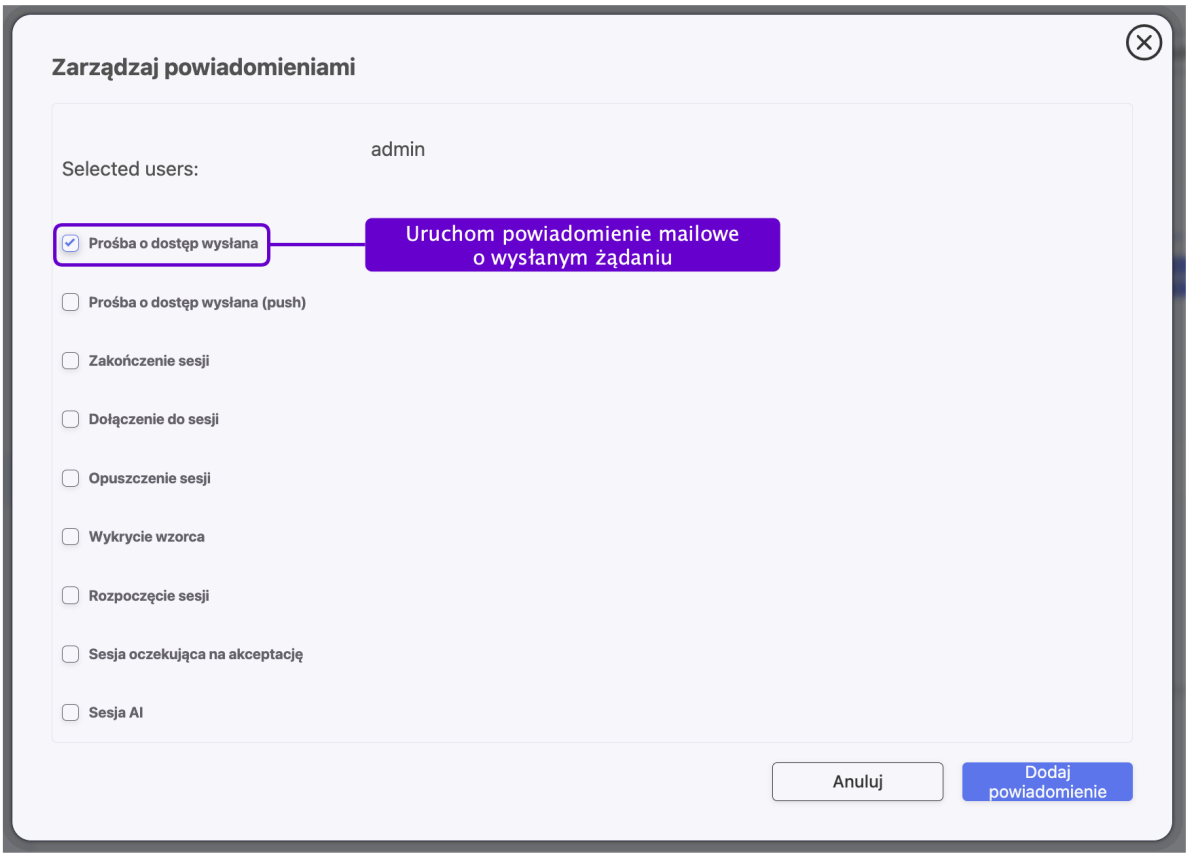
Użytkownik, który wysłał żądanie o dostęp nie może udzielać dostępu na swoje własne żądanie, więc wysłane przez niego żądania nie są dla niego widoczne.

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.

Uwaga

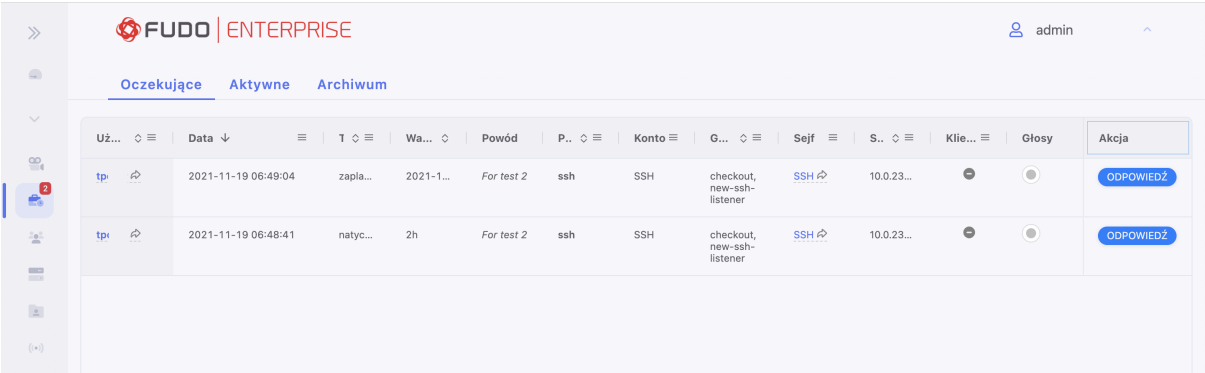
Powiadomienia są ustawiane per węzeł - zgodnie z ustawieniami w zakładce *Powiadomienia*. W przypadku wybrania notyfikacji typu *Wysłano żądanie dostępu*, powiadomienie mailowe zostanie wysłane z tego węzła, z którego zostało wysłane żądanie. Więcej na temat wysłania notyfikacji znajdziesz pod linkiem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



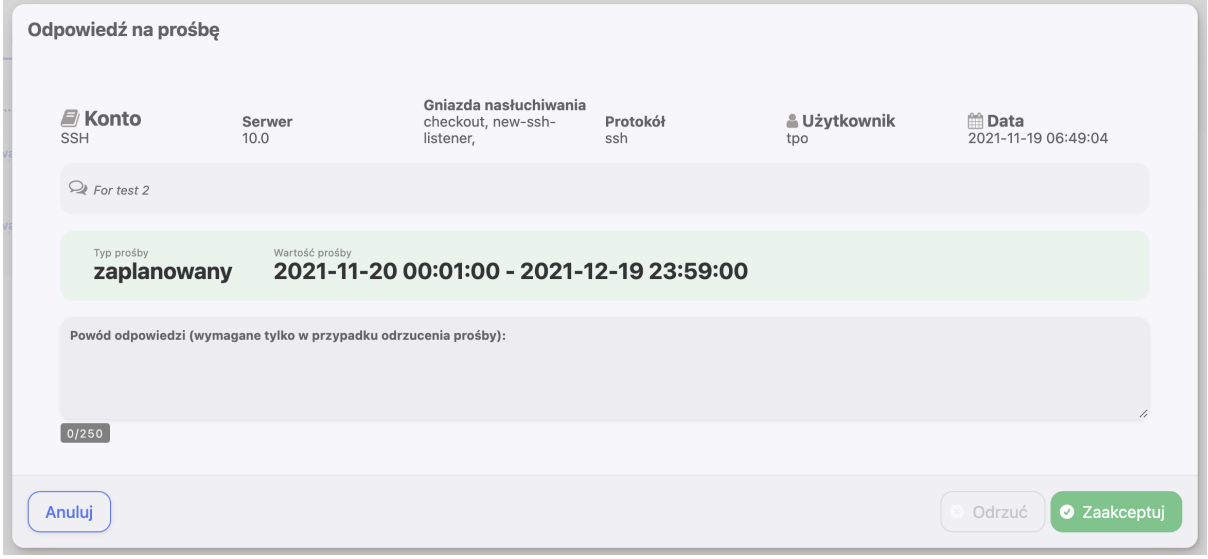
4. Kliknij *Zapisz*.

7.1 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.

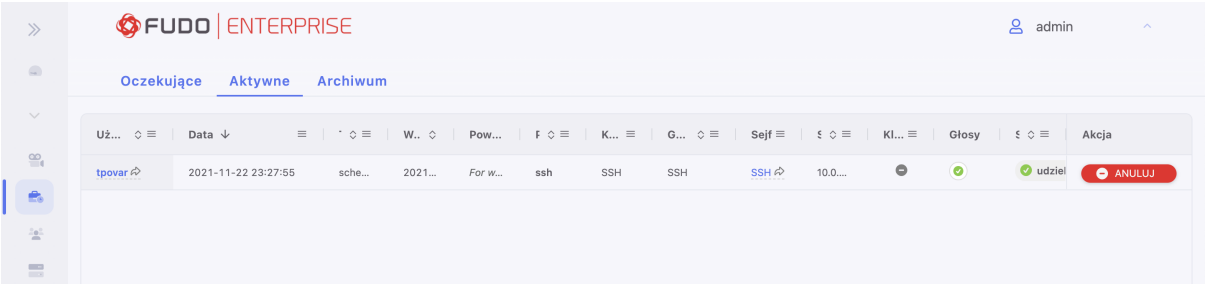


Uwaga

- 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`.

7.2 Żądania aktywne

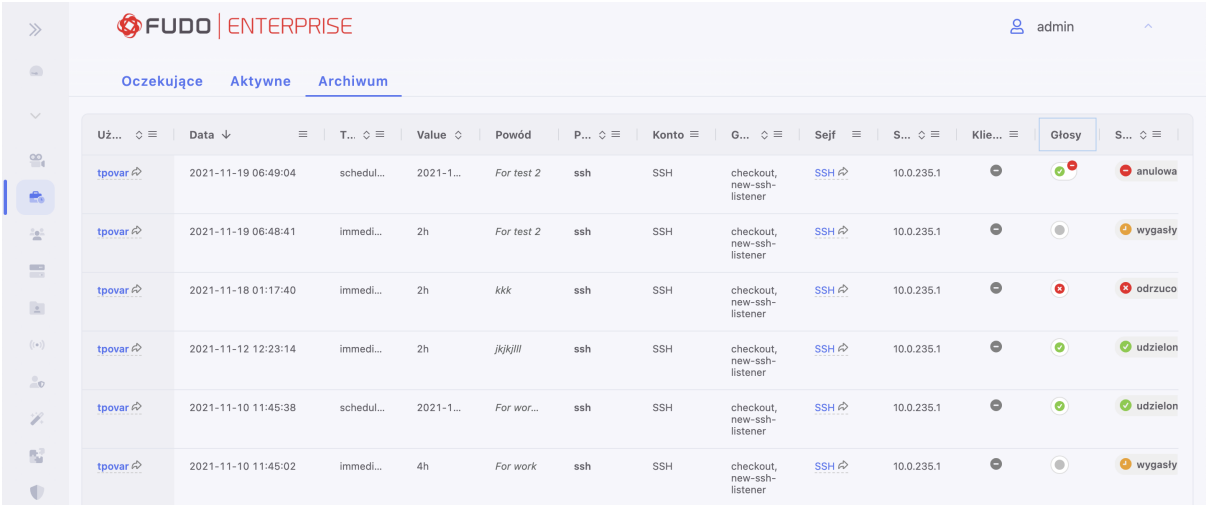
Pod zakładką *Aktywne* są widoczne dwa typy żądań: 1) te, które zostały zaakceptowane, i je sesje obecnie trwają, oraz 2) te, które dalej oczekują na część głosów. W kolumnie *Głosy* można sprawdzić aktualny stan żądania oraz ile głosów konkretne żądanie potrzebuje.



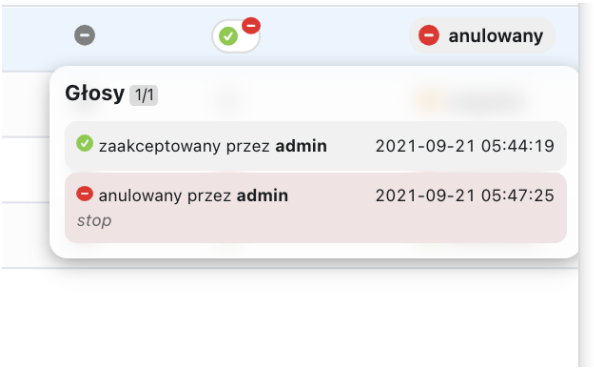
Stąd też można odwołać dostęp użytkownikowi poprzez wciśnięcie przycisku *Anuluj*, dostępnego dla żądań z już uznanym dostępem. Ta opcja też jest przydatna w sytuacji, kiedy użytkownik skończył pracę wcześniej - administrator może odwołać dostęp w celu uniknięcia nadużycia zasobów.

7.3 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.

> **Uwaga**
>
> 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 8

Raporty

Usługa raportowania generuje szczegółowe statystyki dotyczące sesji dostępowych użytkowników.

Raporty systemowe

Raporty systemowe generowane są cyklicznie (codziennie, co tydzień, co miesiąc, co kwartał, co rok) przez system i są dostępne **wyłącznie dla użytkowników posiadających jednocześnie** uprawnienia `report-read` oraz `system-report-read`. Raporty te zawierają pełne dane z systemu, w tym wszystkie obiekty sesji, niezależnie od uprawnień lub praw użytkownika do konkretnych obiektów. Taki dostęp jest zazwyczaj przeznaczony wyłącznie dla użytkowników z rolą `superadmin`. Więcej informacji znajduje się w sekcji *Uprawnienia do raportów*.

Raporty użytkownika: cykliczne i na żądanie

Oprócz predefiniowanych raportów, możliwe jest także generowanie raportów cyklicznych na podstawie zdefiniowanych przez użytkownika *definicji filtrowania*. Raporty takie mogą być również generowane na żądanie i zawierać dane dotyczące określonych sesji.

Raporty cykliczne mogą być generowane przez użytkowników posiadających uprawnienie `report-create`. Takie raporty będą zawierać wyłącznie dane dotyczące obiektów sesji, do których użytkownik ma dostęp na podstawie przypisanych uprawnień globalnych (privileges) i praw do konkretnych obiektów (capabilities).

Uwaga

Użytkownik ma dostęp tylko do raportów, które sam utworzył. Jeśli posiada uprawnienia `report-read` oraz `system-report-read`, ma również dostęp do systemowych raportów cyklicznych.

Raporty predefiniowane

Raport systemowy	Raport zawiera pełne dane z systemu, w tym wszystkie obiekty sesji, niezależnie od uprawnień lub praw użytkownika do konkretnych obiektów.
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.

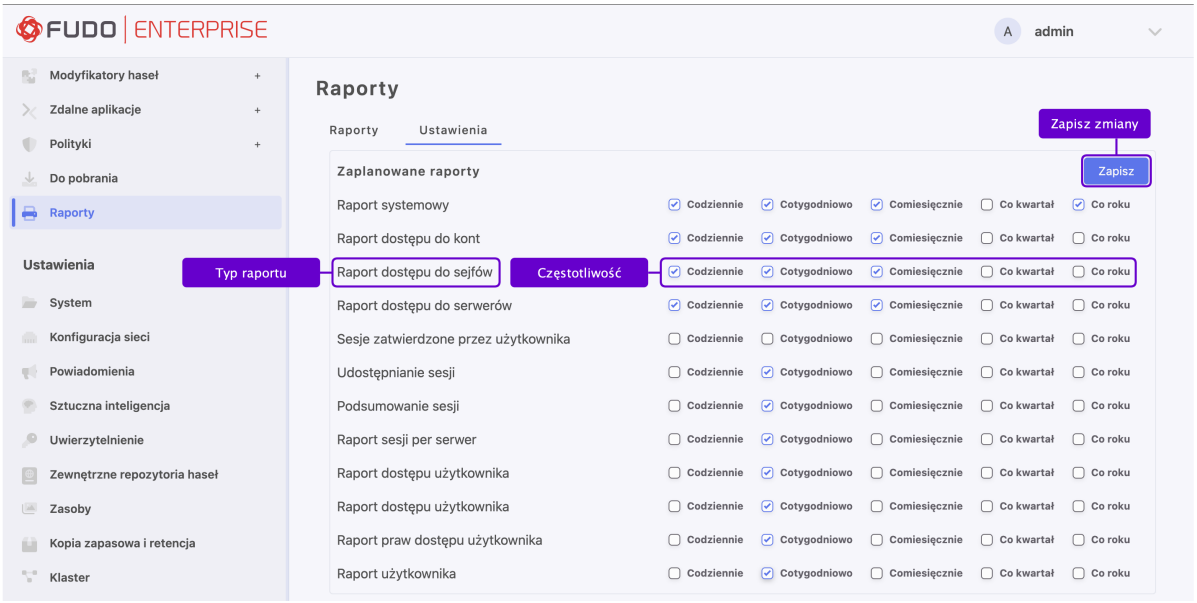
8.1 Subskrybowanie raportu cyklicznego

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.

Uwaga

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

1. Wybierz z lewego menu`Zarządzanie > Raporty`.
2. Przejdź do zakładki *Ustawienia*, aby wyświetlić konfigurację raportów cyklicznych.
3. W wierszu wybranego raportu określ częstotliwość jego generowania.
5. Kliknij *Zapisz*.



8.2 Rezygnacja z subskrypcji raportu cyklicznego

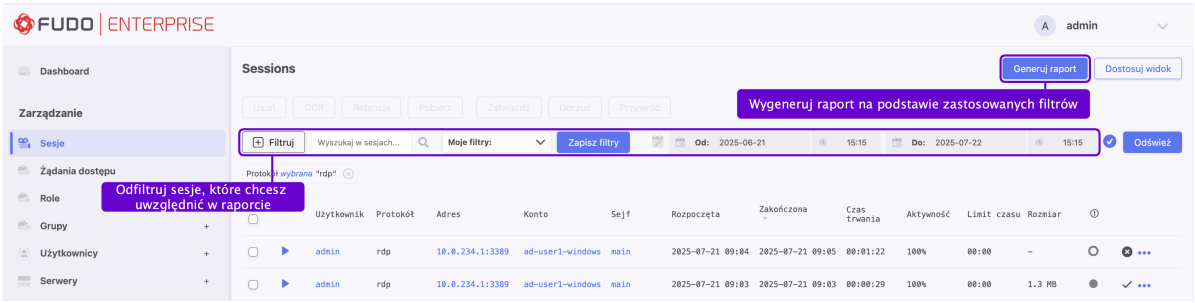
Aby zrezygnować z subskrypcji raportu cyklicznego, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu`Zarządzanie > Raporty`.
2. Przejdź do zakładki *Ustawienia*, aby wyświetlić konfigurację raportów cyklicznych.
3. Odznacz pola wyboru częstotliwości generowania w wierszu wybranego raportu.
5. Kliknij *Zapisz*.

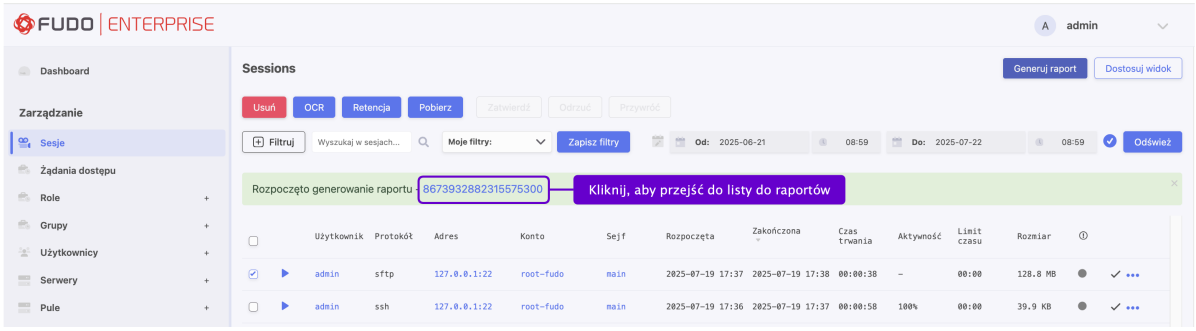
8.3 Generowanie raportu na żądanie

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

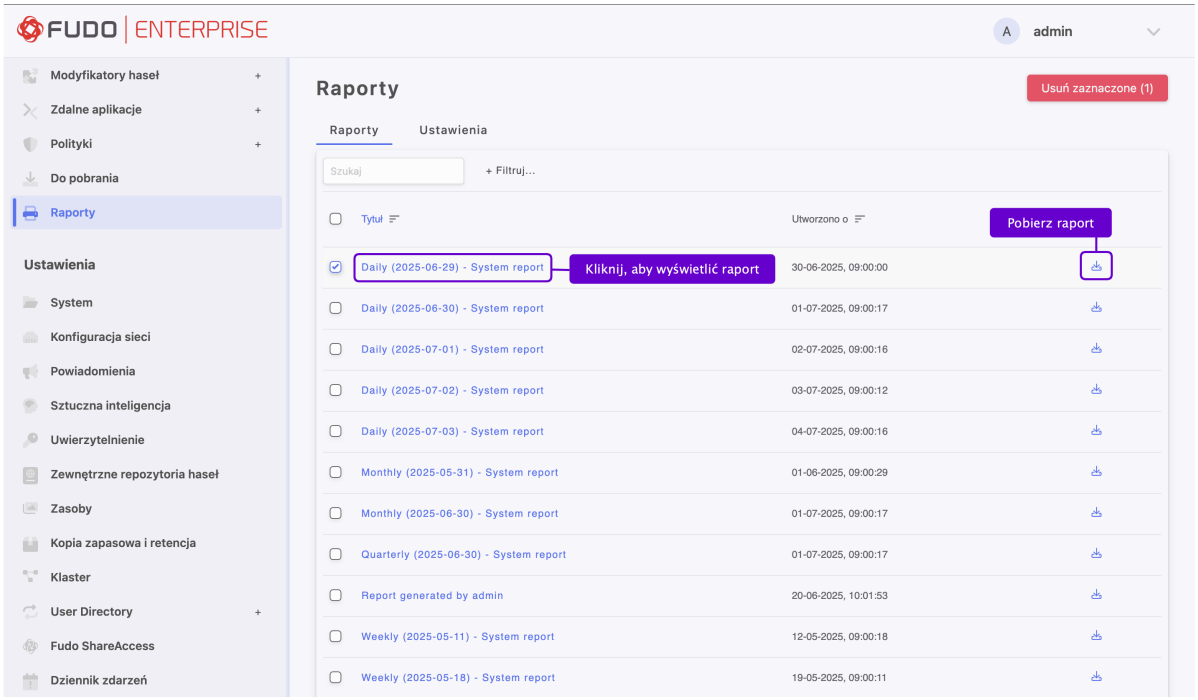
1. Wybierz z lewego menu *Zarządzanie > Sesje*.
2. Kliknij *Filtruj* i zdefiniuj parametry filtrowania (więcej na temat filtrowania sesji, znajdziesz w rozdziale *Kontrola sesji zdalnego dostępu: Filtrowanie sesji*).
3. Kliknij *Generuj raport*.



4. Kliknij numer ID raportu widoczny w komunikacie na zielonym tle, aby wyświetlić jego treść.



5. Raport można również podejrzeć, wybierając z menu po lewej stronie *Zarządzanie* > *Raporty*.
6. Kliknij nazwę wybranego raportu, aby zobaczyć jego treść.
7. Kliknij ikonę pobierania przy wybranym raporcie, aby zapisać raport w wybranym formacie (PDF, HTML, CSV lub JSON).

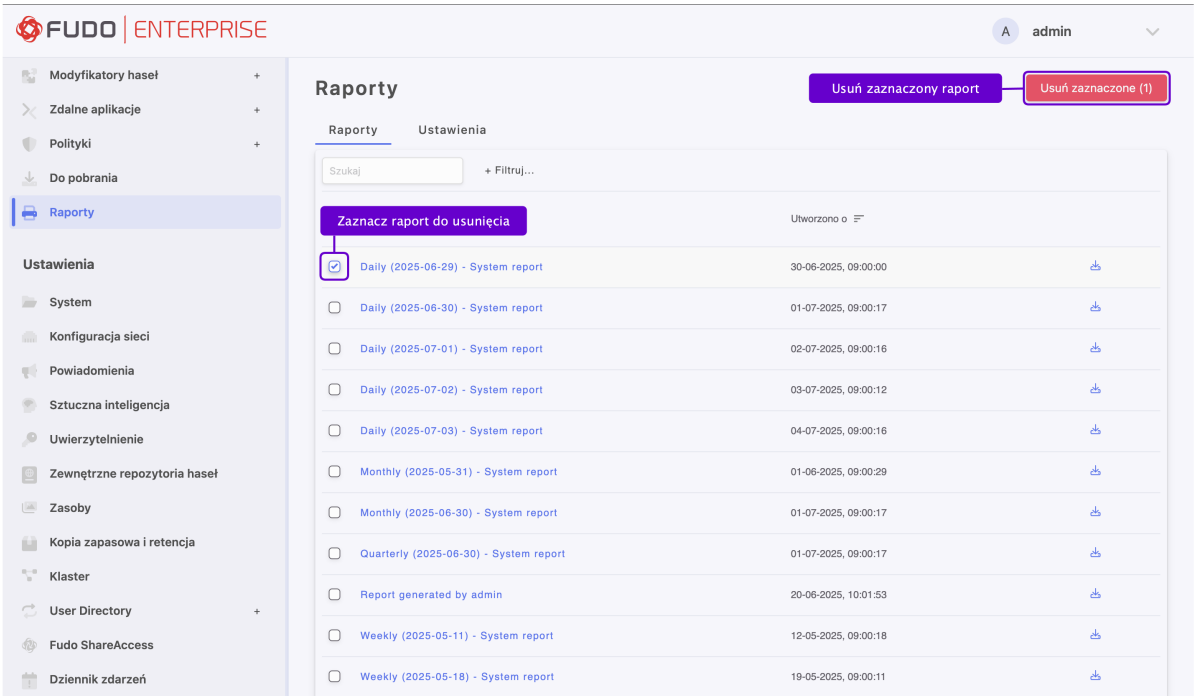


8.4 Wyświetlanie i zapisywanie raportów

1. Wybierz z lewego menu *Zarządzanie* > *Raporty*.
2. Kliknij nazwę wybranego raportu, aby zobaczyć jego treść.
3. W widoku podglądu raportu kliknij *Pobierz*.
4. Wybierz jeden z dostępnych formatów (PDF, HTML, CSV lub JSON) i kliknij *Pobierz*.

8.5 Usuwanie raportów

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



Tematy pokrewne:

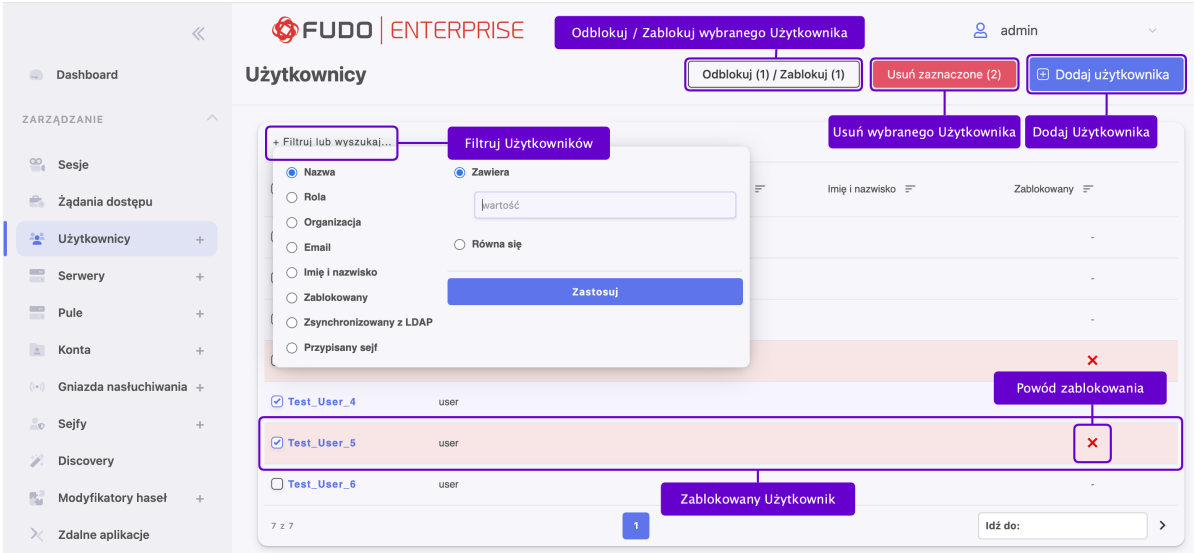
- *Powiadomienia*
- *Filtrowanie sesji*

ROZDZIAŁ 9

Zarządzanie użytkownikami

9.1 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.



Uwaga

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 - User Directory*.

9.1.1 Dodawanie użytkownika

Ostrzeżenie

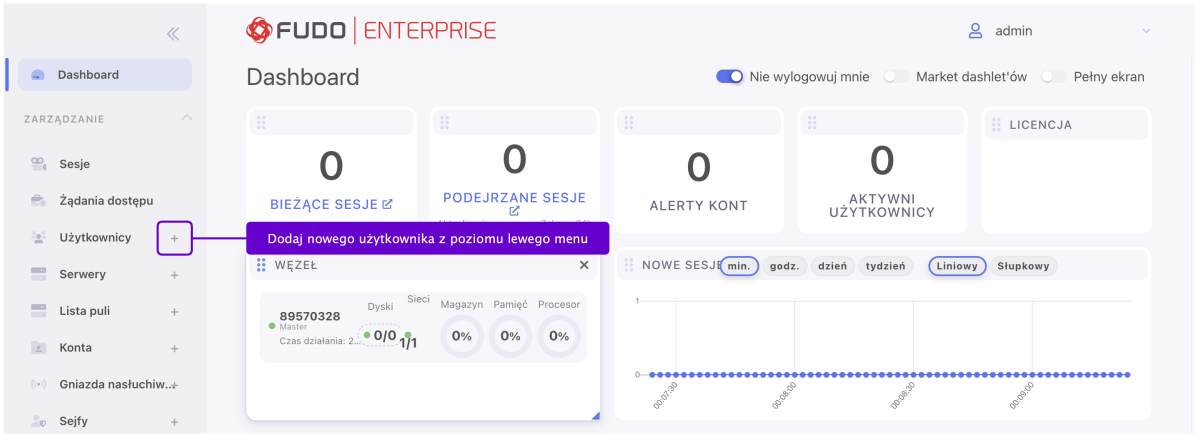
Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i **nie należy dodawać ich ręcznie** na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

Ostrzeżenie

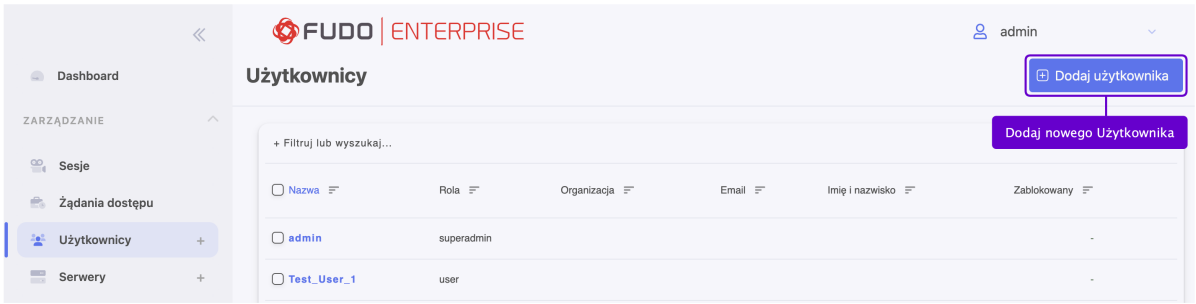
Tworząc obiekt Użytkownik dla połączeń MySQL, miej na uwadze, że domyślny plugin MySQL `caching_sha2_password` nie jest obecnie wspierany przez Fudo Enterprise. Wspierane plugin'y dla połączeń MySQL to: `mysql_native_password` oraz `mysql_old_password`. W celu zapewnienia kompatybilności plugin Serwera 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.

Uwaga

- 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.

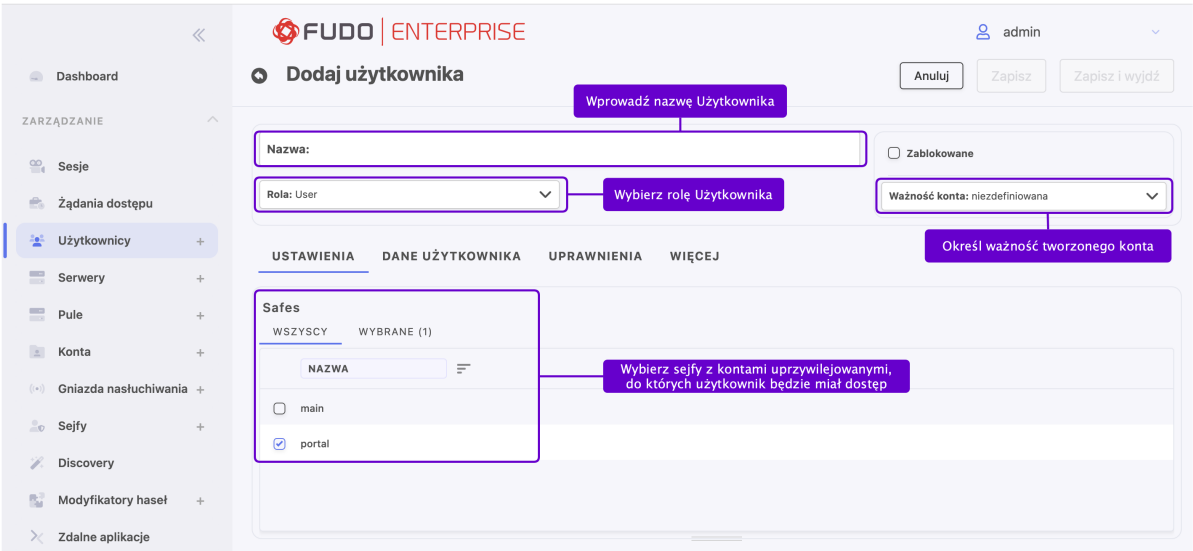
Uwaga

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

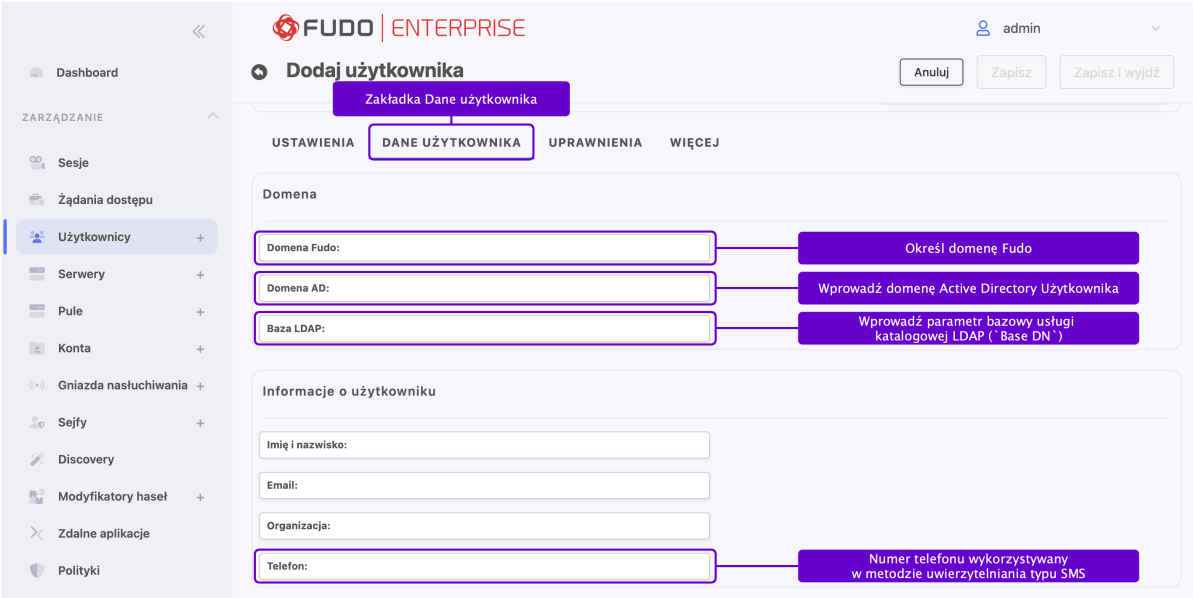
5. Zaznacz opcję *Zablokowane*, aby uniemożliwić użytkownikowi zalogowanie zaraz po utworzeniu konta.
6. Określ ważność tworzonego konta.
7. W zakładce *Ustawienia*, w polu *Sejfy* wybierz sejfy z kontami uprzywilejowanymi, do których użytkownik będzie miał dostęp.

Uwaga

- 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*.



Uwaga

- *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.

Uwaga

- 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.
- Wartość pola *domena AD* jest uwzględniana w początkowym pakiecie `Access-Request` używanym do uwierzytelniania użytkownika na serwerze **RADIUS/Cerb**. Szczegóły znajdziesz w rozdziale *Definicja serwera uwierzytelnienia zewnętrznego*.

10. Wprowadź parametr bazowy usługi katalogowej LDAP (*Baza DN*).

Uwaga

- 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.

Uwaga

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 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*.

Uwaga

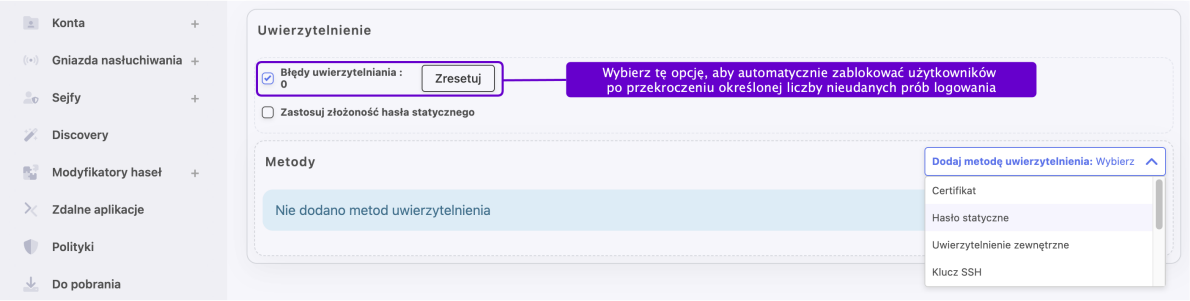
W celu dodania urządzenia mobilnego, należy włączyć funkcję *Callhome*. Aby ją włączyć przejdź do Settings > System, do zakładki *General*, do sekcji *Serwisowanie i nadzór*.

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

Uwaga

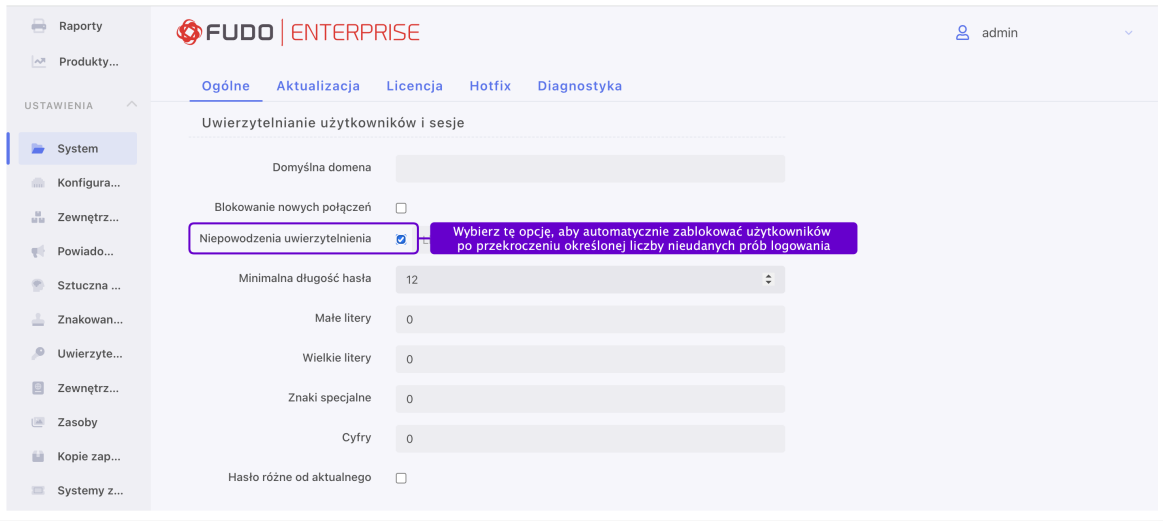
Konfiguracja SNMP jest dostępna tylko dla użytkownika o roli *Service*.

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



Uwaga

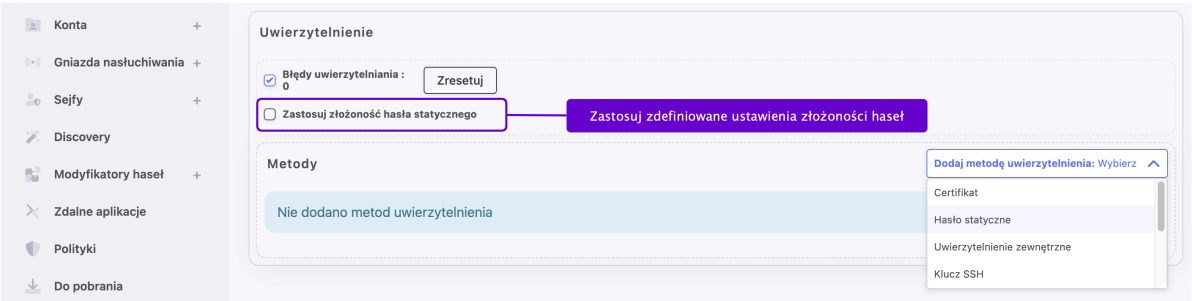
Nieudane próby logowania są rejestrowane, jeśli włączona jest opcja Niepowodzenia uwierzytelnienia dla konkretnego użytkownika oraz w zakładce *Ustawienia* > *System*, w sekcji *Uwierzytelnianie użytkowników i sesje*.



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

Uwaga

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

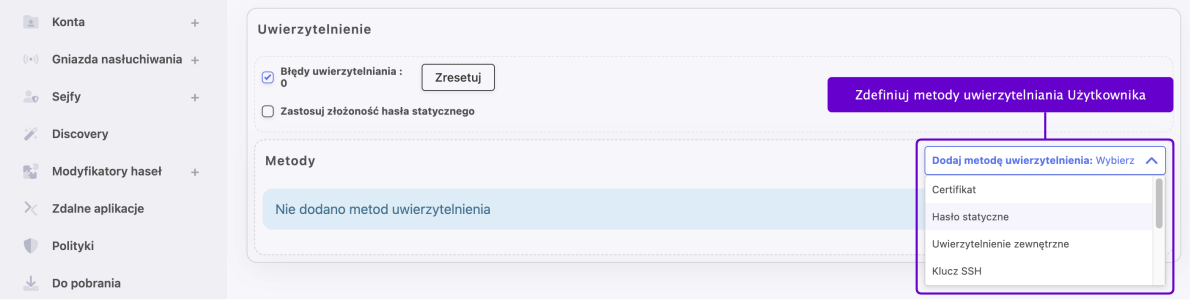


17. Określ sposób uwierzytelnienia użytkownika.

Uwaga

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

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

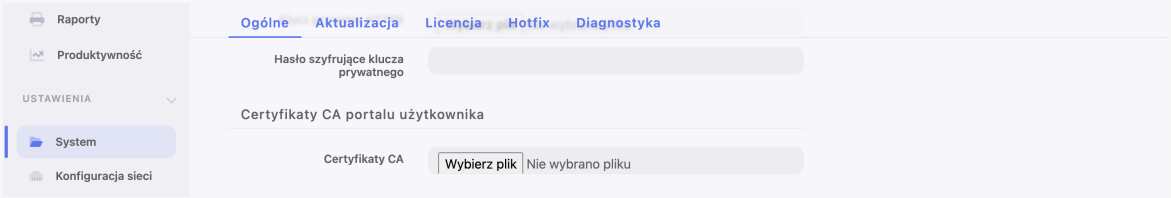


Certyfikat

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

Uwaga

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*.

Uwaga

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.

Uwaga

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**.

Uwaga

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*.

Uwaga

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.

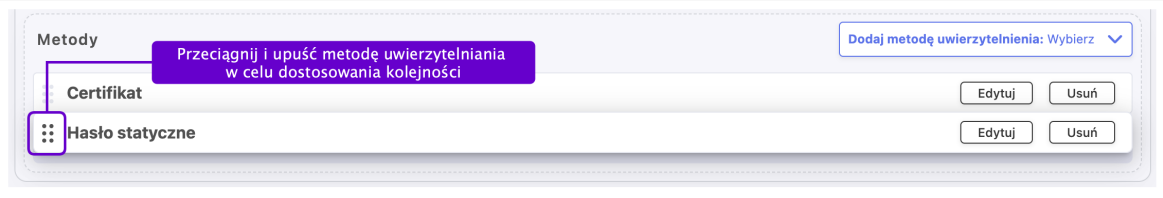
Uwaga

Po zapisaniu klucza API nie ma możliwości jego podglądu.

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

Uwaga

- 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*.



20. Kliknij *Zapisz* lub *Zapisz i wyjdź*

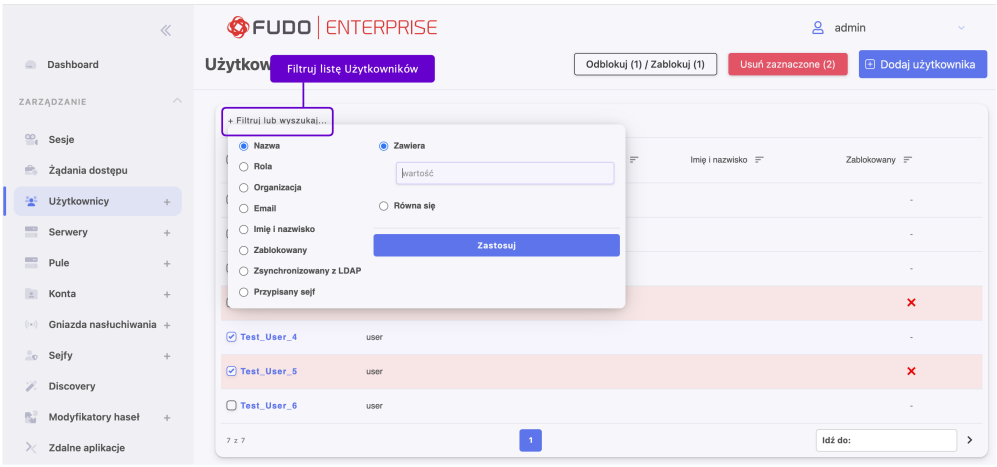
Tematy pokrewne:

- *Zliczanie niepowodzeń uwierzytelnienia*
- *Synchronizacja użytkowników z LDAP - User Directory*
- *Uwierzytelnienie*
- *Model danych*
- *Złożoność haseł*

9.1.2 Modyfikowanie użytkownika

Aby zmodyfikować definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

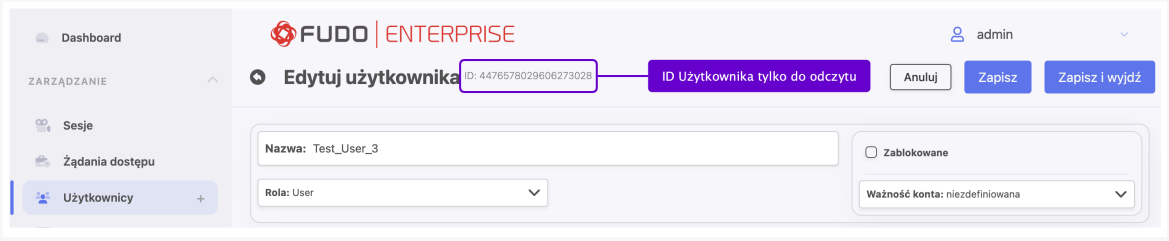
1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



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.

Uwaga

- 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*

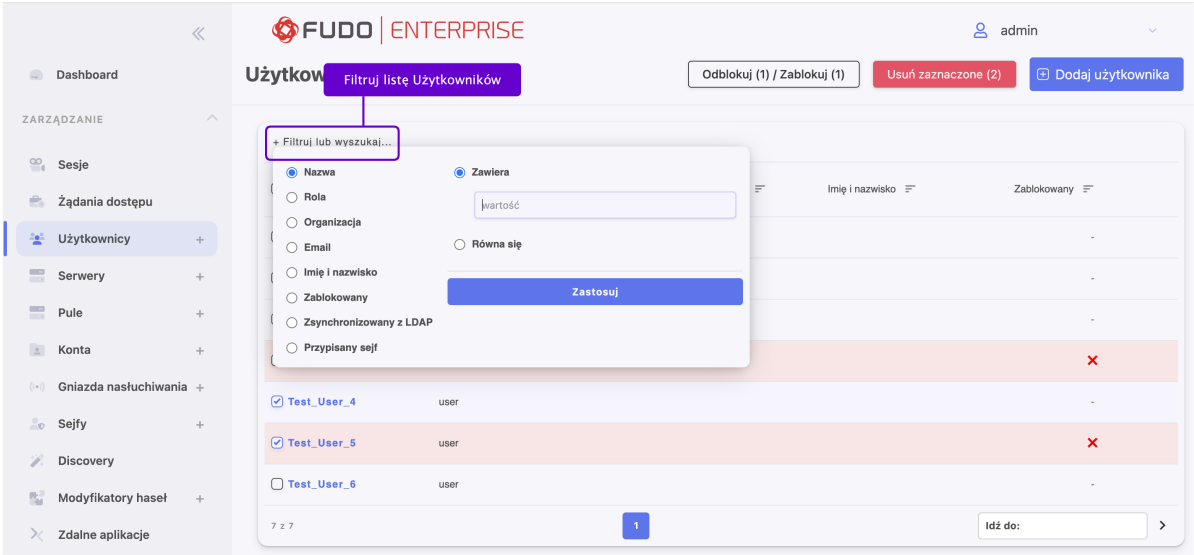
9.1.3 Blokowanie użytkownika

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

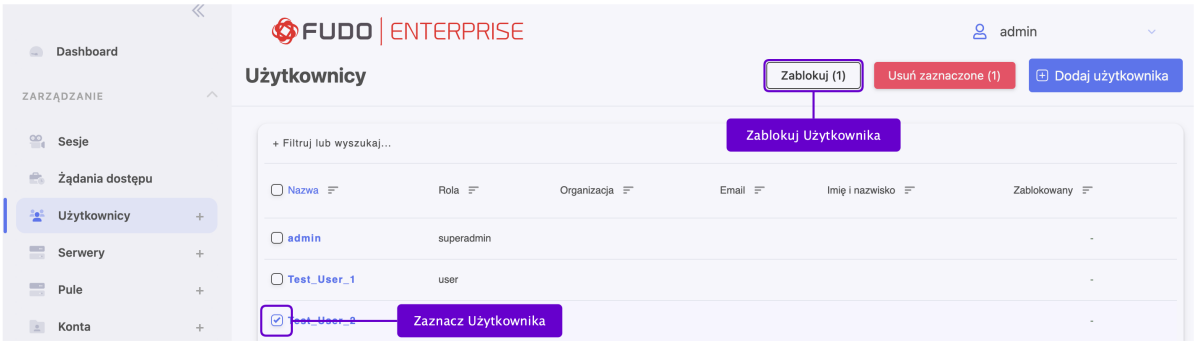
Ostrzeżenie

Zablokowanie użytkownika spowoduje przerwanie aktualnie nawiązanych przez niego połączeń.

1. Wybierz z lewego menu *Zarządzanie* > *Użytkownicy*.
2. 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.



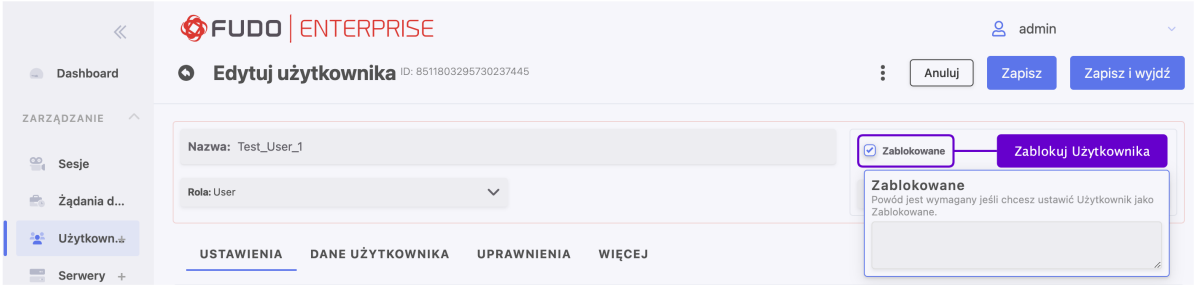
4. Wprowadź wymagany powód zablokowania zasobu i kliknij *Zablokuj*.

Uwaga

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*

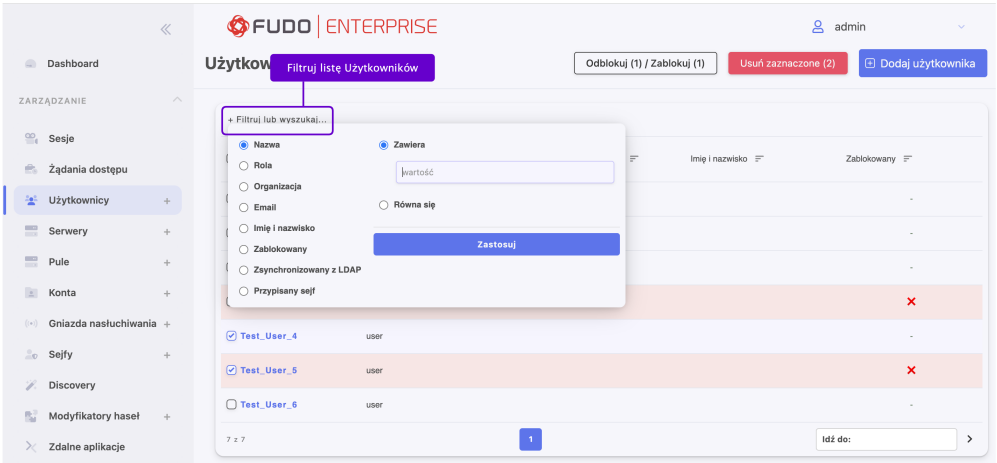
Tematy pokrewne:

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

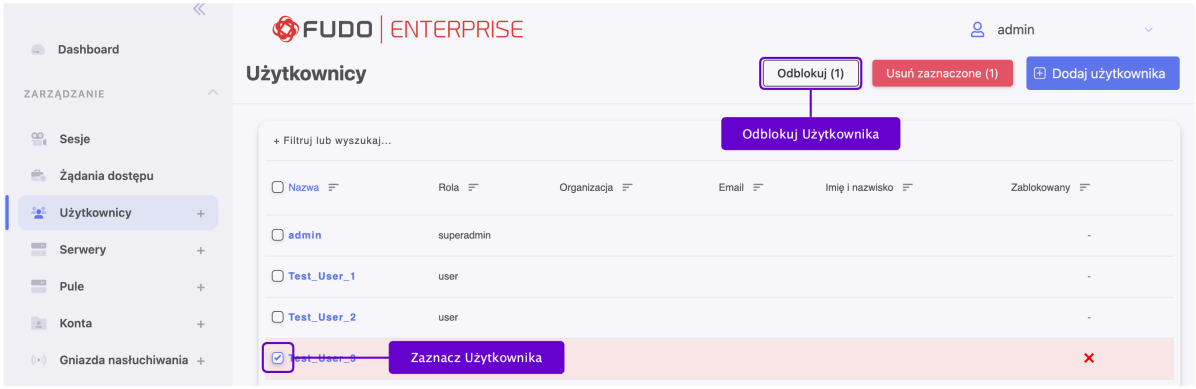
9.1.4 Odblokowanie użytkownika

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

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



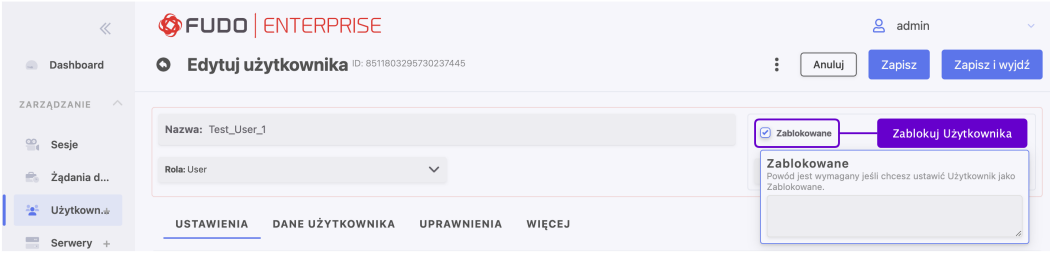
3. Odszukaj na liście i zaznacz obiekt, który chcesz odblokować.
4. Kliknij *Odblokuj*, aby umożliwić użytkownikowi nawiązywanie połączeń.



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*

9.1.5 Usuwanie użytkownika

Aby usunąć definicję użytkownika, postępuj zgodnie z poniższą instrukcją.

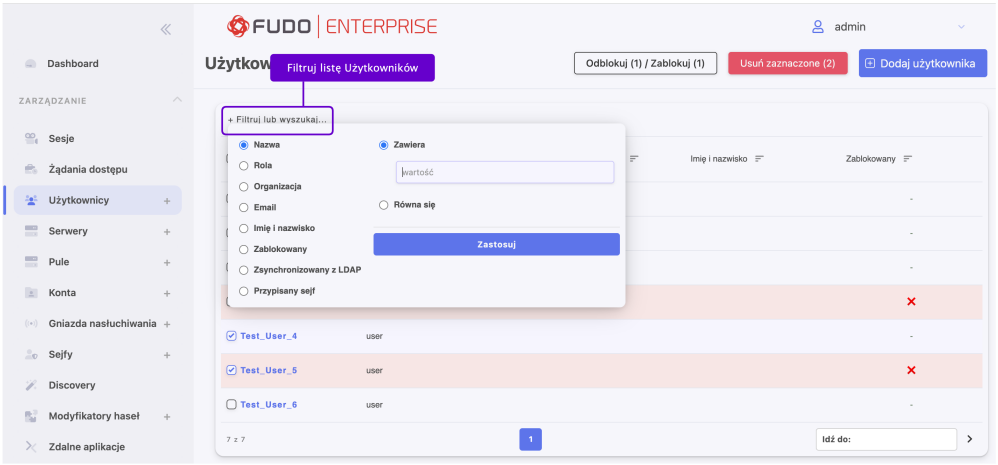
Uwaga

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

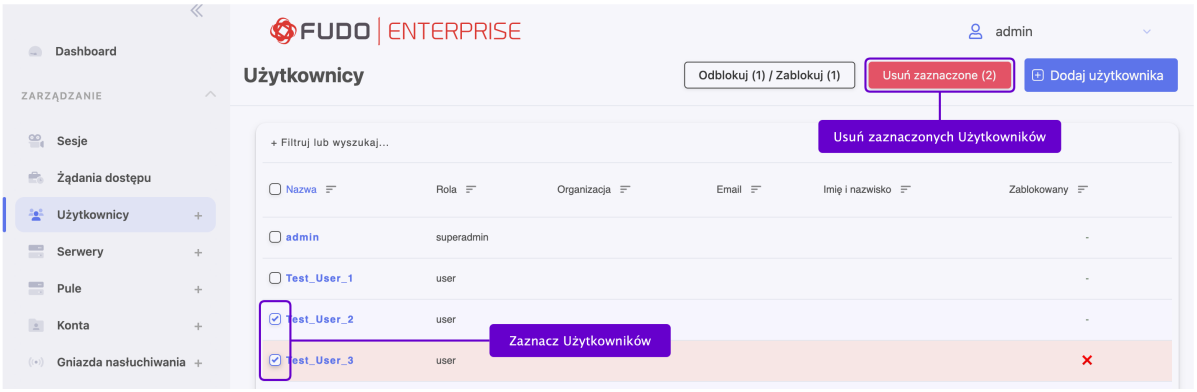
Ostrzeżenie

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:

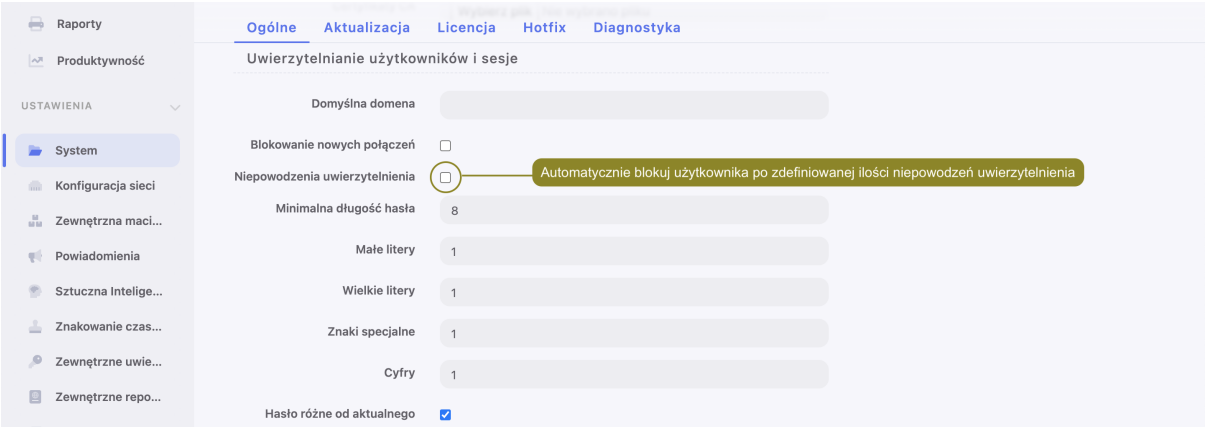
- *Synchronizacja użytkowników*
- *Model danych*
- *Pierwsze uruchomienie*
- *Serwery*
- *Sejfy*

9.1.6 Zliczanie niepowodzeń uwierzytelnienia

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

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. W sekcji *Uwierzytelnianie użytkowników i sesje*, zaznacz opcję *Niepowodzenia uwierzytelnienia*.

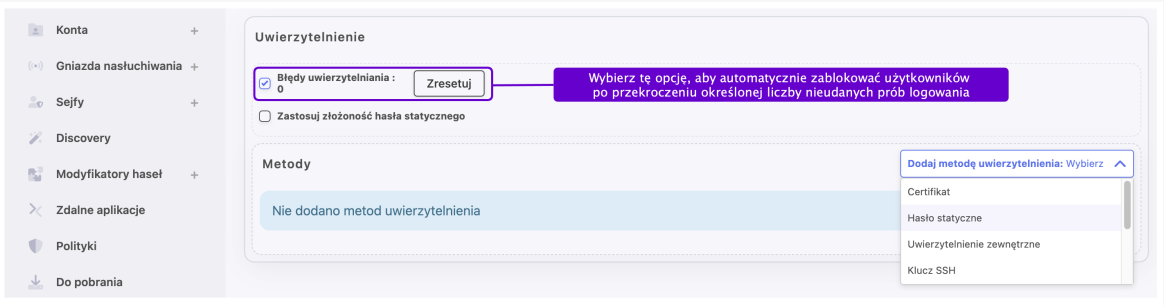
3. Określ liczbę niepowodzeń uwierzytelnienia, po której konto użytkownika zostanie zablokowane.



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

Uwaga

Kliknij Reset aby zresetować wskazanie licznika.



Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*

9.2 Grupy (RBAC)

Grupy zapewniają dodatkową warstwę kontroli dostępu do zasobów. Administratorzy mogą tworzyć grupy użytkowników, aby precyzyjniej zarządzać dostępem do zasobów i zapewnić, że tylko upoważnieni użytkownicy mają dostęp do określonych sejfów. Funkcja ta zwiększa zarówno bezpieczeństwo, jak i elastyczność w zarządzaniu dostępem do danych wrażliwych.

Grupy obsługują integrację z zewnętrznymi systemami wykorzystującymi model kontroli dostępu opartej na rolach (RBAC). Umożliwia to mapowanie konkretnych ról z zewnętrznych katalogów, takich jak Active Directory, do grup w Fudo Enterprise oraz przypisywanie do nich

określonych ról. Użytkownicy automatycznie dziedziczą uprawnienia i dostęp do zasobów na podstawie przypisanej im roli, co zapewnia spójne i scentralizowane zarządzanie dostępem.

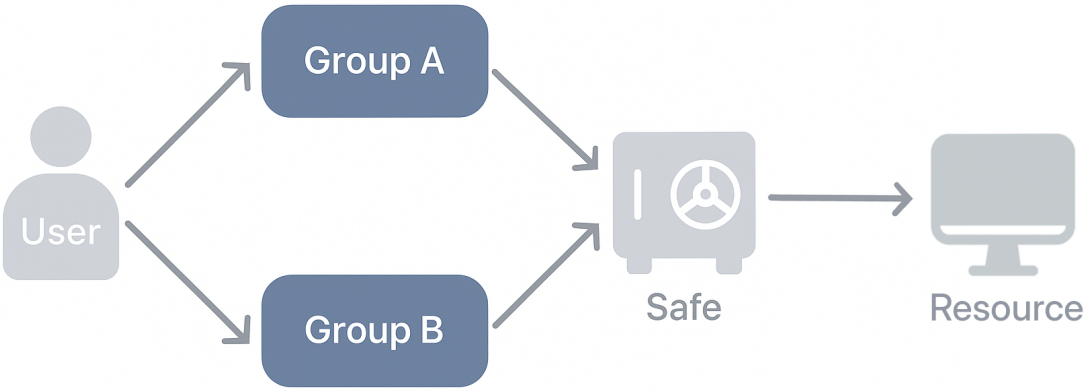
Uwaga

Grupy użytkowników mogą być przypisywane do sejfów, aby zdefiniować, którzy użytkownicy mają dostęp do określonych zasobów. Możliwe jest także przypisanie do sejfu pojedynczych użytkowników. Oznacza to, że dostęp do sejfów można przyznać zarówno grupom użytkowników, jak i indywidualnym osobom, co daje dużą elastyczność w konfiguracji kontroli dostępu.

9.2.1 Rozstrzyganie dostępu i priorytetyzacja

Gdy użytkownik ma dostęp do tego samego zasobu przez wiele sejfów lub przypisań grupowych, Fudo Enterprise ustala ścieżkę dostępu na podstawie zdefiniowanego priorytetu i zestawu reguł. Zapewnia to przewidywalne i bezpieczne zachowanie dostępu w złożonych scenariuszach uprawnień.

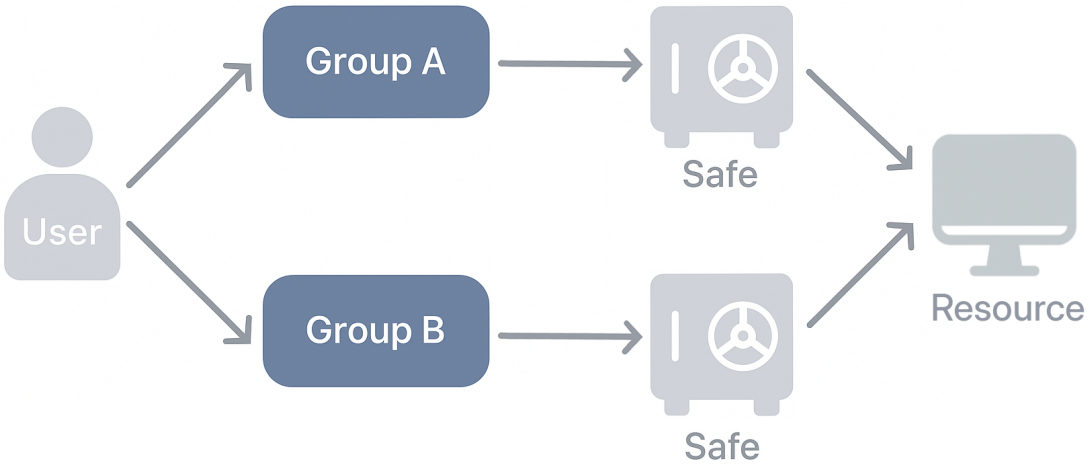
Użytkownik należy do wielu grup przypisanych do tego samego sejfu i zasobu



Jeśli użytkownik należy do dwóch lub więcej grup przypisanych do tego samego sejfu i zasobu, obowiązują następujące reguły:

- **Podgląd hasła:** Jeśli w co najmniej jednej grupie włączono opcję podglądu hasła, użytkownik będzie mógł zobaczyć hasło dla całego sejfu.
- **Okres dostępu:** Jeśli ramy czasowe ważności są skonfigurowane dla obu grup, Fudo Enterprise sprawdza, czy bieżący czas mieści się w dozwolonym zakresie dla każdej z grup. Jeśli warunek jest spełniony w co najmniej jednej grupie, sesja jest dozwolona.
- **Polityka dostępu dziennego:** Jeśli dla użytkownika włączono politykę czasową, Fudo Enterprise ocenia polityki czasowe wszystkich powiązanych grup. Jeśli użytkownik znajduje się w dozwolonym przedziale czasowym w dowolnej grupie, dostęp jest przyznawany.

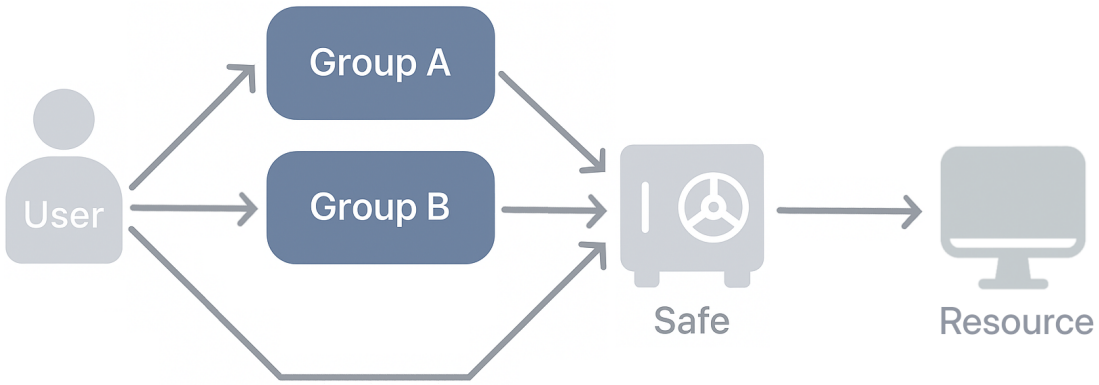
Użytkownik należy do wielu grup przypisanych do różnych sejfów z tym samym zasobem



Jeśli użytkownik ma dostęp do tego samego zasobu poprzez wiele sejfów za pośrednictwem różnych grup, rozstrzyganie odbywa się według następującej logiki:

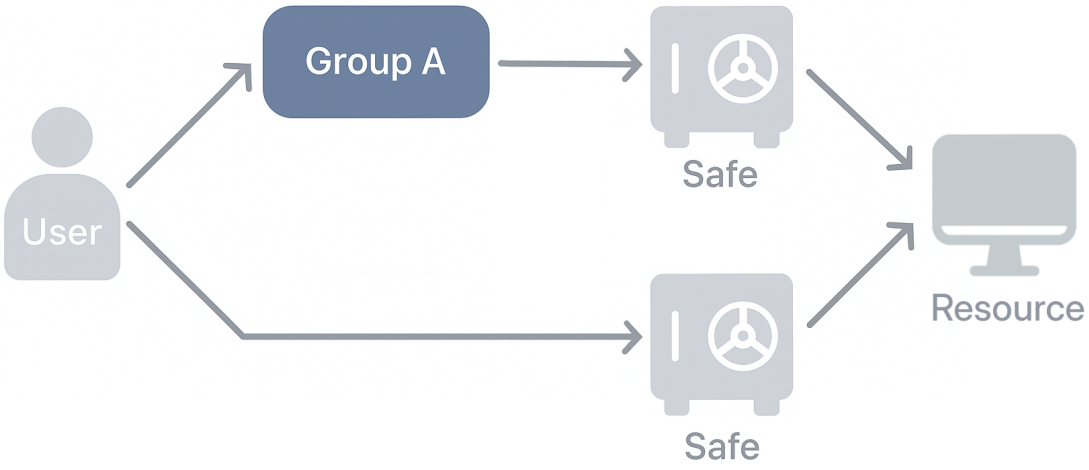
- **Okres dostępu:** Jeśli bieżący czas mieści się w zakresie ważności Grupy A, zostaje ona użyta. W przeciwnym razie oceniana jest Grupa B. Jeśli żadna z grup nie ma ograniczeń czasowych, system wybiera pierwszą grupę alfabetycznie.
- **Polityka dostępu dziennego:** Jeśli obie grupy mają włączoną politykę czasową, Fudo Enterprise sprawdza, która grupa zezwala na dostęp w danym momencie. Dostęp przyznawany jest na podstawie pierwszej grupy w porządku alfabetycznym, której polityka obejmuje bieżący czas lub która nie ma skonfigurowanej polityki.

Użytkownik ma zarówno bezpośredni, jak i grupowy dostęp do tego samego sejfu i zasobu



Jeśli użytkownik ma przypisanie bezpośrednie do sejfu oraz dostęp grupowy do tego samego sejfu i zasobu, **priorytet ma dostęp bezpośredni.** Wszystkie ustawienia, takie jak *Zablokowany, Podgląd hasła, Okres dostępu, Polityka dostępu dziennego* są pobierane z przypisania użytkownik–sejf i mają pierwszeństwo przed ustawieniami grupowymi.

Użytkownik ma dostęp do tego samego zasobu przez bezpośrednie przypisanie do sejfu oraz przez grupę przypisaną do innego sejfu

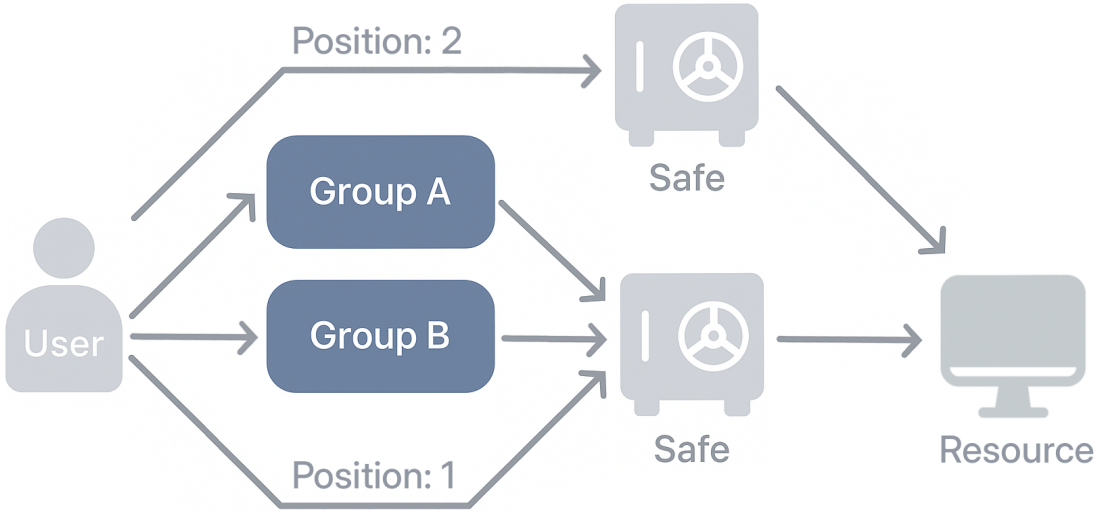


W przypadku, gdy użytkownik ma dostęp do tego samego zasobu:

- bezpośrednio przez przypisanie do sejfu oraz
- pośrednio przez grupę przypisaną do innego sejfu,

Fudo Enterprise **zawsze wybiera połączenie bezpośrednie.** Ocena pomija przypisania grupowe i korzysta z bezpośredniego przypisania sejfu do kontroli dostępu.

Użytkownik ma dostęp do tego samego zasobu przez dwa sejfy o różnych pozycjach



W tym scenariuszu użytkownik ma dostęp do tego samego zasobu przez dwa różne sejfy. Jeden sejf ma przypisaną pozycję 1, a drugi pozycję 2.

Ponieważ wartości pozycji określają preferencje, system **zawsze użyje sejfu o wyższej wartości pozycji** — w tym przypadku sejfu z pozycją 1.

Uwaga

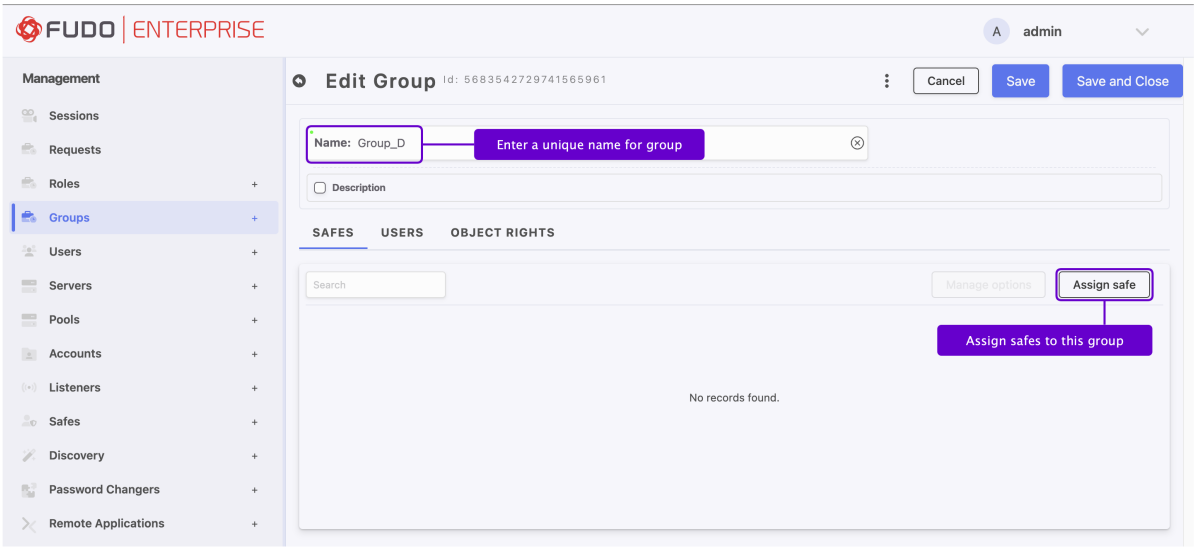
- Najpierw Fudo Enterprise sprawdza, czy użytkownik ma **bezpośrednie przypisanie do sejfów.** Jeśli tak, przypisania grupowe są całkowicie ignorowane.
- Następnie, spośród wszystkich dostępnych połączeń bezpośrednich, Fudo Enterprise **ocenia atrybut pozycji** i wybiera sejf z najwyższą wartością pozycji.

Zobacz także:

- *Tworzenie grupy*
- *Dodawanie sejfu*
- *Użytkownicy*

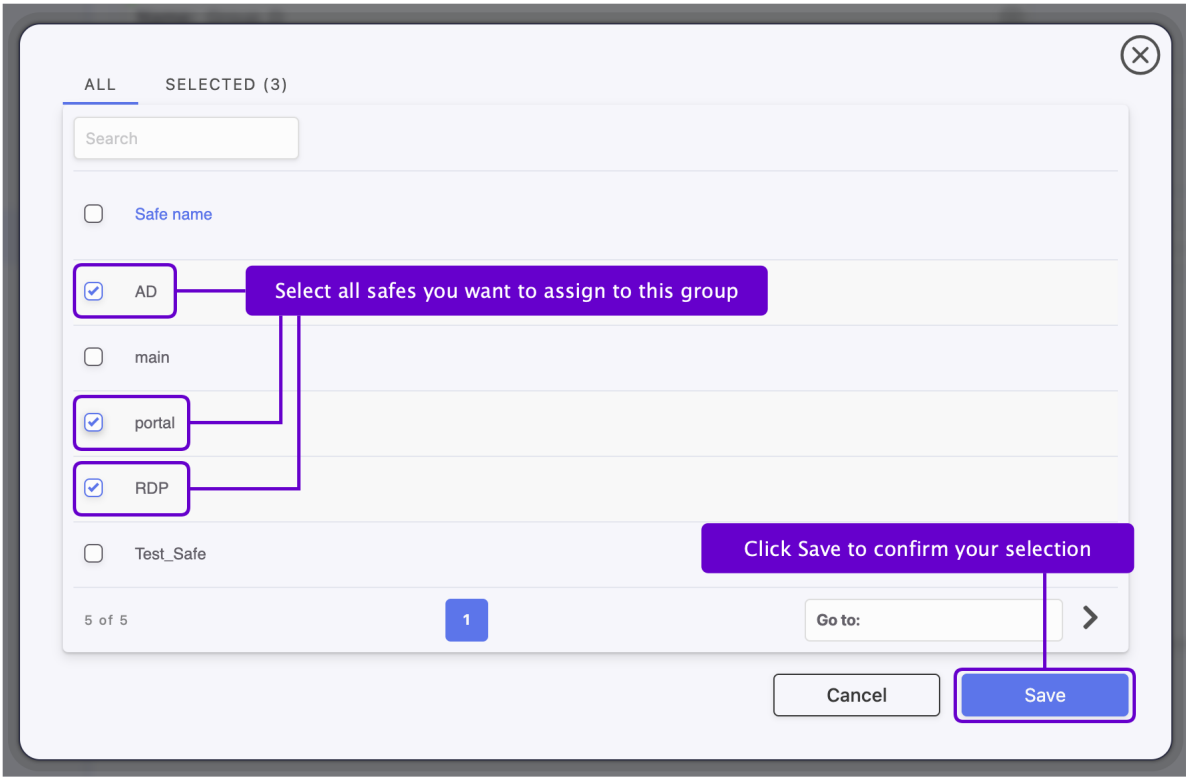
9.2.2 Tworzenie grupy

1. Kliknij ikonę + w menu głównym obok zakładki *Grupy*, lub wybierz *Zarządzanie* > *Grupy*, a następnie kliknij + *Dodaj grupę*.
2. Wprowadź unikalną nazwę dla nowego obiektu.
3. W razie potrzeby zaznacz opcję *Opis*, aby dodać podsumowanie grupy.
4. Kliknij *Zapisz*, aby utworzyć grupę i przejść do dalszej konfiguracji.



ZAKŁADKA SEJFY

5. Przejdź do zakładki **SEJFY** i kliknij *Przypisz sejf*.
6. Zaznacz wszystkie sejfy, które chcesz przypisać do tej grupy, a następnie kliknij *Zapisz*.



Uwaga

W systemie znajdują się dwa domyślne sejfy:

- `main` – zapewnia dostęp do Panelu administratora.
- `portal` – zapewnia dostęp do Bramy dostępu użytkownika.

POLITYKA DOSTĘPU DZIENNEGO

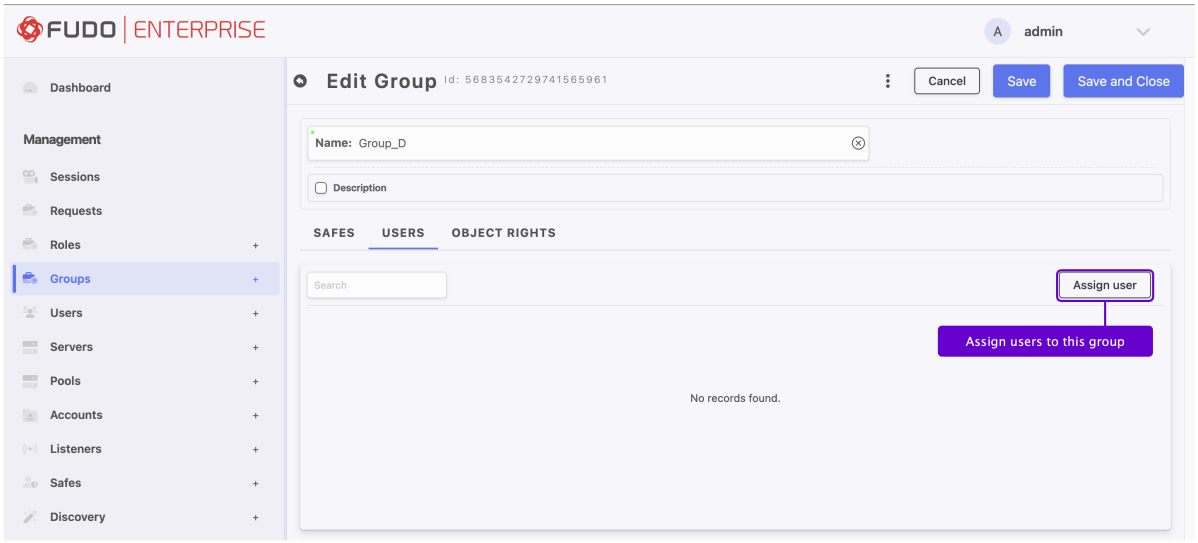
Po przypisaniu sejfów można włączyć i zdefiniować przedziały czasowe, w których użytkownik będzie mógł łączyć się z serwerami.

7. Wybierz odpowiedni sejf i kliknij *Zarządzaj opcjami*.
8. W widoku kalendarza tygodniowego kliknij pole odpowiadające wybranemu dniu tygodnia i godzinie, w której chcesz przyznać dostęp do sejfu.
9. Kliknij zaznaczone pole, aby zmodyfikować ramy czasowe, jeśli chcesz zmienić czas trwania dostępu.
10. Kliknij *Zapisz*, aby zamknąć okno modalne.

ZAKŁADKA UŻYTKOWNICY

W tej zakładce możesz określić, którzy użytkownicy będą należeć do tej grupy.

11. Przejdź do zakładki **UŻYTKOWNICY** i kliknij *Przypisz użytkownika*.
12. Zaznacz wszystkich użytkowników, których chcesz przypisać do tej grupy i kliknij *Zapisz*.

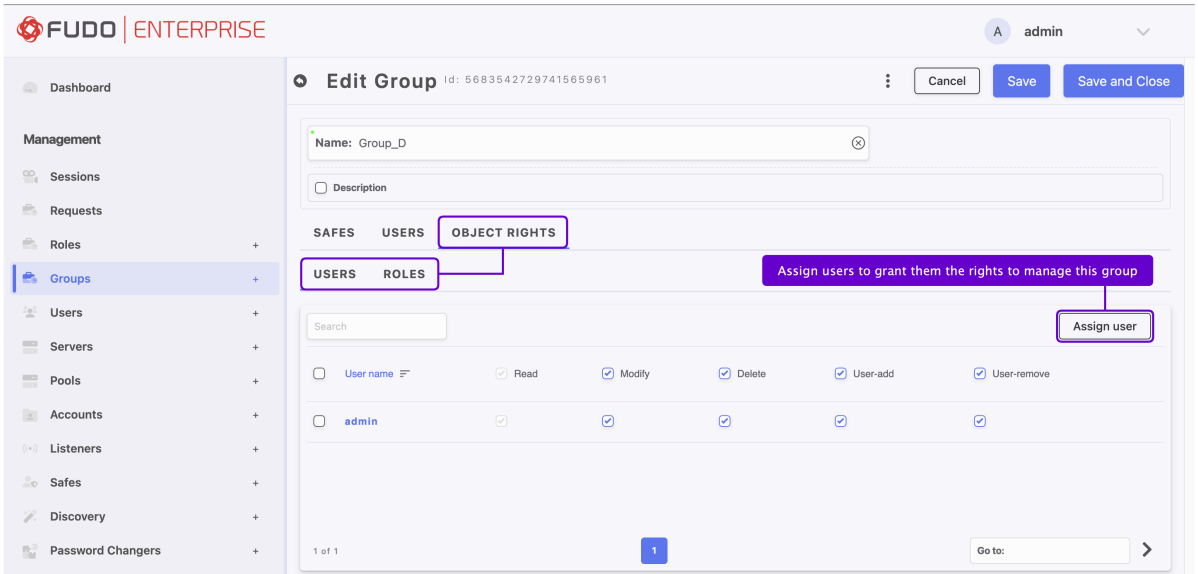


ZAKŁADKA UPRAWNIENIA DO OBIEKTU

W tej zakładce możesz określić, którzy użytkownicy i które role będą miały uprawnienia do zarządzania tą grupą.

Ostrzeżenie

Zwróć uwagę na obecność podzakładki **UŻYTKOWNICY** wewnątrz zakładki **UPRAWNIENIA DO OBIEKTU**. Ta podzakładka służy do przydzielania uprawnień do zarządzania grupą wybranym użytkownikom — **nie** służy do przypisywania użytkowników do grupy.



11. Przejdź do podzakładki **UŻYTKOWNICY** i kliknij *Przypisz użytkownika*.
12. Zaznacz użytkowników, którym chcesz nadać uprawnienia do zarządzania tą grupą, i kliknij *Zapisz*.
13. Przejdź do podzakładki **ROLE** i kliknij *Przypisz rolę*.
14. Zaznacz role, którym chcesz nadać uprawnienia do zarządzania tą grupą, i kliknij *Zapisz*.

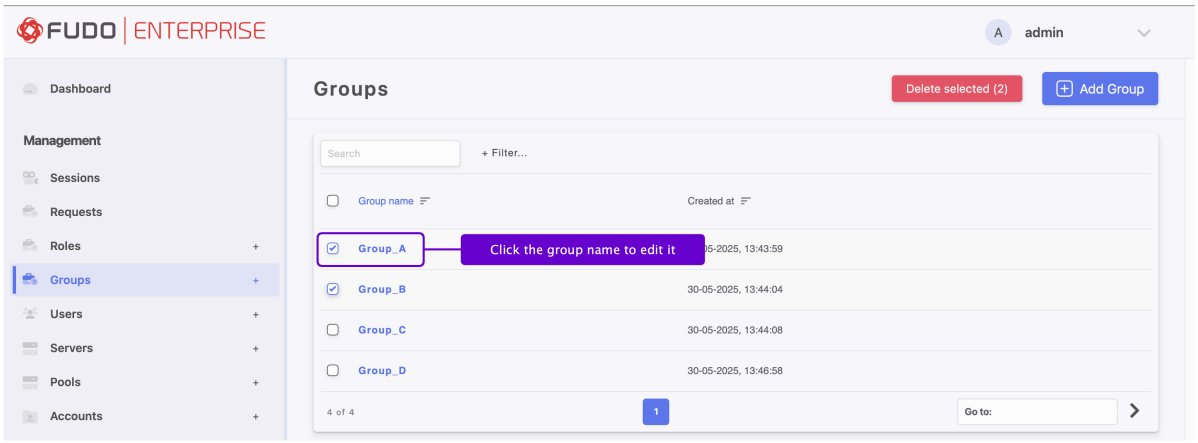
15. Kliknij *Zapisz i zamknij*, aby zapisać utworzoną grupę.

Zobacz także:

- *Grupy (RBAC)*
- *Użytkownicy*

9.2.3 Modyfikowanie grup

1. Wybierz *Zarządzanie* > *Grupy*.
2. Ustaw filtry, aby ograniczyć liczbę wyświetlanych obiektów na liście, lub skorzystaj z paska wyszukiwania.
3. Znajdź i kliknij nazwę wybranej grupy, aby przejść do jej edycji.
4. Wprowadź potrzebne zmiany w konfiguracji.



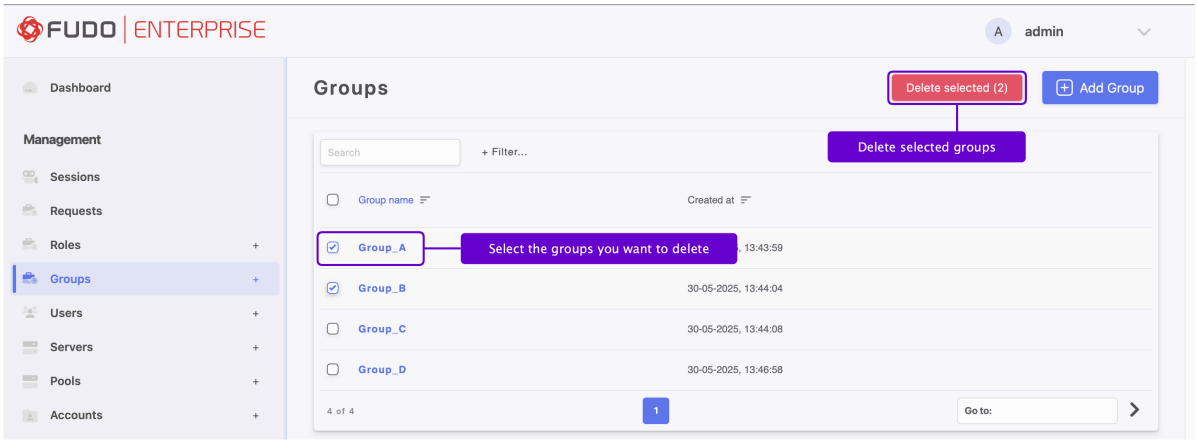
5. Kliknij *Zapisz i zamknij*, aby zapisać zmiany w konfiguracji.

Zobacz także:

- *Kontrola dostępu oparta na rolach (RBAC)*
- *Grupy (RBAC)*
- *Użytkownicy*

9.2.4 Usuwanie grup

1. Wybierz *Zarządzanie* > *Grupy*.
2. Ustaw filtry, aby ograniczyć liczbę wyświetlanych obiektów na liście, lub skorzystaj z paska wyszukiwania.
3. Znajdź i zaznacz pole wyboru obok nazwy wybranej grupy, aby ją zaznaczyć.
4. Kliknij *Usuń zaznaczone*.



5. Alternatywnie możesz edytować grupę bezpośrednio z listy, kliknąć ikonę trzech pionowych kropek i wybrać *Usuń grupę*.

Zobacz także:

- *Grupy (RBAC)*
- *Użytkownicy*

9.3 Kontrola dostępu oparta na rolach (RBAC)

Role implementują mechanizm kontroli dostępu opartego na rolach (RBAC), zapewniając szczegółową i elastyczną kontrolę nad uprawnieniami użytkowników.

Funkcjonalność **RBAC (Role-Based Access Control)** w Fudo Enterprise umożliwia administratorom systemu definiowanie precyzyjnych ról z określonymi uprawnieniami dostępu do obiektów i operacji. Dzięki temu można tworzyć role przeznaczone do wykonywania konkretnych zadań, na przykład rolę uprawniającą wyłącznie do zarządzania użytkownikami – obejmującą tworzenie, edytowanie i usuwanie – bez wpływu na inne obszary systemu.

Podobnie można konfigurować role z uprawnieniami do zarządzania innymi obiektami, takimi jak gniazda nasłuchiwania, pule, serwery czy sejfy. Administratorzy mogą określać uprawnienia ról dla konkretnych akcji, takich jak tworzenie, modyfikacja, eksportowanie, usuwanie czy blokowanie tych obiektów.

Mechanizm zarządzania dostępem obsługuje zarówno uprawnienia globalne, jak i selektywne. Oznacza to, że użytkownik może uzyskać dostęp do przeglądania, modyfikowania lub usuwania wszystkich obiektów danego typu (np. użytkowników, kont, serwerów) lub tylko wybranych, określonych obiektów. Taka elastyczność zapewnia dostosowanie uprawnień do wymagań bezpieczeństwa organizacji.

Uwaga

W celu zachowania kompatybilności ze starszymi wersjami dodano sześć domyślnych ról: *superadmin, admin, safes admin, operator, auditor i session viewer*. Role te można również modyfikować.

9.3.1 Przejście na RBAC po aktualizacji

Wraz z wprowadzeniem kontroli dostępu opartej na rolach (RBAC), system zawiera zestaw predefiniowanych ról zaprojektowanych tak, aby ułatwić przejście z poprzedniego modelu uprawnień. Role te są automatycznie mapowane na podstawie wcześniejszej konfiguracji, co pozwala zachować podstawową strukturę dostępu i zminimalizować zakłócenia podczas aktualizacji.

Rola *superadmin* jest stała i nie można jej modyfikować ani usuwać. Wszystkie pozostałe role predefiniowane — takie jak *admin*, *operator*, *session viewer*, *safes admin* i *auditor* — można modyfikować lub rozszerzać według potrzeb. Elastyczność ta pozwala organizacjom stopniowo dostosowywać model dostępu do wewnętrznych polityk bezpieczeństwa.

Ostrzeżenie

- Po aktualizacji administratorzy powinni przejrzeć i dostosować predefiniowane role, aby upewnić się, że odpowiadają one wymaganiom ich organizacji. Dostosowanie ról jest kluczowe, by w pełni wykorzystać możliwości kontroli i szczegółowości oferowane przez RBAC.
- W przypadku aktualizacji systemu do wersji opartej na zdolnościach (capabilities), konieczne jest odwzorowanie wszystkich obiektów, do których użytkownicy mieli przydzielone zdolności / uprawnienia.
- Automatyczne mapowanie ról z poprzedniego systemu odbywa się jednorazowo i wyłącznie w trakcie aktualizacji z wersji bez RBAC. Role predefiniowane nie mają odwzorowywać poprzednich uprawnień jeden do jednego — mają być punktem wyjścia do dalszych zmian.
- Po zmodyfikowaniu lub usunięciu roli predefiniowanej zmiana ta jest trwała — nie istnieje mechanizm przywracania jej pierwotnej wersji. W przypadku potrzeby przywrócenia domyślnej konfiguracji należy skontaktować się z pomocą techniczną Fudo Enterprise.

9.3.1.1 Zrozumienie uprawnień i zdolności

Odczyt

Uprawnienie `*-read` zapewnia dostęp do danej zakładki w interfejsie, a co za tym idzie — do wszystkich obiektów danego typu w systemie, niezależnie od posiadanych zdolności. Jest to dostęp tylko do podglądu — bez możliwości edycji, usuwania czy wykonywania innych działań.

Przykład:

Użytkownik z uprawnieniem `user-read` może otworzyć zakładkę Użytkownicy i zobaczyć pełną listę kont, w tym kont, których nie utworzył i do których nie ma zdolności. Nie może jednak ich modyfikować, blokować ani usuwać — chyba że ma do tego dodatkowe zdolności lub przywileje.

Tworzenie

Uprawnienia zakończone sufiksem `*-create` pozwalają użytkownikowi tworzyć nowe obiekty danego typu. Przykładowo, `user-create` umożliwia tworzenie nowych użytkowników. System automatycznie przyznaje twórcy wszystkie dostępne zdolności do stworzonego obiektu, co oznacza pełną możliwość jego zarządzania.

Przykład:

Jeśli administrator ma uprawnienie `user-create` i utworzy nowego użytkownika, automatycznie otrzymuje zdolności do:

- modyfikowania ustawień użytkownika,
- blokowania i odblokowywania konta,
- usuwania użytkownika.

W takim przypadku administrator nie potrzebuje osobnych uprawnień, takich jak `user-block` czy `user-delete` — przyznane zdolności są wystarczające.

Usuwanie

Przyznanie roli uprawnienia z grupy `*-delete` (np. `server-delete`) pozwala na usuwanie dowolnych obiektów danego typu — niezależnie od tego, kto je utworzył. W interfejsie może być nadal wymagany dostęp do odpowiedniej zakładki, ale przez API można usuwać dowolne obiekty, jeśli uprawnienie `*-delete` jest obecne. W wielu przypadkach uprawnienie `*-read` nie jest wymagane do takich operacji przez API.

Ostrzeżenie

To może stanowić potencjalne zagrożenie bezpieczeństwa: przyznanie `*-delete` może nieumyślnie zwiększyć poziom dostępu roli. Zalecenia:

- Preferuj przydzielanie uprawnień `*-create`, jeśli rola ma zarządzać tylko obiektami, które sama utworzyła.
- Używaj `*-delete` tylko dla ról, które mają mieć pełną kontrolę nad wszystkimi obiektami danego typu.

Podczas migracji z wersji 5.5 należy dokładnie przeanalizować uprawnienia ról, aby uniknąć niezamierzonego rozszerzenia ich uprawnień.

9.3.1.2 Predefiniowane role jako punkt wyjścia

System zawiera zestaw predefiniowanych ról wspierających zgodność wsteczną i strukturę dostępu sprzed wprowadzenia RBAC:

- **Superadmin** – Ma nieograniczony dostęp do wszystkich funkcji i ustawień systemu. Może tworzyć role niestandardowe z dowolnymi dostępnymi uprawnieniami.
- **Operator** – Ma uprawnienia zbliżone do wcześniejszej roli `operator` sprzed wprowadzenia RBAC. Rola ta jest automatycznie mapowana na podstawie wcześniejszej konfiguracji. Wybrane przykładowe uprawnienia:
  - Może przeglądać listę sesji i ich szczegóły, ale tylko dla sesji powiązanych z obiektami, do których ma przypisane zdolności.
  - Może odtwarzać sesje zarchiwizowane i na żywo, ograniczone do obiektów, do których ma dostęp.
  - **Nie może** tworzyć nowych obiektów.
  - Może blokować tylko obiekty, do których ma przypisane zdolności.
  - **Widzi tylko** obiekty, do których ma zdolności, ale **może podglądać** wszystkie role i grupy.

  - Rola **operator** domyślnie zawiera uprawnienie *listener-read*. W wyniku zmian w RBAC operatorzy widzą obecnie wszystkich listenerów, nawet tych nieprzypisanych.
  - Może podglądać modyfikatory haseł, weryfikatory i polityki haseł.
  - Może podglądać aplikacje zdalne.
  - **Nie może** podglądać polityk ani wyrażeń regularnych.
  - Może zarządzać powiadomieniami i je przeglądać dla użytkowników, do których ma przypisane zdolności.
  - Może widzieć stopkę Panelu administratora.
  - **Nie może** udostępniać sesji do dołączenia ani ich usuwać.
  - Może przeglądać i głosować w oczekujących, aktywnych i zarchiwizowanych żądaniach powiązanych z obiektami, do których ma dostęp (użytkownik wnioskujący, konto, sejf, serwer/pula).
  - Może generować raporty z zakładki Sesje.
  - Może zarządzać subskrypcjami raportów.
  - Może ręcznie dodać subskrypcję do *Raportu systemowego*, ale tylko dla obiektów, do których ma zdolności (użytkownicy nie widzą raportów innych użytkowników).
  - Ma dostęp do zakładki **Uwierzytelnianie**, co umożliwia administratorom przeglądanie i przypisywanie metod uwierzytelniania zewnętrznego.
  - Ma dostęp do zakładki **Zewnętrzne repozytoria haseł**, aby przypisywać repozytoria do kont.
  - Ma dostęp do zakładki **Cluster**, aby przekazywać sesje do innych węzłów.
  - **Nie ma** dostępu do pozostałych podzakładek zakładki **Ustawienia**.
- **Admin** – Posiada uprawnienia zbliżone do wcześniejszej roli `admin` sprzed wprowadzenia RBAC. Rola ta jest automatycznie mapowana na podstawie wcześniejszej konfiguracji. Wybrane przykładowe uprawnienia:
  - Ma dostęp do Dashboardu i jego widżetów, zależnie od przypisanych zdolności.
  - Może tworzyć nowe obiekty, takie jak użytkownicy, grupy, serwery, konta, pule i sejfy. Twórca automatycznie otrzymuje pełne zdolności do utworzonych obiektów.
  - Może zarządzać użytkownikami, grupami, serwerami, kontami, pulami i sejfami **do których ma przypisane zdolności.**
  - **Nie może** tworzyć listenerów.
  - **Może** tworzyć użytkowników i podglądać przypisane im role, ale **nie może** przypisywać ról (wymagane uprawnienie `role-modify`).
  - Może zarządzać powiadomieniami i je przeglądać dla użytkowników, do których ma przypisane zdolności.
  - Może widzieć stopkę Panelu administratora oraz uzyskać dostęp do Menu użytkownika w prawym górnym rogu.
  - Może przeglądać i odtwarzać sesje powiązane z dostępnymi obiektami, zarządzać retencją, usuwać sesje w swoim zakresie, korzystać z funkcji zawartych w uprawnieniu

session-modify (*Uprawnienia do zakładki Sesje*), a także kodować, udostępniać, komentować, kończyć, eksportować i dołączać do sesji.

- Może przeglądać i głosować w oczekujących, aktywnych i zarchiwizowanych żądaniach powiązanych z obiektami, do których ma dostęp.
- Może tworzyć i zarządzać modyfikatorami haseł, weryfikatorami i politykami haseł.
- Może tworzyć i zarządzać aplikacjami zdalnymi.
- Może tworzyć i zarządzać politykami oraz podglądać wyrażenia regularne.
- Może generować raporty z zakładki Sesje.
- Może zarządzać subskrypcjami raportów.
- Może ręcznie dodać subskrypcję do *Raportu systemowego*, ale tylko dla obiektów, do których ma zdolności.
- Ma dostęp do zakładki **Uwierzytelnianie**, co umożliwia przypisywanie metod uwierzytelniania zewnętrznego.
- Ma dostęp do zakładki **Zewnętrzne repozytoria haseł**, aby przypisywać repozytoria do kont.
- Ma dostęp do zakładki **Cluster**, aby przekazywać sesje do innych węzłów.
- **Nie ma** dostępu do pozostałych podzakładek zakładki **Ustawienia**.

- **Session Viewer** – Ma uprawnienia zbliżone do wcześniejszej roli `session viewer` sprzed wprowadzenia RBAC. Rola ta jest automatycznie mapowana na podstawie wcześniejszej konfiguracji. Wybrane przykładowe uprawnienia:
  - Może przeglądać listę sesji i ich szczegóły, ograniczone do sesji powiązanych z obiektami, do których ma uprawnienia.
  - Może odtwarzać sesje zarchiwizowane i na żywo, ograniczone do dostępnych obiektów (zobacz również: *Uprawnienia do zakładki Sesje*).
  - Może dołączać do sesji, kończyć je, komentować oraz kodować, jeśli ma dostęp do odpowiednich obiektów.
  - Ma dostęp do stopki Panelu administratora.
  - **Nie może** modyfikować konfiguracji związanej z sesjami (np. retencji, ustawień kodowania itp.).
  - Ma dostęp do zakładki **Pliki** i może pobierać dostępne pliki powiązane z sesjami, do których ma uprawnienia.
- **Safes Admin** – Posiada uprawnienia zbliżone do roli `admin`, z wyjątkiem dostępu do modyfikatorów haseł i polityk haseł. Dodatkowo nie ma dostępu do konfiguracji klastra ani widgetów. Wybrane przykładowe uprawnienia:
  - Nowo utworzony użytkownik z tą rolą nie zobaczy żadnych obiektów, dopóki nie zostaną mu jawnie przypisane zdolności do istniejących obiektów.
  - Ma dostęp do Dashboardu i jego widżetów, w zależności od przypisanych zdolności.
  - Może tworzyć nowe obiekty, takie jak użytkownicy, grupy, serwery, konta, pule i sejfy. Twórca otrzymuje pełne uprawnienia do utworzonych obiektów.
  - Może podglądać wszystkie role, grupy, użytkowników i konta.

  - Może zarządzać użytkownikami, grupami, serwerami, kontami, pulami i sejfami **do których ma przypisane zdolności.**
  - **Nie może** tworzyć listenerów.
  - **Może** tworzyć użytkowników i podglądać przypisane im role, ale **nie może** przypisywać ról użytkownikom (wymagane uprawnienie `role-modify`).
  - Może przeglądać i zarządzać powiadomieniami użytkowników, do których ma przypisane zdolności.
  - Ma dostęp do stopki Panelu administratora oraz Menu użytkownika w prawym górnym rogu.
  - Może przeglądać i odtwarzać sesje powiązane z dostępem, zarządzać retencją, usuwać sesje w swoim zakresie, korzystać z funkcji uprawnienia session-modify (*Uprawnienia do zakładki Sesje*), kodować, udostępniać, komentować, kończyć, eksportować i dołączać do sesji.
  - Może przeglądać i głosować w oczekujących, aktywnych i zarchiwizowanych żądaniach dotyczących obiektów, do których ma dostęp.
  - Może podglądać modyfikatory haseł, weryfikatory i polityki haseł.
  - Może tworzyć i zarządzać aplikacjami zdalnymi.
  - Może podglądać polityki i wyrażenia regularne.
  - Może generować raporty z zakładki Sesje.
  - Może zarządzać subskrypcjami raportów.
  - Może ręcznie zapisać się na *Raport systemowy*, ale dostęp będzie ograniczony do obiektów, do których ma zdolności (użytkownicy nie widzą raportów innych).
  - Ma dostęp do zakładki **Uwierzytelnianie**, aby przypisywać metody uwierzytelniania zewnętrznego użytkownikom.
  - Ma dostęp do zakładki **Zewnętrzne repozytoria haseł**, aby przypisywać je kontom.
  - Ma dostęp do zakładki **Cluster**, aby przesyłać sesje do innych węzłów.
  - **Nie ma** dostępu do pozostałych podzakładek zakładki **Ustawienia**.
- **Auditor** – Rola tylko do odczytu z wglądem we wszystkie obszary systemu. Pod względem zakresu zbliżona do roli `superadmin`, ale bez możliwości edycji istniejących obiektów ani tworzenia nowych.

Należy pamiętać, że istnieją wyjątki i mapowanie nie zawsze odwzorowuje wcześniejsze role jeden do jednego. Wybrane przykłady:

- Po aktualizacji **administrator** posiadający przypisane zdolności do obiektu automatycznie otrzymuje pełne uprawnienia do tego obiektu.
- Ponieważ listenery są traktowane jako globalna i sieciowa konfiguracja, po aktualizacji do wersji 5.6 użytkownicy **admin** nie mają już uprawnień do ich tworzenia.
- Role **admin**, **safes admin** i **operator** zawierają domyślnie uprawnienie *extauth-read*, by móc przypisywać metody uwierzytelniania zewnętrznego użytkownikom.
- Role **admin**, **safes admin** i **operator** zawierają domyślnie uprawnienie *passvn-read*, by móc przypisywać zewnętrzne repozytoria haseł kontom.

- Role **admin**, **safes admin** i **operator** zawierają domyślnie uprawnienie *cluster-read*, by móc przesyłać sesje do innych węzłów.
- Rola **operator** zawiera domyślnie *listener-read*. W wyniku zmian RBAC operatorzy obecnie widzą wszystkich listenerów, nie tylko tych jawnie przypisanych.
- Zmiana modelu dostępu do listenerów – użytkownik ma albo dostęp do wszystkich listenerów, albo do żadnego. Nie można już przypisywać dostępu do pojedynczych listenerów.
- Można ręcznie dodać subskrypcję tego typu raportu, ale będzie ona ograniczona do obiektów, do których użytkownik ma zdolności.
- Mają dostęp do następujących widżetów dashboardu: sesje równoczesne, podejrzane sesje, wykres sesji równoczesnych, widżet „Aktywni użytkownicy" oraz „Alerty dotyczące kont".
- Mają teraz dostęp do zakładki *Pobieranie* > *Pliki* i mogą pobierać tam wymienione pliki. Uprawnienie to jest wymagane do prawidłowego wyświetlania sesji SFTP/SCP.
- Rola session viewer ma teraz dostęp do dodatkowych elementów interfejsu, w tym nowych zakładek oraz możliwość dodania widżetu Aktywni użytkownicy z marketplace'u widżetów. Odzwierciedla to rozszerzone uprawnienia w nowej macierzy dostępu.

Uwaga

- Rola **superadmin** jest chroniona i nie można jej modyfikować ani usuwać. Dotyczy to:
  - Edycji jej uprawnień i zdolności,
  - Zmiany nazwy lub dezaktywacji roli,
  - Całkowitego usunięcia roli.
- Ograniczenie to gwarantuje, że system zawsze będzie miał przynajmniej jedną rolę z nieograniczonym dostępem administracyjnym.
- System wymusza, aby **przynajmniej jeden użytkownik** zawsze miał przypisaną rolę superadmin.

Ostrzeżenie

- Predefiniowana rola **user** została usunięta z systemu. Po aktualizacji do wersji 5.6 wszyscy użytkownicy, którzy mieli tę rolę, nie będą mieli przypisanej żadnej roli.
- Predefiniowana rola **service** została usunięta z systemu.
  - Przed aktualizacją klienci, którzy mieli przypisanych wielu użytkowników do roli service, muszą usunąć wszystkich poza jednym.
  - Ustawienia SNMP skonfigurowane wcześniej dla tego użytkownika zostaną przeniesione do zakładki System i zastosowane globalnie.

Zobacz także:

- *Kontrola dostępu oparta na rolach (RBAC)*
- *Grupy (RBAC)*
- *Użytkownicy*

9.3.2 Tworzenie roli

Uwaga

Użytkownik może tworzyć lub przypisywać tylko takie role, które zawierają uprawnienia będące w jego własnym zakresie. Aby zdefiniować rolę z określonymi uprawnieniami, użytkownik musi posiadać odpowiednie prawa do zarządzania tymi uprawnieniami.

1. Kliknij ikonę + w menu głównym obok zakładki *Role* lub wybierz *Zarządzanie* > *Role*, a następnie kliknij + *Dodaj rolę*.
2. Wpisz unikalną nazwę dla nowego obiektu.
3. Zaznacz opcję *Opis*, aby dodać podsumowanie roli (opcjonalne).

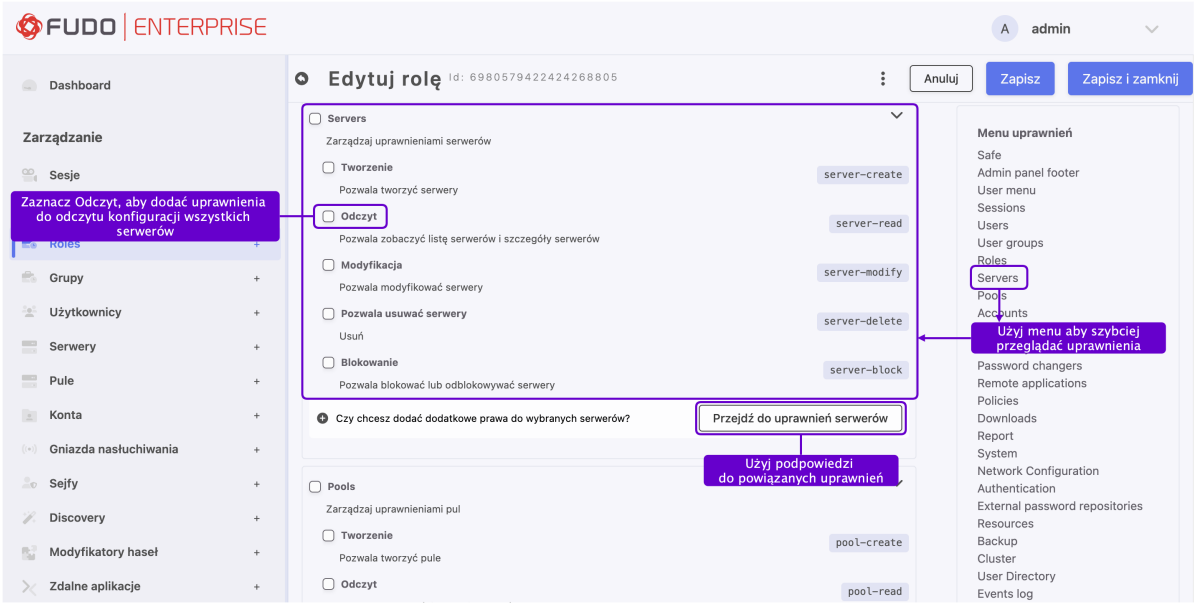
ZAKŁADKA GLOBALNE UPRAWNIENIA

4. Przejdź do zakładki **UPRAWNIENIA GLOBALNE** i zaznacz wszystkie uprawnienia, które chcesz przypisać do tworzonej roli.

Uwaga

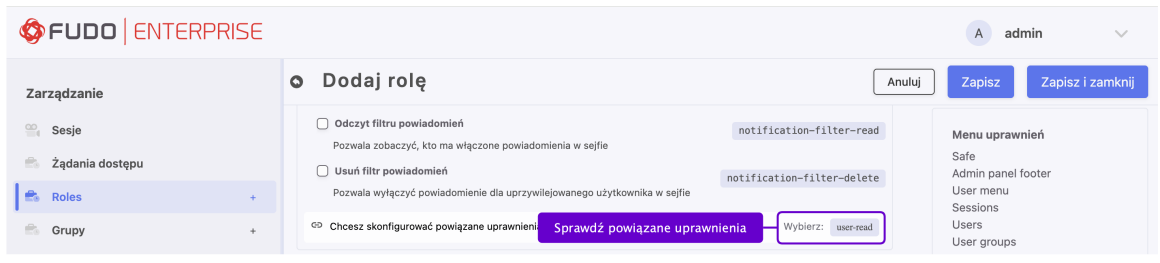
Zaznaczenie wszystkich uprawnień spowoduje przypisanie tej roli pełnego zestawu uprawnień, podobnie jak w przypadku roli *superadmin* w poprzednich wersjach.

5. Przejdź do panelu **Menu uprawnień** i kliknij **Serwery**, aby szybko przejść do sekcji uprawnień dotyczących *Serwerów*.
6. W sekcji **Serwery** zaznacz opcję *Odczyt* (umożliwi to przeglądanie konfiguracji wszystkich serwerów).



Uwaga

Możesz skorzystać ze wskazówek dodanych na końcu każdej sekcji uprawnień, aby przypisać dodatkowe uprawnienia związane z tym typem obiektu, zapewniając pełną operacyjność roli.



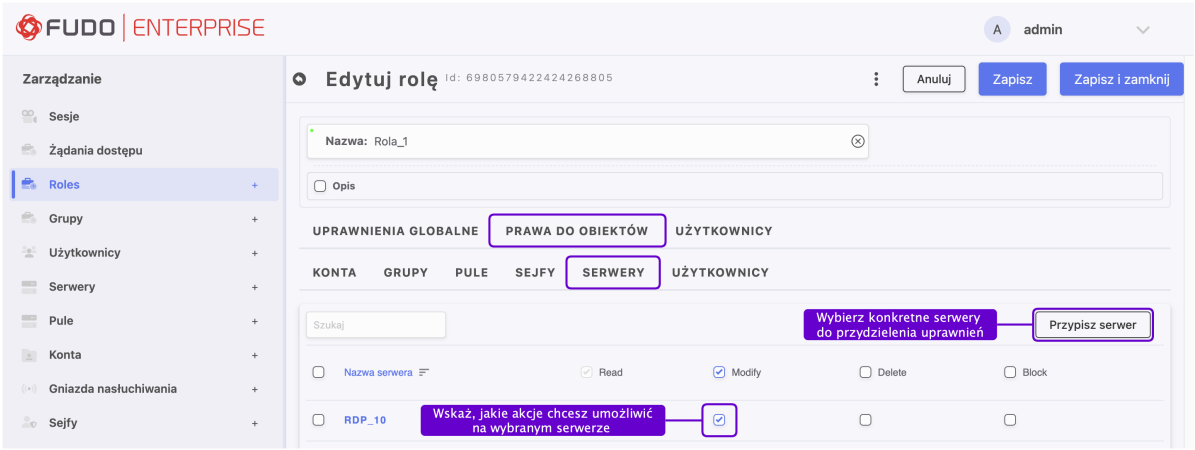
7. Kliknij *Zapisz*, aby utworzyć rolę i przejść do dalszej konfiguracji.
8. Aby dodać dodatkowe uprawnienia do wybranych obiektów, użyj przycisku *Przejdź do...* lub przejdź do zakładki **PRAWA DO OBIEKTÓW**.

ZAKŁADKA PRAWA DO OBIEKTÓW

Uwaga

W zakładce **PRAWA DO OBIEKTÓW** możesz przypisać uprawnienia do pojedynczych obiektów następujących typów: konta, grupy, pule, sejfy, serwery i użytkownicy.

9. Wybierz odpowiednią zakładkę, aby przypisać uprawnienia do określonego obiektu (np. **SERWERY**).
10. Kliknij *Przypisz serwer*.
11. W oknie dialogowym **Uprawnienia do zarządzania serwerami** wybierz z listy serwer, któremu chcesz przypisać uprawnienia.
12. Kliknij *Zapisz*.
13. Następnie wybierz akcje, które będą możliwe do wykonania na wybranym serwerze (np. *Modyfikuj*).



14. Po wykonaniu powyższych kroków utworzysz rolę z uprawnieniami do przeglądania konfiguracji wszystkich serwerów oraz modyfikowania tylko tych serwerów, które zostały wybrane w zakładce **PRAWA DO OBIEKTÓW**.

Ostrzeżenie

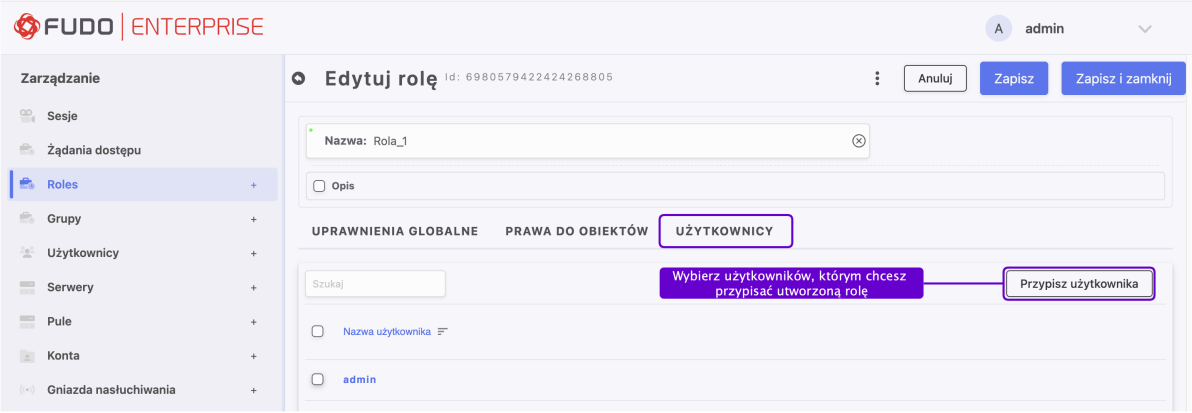
Zwróć uwagę na istnienie zakładki **UŻYTKOWNICY** w obrębie zakładki **UPRAWNIENIA DO OBIEKTÓW**. Ta zakładka odpowiada za przydzielanie możliwości modyfikowania wybranych użytkowników (jako obiektów), a nie za przydzielanie im ról.

ZAKŁADKA UŻYTKOWNICY

Uwaga

W zakładce **UŻYTKOWNICY** możesz przypisać utworzoną rolę użytkownikom, nadając im wszystkie wybrane uprawnienia.

15. Przejdź do zakładki **UŻYTKOWNICY**.
16. Kliknij *Przypisz użytkownika*.
17. Wybierz użytkowników, którym chcesz przypisać utworzoną rolę.



18. Kliknij *Zapisz*.

Powiązane tematy:

- *Typowe scenariusze ról i wymagane uprawnienia*
- *Grupy (RBAC)*
- *Użytkownicy*

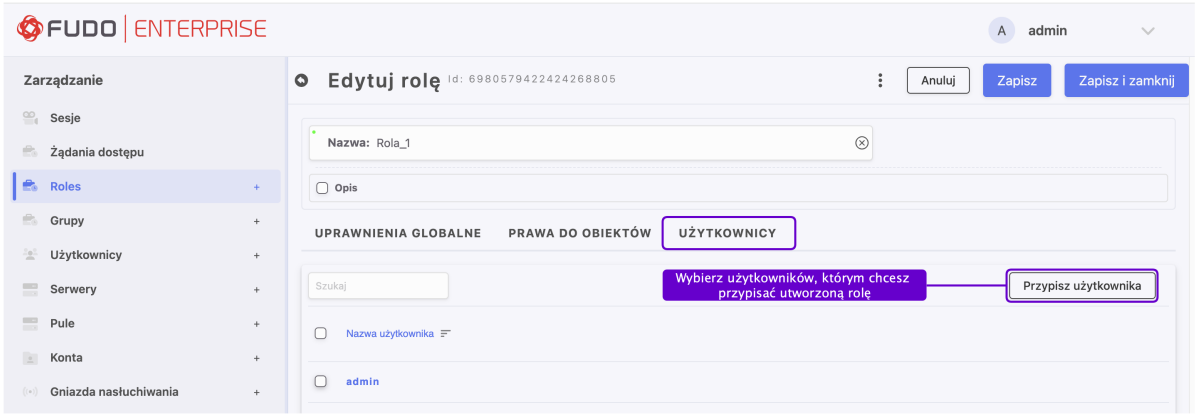
9.3.3 Przypisywanie ról do użytkowników

Możesz przypisać rolę do użytkownika zarówno z poziomu edycji roli, jak i z poziomu edycji użytkownika.

Przypisywanie roli z poziomu edycji roli

1. Wybierz *Zarządzanie* > *Role*.
2. Zdefiniuj filtry, aby ograniczyć liczbę wyświetlanych obiektów na liście lub skorzystaj z paska wyszukiwania.
3. Znajdź i kliknij nazwę żądanej roli, aby ją edytować.
4. Przejdź do zakładki **UŻYTKOWNICY**.

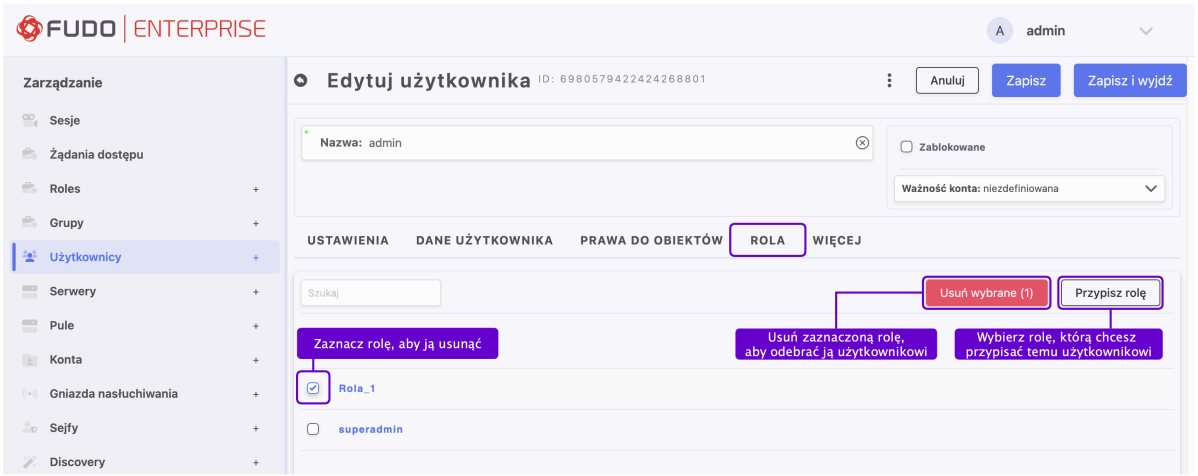
5. Kliknij *Przypisz użytkownika*.
6. Wybierz użytkowników, którym chcesz przypisać utworzoną rolę.



7. Kliknij *Zapisz*.

Przypisywanie roli z poziomu edycji użytkownika

1. Wybierz *Zarządzanie* > *Użytkownicy*.
2. Zdefiniuj filtry, aby ograniczyć liczbę wyświetlanych obiektów na liście.
3. Znajdź i kliknij nazwę żądanego użytkownika, aby przejść do jego konfiguracji.
4. Przejdź do zakładki **ROLA**.
5. Kliknij *Przypisz rolę* i wybierz żądaną rolę z listy.
6. Kliknij *Zapisz*, aby zamknąć okno modalne.
7. Kliknij *Zapisz i zamknij*, aby zapisać zmiany w konfiguracji użytkownika.

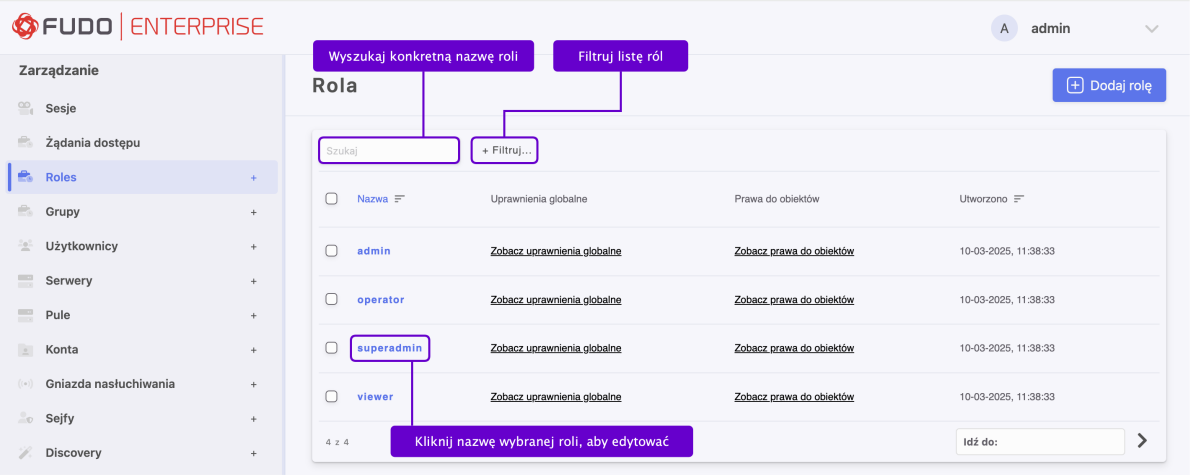


Powiązane tematy:

- *Kontrola dostępu oparta na rolach (RBAC)*
- *Grupy (RBAC)*
- *Użytkownicy*

9.3.4 Modyfikowanie ról

1. Wybierz *Zarządzanie* > *Role*.
2. Zdefiniuj filtry, aby ograniczyć liczbę wyświetlanych obiektów na liście, lub skorzystaj z paska wyszukiwania.
3. Znajdź i kliknij nazwę żądanej roli, aby ją edytować.
4. Zmodyfikuj parametry konfiguracji zgodnie z potrzebami.



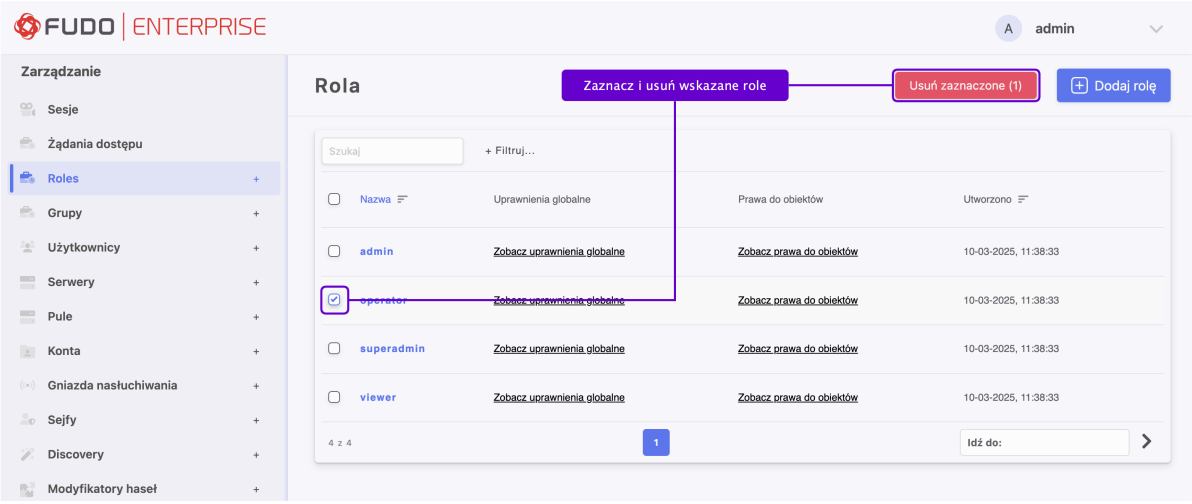
5. Kliknij *Zapisz i zamknij*, aby zapisać zmiany w tej konfiguracji.

Powiązane tematy:

- *Kontrola dostępu oparta na rolach (RBAC)*
- *Grupy (RBAC)*
- *Użytkownicy*

9.3.5 Usuwanie ról

1. Wybierz *Zarządzanie* > *Role*.
2. Zdefiniuj filtry, aby ograniczyć liczbę wyświetlanych obiektów na liście, lub skorzystaj z paska wyszukiwania.
3. Znajdź i kliknij pole wyboru obok nazwy żądanej roli, aby ją zaznaczyć.
4. Kliknij *Usuń zaznaczone*.



5. Alternatywnie, możesz edytować rolę przeznaczoną do usunięcia bezpośrednio z listy, klikając ikonę trzech pionowych kropek i wybrać *Usuń rolę*.

Ostrzeżenie

Usunięcie roli przypisanej do użytkowników lub grup spowoduje natychmiastowe odebranie im wszystkich uprawnień i praw dostępu do obiektów nadanych za pośrednictwem tej roli.

Powiązane tematy:

- *Kontrola dostępu oparta na rolach (RBAC)*
- *Grupy (RBAC)*
- *Użytkownicy*

9.3.6 Typowe scenariusze ról i wymagane uprawnienia

9.3.6.1 Macierz kontroli dostępu na poziomie zakładek

Ta sekcja zawiera szczegółowy przegląd uprawnień i/lub zdolności wymaganych do uzyskania dostępu i wykonywania operacji w poszczególnych częściach interfejsu użytkownika Fudo Enterprise.

Każda tabela odpowiada jednej z głównych zakładek w systemie. W zależności od złożoności zakładki, tabela może zawierać:

- **Podsekcja**: zagnieżdżony komponent lub funkcja w zakładce (np. „Ogólne > Data i czas" w zakładce System).
- **Akcja**: konkretna operacja (np. *widoczna*, *tworzenie*, *konfiguracja*) kontrolowana przez prawa dostępu.
- **Uprawnienia**: wymagane przywileje, które umożliwiają użytkownikowi wykonanie danej akcji.
- **Zdolności**: jeśli dotyczy, wymienione są dodatkowe wymagania dotyczące zdolności. W przypadku ich braku, kolumna zawiera *Brak*.

Kontrola dostępu w systemie jest egzekwowana na podstawie przypisanych ról użytkownika, które z kolei nadają odpowiednie przywileje i zdolności.

Uwaga

- Przydzielone zdolności do konkretnych obiektów mogą powodować wyświetlanie się zakładek w interfejsie, nawet jeśli użytkownik nie ma odpowiednich uprawnień do wykonywania jakichkolwiek operacji w tych zakładkach.
- Niektóre zaawansowane zakładki, jak Sejfy, wymagają więcej niż tylko własnych przywilejów (np. `safe-read`, `safe-create`). Aby w pełni utworzyć lub zarządzać sejfem, użytkownik musi mieć także uprawnienia do podglądu i wyboru zasobów powiązanych – takich jak konta, serwery, pule lub grupy – które są częścią konfiguracji sejfu.

Tabela 1: Macierz uprawnień/zdolności: zakładka Dashboard

Akcja	Uprawnienia	Zdolności
read	`dashboard`	Brak

Tabela 2: Macierz uprawnień/zdolności: zakładka Sesje

Akcja	Uprawnienia	Zdolności
read	`session-read`	Brak
backup	`session-backup`	Brak
delete	`session-delete`	Brak
download	`session-file-download`, `session-movie-download`	Brak
encode	`session-encode`	Brak
retention	`session-modify`	Brak

Tabela 3: Macierz uprawnień/zdolności: zakładka Żądania

Akcja	Uprawnienia	Zdolności
read	`access-request-read`	Brak

Tabela 4: Macierz uprawnień/zdolności: zakładka Role

Akcja	Uprawnienia	Zdolności
read	`role-read`	Brak
create	`role-create`	Brak
modify	`role-modify`	Brak
delete	`role-delete`	Brak

Tabela 5: Macierz uprawnień/zdolności: zakładka Użytkownicy

Akcja	Uprawnienia	Zdolności
read	`user-create`, `user-read`	`user`
create	`user-create`	Brak

Tabela 6: Macierz uprawnień/zdolności: zakładka Grupy

Akcja	Uprawnienia	Zdolności
read	`group-create`, `group-read`	`group`
create	`group-create`	Brak

Tabela 7: Macierz uprawnień/zdolności: zakładka Serwery

Akcja	Uprawnienia	Zdolności
read	`server-create`, `server-read`	`server`
create	`server-create`	Brak

Tabela 8: Macierz uprawnień/zdolności: zakładka Pule

Akcja	Uprawnienia	Zdolności
read	`pool-create`, `pool-read`	`pool`
create	`pool-create`	Brak

Tabela 9: Macierz uprawnień/zdolności: zakładka Konta

Akcja	Uprawnienia	Zdolności
read	`account-create`, `account-read`	`account`
create	`account-create`	Brak

Tabela 10: Macierz uprawnień/zdolności: zakładka Listenery

Akcja	Uprawnienia	Zdolności
read	`listener-create`, `listener-read`	Brak
create	`listener-create`	Brak
modify	`listener-modify`	Brak
delete	`listener-delete`	Brak

Tabela 11: Macierz uprawnień/zdolności: zakładka Sejfy

Podsekcja	Akcja	Uprawnienia	Zdolności
Sejfy			
	read	`safe-create`, `safe-read`	`safe`
	create	`safe-create`	Brak
Powiadomienia			
	read	`notification-filter-read`, `notification-filter-create`	Brak
	create	`notification-filter-create`	Brak
	delete	`notification-filter-delete`	Brak

Tabela 12: Macierz uprawnień/zdolności: zakładka Discovery

Podsekcja	Akcja	Uprawnienia	Zdolności
Skanery			
	read	`scanner-read`	Brak
	create	`scanner-create`	Brak
	modify	`scanner-modify`	Brak
	delete	`scanner-delete`	Brak
	start	`scanner-start`	Brak
Reguły			
	read	`discovery-rule-read`	Brak
	create	`discovery-rule-create`	Brak
	modify	`discovery-rule-modify`	Brak
	delete	`discovery-rule-delete`	Brak

Tabela 13: Macierz uprawnień/zdolności: zakładka Modyfikatory haseł

Podsekcja	Akcja	Uprawnienia	Zdolności
Modyfikator haseł			
	read	`password-changer-read`	Brak
	create	`password-changer-create`	Brak
	modify	`password-changer-modify`	Brak
	delete	`password-changer-delete`	Brak
Polityka haseł			
	read	`password-change-policy-read`	Brak
	create	`password-change-policy-create`	Brak
	modify	`password-change-policy-modify`	Brak
	delete	`password-change-policy-delete`	Brak

Tabela 14: Macierz uprawnień/zdolności: zakładka Aplikacje zdalne

Akcja	Uprawnienia	Zdolności
read	`remoteapp-read`	Brak
create	`remoteapp-create`	Brak
modify	`remoteapp-modify`	Brak
delete	`remoteapp-delete`	Brak

Tabela 15: Macierz uprawnień/zdolności: zakładka Polityki

Podsekcja	Akcja	Uprawnienia	Zdolności
Polityka			
	read	`policy-read`	Brak
	create	`policy-create`	Brak
	modify	`policy-modify`	Brak
	delete	`policy-delete`	Brak
Wyrażenia regularne			
	read	`regexp-read`	Brak
	create	`regexp-create`	Brak
	modify	`regexp-modify`	Brak
	delete	`regexp-delete`	Brak

Tabela 16: Macierz uprawnień/zdolności: zakładka Do pobrania

Podsekcja	Akcja	Uprawnienia	Zdolności
Pliki			
	read	`session-file-read`	Brak
	download	`session-file-download`	Brak
	delete	`session-file-delete`	Brak
Nagrania			
	read	`session-movie-read`	Brak
	download	`session-movie-download`	Brak
	delete	`session-movie-delete`	Brak

Tabela 17: Macierz uprawnień/zdolności: zakładka Raporty

Akcja	Uprawnienia	Zdolności
read	`report-read`	Brak
create	`report-create`	Brak
modify	`report-modify`	Brak
delete	`report-delete`	Brak

Tabela 18: Macierz uprawnień/zdolności: zakładka Produktywność

Akcja	Uprawnienia	Zdolności
read	`productivity-read`	Brak

Tabela 19: Macierz uprawnień/zdolności: zakładka System

Podsekcja	Akcja	Uprawnienia	Zdolności
Ogólne > Data i czas			
	read	`datetime-read`	Brak
	configure	`datetime-modify`	Brak
Ogólne > NTP			
	read	`ntp-read`	Brak
	configure	`ntp-modify`	Brak
Ogólne > Certyfikaty			
	read	`certificate-read`	Brak
Ogólne > Certyfikaty > Panel administracyjny			
	read	`certificate-read`	Brak
	configure	`certificate-mgmt`	Brak
Ogólne > Certyfikaty > Brama dostępu			
	read	`certificate-read`	Brak
	configure	`certificate-uag`	Brak
Ogólne > Certyfikaty > CA użytkownika			
	read	`certificate-read`	Brak
	configure	`certificate-client`	Brak
Ogólne > Nadzór konserwacyjny > Odrzuć nowe połączenia			
	read	`maintenance-read`	Brak
	configure	`deny-new-connections`	Brak
Ogólne > Nadzór konserwacyjny > Dostęp pomocy technicznej			
	read	`maintenance-read`	Brak
	configure	`tech-support-access`	Brak
Ogólne > Nadzór konserwacyjny > API healthcheck			

ciąg dalszy na następnej stronie

Tabela 19 – kontynuacja poprzedniej strony

Podsekcja	Akcja	Uprawnienia	Zdolności
	read	`maintenance-read`	Brak
	configure	`healthcheck-api`	Brak
Ogólne > Nadzór konserwacyjny > Callhome			
	read	`maintenance-read`	Brak
	configure	`callhome`	Brak
Ogólne > Klucz główny			
	read	`masterkey-read`	Brak
	eksport	`masterkey-export`	Brak
	invalidate	`masterkey-invalidate`	Brak
Ogólne > SNMP			
	read	`snmp-read`	Brak
	configure	`snmp-modify`	Brak
Ogólne > Podpis czasowy			
	read	`timestamp-read`	Brak
	configure	`timestamp-modify`	Brak
Ogólne > Węzły modyfikatorów haseł			
	read	`password-changer-node-read`	Brak
	configure	`password-changer-node-modify`	Brak
Ogólne > Discovery			
	read	`discovery-node-read`	Brak
	configure	`discovery-node-modify`	Brak
Ogólne > Funkcje wrażliwe			
	read	`sensitive-feature-read`	Brak
	configure	`sensitive-feature-modify`	Brak
Ogólne > HTTP Proxy			
	read	`http-proxy-read`	Brak
	configure	`http-proxy-modify`	Brak
Aktualizacja			
	read	`upgrade-read`	Brak

ciąg dalszy na następnej stronie

Tabela 19 – kontynuacja poprzedniej strony

Podsekcja	Akcja	Uprawnienia	Zdolności
	upload	`upgrade-upload`	Brak
	check	`upgrade-check`	Brak
	install	`upgrade-install`	Brak
	delete	`upgrade-delete`	Brak
	usuń migawkę	`upgrade-snapshot-delete`	Brak
Hotfix			
	read	`hotfix-read`	Brak
	upload	`hotfix-upload`	Brak
	install	`hotfix-install`	Brak
	delete	`hotfix-delete`	Brak
Licencja			
	read	`license-read`	Brak
	configure	`license-upload`	Brak
Diagnostyka			
	read	`diagnostic`	Brak
Konfiguracja > Eksport			
	read	`configuration-export`	Brak
Konfiguracja > Import			
	read	`configuration-import`	Brak
Konfiguracja > Dane serwisowe			
	read	`service-data`	Brak

Tabela 20: Macierz uprawnień/zdolności: zakładka Sieć

Podsekcja	Akcja	Uprawnienia	Zdolności
Interfejsy			
	read	`network-read`	Brak
	configure	`network-modify`	Brak
DNS			
	read	`network-read`	Brak
	configure	`network-modify`	Brak
Routing			
	read	`network-read`	Brak
	configure	`network-modify`	Brak
ARP			
	read	`network-read`	Brak
	configure	`network-modify`	Brak
Etykiety			
	read	`label-read`	Brak
	configure	`label-modify`	Brak

Tabela 21: Macierz uprawnień/zdolności: zakładka Zewnętrzne repozytoria

Akcja	Uprawnienia	Zdolności
read	`external-storage-read`	Brak
configure	`external-storage-modify`	Brak

Tabela 22: Macierz uprawnień/zdolności: zakładka Powiadomienia

Akcja	Uprawnienia	Zdolności
read	`smtp-read`	Brak
configure	`smtp-modify`	Brak

Tabela 23: Macierz uprawnień/zdolności: zakładka Sztuczna inteligencja

Akcja	Uprawnienia	Zdolności
read	`ai-read`	Brak
configure	`ai-modify`	Brak

Tabela 24: Macierz uprawnień/zdolności: zakładka Uwierzytelnianie

Podsekcja	Akcja	Uprawnienia	Zdolności
Zewnętrzne			
	read	`extauth-read`	Brak
	create	`extauth-create`	Brak
	modify	`extauth-modify`	Brak
	delete	`extauth-delete`	Brak
OpenID Connect			
	read	`oidc-read`	Brak
	create	`oidc-create`	Brak
	modify	`oidc-modify`	Brak
	delete	`oidc-delete`	Brak
Globalne			
	read	`authentication-read`	Brak
	configure	`authentication-modify`	Brak

Tabela 25: Macierz uprawnień/zdolności: zakładka Repozytoria haseł

Akcja	Uprawnienia	Zdolności
read	`passvn-read`	Brak
create	`passvn-create`	Brak
modify	`passvn-modify`	Brak
delete	`passvn-delete`	Brak

Tabela 26: Macierz uprawnień/zdolności: zakładka Zasoby

Podsekcja	Akcja	Uprawnienia	Zdolności
Protokoły			
	read	`logo-read`	Brak
	configure	`logo-modify`	Brak
Portal użytkownika			
	read	`logo-read`	Brak
	configure	`logo-modify`	Brak

Tabela 27: Macierz uprawnień/zdolności: zakładka Kopie zapasowe i retencja

Podsekcja	Akcja	Uprawnienia	Zdolności
Kopia zapasowa			
	read	`backup-read`	Brak
	create	`backup-create`	Brak
	modify	`backup-modify`	Brak
	delete	`backup-delete`	Brak
Retencja			
	read	`retention-read`	Brak
	configure	`retention-modify`	Brak

Tabela 28: Macierz uprawnień/zdolności: zakładka Cluster

Podsekcja	Akcja	Uprawnienia	Zdolności
Węzły			
	read	`cluster-read`	Brak
	create	`cluster-modify`	Brak
	modify	`cluster-modify`	Brak
	delete	`cluster-modify`	Brak
	cluster_cr	`cluster-modify`	Brak
	cluster_jo	`cluster-modify`	Brak
Grupy nadmiarowości			
	read	`cluster-read`	Brak
	create	`cluster-modify`	Brak
	modify	`cluster-modify`	Brak
	delete	`cluster-modify`	Brak
	failover	`cluster-failover`	Brak

Tabela 29: Macierz uprawnień/zdolności: zakładka Katalog użytkowników

Akcja	Uprawnienia	Zdolności
read	`user-directory-read`	Brak
create	`user-directory-create`	Brak
modify	`user-directory-modify`	Brak
delete	`user-directory-delete`	Brak

Tabela 30: Macierz uprawnień/zdolności: zakładka Logi zdarzeń

Akcja	Uprawnienia	Zdolności
read	`log-read`	Brak

Tabela 31: Macierz uprawnień/zdolności: zakładka Sieć Fudo

Akcja	Uprawnienia	Zdolności
read	`fudo-network`	Brak

9.3.6.2 Widoczność widżetów Dashboardu

Widoczność poszczególnych widżetów na Dashboardzie zależy od następujących uprawnień:

Tabela 32: Wymagane uprawnienia do wyświetlenia wszystkich widżetów Dashboardu

Uprawnienie	Opis	Powiązany widżet
`dashboard`	Dostęp do zakładki Dashboard	Zakładka Dashboard
`account-rea`	Podgląd listy kont i ich szczegółów	Alerty kont
`user-read`	Podgląd listy użytkowników i ich szczegółów	Aktywni użytkownicy
`session-rea`	Podgląd listy sesji i ich szczegółów	Podejrzane sesje, Nowe sesje, Sesje równoczesne
`configurati`	Podgląd zakładki Konfiguracja	Licencja
`log-read`	Podgląd logów zdarzeń	Logi
`cluster-rea`	Podgląd konfiguracji klastra	Węzeł

Jeśli użytkownik ma zdolność do jakiegokolwiek **użytkownika** lub **konta** oraz przywilej `dashboard`, zobaczy odpowiednio widżety **Aktywni użytkownicy** i **Alerty kont**.

> **Uwaga**
>
> Jeśli rola użytkownika zostanie zmieniona, niektóre widżety mogą zniknąć z pulpitu i trafić do Marketu widżetów. Aby je przywrócić, należy dodać je ręcznie z Marketu do Dashboardu.

9.3.6.3 Uprawnienia do zakładki Sesje

Aby wyświetlić i korzystać z zakładki **Sesje**, użytkownik musi posiadać następujące przywileje:

- `session-view`
- `session-read`

Dodatkowo, aby zobaczyć konkretną sesję na liście, użytkownik musi mieć **uprawnienia odczytu do wszystkich obiektów** powiązanych z tą sesją:

- użytkownika uczestniczącego w sesji,
- serwera docelowego,

- użytego konta,
- powiązanego sejfu (jeśli dotyczy).

Odtwarzanie i podgląd

Aby wyświetlić lub odtworzyć sesję, wymagane są następujące uprawnienia:

- `user-session-view`
- `session-view`
- `session-read`
- uprawnienie odczytu do wszystkich obiektów powiązanych (użytkownik, serwer, konto, sejf)

Kopia zapasowa sesji

Uprawnienie `session-backup` umożliwia przesłanie sesji do kopii zapasowej. Działanie to **nie** modyfikuje sesji, dlatego ma dedykowane przywileje.

Zarządzanie sesjami

Uprawnienie `session-modify` umożliwia wykonywanie zaawansowanych operacji na sesjach. Użytkownicy z tym przywilejem mogą wykonywać następujące czynności **dla sesji, do których mają dostęp**:

- przywracanie sesji z kopii zapasowej,
- pobieranie plików przesłanych przez SCP lub SFTP,
- zatwierdzanie lub odrzucanie sesji (jeśli sejf wymaga zatwierdzania),
- przesyłanie sesji do innych węzłów,
- cofanie udostępnienia sesji,
- modyfikowanie edytowalnych atrybutów sesji,
- modyfikowanie znaczników czasu sesji.

9.3.6.4 Uprawnienia do zakładki Pobieranie

Dostęp do zakładki **Pobieranie**, która pozwala użytkownikom na pobieranie plików powiązanych z sesjami (np. nagrania, przesłane pliki), jest kontrolowany przez następujące uprawnienia:

- `session-*`
- `session-file-*`
- `session-movie-*`

Jednak same te przywileje **nie zapewniają dostępu globalnego** do wszystkich sesji. Aby użytkownik mógł zobaczyć i pobrać pliki z konkretnej sesji, musi również mieć prawa dostępu do wszystkich obiektów powiązanych z tą sesją:

- użytkownika, który zainicjował sesję,
- docelowego serwera,

- użytego konta,
- sejfu, w którym te obiekty się znajdują.

Prawa te można nadać poprzez globalne uprawnienia lub przypisanie odpowiednich zdolności.

9.3.6.5 Zarządzanie sejfami

Uwaga

Aby zarządzać kontami w sejfach, użytkownik musi mieć co najmniej uprawnienie `listener-read`, niezależnie od posiadanych uprawnień do samych kont.

Aby utworzyć sejf, wymagane są następujące **minimalne** uprawnienia:

- `safe-read`
- `safe-create`
- `safe-user-add`
- `user-read`
- `account-read`
- `listener-read`

Dodatkowe wymagania dla konkretnych operacji:

- Aby przypisywać grupy do sejfu:
  - `group-read`
- Aby zarządzać powiadomieniami:
  - `notification-filter-read`
  - `notification-filter-create`
  - `notification-filter-delete`
- Aby przypisywać polityki:
  - `policy-read`

9.3.6.6 Uprawnienia do żądań dostępu

Aby głosować nad żądaniem dostępu, użytkownik musi spełniać następujące warunki:

- posiadać uprawnienie `access-request-read` – umożliwia dostęp do zakładki *Żądania*,
- posiadać uprawnienie `access-request-vote` – umożliwia oddanie głosu,
- mieć uprawnienia odczytu do powiązanych obiektów:
  - **Użytkownik** – użytkownik wnioskujący,
  - **Serwer/Pula** - do którego wnioskowany jest dostęp.
  - **Sejf** – zawierający żądane konto,
  - **Konto** – którego dotyczy żądanie.

Do uczestnictwa w procesie zatwierdzania wymagane są poprawne konfiguracje uprawnień i zdolności.

9.3.6.7 Fudo Officer

Aby sparować lub odłączyć aplikację mobilną Fudo Officer z kontem, użytkownik musi mieć dostęp do Panelu administratora i posiadać zdolność `modify` do własnego konta.

Aby aplikacja Fudo Officer działała w pełni, użytkownik musi posiadać następujące uprawnienia:

- `user-read`
- `server-read`
- `listener-read`
- `safe-read`
- `account-read`
- `access-request-vote`
- `access-request-read`

9.3.6.8 Uprawnienia do raportów

Uwaga

Tylko użytkownicy posiadający uprawnienia `report-read` oraz `system-report-read` mają dostęp do raportów systemowych, które są automatycznie generowane przez system. Takie raporty zawierają wszystkie dane z systemu, w tym dotyczące wszystkich obiektów.

`report-create`

- Gwarantuje, że raport zostanie wygenerowany i pojawi się w zakładce **Reports** → **Reports**.
- Umożliwia generowanie raportów z poziomu zakładki **Sessions**.

`report-read`

- Wymagane do przeglądania jakichkolwiek raportów.
- Użytkownicy nie mogą przeglądać raportów wygenerowanych przez innych użytkowników.
- Umożliwia przeglądanie raportów zgodnie z istniejącymi subskrypcjami, raportów historycznych oraz tych wygenerowanych z zakładki **Sessions**.

`report-modify`

- Umożliwia zarządzanie subskrypcjami raportów z poziomu zakładki **Reports** → **Settings**.
- Administrator może dodać subskrypcję na dowolny typ raportu.
- Dane w wygenerowanym raporcie są ograniczone do obiektów i informacji, do których użytkownik ma uprawnienia.

Uwaga

Dane zawarte w wygenerowanym raporcie są ograniczone do obiektów oraz innych informacji, do których użytkownik ma dostęp.

`report-delete`

- Użytkownicy mogą usuwać wyłącznie swoje własne raporty.

`system-report-read`

- Zapewnia dostęp do treści raportów systemowych, **niezależnie od przyznanych capabilities lub uprawnień**.
- Musi być połączone z uprawnieniem `report-read`, aby raporty systemowe oraz zakładka **Reports** były widoczne.
- To uprawnienie jest **przeznaczone wyłącznie** dla użytkowników z rolą `superadmin`.

Zobacz także:

- *Grupy (RBAC)*
- *Użytkownicy*

ROZDZIAŁ 10

Zarządzanie sesjami

10.1 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.

10.1.1 Dodawanie serwera

10.1.1.1 Dodawanie serwera HTTP

Uwaga

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

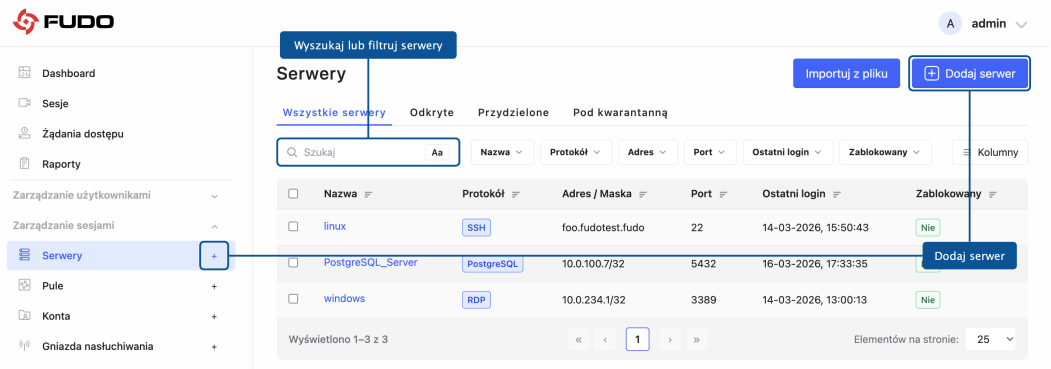
Ostrzeżenie

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

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

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

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



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `HTTP`.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

3. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
4. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
5. W polu *Host HTTP*, wprowadź nagłówek HTTP. Nagłówek HTTP wskazuje zasób na serwerze, na którym hostowanych jest wiele stron internetowych.
6. Wprowadź *Limit czasu HTTP* wyrażony w sekundach czas bezczynności, po upłynięciu którego, połączenie będzie wymagało ponownego uwierzytelnienia.
7. 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*.

Uwaga

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*.

8. Zaznacz opcję *Użyj SSH tunelu* i podaj *Klucz SSH tunelu*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

9. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.
10. Z listy rozwijanej *Adres sieci* wybierz adres IP, z którego inicjowane będą połączenia z monitorowanym serwerem.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

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

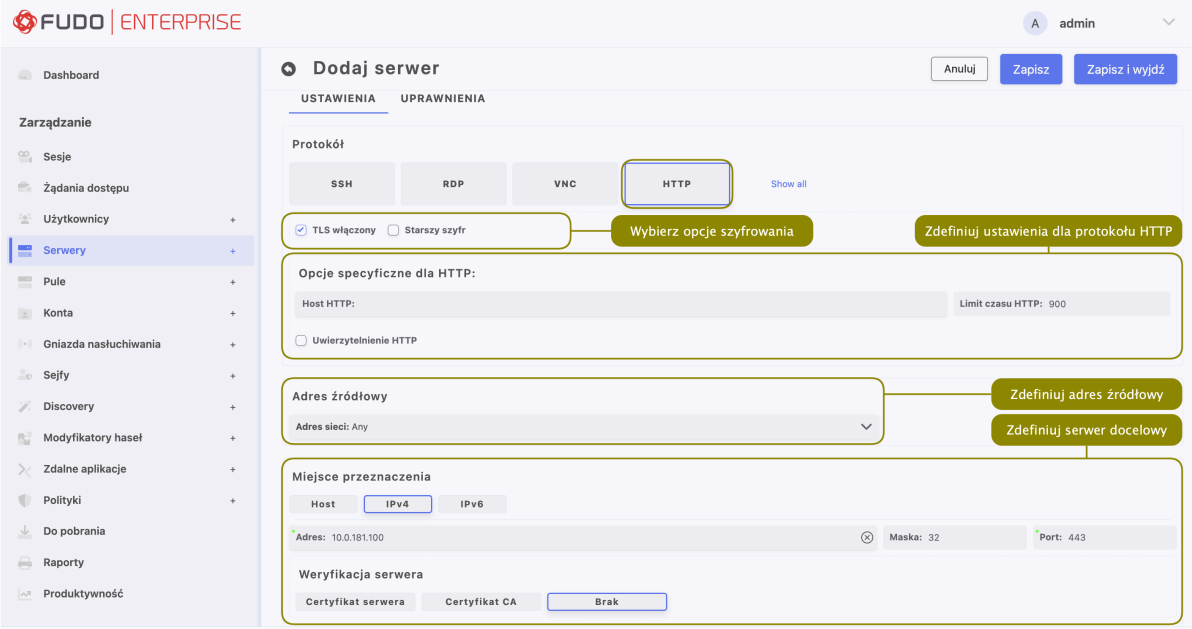
- Wybierz `Host`, `IPv4` albo `IPv6`,
- Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Uwaga

- 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*.

- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

- 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.

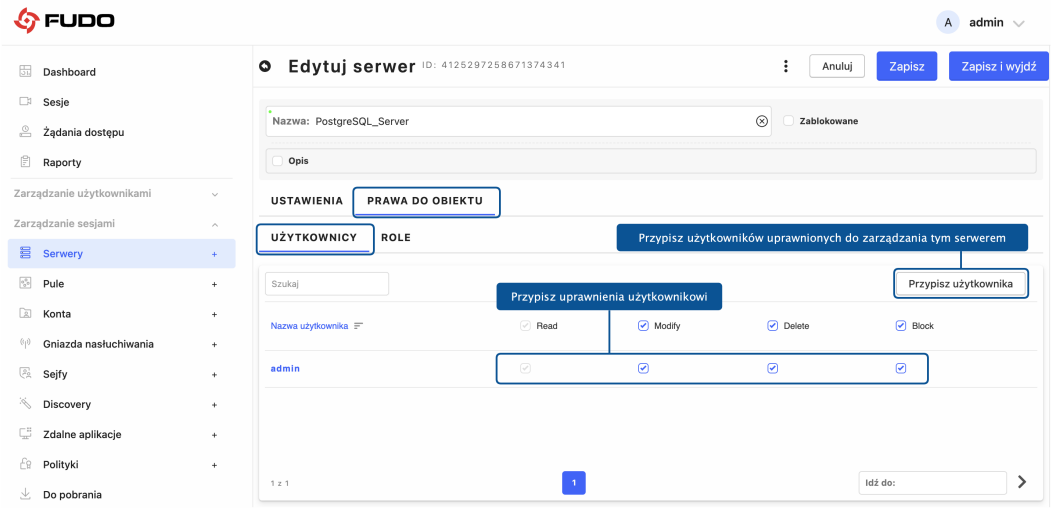


12. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

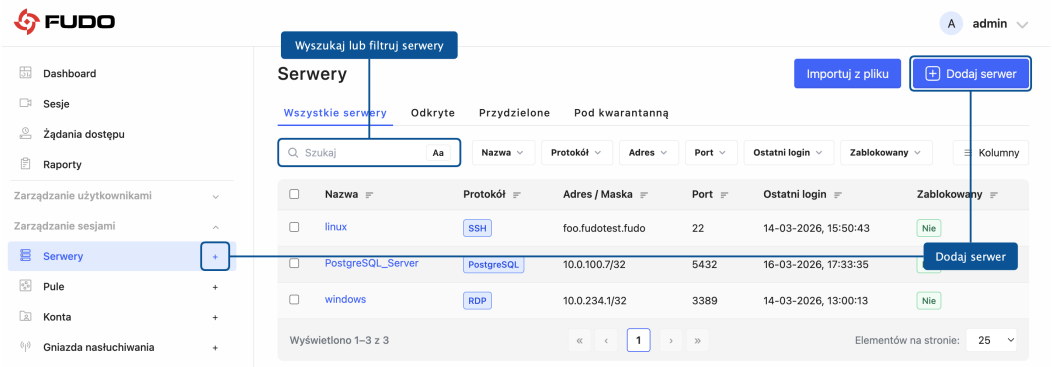
- *Pule*
- *Protokoły - HTTP*
- *Model danych*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

10.1.1.2 Dodawanie serwera Modbus

Uwaga

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

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



3. Wpisz unikalną nazwę serwera.

4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `Modbus`.
3. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

4. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

Uwaga

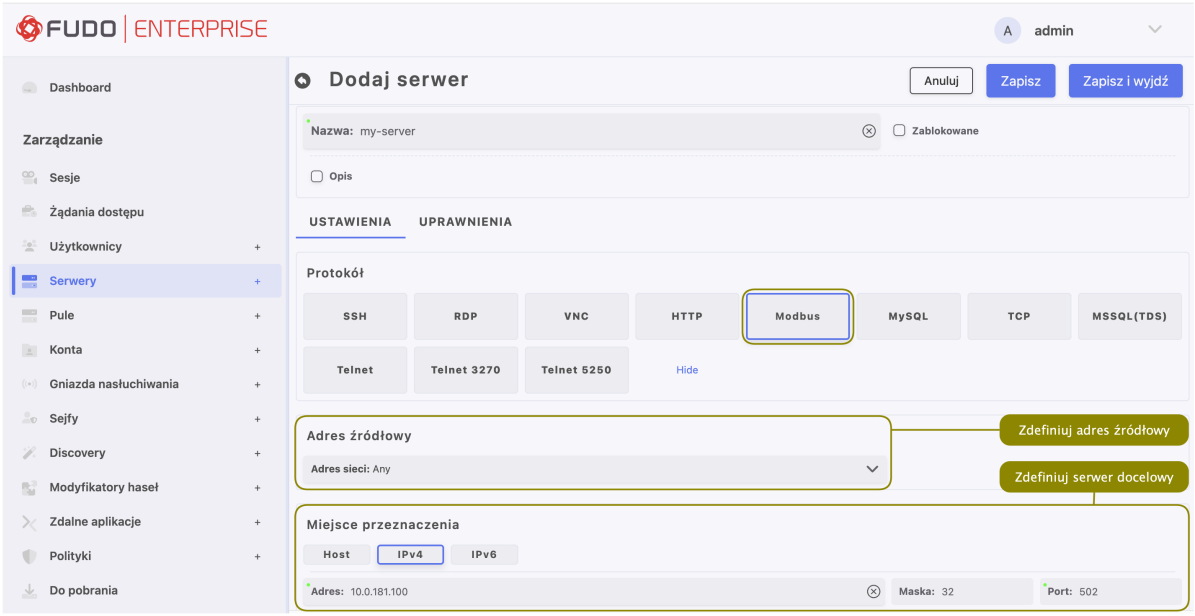
- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* wybierz etykietowany adres 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 *Etykietowane adresy IP*.

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

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

Uwaga

- 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*.
- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

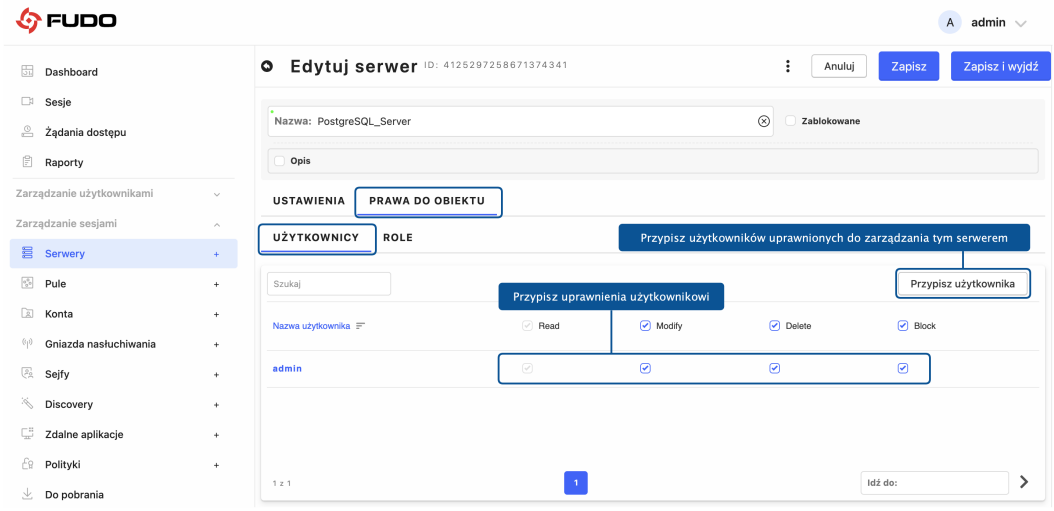


6. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

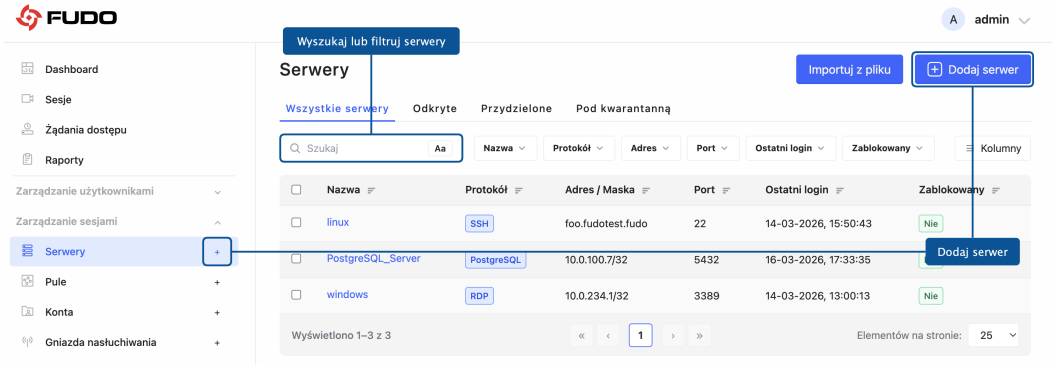
- *Pule*
- *Model danych*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

10.1.1.3 Dodawanie serwera MS SQL

Uwaga

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

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



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.

5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `MSSQL(TDS)`.
3. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

4. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

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

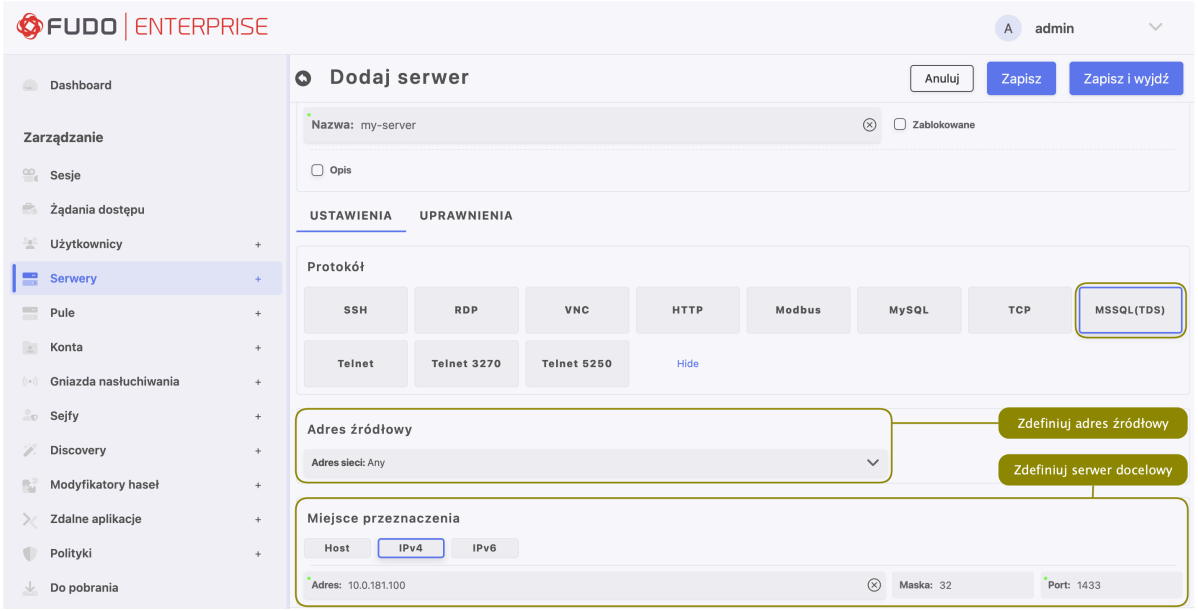
- Wybierz `Host`, `IPv4` albo `IPv6`,
- Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Uwaga

- 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*.

- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

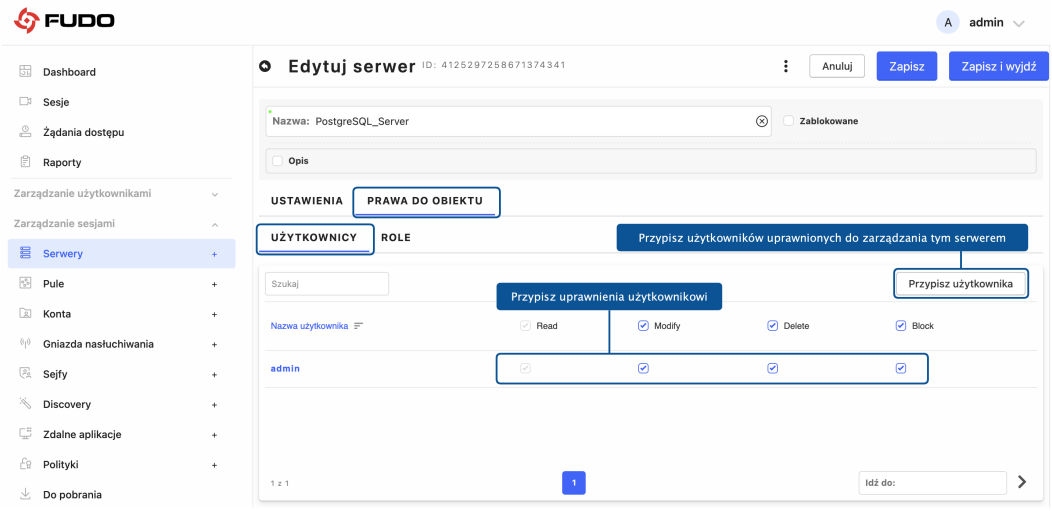


6. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

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

10.1.1.4 Dodawanie serwera MySQL

Ostrzeżenie

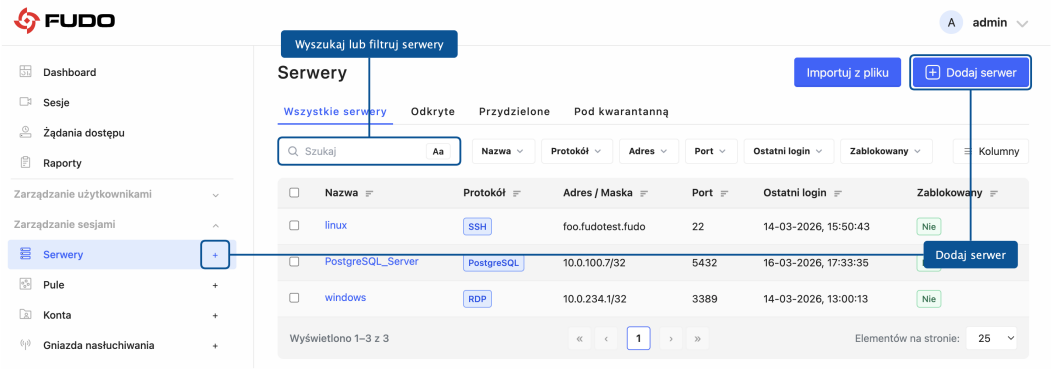
Obsługiwane wtyczki uwierzytelniania:

- dla komunikacji między Fudo Enterprise a serwerem bazy danych: `mysql_clear_password`, `mysql_native_password`, `caching_sha2_password`;
- dla komunikacji między klientem a Fudo Enterprise: `mysql_clear_password`.

Uwaga

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

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



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `MySQL`.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

3. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
4. Zaznacz dodatkowo opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych.
5. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

6. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Uwaga

- Elementami listy rozwijanej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

7. W sekcji *Miejsce przeznaczenia* zdefiniuj adres serwera docelowego:

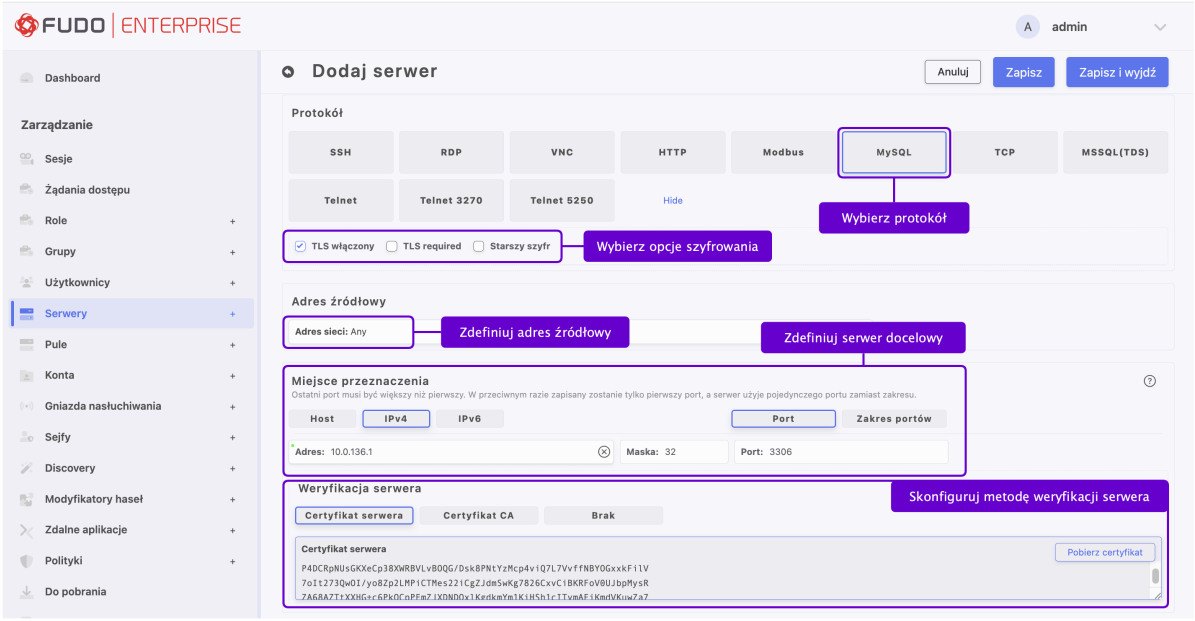
- Wybierz `Host`, `IPv4` lub `IPv6`,
- Wprowadź *Adres* oraz *Port*, jeśli jest inny, niż natywny dla protokołu; możliwe jest także określenie zakresu portów (zob. *Zakresy portów w konfiguracji serwerów*).

Uwaga

- 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*.
- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

8. W sekcji *Weryfikacja serwera* (dostępnej, jeśli obsługa TLS została włączona) określ metodę weryfikacji serwera:

- Wybierz `Certyfikat serwera`, aby weryfikować serwer na podstawie jego certyfikatu,
- Wybierz `Certyfikat CA`, aby weryfikować certyfikat serwera przy użyciu zaufanego urzędu certyfikacji,
- Wybierz `Brak`, aby wyłączyć weryfikację certyfikatu serwera.

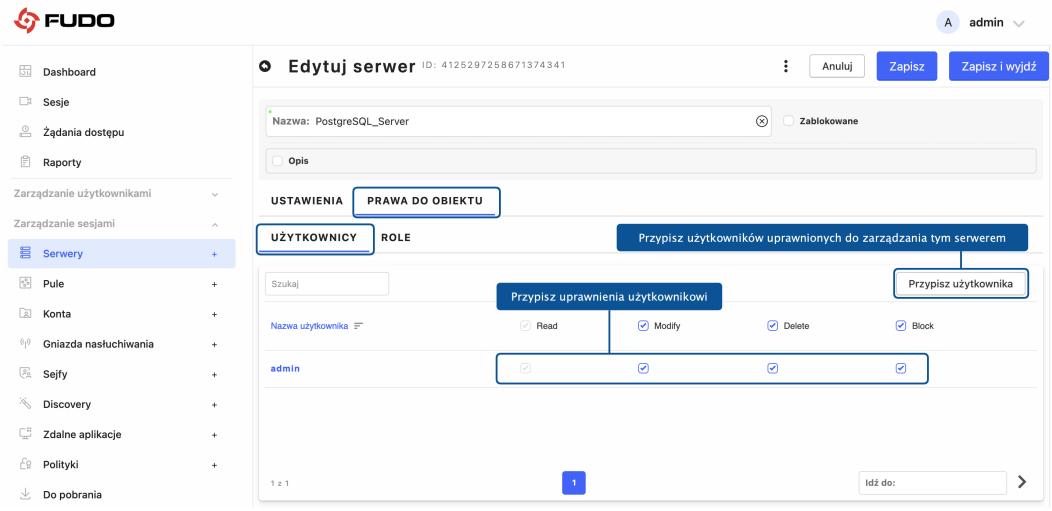


9. Kliknij *Zapisz* albo *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.

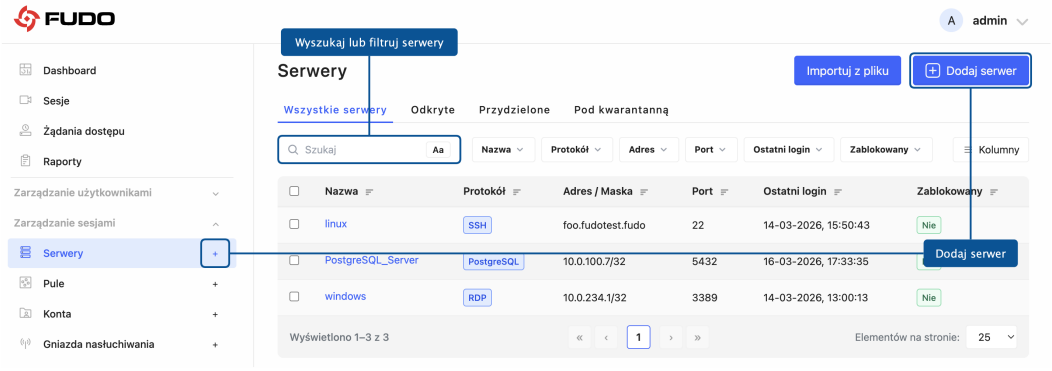


Tematy pokrewne:

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

10.1.1.5 Tworzenie serwera PostgreSQL

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



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `PostgreSQL`.

Ostrzeżenie

Po zapisaniu definicji serwera pole protokołu nie może być edytowane.

3. Zaznacz opcję *Włączone TLS*, aby połączyć się z monitorowanym serwerem przez TLS.
4. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych.
5. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

6. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

7. W sekcji *Miejsce docelowe* zdefiniuj adres serwera docelowego:
   - Wybierz `Host`, `IPv4` lub `IPv6`,
   - Wprowadź *Adres* i *Port*, jeśli port różni się od domyślnego dla protokołu (5432). Możesz również określić zakres portów. Szczegóły znajdują się w *Zakresy portów w konfiguracji serwerów*.

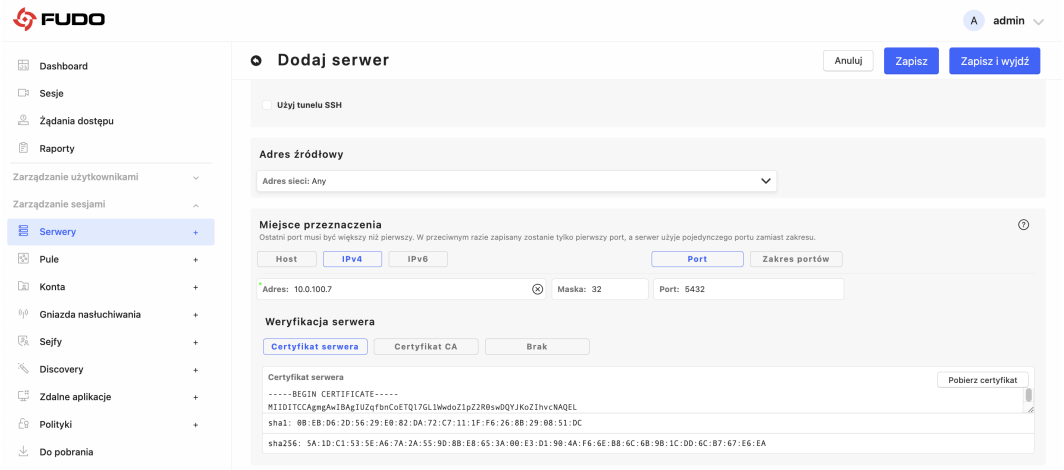
Uwaga

- W zależności od wybranej opcji domyślne wartości dla pól *Maska* i *Port* są wypełniane automatycznie. W ten sposób system Fudo Enterprise wykrywa serwer jako ten z unikalnym adresem. Aby skonfigurować adres dla całej podsieci, podaj dedykowaną

wartość dla pól *Adres* i *Maska*.

- W przypadku nakładających się definicji adresów, podczas ustanawiania połączenia zawsze wybierana jest bardziej szczegółowa konfiguracja (wyższa maska sieciowa), nawet jeśli użytkownik nie ma przypisanych do niej uprawnień. Ten mechanizm umożliwia definiowanie wyjątków w szerszych regułach dostępu (np. przyznanie dostępu do `/24` przy jednoczesnym wyłączeniu `/32`).

8. W sekcji *Weryfikacja serwera* określ metodę weryfikacji serwera:
   - Wybierz `Certyfikat serwera`, aby zweryfikować serwer na podstawie jego certyfikatu,
   - Wybierz `Certyfikat CA`, aby zweryfikować certyfikat serwera za pomocą zaufanego urzędu certyfikacji,
   - Wybierz `Brak`, aby wyłączyć weryfikację certyfikatu serwera.

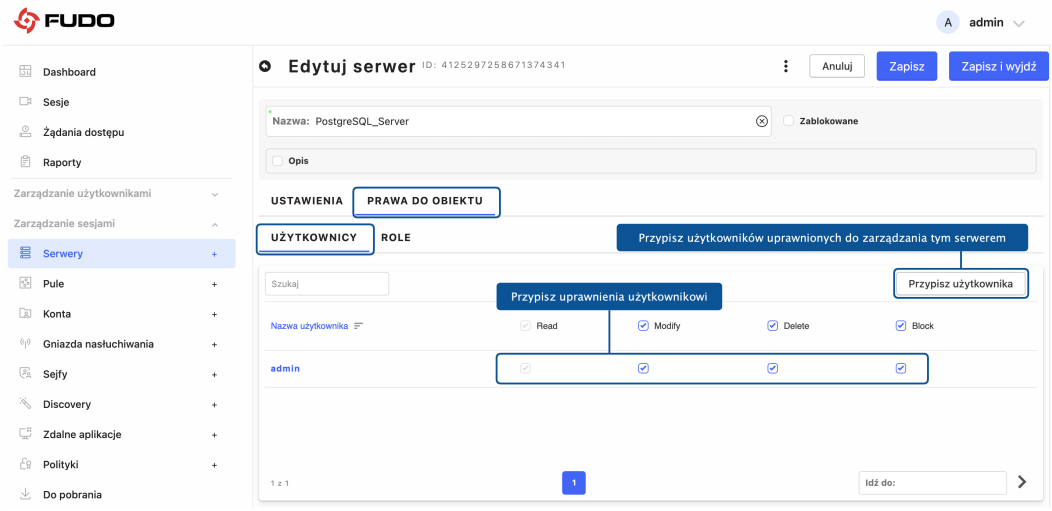


9. Kliknij *Zapisz* lub *Zapisz i wyjdź*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

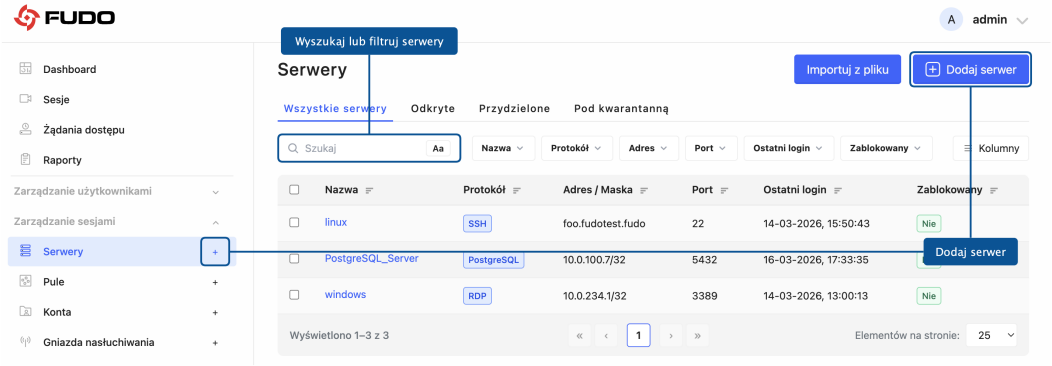
- *Pule*
- *Model danych*
- *Inicjowanie systemu*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*
- *Konta*

10.1.1.6 Dodawanie serwera RDP

Uwaga

- 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 ikonę + obok zakładki *Serwery* w podsekcji *Zarządzanie sesjami*, lub
2. Wybierz *Zarządzanie sesjami* > *Serwery*, a następnie kliknij + *Dodaj serwer*.



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `RDP`.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

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

Uwaga

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.

5. Zaznacz dodatkowo opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
6. Zaznacz opcję *Poinformuj o istniejącym połączeniu*, aby użytkownik, łączący się do serwera, był informowany o tym, że inny użytkownik jest obecnie połączony z danym serwerem.
7. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

8. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

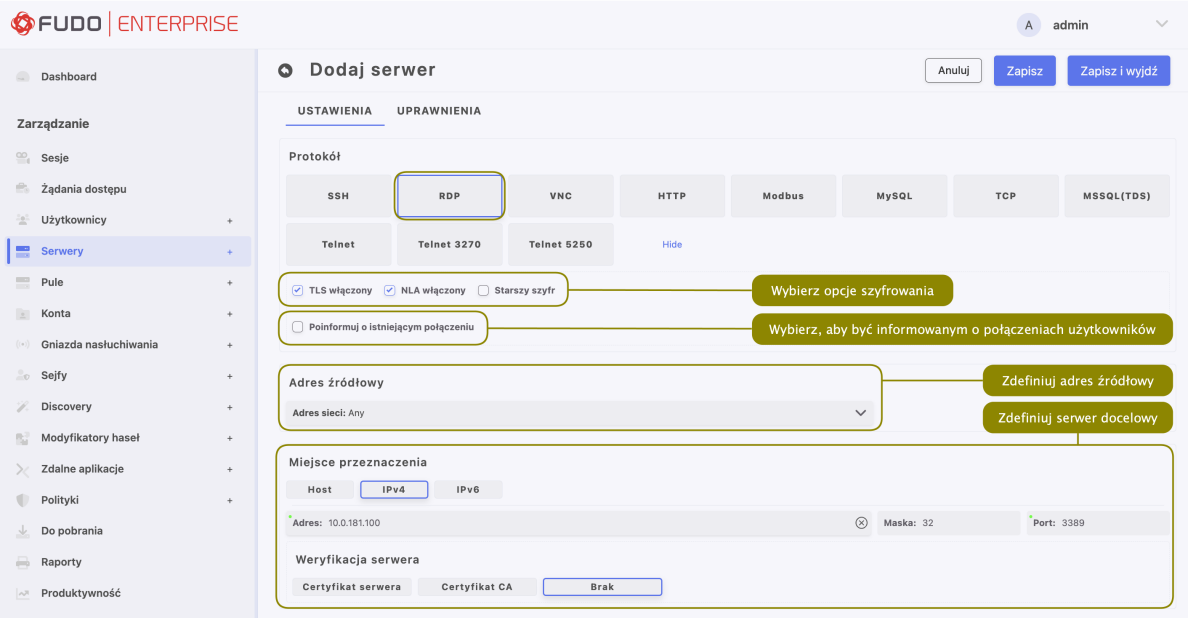
9. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

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

Uwaga

- 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*.
- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

- 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.

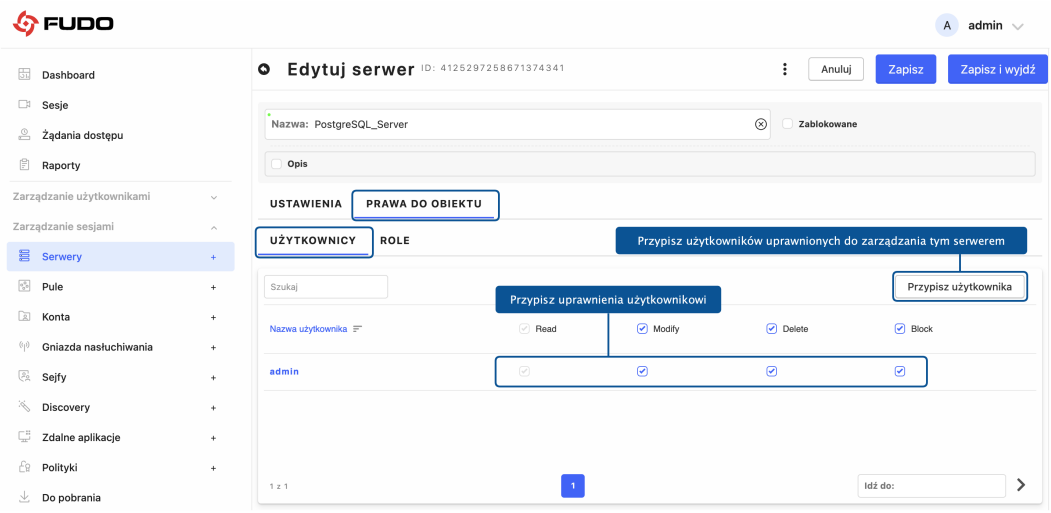


10. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

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

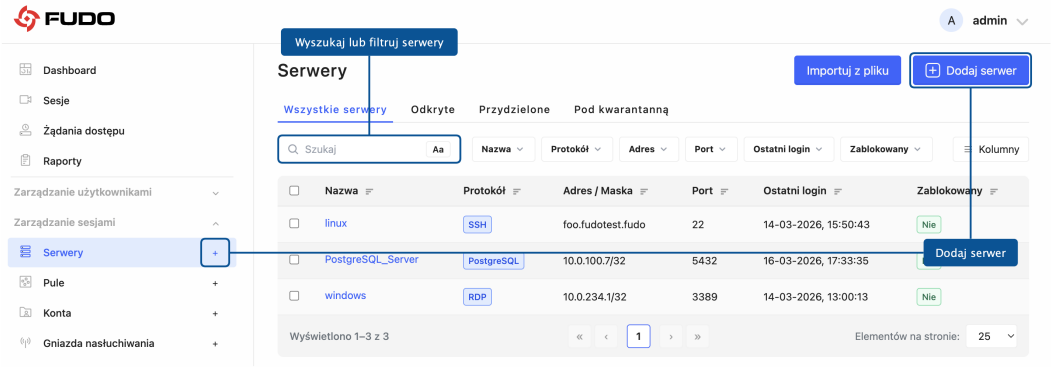
10.1.1.7 Dodawanie serwera SSH

Uwaga

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

1. Kliknij ikonę + obok zakładki *Serwery* w podsekcji *Zarządzanie sesjami*, lub

2. Wybierz *Zarządzanie sesjami* > *Serwery*, a następnie kliknij + *Dodaj serwer*.



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `SSH`.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

3. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
4. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

5. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

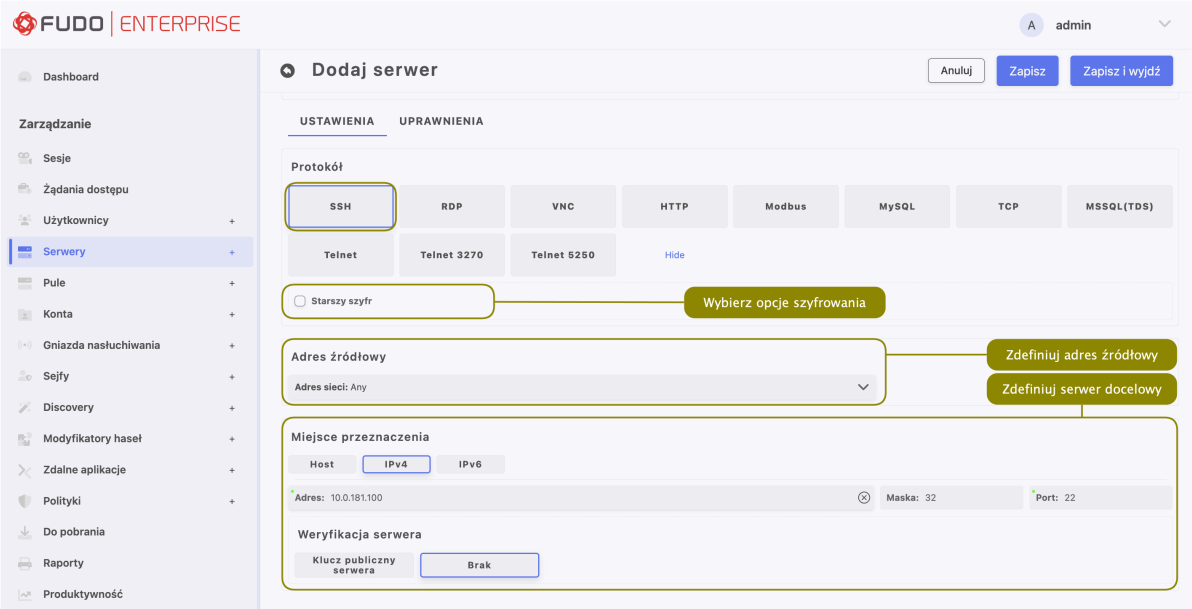
6. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

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

Uwaga

- 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*.
- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

7. W sekcji *Weryfikacja serwera* wybierz `Klucz publiczny serwera` i pobierz certyfikat, albo wybierz `Brak`, aby wyłączyć weryfikację serwera SSH.

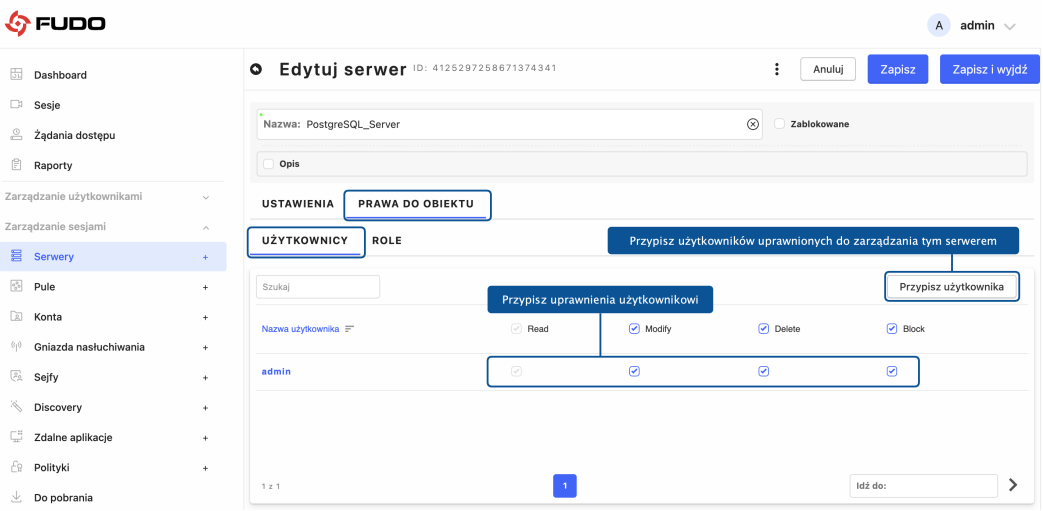


8. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

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

10.1.1.8 Dodawanie serwera Telnet

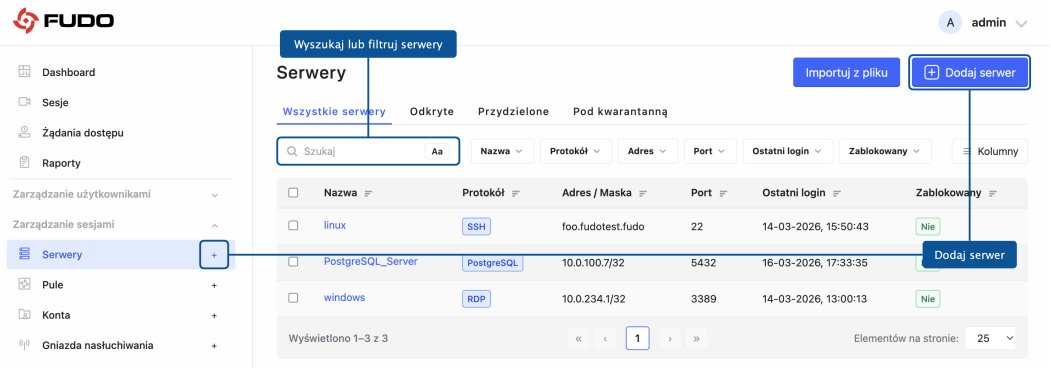
Dodawanie definicji serwera

Uwaga

- 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 ikonę + obok zakładki *Serwery* w podsekcji *Zarządzanie sesjami*, lub
2. Wybierz *Zarządzanie sesjami* > *Serwery*, a następnie kliknij + *Dodaj serwer*.



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `Telnet`.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

3. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
4. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
5. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.

- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

6. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

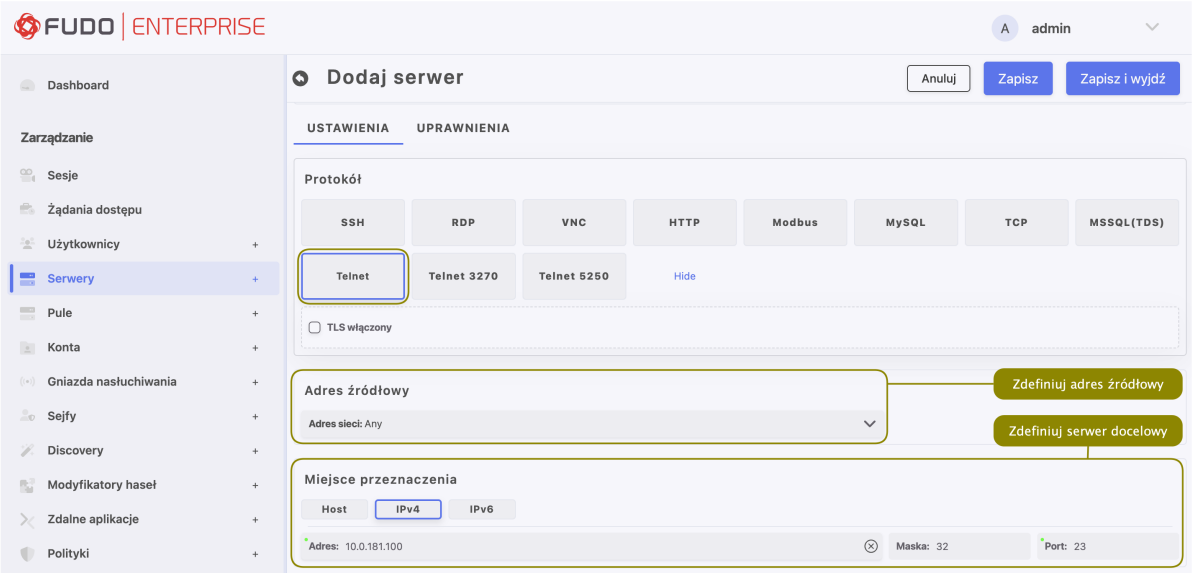
7. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

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

Uwaga

- 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*.
- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

- 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.

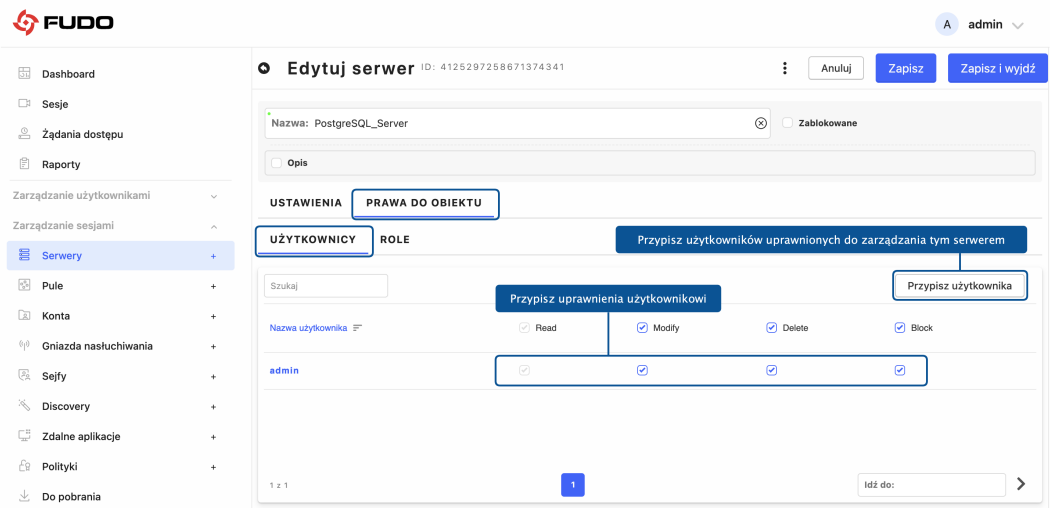


8. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

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

10.1.1.9 Dodawanie serwera Telnet 3270

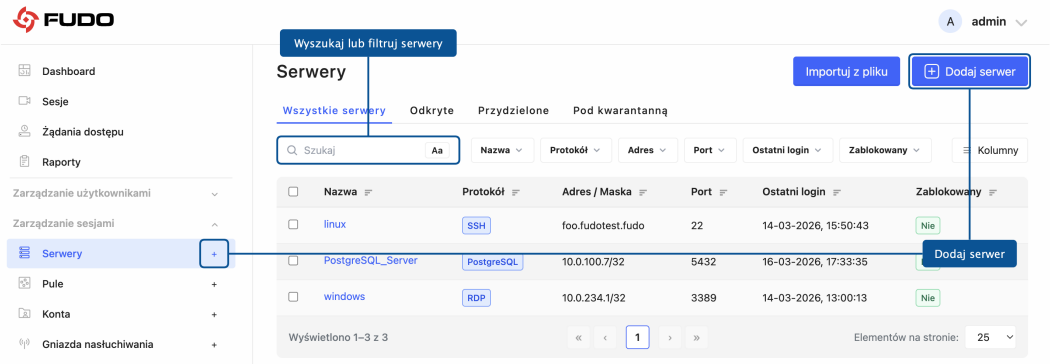
Deprecated since version 6.0 :class: danger

Wsparcie dla protokołu **Telnet 3270** jest obecnie **w fazie przeglądu** i może zostać usunięte w jednej z kolejnych wersji. Jeśli protokół ten jest kluczowy dla Twojego środowiska, skontaktuj się z pomocą techniczną Fudo w celu uzyskania dodatkowych informacji.

Uwaga

- 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 ikonę + obok zakładki *Serwery* w podsekcji *Zarządzanie sesjami*, lub
2. Wybierz *Zarządzanie sesjami* > *Serwery*, a następnie kliknij + *Dodaj serwer*.



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `Telnet 3270`.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

3. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
4. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
5. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

6. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Uwaga

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

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

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

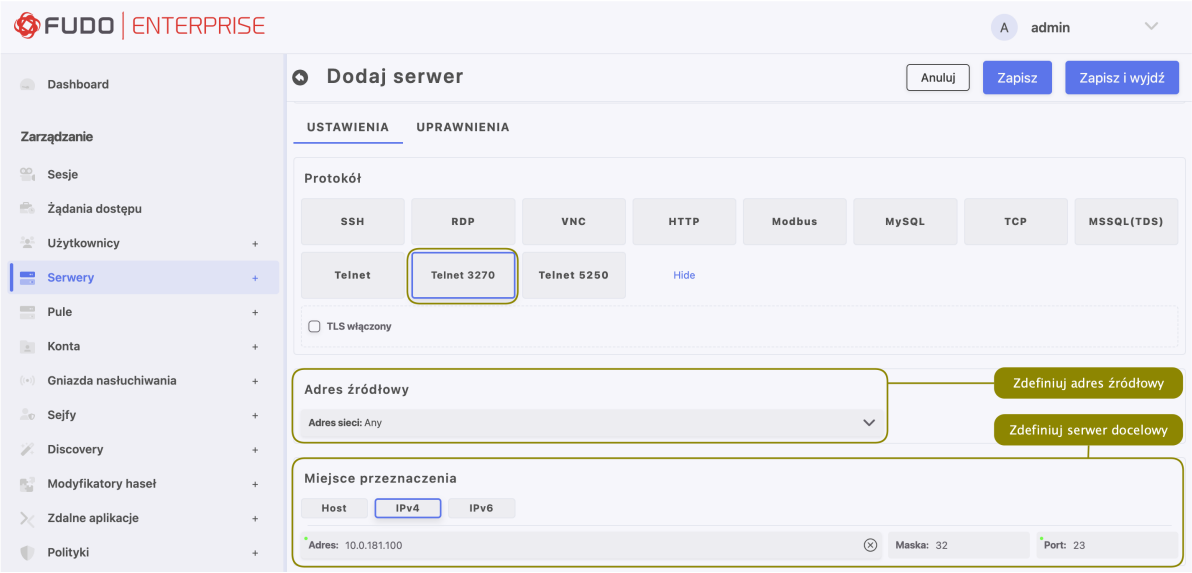
Uwaga

- 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*.

- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

- 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.

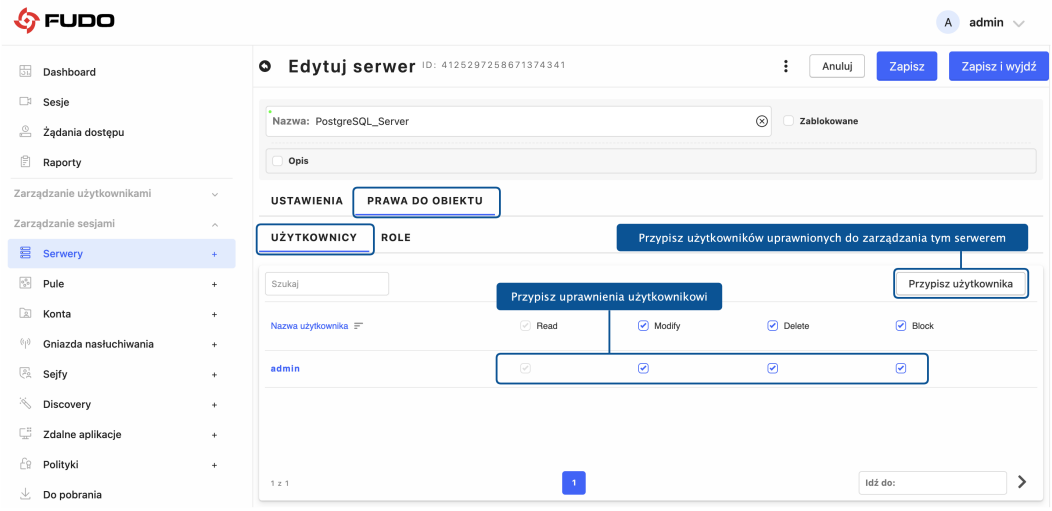


8. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

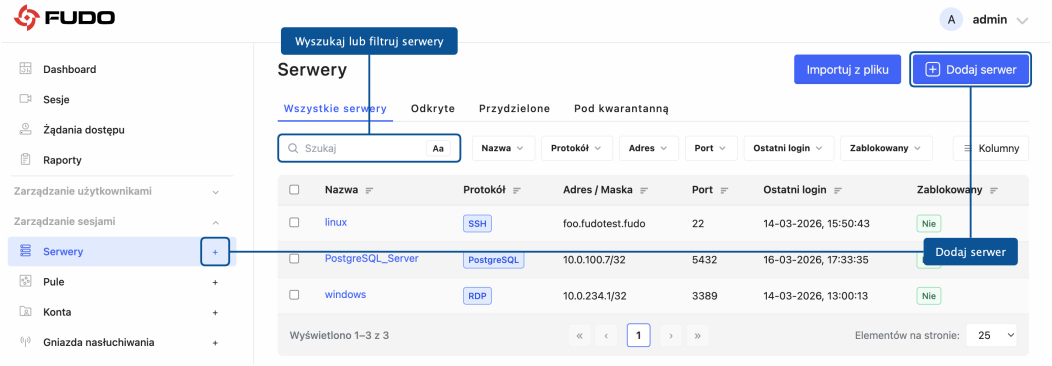
- *Pule*
- *Model danych*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

10.1.1.10 Dodawanie serwera Telnet 5250

Uwaga

- 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 ikonę + obok zakładki *Serwery* w podsekcji *Zarządzanie sesjami*, lub
2. Wybierz *Zarządzanie sesjami* > *Serwery*, a następnie kliknij + *Dodaj serwer*.



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `Telnet 5250`.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

3. Zaznacz opcję *TLS włączony*, aby połączenie z serwerem było szyfrowane.
4. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych: DSA (1024), RSA (1024).
5. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

6. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

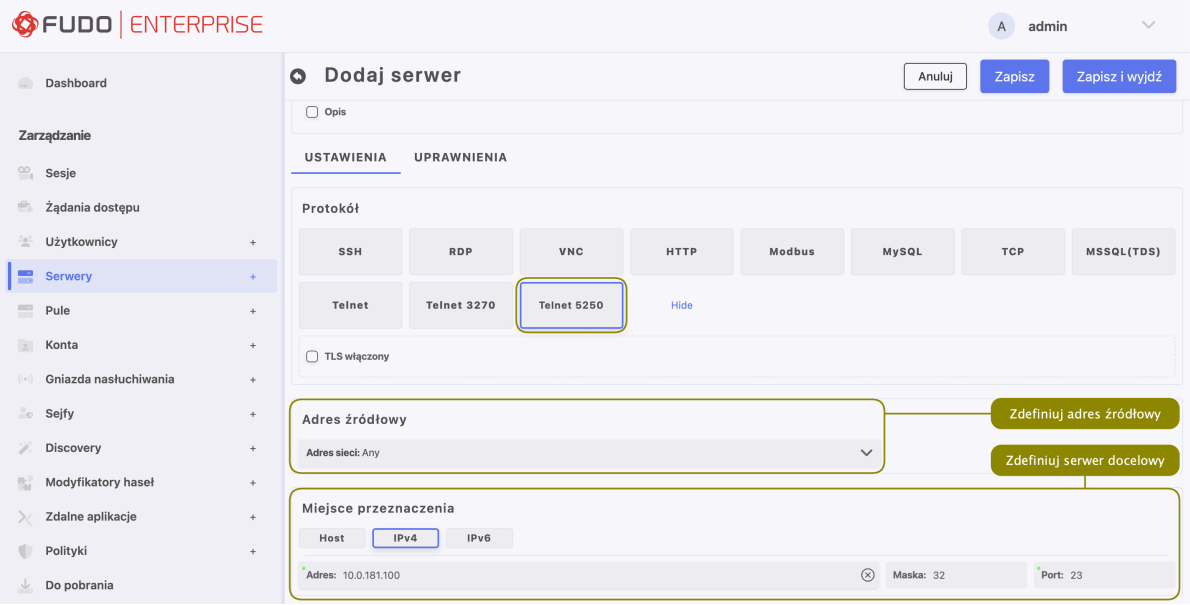
7. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

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

Uwaga

- 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*.
- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

- 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.



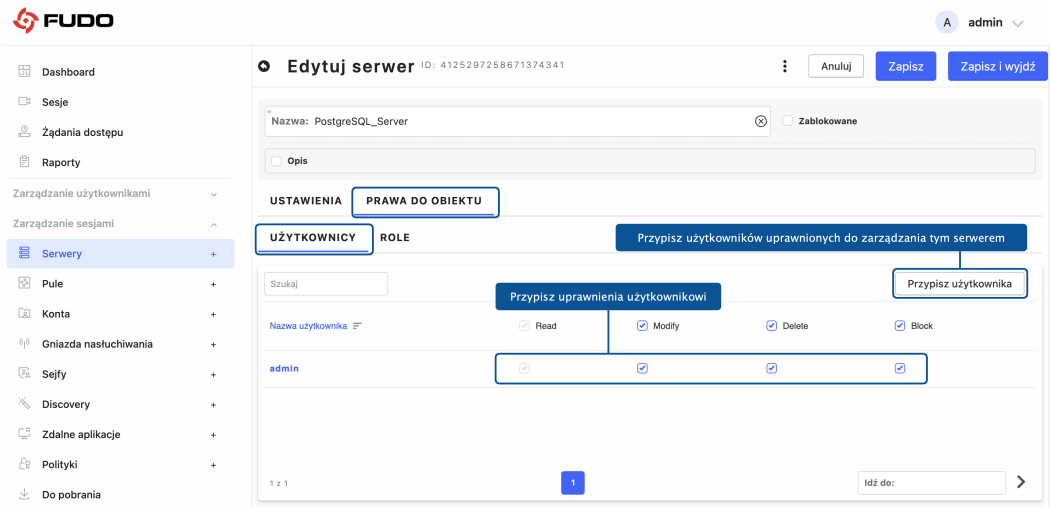
8. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.

6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

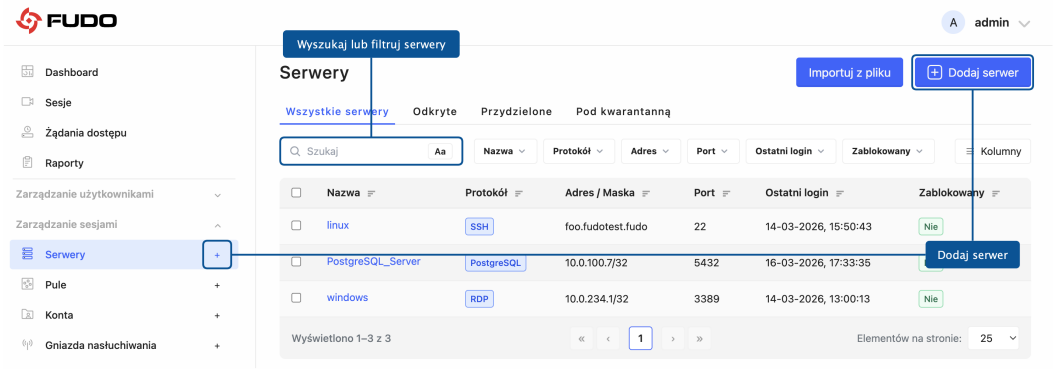
- *Pule*
- *Model danych*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

10.1.1.11 Dodawanie serwera VNC

Uwaga

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

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



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `VNC`.

Ostrzeżenie

Po zapisaniu definicji serwera pole protokołu nie może być edytowane.

3. Zaznacz opcję *Włączone TLS*, aby połączyć się z monitorowanym serwerem przez TLS.
4. Zaznacz opcję *Starszy szyfr*, aby przy zestawianiu połączenia, zezwolić na negocjowanie starszych algorytmów kryptograficznych.
5. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

6. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* 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 *Etykietowane adresy IP*.

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

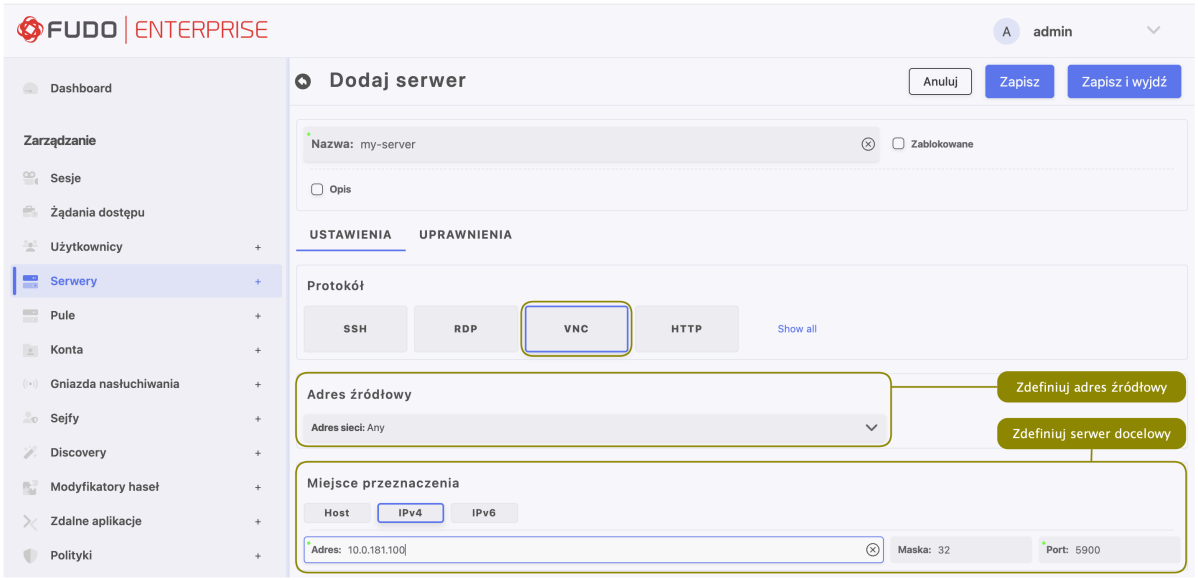
- Wybierz `Host`, `IPv4` albo `IPv6`,
- Wprowadź *Adres* oraz *port*, jeśli jest inny, niż natywny dla protokołu.

Uwaga

- 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*.
- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

8. W sekcji *Weryfikacja serwera* (dostępnej, jeśli obsługa TLS została włączona) określ metodę weryfikacji serwera:

- Wybierz `Certyfikat serwera`, aby weryfikować serwer na podstawie jego certyfikatu,
- Wybierz `Certyfikat CA`, aby weryfikować certyfikat serwera przy użyciu zaufanego urzędu certyfikacji,
- Wybierz `Brak`, aby wyłączyć weryfikację certyfikatu serwera.

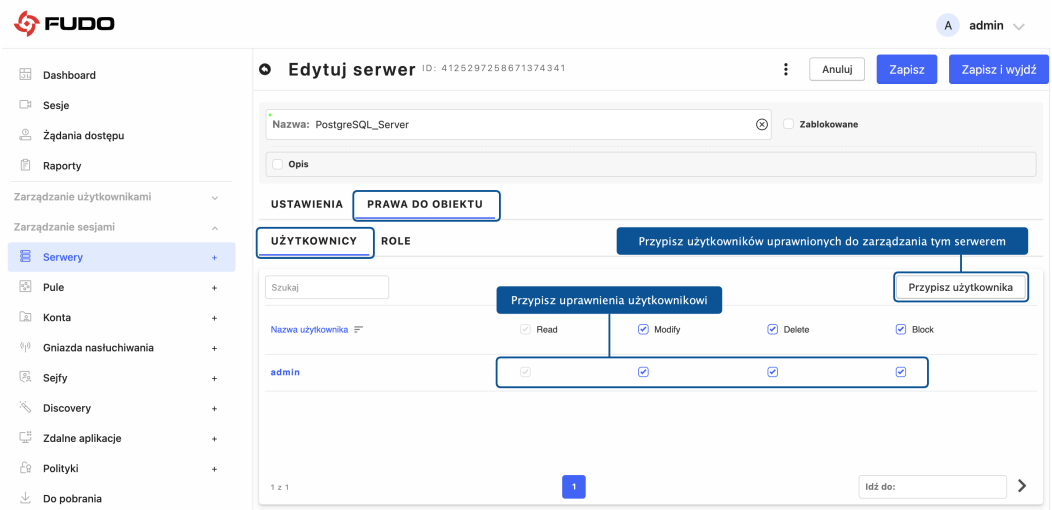


9. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.

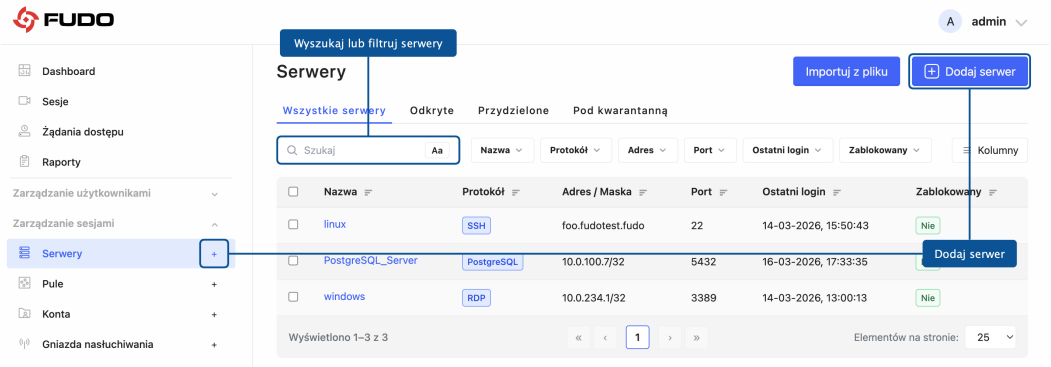


Tematy pokrewne:

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

10.1.1.12 Dodawanie serwera TCP

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



3. Wpisz unikalną nazwę serwera.
4. Zaznacz opcję *Zablokowane*, jeśli obiekt ma być niedostępny po utworzeniu (np. do czasu zakończenia konfiguracji lub weryfikacji) (np. do czasu zakończenia konfiguracji lub weryfikacji). Wymagane jest wpisanie powodu zablokowania.
5. Zaznacz opcję *Opis* i wprowadź tekst, który ułatwi identyfikację tego zasobu.

ZAKŁADKA USTAWIENIA

1. Przejdź do zakładki *USTAWIENIA*.
2. W sekcji *Protokół* wybierz `TCP`.
3. Zaznacz opcję *Użyj tunelu SSH* i podaj *Klucz tunelu SSH*, jeśli chcesz zestawić połączenie przez odwrotny tunel SSH.

Uwaga

- W trybie *Tunel* docelowy host i port są udostępniane przez bezpieczny zdalny endpoint tunelu, zamiast być osiągane bezpośrednio za pomocą ustawień w sekcjach *Adres źródłowy* i *Miejsce przeznaczenia*. Zobacz *Konfiguracja serwera z odwrotnym tunelem SSH*.
- Jeśli chcesz połączyć się używając gniazda nasłuchiwania typu Tunnel do serwera skonfigurowanego z opcją *Użyj tunelu SSH* (odwrotny tunel SSH), musisz użyć nazwy serwera

zamiast bezpośredniego adresu IP i portu. Zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

4. Jeśli tunel SSH nie jest używany, z listy rozwijanej *Adres źródłowy* wybierz adres IP, z którego będą inicjowane połączenia do monitorowanego serwera, a następnie skonfiguruj ustawienia w sekcjach *Adres nasłuchu* i *Miejsce przeznaczenia*.

Ostrzeżenie

Po zapisaniu definicji serwera protokół jest nieedytowalny.

Uwaga

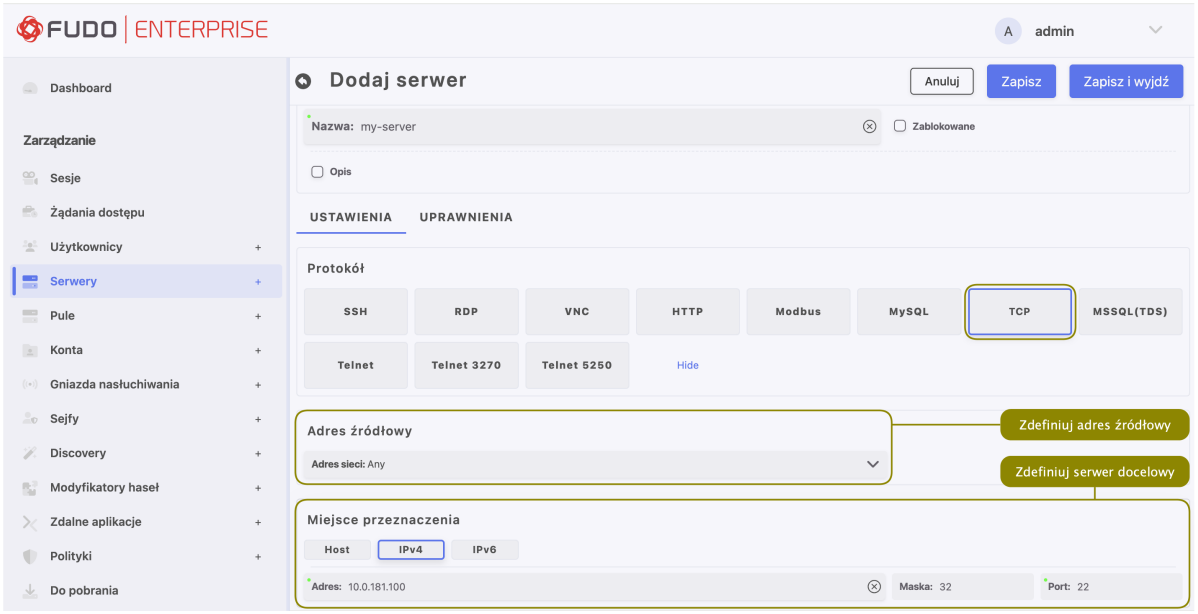
- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- W przypadku konfiguracji klastrowej, z listy rozwijanej *Adres sieci* wybierz etykietowany adres 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 *Etykietowane adresy IP*.

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

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

Uwaga

- 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*.
- W przypadku nakładających się definicji adresowych podczas nawiązywania połączenia zawsze wybierana jest konfiguracja bardziej szczegółowa (wyższa maska), nawet jeśli użytkownik nie posiada do niej uprawnień. Mechanizm ten umożliwia definiowanie wyjątków w obrębie szerszych reguł (np. przyznanie dostępu do `/24` z jednoczesnym wykluczeniem `/32`).

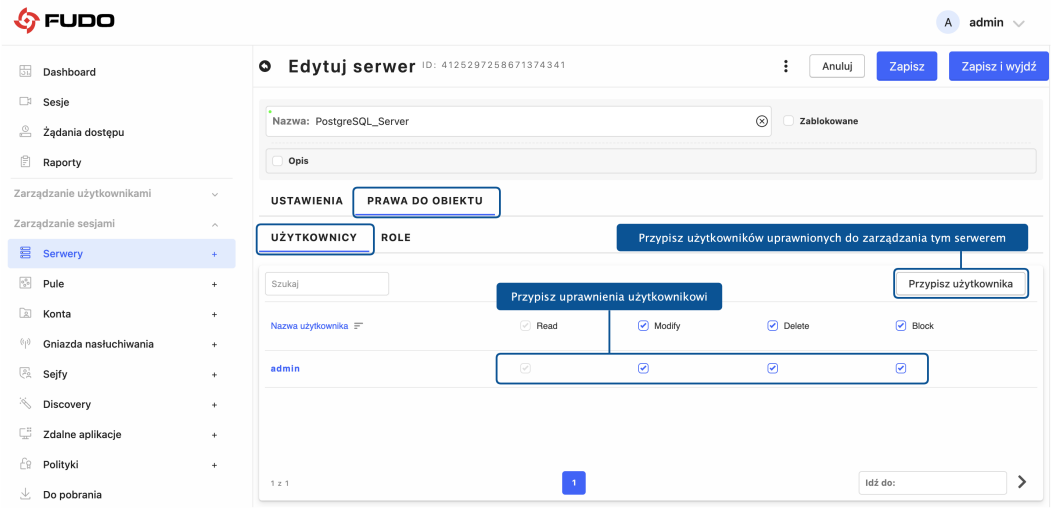


6. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Tematy pokrewne:

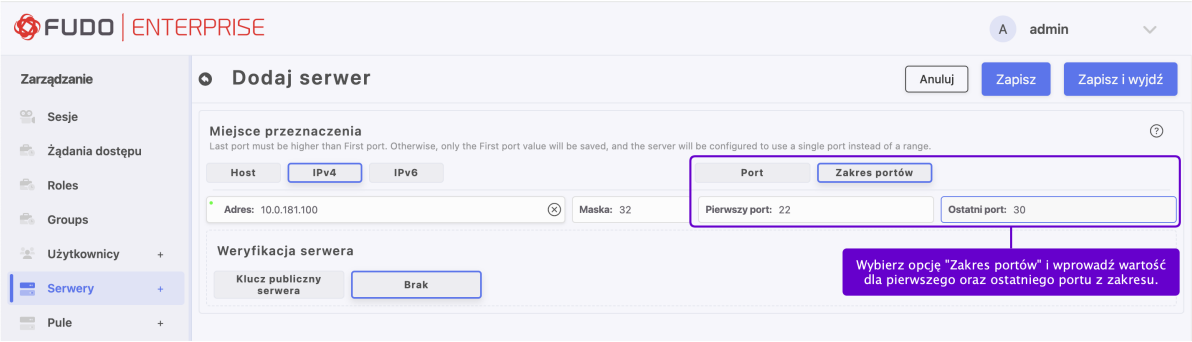
- *Pule*
- *TCP*
- *Konfigurowanie gniazda nasłuchiwania TCP*
- *Model danych*

10.1.2 Zakresy portów w konfiguracji serwerów

Funkcjonalność **Zakres portów** umożliwia skonfigurowanie w Fudo Enterprise obiektu typu Serwer z określeniem zakresu portów. Dzięki temu eliminowana jest konieczność tworzenia osobnych serwerów dla każdego portu w sytuacjach wymagających przekierowania ruchu z wielu portów jednocześnie, co znacząco upraszcza proces konfiguracji i redukuje ilość pracy ręcznej.

10.1.2.1 Konfiguracja zakresu portów

1. Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj serwer*.
2. Wprowadź unikalną nazwę dla tworzonego obiektu (np: Server_1).
3. Przejdź do sekcji **Ustawienia.**
4. W polu **Protokół** wybierz protokół dla tworzonego serwera.
5. W sekcji **Miejsce przeznaczenia** zdefiniuj parametry serwera docelowego:
   - Wybierz **Host, IPv4** albo **IPv6**.
   - Wprowadź **Adres** serwera oraz ewentualnie **Maskę**.
6. Kliknij **Zakres portów** i wpisz wartości w polach **Pierwszy port** oraz **Ostatni port** (np: Pierwszy port: 22, Ostatni port: 30).
7. Kliknij **Zapisz i wyjdź.**



Uwaga

- Maksymalna dopuszczalna wartość dla obu pól wynosi **65535**. W przypadku wprowadzenia wartości wyższej, zostanie **automatycznie** ustawiona **wartość maksymalna**.
- Numer ostatniego portu musi być większy niż numer pierwszego portu. Wprowadzenie w polu *Ostatni port* wartości mniejszej lub równej wartości z pola *Pierwszy port* spowoduje zapisanie jedynie wartości z pola *Pierwszy port* oraz skonfigurowanie serwera do korzystania z pojedynczego portu zamiast zakresu.
- Po wybraniu opcji *Zakres portów* funkcja automatycznego pobierania certyfikatu lub klucza publicznego zostaje dezaktywowana i należy wprowadzić go ręcznie.

10.1.2.2 Priorytetyzacja konfiguracji serwerów w przypadku konfliktu

W sytuacji, gdy zostanie skonfigurowany serwer z zakresem portów oraz drugi serwer o tym samym adresie, ale z pojedynczym portem mieszczącym się w zakresie portów pierwszego serwera, np:

```
Serwer_1 - 10.0.130.100:22-24
Serwer_2 - 10.0.130.100:23
```

wtedy Fudo Enterprise przy nawiązywaniu połączenia przez ten port (23) zawsze wybierze bardziej precyzyjną konfigurację, czyli w tym przypadku `Serwer_2`.

Uwaga

W konsekwencji, jeśli użytkownik posiadający uprawnienia do `Serwer_1` wybierze z dostępnego zakresu port 23, a jednocześnie nie ma w Fudo Enterprise przydzielonych uprawień dostępu do `Serwer_2`, nie będzie mógł nawiązać takiego połączenia.

Tematy pokrewne:

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

10.1.3 Konfiguracja serwera z odwrotnym tunelem SSH

W niektórych środowiskach sieciowych system Fudo Enterprise może nie mieć bezpośredniego dostępu do serwera docelowego ze względu na:

- Ograniczenia zapory sieciowej
- Segmentację sieci
- Serwer znajduje się w prywatnej sieci

W takim przypadku można użyć **jump hosta** (serwera pośredniczącego), który ma dostęp zarówno do systemu Fudo Enterprise jak i do serwera docelowego.

> **Uwaga**
>
> Jump host działa jako pośrednik, zestawiając odwrotny tunel SSH między systemem Fudo Enterprise a serwerem docelowym.

Wymagania

1. Jump host z dostępem do Fudo Enterprise oraz serwera docelowego.
2. Zainstalowany klient SSH na jump hoście.
3. Możliwość uruchomienia komend SSH na jump hoście.

Przygotowanie kluczy SSH na jump hoście

1. Na jump hoście wygeneruj parę kluczy SSH (jeśli nie istnieje):

```
ssh-keygen -t rsa -b 4096 -f ~/.ssh/fudo_jumphost
```

2. Skopiuj zawartość klucza publicznego:

```
cat ~/.ssh/fudo_jumphost.pub
```

Tworzenie serwera z opcją tunelu SSH

1. Wybierz z lewego menu *Zarządzanie sesjami* > *Serwery* i kliknij + *Dodaj serwer*
2. Wprowadź nazwę (np: `Jump_Server_Target`).
3. W zakładce *USTAWIENIA*, wybierz protokół odpowiedni dla serwera docelowego (np. SSH).
4. Zaznacz opcję *Użyj tunelu SSH*.
5. W polu *Klucz tunelu SSH* wklej klucz publiczny SSH jump hosta.
6. Kliknij *Zapisz*.

Pobranie komendy SSH

Po zapisaniu konfiguracji serwera, system Fudo Enterprise wygeneruje komendę SSH do wykonania na jump hoście.

Przykład wygenerowanej komendy:

```
ssh -l tunnel -p 65522 -o ExitOnForwardFailure=yes -N -f -R /tunnel/
↪8754997675608244234:<target>:<port> 10.31.135.179
```

gdzie należy zastąpić:

- `<target>` - adresem IP serwera docelowego
- `<port>` - portem serwera docelowego

Zestawienie tunelu

Wykonaj komendę wygenerowaną przez system Fudo Enterprise na jump hoście, podstawiając rzeczywiste wartości:

```
ssh -l tunnel -p 65522 -o ExitOnForwardFailure=yes -N -f -R /tunnel/
↪8754997675608244234:192.168.1.100:22 10.31.135.179
```

gdzie:

- `192.168.1.100:22` - adres i port serwera docelowego
- `10.31.135.179` - adres systemu Fudo Enterprise

Wyjaśnienie parametrów komendy:

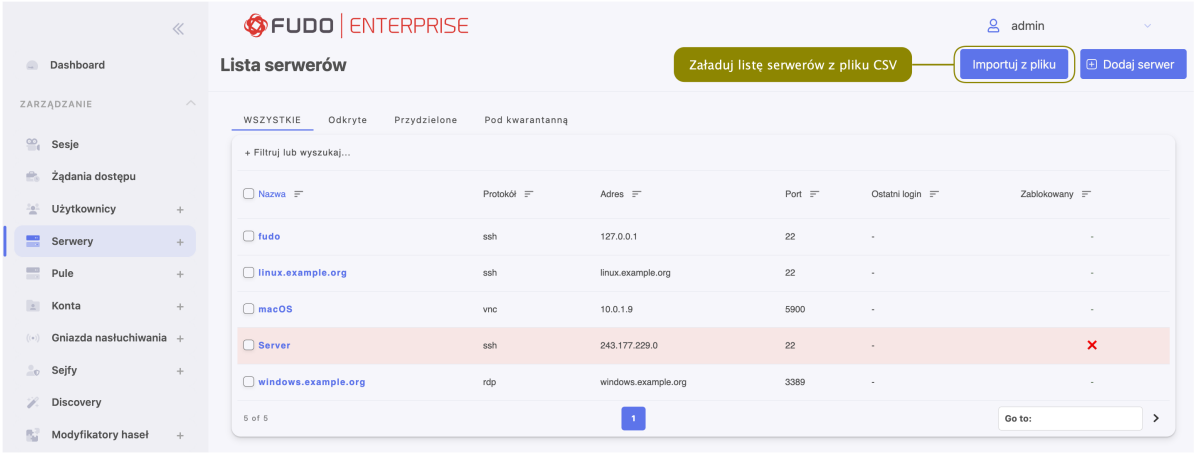
- `-l tunnel` - nazwa użytkownika tunelu
- `-p 65522` - port systemu Fudo Enterprise do tuneli
- `-o ExitOnForwardFailure=yes` - zakończ jeśli przekierowanie się nie powiedzie
- `-N` - nie wykonuj zdalnych komend
- `-f` - uruchom w tle
- `-R /tunnel/ID:target:port` - utwórz odwrotny tunel

Tematy pokrewne:

- *Dodawanie serwera SSH*
- *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*
- *Nawiązywanie połączenia SSH*

10.1.4 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.

Uwaga

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,bind_ip,address,mask,port,port_first,port_last,protocol,legacy_crypto,rdp_
↪hotseat,rdp_nla_enabled,tls_enabled
z1,10.0.136.1,10.0.136.10,32,2137,,,ssh,TRUE,,,
z2,10.0.136.1,10.0.136.10,32,,7312,9000,rdp,,TRUE,TRUE,TRUE
z3,10.0.136.1,10.0.136.10,32,,5000,7313,rdp,,TRUE,TRUE,TRUE
```

Uwaga

W przypadku serwerów z ustawionym zakresem portów plik w formacie CSV powinien zawierać:

- wypełnioną kolumnę `port` dla serwera z pojedynczym portem,
- wypełnione kolumny `port_first` oraz `port_last` dla serwera z zakresem portów.

Tematy pokrewne:

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

10.1.5 Modyfikowanie serwera

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

Uwaga

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*

10.1.6 Blokowanie serwera

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

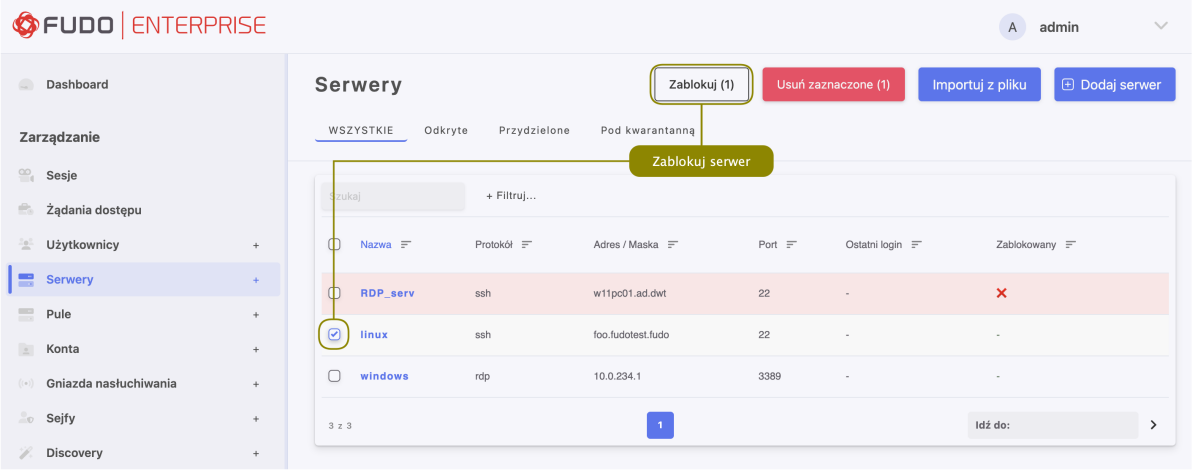
Ostrzeżenie

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

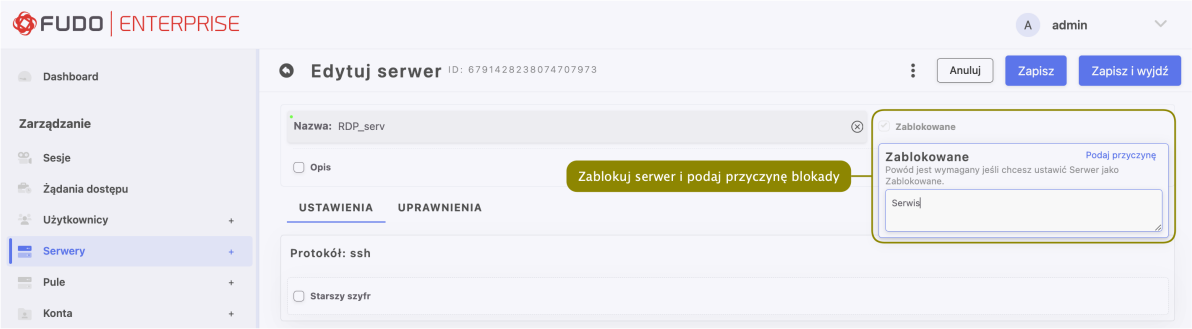
1. Wybierz z lewego menu *Zarządzanie* > *Serwery*.
2. Odszukaj na liście i wybierz serwer, który chcesz zablokować.

> **Uwaga**
>
> Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.

3. Kliknij *Zablokuj*, aby zablokować możliwość nawiązywania połączeń z wybranymi zasobami.



4. Wprowadź powód zablokowania zasobu i kliknij *Potwierdź*.
5. Kliknij *Zapisz* albo *Zapisz i wyjdź*.
6. Możesz także zablokować serwer z poziomu formularza edycji. Edytuj serwer, zaznacz opcję *Zablokuj* i podaj powód zablokowania. Zapisz serwer.



Tematy pokrewne:

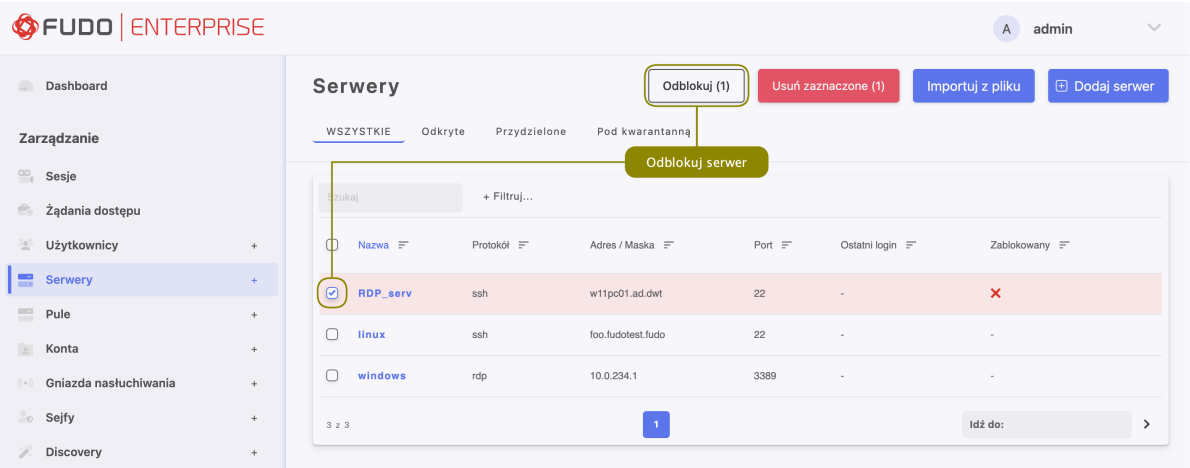
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*
- *Konta*

10.1.7 Odblokowanie serwera

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

Uwaga

Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



3. Kliknij *Odblokuj*, aby przywrócić możliwość nawiązywania połączeń z serwerami.
4. Kliknij *Potwierdź*.
5. Kliknij *Zapisz* albo *Zapisz i wyjdź*.
6. Możesz także odblokować serwer z poziomu formularza edycji. Edytuj serwer, odznacz opcję Zablokuj i zapisz serwer.



Tematy pokrewne:

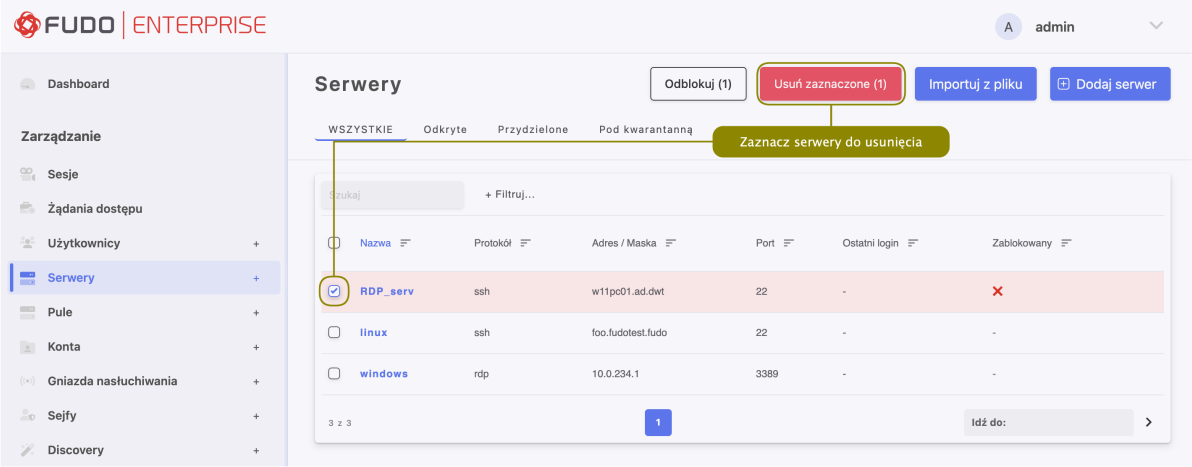
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Gniazda nasłuchiwania*
- *Sejfy*
- *Konta*

10.1.8 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*.



4. Kliknij *Potwierdź*.

Tematy pokrewne:

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

10.2 Pule

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

Uwaga

Serwery są grupowane na podstawie protokołu.

10.2.1 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 zakładce *USTAWIENIA* zaznacz serwery, które będą dodane do puli.

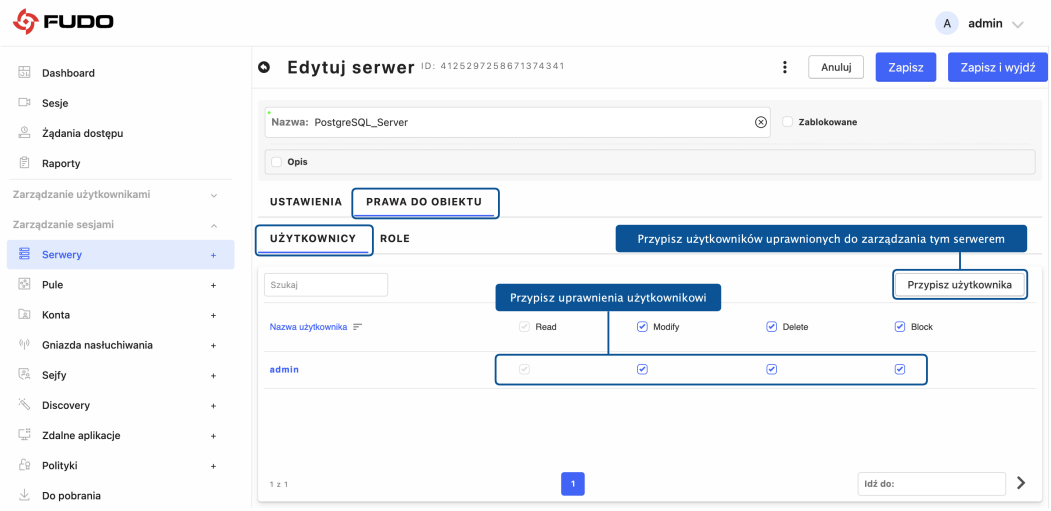
> **Uwaga**
>
> Protokół dodawanych serwerów powinien być unikalny w ramach puli.

5. Kliknij *Zapisz*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



10.2.2 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:

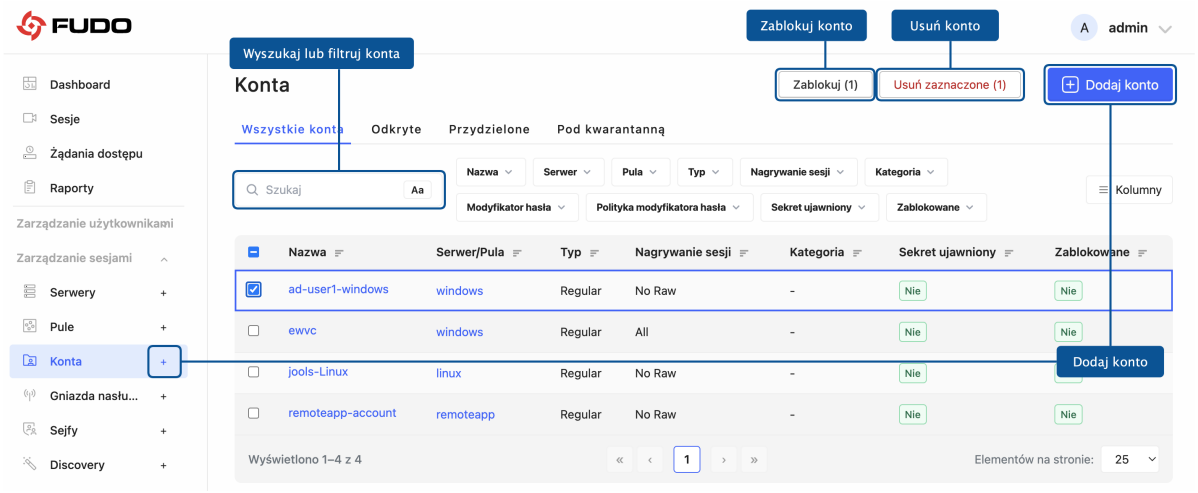
- *Model danych*
- *Dodawanie serwera*
- *Blokowanie serwera*
- *Odblokowanie serwera*
- *Usuwanie serwera*

10.3 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.

Uwaga

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.



10.3.1 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.

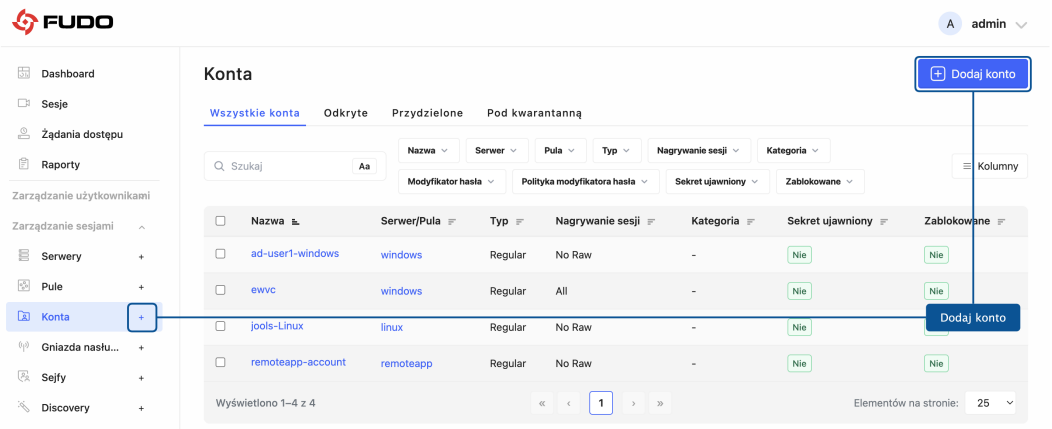
10.3.1.1 Dodawanie konta typu *anonymous*

Ostrzeżenie

Jeśli konto `anonymous` jest używane w sesji ustanowionej przez `tunel SSH`, na liście sesji wyświetlana jest nazwa użytkownika, który utworzył tunel.

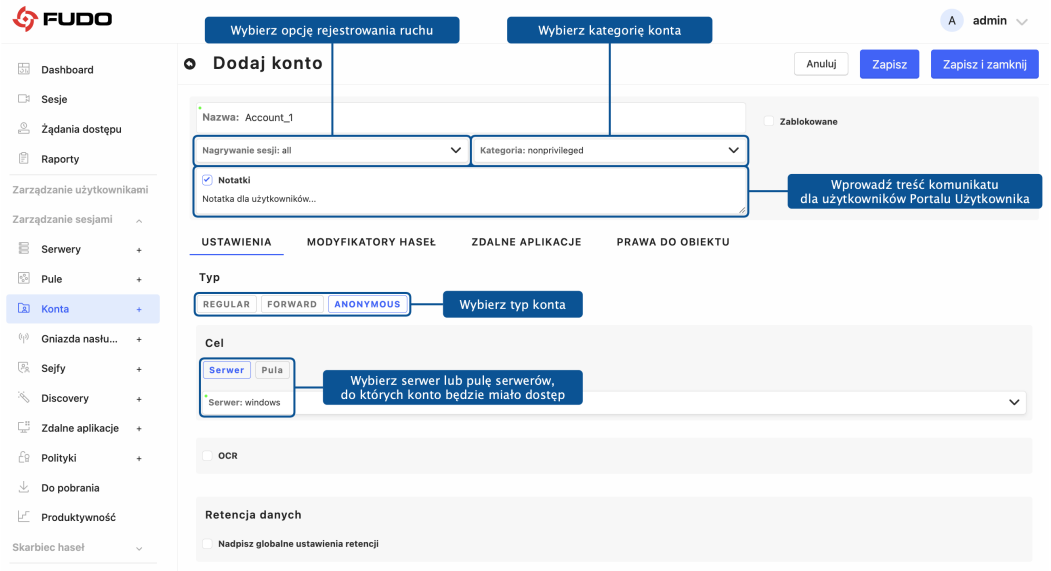
Aby utworzyć definicję konta, postępuj zgodnie z poniższymi instrukcjami.

1. Kliknij ikonę + obok zakładki *Konta* w podsekcji *Zarządzanie sesjami*, lub
2. Wybierz *Zarządzanie sesjami* > *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`.

> **Uwaga**
>
> 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 *Portalu Użytkownika*. Jeśli uprawnienia są przyznane, notatki mogą być również edytowane. Uprawnienia są nadawane z poziomu sejfu.

Uwaga

Notatki konta mogą być wyświetlane w *Portalu Użytkownika*.



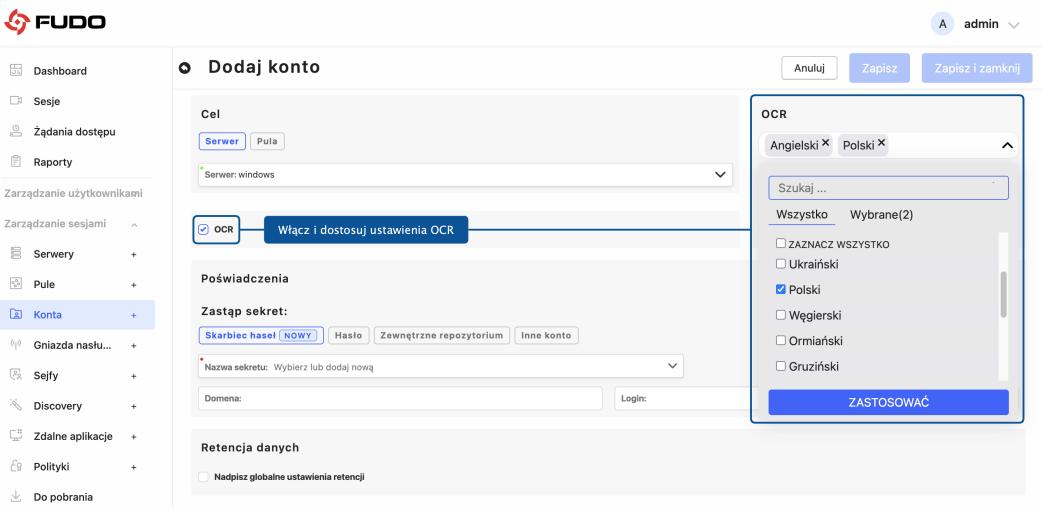
ZAKŁADKA USTAWIENIA

1. W zakładce *USTAWIENIA*, w polu Typ, naciśnij przycisk *ANONYMOUS*.
2. 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*.
3. Wybierz opcję *SSH Agent forwarding* w celu uwierzytelnienia na serwerze docelowym wykorzystując klucz SSH klienta.

Uwaga

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

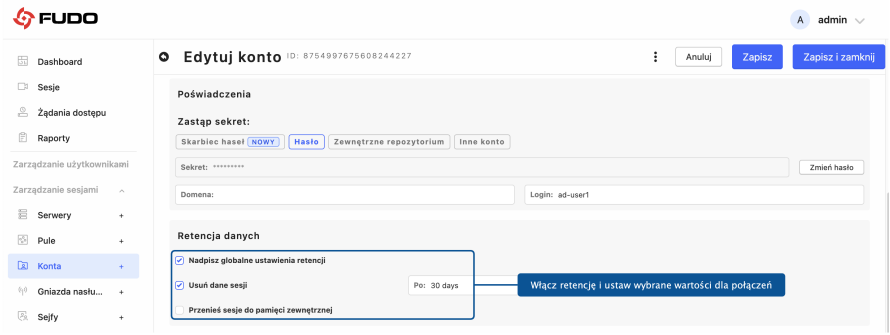
4. Aby automatycznie przetwarzać sesje RDP, VNC lub renderowane HTTP, możesz włączyć opcję *Sesja OCR* dla tego konta i wybrać język przetwarzanych danych.



Uwaga

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

5. 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.



Uwaga

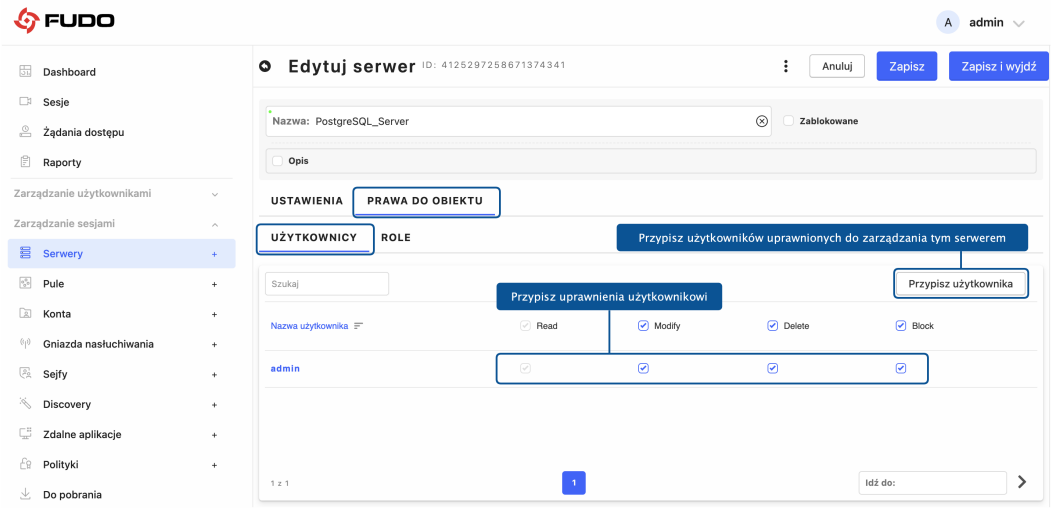
Retencja danych dla sesji nawiązanych za pośrednictwem tego konta będzie aktywna tylko w sytuacji, kiedy włączona jest opcja retencji na poziomie globalnym. W celu sprawdzenia globalnych ustawień retencji przejdź do rozdziału *Retencja danych*.

6. Kliknij *Zapisz*, aby przejść do dalszej konfiguracji.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Uwaga

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

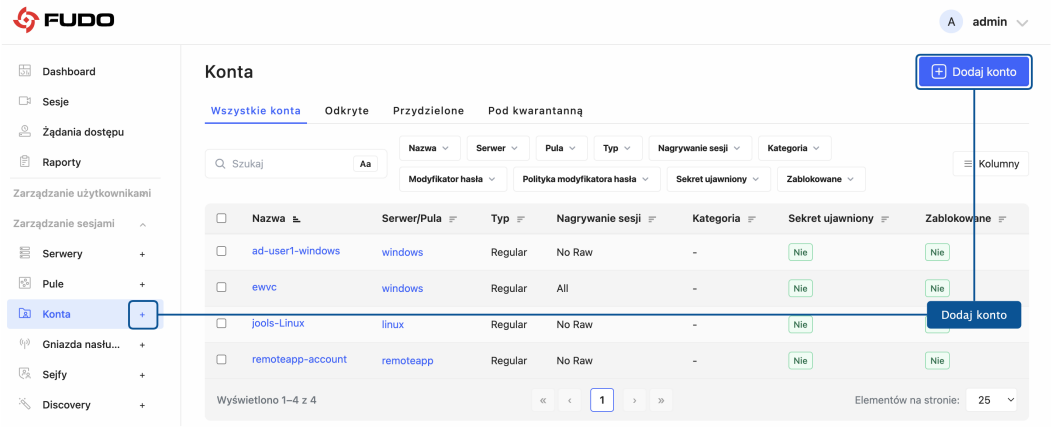
Tematy pokrewne:

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

10.3.1.2 Tworzenie konta typu *forward*

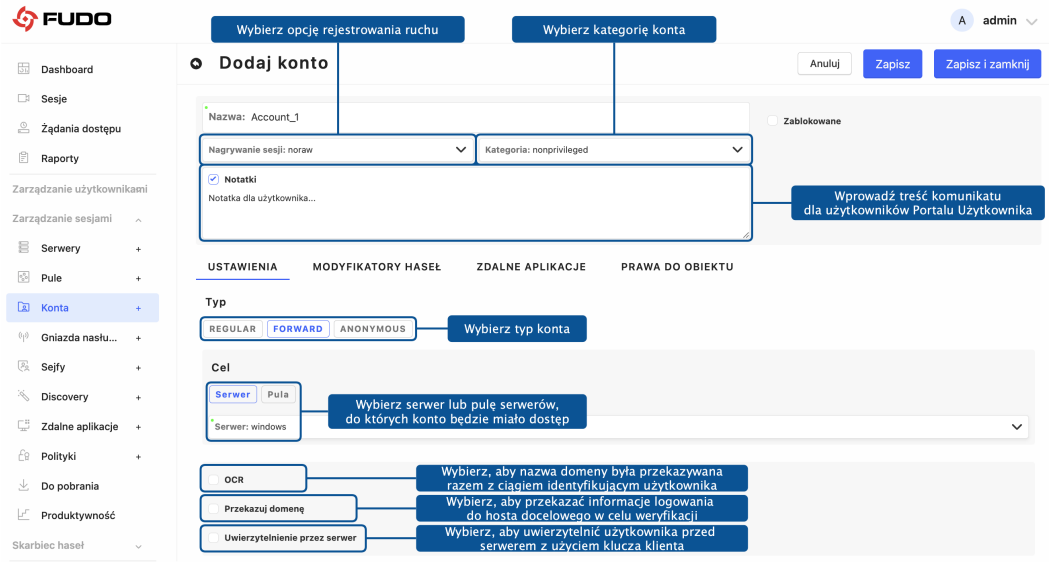
Aby utworzyć definicję konta, postępuj zgodnie z poniższymi instrukcjami.

1. Kliknij ikonę + obok zakładki *Konta* w podsekcji *Zarządzanie sesjami*, lub
2. Wybierz *Zarządzanie sesjami* > *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`.

> **Uwaga**
>
> 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 *Portalu Użytkownika*. Jeśli uprawnienia są przyznane, notatki mogą być również edytowane. Uprawnienia są nadawane z poziomu sejfu.

Uwaga

Notatki konta mogą być wyświetlane w *Portalu Użytkownika*.



ZAKŁADKA USTAWIENIA

1. W zakładce *USTAWIENIA*, w polu Typ, naciśnij przycisk *FORWARD*.
2. 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*.
3. Zaznacz opcję *Przekazuj domenę*, aby nazwa domeny była przekazywana razem z ciągiem identyfikującym użytkownika.

Uwaga

Włączona opcja *Przekazuj domenę* wykorzystuje *ustawienia domen konta użytkownika* w następujący sposób:

- 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.

4. 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 *Poświadczenia* (dostępne tylko dla serwerów MySQL, SSH oraz RDP w trybie bezpieczeństwa *Enhanced RDP Security (TLS) + NLA*.

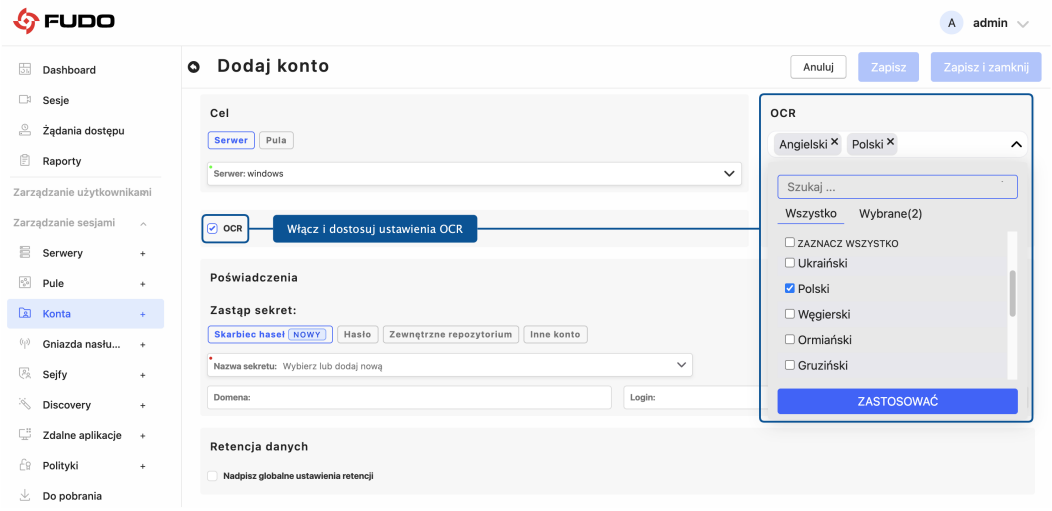
Uwaga

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.

5. Wybierz opcję *SSH Agent forwarding*, aby uwierzytelnić użytkownika przed serwerem z użyciem klucza klienta.

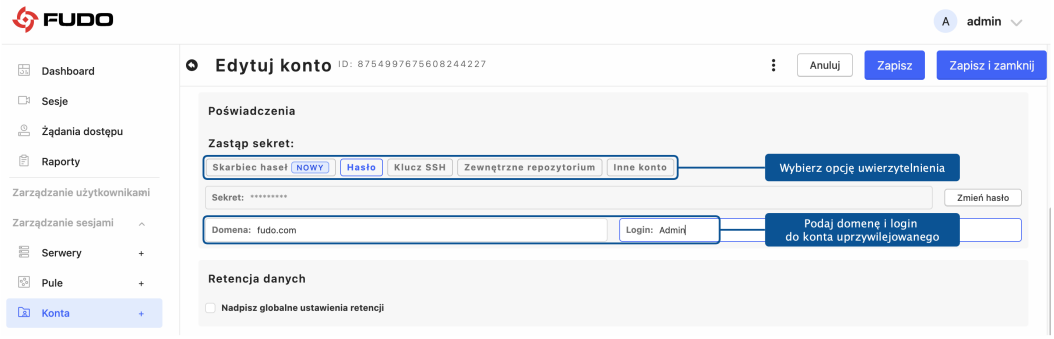
> **Uwaga**
>
> Opcja *SSH Agent forwarding* dostępna jest w przypadku wybrania serwera SSH. Zastosuj opcję -A w celu połączenia z serwerem SSH.

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



> **Uwaga**
>
> Opcja *OCR* jest dostępna tylko po wybraniu serwera RDP, VNC lub HTTP.

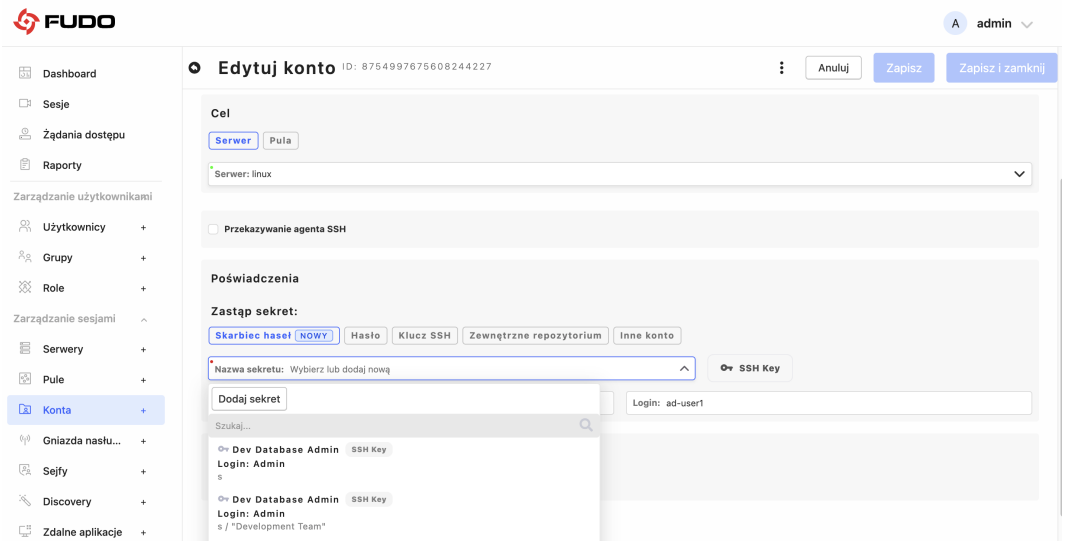
7. W sekcji *Poświadczenia* wybierz metodę zastępowania tajnego klucza. Kliknij przycisk odpowiadający jednej z wybranych opcji.



Skarbiec haseł

- Kliknij listę rozwijaną *Nazwa sekretu*, aby wyświetlić dostępne sekrety.
- Wybierz sekret z listy.
- Opcjonalnie zaznacz pola wyboru:
  - *Użyj domeny z sekretu* — używa domeny zapisanej w sekrecie

– *Użyj loginu z sekretu* — używa nazwy logowania zapisanej w sekrecie



Uwaga

Przycisk *Dodaj sekret* na liście rozwijanej wyboru sekretu umożliwia utworzenie nowego sekretu bezpośrednio z poziomu interfejsu konfiguracji konta.

Hasło

- Podaj hasło konta w polu *Sekret*.

Uwaga

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.

Uwaga

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

Inne konto

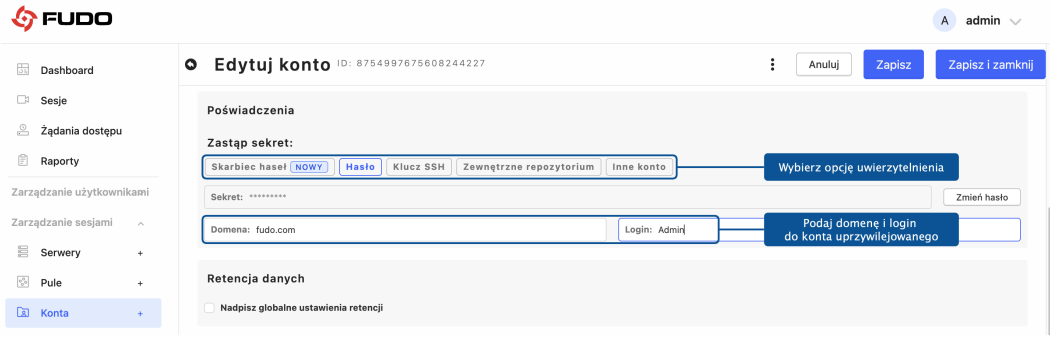
- Z listy rozwijanej *Konto* wybierz obiekt konta, którego dane uwierzytelniające będą używane do uwierzytelniania użytkownika podczas nawiązywania połączenia z monitorowanym serwerem.

> **Uwaga**
>
> Lista zawiera tylko obiekty, do których masz uprawnienia dostępu.

Brak

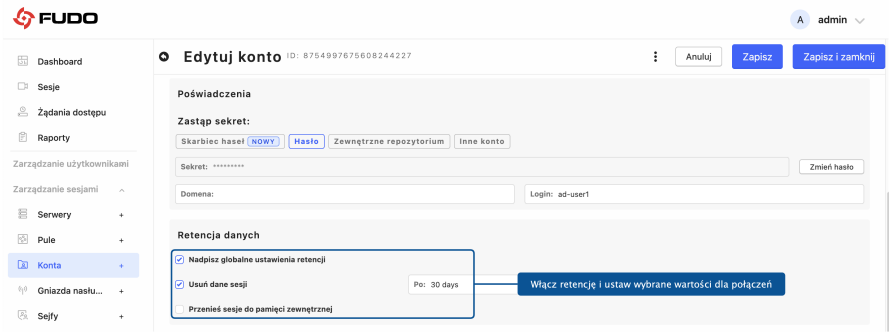
- W takim przypadku żadne dane uwierzytelniające nie będą przesyłane.

8. W polu *Domena* wprowadź domenę konta uprzywilejowanego.



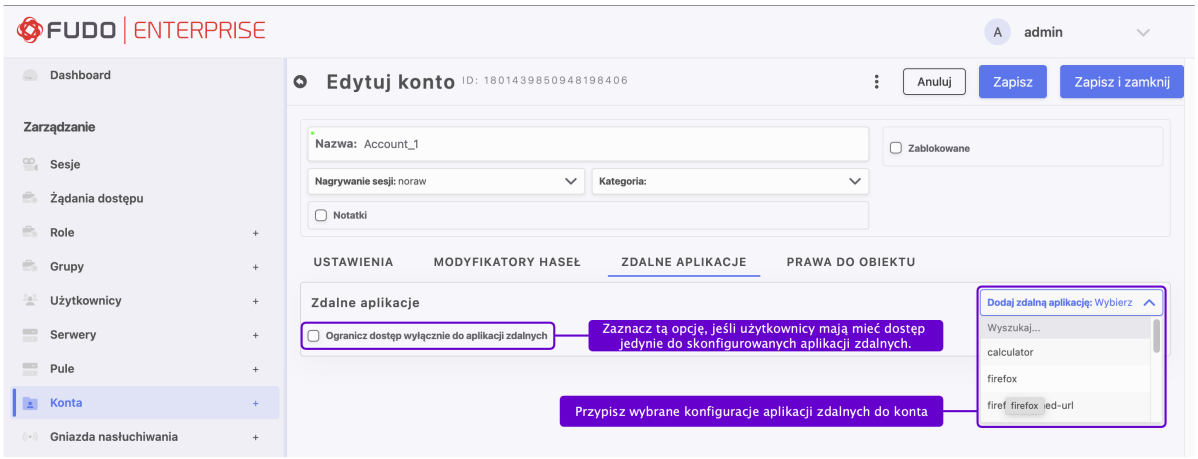
> **Uwaga**
>
> Jeśli domena zostanie wprowadzona w polu *Domena*, Fudo Enterprise zawsze użyje jej do uwierzytelniania wobec serwera. Domena zostanie automatycznie dodana do logowania użytkownika.

9. 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.



ZAKŁADKA ZDALNE APLIKACJE

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



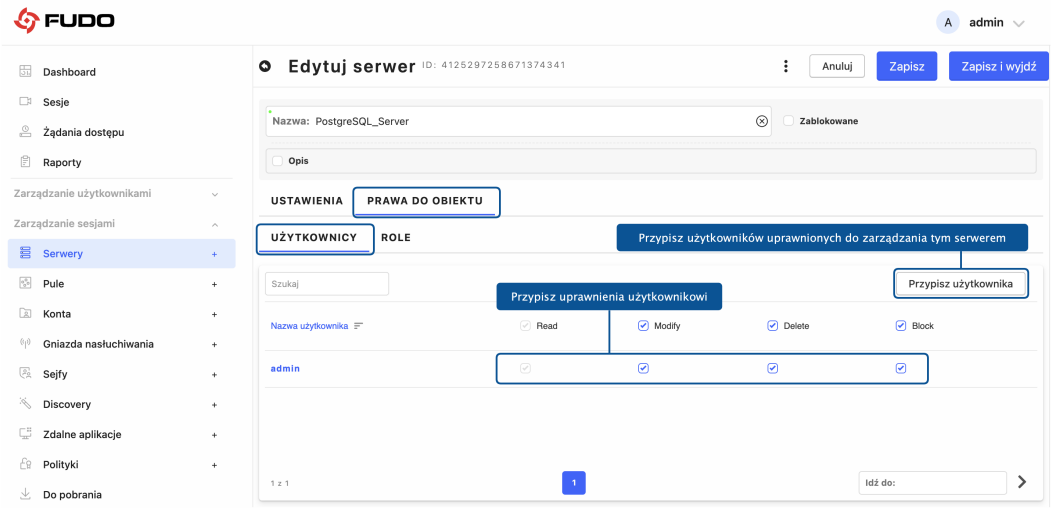
Uwaga

Aby dowiedzieć się więcej o definiowaniu aplikacji zdalnych oraz ograniczaniu pełnego dostępu do pulpitu, zapoznaj się z rozdziałem *Zdalne aplikacje*.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



Uwaga

- Zakładka *ZDALNE APLIKACJE* 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*.

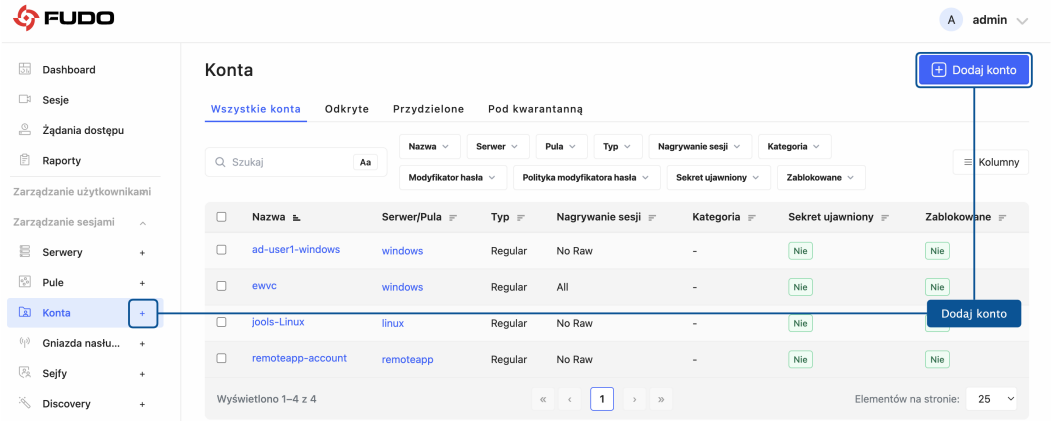
Tematy pokrewne:

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

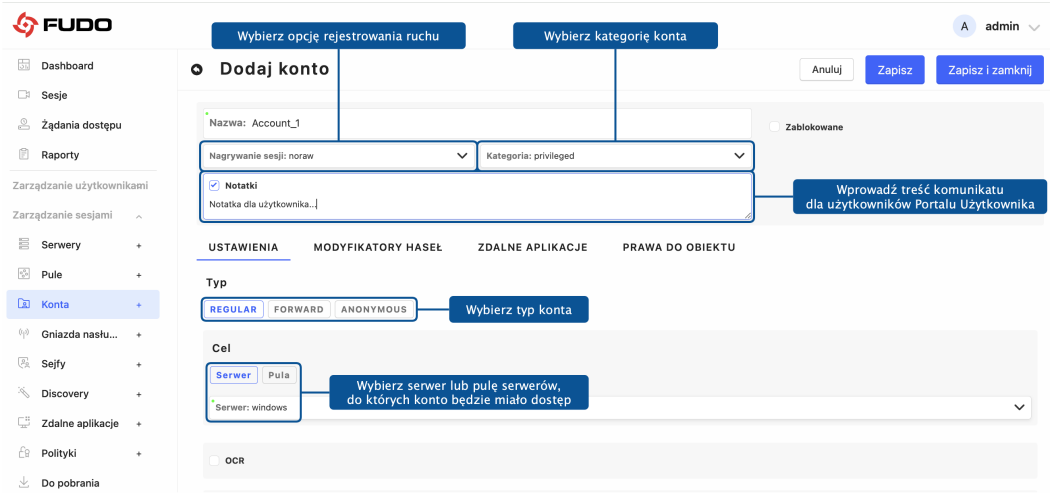
10.3.1.3 Tworzenie konta typu *regular*

Aby utworzyć definicję konta, postępuj zgodnie z poniższymi instrukcjami.

1. Kliknij ikonę + obok zakładki *Konta* w podsekcji *Zarządzanie sesjami*, lub
2. Wybierz *Zarządzanie sesjami* > *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`.

Uwaga

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 *Portalu Użytkownika*. Jeśli uprawnienia są przyznane, notatki mogą być również edytowane. Uprawnienia są nadawane z poziomu sejfu.

Uwaga

Notatki konta mogą być wyświetlane w *Portalu Użytkownika*.



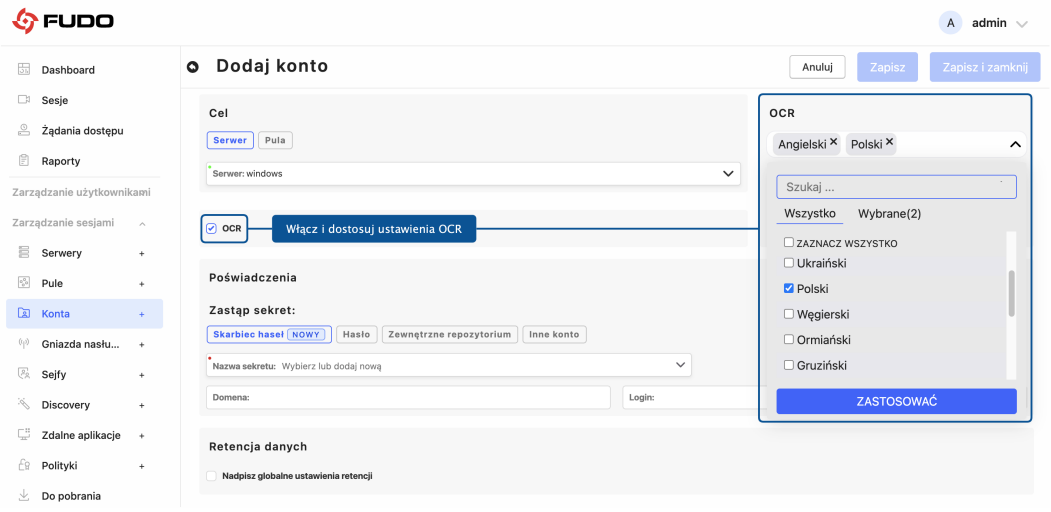
ZAKŁADKA USTAWIENIA

1. W zakładce *USTAWIENIA*, w polu Typ, naciśnij przycisk *REGULAR*.
2. 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*.
3. Wybierz opcję *SSH Agent forwarding*, aby uwierzytelnić użytkownika przed serwerem z użyciem klucza klienta.

Uwaga

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

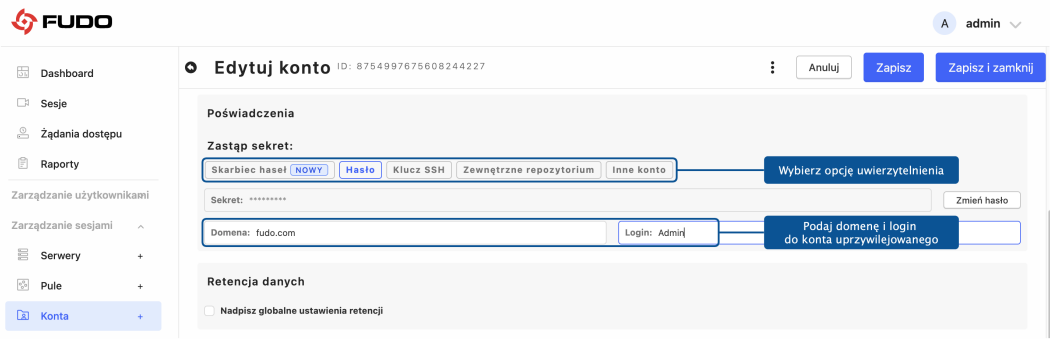
4. Aby automatycznie przetwarzać sesje RDP, VNC lub renderowane HTTP, możesz włączyć opcję *Sesja OCR* dla tego konta i wybrać język przetwarzanych danych.



Uwaga

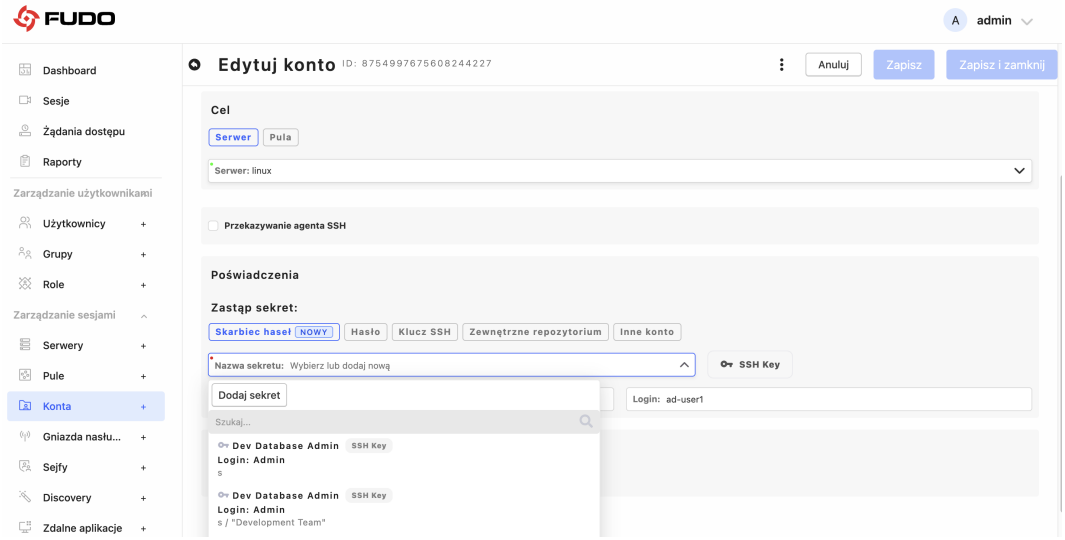
Opcja *OCR* jest dostępna tylko po wybraniu serwera RDP, VNC lub HTTP.

5. W sekcji *Poświadczenia* wybierz metodę zastępowania tajnego klucza. Kliknij przycisk odpowiadający jednej z wybranych opcji.



Skarbiec haseł

- Kliknij listę rozwijaną *Nazwa sekretu*, aby wyświetlić dostępne sekrety.
- Wybierz sekret z listy.
- Opcjonalnie zaznacz pola wyboru:
  - *Użyj domeny z sekretu* — używa domeny zapisanej w sekrecie
  - *Użyj loginu z sekretu* — używa nazwy logowania zapisanej w sekrecie



> **Uwaga**
>
> Przycisk *Dodaj sekret* na liście rozwijanej wyboru sekretu umożliwia utworzenie nowego sekretu bezpośrednio z poziomu interfejsu konfiguracji konta.

Hasło

- Podaj hasło konta w polu *Sekret*.

> **Uwaga**
>
> *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.

Uwaga

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

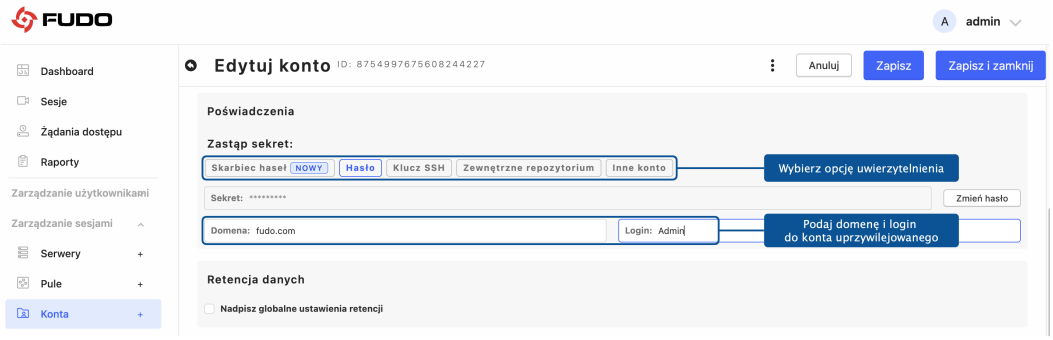
Inne konto

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

Uwaga

Lista zawiera tylko obiekty, do których masz uprawnienia dostępu.

6. W polu *Domena* wprowadź domenę konta uprzywilejowanego.



Uwaga

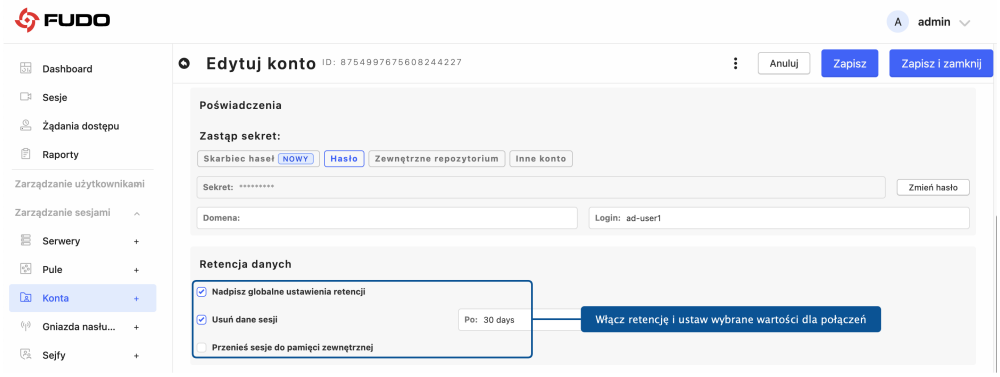
Jeśli domena zostanie wprowadzona w polu *Domena*, Fudo Enterprise zawsze użyje jej do uwierzytelniania wobec serwera. Domena zostanie automatycznie dodana do logowania użytkownika.

7. W polu *Login* wprowadź login do konta uprzywilejowanego.

Ostrzeżenie

Dla kont typu *regular* z pustym loginem **domena nie jest obsługiwana.** Próba zapisania takiej konfiguracji spowoduje wyświetlenie błędu. Jeśli takie konto już istnieje, wartość pola **Domena** zostanie **automatycznie usunięta podczas aktualizacji** do wersji zawierającej ten mechanizm veryfikacji (Fudo Enterprise 5.5.8 i nowsze).

8. 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.



9. Jeśli wybrano opcję Hasło jako metodę uwierzytelniania, skonfiguruj dodatkowo zakładkę *Modyfikatory haseł*. W przeciwnym przypadku przejdź od razu do sekcji opisującej konfigurację *aplikacji zdalnych*.

Uwaga

Zakładka *MODYFIKATORY HASEŁ* jest aktywna tylko podczas tworzenia konta *regular* z wybraną metodą *Hasło* i podanym loginem do konta uprzywilejowanego w sekcji *Poświadczenia*.

ZAKŁADKA MODYFIKATORY HASEŁ

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

Uwaga

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

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

Uwaga

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

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

Uwaga

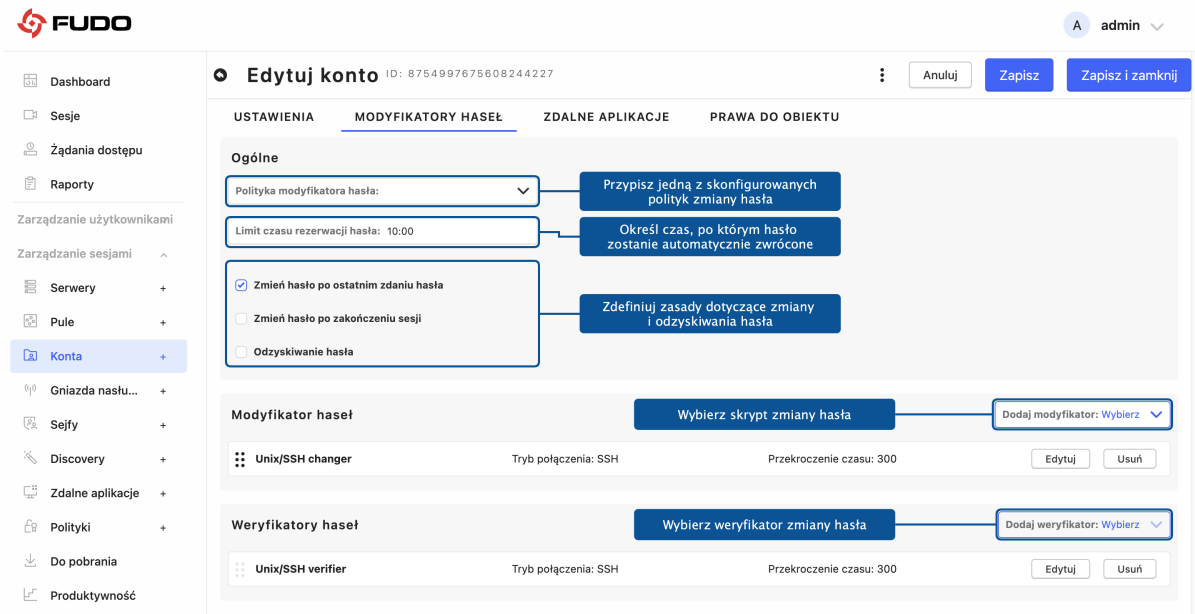
Opcja ta wymaga wybrania co najmniej jednego *Modyfikatora hasła* i *Polityki zmiany haseł* **innej niż** `Static, without restrictions`.

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

5. 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.

Uwaga

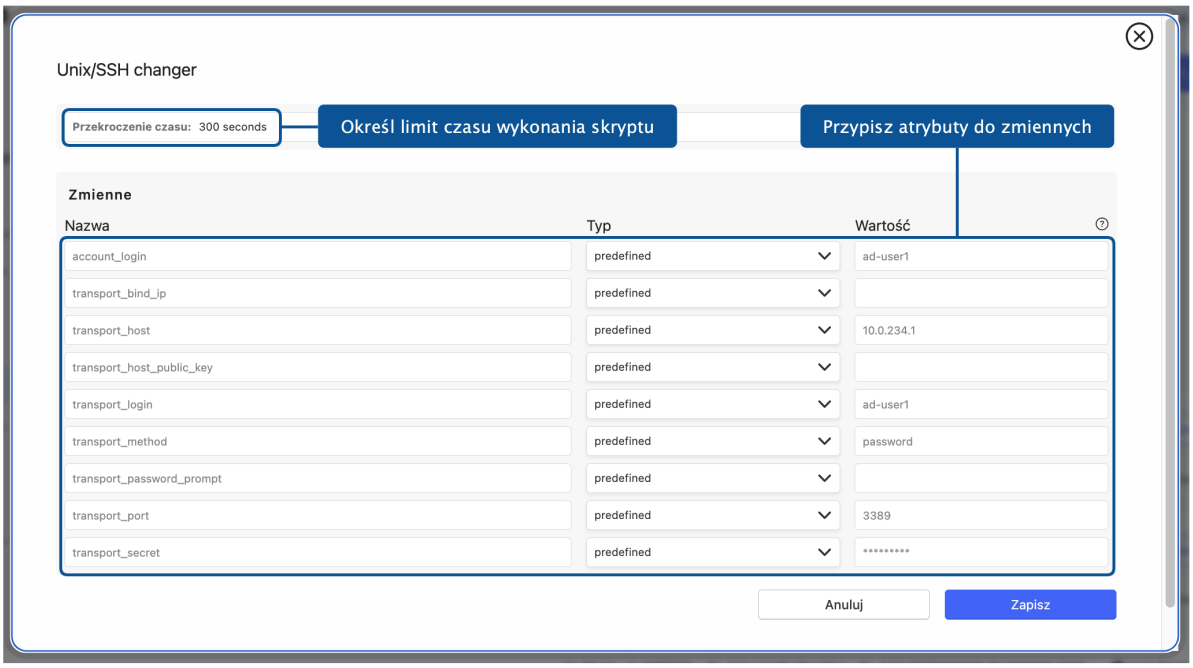
Po włączeniu opcji *Odzyskiwanie hasła*, *Weryfikator Haseł* uruchamia akcję „Trigger password changer" na koncie. Kiedy opcja ta jest wyłączona, *Weryfikator Haseł* wysyła komunikat: „Nie udało się zweryfikować hasła dla konta <nazwa_konta>".



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

Ostrzeżenie

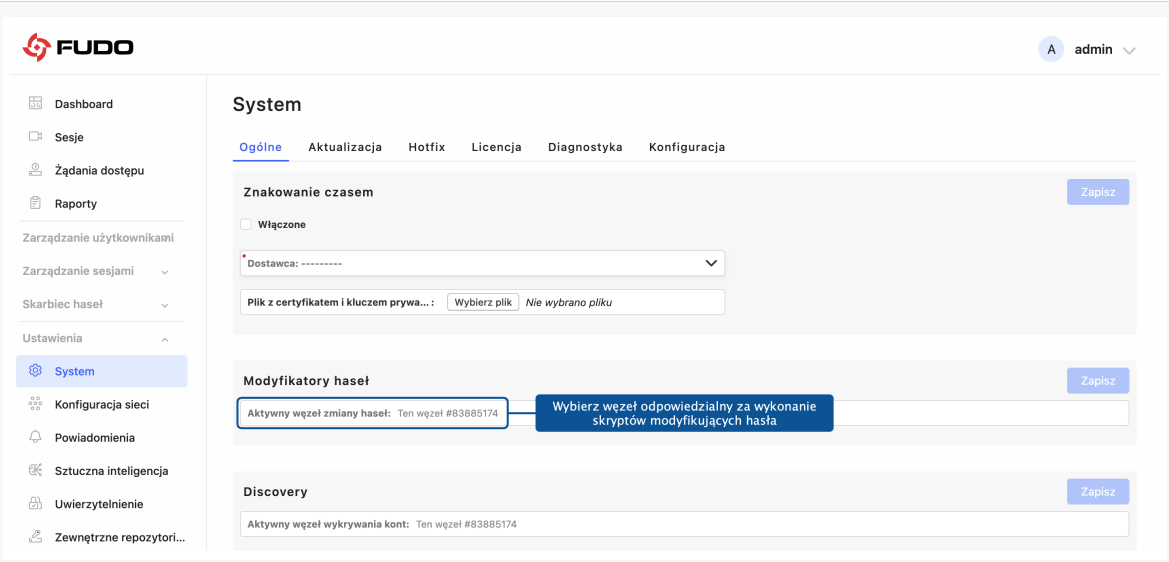
Do przeprowadzania zmiany haseł należy użyć konta (`transport_login` i `transport_secret`), które ma delegowane uprawnienia *Reset user passwords and force password change at next logon* dla *Organizational Unit (OU)* zawierającej użytkowników, których hasła będą zmieniane, lub konto musi należeć do grupy *Account Operators*.



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

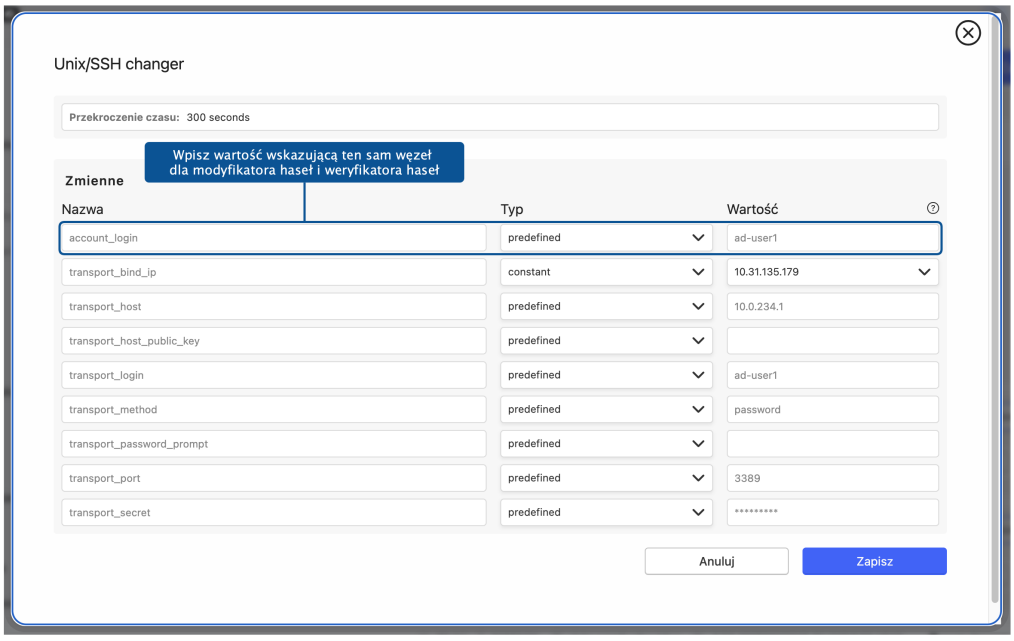
Uwaga

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:

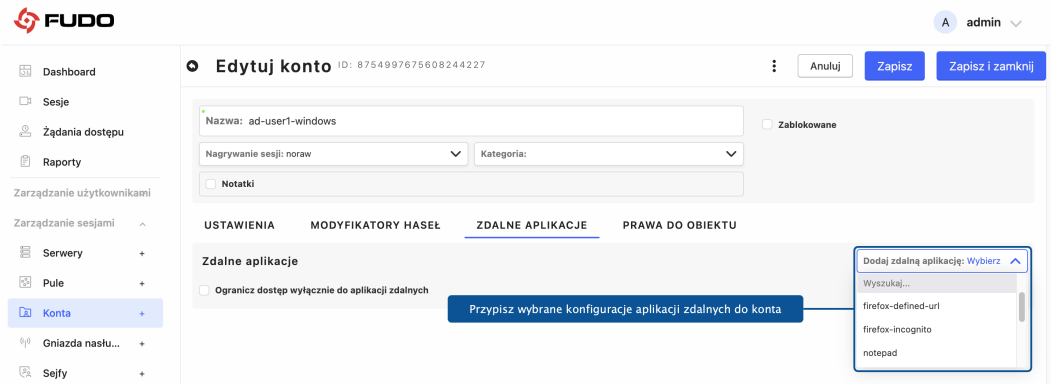
- Definiując Modyfikator / Weryfikator hasła dla konta, wartość zmiennej `transport_bind_ip` powinna wskazywać ten sam węzeł dla wszystkich Modyfikatorów oraz Weryfikatorów hasła.



- 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*.

ZAKŁADKA ZDALNE APLIKACJE

W zakładce *APLIKACJE ZDALNE* możesz przypisać do konta wybrane konfiguracje aplikacji zdalnych, umożliwiając bezpośrednie połączenia RDP przy ich użyciu.



Uwaga

Aby dowiedzieć się więcej o definiowaniu aplikacji zdalnych oraz ograniczaniu pełnego dostępu do pulpitu, zapoznaj się z rozdziałem *Zdalne aplikacje*.

Uwaga

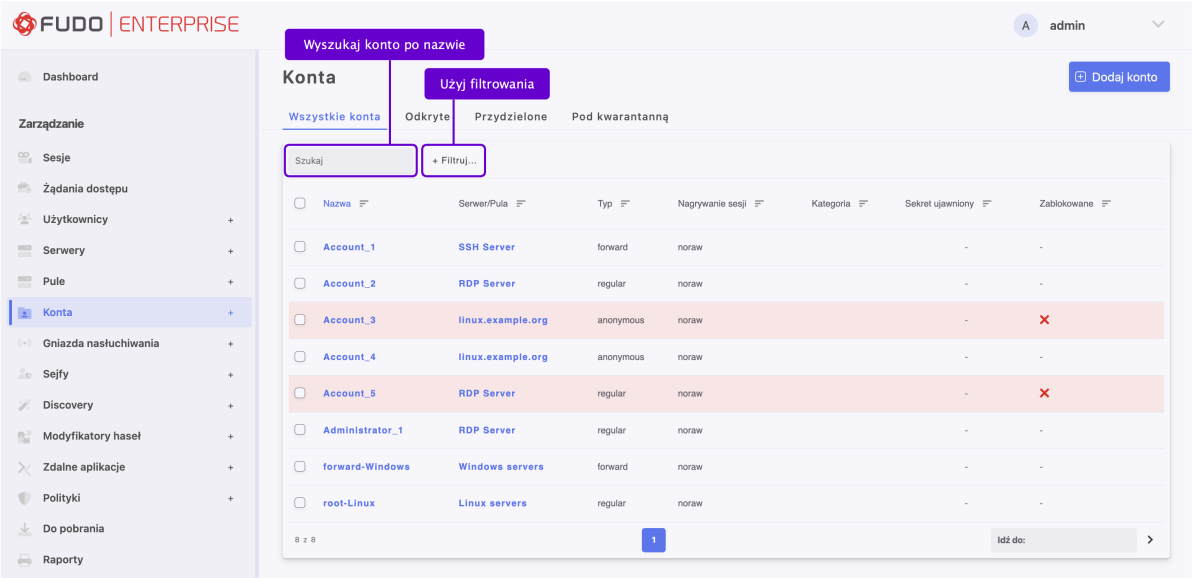
Zakładka *ZDALNE APLIKACJE* jest aktywna tylko podczas tworzenia konta typu *forward* lub *regular* z przypisanym serwerem lub pulą RDP.

Tematy pokrewne:

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

10.3.2 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:

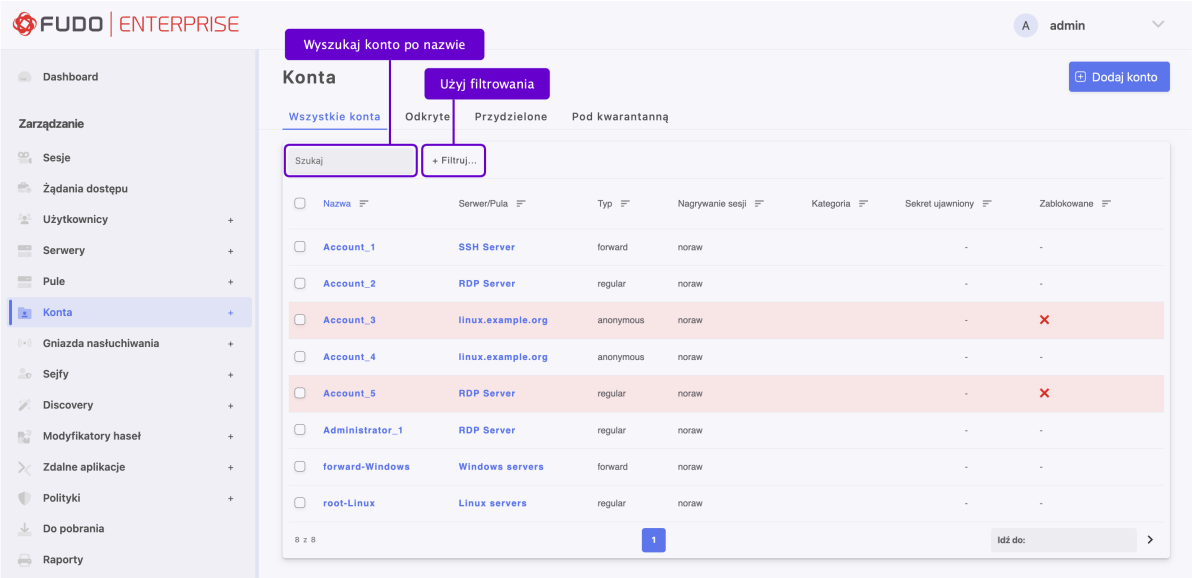
- *Dodawanie konta*
- *Blokowanie konta*
- *Odblokowywanie konta*
- *Usuwanie konta*

10.3.3 Blokowanie konta

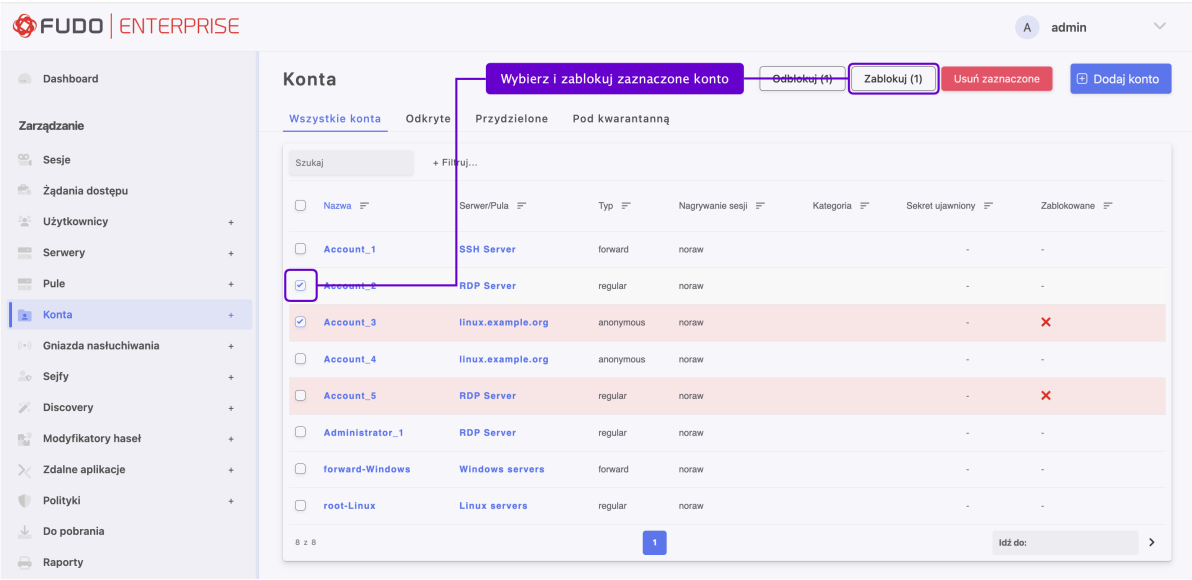
Ostrzeżenie

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*.

Uwaga

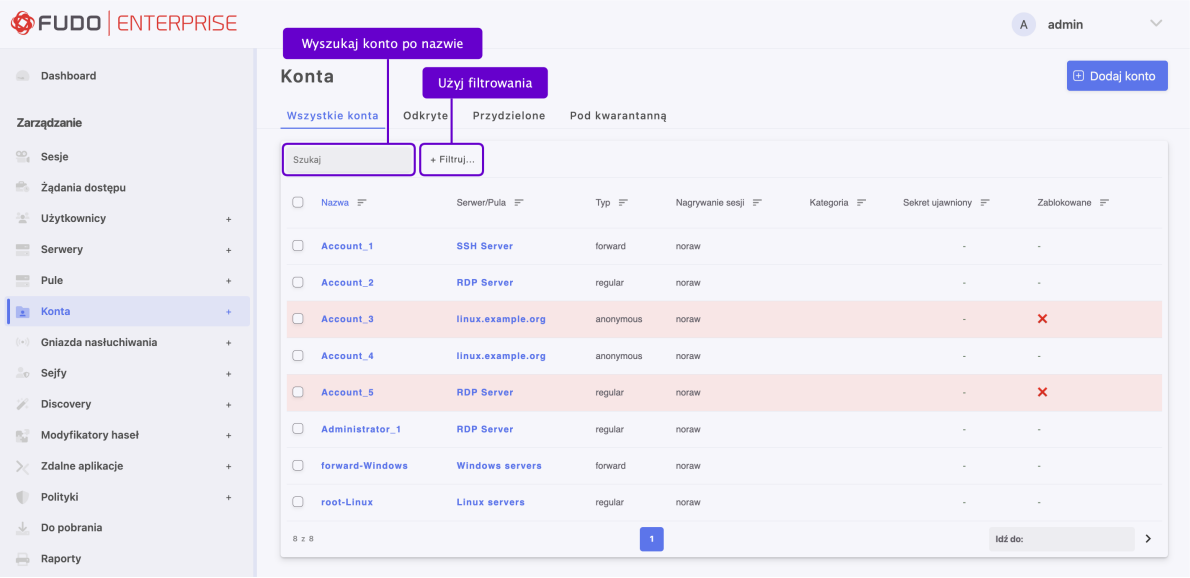
Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę czerwonego krzyżyka.

Tematy pokrewne:

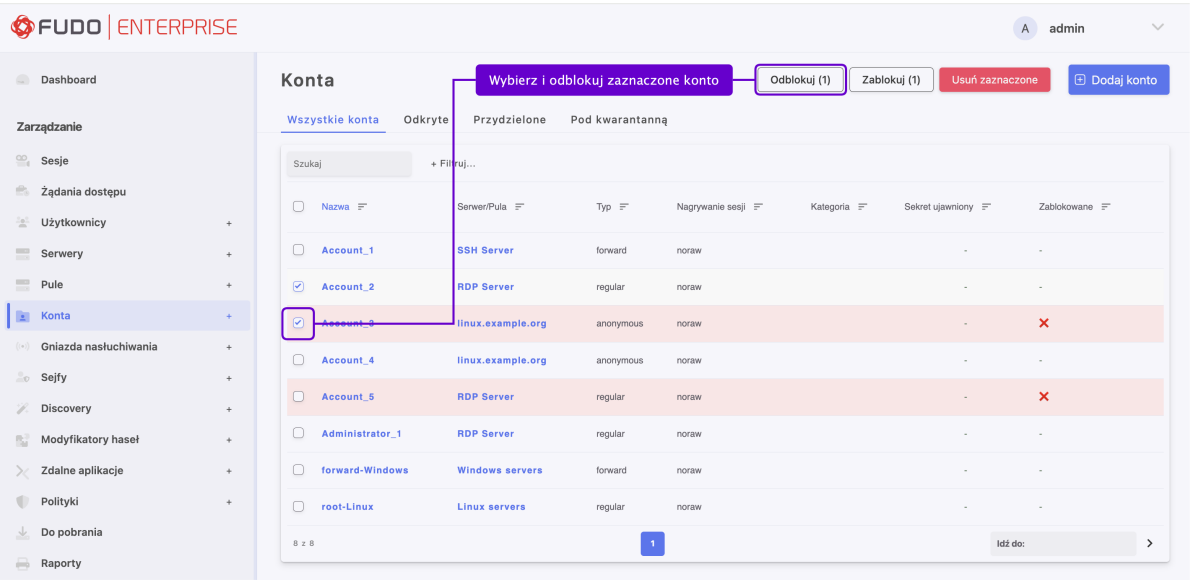
- *Dodawanie konta*
- *Edytowanie konta*
- *Odblokowywanie konta*
- *Usuwanie konta*

10.3.4 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:

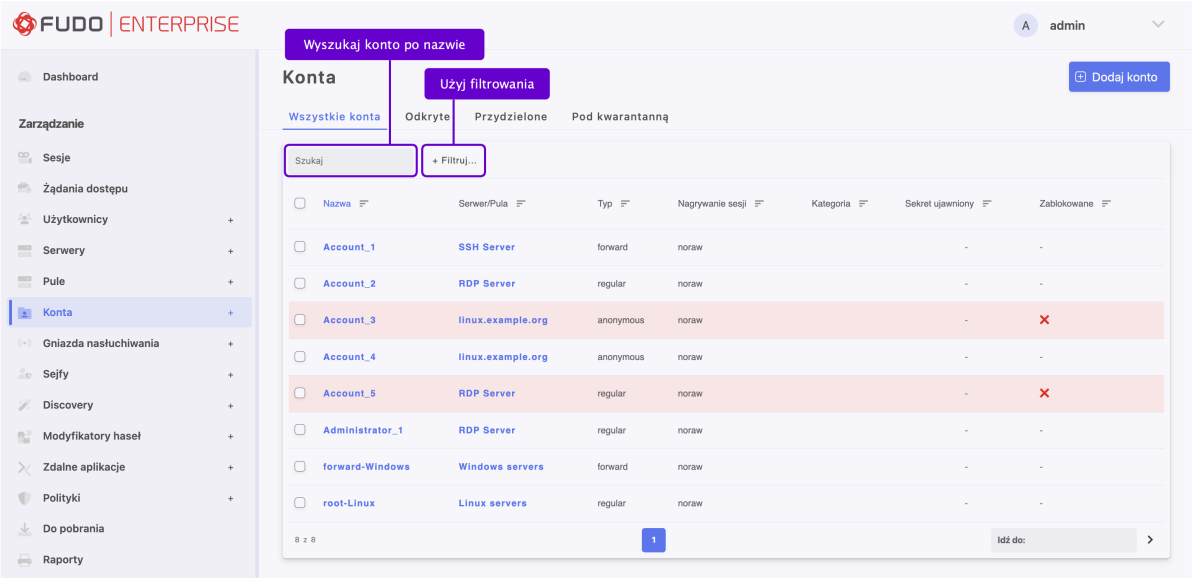
- *Blokowanie konta*
- *Dodawanie konta*
- *Edytowanie konta*
- *Usuwanie konta*

10.3.5 Usuwanie konta

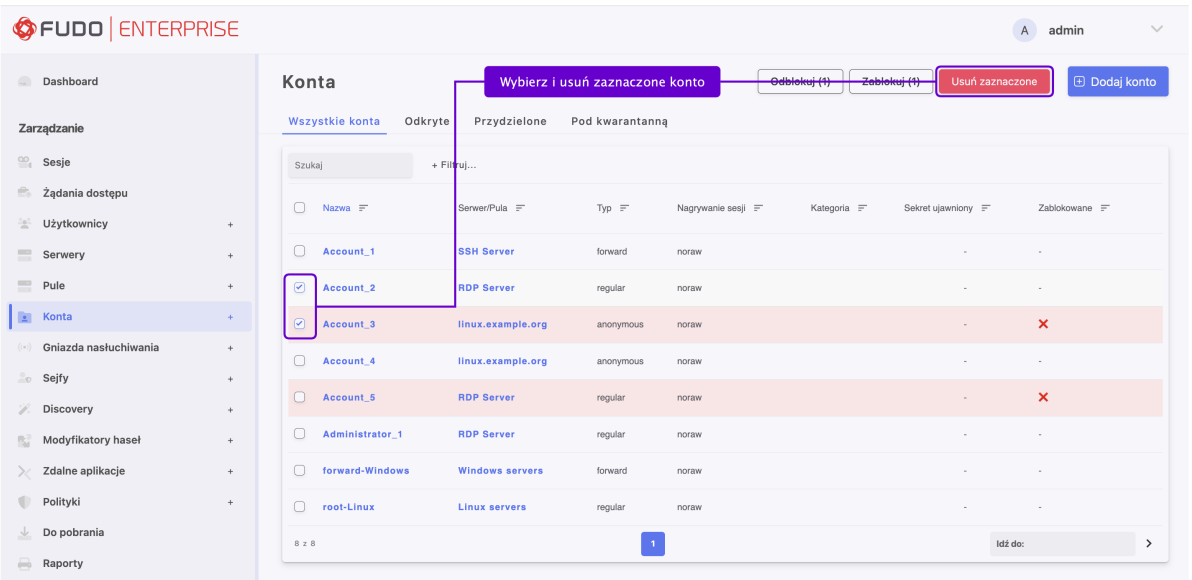
Ostrzeżenie

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*

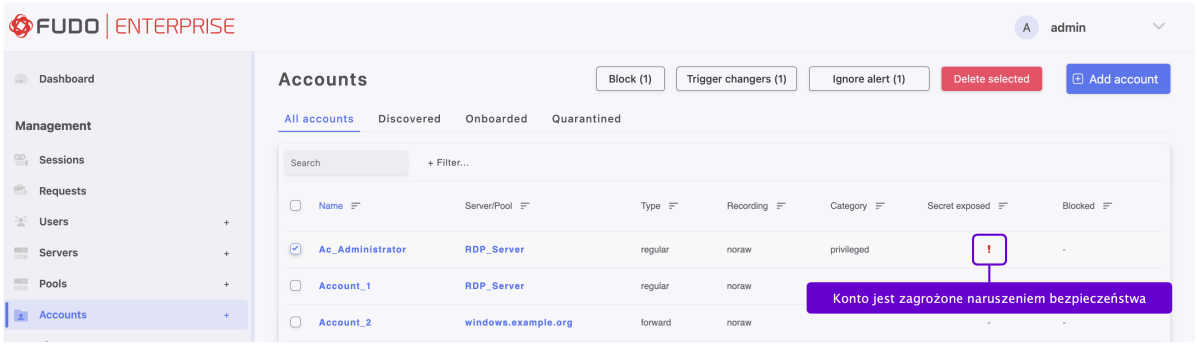
- *Edytowanie konta*
- *Blokowanie konta*
- *Odblokowywanie konta*

10.3.6 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.

Uwaga

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

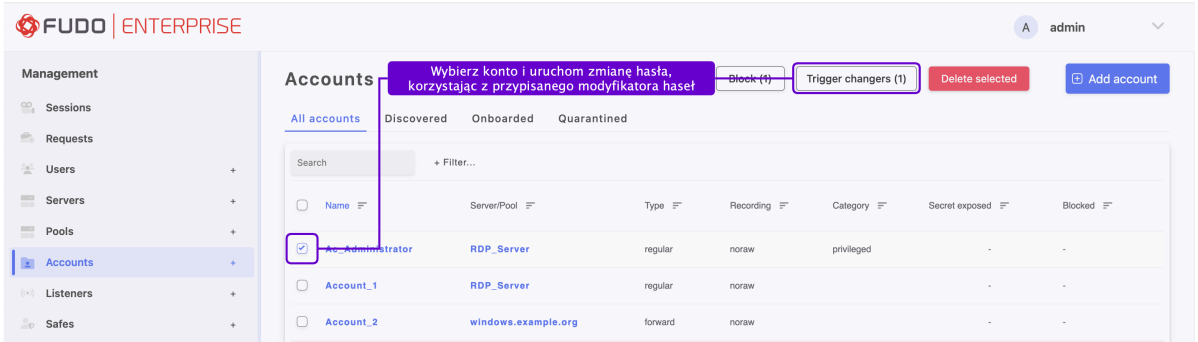


Administrator może zignorować alarm dla wybranego konta lub wymusić zmianę hasła za pomocą przypisanego *modyfikatora haseł*.

10.3.6.1 Zmiana hasła konta

Zmiana hasła z poziomu listy kont

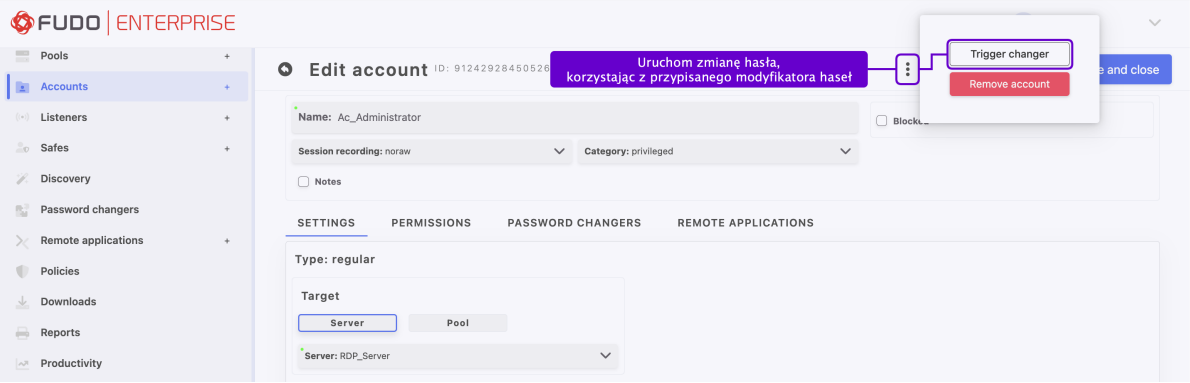
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i zaznacz konta, dla których chcesz zmienić hasło.
3. Kliknij *Aktywuj modyfikatory*.



4. Kliknij *Zatwierdź*.

Zmiana hasła z poziomu formularza edycji konta

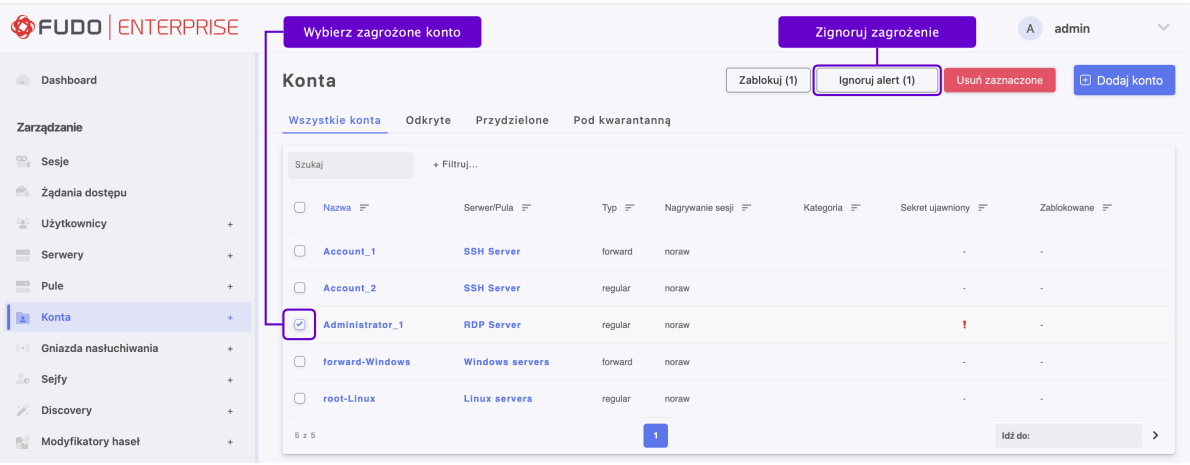
1. Wybierz z lewego menu *Zarządzanie* > *Konta*.
2. Odszukaj na liście i kliknij wybrane konto, aby otworzyć formularz edycji.
3. Kliknij symbol trzech kropek przed przyciskami *Anuluj* i *Zapisz*, aby odsłonić dodatkowe menu, a następnie kliknij *Aktywuj modyfikator*.



10.3.6.2 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*.

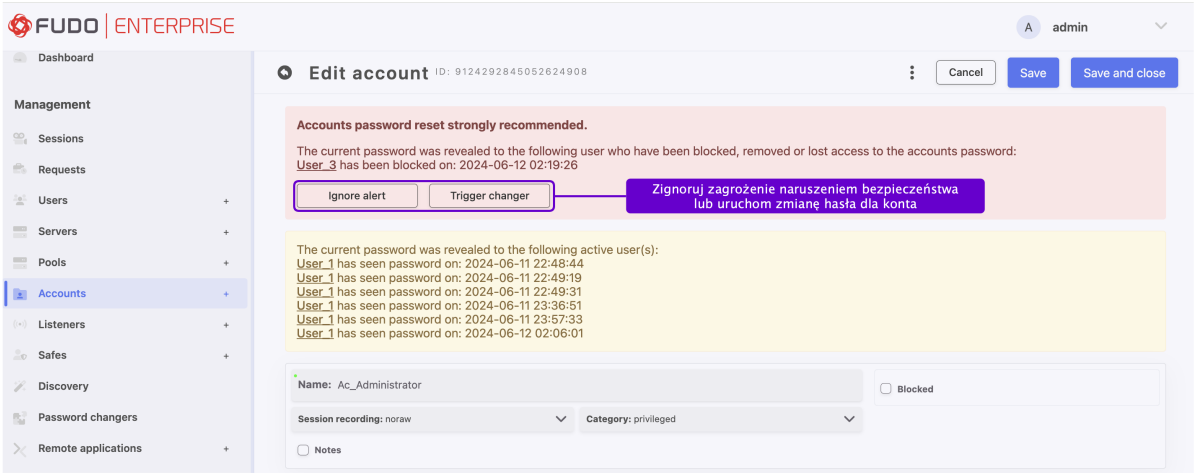


4. Kliknij *Zatwierdź*.

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.

> **Uwaga**
>
> Formularz edycji konta zawiera listę zablokowanych użytkowników, którzy widzieli aktualne hasło.



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

Tematy pokrewne:

- *Modyfikatory haseł*
- *Portal Użytkownika*

10.4 Gniazda nasłuchiwania

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

10.4.1 Dodawanie gniazda nasłuchiwania

Ostrzeżenie

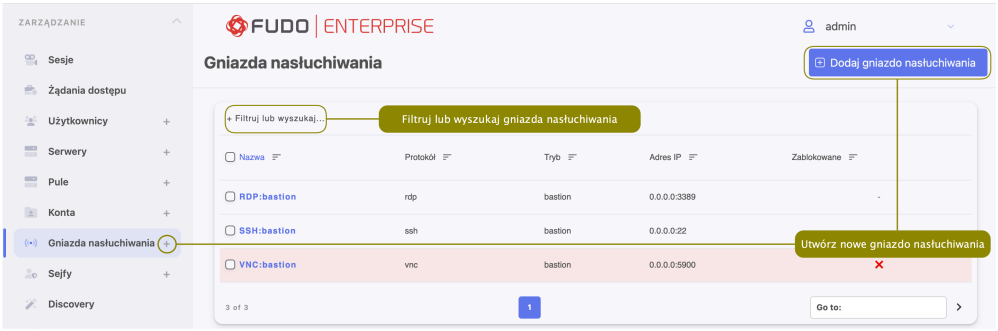
Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i **nie należy dodawać ich ręcznie** na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.

Uwaga

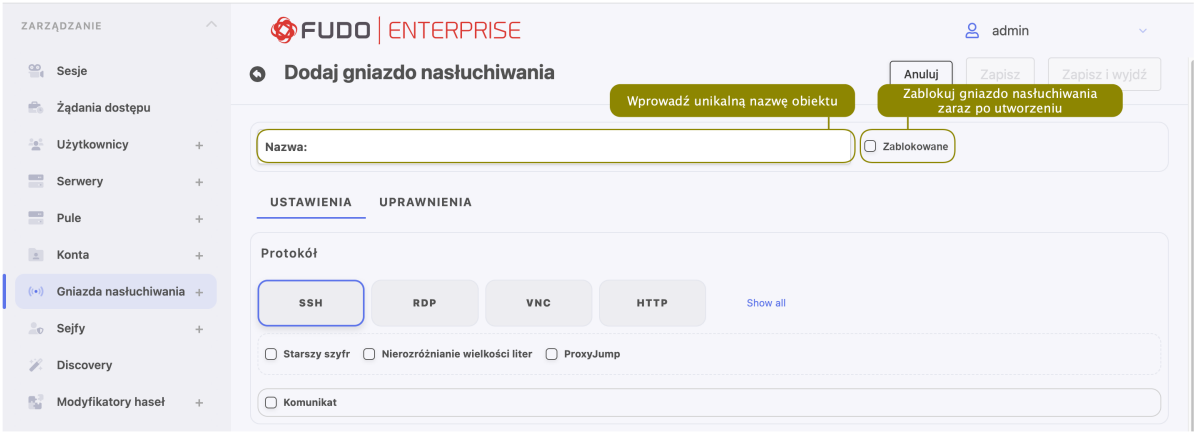
- Gniazdo nasłuchiwania nie może być skojarzone z kontem przypisanym do serwera o protokole innym niż protokół gniazda nasłuchiwania.
- Gniazdo nasłuchiwania typu *proxy* może być skojarzone tylko z jednym serwerem.
- Gniazdo nasłuchiwania typu *bastion* nie może być skojarzone z kontem anonimowym.
- 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 ikonę + w menu głównym obok zakładki *Gniazda nasłuchiwania* w podsekcji *Zarządzanie*, lub
2. Wybierz *Zarządzanie* > *Gniazda nasłuchiwania*, a następnie kliknij + *Dodaj*.



2. Wprowadź unikalną nazwę obiektu.
3. Zaznacz opcję *Zablokowane*, aby gniazdo było niedostępne po utworzeniu.



4. Wybierz odpowiedni rozdział poniżej, aby kontynuować konfigurację gniazda nasłuchiwania dla wybranego protokołu:

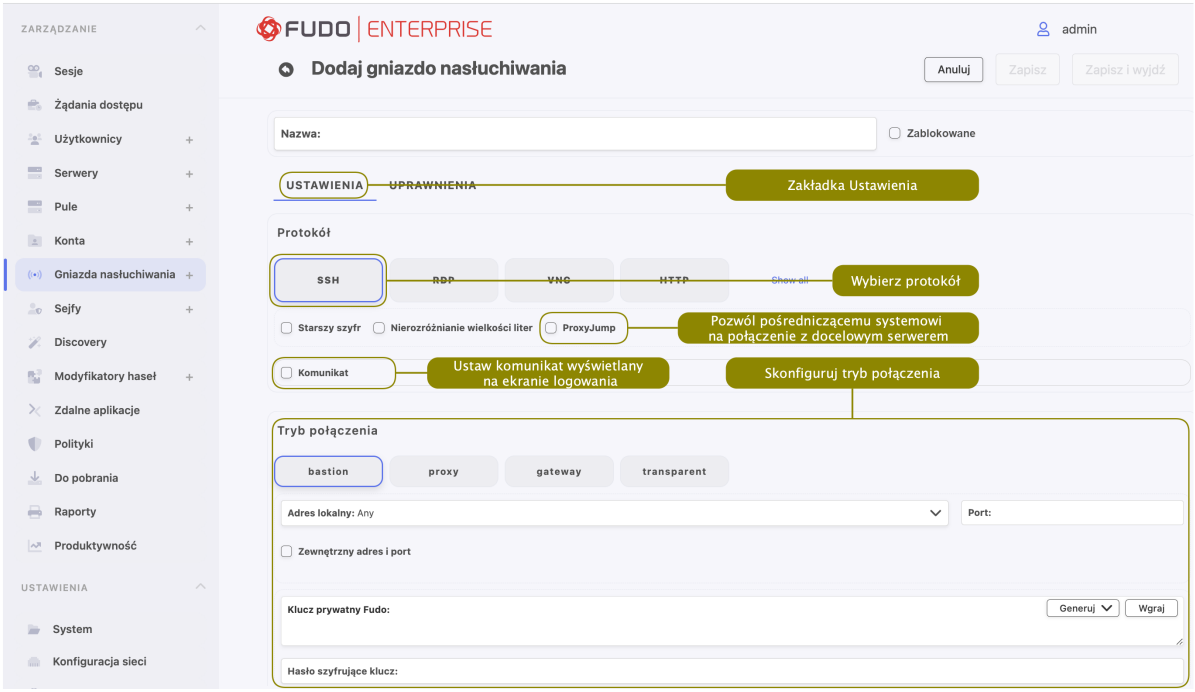
- *Konfigurowanie gniazda nasłuchiwania SSH*
- *Konfigurowanie gniazda nasłuchiwania RDP*
- *Konfigurowanie gniazda nasłuchiwania VNC*
- *Konfigurowanie gniazda nasłuchiwania HTTP*
- *Konfigurowanie gniazda nasłuchiwania Modbus*
- *Konfigurowanie gniazda nasłuchiwania MySQL*
- *Setting up the PostgreSQL listener*
- *Konfigurowanie gniazda nasłuchiwania TCP*
- *Konfigurowanie gniazda nasłuchiwania MS SQL*
- *Konfigurowanie gniazda nasłuchiwania Telnet*

- *Konfigurowanie gniazda nasłuchiwania Telnet 3270*
- *Konfigurowanie gniazda nasłuchiwania Telnet 5250*

10.4.1.1 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.

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

Tryb: bastion

Uwaga

- 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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy 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.

Uwaga

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

Tryb: proxy

Uwaga

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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy 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.

Tryb: tunnel

Uwaga

Użytkownik łączy się z serwerem docelowym przez tunel SSH.

- Wciśnij przycisk `tunnel` w polu *Tryb połączenia*.
- Z listy rozwijalnej *Adres lokalny* wybierz adres IP i podaj port.

Uwaga

- W polu **Klucze** widoczne są wygenerowane automatycznie klucze SSH, TLS i Standard RDP Security oraz certyfikat TLS potrzebne do prawidłowej pracy gniazda typu „Tunel". Można tu również wgrać własne klucze i certyfikat.
- Rozdział *Nawiązywanie połączeń z serwerami przez tunel SSH w Fudo Enterprise* zawiera przykłady nawiązywania tego typu połączeń dla wybranych protokołów.

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*.

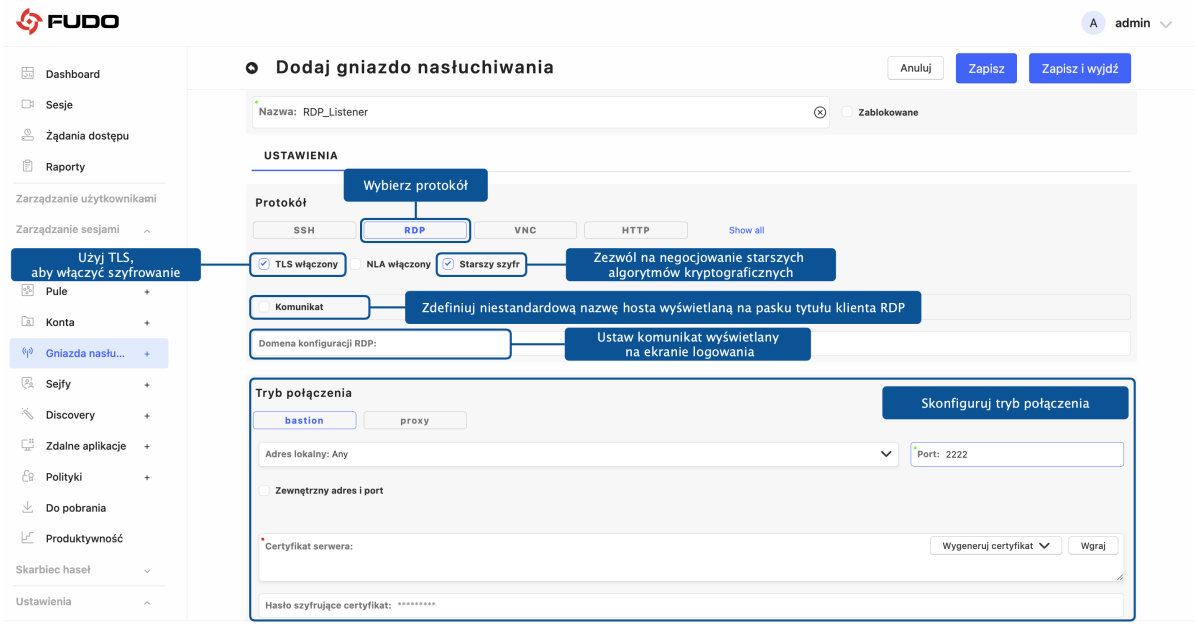
Tematy pokrewne:

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

10.4.1.2 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.

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

Tryb: bastion

Uwaga

- 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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy 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.

Uwaga

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

Tryb: proxy

Uwaga

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.

Uwaga

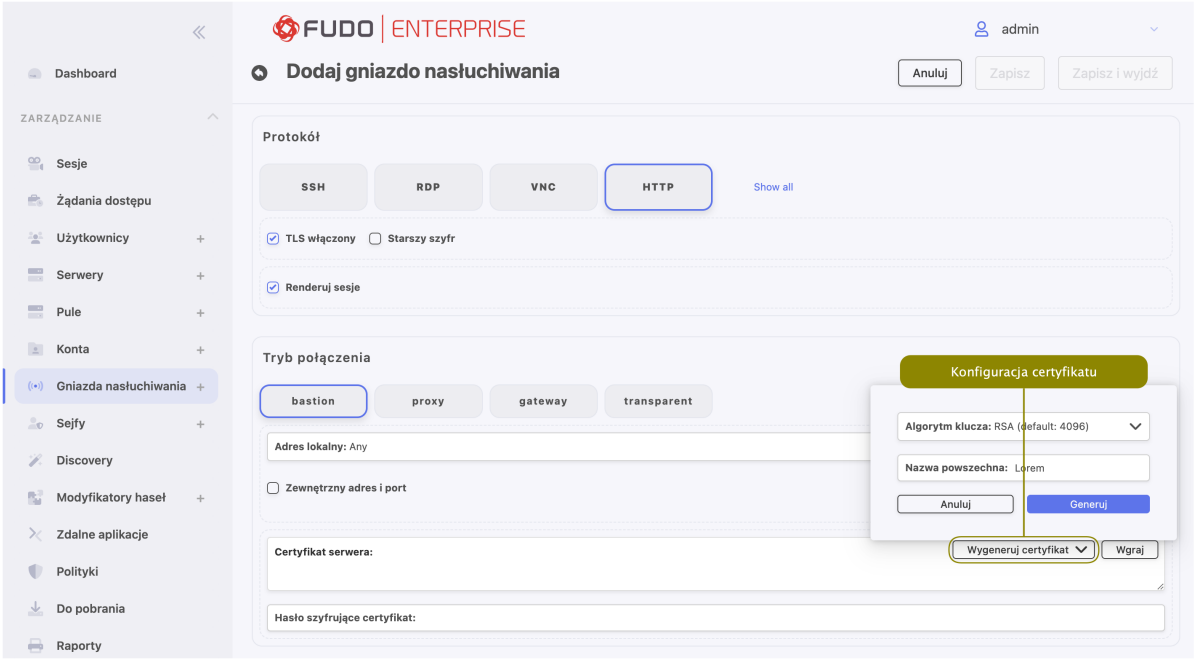
- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy 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.

Uwaga

Pole RDP config domain pozwala zdefiniować własną nazwę hosta wyświetlaną w tytule okna dla połączeń uruchamianych z Portalu Użytkownika przy użyciu natywnego klienta RDP. Pełny przykład konfiguracji znajdziesz w rozdziale *Niestandardowa nazwa hosta RDP w tytule sesji*.

6. W polu *Certyfikat serwera*, kliknij *Wygeneruj certyfikat*, aby wygenerować certyfikat TLS, albo kliknij *Wgraj*, 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*.

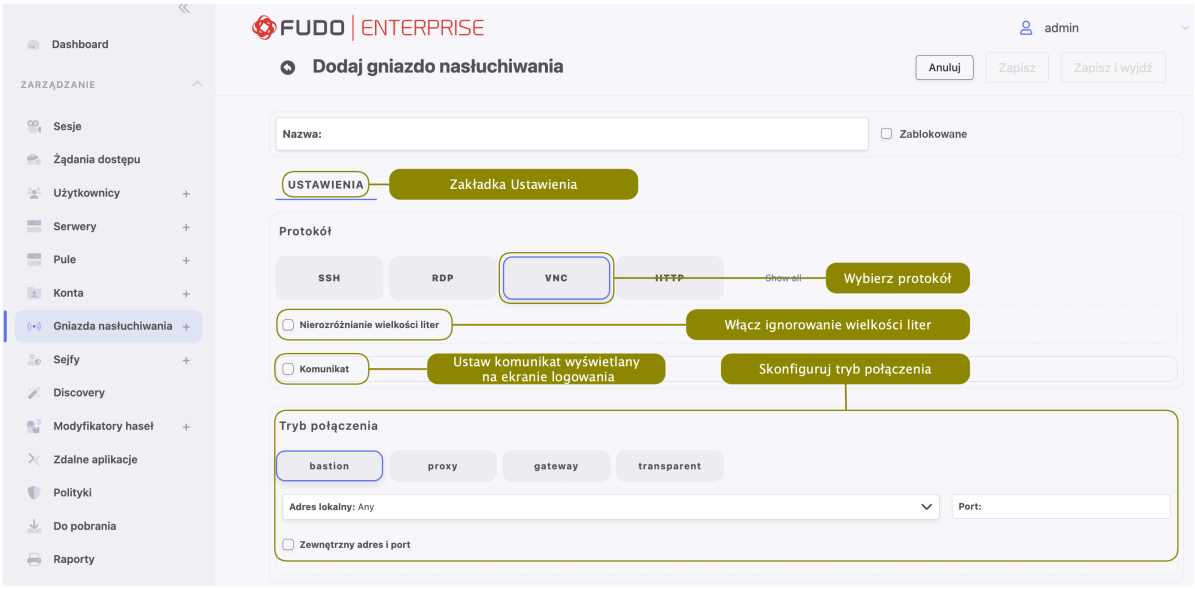
Tematy pokrewne:

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

10.4.1.3 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 *TLS włączony* w celu uruchomienia trybu szyfrowania.
3. (Opcjonalnie) Zaznacz pole wyboru *Starszy szyfr*, aby włączyć obsługę starszych algorytmów szyfrowania, jeśli są wymagane przez używanych klientów PostgreSQL.
4. Zaznacz opcję *Nierozróżnianie wielkości liter*, aby proces uwierzytelnienia nie rozróżniał wielkości liter w nazwie użytkownika.



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.

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

Tryb: bastion

> **Uwaga**
>
> - 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.

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

- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy 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.

Uwaga

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

Tryb: proxy

Uwaga

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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy 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.

7. Jeśli włączona jest obsługa TLS, w polu *Certyfikat serwera* kliknij *Wygeneruj certyfikat*, aby wygenerować certyfikat TLS, albo kliknij *Wgraj*, 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`.

Uwaga

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

8. Kliknij *Zapisz*.

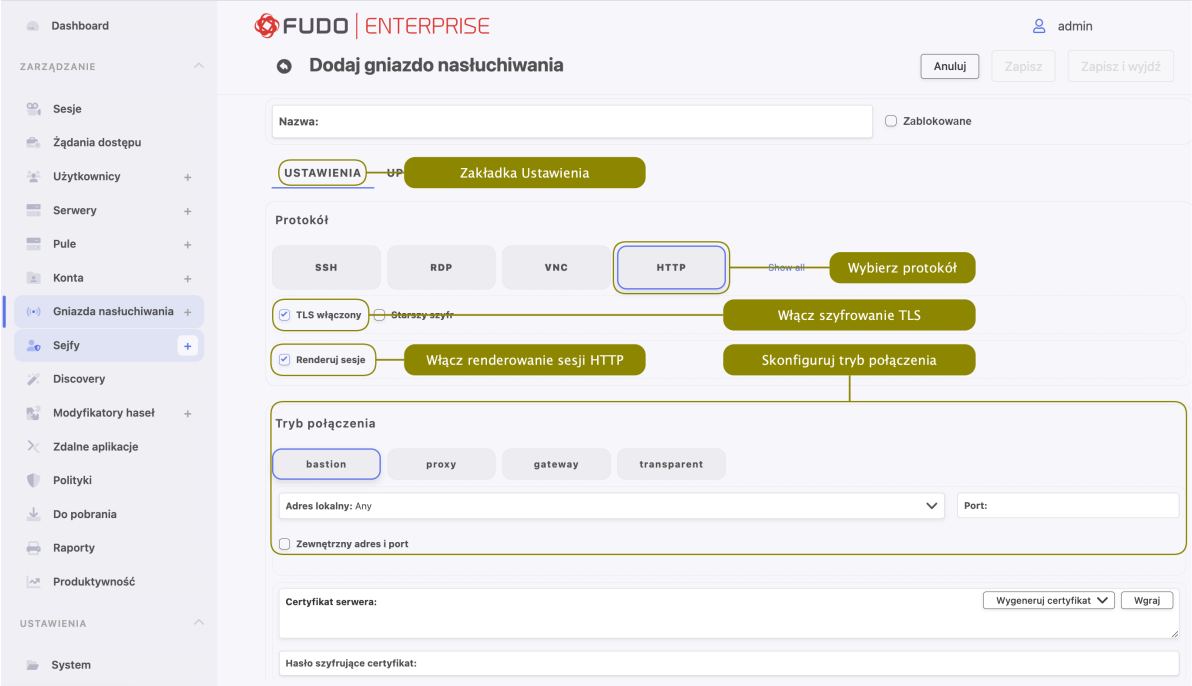
Tematy pokrewne:

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

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

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

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

Uwaga

- 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.

Uwaga

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

Tryb: bastion

Uwaga

- 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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

Uwaga

- 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.

Tryb: proxy

Uwaga

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.

Uwaga

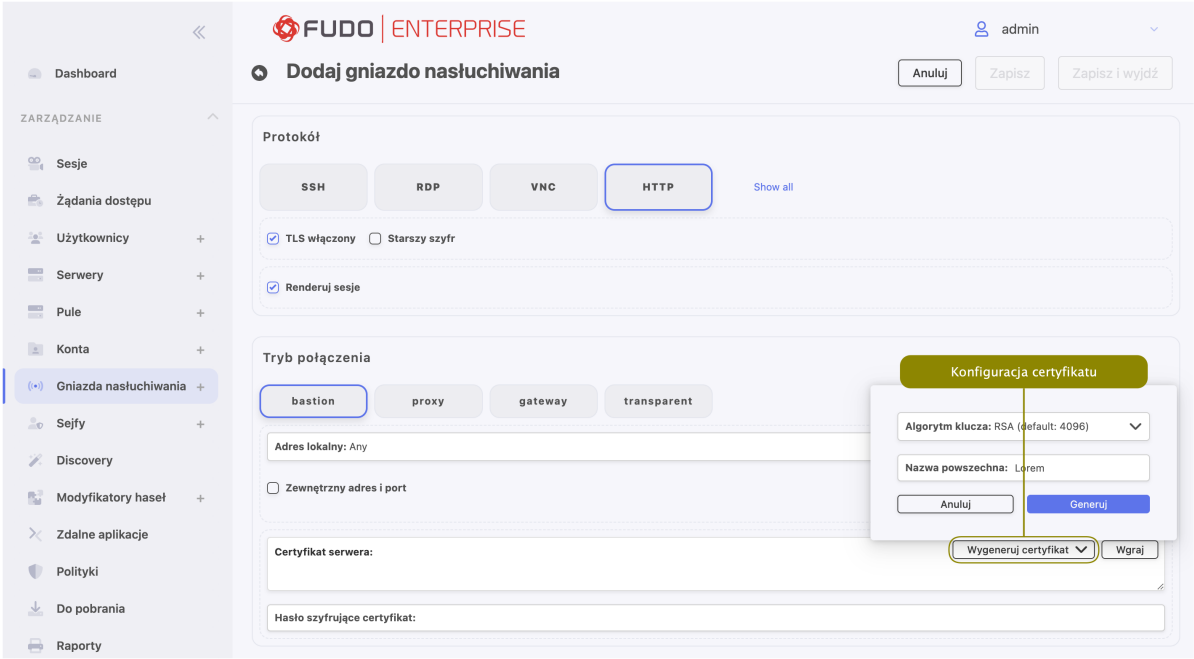
- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy 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.

Uwaga

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

6. W polu *Certyfikat serwera*, kliknij *Generuj certyfikat*, aby wygenerować certyfikat TLS, albo kliknij *Wgraj*, 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`.



Uwaga

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

7. Kliknij *Zapisz*.

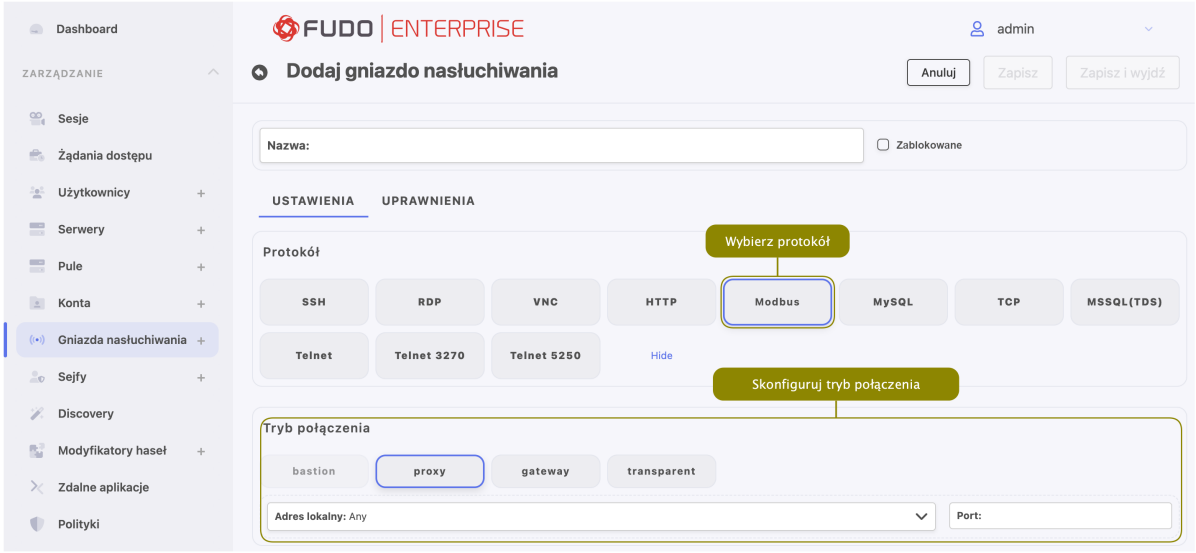
Tematy pokrewne:

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

10.4.1.5 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.

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

Tryb: proxy

> **Uwaga**
>
> 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.

> **Uwaga**
>
> - Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
> - Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
> - Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
> - W przypadku konfiguracji klastrowej, z listy rozwijalnej *Adres lokalny* wy-

bierz 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 *Etykietowane adresy IP*.

6. Kliknij *Zapisz*.

Tematy pokrewne:

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

10.4.1.6 Konfigurowanie gniazda nasłuchiwania MySQL

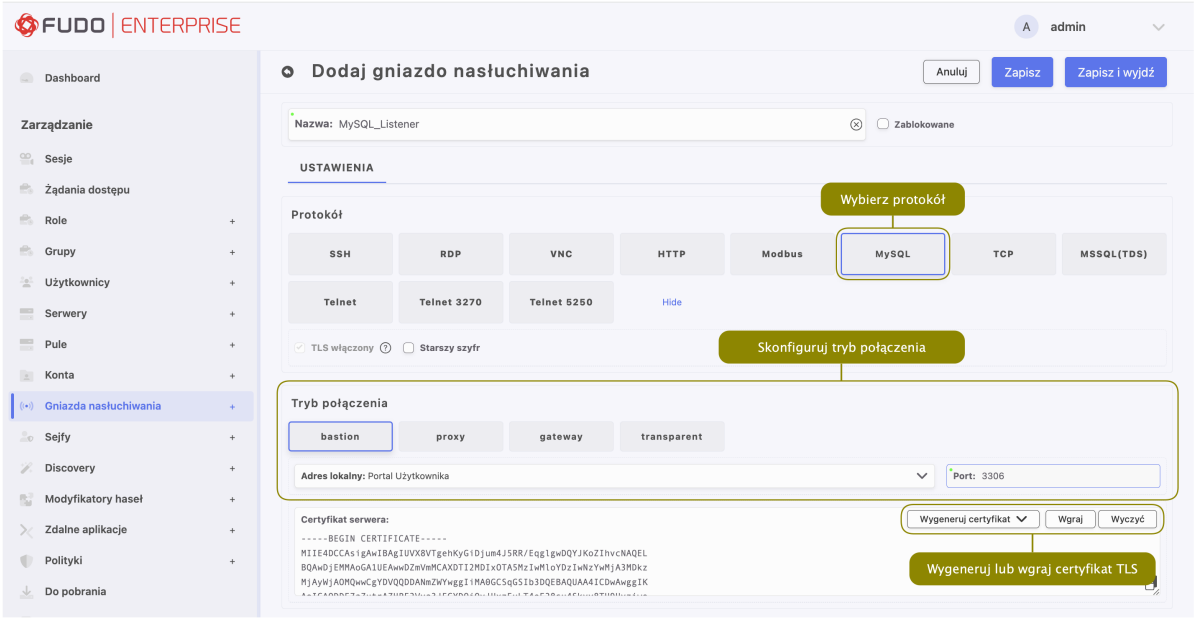
Rozdział zawiera opis konfiguracji nowego gniazda nasłuchiwania zgodnie z protokołem MySQL. Pierwsze kroki dodawania nowego gniazda nasłuchiwania opisane zostały w rozdziale *Dodawanie gniazda nasłuchiwania*.

Ostrzeżenie

Obsługiwane wtyczki uwierzytelniania:

- dla komunikacji między Fudo Enterprise a serwerem bazy danych: `mysql_clear_password`, `mysql_native_password`, `caching_sha2_password`;
- dla komunikacji między klientem a Fudo Enterprise: `mysql_clear_password`.

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



Uwaga

TLS jest zawsze włączony dla gniazd nasłuchiwania MySQL — nie ma możliwości jego wyłączenia.

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

Uwaga

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

Tryb: bastion

Uwaga

- 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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom

zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.

- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

Tryb: proxy

Uwaga

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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

4. W polu *Certyfikat serwera*, kliknij *Wygeneruj certyfikat*, aby wygenerować certyfikat TLS, albo kliknij *Wgraj*, 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`.

Uwaga

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

5. Kliknij *Zapisz*.

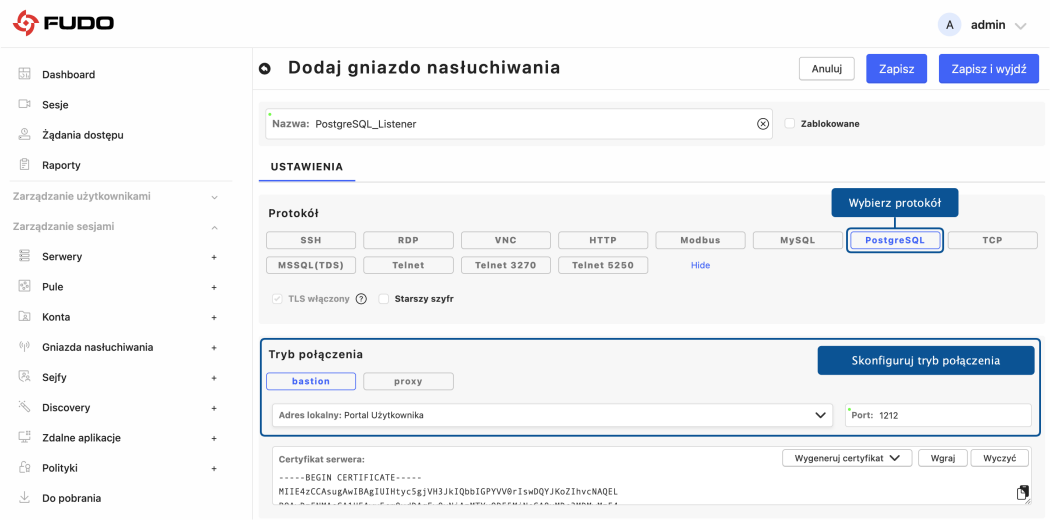
Tematy pokrewne:

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

10.4.1.7 Konfigurowanie gniazda nasłuchiwania PostgreSQL

W tym rozdziale opisano sposób konfiguracji gniazda nasłuchiwania PostgreSQL. Aby poznać pierwsze kroki tworzenia gniazda nasłuchiwania, przejdź do sekcji *Tworzenie gniazda nasłuchiwania*.

1. Przejdź do zakładki *USTAWIENIA* i naciśnij przycisk `Pokaż wszystkie`, aby rozwinąć listę obsługiwanych protokołów.
2. Naciśnij przycisk `PostgreSQL` w polu *Protokół*.



Uwaga

TLS jest zawsze włączony dla gniazda nasłuchiwania PostgreSQL i nie można go wyłączyć.

3. (Opcjonalnie) Zaznacz pole wyboru *Starszy szyfr*, aby włączyć obsługę starszych algorytmów szyfrowania, jeśli są wymagane przez używanych klientów PostgreSQL.
4. W sekcji *Tryb połączenia* wybierz żądany tryb połączenia.

5. W polu *Certyfikat serwera* kliknij *Wygeneruj certyfikat*, aby wygenerować certyfikat TLS, lub kliknij *Prześlij*, aby przesłać plik certyfikatu serwera z kluczem prywatnym wklejonym na końcu pliku. Pozostałe wymagane pola zostaną uzupełnione automatycznie. Dozwolonym formatem pliku certyfikatu serwera jest PEM, przy czym oprócz rozszerzenia `.pem` akceptowane są również rozszerzenia `.txt` i `.cert`.

Ostrzeżenie

Dla gniazda nasłuchiwania PostgreSQL nazwa Common Name (CN) certyfikatu powinna odpowiadać nazwie hosta, której klienci będą używać do połączenia. Niezgodność CN może powodować błędy weryfikacji certyfikatu w klientach PostgreSQL.

6. Kliknij *Zapisz*.

Uwaga

- Po utworzeniu gniazda nasłuchiwania PostgreSQL użytkownicy mogą łączyć się za pomocą natywnego klienta PostgreSQL, `psql`.
- Polecenie służące do ustanowienia połączenia jest dostępne dla użytkownika po zalogowaniu się do Portalu Użytkownika. Na przykład:

```
psql postgres:1/85156504WW4NEopiQ0vePxbIqaXiEYcT:empty@<listener_address>
↪[:port]/<database_name>
```

- Użytkownik musi zastąpić `<database_name>` właściwą nazwą bazy danych.

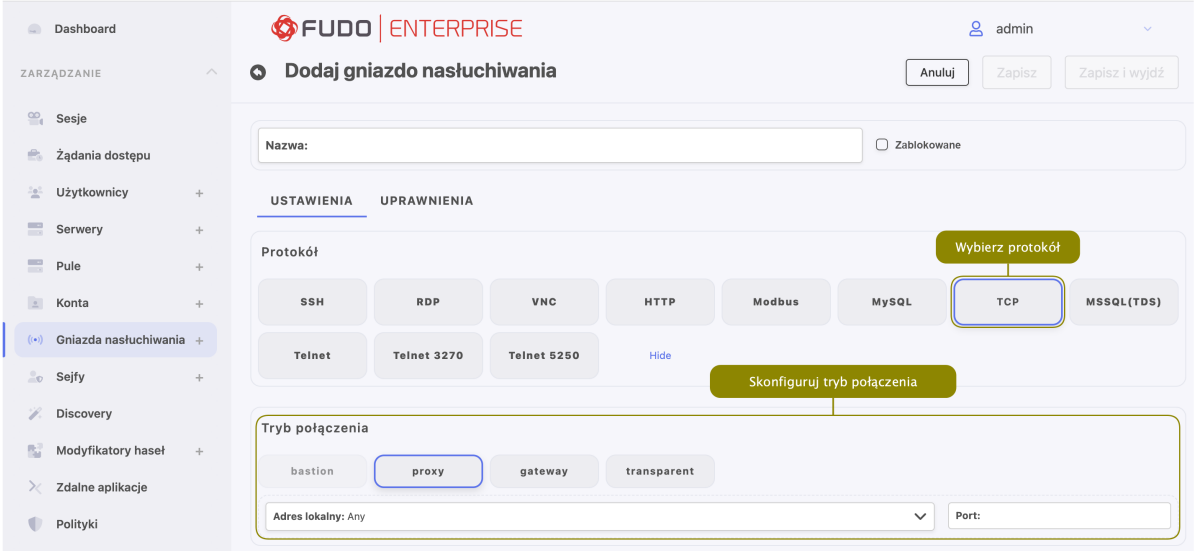
Tematy powiązane:

- *Model danych*
- *Modyfikowanie gniazda nasłuchiwania*
- *Usuwanie gniazda nasłuchiwania*
- *Blokowanie gniazda nasłuchiwania*
- *Odblokowanie gniazda nasłuchiwania*
- *Tworzenie serwera PostgreSQL*
- *PostgreSQL*

10.4.1.8 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.

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

Tryb: proxy

> **Uwaga**
>
> 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.

> **Uwaga**
>
> - Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.

- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

4. Kliknij *Zapisz*.

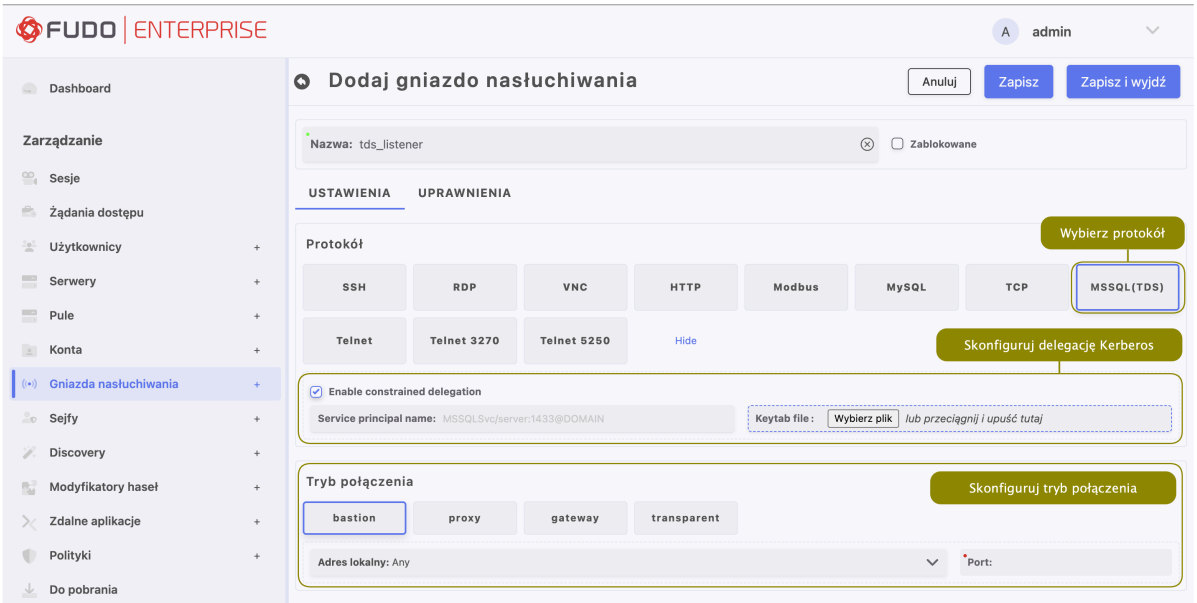
Tematy pokrewne:

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

10.4.1.9 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. Jeśli chcesz skonfigurować *delegację Kerberos*:
   - Zaznacz opcję *Włącz ograniczoną delegację*.
   - W polu *Nazwa główna usługi (SPN)* wprowadź nazwę w następującym formacie (np. `MSSQLSvc/mgmt.qa.fudo:1433@QA.FUDO`).
   - Wczytaj plik Keytab wygenerowany na potrzeby delegacji.



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

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

Tryb: bastion

> **Uwaga**
>
> - 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.

> **Uwaga**
>
> - Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
> - Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
> - Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja

połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.

- 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 *Etykietowane adresy IP*.

Tryb: proxy

Uwaga

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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

5. Kliknij *Zapisz*.

Tematy pokrewne:

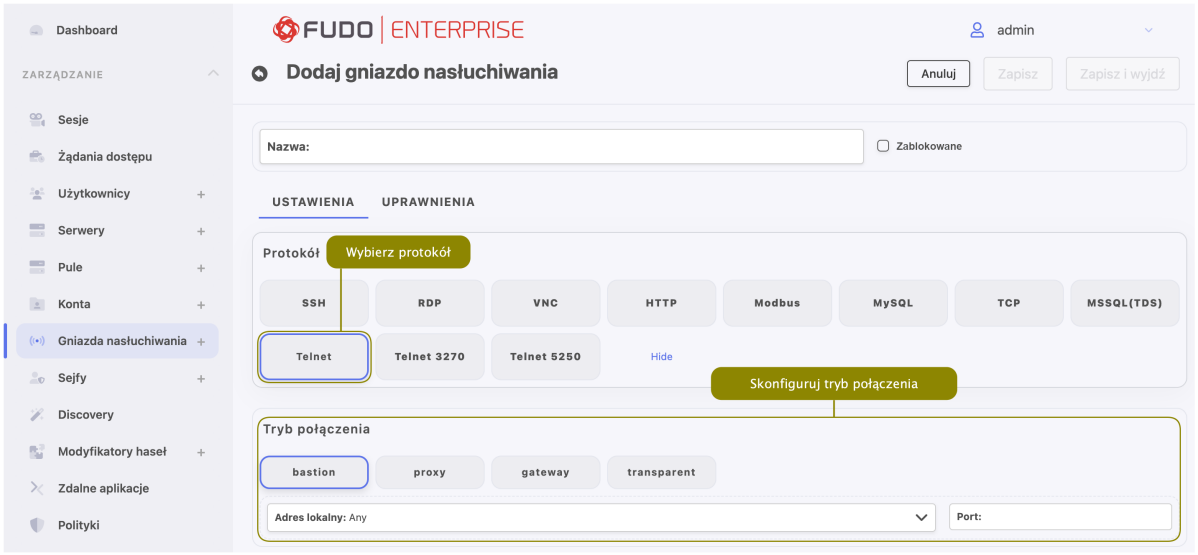
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*

- *Konta*

10.4.1.10 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.

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

Tryb: bastion

> **Uwaga**
>
> - 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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

Tryb: proxy

Uwaga

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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

4. Kliknij *Zapisz*.

Tematy pokrewne:

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

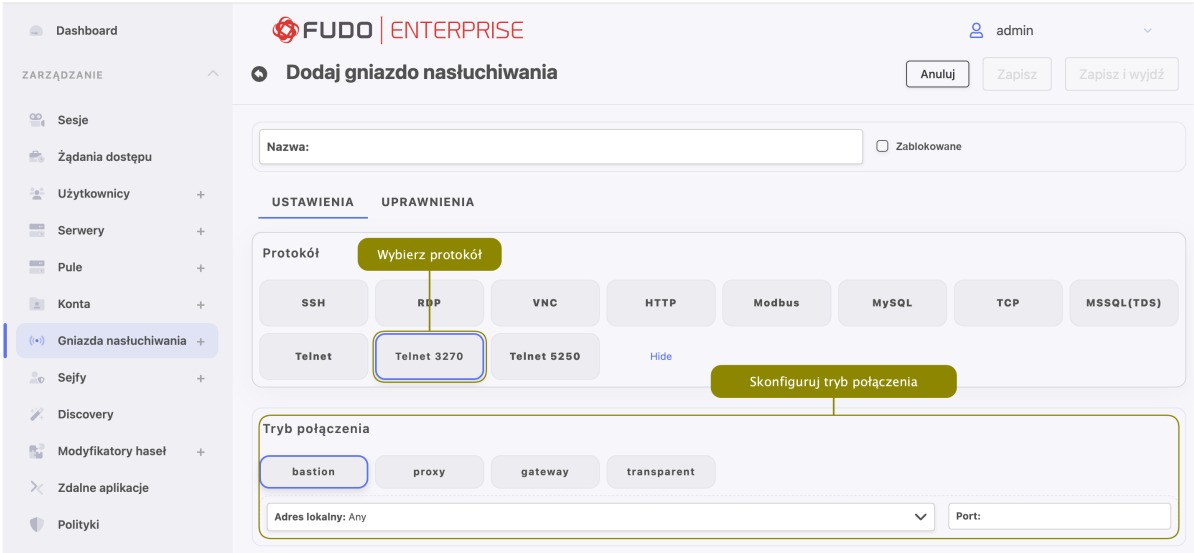
10.4.1.11 Konfigurowanie gniazda nasłuchiwania Telnet 3270

Deprecated since version 6.0 :class: danger

Wsparcie dla protokołu **Telnet 3270** jest obecnie **w fazie przeglądu** i może zostać usunięte w jednej z kolejnych wersji. Jeśli protokół ten jest kluczowy dla Twojego środowiska, skontaktuj się z pomocą techniczną Fudo w celu uzyskania dodatkowych informacji.

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.

Uwaga

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

Tryb: bastion

Uwaga

- 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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

Tryb: proxy

Uwaga

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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom

zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.

- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

4. Kliknij *Zapisz*.

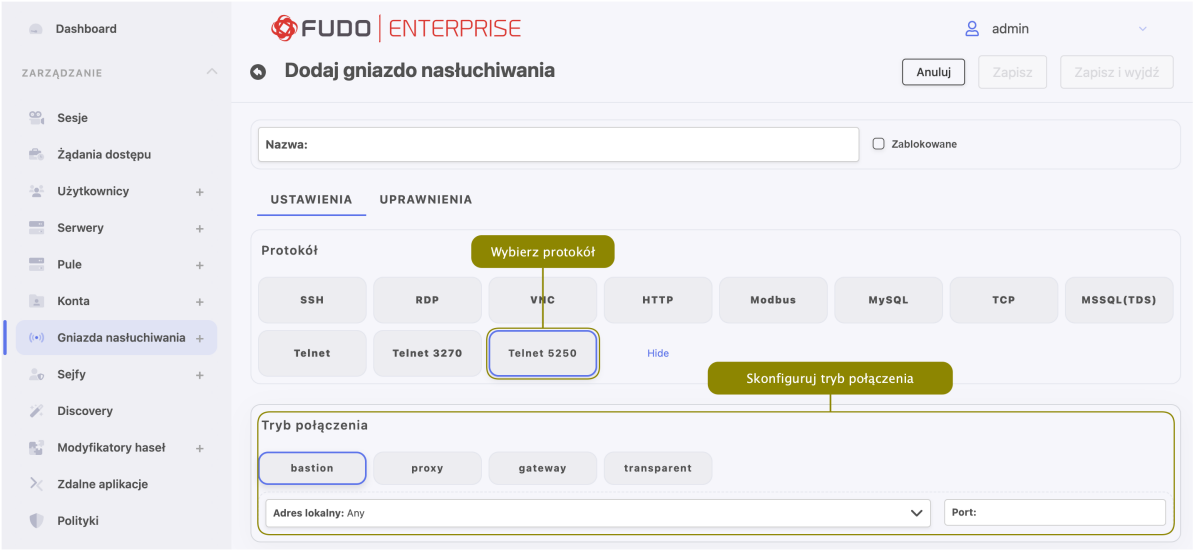
Tematy pokrewne:

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

10.4.1.12 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.

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

Tryb: bastion

> **Uwaga**
>
> - 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.

> **Uwaga**
>
> - Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
> - Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
> - Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać

adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.

- 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 *Etykietowane adresy IP*.

Tryb: proxy

Uwaga

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.

Uwaga

- Elementami listy rozwijalnej są adresy IP nadane fizycznym interfejsom zgodnie z opisem w sekcji *Konfiguracja ustawień sieciowych* lub etykietowane adresy IP opisane w rozdziale *Etykietowane adresy IP*.
- Wybranie opcji *Any*, skutkuje nasłuchiwaniem na połączenia użytkowników na wszystkich skonfigurowanych adresach IP.
- Wybranie opcji *User Access Gateway* jako adres lokalny spowoduje, że po zalogowaniu do Portalu Użytkownika wyświetlana będzie tylko jedna opcja połączenia (dla przejrzystości), a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.
- 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 *Etykietowane adresy IP*.

4. Kliknij *Zapisz*.

Tematy pokrewne:

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

Uwaga

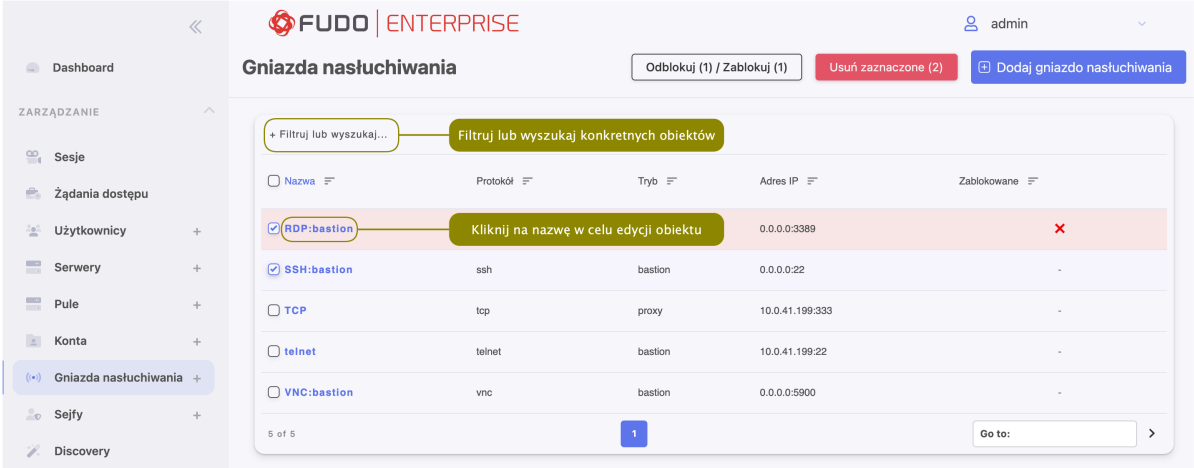
Od wydania 5.6 **ulepszona** została **konfiguracja gniazd nasłuchiwania dla Portalu Użytkownika.** Wybranie opcji **User Access Gateway** jako **adres lokalny** spowoduje, że po zalogowaniu do Portalu Użytkownika dla przejrzystości wyświetlana będzie tylko jedna opcja połączenia, a samo połączenie będzie wykorzystywać adres z paska adresu przeglądarki wraz ze skonfigurowanym portem listenera.

10.4.2 Modyfikowanie gniazda nasłuchiwania

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

Uwaga

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*

10.4.3 Blokowanie gniazda nasłuchiwania

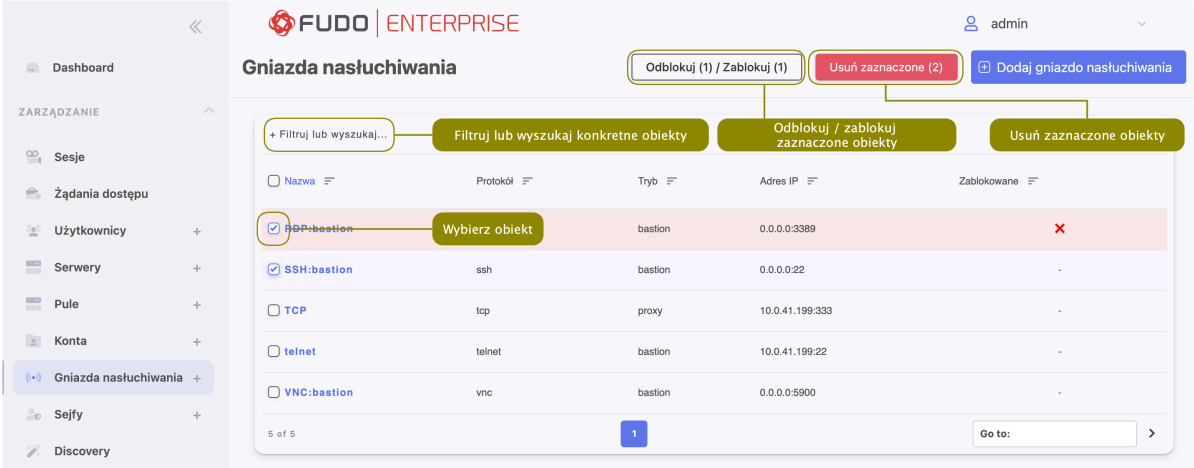
Ostrzeżenie

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.

Uwaga

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*.

Uwaga

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

Tematy pokrewne:

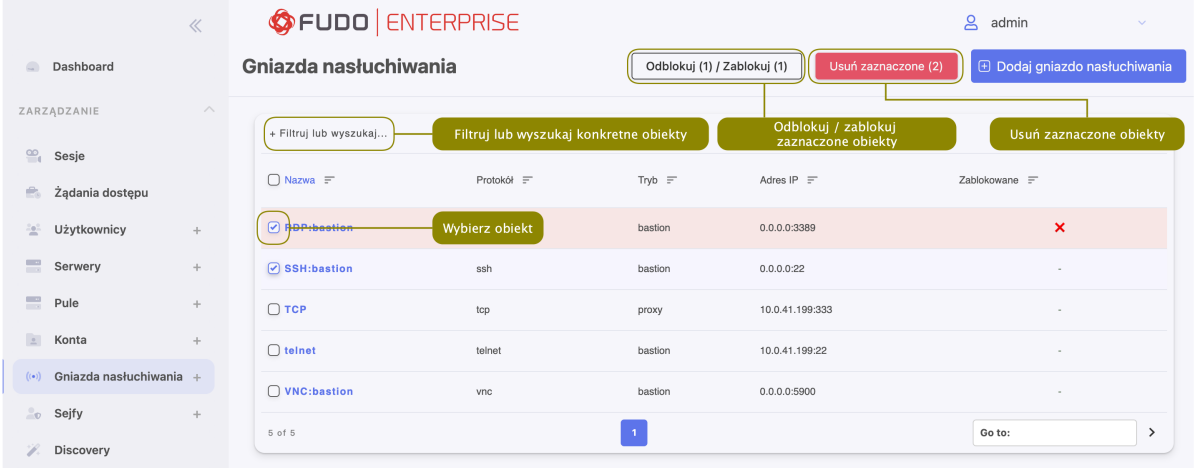
- *Model danych*
- *Pierwsze uruchomienie*
- *Użytkownicy*
- *Sejfy*
- *Konta*

10.4.4 Odblokowanie gniazda nasłuchiwania

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

Uwaga

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*

10.4.5 Usuwanie gniazda nasłuchiwania

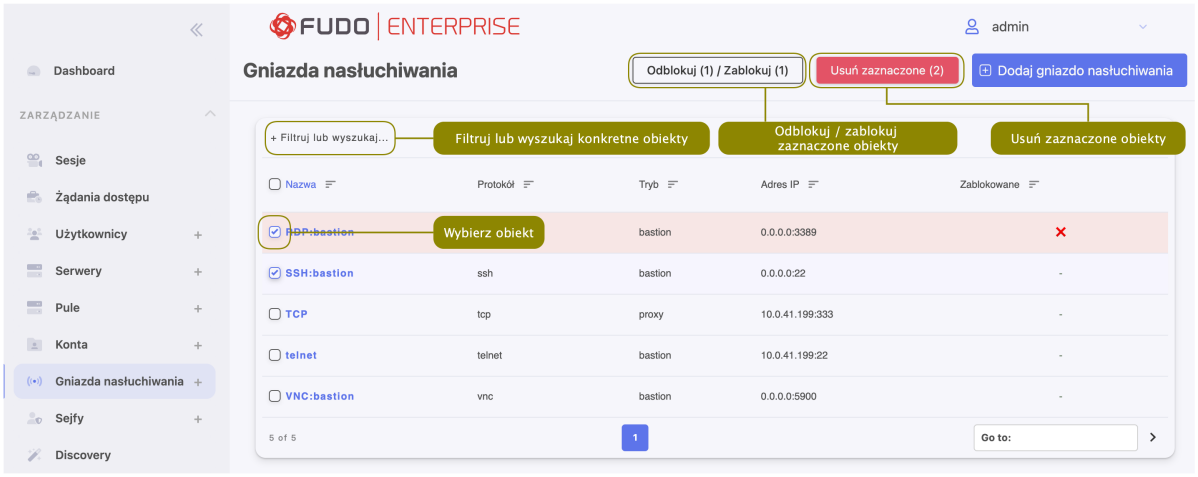
Ostrzeżenie

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.

Uwaga

Zdefiniuj filtr, aby ograniczyć liczbę elementów listy.



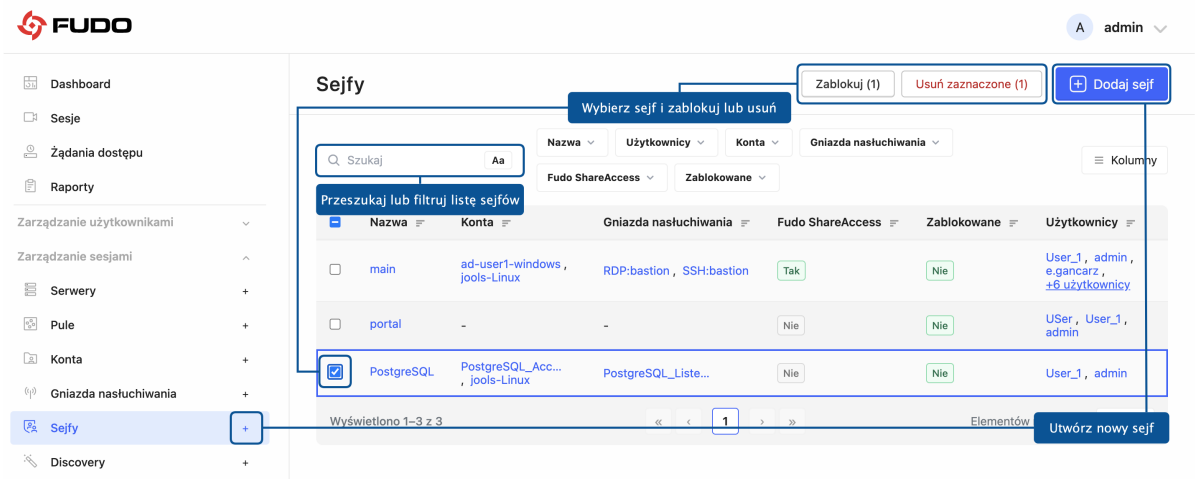
3. Kliknij *Usuń zaznaczone*.
4. Kliknij *Potwierdź*, aby zatwierdzić usunięcie zaznaczonych obiektów.

Tematy pokrewne:

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

10.5 Sejfy

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

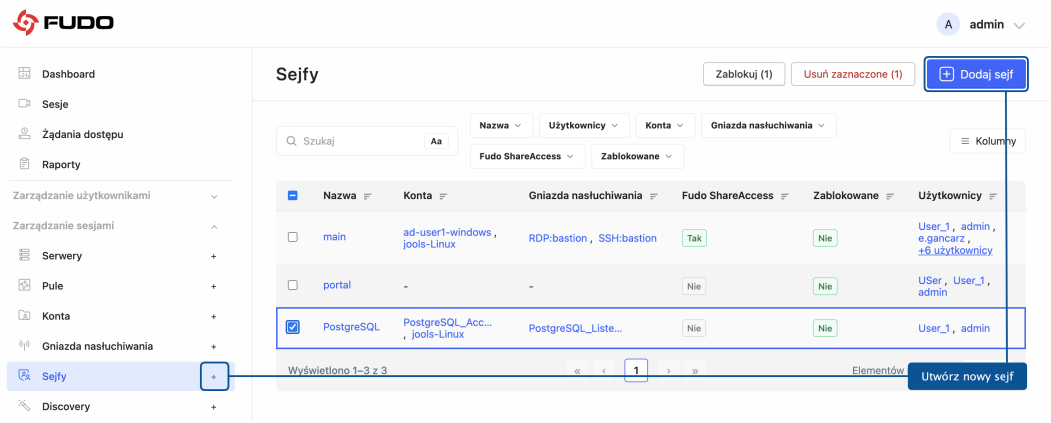


10.5.1 Dodawanie sejfu

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 sesjami*, lub
2. Wybierz *Zarządzanie sesjami* > *Sejfy*, a następnie kliknij + *Dodaj sejf*.



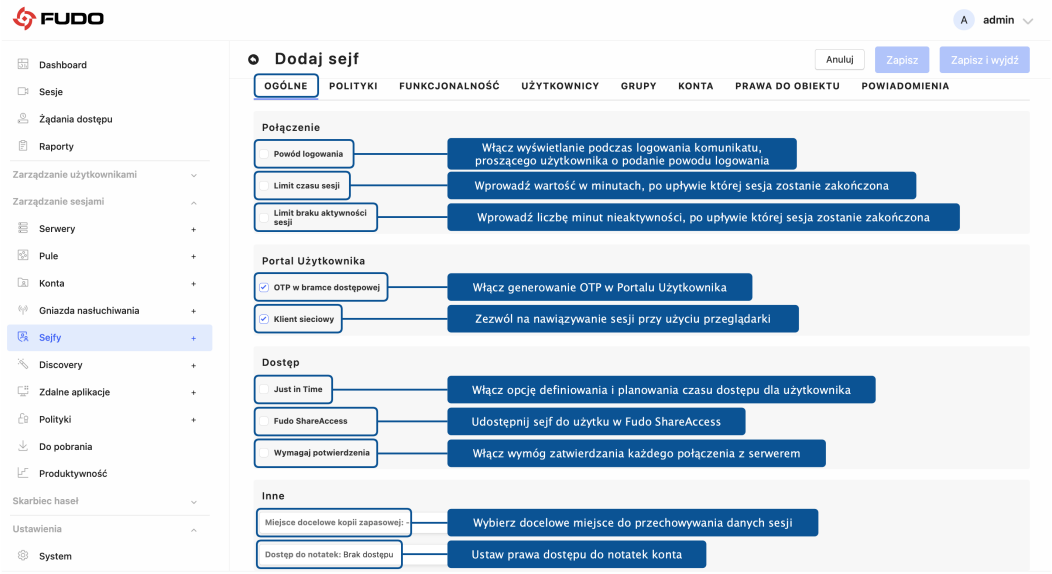
3. Wprowadź nazwę obiektu.
4. Wybierz opcję *Zablokowany*, jeśli chcesz uniemożliwić dostęp do obiektu po jego utworzeniu.
5. Kliknij *Zapisz*, aby zapisać obiekt i kontynuować dalszą konfigurację.

ZAKŁADKA OGÓLNE

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

Uwaga

Powód logowania nie jest obsługiwany w połączeniach *HTTP*.



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

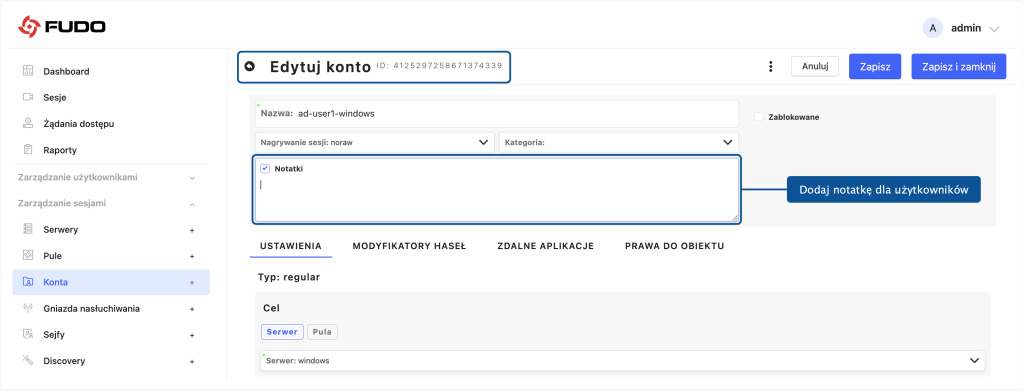
Ostrzeżenie

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

5. W przypadku sejfów opartych na protokołach RDP, VNC oraz SSH, wybierz opcję *Klient webowy*, jeśli chcesz nawiązywać połączenia z serwerem bezpośrednio w przeglądarce.
6. 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*.
7. 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.
8. 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*.
9. Z rozwijanego menu *Dostęp do notatek*, wybierz prawa dostępu do notatek danego konta: `read, write` lub `none`.

Uwaga

Notatki mogą być dostępne zarówno z formularza edycji konta

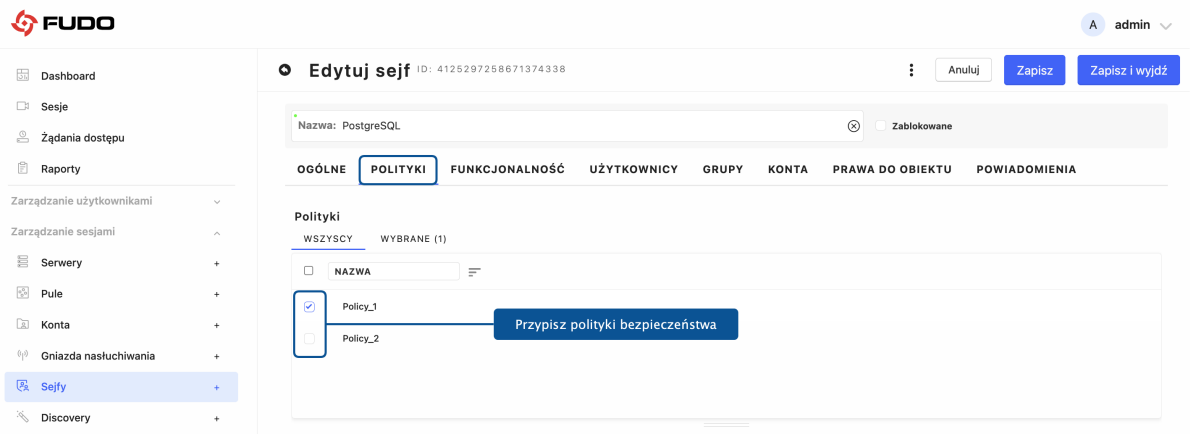


jak i w *Portalu Użytkownika*.



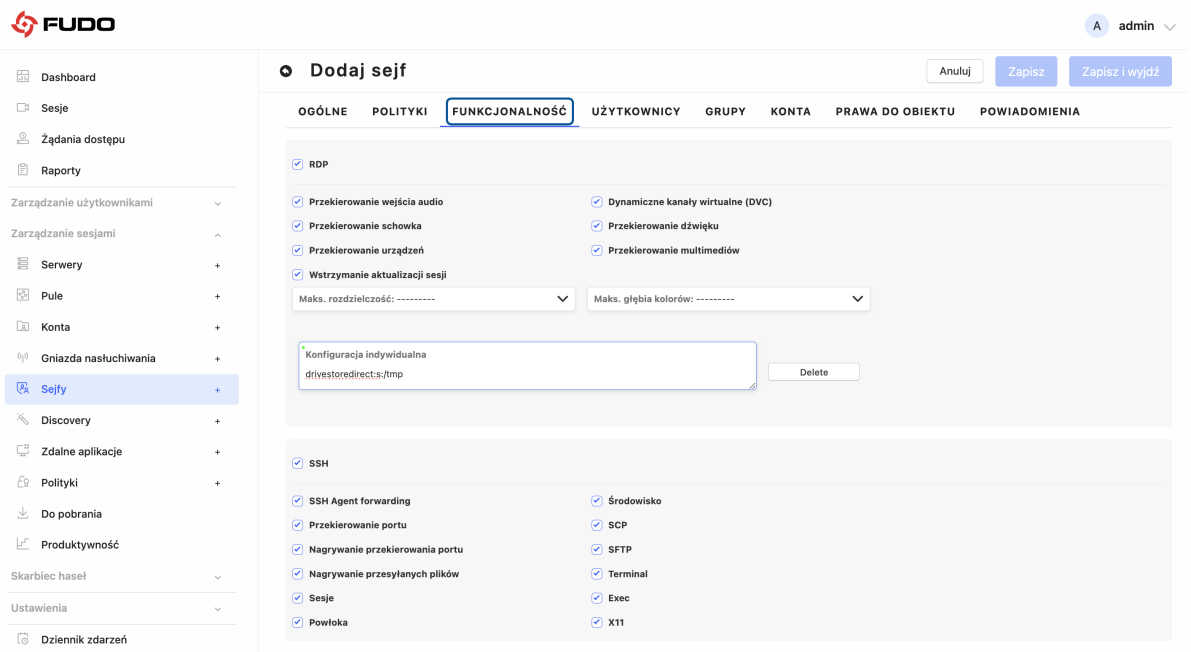
ZAKŁADKA POLITYKI

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



ZAKŁADKA FUNKCJONALNOŚĆ

Przejdź do zakładki *FUNKCJONALNOŚĆ* i włącz wybrane funkcje protokołów.



Uwaga

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. Jest bezpośrednio powiązana z obsługą sterownika GFX. Wyłącz tę opcję, aby wyłączyć obsługę GFX, jeśli napotkasz problemy z wydajnością. Wyłączenie tej opcji jest również wymagane do przywrócenia kompatybilności z xrdp.
  - **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. **Uwaga:** Starsze systemy Windows wymagają głębi kolorów mniejszej niż 32 bpp, podczas gdy nowsze wersje potrzebują 32 bpp. Aby zapewnić kompatybilność, możesz przypisać serwery ze starszymi wersjami Windows do odrębnych sejfów i skonfigurować dla nich niższą głębię kolorów, jednocześnie utrzymując limit 32 bpp dla nowszych systemów.
  - **Konfiguracja indywidualna** – Umożliwia dodanie własnej zawartości do pliku konfiguracyjnego RDP. Na przykład, aby udostępnić katalog `/tmp`, można dodać w polu następującą linię: `drivestoredirect:s:/tmp`.

- 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.*

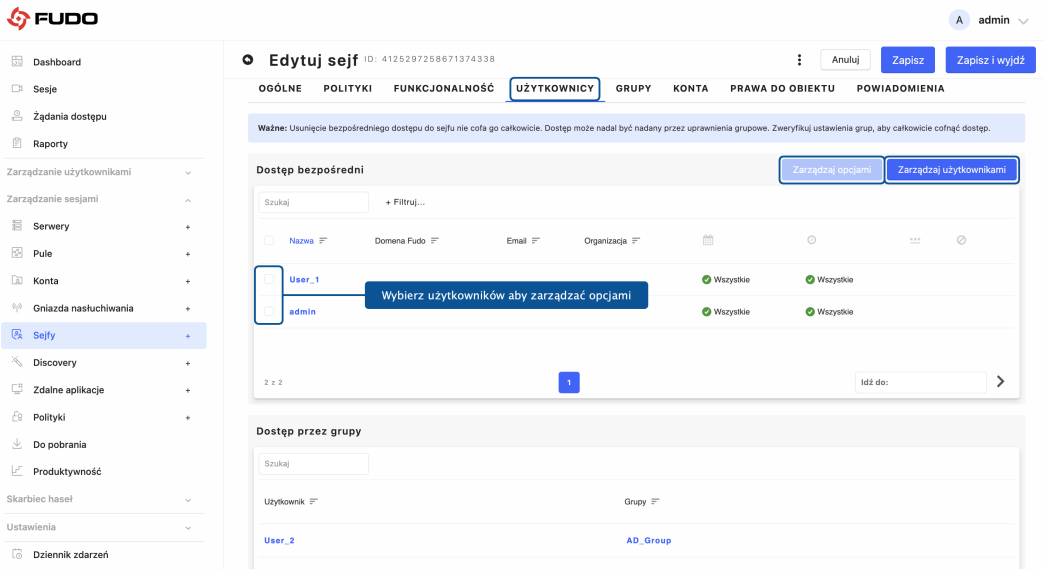
ZAKŁADKA UŻYTKOWNICY

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

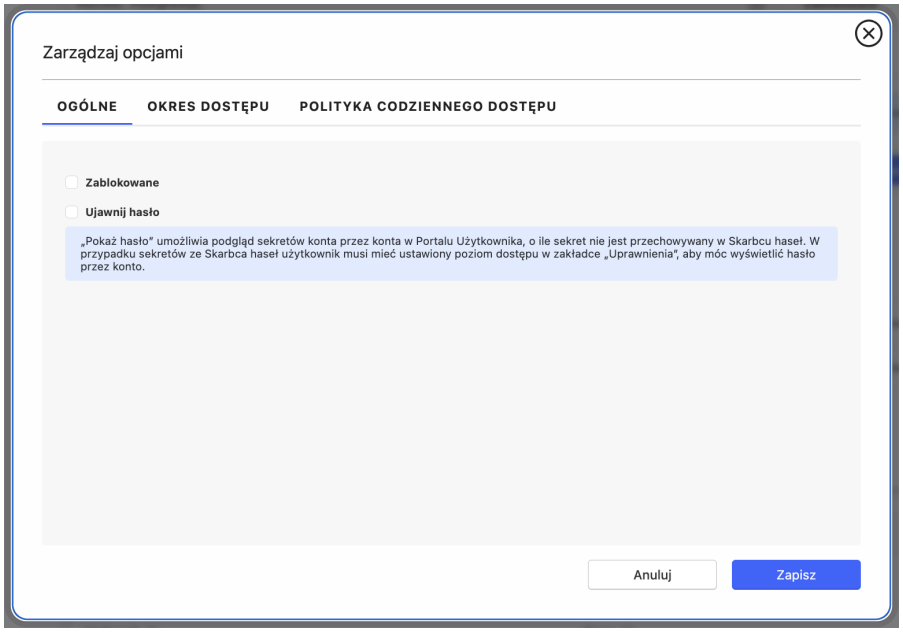
Uwaga

Aby zrozumieć zasadę priorytetyzacji dostępu użytkowników i grup do sejfu, zapoznaj się z rozdziałem *Rozstrzyganie dostępu i priorytetyzacja*.

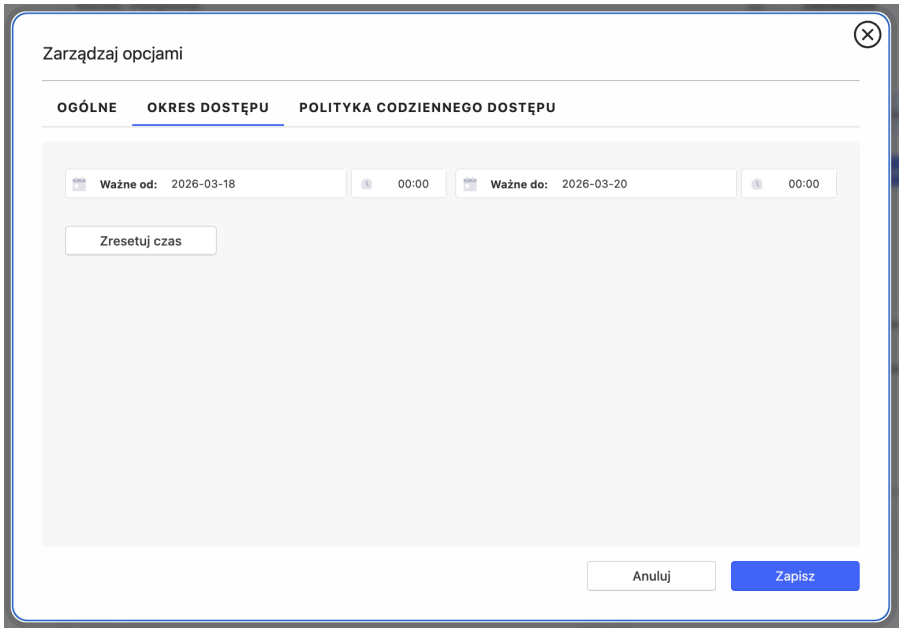
1. Kliknij *Zarządzaj użytkownikami*.
2. Zaznacz pole wyboru przed nazwami użytkowników, aby umożliwić im dostęp do serwerów poprzez monitorowany sejf.



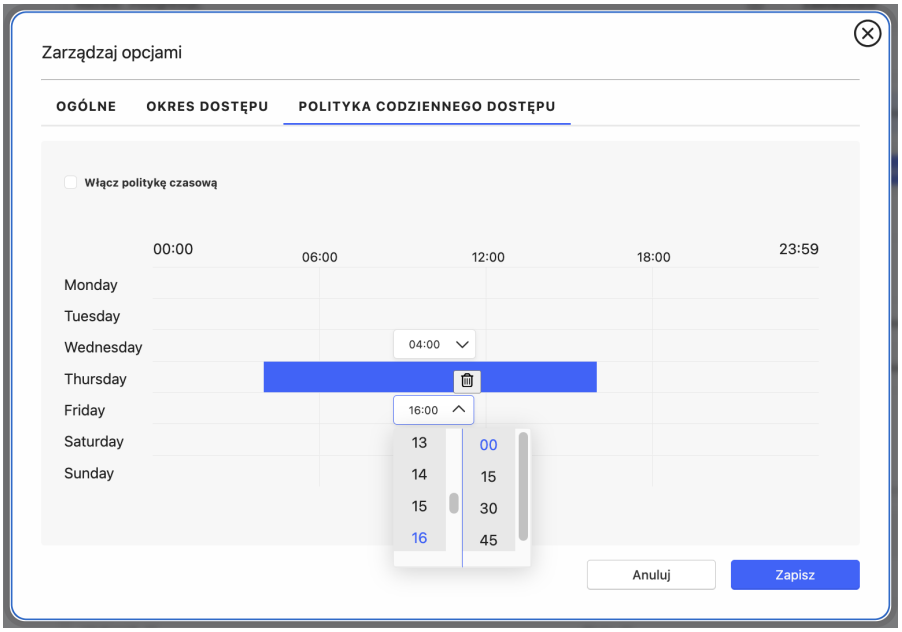
3. Kliknij *Zapisz*, aby zamknąć okno dialogowe.
4. Aby zdefiniować opcje dostępu do sejfu dla użytkownika, zaznacz pole wyboru przed nazwami pożądanych użytkowników i kliknij *Zarządzaj opcjami*.
    - Przejdź do zakładki *OGÓLNE* i wybierz opcję *Zablokowany*, jeśli chcesz zablokować użytkowników wybranych 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.



Uwaga

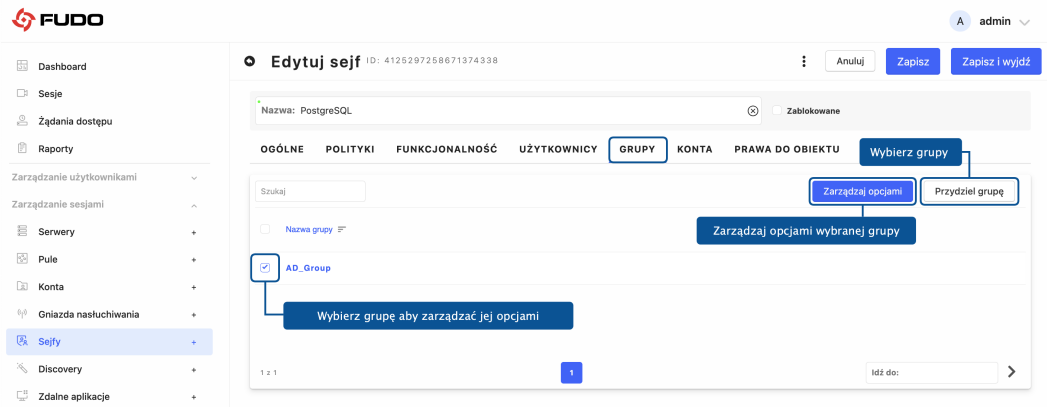
Opcje polityki czasu dostępu są wyłączone, gdy dla sejfu jest włączona opcja *Just in time*.

ZAKŁADKA GRUPY

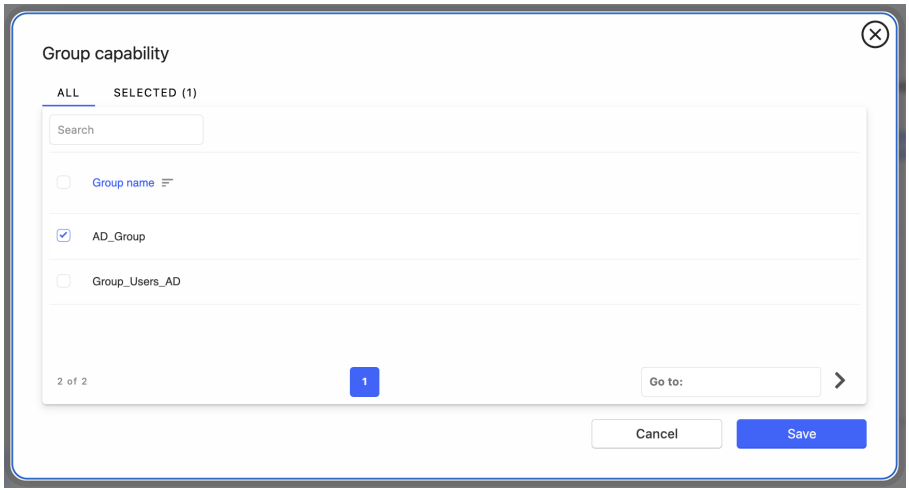
W zakładce *GRUPY* możesz wskazać grupy użytkowników, którym będzie wolno uzyskiwać dostęp do kont przypisanych do tego sejfu.

Uwaga

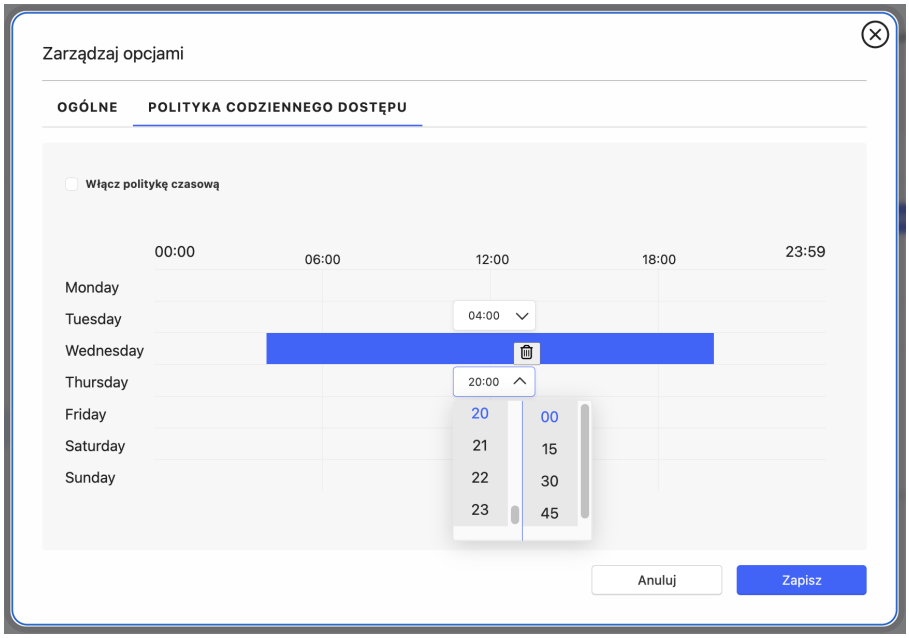
Aby zrozumieć zasadę priorytetyzacji dostępu użytkowników i grup do sejfu, zapoznaj się z rozdziałem *Rozstrzyganie dostępu i priorytetyzacja*.



1. Kliknij *Przydziel grupę*.
2. Zaznacz pole wyboru przy nazwach grup, aby je dodać.



3. Kliknij *Zapisz*, aby zamknąć okno modalne.
4. Wybierz żądaną grupę i kliknij *Zarządzaj opcjami*, aby zdefiniować ustawienia ogólne oraz dzienne reguły dostępu.



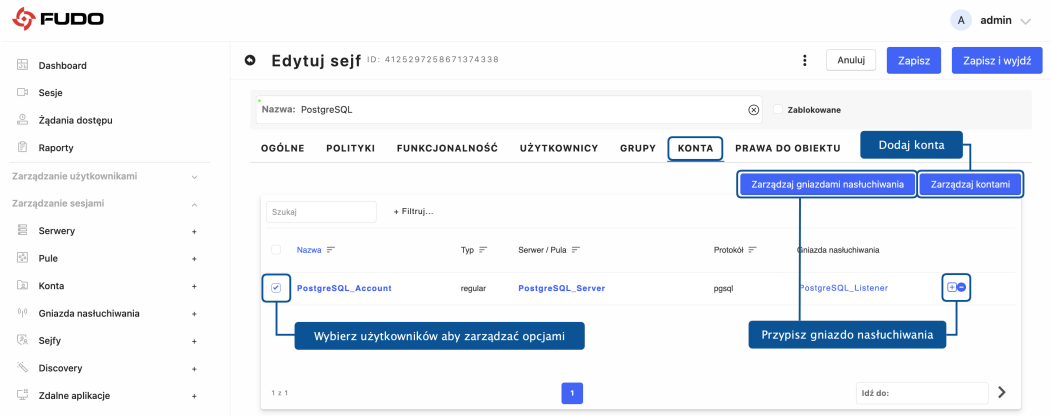
5. Kliknij *Zapisz*, aby zamknąć okno modalne.

ZAKŁADKA KONTA

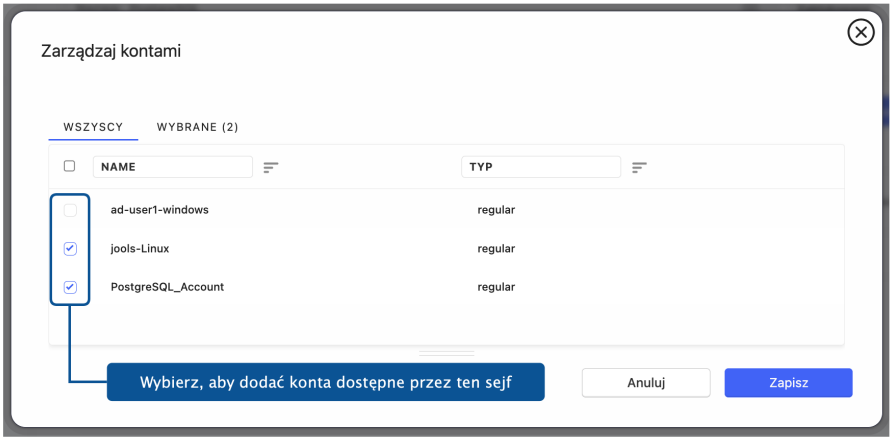
Uwaga

Aby zarządzać kontami w sejfie, użytkownik musi mieć również przypisane uprawnienie *listener-read*.

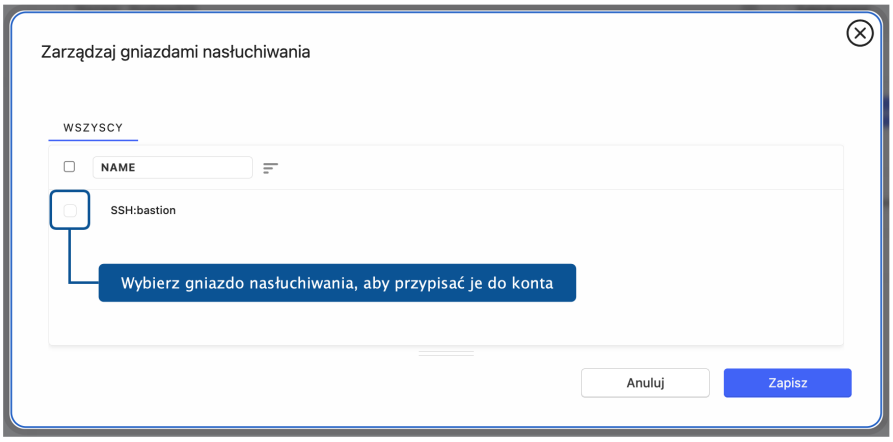
Wybierz zakładkę *Konta*, aby dodać konta dostępne przez ten sejf.



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



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

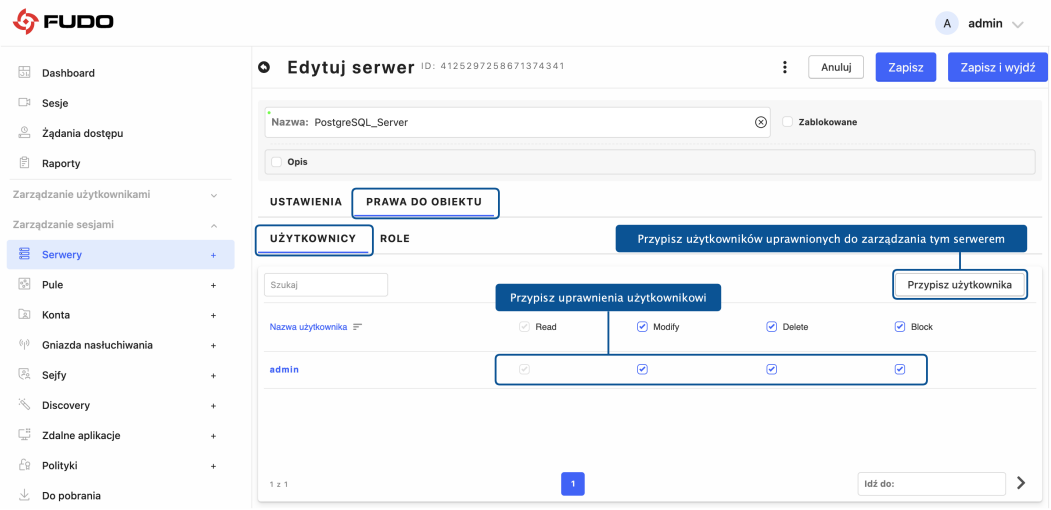


5. Kliknij *Zapisz*, aby zamknąć okno dialogowe.

ZAKŁADKA PRAWA DO OBIEKTU

Zakładka **PRAWA DO OBIEKTU** służy do określenia, którzy użytkownicy i role mogą zarządzać obiektem oraz jakie uprawnienia (Read, Modify, Delete, Block) są im przypisane.

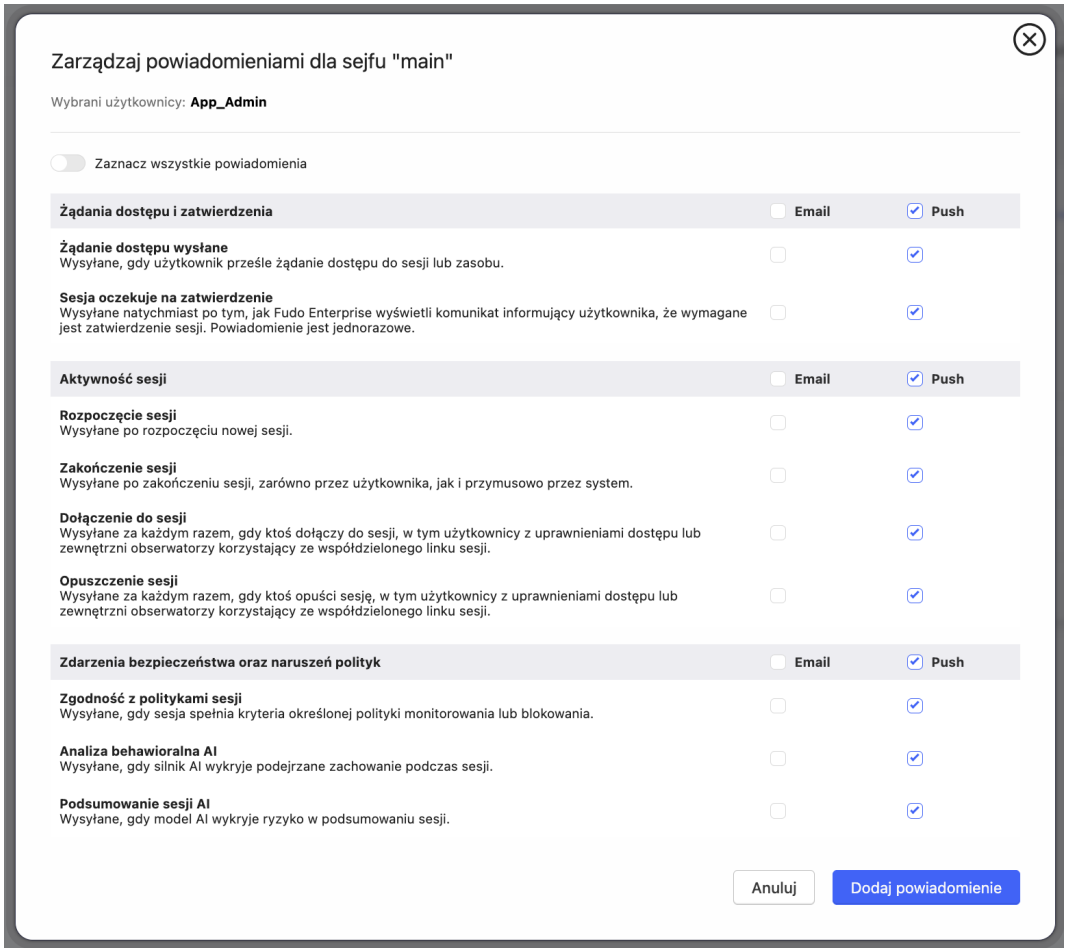
1. Przejdź do zakładki **PRAWA DO OBIEKTU**.
2. Otwórz podzakładkę **UŻYTKOWNICY**.
3. Kliknij **Przypisz użytkownika**, wybierz użytkowników z listy i kliknij **Zapisz**.
4. Na liście **UŻYTKOWNICY** zaznacz dla każdego użytkownika odpowiednie uprawnienia, wybierając jedną lub więcej z dostępnych opcji, np: Read, Modify, Delete lub Block.
5. Otwórz podzakładkę **ROLE**.
6. Kliknij **Przypisz rolę**, wybierz role z listy i kliknij **Zapisz**.
7. Na liście **ROLE** zaznacz dla każdej roli odpowiednie uprawnienia, wybierając jedną lub więcej z następujących opcji: Read, Modify, Delete lub Block.
8. Kliknij *Zapisz i wyjdź*.



ZAKŁADKA POWIADOMIENIA

Wybierz zakładkę *POWIADOMIENIA*, aby określić powiadomienia, które będą włączone dla poszczególnych użytkowników. Szczegółowe informacje o typach powiadomień znajdziesz w sekcji *Powiadomienia*.

1. Aby zdefiniować określone typy powiadomień dla użytkownika, zaznacz pole wyboru przed nazwami wybranych użytkowników i kliknij *Zarządzaj powiadomieniami*.



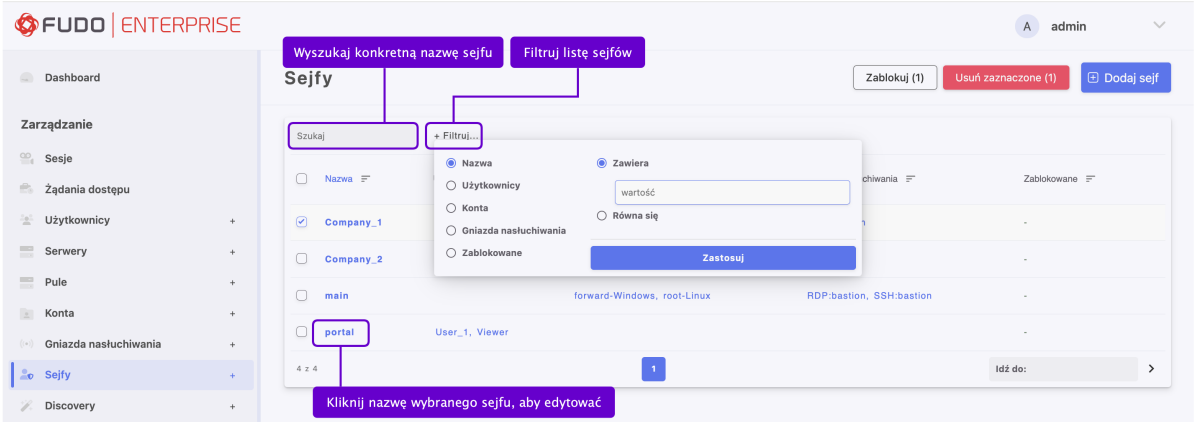
2. Z listy wybierz typy powiadomień, które chcesz przypisać użytkownikowi.
3. Kliknij *Dodaj powiadomienie*, aby zamknąć okno dialogowe.
4. Kliknij *Zapisz* lub *Zapisz i zamknij*, aby zapisać konfigurację sejfu.

Tematy pokrewne:

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

10.5.2 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:

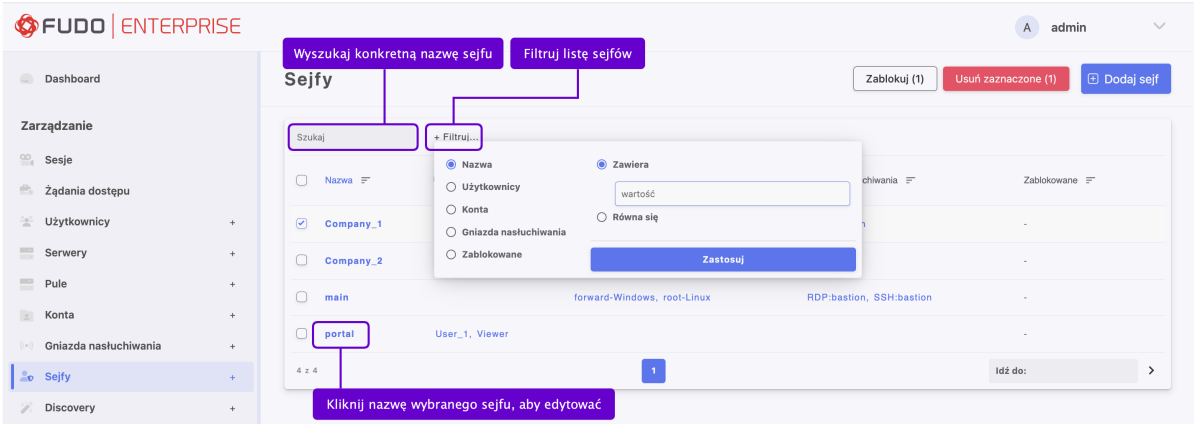
- *Model danych*
- *Dodawanie sejfu*
- *Blokowanie sejfu*
- *Usuwanie sejfu*

10.5.3 Blokowanie sejfu

Ostrzeżenie

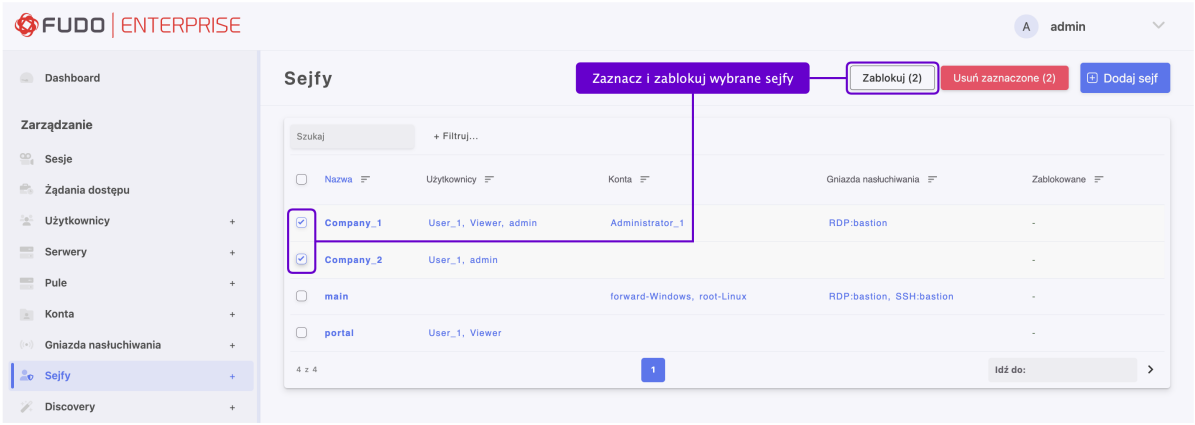
Zablokowanie sejfu spowoduje zerwanie aktualnie trwających sesji połączeniowych, wykorzystujących konta przypisane wybranego obiektu.

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.

Uwaga

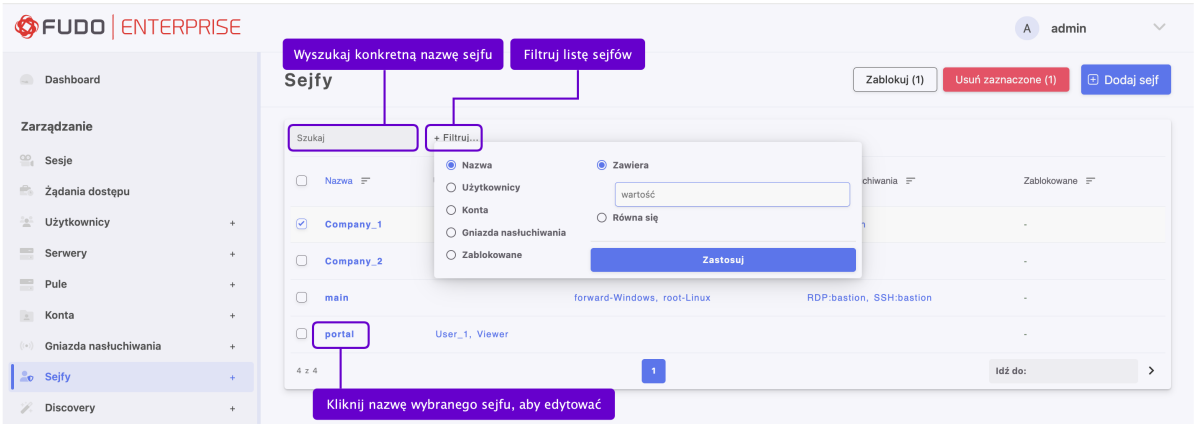
Powód zablokowania wyświetlany jest na liście obiektów po najechaniu kursorem na ikonę czerwonego X.

Tematy pokrewne:

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

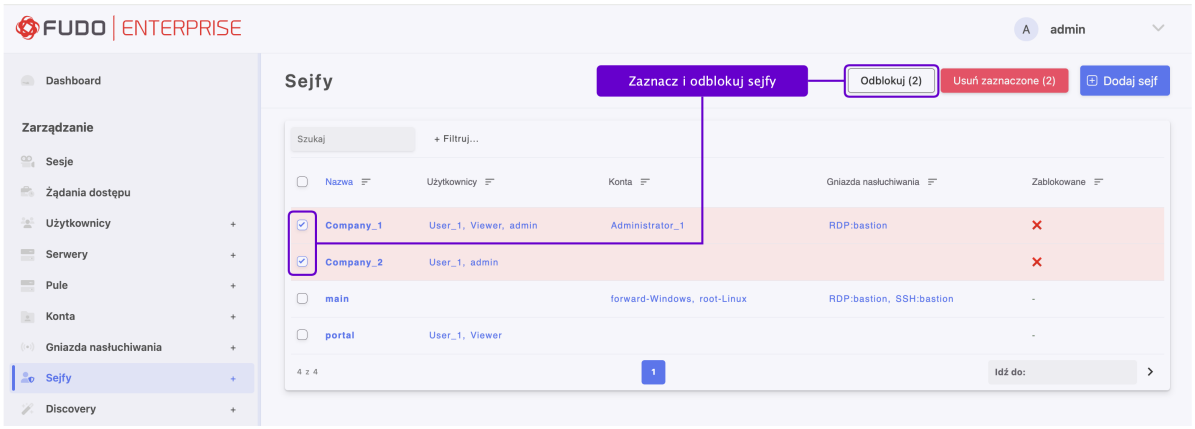
10.5.4 Odblokowanie sejfu

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.

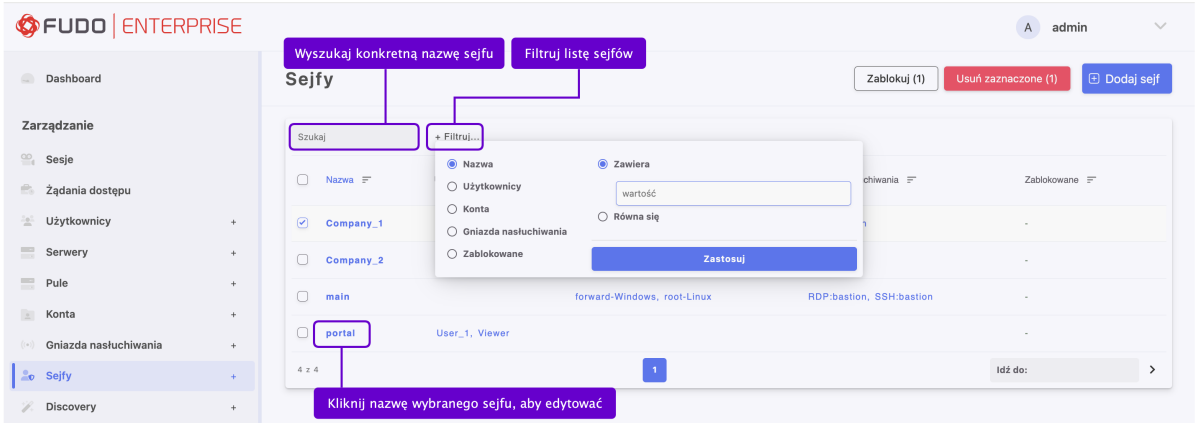
Tematy pokrewne:

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

10.5.5 Usuwanie sejfu

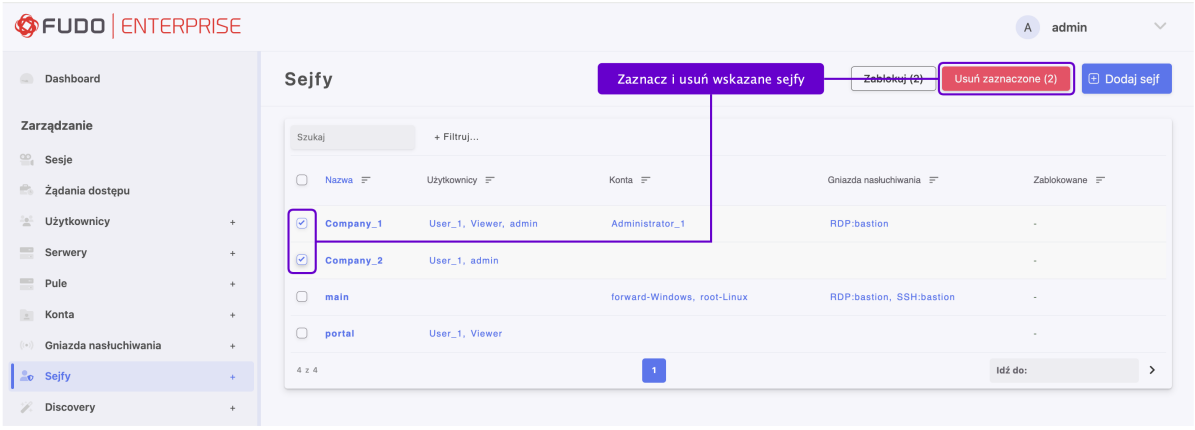
> **Ostrzeżenie**
>
> Usunięcie sejfu spowoduje przerwanie aktualnie trwających sesji z serwerami, do połączenia z którymi zostały wykorzystane konta przypisane do sejfu.

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*

10.6 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.

Uwaga

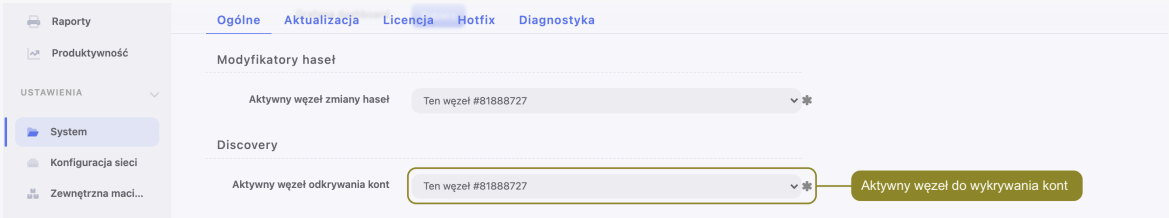
- Funkcja *Discovery* wykonuje skanowanie serwera Active Directory łącząc się przy pomocy protokołu LDAP.
- Do łączenia się z serwerem i skanowania w poszukiwaniu kont lokalnych wykorzystywany jest protokół WinRM.

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.

Uwaga

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



10.6.1 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.

10.6.1.1 Tworzenie reguły dla kont

W celu stworzenia reguły postępuj zgodnie z poniższą instrukcją:

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



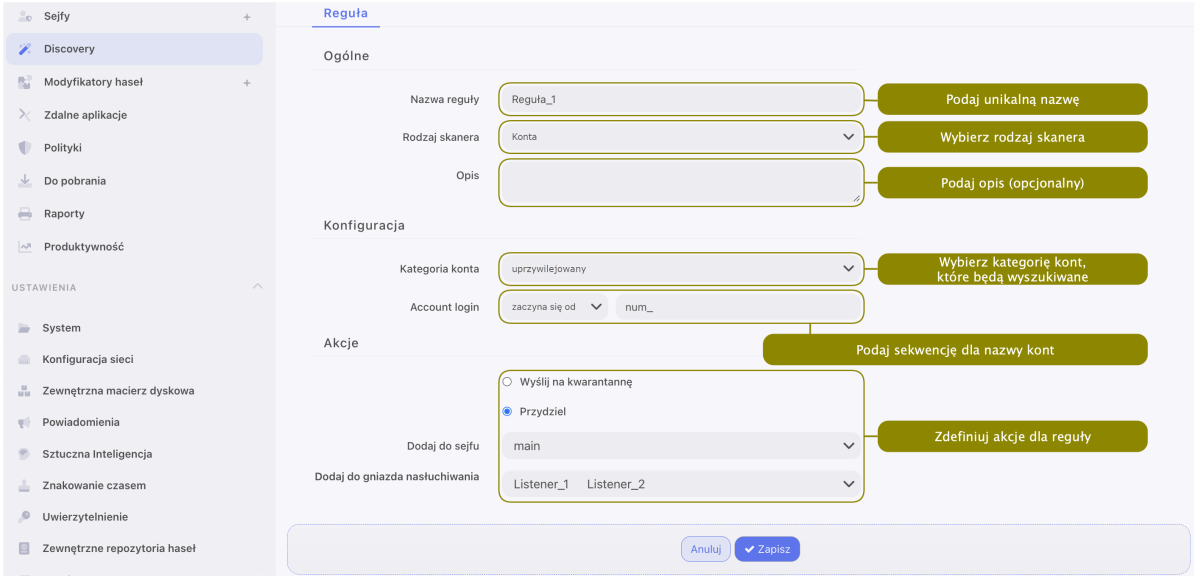
3. Wprowadź nazwę reguły.
4. Z rozwijanej listy *Typ skanera* wybierz *Konta*.
5. Opcjonalnie, wprowadź opis reguły.
6. W sekcji *Konfiguracja*:

   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*

10.6.1.2 Tworzenie reguły dla serwerów

W celu stworzenia reguły postępuj zgodnie z poniższą instrukcją:

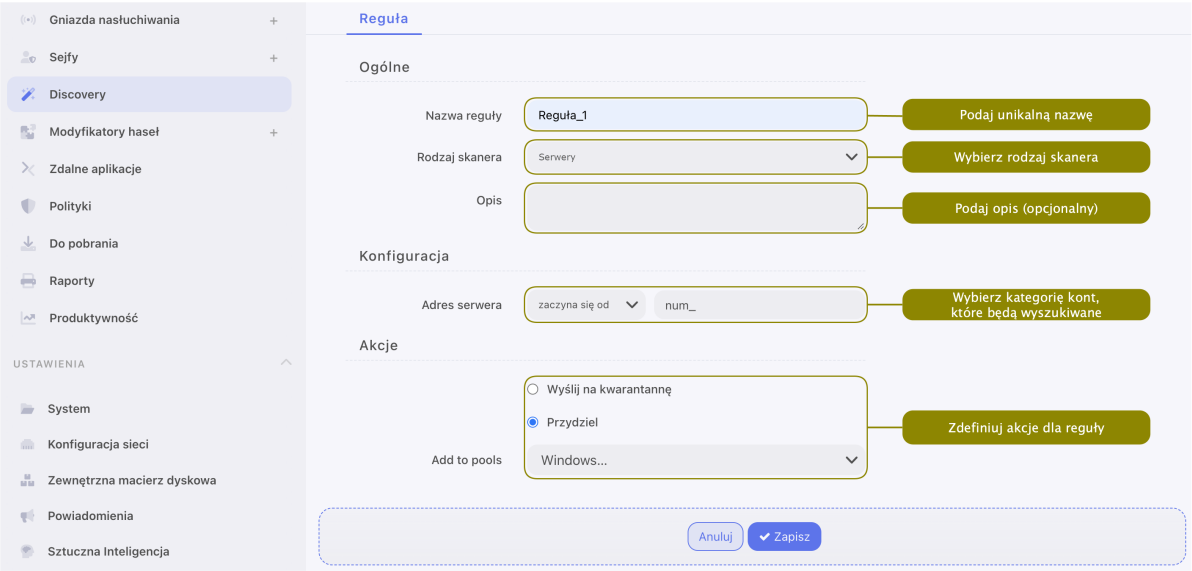
1. Wybierz *Zarządzanie* > *Discovery* > *Reguły*.
2. Kliknij + *Dodaj*.



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.



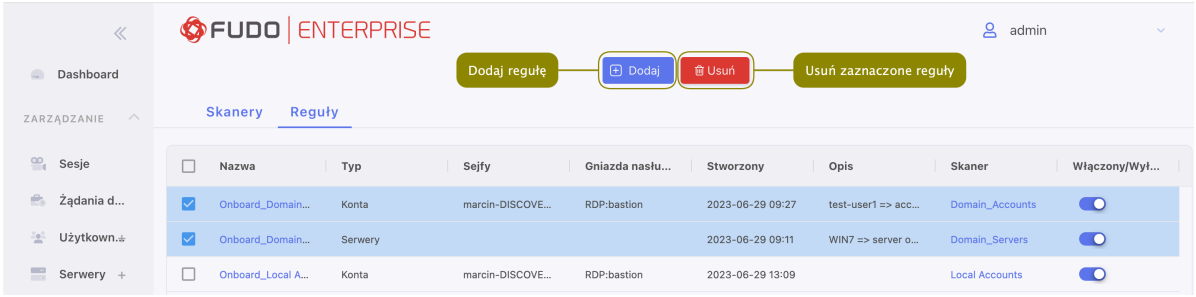
8. Kliknij *Zapisz*.

Tematy pokrewne:

- *Tworzenie skanera*
- *Zarządzanie wykrytymi kontami*

10.6.2 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*

10.6.3 Tworzenie skanera

10.6.3.1 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*.

Uwaga

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`.

   Uwaga

   Jeśli podano tylko *Base DN*, skaner przeszuka całą domenę. Określenie *Base DN* jest wymagane.

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

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

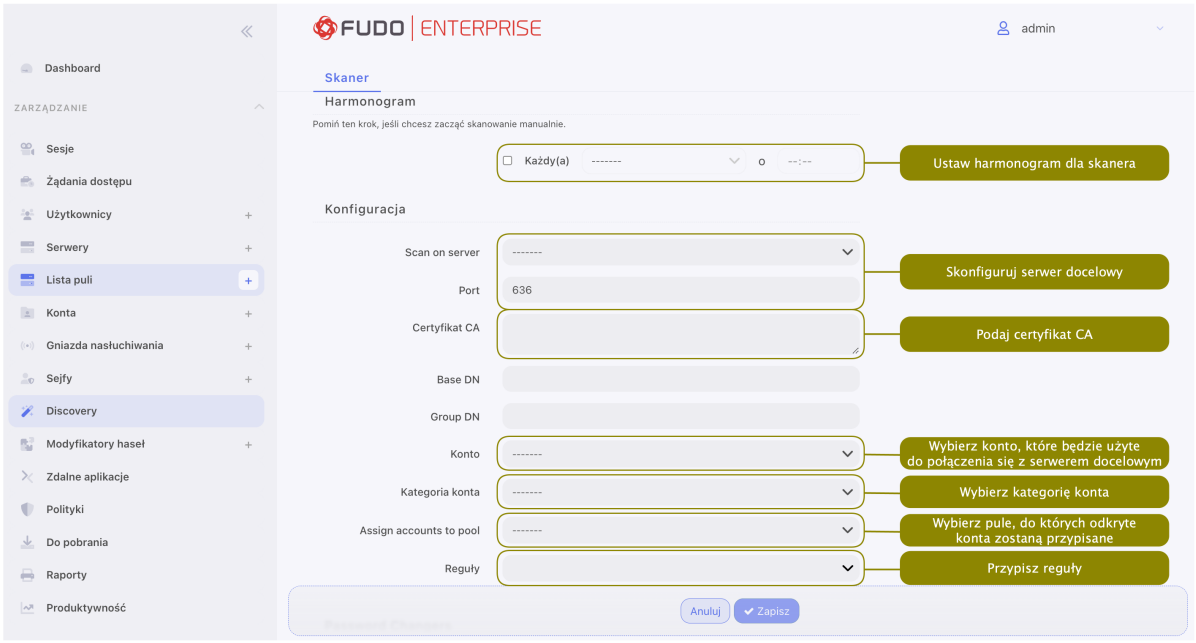
   Uwaga

   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.

Uwaga

- 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*

10.6.3.2 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*.

Uwaga

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`.

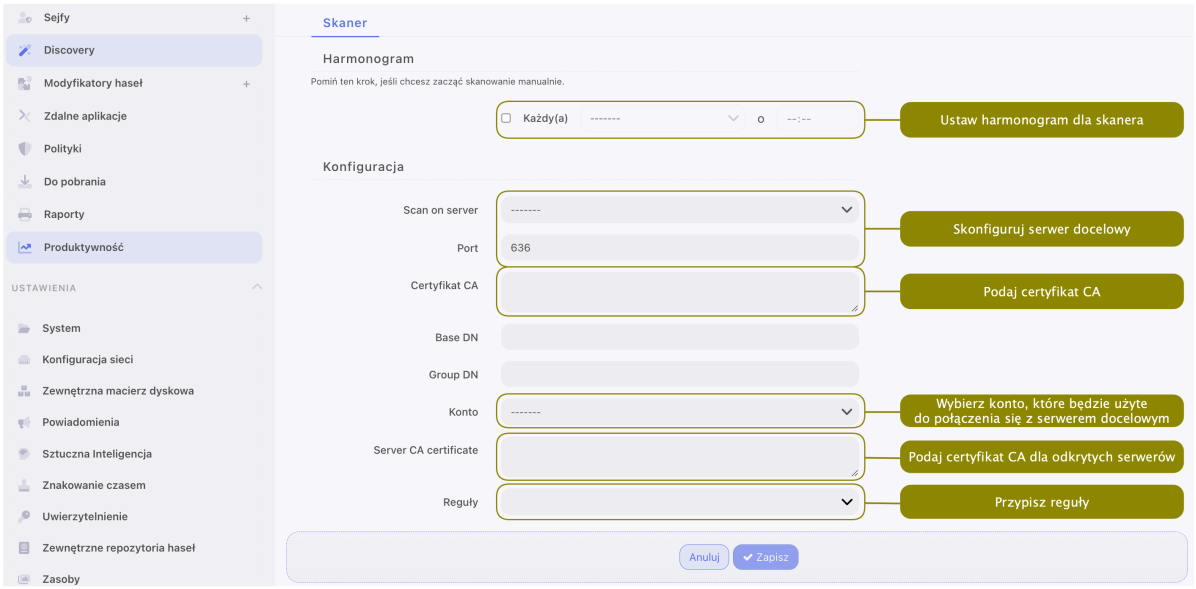
   Uwaga

   Jeśli podano tylko *Base DN*, skaner przeszuka całą domenę. Określenie *Base DN* jest wymagane.

   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*

10.6.3.3 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*.

Uwaga

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.

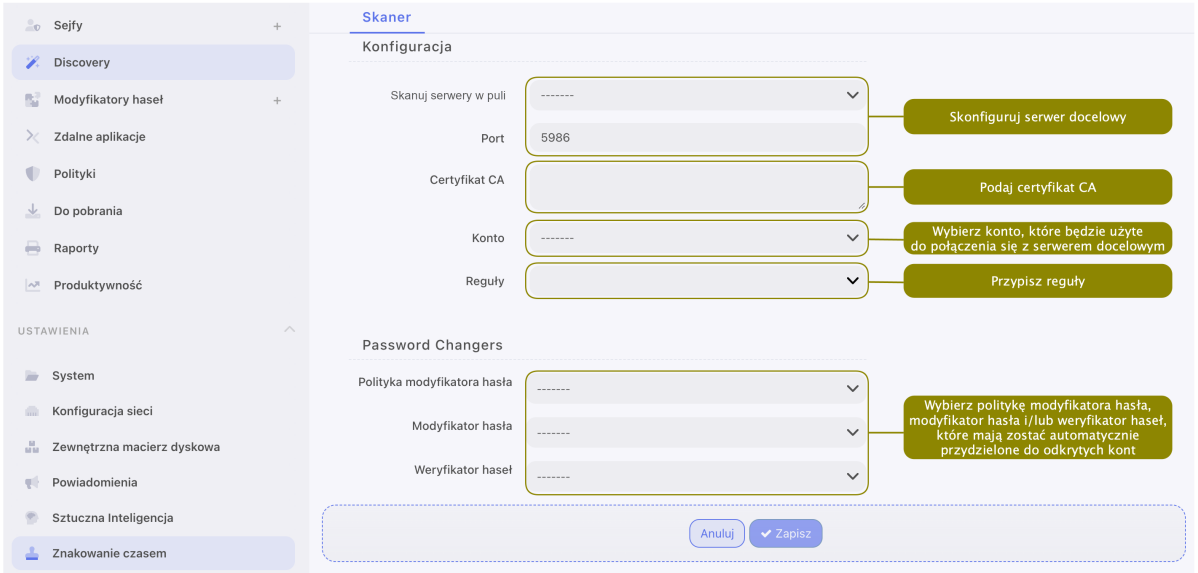
   7.3. Wprowadź *Certyfikat CA*.

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

   > **Uwaga**
   >
   > 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.

> **Uwaga**
>
> - 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*

10.6.4 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.



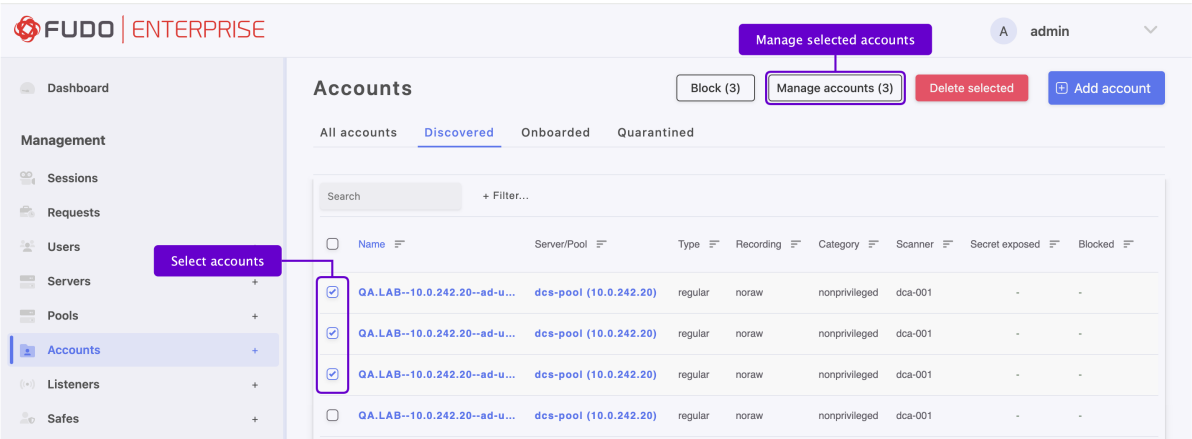
Można jednocześnie uruchomić lub usunąć kilka skanerów poprzez ich zaznaczenie i wybranie *Start* lub *Usuń*.

Tematy pokrewne:

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

10.6.5 Zarządzanie wykrytymi kontami

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

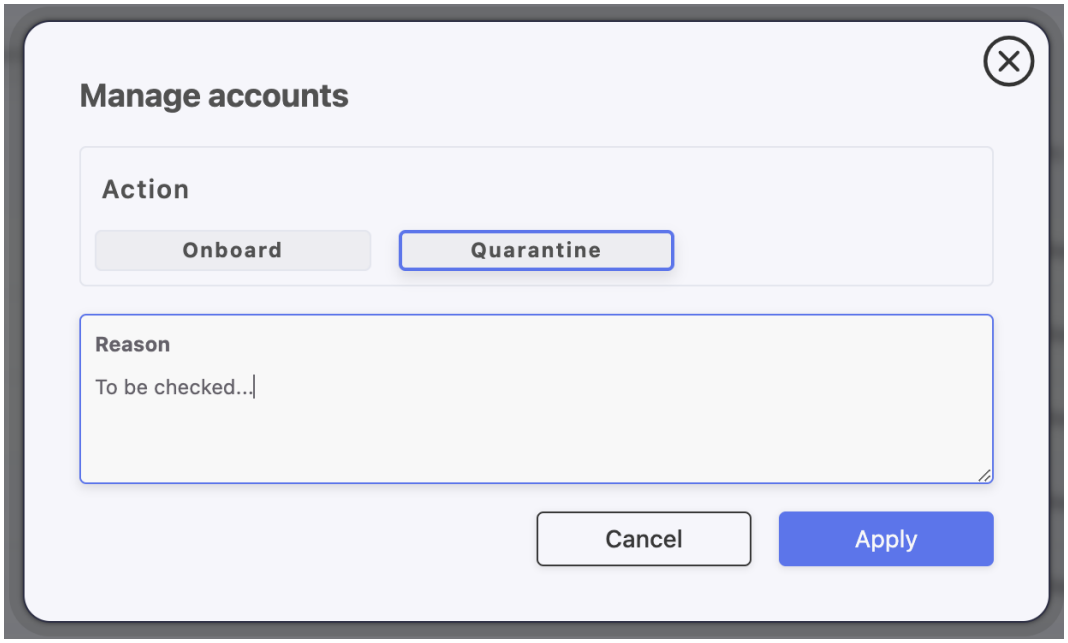


Uwaga

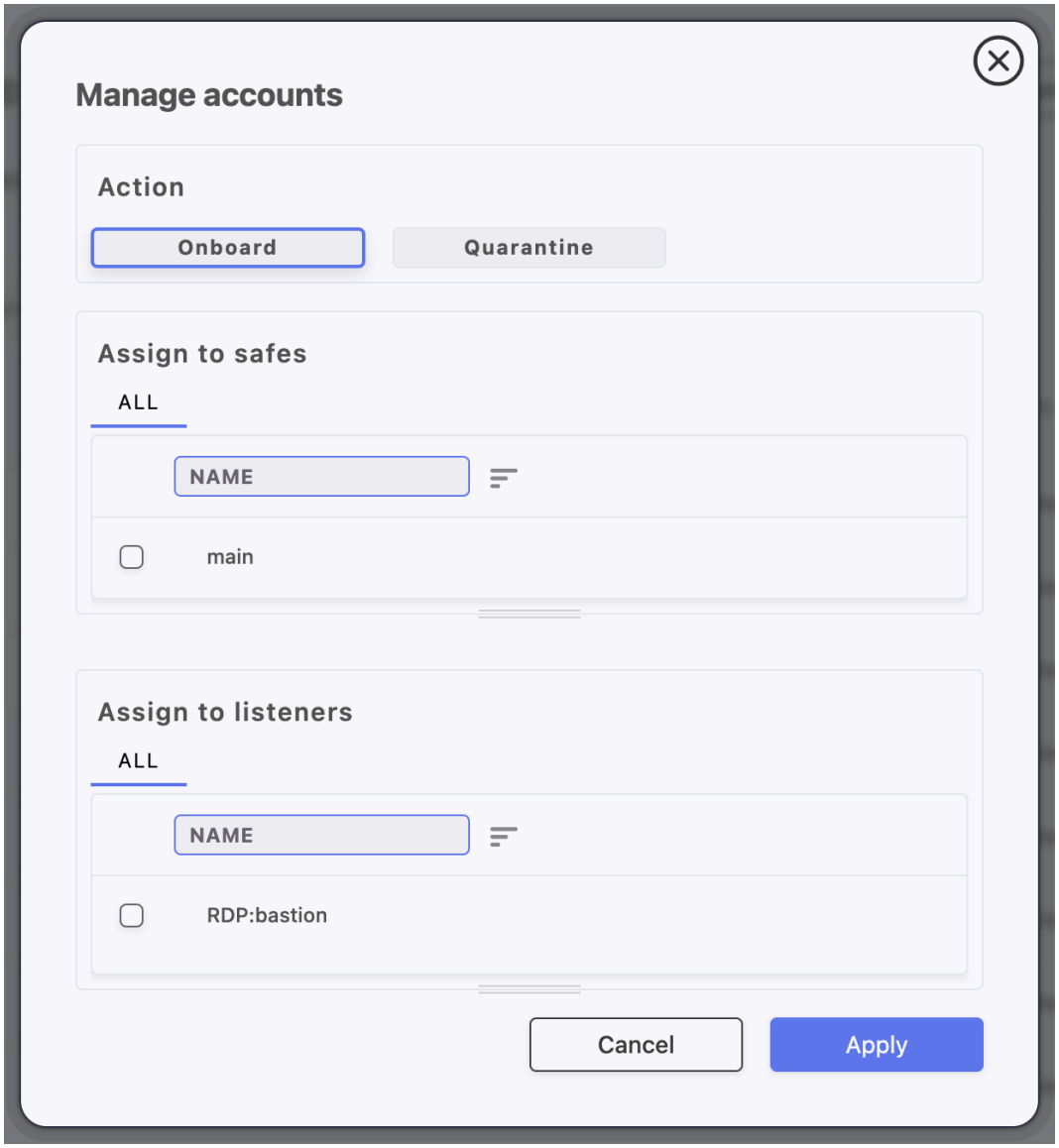
Konta, które znajdą się w zakładce *Odkryte* zostały wykryte przez skaner, lecz nie zostały ani przydzielone, ani wysłane na kwarantannę. Jest to zazwyczaj spowodowane brakiem ustawienia automatycznej reguły. Administrator może je przydzielić lub wysłać na kwarantannę manualnie, korzystając z opcji *Zarządzaj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

10.6.6 Zarządzanie wykrytymi serwerami

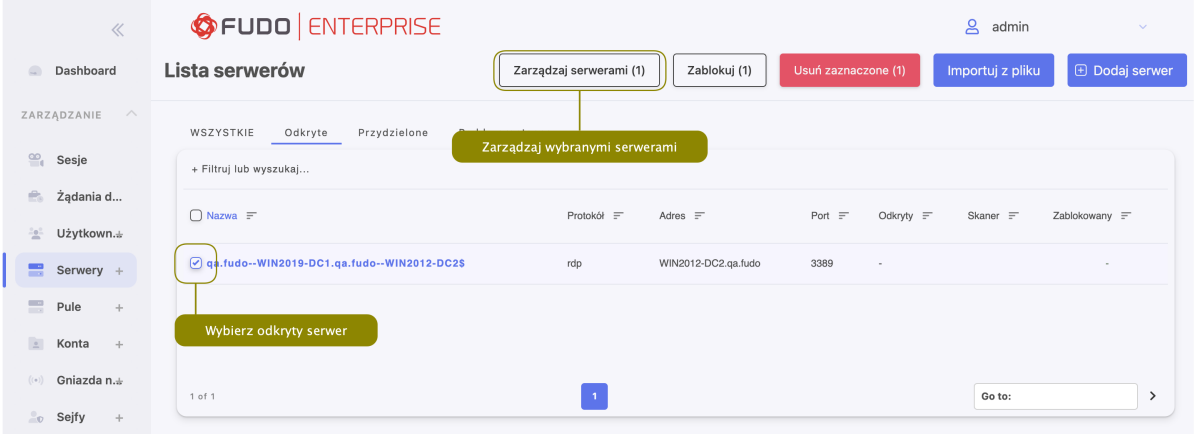
Serwery *odkryte*, *przydzielone* oraz *pod kwarantanną* dostępne są w głównym widoku zakładki *Serwery*.

Uwaga

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.

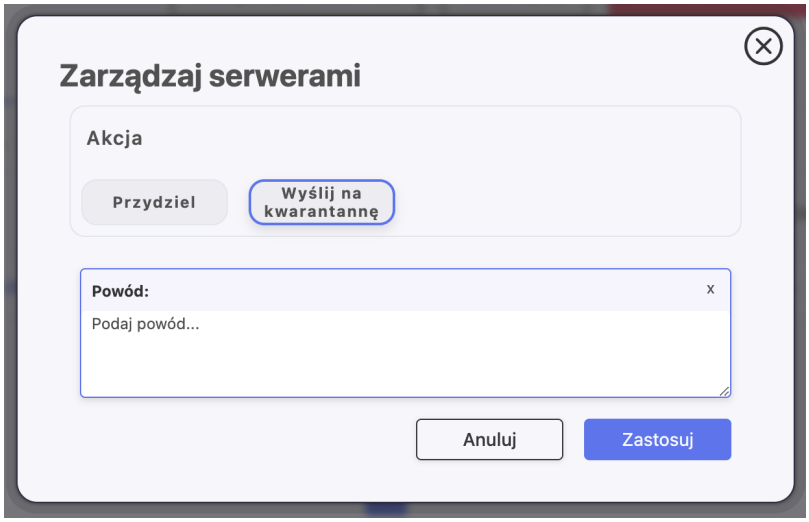
1. Wybierz *Zarządzanie* > *Serwery* > *Odkryte*
2. Zaznacz serwery, które chcesz przydzielić albo wysłać na kwarantannę.
3. Wybierz opcję *Zarządzaj serwerami*.



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*

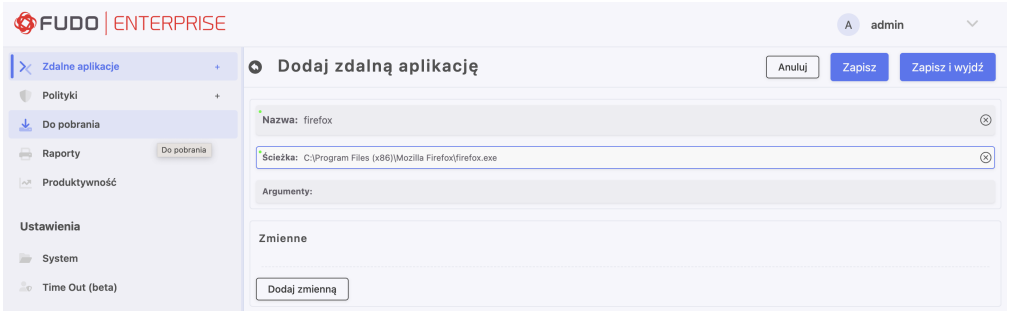
10.7 Zdalne aplikacje

Funkcja *Zdalne aplikacje* Fudo Enterprise umożliwia bezpośrednie połączenie się z wybraną aplikacją przy użyciu protokołu RDP.

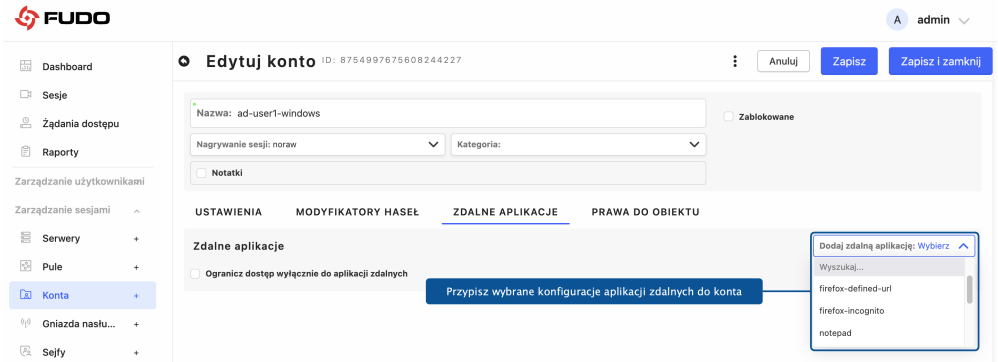
10.7.1 Dodawanie aplikacji zdalnej

Aby skonfigurować aplikację zdalną, postępuj zgodnie z instrukcją:

1. Wybierz *Zarządzanie* > *Zdalne aplikacje*.
2. Kliknij przycisk *Dodaj zdalną aplikację*.
3. Skonfiguruj aplikację zdalną według poniszych parametrów:
    - Wprowadź *Nazwę* dla aplikacji.
    - Określ *Ścieżkę* do pliku wykonywalnego aplikacji (np. `C:\Windows\System32\putty.exe`).



4. Kliknij *Zapisz i wyjdź*.
5. Dodaj utworzoną definicję aplikacji zdalnej do konta, które będzie używane do uzyskania dostępu do serwera RDP, na którym znajduje się aplikacja:
    - Wybierz *Zarządzanie* > *Konta*.
    - Edytuj konto, które będzie używane do dostępu do serwera RDP.
    - W zakładce *ZDALNE APLIKACJE* rozwiń listę *Dodaj zdalną aplikację* i wybierz definicję aplikacji zdalnej utworzoną we wcześniejszych krokach.
    - Kliknij *Zapisz*.



10.7.2 Dodawanie Argumentów

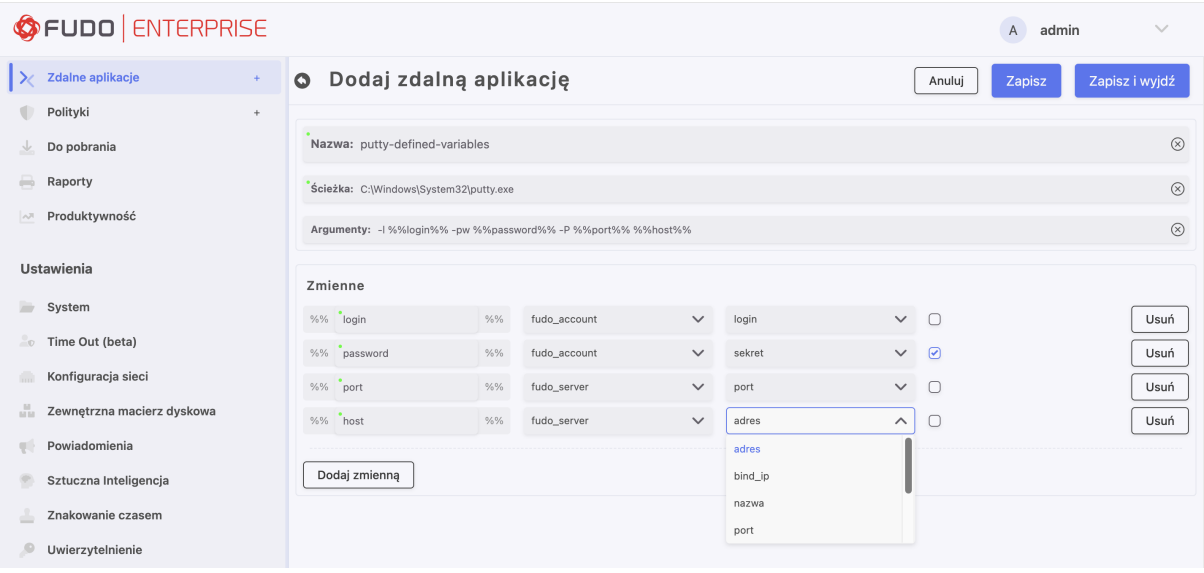
Zdalne aplikacje umożliwiają administratorom ustawienie poleceń, które są automatycznie uruchamiane przy starcie, co umożliwia bezproblemowe połączenia z wypełnionymi danymi logowania i szczegółami połączenia. Można również utworzyć zmienne do pobierania danych bezpośrednio z konfiguracji Fudo Enterprise.

1. Wybierz *Zarządzanie* > *Zdalne aplikacje*.
2. Kliknij przycisk *Dodaj zdalną aplikację* lub edytuj istniejącą konfigurację aplikacji zdalnej.
3. Przejdź do pola *Argumenty* i wprowadź polecenie, które ma być automatycznie uruchamiane przy starcie. Przykład dla aplikacji *PuTTY* z użyciem zmiennych: `-l %%login%% -pw %%password%% -P %%port%% %%host%%`.

Uwaga

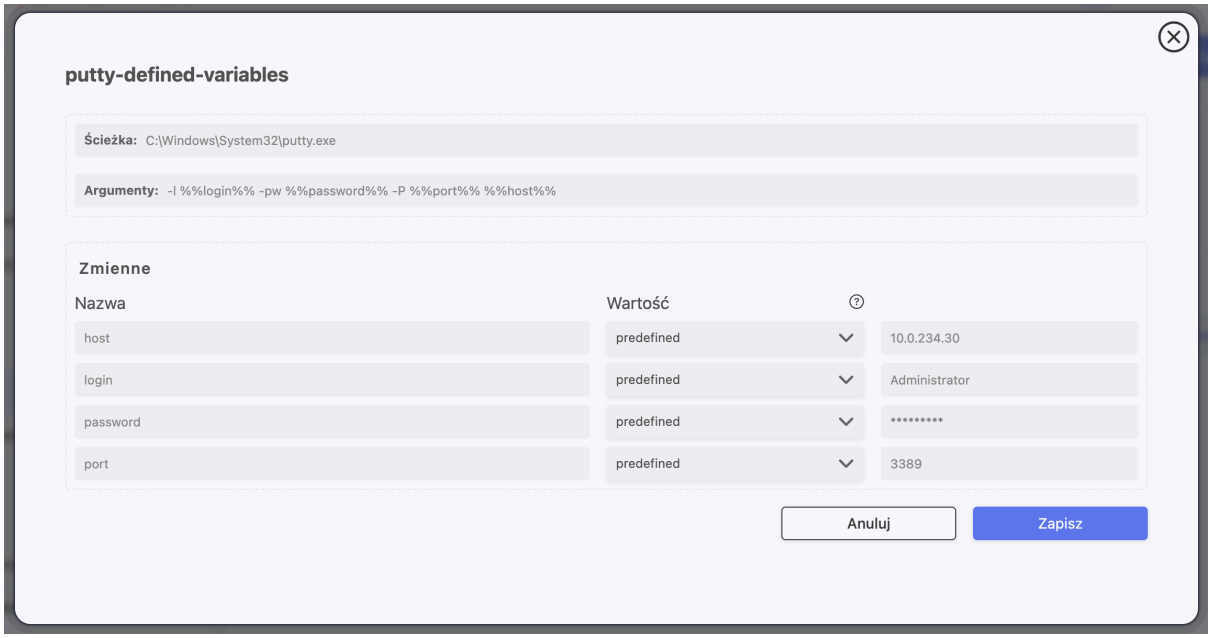
Podczas definiowania zmiennych możesz określić, którego obiektu i jakiej właściwości obiektu użyć. Możesz wybrać *Typ obiektu* i *Właściwość obiektu* dla każdego z Argumentów oraz zaszyfrować dane argumenty, zaznaczając opcję *Zaszyfruj* w wierszu obok nazwy zmiennej.

4. Używając przycisku *Dodaj zmienną*, dodaj cztery zmienne odpowiadające poleceniu wprowadzonemu w polu *Argumenty*. Przykład:
   - Nazwa zmiennej: `%%login%%`, Typ obiektu: `fudo_account`, Właściwość obiektu: `login`.
   - Nazwa zmiennej: `%%password%%`, Typ obiektu: `fudo_account`, Właściwość obiektu: `secret`.
   - Nazwa zmiennej: `%%port%%`, Typ obiektu: `fudo_server`, Właściwość obiektu: `port`.
   - Nazwa zmiennej: `%%host%%`, Typ obiektu: `fudo_server`, Właściwość obiektu: `address`.



5. Kliknij *Zapisz i wyjdź*.
6. Wartości zmiennych można zweryfikować przy dodawaniu aplikacji zdalnej do konta:
   - Wybierz *Zarządzanie* > *Konta*.

- Edytuj konto, do którego zostanie przypisana utworzona aplikacja zdalna.
- W zakładce *ZDALNE APLIKACJE* rozwiń listę *Dodaj zdalną aplikację* i wybierz definicję aplikacji zdalnej utworzoną we wcześniejszych krokach.
- Przyporządkowane wartości zmiennych będą wyświetlone w oknie modalnym.
- Kliknij przycisk *Zapisz*.



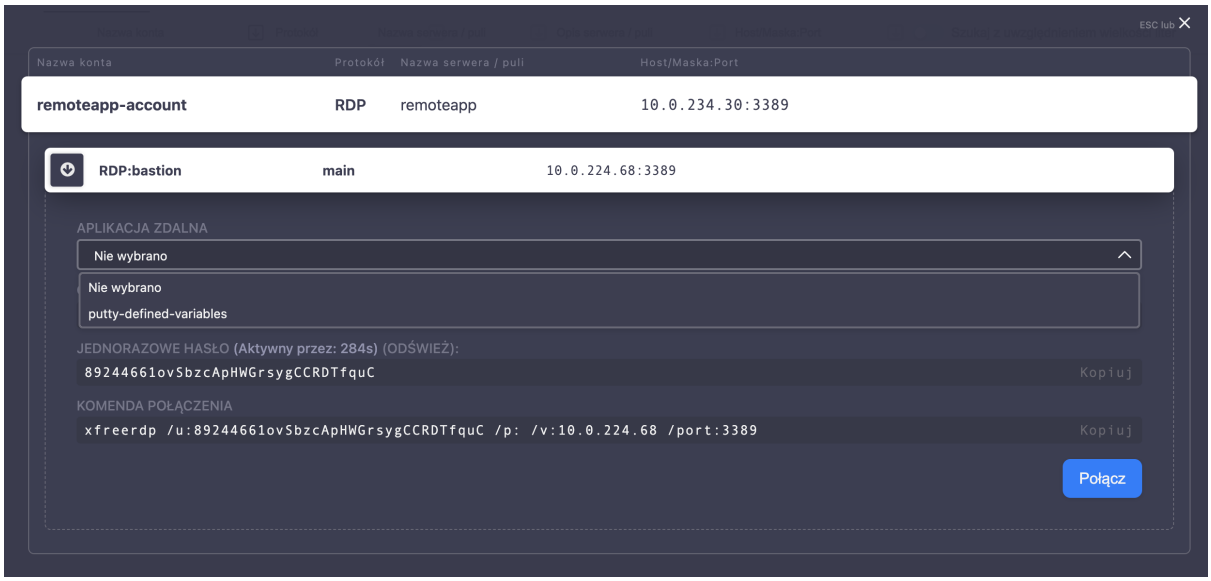
Opis dostępnych Typów Obiektów

Typ obiektu	Opis
`constant`	Zmienna o stałej wartości, edytowalna po przypisaniu aplikacji zdalnej do konkretnego konta.
`special`	Zmienna dziedziczy tajny klucz używany do ustanowienia sesji.
`fudo_server`	Zmienna dziedziczy swoją wartość z serwera przypisanego do konta korzystającego z aplikacji zdalnej. Dostępne właściwości: • `adres` - wartość z pola *Adres* serwera, • `bind_ip` - adres powiązany z serwerem, • `nazwa` - wartość z pola *Nazwa* serwera, • `port` - port przypisany do serwera, • `ssh_public_key` - klucz publiczny serwera, • `tls_ca_certificate` - certyfikat CA, • `tls_certificate` - certyfikat serwera
`fudo_account`	Zmienna dziedziczy swoją wartość z konta, do którego aplikacja zdalna jest przypisana. Dostępne właściwości:

10.7.3 Połączenie do zdalnej aplikacji przez Portal Użytkownika

Aby nawiązać połączenie, zaloguj się do Portalu Użytkownika i wybierz konto oraz gniazdo nasłuchiwania. Aby użyć aplikacji zdalnej:

1. Wybierz opcję *Klient natywny*.
2. Rozwiń listę *APLIKACJA ZDALNA* i wybierz żądaną aplikację zdalną, aby nawiązać połączenie.
3. Kliknij *Połącz*.



Uwaga

Kiedy połączenie zostaje ustanowione, sesja użytkownika jest nawiązana tylko z aplikacją. Ponieważ użytkownik nie ma dostępu do całego pulpitu, zamknięcie aplikacji automatcznie przerywa połączenie.

10.7.4 Granularny dostęp do aplikacji zdalnych

Ostrzeżenie

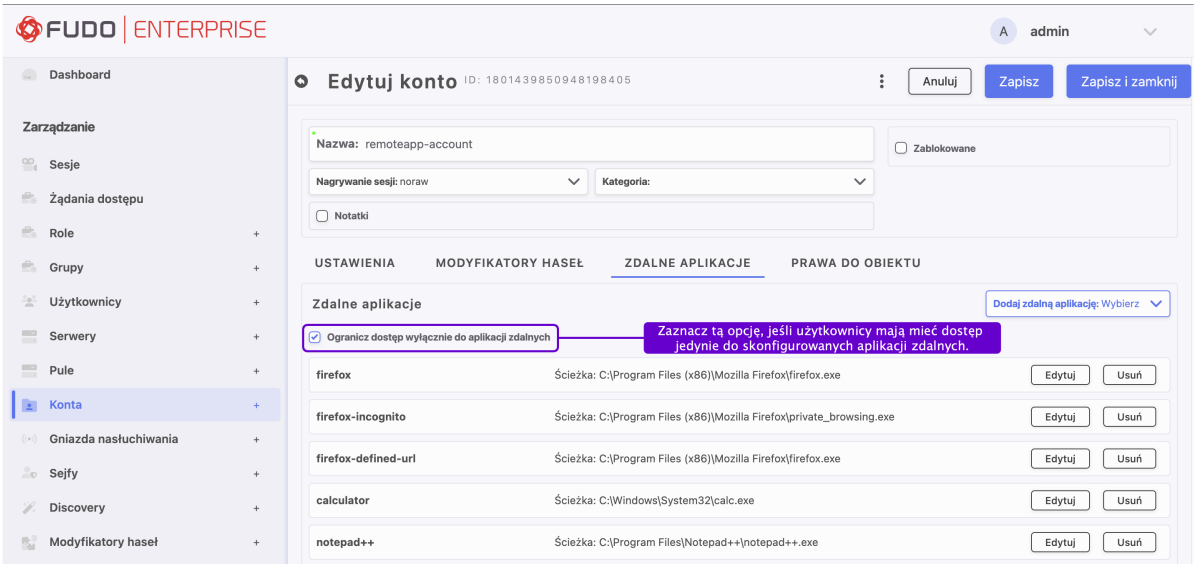
Aplikacje zdalne **nie są automatycznie zamykane** po zakończeniu sesji. Jeśli uruchomisz kolejną sesję z inną aplikacją zdalną, wcześniej otwarte aplikacje pozostaną aktywne. Może to spowodować:

- Widoczność danych lub pracy wykonanej w poprzedniej aplikacji.
- Nakładanie się okien wcześniej uruchomionych aplikacji na nowe.

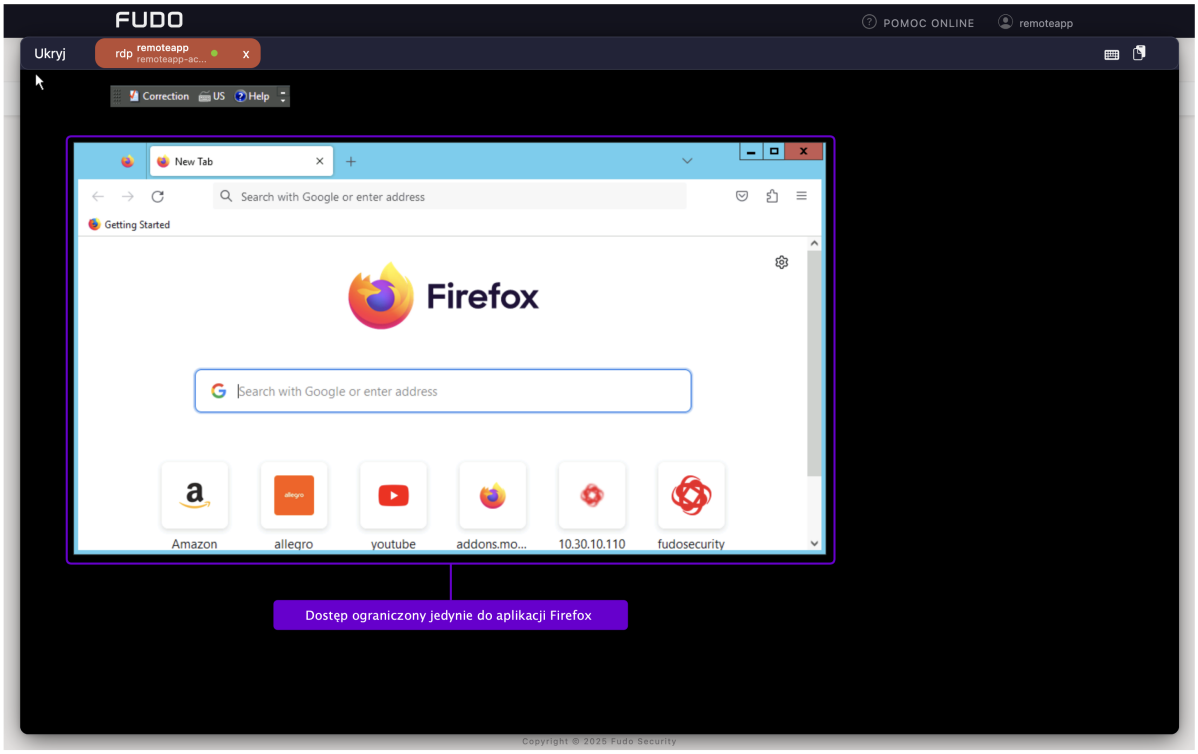
Aby usprawnić kontrolę dostępu i ograniczyć powierzchnię ataku, administratorzy ds. bezpieczeństwa mogą ograniczyć użytkownikom dostęp wyłącznie do określonych aplikacji zdalnych, bez przyznawania dostępu do pełnego pulpitu zdalnego. To udoskonalenie umożliwia precyzyjniejsze zarządzanie uprawnieniami i zapewnia, że użytkownicy mają dostęp tylko do zasobów niezbędnych do wykonywania swoich ról.

Aby włączyć to ograniczenie dla konta użytkownika:

1. Przejdź do *Zarządzanie* > *Konta*.
2. Edytuj wybrane konto użytkownika.
3. Przejdź do zakładki *ZDALNE APLIKACJE*.
4. Zaznacz pole wyboru *Ogranicz dostęp tylko do aplikacji zdalnych*.
5. Kliknij przycisk *Zapisz*.



Po włączeniu tej opcji użytkownik będzie mógł uruchamiać wyłącznie aplikacje zdalne przypisane do jego konta i nie uzyska dostępu do pełnej sesji pulpitu zdalnego.



10.7.5 Usuwanie 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 i edytuj konto posiadające skonfigurowaną zdalną aplikację.
3. W zakładce *ZDALNE APLIKACJE* wybierz opcję *Usuń* obok nazwy zdalnej aplikacji, którą zamierzasz usunąć.
4. Kliknij *Zapisz*.

Usuwanie definicji zdalnej aplikacji

Aby usunąć konfigurację zdalnej aplikacji, postępuj zgodnie z instrukcją:

1. Wybierz *Zarządzanie* > *Zdalne aplikacje*.
2. Zaznacz konfigurację zdalnej aplikacji, którą chcesz usunąć.
3. Kliknij przycisk *Usuń zaznaczone*.
4. Potwierdź usunięcie zdalnej aplikacji.

Related topics:

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

10.8 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.

10.8.1 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.

Uwaga

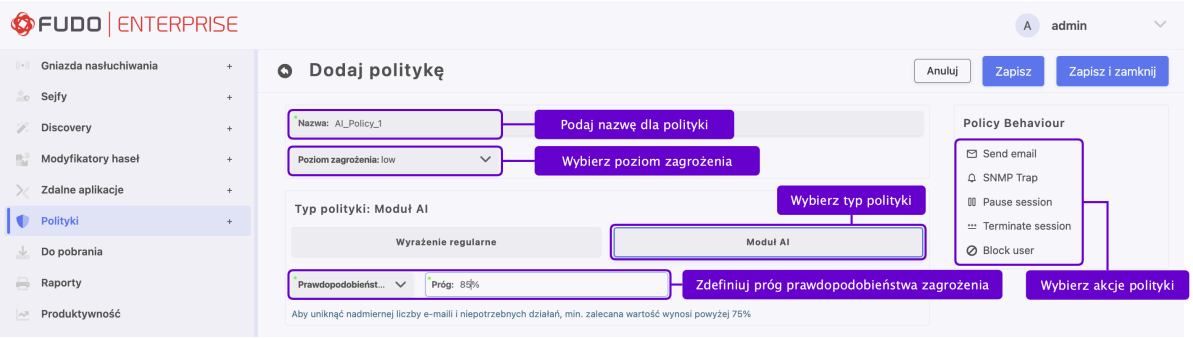
Wartości dla *Prawdopodobieństwa zagrożenia* są kalkulowane *modelem behawioralnym* dla każdego segmentu sesji. Oceny segmentów są uśredniane per model (Mouse Biometric, Keyboard Biometric), tworząc *Prawdopodobieństwo zagrożenia Modelu*, co powoduje, że moduł AI dostarcza jedną wartość dla Prawdopodobieństwa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

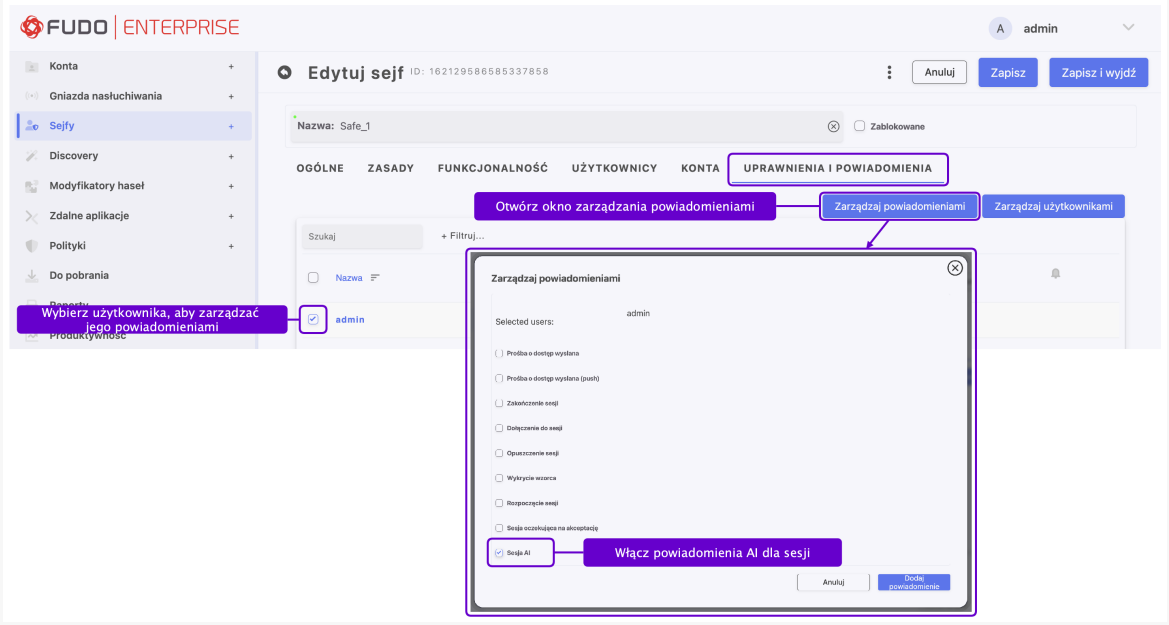
Dla drastycznych akcji, na przykład przerwanie połączenia bądź blokowania użytkownika, jest polecane korzystanie z maksymalnych progów, aby zminimalizować konsekwencje fałszywie dodatnich wyników.



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.

Uwaga

- 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*.

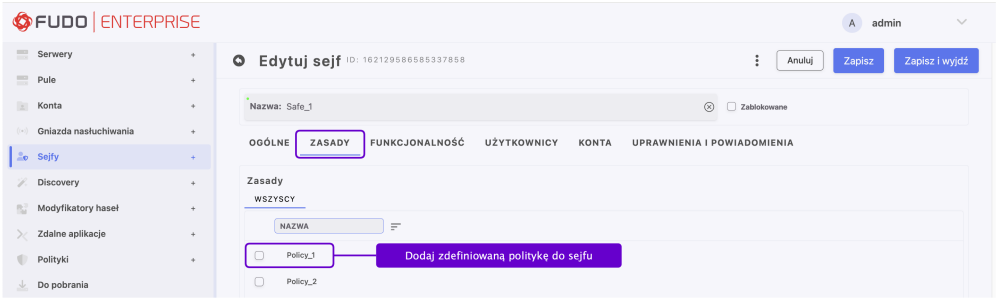
10.8.2 Przykłady polityk opartych na module AI

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.

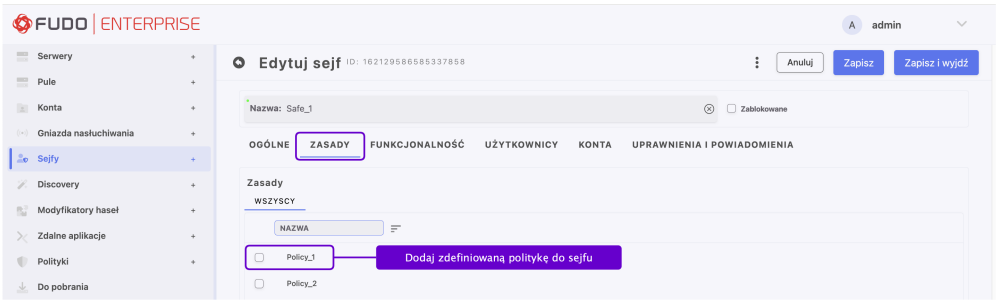
by skonfigurować politykę, przerywającą podejrzane sesje, kiedy próg Prawdopodobieństwa zagrożenia zostanie przekroczony, postępuj zgodnie z instrukcją:

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*.

Uwaga

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*
- *AI - Analiza behawioralna sesji*
- *Sejfy*
- *Terminating connection*
- *Notifications*
- *Security*

10.8.3 Definiowanie polityki na podstawie wzorca

> **Uwaga**
>
> 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.



> **Uwaga**
>
> - 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*.

Uwaga

Przykłady wyrażeń regularnych

Komenda `rm`

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

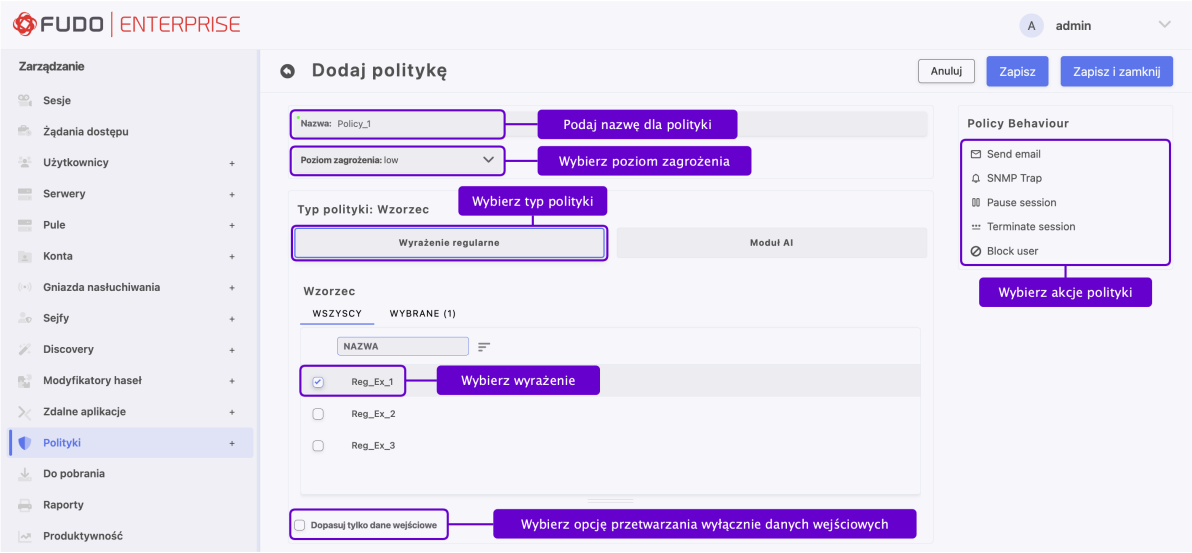
Komenda `rm -rf` (*także* `-fr`; `-Rf`; `-fR`)

```
(^|[^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.

Uwaga

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.

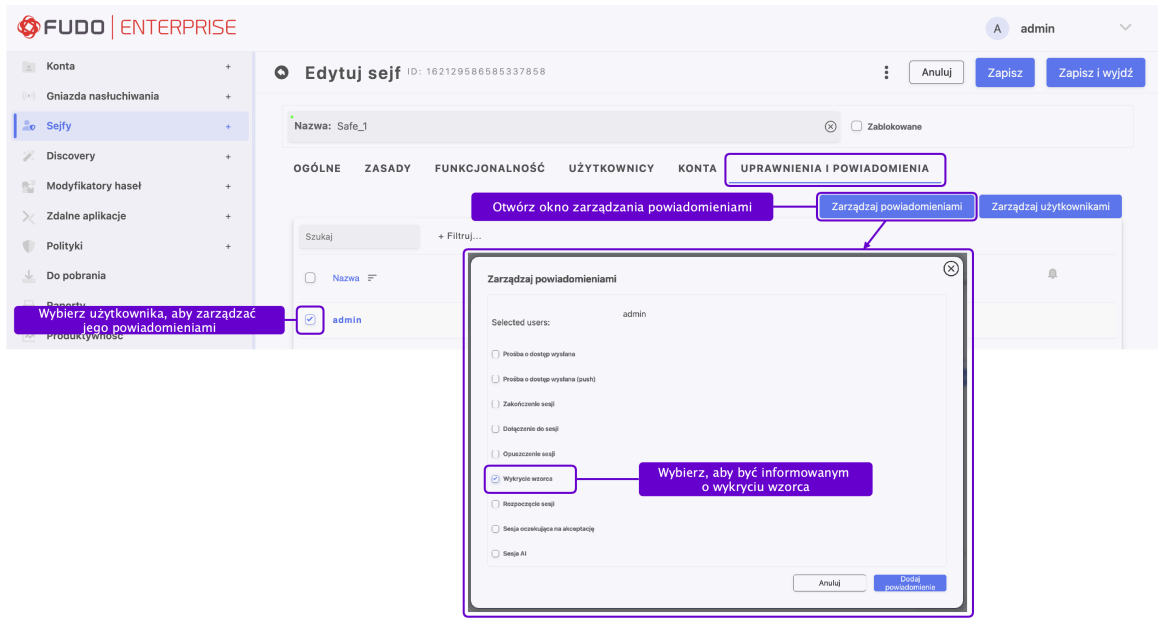
Uwaga

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.*

Uwaga

- 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*
- *AI - Analiza behawioralna sesji*

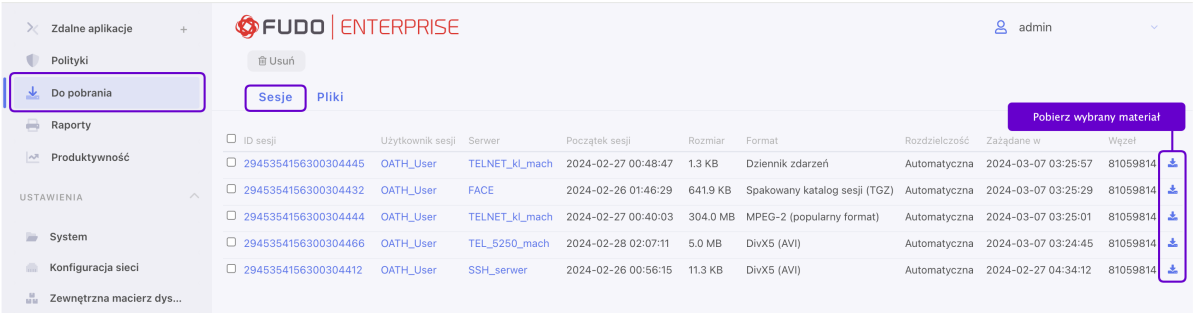
- *Sejfy*
- *Zakończenie połączenia*
- *Powiadomienia*
- *Bezpieczeństwo*

10.9 Do pobrania

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

10.9.1 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*.



10.9.2 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.

Uwaga

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*

10.10 Produktywność

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

10.10.1 Zestawienie

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

Uwaga

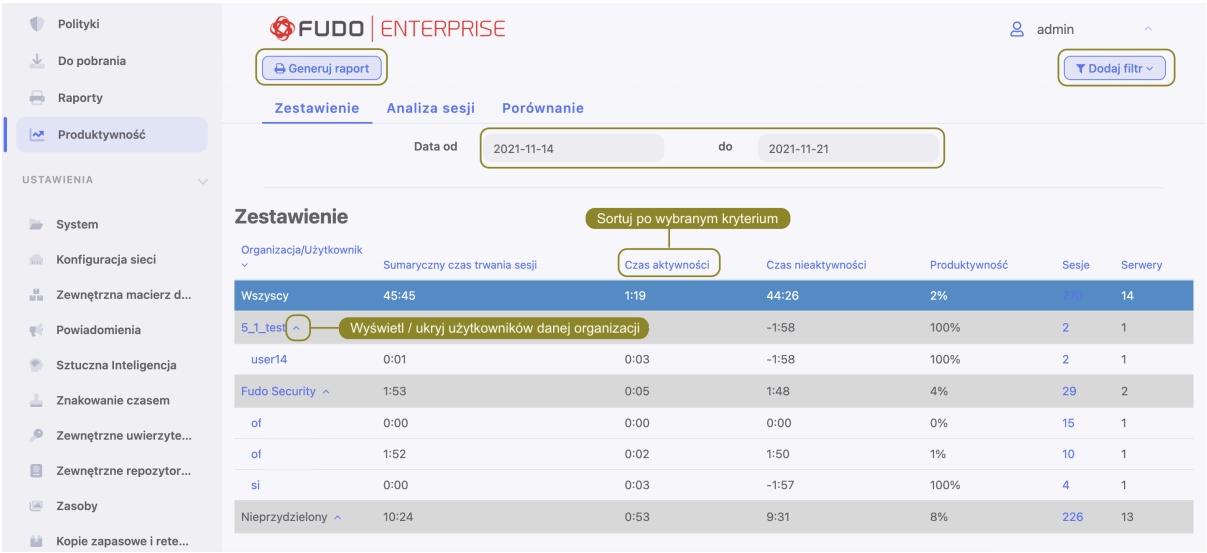
Wskaźnik aktywności określany jest na podstawie interakcji użytkownika z systemem. Fudo Enterprise dzieli czas sesji na 60 sekundowe interwały. Brak akcji ze strony użytkownika przez czas trwania interwału powoduje zaliczenie danego przedziału do czasu bezczynności.

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.

Uwaga

Zestawienie dostępne jest w sekcji *Raporty*.



Tematy pokrewne:

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

10.10.2 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.



Uwaga

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*

10.10.3 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 11

Skarbiec haseł

11.1 Opis modułu

Skarbiec haseł to moduł zarządzania poświadczeniami w Fudo Enterprise, który rozszerza standardowe funkcje systemów Privileged Access Management (PAM). Umożliwia bezpieczne, szyfrowane przechowywanie sekretów, zarządzanie ich cyklem życia, kontrolę dostępu oraz pełny audyt wykorzystania danych wrażliwych.

Moduł umożliwia bezpieczne przechowywanie i zarządzanie m.in.:

- hasłami
- kluczami SSH
- certyfikatami X.509
- kluczami API
- notatkami oraz sekretami w formie danych ustrukturyzowanych

Skarbiec haseł jest przeznaczony do zastosowań w środowiskach korporacyjnych. Obsługuje hierarchiczną organizację zasobów, kontrolę dostępu opartą na rolach, procesy dostępu ograniczonego czasowo, rotację sekretów oraz integrację z pozostałymi komponentami Fudo Enterprise.

Najważniejsze możliwości:

- przechowywanie sekretów różnych typów
- hierarchiczne kolekcje (do 5 poziomów)
- uprawnienia oparte na rolach wraz z dziedziczeniem
- wnioski o dostęp w trybie Just-in-Time i ich zatwierdzanie

- bezpieczne udostępnianie sekretów
- pełny ślad audytowy oraz niezmienna historia zmian
- wbudowane generowanie haseł i kluczy
- automatyczna rotacja poświadczeń

W kolejnych rozdziałach opisano elementy modułu Skarbiec haseł związane ze strukturą danych, modelem bezpieczeństwa oraz mechanizmami audytu.

11.1.1 Struktura skarbca haseł

Logiczna struktura skarbca haseł opiera się na sekretach i kolekcjach.

Sekrety

Sekret to pojedyncze poświadczenie lub obiekt danych poufnych, przechowywany w postaci zaszyfrowanej.

Obsługiwane typy sekretów:

- hasło
- klucz SSH (RSA, ECDSA, Ed25519)
- certyfikat X.509
- klucz API / token
- klucz szyfrowania
- notatka

Każdy sekret ma niezmienną historię zmian oraz umożliwia śledzenie dostępu.

Uwaga

Dostępność poszczególnych typów sekretów zależy od posiadanej licencji.

Kolekcje

Kolekcje służą do hierarchicznej organizacji sekretów. Ułatwiają grupowanie powiązanych poświadczeń zgodnie z logiką biznesową, strukturą działów, systemami lub środowiskami.

Cechy:

- struktura drzewiasta
- maksymalna głębokość zagnieżdżenia: 5 poziomów
- model dziedziczenia uprawnień

- osobny zakres uprawnień dla każdej kolekcji

Kolekcje stanowią podstawową granicę egzekwowania kontroli dostępu.

Typy skarbca

Skarbiec haseł jest dostępny w dwóch formach:

- Sejf osobisty – sekrety zarządzane indywidualnie przez użytkownika
- Sejf organizacji – sekrety zarządzane centralnie w organizacji

11.1.2 Przegląd architektury – model bezpieczeństwa

Skarbiec haseł wykorzystuje wielowarstwową architekturę bezpieczeństwa, która chroni dane w spoczynku, podczas transmisji oraz w trakcie przetwarzania.

Szyfrowanie



Dane przechowywane w systemie są szyfrowane przy użyciu AES-256.


Komunikacja pomiędzy komponentami systemu odbywa się z wykorzystaniem szyfrowania TLS.


Sekrety są odszyfrowywane wyłącznie wtedy, gdy jest to niezbędne do wykonania autoryzowanej operacji.

Kontrola dostępu

Kontrola dostępu jest realizowana w modelu dwuwarstwowym:

- Kontrola dostępu oparta na rolach (RBAC) – określa, kto może zarządzać kolekcjami i sekretami oraz jakie operacje może na nich wykonywać w Panelu Administracyjnym.
- Polityki dostępu – określają warunki i reguły przepływu pracy związane z przyznawaniem dostępu do sekretów, takie jak zatwierdzenia i limity czasowe, dla użytkowników uzyskujących dostęp do sekretów przez Portal Użytkownika.

Najważniejsze cechy:

- dziedziczenie uprawnień w hierarchii kolekcji,
- możliwość nadpisania polityk na niższych poziomach,
- wnioski o dostęp w trybie Just-in-Time.

Audyt

Wszystkie operacje wykonywane w skarbcu haseł są rejestrowane przez mechanizm audytu. Można je śledzić w zakładce **Skarbiec haseł** > **Dostęp do sekretów**.

Uwaga

- Operacje na sekretach (podgląd, wypożyczanie / zwrot) można śledzić w zakładce **Skarbiec haseł > Dostęp do sekretów**.
- Aby wyświetlić wszystkie logi związane ze skarbcem haseł, przejdź do zakładki Dzienniki zdarzeń.

Fudo Enterprise śledzi m.in.:

- zmiany uprawnień,
- wnioski o dostęp oraz ich zatwierdzanie,
- operacje wypożyczania i zwrotu sekretu,
- zdarzenia użycia sekretów,
- operacje rotacji.

Uwaga

Każdy sekret ma niezmienną historię wersji. Aby wyświetlić logi dla konkretnego sekretu, edytuj sekret i otwórz podzakładkę Logi aktywności.

11.1.3 Rejestrowanie zdarzeń i ślad audytowy

Skarbiec haseł zapewnia kompleksowe rejestrowanie zdarzeń i pełną rozliczalność dostępu do kolekcji oraz sekretów.

Rejestrowane zdarzenia obejmują m.in.:

- próby uwierzytelniania i autoryzacji,
- dostęp do sekretów (podgląd, kopiowanie, pobieranie),
- wypożyczenie sekretu oraz automatyczny zwrot,
- zdarzenia generowania sekretów,
- operacje rotacji haseł/kluczy,
- zmiany polityk,
- działania administracyjne.

Uwaga

Aby wyświetlić wszystkie logi, przejdź do zakładki Dzienniki zdarzeń. Aby wyświetlić logi dla konkretnego sekretu, edytuj sekret i otwórz podzakładkę Logi aktywności.

Śledzenie wypożyczenia / zwrotu sekretów

W przypadku wykonania operacji wypożyczenia:

- sekret może zostać zablokowany do wyłącznego użycia,

- operacja jest rejestrowana wraz z identyfikatorem użytkownika, znacznikiem czasu oraz zakresem,
- po przekroczeniu limitu bezczynności może nastąpić automatyczny zwrot sekretu.

Wszystkie zdarzenia wypożyczenia / zwrotu sekretów są przechowywane w logach.

Zgodność

Funkcjonalność audytu zapewnia:

- pełną historię operacyjną,
- niezmienne śledzenie zmian,
- przekazywanie logów do systemów zewnętrznych (np. integrację z SIEM).

Ślad audytowy zapewnia rozliczalność wszystkich operacji wykonywanych na poświadczeniach kont uprzywilejowanych w systemie.

11.2 Kolekcje

11.2.1 Tworzenie kolekcji

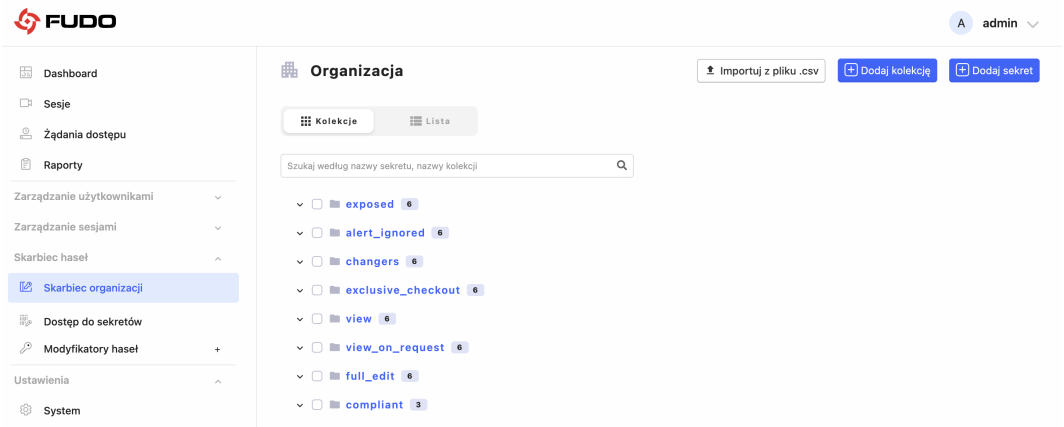
Kolekcje służą do organizowania i grupowania sekretów w uporządkowany sposób. Pomaga to w zarządzaniu uprawnieniami dostępu i utrzymywaniu powiązanych sekretów razem.

Uwaga

Funkcje Kolekcji:

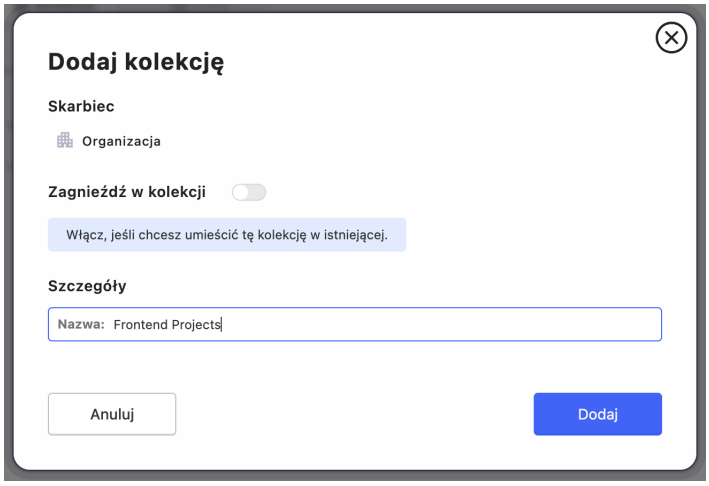
- **Organizacja**: Kolekcje pomagają organizować sekrety według projektu, zespołu lub celu.
- **Struktura Zagnieżdżona**: Kolekcje mogą być zagnieżdżane w innych kolekcjach dla hierarchicznej organizacji.
- **Kontrola Dostępu**: Różne uprawnienia mogą być przypisane do różnych kolekcji.

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij *+ Dodaj kolekcję*.

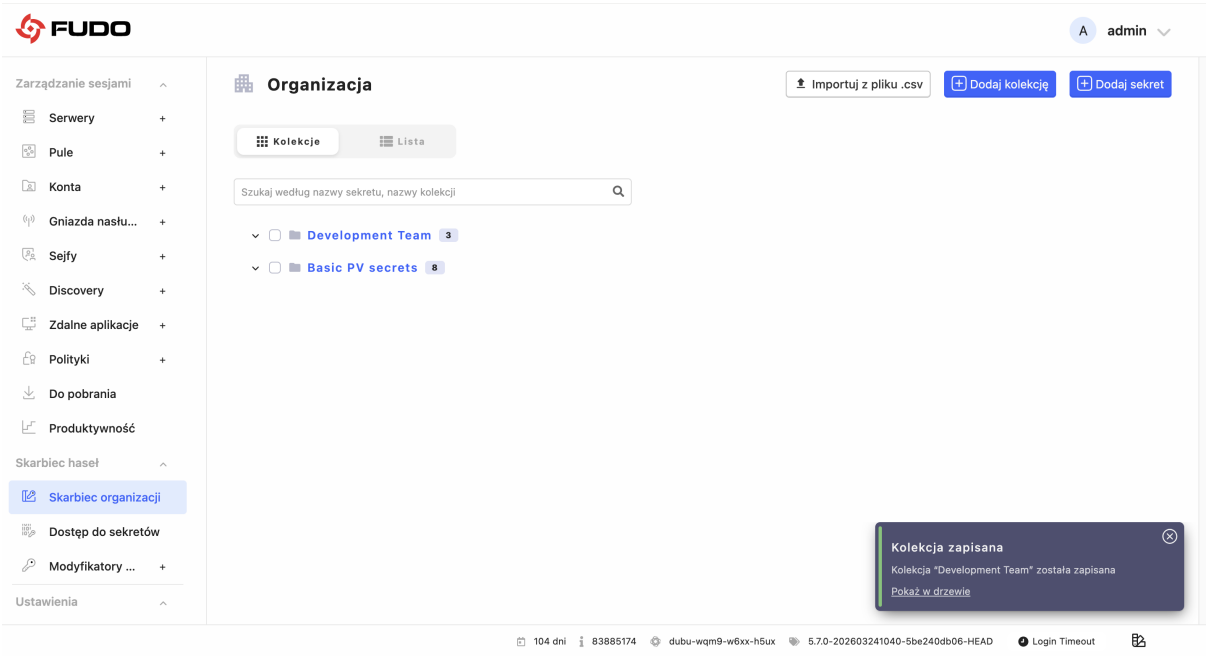


3. W oknie modalnym wprowadź nazwę kolekcji w polu *Nazwa*.

4. Opcjonalnie włącz *Zagnieźdź w kolekcji* jeśli chcesz umieścić tę kolekcję wewnątrz istniejącej.
5. Kliknij *Dodaj* aby utworzyć kolekcję lub *Anuluj* aby przerwać.



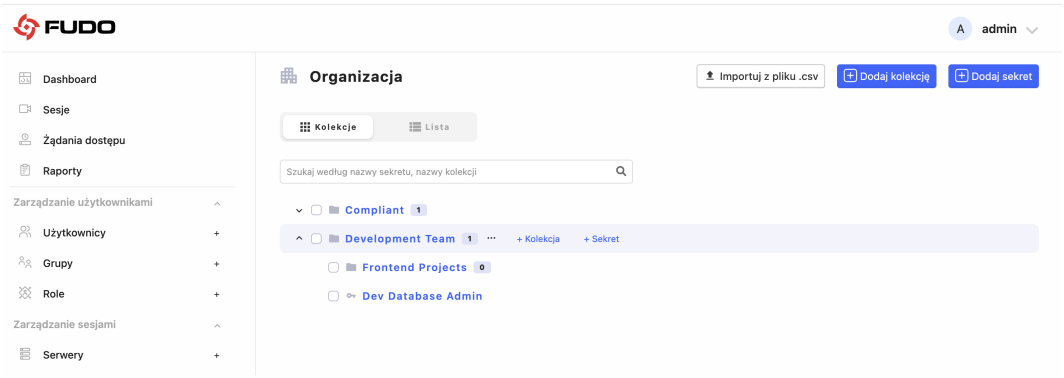
Po pomyślnym utworzeniu kolekcji, zobaczysz komunikat potwierdzający, a nowa kolekcja pojawi się na liście.



Alternatywne metody tworzenia kolekcji:

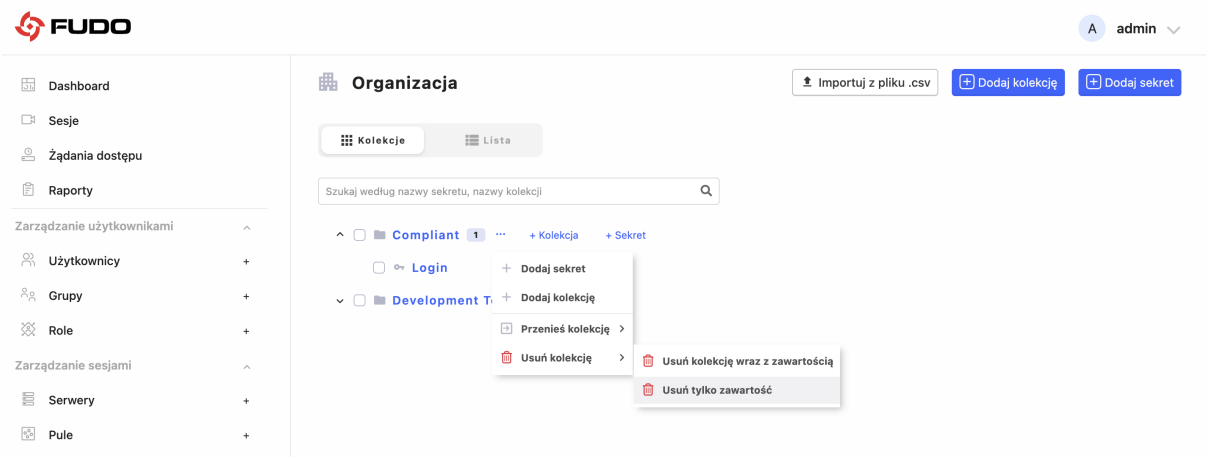
Możesz również tworzyć kolekcje używając menu szybkich akcji:

1. Najedź kursorem na istniejącą kolekcję aby wywołać przyciski akcji
2. Kliknij *+ Kolekcja* aby utworzyć zagnieżdżoną kolekcję wewnątrz wybranej kolekcji



Lub użyj menu kontekstowego:

1. Najedź kursorem na kolekcję i kliknij przycisk trzech kropek (. . .)
2. Wybierz **Dodaj Kolekcję** z menu kontekstowego



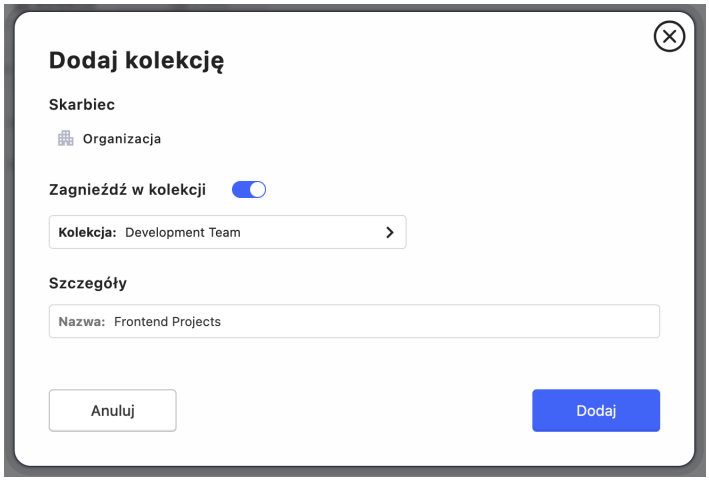
Powiązane tematy:

- *Dostęp do edycji kolekcji*
- *Zagnieżdżanie kolekcji*
- *Opis modułu*

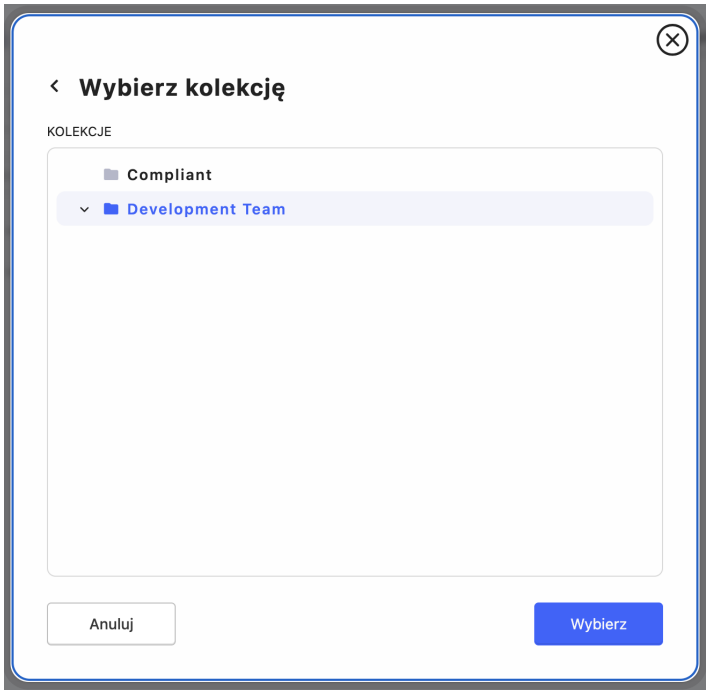
11.2.2 Zagnieżdżanie kolekcji

Kolekcje mogą być organizowane w strukturze hierarchicznej poprzez zagnieżdżanie ich w innych kolekcjach. Funkcja ta pozwala na tworzenie logicznych grup i podgrup sekretów dla lepszej organizacji i kontroli dostępu.

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij *Dodaj kolekcję*.
3. W oknie modalnym włącz opcję *Zagnieźdź w kolekcji*.

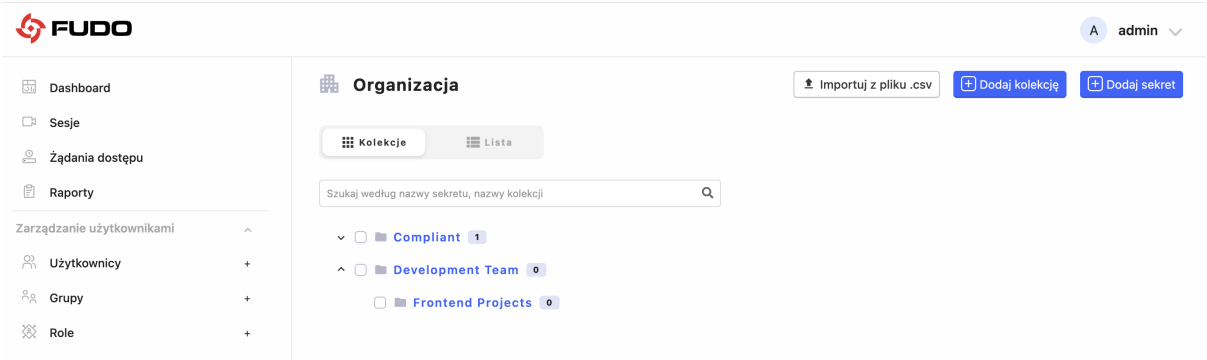


4. Kliknij na rozwijaną listę *Kolekcja* aby wybrać kolekcję nadrzędną.
5. Wybierz żądaną kolekcję nadrzędną z listy i kliknij *Wybierz*.



6. Wprowadź nazwę dla zagnieżdżonej kolekcji w polu *Nazwa*.
7. Kliknij *Dodaj* aby utworzyć zagnieżdżoną kolekcję.

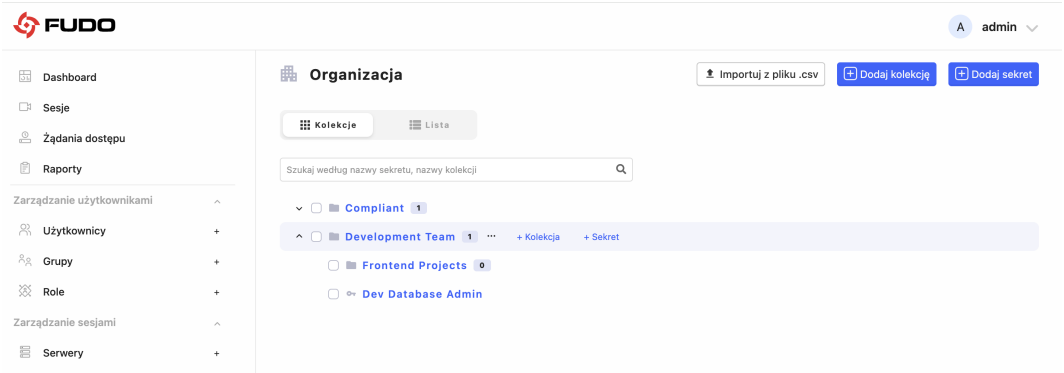
Po utworzeniu zagnieżdżonej kolekcji zobaczysz ją wyświetloną w hierarchicznej strukturze drzewa. Aby zobaczyć zagnieżdżone kolekcje, rozwiń kolekcję nadrzędną klikając na strzałkę obok niej.



Alternatywne metody zagnieżdżania:

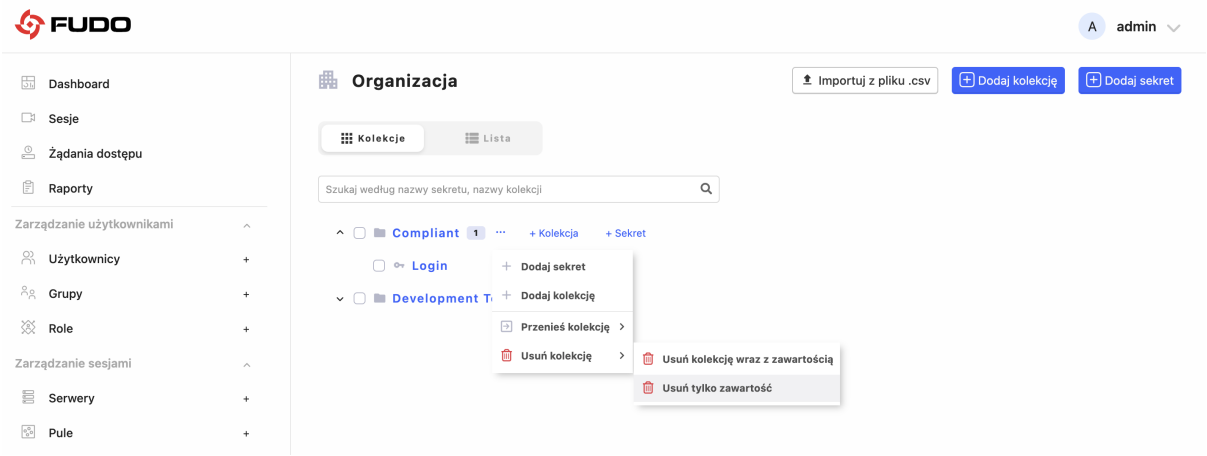
Możesz również zagnieżdżać kolekcje używając menu szybkich akcji:

1. Najedź kursorem na istniejącą kolekcję aby wywołać przyciski akcji.
2. Kliknij *+ Kolekcja* aby utworzyć zagnieżdżoną kolekcję w wybranej kolekcji.



Lub użyj menu kontekstowego:

1. Najedź kursorem na kolekcję i kliknij przycisk trzech kropek (. . .).
2. Wybierz **Dodaj Kolekcję** z menu kontekstowego.



Przykładowe zastosowania

Kolekcje umożliwiają uporządkowanie sekretów zgodnie z potrzebami organizacji. Mogą odzwierciedlać strukturę projektową, zespołową lub podział według usług i aplikacji:

- **Struktura projektowa** – podział na projekty oraz środowiska, na przykład deweloperskie, testowe i produkcyjne.

- **Struktura zespołowa** – podział zgodny ze strukturą zespołów i podzespołów.
- **Kategorie usług** – grupowanie według typu usługi oraz konkretnych aplikacji lub systemów.

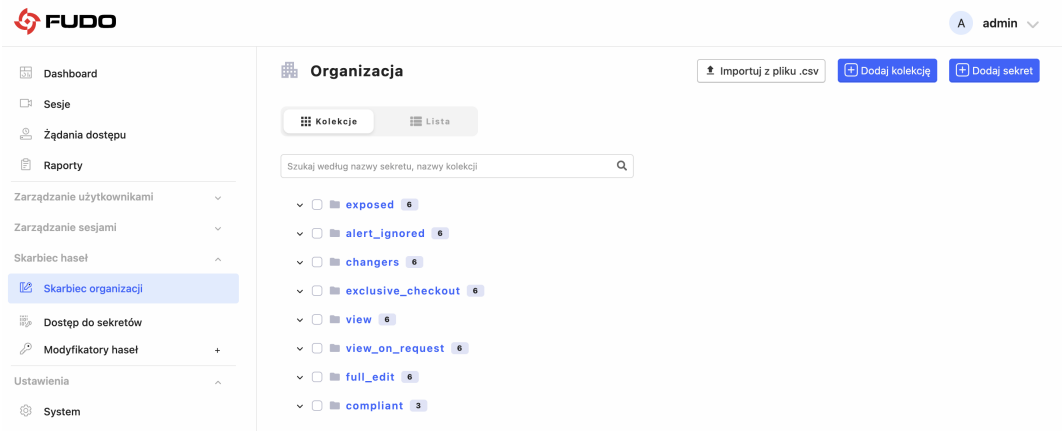
Powiązane tematy:

- *Tworzenie kolekcji*
- *Opis modułu*
- *Sekrety*
- *Kolekcje*

11.2.3 Dostęp do edycji kolekcji

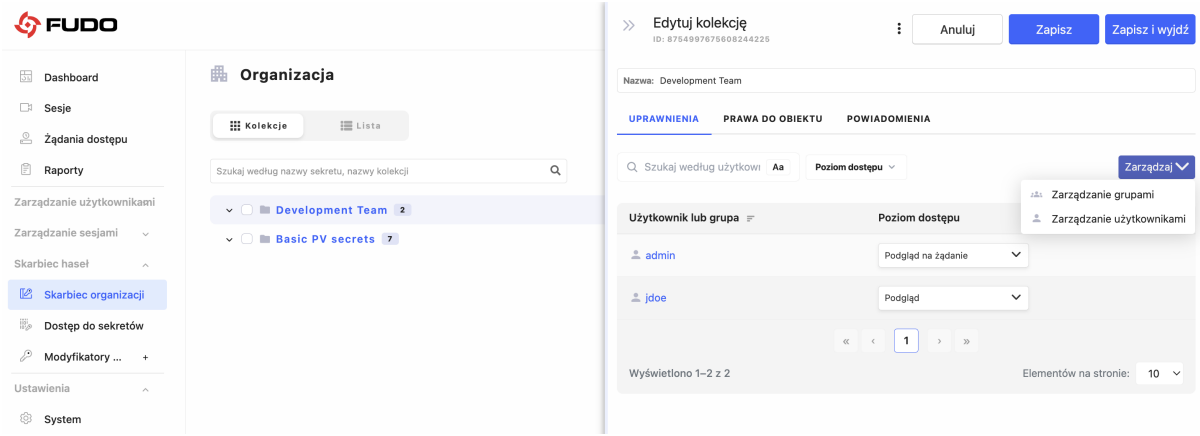
Kolekcje można edytować w celu modyfikowania ich właściwości, zarządzania uprawnieniami, przypisywania użytkowników i ról oraz konfigurowania powiadomień. Istnieje kilka sposobów uzyskania dostępu do interfejsu edycji kolekcji.

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij nazwę kolekcji, którą chcesz edytować.



11.2.3.1 Panel edycji kolekcji

Kliknięcie na nazwę kolekcji otwiera rozbudowany panel edycji z następującymi zakładkami:



USTAWIENIA OGÓLNE

W widoku ogólnym można zmienić nazwę kolekcji oraz wyświetlić unikalny identyfikator kolekcji (tylko do odczytu).

ZAKŁADKA UPRAWNIENIA

Zakładka *UPRAWNIENIA* umożliwia przypisywanie do kolekcji użytkowników i grup oraz określenie, w jaki sposób mogą oni uzyskiwać dostęp do przechowywanych w niej sekretów przez Portal Użytkownika.

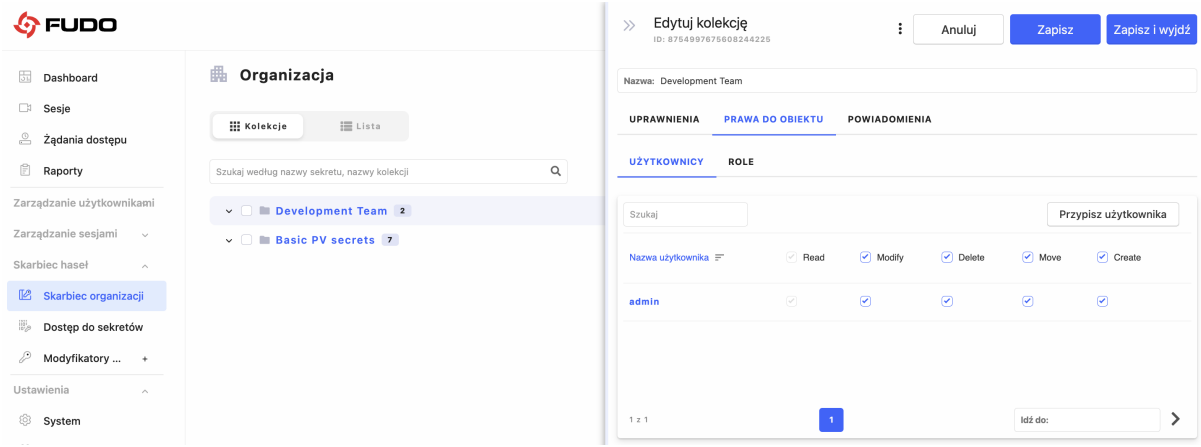
Uwaga

Uprawnienia kontrolują widoczność kolekcji w Portalu Użytkownika oraz określają, co użytkownicy mogą robić z przechowywanymi w niej sekretami. W zależności od przypisanego poziomu uprawnień użytkownicy mogą wyświetlać sekrety na żądanie, wyświetlać je bezpośrednio, edytować istniejące sekrety oraz dodawać nowe sekrety do kolekcji.

Uwaga

Szczegółowy opis uprawnień kolekcji znajduje się w sekcji *Przypisywanie użytkowników i grup do kolekcji*.

ZAKŁADKA PRAWA DO OBIEKTU



Zakładka *PRAWA DO OBIEKTU* jest częścią modelu RBAC i umożliwia zarządzanie kolekcją jako obiektem administracyjnym.

Uwaga

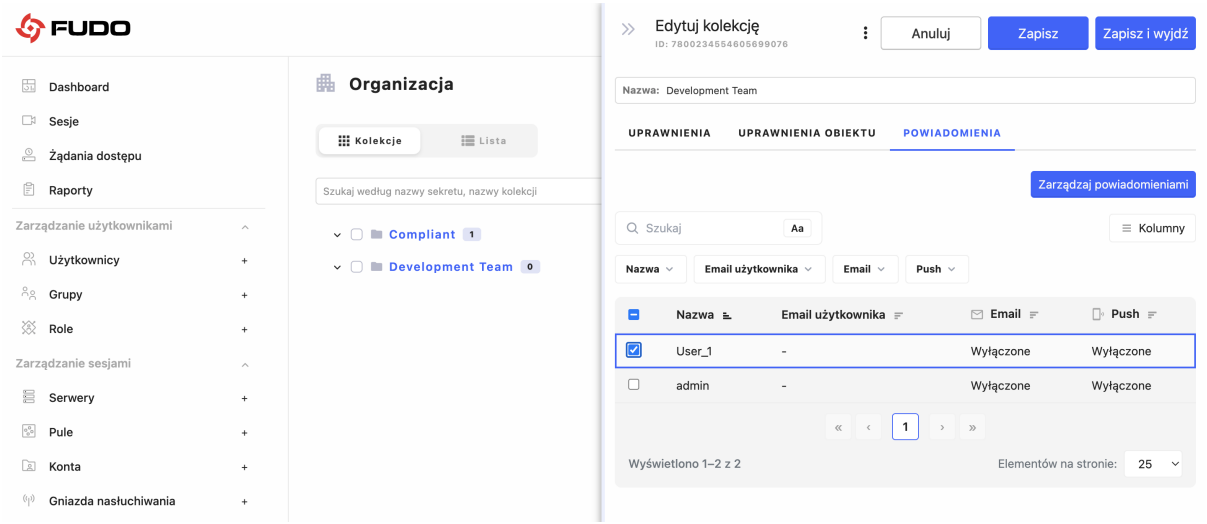
Prawa do obiektu nie decydują o widoczności kolekcji w Portalu Użytkownika. Określają natomiast, jakie czynności użytkownicy i role mogą wykonywać na kolekcji w Panelu Administracyjnym, na przykład wyświetlać ją, modyfikować, usuwać, przenosić lub tworzyć nowe obiekty. W połączeniu z odpowiednimi uprawnieniami prawa do obiektu mogą również umożliwiać użytkownikom dodawanie sekretów z Portalu Użytkownika, oprócz dostępu do sekretów przechowywanych w kolekcji.

Zakładka *PRAWA DO OBIEKTU* udostępnia szczegółowe opcje zarządzania użytkownikami i rolami:

- Podzakładka **UŻYTKOWNICY**: przypisywanie poszczególnych użytkowników z określonymi prawami (odczyt, modyfikacja, usuwanie, przenoszenie, tworzenie).
- Podzakładka **ROLE**: przypisywanie ról organizacyjnych z odpowiednimi prawami.

> **Uwaga**
>
> Szczegółowy opis praw do obiektu dla kolekcji znajduje się w sekcji *Zarządzanie prawami do kolekcji*.

ZAKŁADKA POWIADOMIENIA



W tej zakładce można skonfigurować ustawienia powiadomień dla działań związanych z kolekcją:

- **Wybór użytkowników**: wybór użytkowników, którzy będą otrzymywać powiadomienia.
- **Powiadomienia email**: włączanie lub wyłączanie powiadomień email o zdarzeniach związanych z kolekcją.
- **Powiadomienia push**: konfigurowanie powiadomień push w aplikacji.

Powiązane tematy:

- *Tworzenie kolekcji*
- *Zarządzanie prawami do kolekcji*
- *Powiadomienia kolekcji*
- *Usuwanie kolekcji*

11.2.4 Przypisywanie użytkowników i grup do kolekcji

Do kolekcji można przypisywać określonych użytkowników lub grupy, co pozwala na szczegółową kontrolę dostępu do sekretów. Przypisując użytkowników do kolekcji, możesz określić, kto ma dostęp do których sekretów.

Ostrzeżenie

Kolekcje zagnieżdżone mogą dziedziczyć uprawnienia z kolekcji nadrzędnych. Włączenie opcji **Dziedzicz z kolekcji nadrzędnej** usuwa uprawnienia przypisane bezpośrednio. Wszelkie przyszłe uprawnienia będą dziedziczone z kolekcji nadrzędnej.

Dostępne są następujące poziomy dostępu:

- **Podgląd na żądanie** – umożliwia użytkownikowi lub grupie wyświetlanie kolekcji i jej sekretów na liście oraz wysłanie żądania jednorazowego dostępu do podglądu zawartości sekretu. Dostęp wymaga zatwierdzenia przez administratora.
- **Podgląd** – umożliwia użytkownikowi lub grupie wyświetlanie szczegółów wszystkich sekretów w kolekcji w dowolnym momencie. Zatwierdzenie nie jest wymagane.
- **Pełna edycja** – umożliwia użytkownikowi lub grupie pełne zarządzanie wszystkimi sekretami w kolekcji. Zatwierdzenie przez administratora nie jest wymagane.

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij na kolekcję, do której chcesz przypisać użytkowników lub grupy, aby ją edytować.
3. Kliknij *Zarządzaj* i wybierz *Zarządzaj użytkownikami* lub *Zarządzaj grupami*, w zależności od tego, czy chcesz przypisać do kolekcji użytkowników, czy grupy.
4. W odpowiednim oknie zarządzania wyszukaj i wybierz użytkowników lub grupy, które chcesz przypisać.
5. Kliknij *Zapisz*, aby potwierdzić przypisanie.
6. Kliknij *Zapisz*, aby zastosować zmiany.

Powiązane tematy:

- *Zarządzanie prawami do kolekcji*
- *Tworzenie kolekcji*
- *Opis modułu*

11.2.5 Zarządzanie prawami do kolekcji

Prawa do obiektu kolekcji określają, jakie operacje administracyjne użytkownicy i role mogą wykonywać na kolekcjach. Prawa te dotyczą samej kolekcji jako obiektu, na przykład jej wyświetlania, modyfikowania, usuwania, przenoszenia i tworzenia, i różnią się od poziomów dostępu używanych do kontrolowania dostępu do sekretów przechowywanych w kolekcjach.

Prawa do obiektu kolekcji są częścią modelu kontroli dostępu opartej na rolach (RBAC) stosowanego w Skarbcu haseł. Za pomocą modelu RBAC prawa administracyjne mogą być przypisywane rolom i poszczególnym użytkownikom w celu kontrolowania administracyjnego dostępu do kolekcji. Więcej informacji o modelu RBAC znajduje się w sekcji *Kontrola dostępu oparta na rolach (RBAC)*.

Uwaga

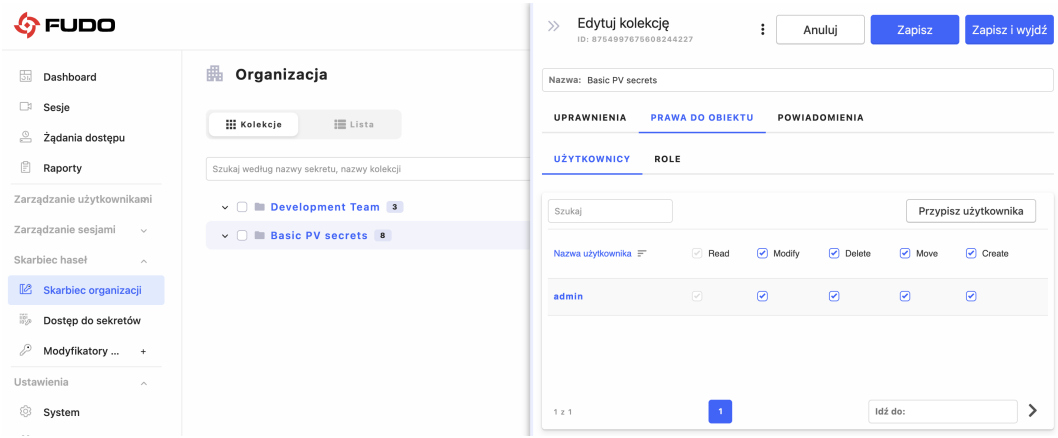
Prawa do obiektu a uprawnienia

Ważne jest zrozumienie różnicy między prawami do obiektu a uprawnieniami:

- **Prawa do obiektu** określają, co użytkownicy mogą robić z samą kolekcją, na przykład tworzyć, modyfikować, usuwać lub przenosić.
- **Uprawnienia** określają dostęp do sekretów przechowywanych w kolekcji, na przykład *Podgląd na żądanie*, *Podgląd* lub *Pełna edycja*.

11.2.5.1 Przypisywanie praw do obiektu użytkownikom

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij lewym przyciskiem myszy kolekcję, którą chcesz zarządzać.
3. Przejdź do zakładki *PRAWA DO OBIEKTU*.
4. W podzakładce *UŻYTKOWNICY* kliknij *Przypisz użytkownika*.

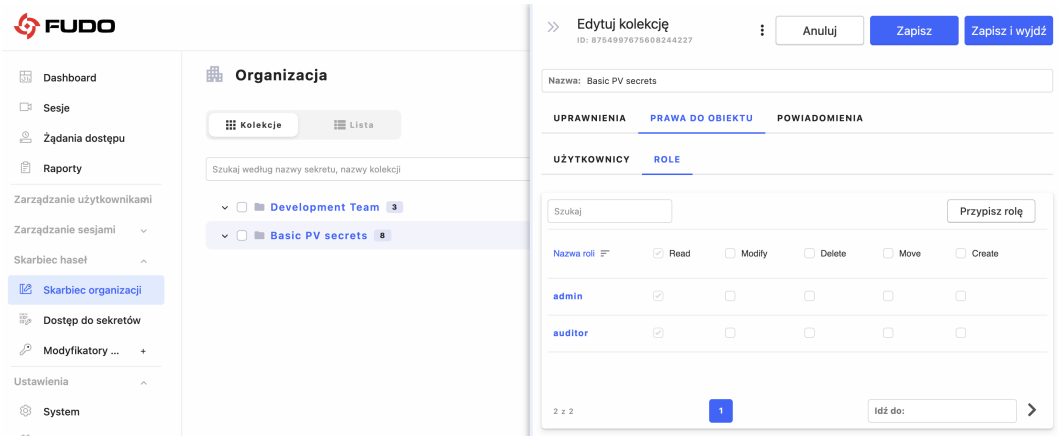


5. Wybierz użytkowników, których chcesz przypisać, i kliknij *Zapisz*.
6. Użyj pól wyboru, aby nadać każdemu użytkownikowi określone prawa (Modyfikacja, Usuwanie, Przenoszenie, Tworzenie).
7. Kliknij *Zapisz i zamknij*, aby zastosować zmiany.

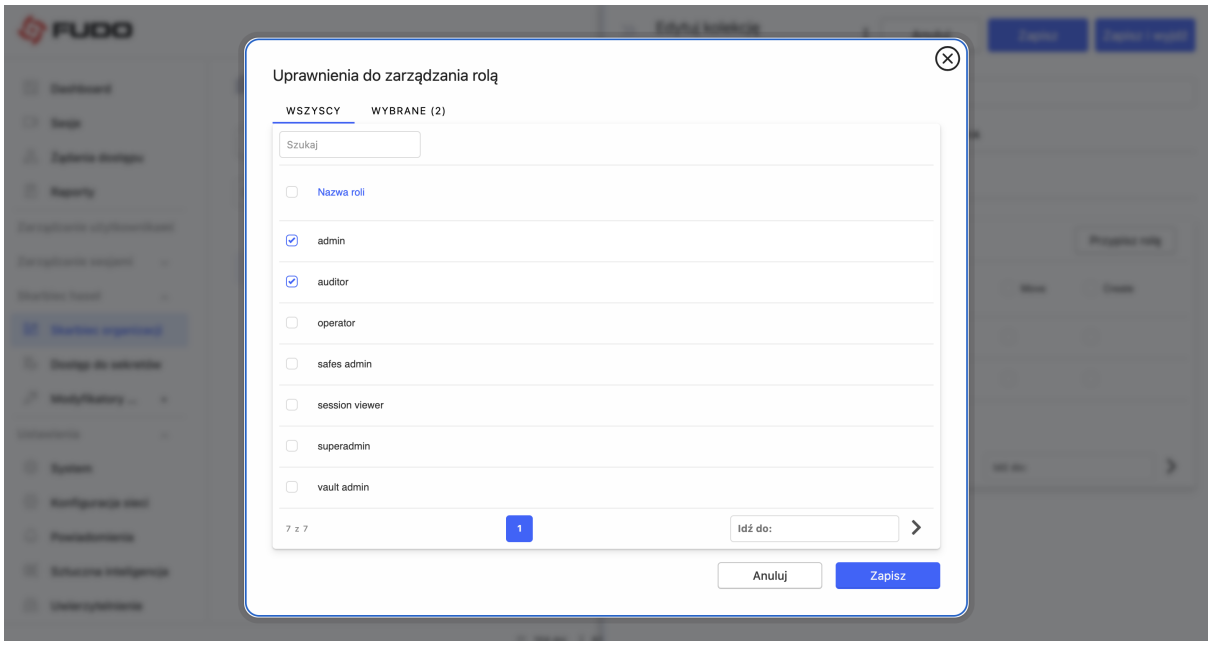
11.2.5.2 Przypisywanie praw do obiektu rolom

Kontrola dostępu oparta na rolach umożliwia przypisywanie do kolekcji predefiniowanych ról zamiast zarządzania uprawnieniami poszczególnych użytkowników. Takie podejście upraszcza zarządzanie uprawnieniami, szczególnie w większych organizacjach z ustaloną hierarchią ról.

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij lewym przyciskiem myszy kolekcję, którą chcesz zarządzać.
3. Przejdź do zakładki *PRAWA DO OBIEKTU*.
4. W podzakładce *ROLE* kliknij *Przypisz rolę*.



5. Wybierz role, które chcesz przypisać, i kliknij *Zapisz*.
6. Użyj pól wyboru, aby nadać każdej roli określone prawa (Modyfikacja, Usuwanie, Przenoszenie, Tworzenie).
7. Kliknij *Zapisz i zamknij*, aby zastosować zmiany.



Uwaga

Użytkownicy dziedziczą prawa do obiektu ze swoich przypisanych ról. Jeśli użytkownik należy do wielu ról, otrzymuje łączne prawa wynikające ze wszystkich tych ról.

Powiązane tematy:

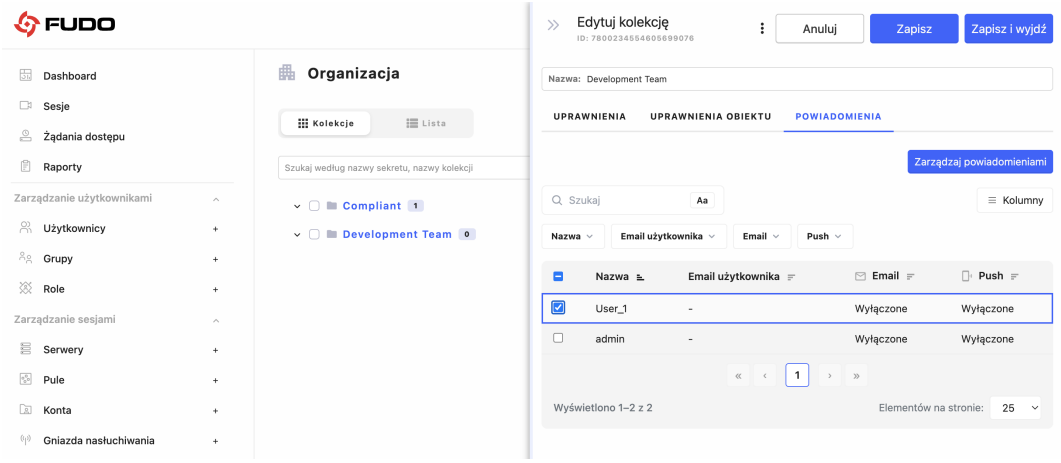
- *Przypisywanie użytkowników i grup do kolekcji*
- *Tworzenie kolekcji*
- *Kolekcje*

- *Opis modułu*

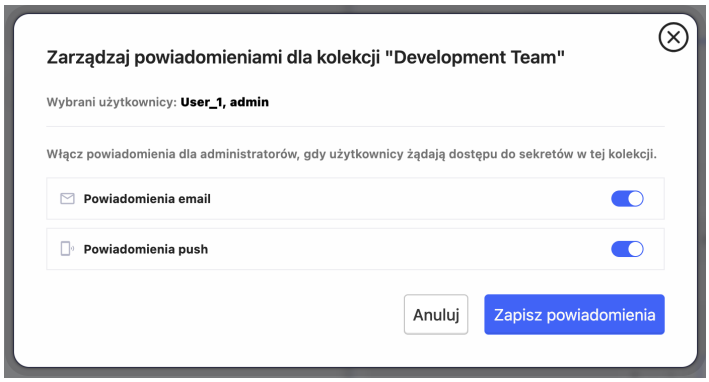
11.2.6 Powiadomienia kolekcji

Funkcja powiadomień umożliwia informowanie użytkowników o istotnych zdarzeniach i zmianach dotyczących przypisanych im kolekcji. Pomaga to monitorować działania związane z zarządzaniem sekretami oraz wspiera nadzór nad bezpieczeństwem.

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij na kolekcję, dla której chcesz skonfigurować powiadomienia.
3. Przejdź do zakładki *POWIADOMIENIA*.



4. Zaznacz użytkowników, dla których chcesz skonfigurować powiadomienia.
5. Kliknij *Zarządzaj powiadomieniami*.
6. W oknie modalnym ustawień powiadomień wybierz metody dostarczania powiadomień (Email, Push).
7. Kliknij *Zapisz powiadomienia* aby zastosować ustawienia powiadomień.



Powiązane tematy:

- *Przypisywanie użytkowników i grup do kolekcji*
- *Opis modułu*

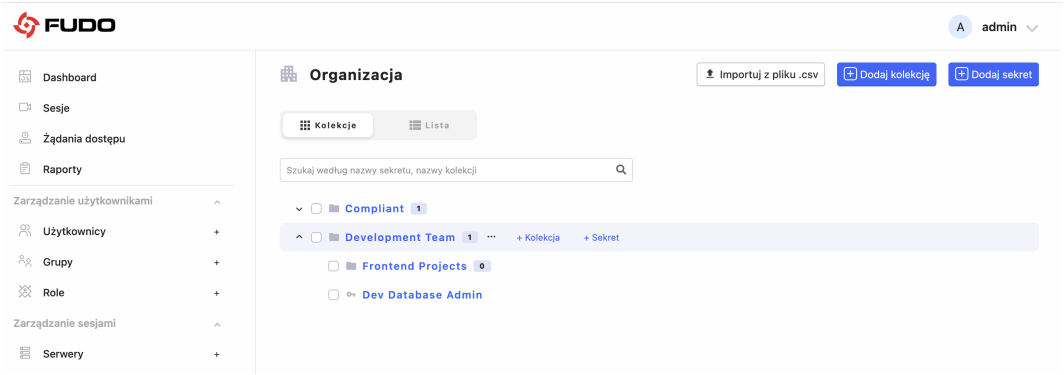
11.2.7 Usuwanie kolekcji

Kolekcje można usuwać, gdy nie są już potrzebne. Przed usunięciem kolekcji upewnij się, że wszystkie istotne sekrety zostały przeniesione do innych kolekcji lub zabezpieczone w kopii zapasowej, ponieważ tej operacji nie można cofnąć.

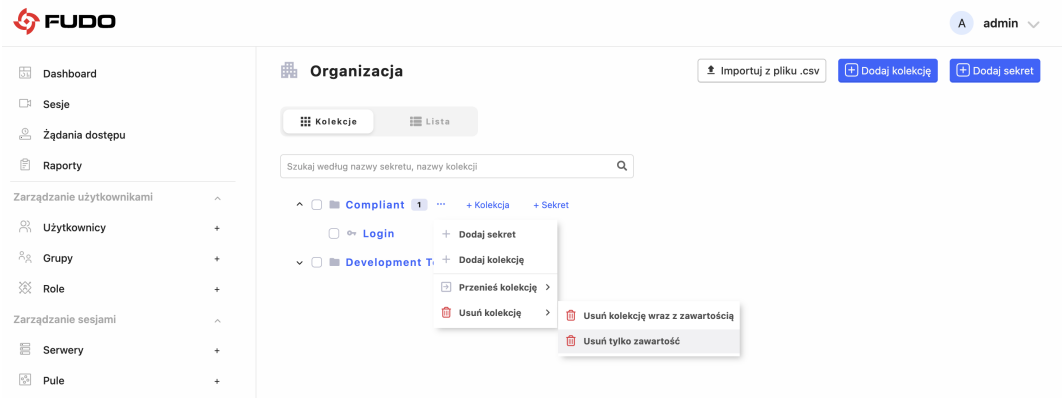
Ostrzeżenie

Usunięcie kolekcji jest operacją trwałą i nieodwracalną. Wszystkie sekrety znajdujące się w kolekcji również zostaną usunięte, chyba że wcześniej zostaną przeniesione do innej kolekcji.

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Najedź kursorem na kolekcję, którą chcesz usunąć, aby wywołać menu opcji.



3. Kliknij przycisk trzech kropek (. . .) aby otworzyć menu kontekstowe.
4. Wybierz *Usuń kolekcję* z menu kontekstowego.
5. Możesz wtedy wybrać, czy usunąć tylko zawartość kolekcji czy kolekcję wraz z jej zawartością.



6. W oknie dialogowym potwierdzenia przejrzyj nazwę kolekcji.
7. Kliknij *Usuń* aby trwale usunąć kolekcję.



Ostrzeżenie

Usunięcie kolekcji nadrzędnej usuwa również wszystkie zagnieżdżone kolekcje.

Powiązane tematy:

- *Tworzenie kolekcji*
- *Zagnieżdżanie kolekcji*
- *Opis modułu*

11.3 Sekrety

11.3.1 Tworzenie sekretów

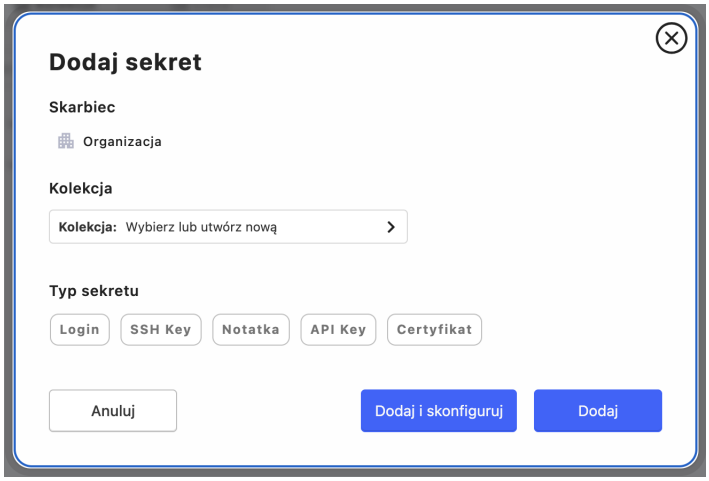
Sekrety przechowują wrażliwe informacje takie jak poświadczenia logowania, klucze API, certyfikaty, klucze SSH i notatki. Każdy sekret jest przypisany do kolekcji w celu organizacji i kontroli dostępu.

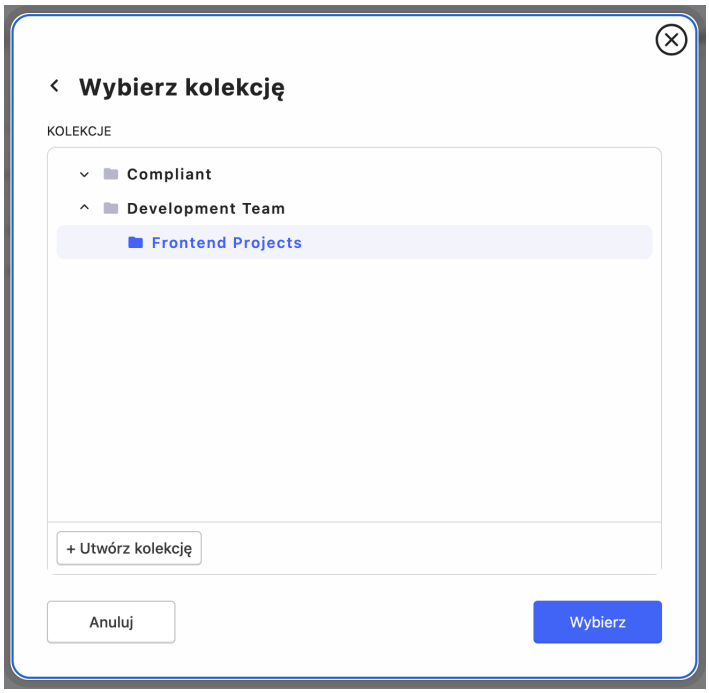
Uwaga

Dostępne typy sekretów:

- **Login**: Dane logowania nazwy użytkownika/hasła z informacjami o domenie i URL
- **Klucz SSH**: Prywatne klucze SSH do dostępu do serwerów
- **Notatka**: Notatki w postaci zwykłego tekstu do przechowywania informacji innych niż dane logowania
- **Klucz API**: Tokeny i klucze API do uwierzytelniania usług
- **Certyfikat**: Certyfikaty cyfrowe i klucze prywatne

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij + *Dodaj sekret*.

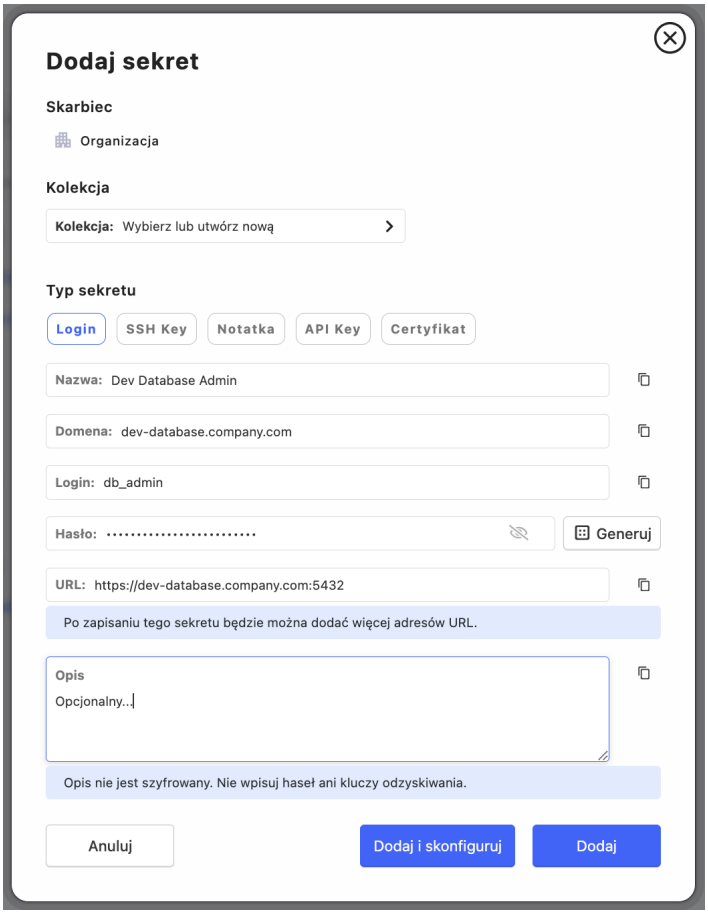




3. Wybierz kolekcję, w której sekret będzie przechowywany, klikając listę rozwijaną *Kolekcja*.
4. Kliknij *Wybierz*.
5. Wybierz odpowiedni typ sekretu (Login, Klucz SSH, Notatka, Klucz API, Certyfikat).

Dla sekretów typu Login:

- Wypełnij wymagane pola:
  - *Nazwa*: Wprowadź opisową nazwę dla sekretu
  - *Domena*: Adres domeny docelowej lub serwera
  - *Login*: Nazwa użytkownika lub konta
  - *Hasło*: Możesz użyć przycisku *Generuj* dla bezpiecznych haseł
  - *URL*: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - *Opis*: Opcjonalne dodatkowe informacje (nieszyfrowane)

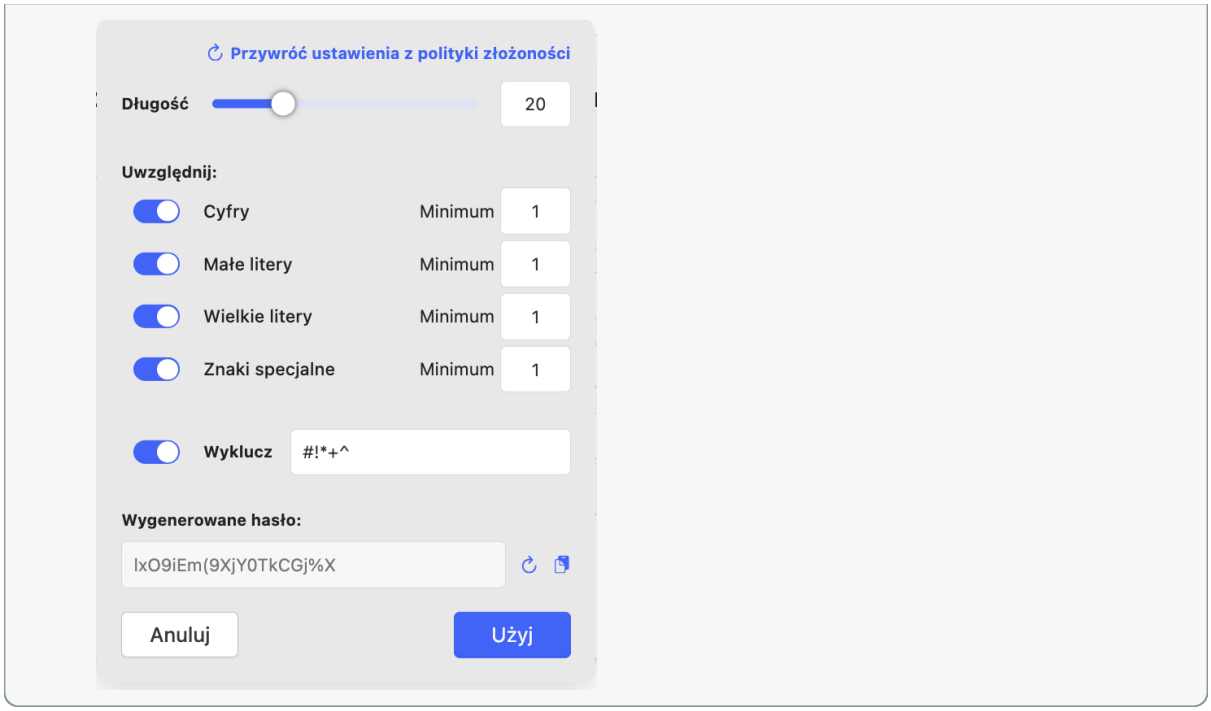


Uwaga

Generator Haseł:

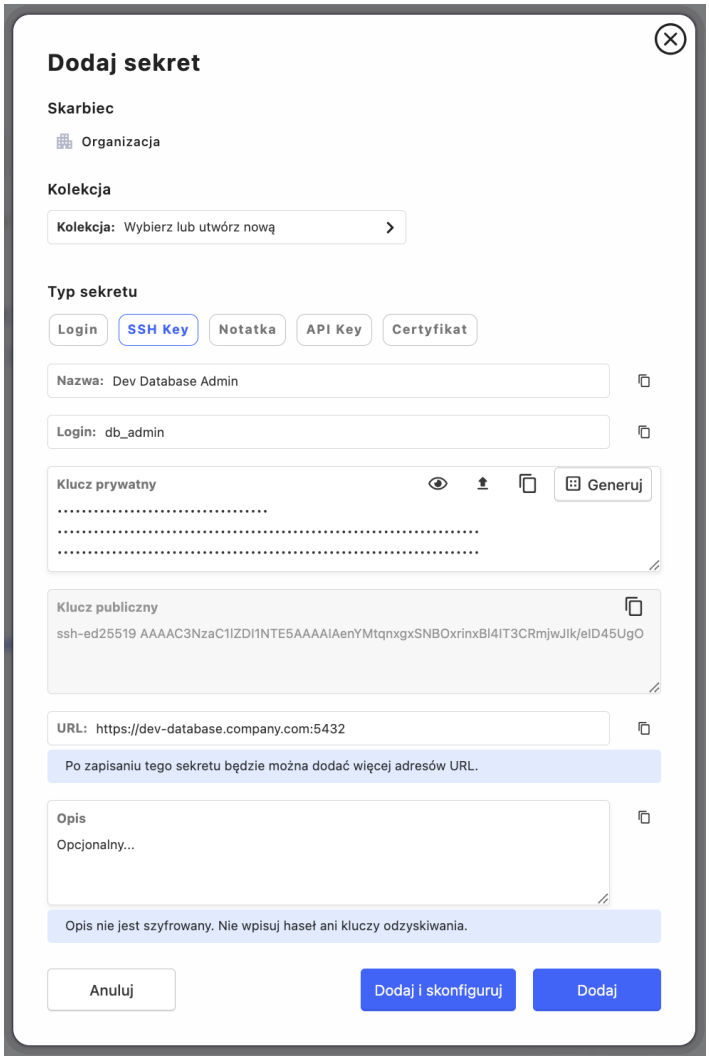
Zintegrowany generator haseł (przycisk *Generuj*) zapewnia bezpieczne tworzenie haseł z konfigurowalnymi opcjami:

- **Długość**: Ustaw długość hasła (domyślnie: 20 znaków)
- **Typy Znaków**: Uwzględnij cyfry, małe litery, wielkie litery, znaki specjalne
- **Minimalne Wymagania**: Ustaw minimalną liczbę dla każdego typu znaku
- **Opcje Wykluczania**: Wyklucz niejednoznaczne lub określone znaki
- **Wygenerowane Hasło**: Podgląd i kopiowanie wygenerowanego hasła



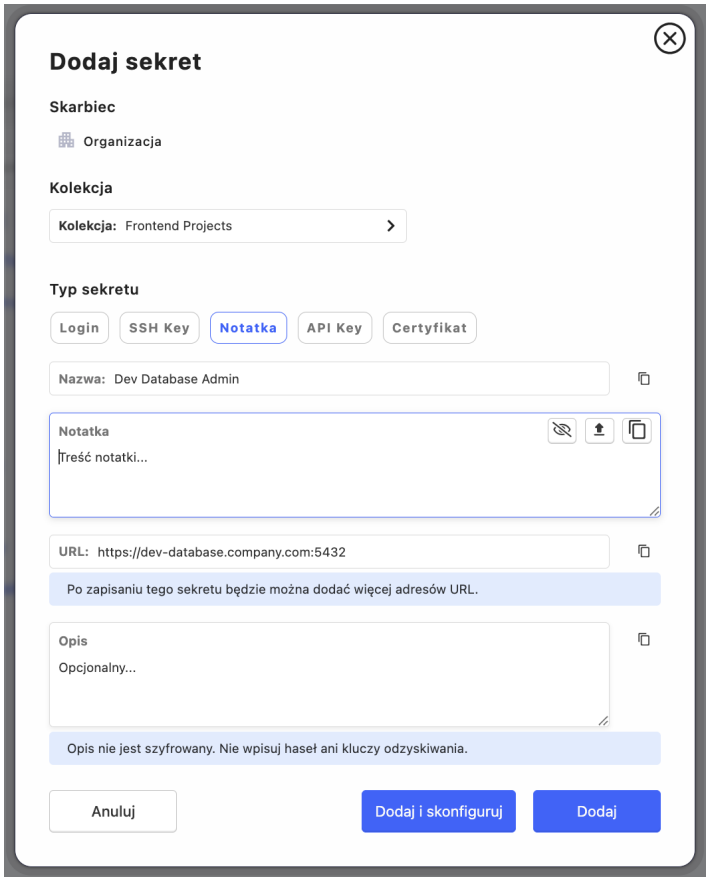
Dla sekretów typu Klucz SSH:

- Wypełnij wymagane pola:
  - Nazwa: Wprowadź opisową nazwę dla sekretu
  - Login: Wprowadź nazwę użytkownika lub konta
  - Klucz prywatny: Wprowadź klucz prywatny lub kliknij *Generuj*, aby wygenerować klucze prywatny i publiczny
  - URL: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - Opis: Opcjonalne dodatkowe informacje (nieszyfrowane)



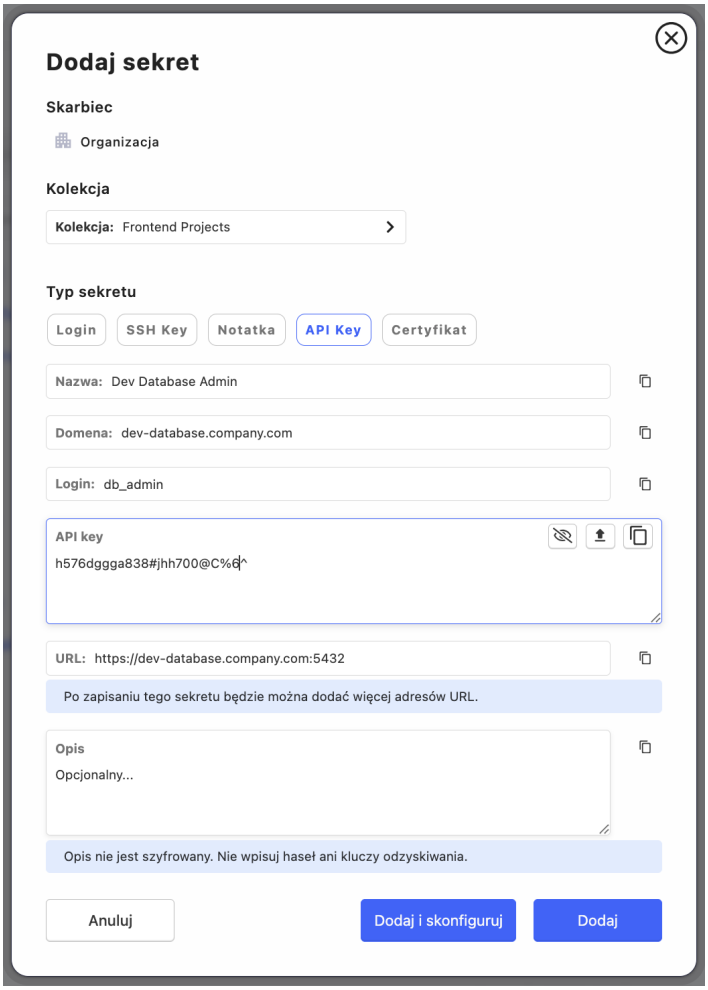
Dla sekretów typu Notatka:

- Wypełnij wymagane pola:
  - Nazwa: Wprowadź opisową nazwę dla sekretu
  - Notatka: Wprowadź zawartość notatki
  - URL: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - Opis: Opcjonalne dodatkowe informacje (nieszyfrowane)



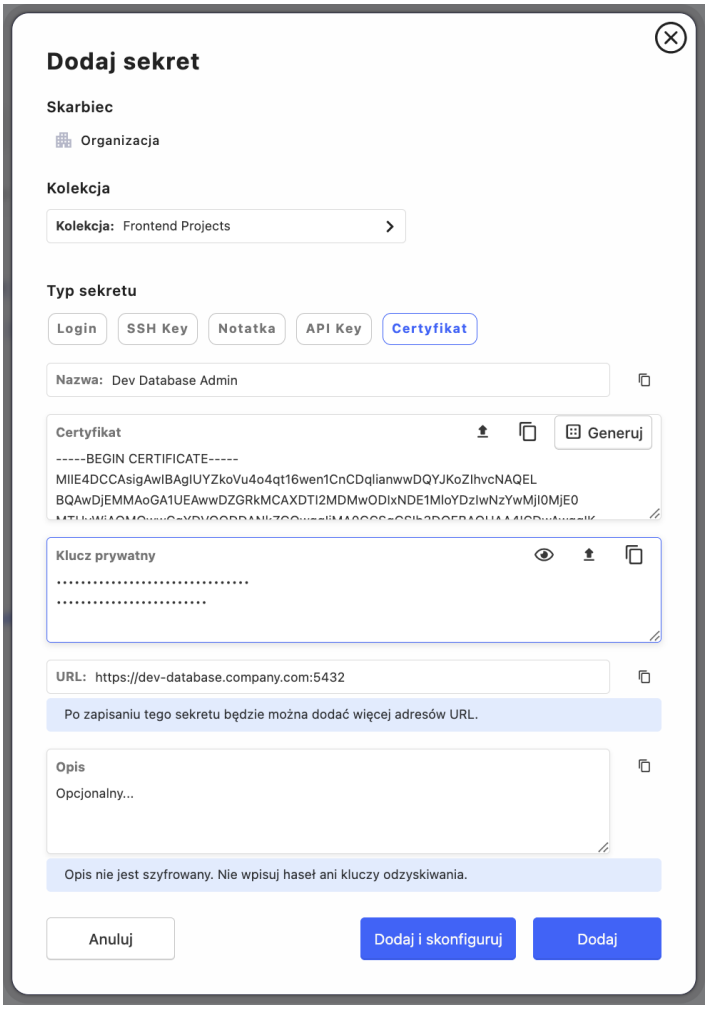
Dla sekretów typu Klucz API:

- Wypełnij wymagane pola:
  - Nazwa: Wprowadź opisową nazwę dla sekretu
  - Domena: Wprowadź adres domeny docelowej lub serwera
  - Login: Wprowadź nazwę użytkownika lub konta
  - Klucz API: Wprowadź lub prześlij klucz API
  - URL: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - Opis: Opcjonalne dodatkowe informacje (nieszyfrowane)



Dla sekretów typu Certyfikat:

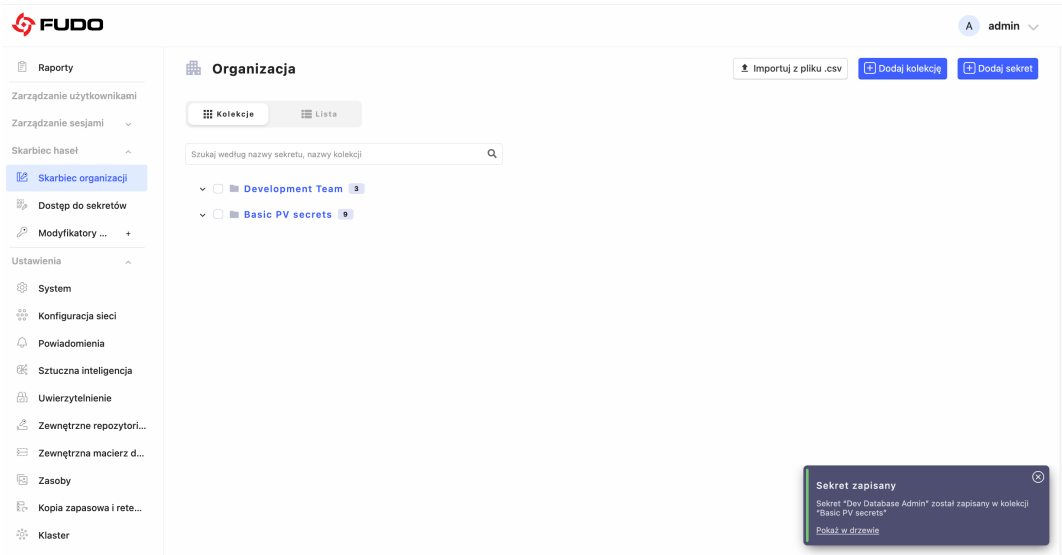
- Wypełnij wymagane pola:
  - Nazwa: Wprowadź opisową nazwę dla sekretu
  - Certyfikat: Prześlij lub wygeneruj certyfikat
  - Klucz prywatny: Prześlij swój klucz prywatny
  - URL: Wprowadź adres URL powiązanej strony internetowej lub usługi
  - Opis: Opcjonalne dodatkowe informacje (nieszyfrowane)



7. Kliknij *Dodaj* aby utworzyć sekret i zamknąć okno, lub *Dodaj i skonfiguruj* aby utworzyć sekret i otworzyć jego okno konfiguracji, gdzie możesz kontynuować konfigurację.

Potwierdzenie sukcesu:

Po utworzeniu sekretu zobaczysz komunikat potwierdzający, a liczba sekretów w kolekcji zostanie zaktualizowana.



Alternatywne metody tworzenia sekretu:

Możesz również tworzyć sekrety za pomocą szybkich akcji:

1. **Z menu podręcznego po najechaniu na kolekcję**: Najedź na kolekcję i kliknij *+ Sekret*
2. **Z menu kontekstowego**: Kliknij menu trzech kropek (. . .) na kolekcji i wybierz **+ Dodaj sekret**

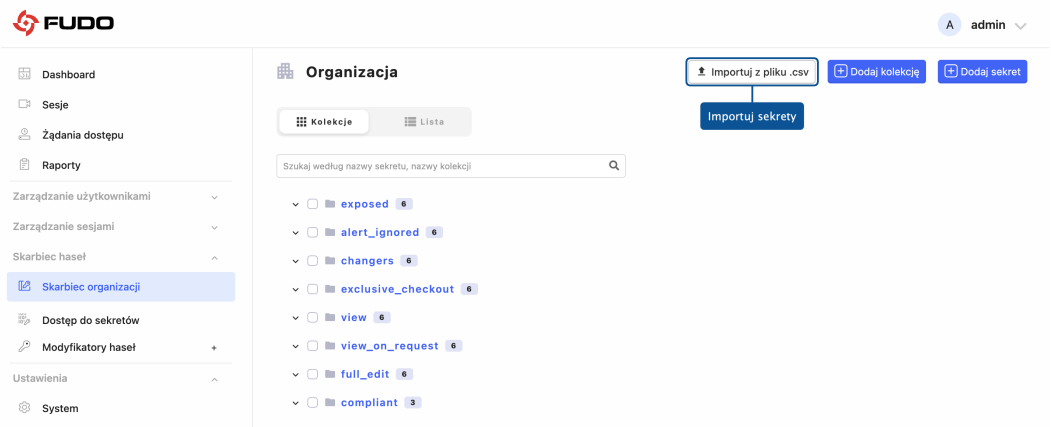
Powiązane tematy:

- *Dostęp do edycji sekretów*
- *Tworzenie kolekcji*
- *Opis modułu*

11.3.2 Importowanie sekretów

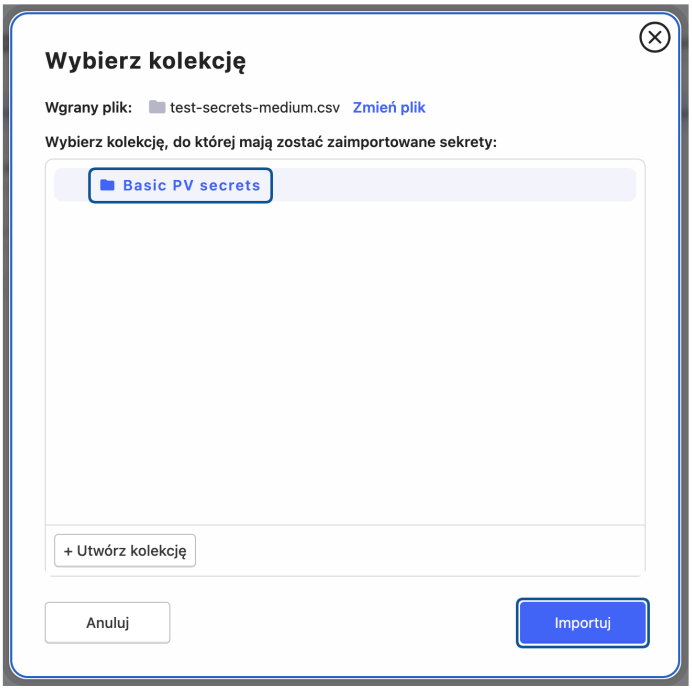
> **Uwaga**
>
> Maksymalny dozwolony rozmiar pliku do importu sekretów z pliku CSV wynosi 2 MB.

1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij *Importuj z pliku .csv*.



class
image_shadow

3. Przeciągnij i upuść plik do obszaru przesyłania w oknie modalnym lub kliknij *Przeglądaj pliki*, aby wgrać go z katalogu lokalnego.
4. Wybierz lub utwórz kolekcję, do której mają zostać zaimportowane sekrety.
5. Kliknij *Importuj*, aby wgrać sekrety do konfiguracji Fudo Enterprise, lub *Anuluj*, aby przerwać proces wgrywania.



Format pliku CSV

Plik CSV musi zostać przygotowany zgodnie z następującymi zasadami:

- Pierwszy wiersz to *wiersz nagłówkowy* zawierający nazwy odpowiadające nazwom pól API (zobacz *Dokumentacja API:* API v2: Secrets).
- *Wiersz nagłówkowy* musi zawierać wszystkie pola wymagane przy ręcznym tworzeniu sekretu danego typu. Pozostałe pola są opcjonalne i mogą pozostać puste.
- Jako separator pól należy użyć przecinka (,).

Przykładowy plik CSV:

```
name,type,login,domain,secret,uri
login,login,admin,portal.example.com,SuperSecure123!,https://portal.example.com/
↪login
login2,login,db_admin,db.example.com,DbPassword2024,https://db.example.com/admin
note,note,,,Quarterly meeting notes: Q4 targets discussed.,
api_key,apikey,aws_service_account,api.aws.amazon.com,AKIAIOSFODNN7EXAMPLE,
↪https://api.aws.amazon.com
cert,certificate,,,,
ssh_key,sshkey,,,,
```

Uwaga

Prywatne klucze SSH i certyfikaty są zazwyczaj przechowywane w wieloliniowym formacie PEM. Podczas ich importu z pliku CSV należy ująć całą wartość w podwójne cudzysłowy (""), aby została potraktowana jako pojedyncze pole CSV.

Przykładowy plik CSV dla sekretu typu certyfikat:

```
name,type,login,domain,certificate,secret
"secret-1","certificate","","","-----BEGIN CERTIFICATE-----
MIID...EXAMPLE...DATA
-----END CERTIFICATE-----","-----BEGIN PRIVATE KEY-----
MIIE...EXAMPLE...DATA
-----END PRIVATE KEY-----"
```

Powiązane tematy:

- *Opis modułu*
- *Tworzenie sekretów*
- *Dostęp do edycji sekretów*

11.3.3 Dostęp do edycji sekretów

Sekrety można edytować w celu aktualizacji ich informacji, zmiany haseł, modyfikacji adresów URL lub aktualizacji opisów. Istnieje wiele sposobów dostępu do sekretów i ich edycji w Skarbcu haseł.

Metoda 1: Z widoku kolekcji

1. Przejdź do kolekcji zawierającej sekret.
2. Rozwiń kolekcję, aby wyświetlić jej sekrety.
3. Kliknij na nazwę sekretu, aby go edytować.

Metoda 2: Z widoku listy

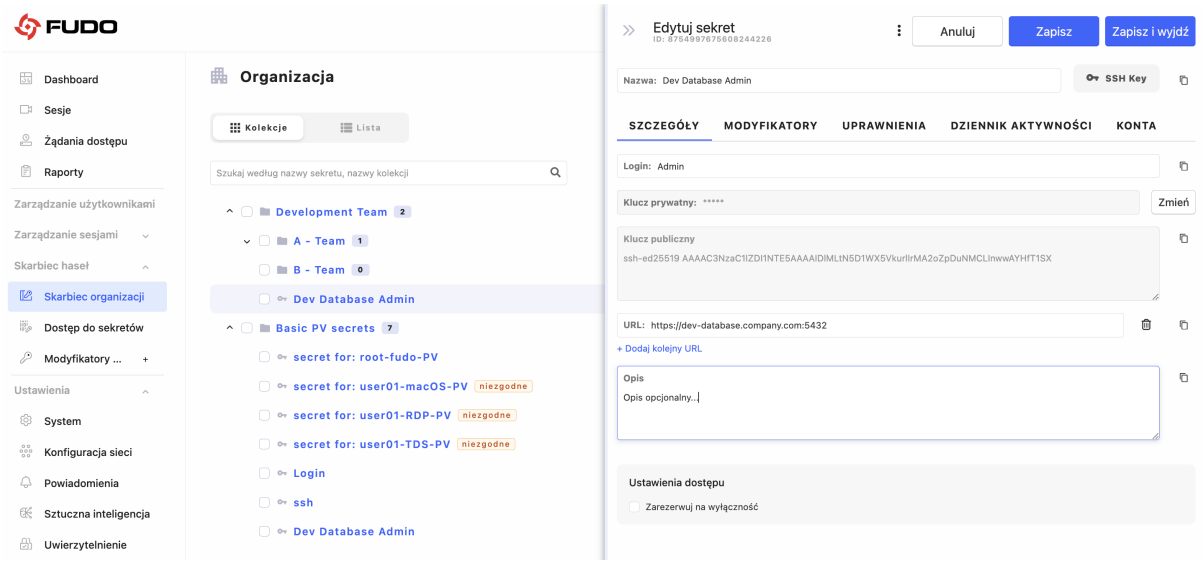
1. Wybierz *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij *Lista*, aby przełączyć na widok listy.
3. Kliknij na nazwę sekretu, aby otworzyć panel edycji.

11.3.3.1 Panel edycji sekretu

Panel edycji sekretu zapewnia kompleksowe możliwości edycji z następującymi kartami:

KARTA SZCZEGÓŁY

Karta Szczegóły to główny interfejs edycji informacji o sekrecie, gdzie możesz modyfikować wszystkie podstawowe atrybuty sekretu.



Dostępne pola (przykład dla typu Login):

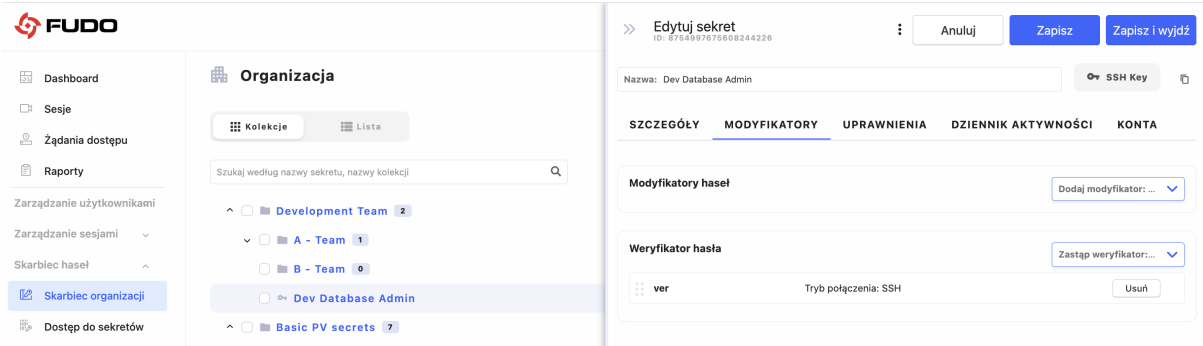
- **Nazwa**: Nazwa wyświetlana dla sekretu (musi być unikalna w ramach kolekcji)
- **Domena**: Domena lub nazwa hosta powiązana z poświadczeniami
- **Login**: Nazwa użytkownika lub identyfikator logowania
- **Hasło**: Sekretne hasło (domyślnie zamaskowane z przyciskiem „Zmień” do aktualizacji)
- **URL**: Jeden lub więcej adresów URL gdzie te poświadczenia mogą być używane
  - Kliknij + Dodaj kolejny URL aby dodać wiele adresów URL
  - Kliknij ikonę kosza aby usunąć URL
  - Każdy URL musi zawierać protokół (https://, ssh://, itp.)
- **Opis**: Opcjonalne notatki lub dodatkowe informacje o sekrecie

Ustawienia Dostępu:

- **Wyłączne wypożyczenie**: Gdy włączone, tylko jeden użytkownik może uzyskać dostęp do sekretu na raz. Inni użytkownicy muszą poczekać aż sekret zostanie zwrócony.

KARTA MODYFIKATORY

Karta Modyfikatory pozwala skonfigurować automatyczne zarządzanie hasłami przez modyfikatory haseł i weryfikatory haseł.



Modyfikatory haseł:

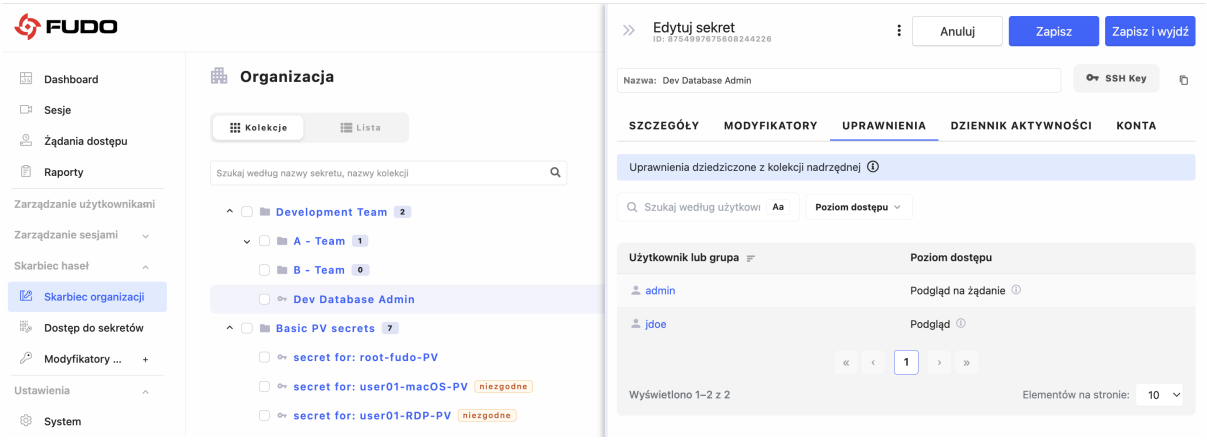
Modyfikatory haseł automatyzują proces rotacji haseł w systemach docelowych. Możesz wybrać modyfikator haseł z listy rozwijanej aby zautomatyzować rotację haseł.

Weryfikatory haseł:

Weryfikatory haseł zapewniają, że przechowywane poświadczenia odpowiadają temu, co jest skonfigurowane w systemie docelowym. Możesz wybrać weryfikator do okresowego sprawdzania poprawności haseł.

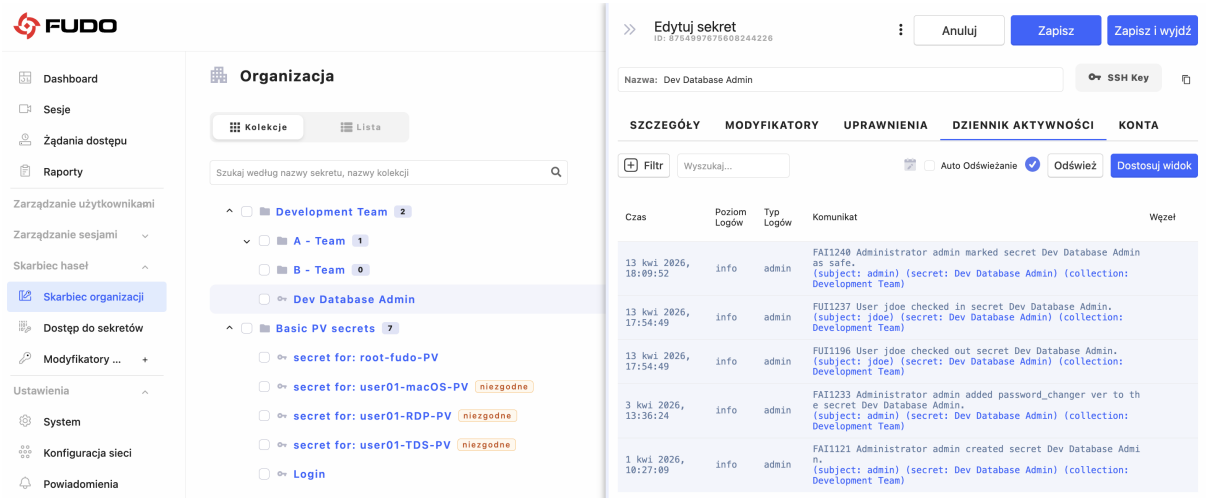
KARTA UPRAWNIENIA

Karta Uprawnienia pozwala podejrzeć dostęp użytkowników lub grup do sekretu. Sekrety dziedziczą uprawnienia z ich kolekcji nadrzędnej.



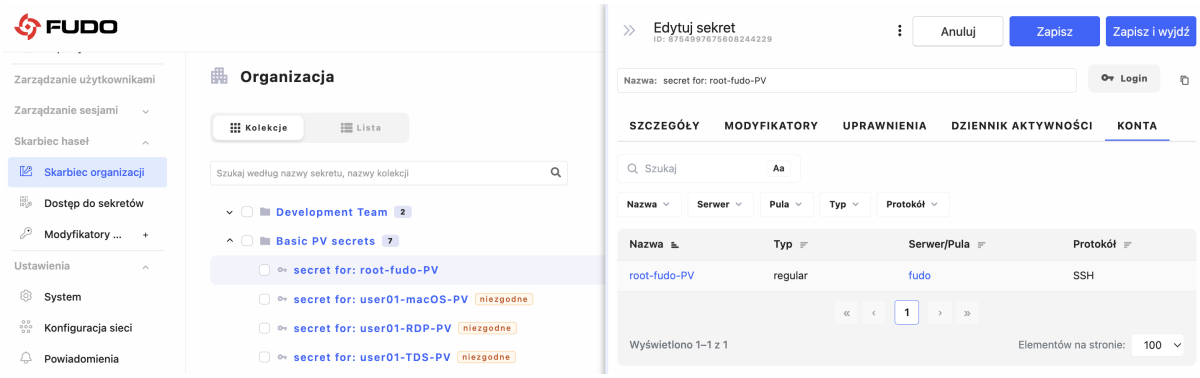
KARTA LOGI AKTYWNOŚCI

Karta Logi Aktywności zapewnia kompleksową ścieżkę audytu wszystkich działań wykonanych na sekrecie. Możesz filtrować wpisy logów i dostosować które kolumny są wyświetlane.



KARTA KONTA

Karta Konta wyświetla wszystkie konta powiązane z tym sekretem.



Powiązane tematy:

- *Tworzenie sekretów*
- *Usuwanie sekretów*
- *Dostęp do edycji kolekcji*
- *Opis modułu*

11.3.4 Przenoszenie sekretów między kolekcjami

Sekrety można przenosić między kolekcjami w celu reorganizacji struktury skarbca haseł, dostosowania uprawnień dostępu lub odzwierciedlenia zmian w organizacji zespołu. Przeniesienie sekretów aktualizuje ich kontrolę dostępu na podstawie uprawnień kolekcji docelowej.

Uwaga

Przeniesienie sekretu do innej kolekcji zmieni jego uprawnienia dostępu na podstawie przypisań użytkowników i ról kolekcji docelowej.

Istnieje kilka metod przenoszenia sekretów między kolekcjami:

Metoda 1: Przenoszenie przy użyciu menu kontekstowego

1. Najedź kursorem na sekret, który chcesz edytować, aby wywołać menu opcji.
2. Kliknij przycisk trzech kropek (...) aby otworzyć menu kontekstowe.
3. Wybierz *Przenieś do*.
4. Wybierz kolekcję docelową ze struktury drzewa.
5. Kliknij *Wybierz* aby potwierdzić operację przenoszenia.

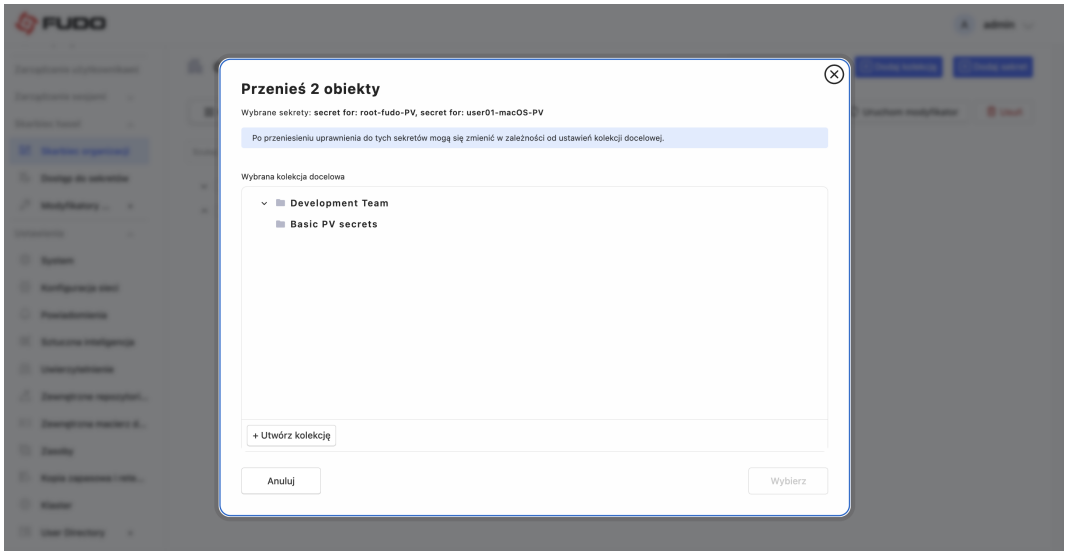
Metoda 2: Przenoszenie zbiorcze w widoku kolekcji

1. Przejdź do *Skarbiec haseł* > *Skarbiec organizacji*.
2. W widoku *Kolekcje* wybierz wiele sekretów zaznaczając ich pola wyboru.
3. Kliknij przycisk *Przenieś*, który pojawi się na pasku akcji.
4. Wybierz kolekcję docelową ze struktury drzewa.
5. Kliknij *Wybierz* aby potwierdzić operację przenoszenia.

Metoda 3: Przenoszenie zbiorcze w widoku listy

Ta metoda pozwala przenosić wiele sekretów naraz.

1. Przejdź do *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij *Lista* aby przełączyć się na widok listy.
3. Zaznacz pola wyboru obok sekretów, które chcesz przenieść.
4. Kliknij przycisk *Przenieś*, który pojawi się na pasku akcji.
5. Wybierz kolekcję docelową ze struktury drzewa.
6. Kliknij *Wybierz* aby potwierdzić operację przenoszenia.



Metoda 4: Przenoszenie podczas edycji

1. Otwórz dowolny sekret do edycji.
2. Kliknij przycisk trzech kropek (...) obok ID sekretu w panelu edycji i wybierz *Przenieś do*.
3. Wybierz kolekcję docelową ze struktury drzewa.
4. Kliknij *Wybierz* aby potwierdzić operację przenoszenia.
5. Zapisz sekret.

Powiązane tematy:

- *Dostęp do edycji sekretów*
- *Tworzenie kolekcji*
- *Opis modułu*

11.3.5 Usuwanie sekretów

Sekrety można usuwać, gdy nie są już potrzebne lub gdy dane logowania zostały wycofane z użycia. Przed usunięciem sekretów upewnij się, że rozumiesz wpływ na użytkowników i aplikacje, które mogą od nich zależeć.

Ostrzeżenie

Usuwanie sekretu to trwała akcja, której nie można cofnąć. Upewnij się, że masz kopie zapasowe lub alternatywne metody dostępu przed przystąpieniem do usuwania.

Istnieje kilka metod usuwania sekretów ze Skarbca haseł:

Metoda 1: Używanie menu kontekstowego

1. Najedź kursorem na sekret, który chcesz usunąć, aby wywołać menu opcji.
2. Kliknij przycisk trzech kropek (...) aby otworzyć menu kontekstowe.
3. Wybierz *Usuń*.
4. Potwierdź usunięcie w oknie dialogowym ostrzeżenia.

Metoda 2: Usuwanie zbiorcze w widoku kolekcji

1. Przejdź do *Skarbiec haseł* > *Skarbiec organizacji*.
2. W widoku *Kolekcje* wybierz wiele sekretów zaznaczając ich pola wyboru.
3. Kliknij przycisk *Usuń*, który pojawi się na pasku akcji.
4. Przejrzyj komunikat ostrzegawczy i potwierdź usunięcie.

Metoda 3: Usuwanie zbiorcze w widoku listy

Ta metoda pozwala usunąć wiele sekretów naraz.

1. Przejdź do *Skarbiec haseł* > *Skarbiec organizacji*.
2. Kliknij *Lista* aby przełączyć się na widok listy.
3. Zaznacz pola wyboru obok sekretów, które chcesz usunąć.
4. Kliknij przycisk *Usuń*, który pojawi się na pasku akcji.
5. Przejrzyj komunikat ostrzegawczy i potwierdź usunięcie.

Metoda 4: Usuwanie z panelu edycji

1. Otwórz dowolny sekret do edycji.
2. Kliknij przycisk trzech kropek (...) obok ID sekretu w panelu edycji.
3. Wybierz *Usuń* z menu rozwijanego.
4. Potwierdź usunięcie w oknie dialogowym ostrzeżenia.

Powiązane tematy:

- *Tworzenie sekretów*
- *Dostęp do edycji sekretów*
- *Przenoszenie sekretów między kolekcjami*
- *Usuwanie kolekcji*
- *Opis modułu*

11.3.6 Przypisywanie sekretów ze Skarbca haseł do kont

Uwaga

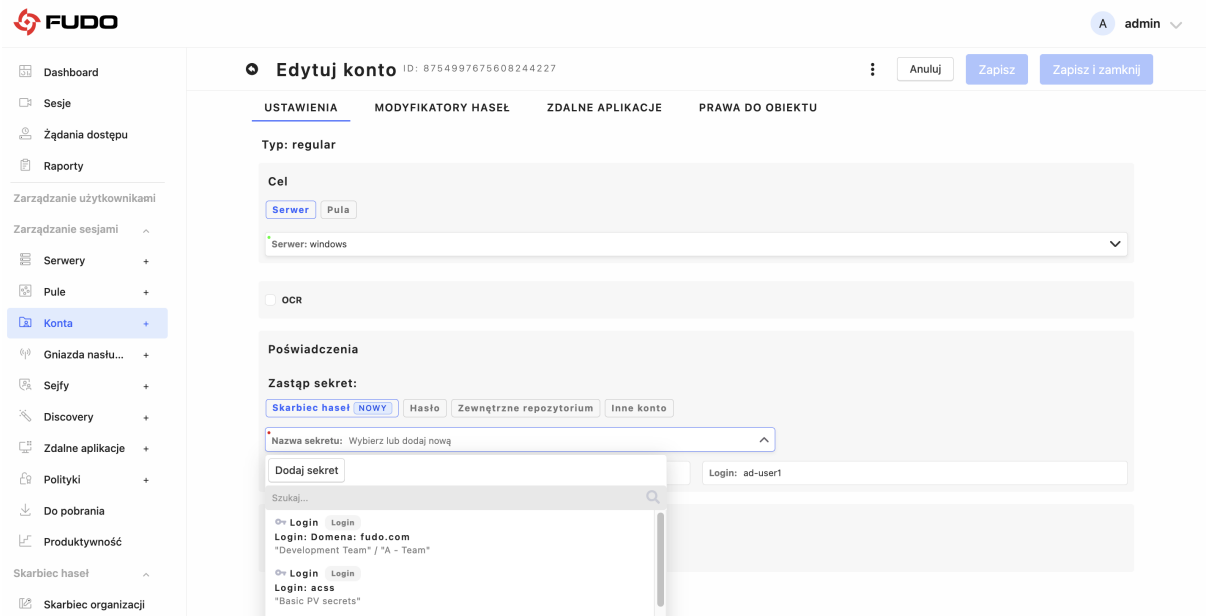
Przed rozpoczęciem procedury upewnij się, że masz odpowiednie uprawnienia do edycji kont oraz dostęp do Skarbca haseł.

Sekrety przechowywane w Skarbcu haseł można przypisywać do kont Fudo Enterprise, aby zapewnić scentralizowane zarządzanie poświadczeniami. Dzięki tej integracji administratorzy mogą używać sekretów zapisanych w Skarbcu haseł do uwierzytelniania połączeń z serwerami docelowymi.

Uwaga

Do kont można przypisać dwa typy sekretów: **Login** i **Klucz SSH**.

1. Przejdź do *Zarządzanie sesjami* > *Konta*.
2. Kliknij na nazwę konta, które chcesz edytować.
3. W ustawieniach konta znajdź sekcję *Poświadczenia*.
4. Pod *Zastąp sekret przez:*, wybierz *Skarbiec haseł*.



5. Kliknij listę rozwijaną *Nazwa sekretu* aby zobaczyć dostępne sekrety.
6. Wybierz sekret z listy.
7. Szczegóły sekretu zostaną wyświetlone, pokazując informacje o loginie i domenie.
8. Opcjonalnie włącz pola wyboru:
   - *Użyj domeny z sekretu* - Używa domeny zapisanej w sekrecie
   - *Użyj loginu z sekretu* - Używa nazwy loginu zapisanej w sekrecie
9. Kliknij *Zapisz* lub *Zapisz i zamknij* aby zastosować zmiany.

Uwaga

Przycisk *Dodaj sekret* w liście rozwijanej wyboru sekretów pozwala utworzyć nowy sekret bezpośrednio z interfejsu konfiguracji konta jeśli wymagany sekret jeszcze nie istnieje.

Uwaga

- **Uprawnienia**: Użytkownicy muszą mieć odpowiednie uprawnienia zarówno do konta jak i sekretu w skarbcu haseł aby móc ustanowić połączenie.
- **Ścieżka audytu**: Dostęp do sekretów przez konta jest rejestrowany zarówno w logach aktywności konta jak i w karcie Dostęp do sekretów.
- **Wyłączność wypożyczania**: Jeśli sekret ma włączoną opcję **Zarezerwuj na wyłączność**, tylko jeden użytkownik może uzyskać do niego dostęp na raz poprzez konto.

Powiązane tematy:

- *Tworzenie sekretów*
- *Dostęp do edycji sekretów*
- *Monitorowanie dostępu do sekretów*
- *Opis modułu*

11.4 Monitorowanie dostępu do sekretów

Zakładka **Dostęp do sekretów** umożliwia szczegółowe śledzenie wszystkich zdarzeń związanych z dostępem do sekretów w Skarbcu haseł. Ten scentralizowany widok pozwala administratorom monitorować, kto uzyskał dostęp do poszczególnych sekretów, kiedy nastąpił dostęp oraz czy wykryto jakiekolwiek zagrożenia bezpieczeństwa.

Przejdź do *Skarbiec haseł* > *Dostęp do sekretów* aby uzyskać dostęp do interfejsu monitorowania.

Widok dostępu do sekretów wyświetla kompleksową tabelę z następującymi informacjami dla każdego zdarzenia:

- **Użytkownik**: Użytkownik, który uzyskał dostęp do sekretu (klikalne łącze do profilu użytkownika).
- **Sekret**: Nazwa sekretu, do którego uzyskano dostęp (klikalne łącze do szczegółów sekretu).
- **Kolekcja**: Kolekcja zawierająca sekret (klikalne łącze do kolekcji).
- **Data rozpoczęcia**: Kiedy rozpoczął się dostęp do sekretu.
- **Data zakończenia**: Kiedy dostęp do sekretu został zakończony.
- **Status**: Aktualny status dostępu (Trwający lub Zakończony).
- **Zdarzenia**: Zdarzenia bezpieczeństwa wykryte podczas dostępu.

11.4.1 Typy zdarzeń i wskaźniki statusu

Status dostępu

System śledzi cykl życia każdego dostępu do sekretu:

- **Zakończony**: Sesja dostępu do sekretu została zakończona.
- **Trwający**: Sekret jest obecnie używany.

Wykrywanie ujawnienia sekretu

W ramach monitorowania dostępu do sekretów system umożliwia również wykrywanie potencjalnych narażeń. Informacja o wykrytym zagrożeniu bezpieczeństwa jest wyświetlana w kolumnie **Zdarzenia** jako **Wykryto ujawnienie**.

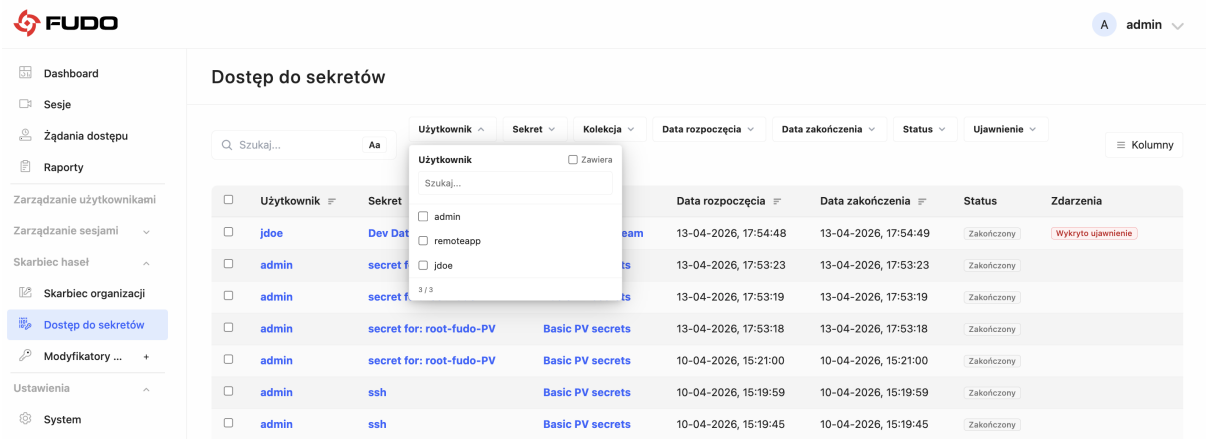
> **Uwaga**
>
> Wykrycie ujawnienia następuje, gdy użytkownik, który podejrzał sekret, zostanie zablokowany w Fudo Enterprise.

Najechanie kursorem na zdarzenie wykrycia ujawnienia sekretu wyświetla dodatkowe informacje o przyczynie narażenia, takie jak:

- **Użytkownik zablokowany**: Konto użytkownika zostało zablokowane lub dezaktywowane.
- **Podejrzana aktywność**: Wykryto nietypowe wzorce dostępu.
- **Naruszenie polityki**: Dostęp naruszył zdefiniowane polityki bezpieczeństwa.

11.4.2 Filtrowanie i przeglądanie zdarzeń

Interfejs dostępu do sekretów pozwala filtrować zdarzenia według użytkownika, sekretu, kolekcji, zakresu czasu, statusu, narażenia i obsługi alertów.



Funkcjonalność wyszukiwania

Pasek wyszukiwania na górze interfejsu umożliwia szybkie wyszukiwanie tekstowe we wszystkich widocznych polach danych.

Uwaga

Wyszukiwanie domyślnie nie uwzględnia wielkości liter, z przyciskiem przełączania *Aa* do wyszukiwania uwzględniającego wielkość liter.

Zarządzanie kolumnami

Administratorzy mogą dostosować widoczne kolumny używając przycisku „Kolumny". To pozwala na pokazywanie lub ukrywanie określonych kolumn w zależności od potrzeb monitorowania.

Powiązane tematy:

- *Opis modułu*
- *Zarządzanie prawami do kolekcji*
- *Dostęp do edycji sekretów*

11.5 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*.

Wbudowane modyfikatory haseł obejmują następujące scenariusze:

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

11.5.1 Polityki haseł

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

11.5.1.1 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.

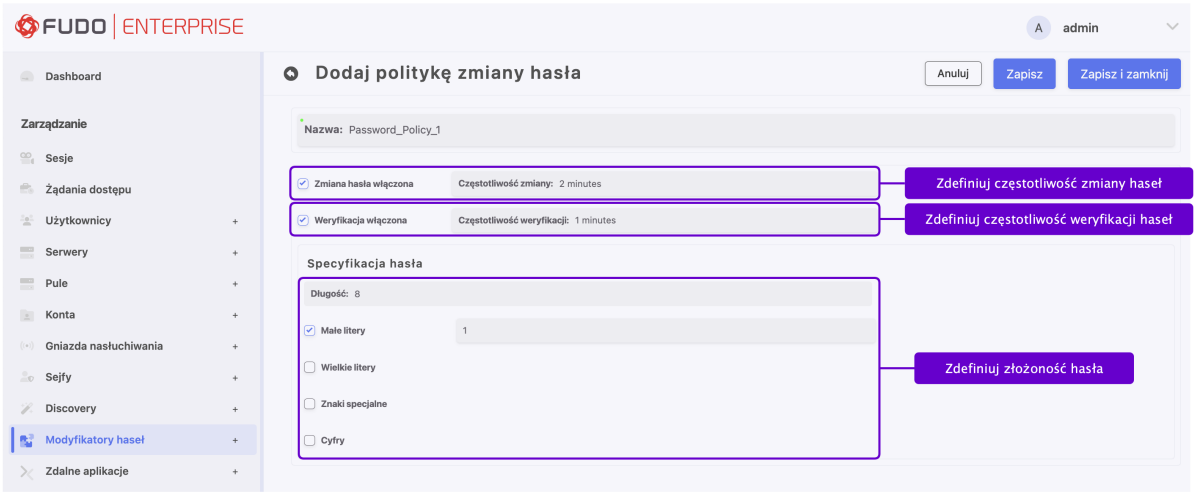
6. Wybierz opcję *Weryfikacja włączona* i określ przedział czasu między każdą weryfikacją hasła.
7. Zdefiniuj złożoność hasła.

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.

Uwaga

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

7. Kliknij *Zapisz*.

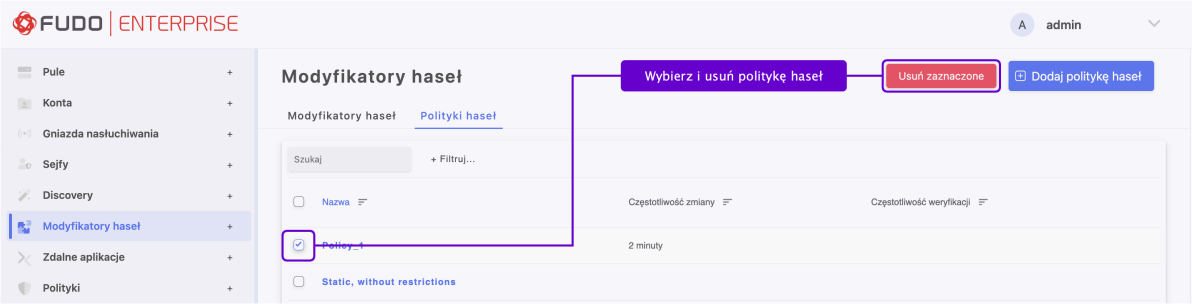


11.5.1.2 Edycja polityki zmiany haseł

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*.

11.5.1.3 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*

11.5.2 Uniwersalne modyfikatory haseł

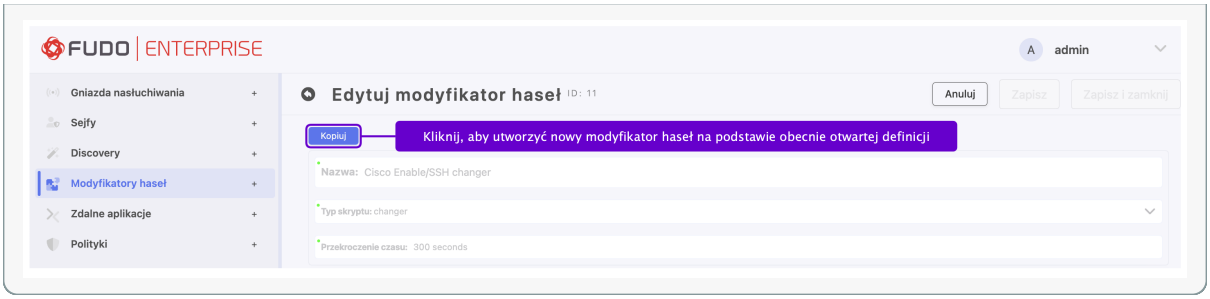
Uniwersalne modyfikatory haseł umożliwiają zdefiniowanie sekwencji komend, które zostaną wykonane na zdalnej maszynie w celu zmiany hasła.

> **Uwaga**
>
> 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*.

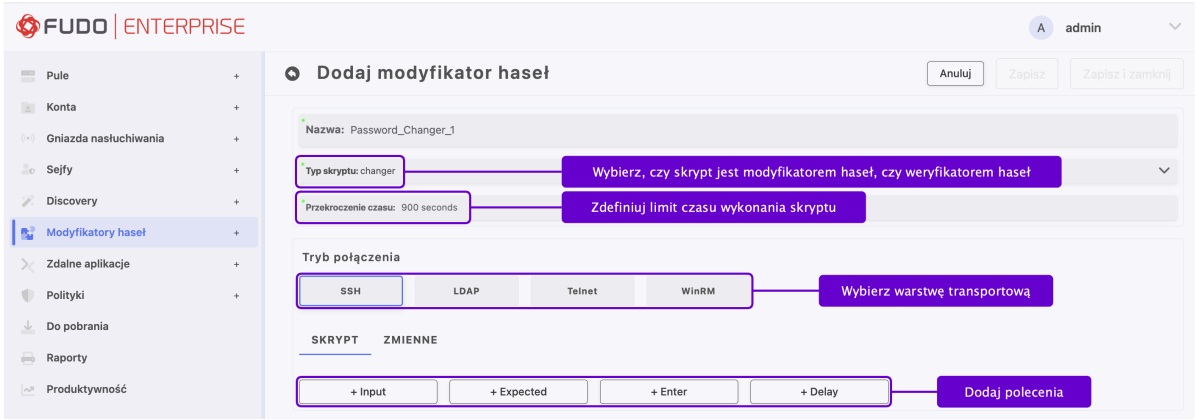
11.5.2.1 Definiowanie modyfikatora haseł

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

> **Uwaga**
>
> 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.



Uwaga

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

- Do przeprowadzania zmiany haseł należy użyć konta (`transport_login`

i `transport_secret`), które ma delegowane uprawnienia *Reset user passwords and force password change at next logon* dla *Organizational Unit (OU)* zawierającej użytkowników, których hasła będą zmieniane, lub konto musi należeć do grupy *Account Operators*.

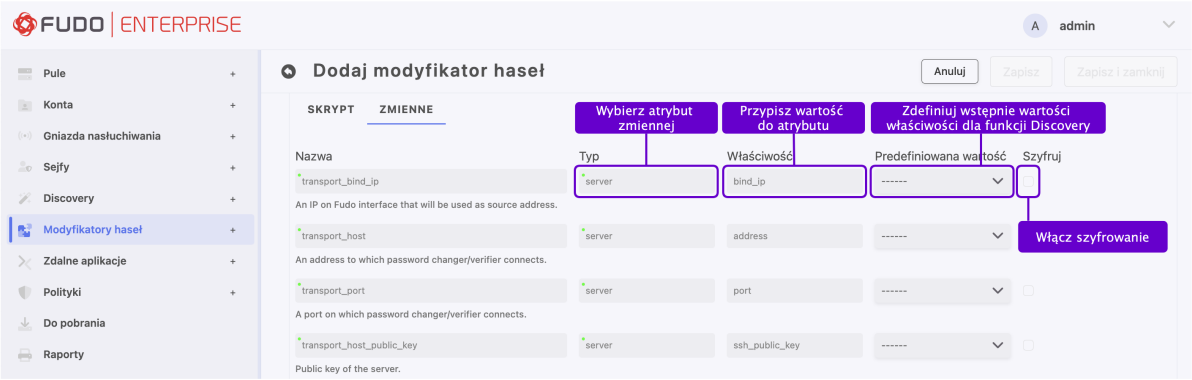
- Aby skonfigurować modyfikatory haseł **WinRM**, musisz podać dane uwierzytelniające użytkownika z uprawnieniami do zmiany haseł (zwykle konto na poziomie administratora). Ważne jest jednak, aby nie używać tego konta do zmiany jego własnego hasła, ponieważ WinRM zwróci błąd, którego Fudo Enterprise nie może obsłużyć. **Upewnij się, że zmienne ``account_login`` i ``transport_login`` mają różne wartości.**

8. Wprowadź polecenie lub zdefiniuj parametry działania.

Uwaga

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.



Uwaga

- 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*.

Uwaga

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	✗

11.5.2.2 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*.

11.5.2.3 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*

11.5.3 Importowanie i eksportowanie modyfikatorów haseł

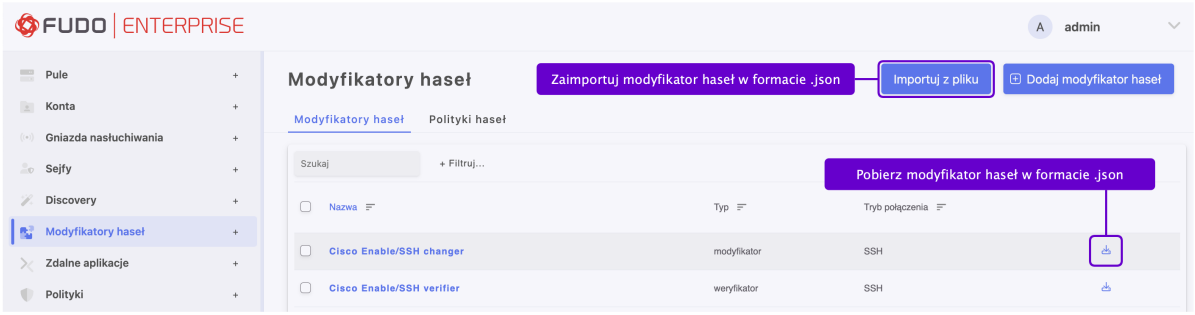
Modyfikatory haseł utworzone w Fudo Enterprise mogą być pobrane i zaimportowane do innej instancji Fudo Enterprise.

11.5.3.1 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.



11.5.3.2 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*

11.5.4 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.

11.5.4.1 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. **Uwaga** 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.

11.5.4.2 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.

Uwaga

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.

11.5.4.3 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.

11.5.4.4 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.

Uwaga

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.**

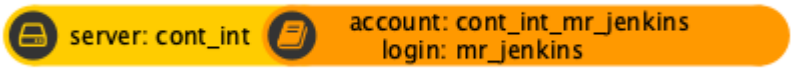
Zmienna	Opis
transport_bind_ip	Adres IP używany przez Fudo przy komunikacji ze zdalnym systemem.
transport_ca_certificate	Certyfikat CA systemu docelowego.
transport_encoding	Kodowanie tekstu na systemie docelowym.
transport_host	Adres IP zdalnego systemu, z którym łączy się modyfikator hasła.
transport_login	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*

11.5.5 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.

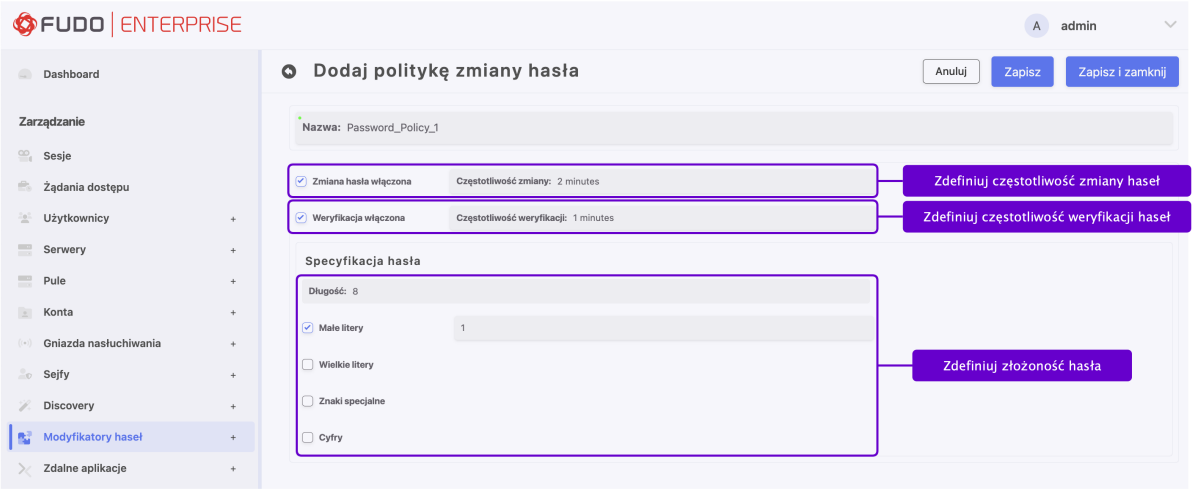
Dodawanie polityki zmiany hasła

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.

Uwaga

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*.

> **Uwaga**
>
> 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*.

Uwaga

- 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 12

Ustawienia

Poniższy rozdział zawiera opisy czynności administracyjnych.

12.1 System

12.1.1 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* oraz korzystania z *Fudo ShareAccess*.

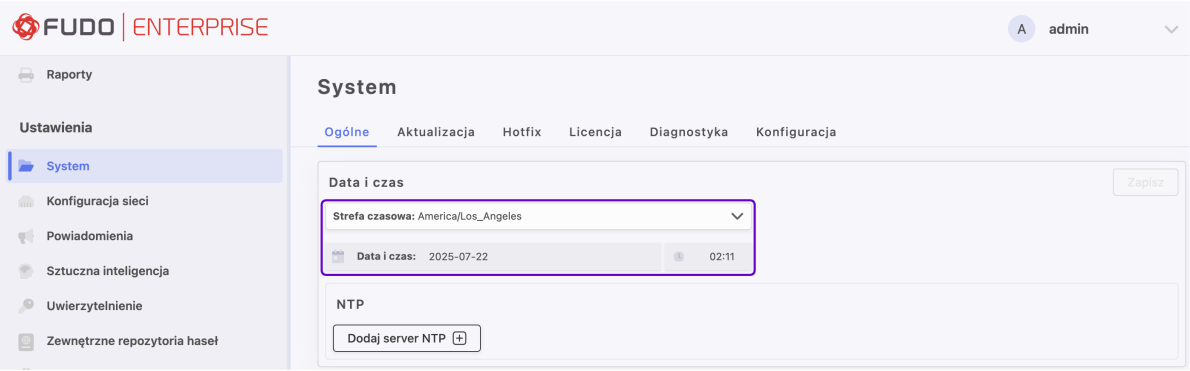
Zmiana daty i czasu

Uwaga

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. Przejdź do załadki *Ogólne*.
3. Zmień ustawienia daty i czasu w sekcji *Data i czas*.



4. Kliknij *Zapisz*.
5. Uruchom ponownie Fudo Enterprise aby zastosować zmiany.

Uwaga

Aby wyszukać strefę czasową, rozwiń listę i wpisz kilka pierwszych liter jej nazwy w polu *Szukaj...*.

Konfiguracja serwerów czasu

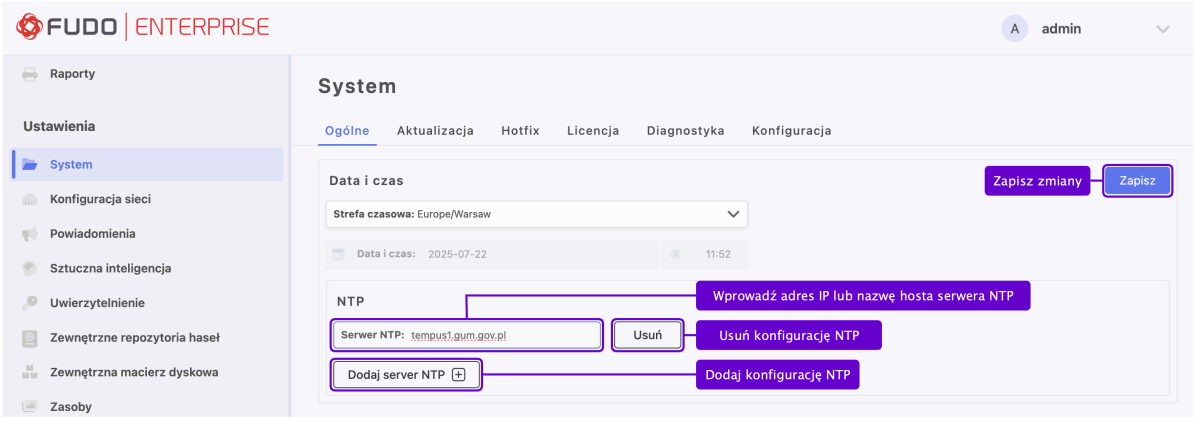
Uwaga

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. Przejdź do załadki *Ogólne*.
3. Kliknij *Dodaj serwer NTP* + w sekcji *NTP*, aby dodać definicję serwera czasu.
4. Wprowadź adres IP lub nazwę hosta serwera NTP.



5. Kliknij *Zapisz*.
6. Uruchom ponownie Fudo Enterprise aby zastosowa zmiany (skorzystaj z linku w komunikacie, lub 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. Przejdź do załadki *Ogólne*.
3. Wyszukaj i zmodyfikuj żądany wpis w sekcji *Serwery NTP*.
4. Kliknij *Zapisz*.
5. Uruchom ponownie Fudo Enterprise aby zastosowa zmiany (skorzystaj z linku w komunikacie, lub 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. Przejdź do załadki *Ogólne*.
3. Kliknij *Usuń* przy żądanej definicji serwera NTP i kliknij *Zapisz*.
4. Uruchom ponownie Fudo Enterprise aby zastosowa zmiany (skorzystaj z linku w komunikacie, lub wybierz z menu użyktownika opcję *Uruchom ponownie*).

Tematy pokrewne:

- *Znakowanie czasem*

12.1.2 Certyfikaty SSL

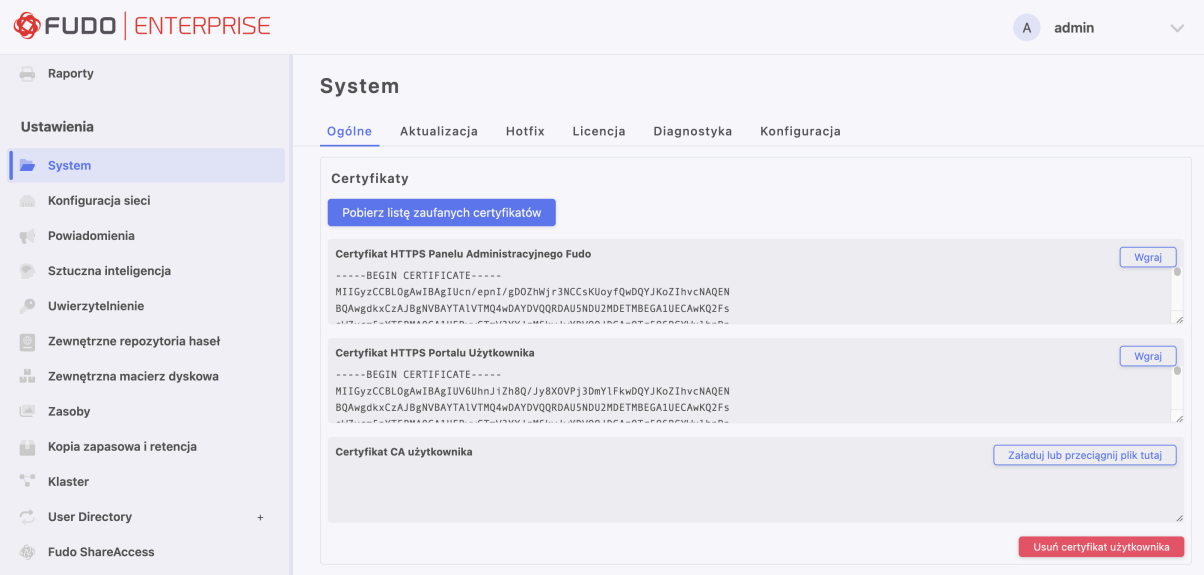
Certyfikat HTTPS pozwala administratorowi upewnić się, że nawiązał połączenie z panelem administracyjnym Fudo Enterprise a nie ze stroną próbującą podszyć pod panel administracyjny celem pozyskania danych logowania konta administratora.

- **Certyfikat HTTPS Panelu Administracyjnego Fudo** – zabezpiecza dostęp do Panelu Administracyjnego przez HTTPS.
- **Certyfikat HTTPS Portalu Użytkownika** – zabezpiecza portal logowania użytkowników końcowych.

- **Certyfikat CA użytkowników** – zaufane urzędy certyfikacji wykorzystywane do weryfikacji certyfikatów klientów podczas uwierzytelniania.

Uwaga

Fudo Enterprise wymaga użycia niezaszyfrowanych kluczy do certyfikatów. Dzięki temu użytkownik nie musi podawać hasła do klucza przy każdym ponownym uruchomieniu. Zobacz: Jak odszyfrować klucz prywatny RSA chroniony hasłem.



Konfiguracja certyfikatu SSL dla Panelu Administracyjnego Fudo

1. Wybierz *Ustawienia* > *System*.
2. Przejdź do zakładki *Ogólne*.
3. W sekcji *Certyfikat HTTPS Panelu Administracyjnego Fudo* kliknij przycisk *Wgraj*.
4. Kliknij *Wybierz plik* w polu *Certyfikat HTTPS Panelu Administracyjnego Fudo* i wskaż lokalizację pliku certyfikatu SSL w formacie PEM.
5. Kliknij *Wybierz plik* w polu *Klucz prywatny HTTPS* i wskaż lokalizację pliku klucza prywatnego.
6. Wprowadź hasło do klucza prywatnego, jeśli klucz jest zaszyfrowany.
7. Kliknij *Zapisz*.

Konfiguracja certyfikatu SSL dla Portalu Użytkownika

1. Wybierz *Ustawienia* > *System*.
2. Przejdź do zakładki *Ogólne*.
3. W sekcji *Certyfikat HTTPS Portalu Użytkownika* kliknij przycisk *Wgraj*.
4. Kliknij *Wybierz plik* w polu *Certyfikat HTTPS Portalu Użytkownika* i wskaż lokalizację pliku certyfikatu SSL w formacie PEM.
5. Kliknij *Wybierz plik* w polu *Klucz prywatny HTTPS* i wskaż lokalizację pliku klucza prywatnego.

6. Wprowadź hasło do klucza prywatnego, jeśli klucz jest zaszyfrowany.
7. Kliknij *Zapisz*.

Konfiguracja certyfikatu CA użytkownika

1. Wybierz *Ustawienia* > *System*.
2. Przejdź do zakładki *Ogólne*.
3. W sekcji *Certyfikat CA użytkowników* kliknij przycisk *Załaduj lub przeciągnij plik tutaj* i wskaż lokalizację pliku certyfikatu CA.

Uwaga

Aby usunąć certyfikat CA użytkownika, kliknij przycisk *Usuń certyfikat użytkownika* poniżej okna certyfikatu.

Tematy pokrewne:

- *Bezpieczeństwo*
- *Zarządzanie serwerami*

12.1.3 Dostęp SSH

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

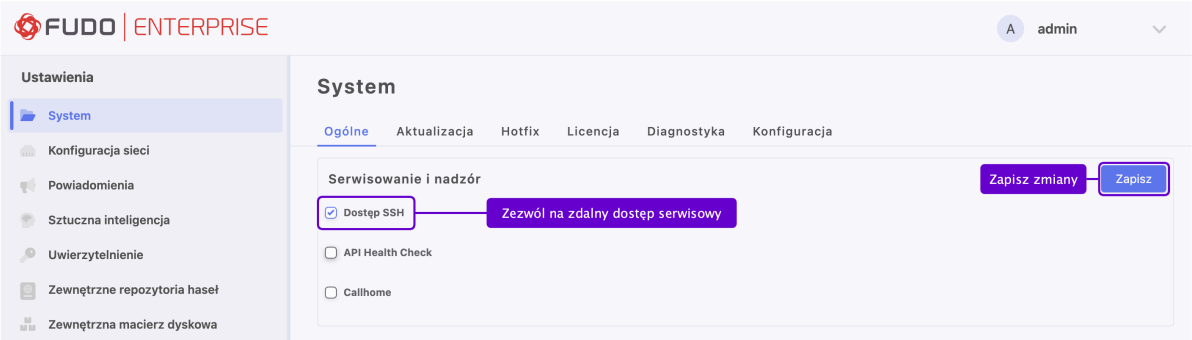
Uwaga

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 *Ustawienia* > *System*.
2. Przejdź do zakładki *Ogólne*.
3. W sekcji *Serwisowanie i nadzór* zaznacz opcję *Dostęp SSH*.



4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Callhome*
- *Konfiguracja ustawień sieciowych*

12.1.4 Szyfrowanie konfiguracji

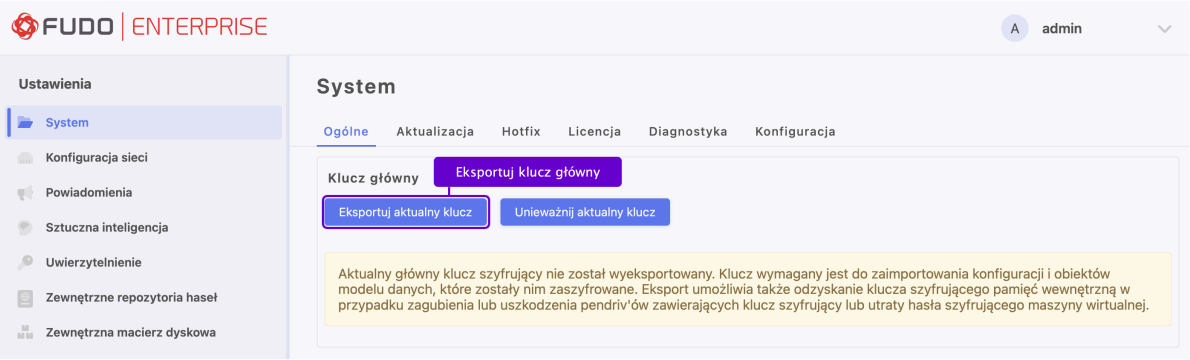
Główny klucz szyfrujący zapewnia bezpieczeństwo i poufność danych konfiguracyjnych, kopii zapasowych systemu i zewnętrznych wolumenów przechowywania danych. Klucz umożliwia również odzyskanie klucza szyfrującego wewnętrznego wolumenu danych w przypadku zaginięcia lub uszkodzenia kluczy zapisanych na nośnikach pamięci podczas inicjalizacji systemu.

Uwaga

- 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 z lewego menu *Ustawienia* > *System*.
2. Przejdź do załadki *Ogólne*.
3. W sekcji *Klucz główny*, kliknij *Eksportuj aktualny klucz*.



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

Uwaga

- 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
```

5. Kliknij *Zapisz* aby zapisać 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. Przejdź do załadki *Ogólne*.
3. W sekcji *Klucz główny*, kliknij *Unieważnij aktualny klucz*.



4. Kliknij *Potwierdź*.
5. Pamiętaj o konieczności *wyeksportowania nowego klucza*.

Tematy pokrewne:

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

12.1.5 SNMP

Fudo Enterprise wspiera funkcję monitorowania stanu systemu z wykorzystaniem protokołu SNMP.

12.1.5.1 Konfigurowanie SNMP

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Przejdź do zakładki *Ogólne*.
3. W sekcji *SNMP* podaj nazwę uytkownika i hasło do uwierzytelniania przez usługę SNMP.
4. Z listy rozwijanej *Metoda szyfrowania*, wybierz algorytm szyfrujący komunikację SNMP (*AES* lub *DES*).
5. Z listy rozwijanej *Metoda uwierzytelnienia*, wybierz metodę *SHA* lub *MD5*.
6. Zaznacz opcję *SNMPv3*.
7. Z listy rozwijanej *Adres źródłowy* wybierz adres IP, który będzie używany do komunikacji z innymi systemami poprzez protokół SNMP.
8. Podaj *port*.
9. Kliknij *Zapisz*.

Uwaga

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.

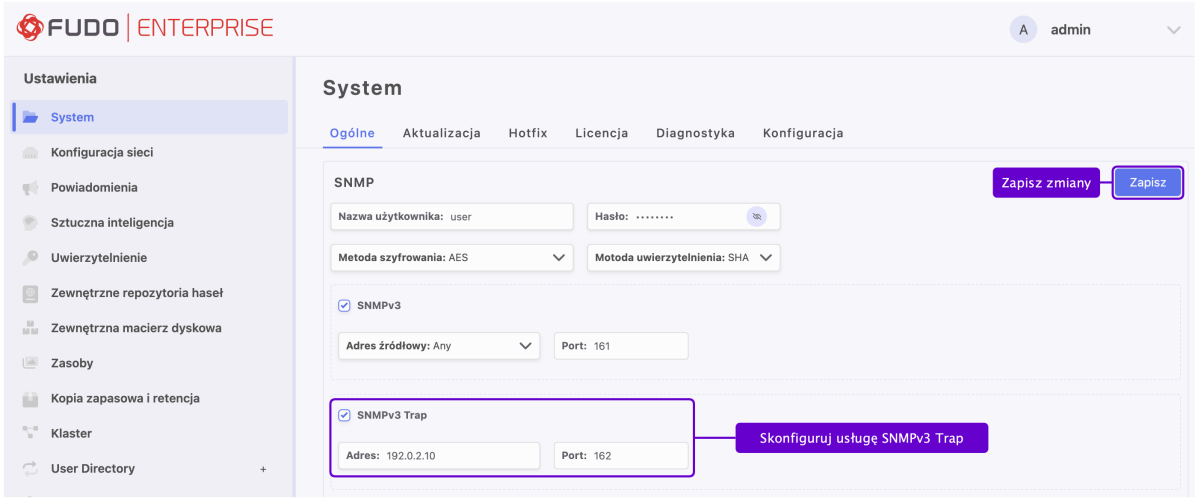
12.1.5.2 Konfigurowanie SNMPv3 TRAP

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 *Ustawienia* > *System*.
2. Przejdź do zakładki *Ogólne*.
3. W sekcji *SNMP* podaj nazwę uytkownika i hasło do uwierzytelniania przez usługę SNMP.
4. Z listy rozwijanej *Metoda szyfrowania*, wybierz algorytm szyfrujący komunikację SNMP (*AES* lub *DES*).
5. Z listy rozwijanej *Metoda uwierzytelnienia*, wybierz metodę *SHA* lub *MD5*.
6. Zaznacz opcję *SNMPv3 Trap*.
7. W polu *Adres* wybierz adres IP, który będzie używany do komunikacji z innymi systemami poprzez protokół SNMP.
8. Podaj *port*.
9. 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.

Uwaga

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.

12.1.5.3 SNMP MIBs

MIB wspierane przez Fudo Enterprise:

- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB (RFC 2790) - częściowe wsparcie
- UCD-SNMP-MIB

12.1.5.4 Odczytywanie informacji SNMP poprzez `snmpwalk`

Uwaga

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 **Uwaga** 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

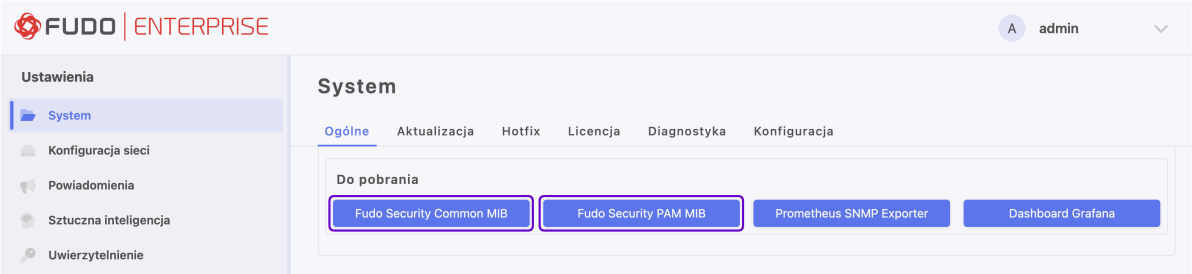
12.1.5.5 Rozszerzenia SNMP Fudo Enterprise

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

Pliki specyfikacji MIB (Fudo Security Common MIB oraz Fudo Security PAM MIB) są dostępne do pobrania w sekcji *Utrzymanie i nadzór* w Ustawienia > System. Pliki te mogą zostać wczytane do managera SNMP w celu obsługi rozszerzeń specyficznych dla Fudo Enterprise.



Uwaga

W Fudo Enterprise 5.5.8 zaktualizowano definicję MIB. Plik `FUDO-SECURITY-COMMON-MIB.txt` został zmodyfikowany: `smartHealth` obsługuje teraz tylko następujące stany: `ok (1)` i `failed (2)`.

Tematy pokrewne:

- *Bezpieczeństwo*
- *Rozwiązywanie problemów*
- *Polityki*

12.1.6 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.

Uwaga

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

Uwaga

Znacznikiem czasu zostaną opatrzone jedynie sesje, które zostały zakończone po włączeniu usługi.

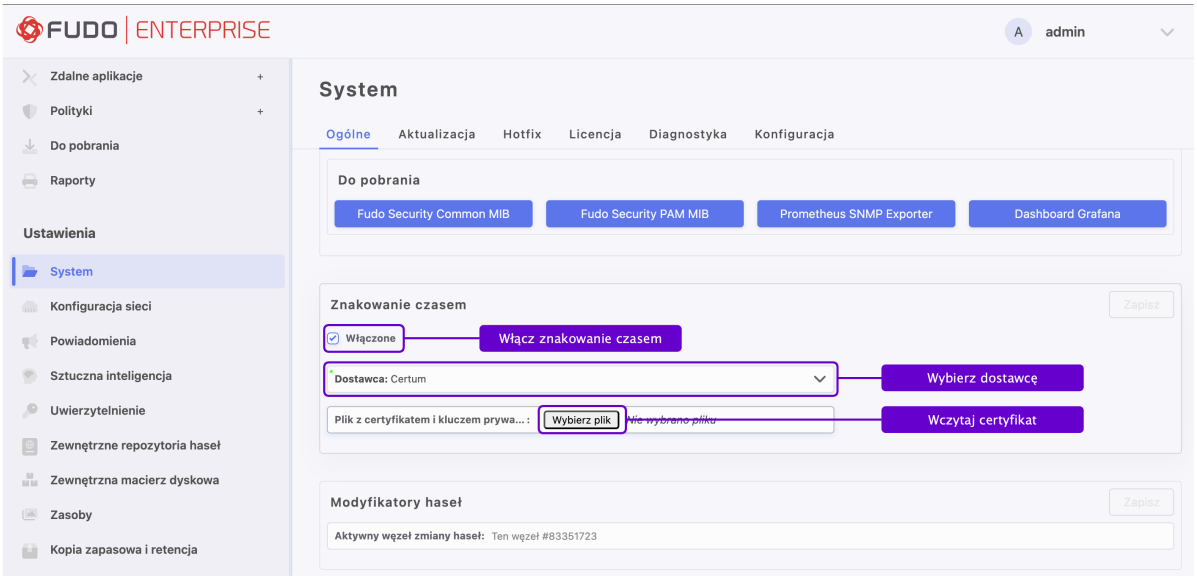
Aby włączyć i skonfigurować usługę znakowania czasem, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Przejdź do zakładki *Ogólne*, a następnie przewiń w dół do sekcji *Znakowanie czasem*.
3. Zaznacz opcję *Włącz*, aby znakować znacznikiem czasu zarejestrowane sesje.
4. Z listy rozwijanej wybierz dostawcę usługi znakowania czasem.
5. Wskaż pliki zawierające certyfikat oraz klucz prywatny otrzymane od dostawcy.

Uwaga

Certyfikat oraz klucz prywatny otrzymasz od dostawcy usługi znakowania czasem.

5. Kliknij *Zapisz*.



Tematy pokrewne:

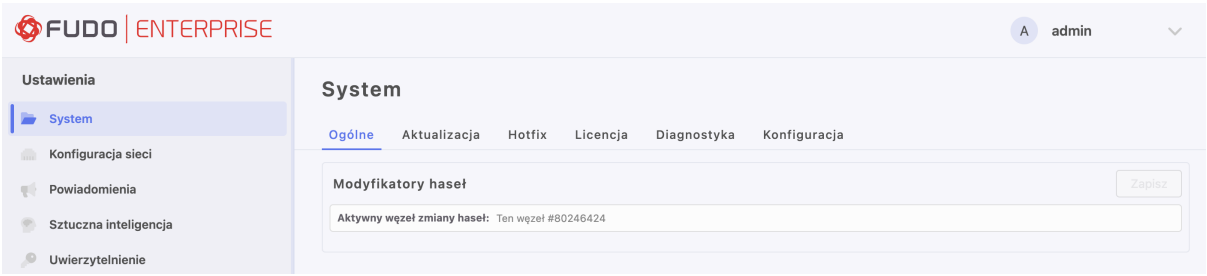
- *Mechanizmy bezpieczeństwa*

12.1.7 Modyfikatory haseł - aktywny węzeł klastra

Opcja wyboru aktywnego węzła klastra wskazuje instancję Fudo Enterprise, która realizuje zmianę haseł na monitorowanych systemach.

> **Uwaga**
>
> Aby modyfikatory haseł działały poprawnie, wymagane są co najmniej dwa aktywne węzły. W konfiguracji dwuwęzłowej awaria jednego węzła powoduje zatrzymanie działania modyfikatorów haseł, dlatego zalecana jest konfiguracja **trzech węzłów**.

1. Wybierz z lewego menu *Ustawienia* > *System*.
2. Wybierz zakładkę *Ogólne*.
3. W sekcji *Modyfikatory haseł*, z listy rozwijalnej *Aktywny węzeł zmiany haseł*, wybierz węzeł odpowiedzialny za wykonanie skryptów modyfikujących hasła.



4. Kliknij *Zapisz*.

> **Uwaga**
>
> W sytuacji, w której wskazany węzeł ulegnie awarii, zadanie zmiany haseł nie zostanie auto-

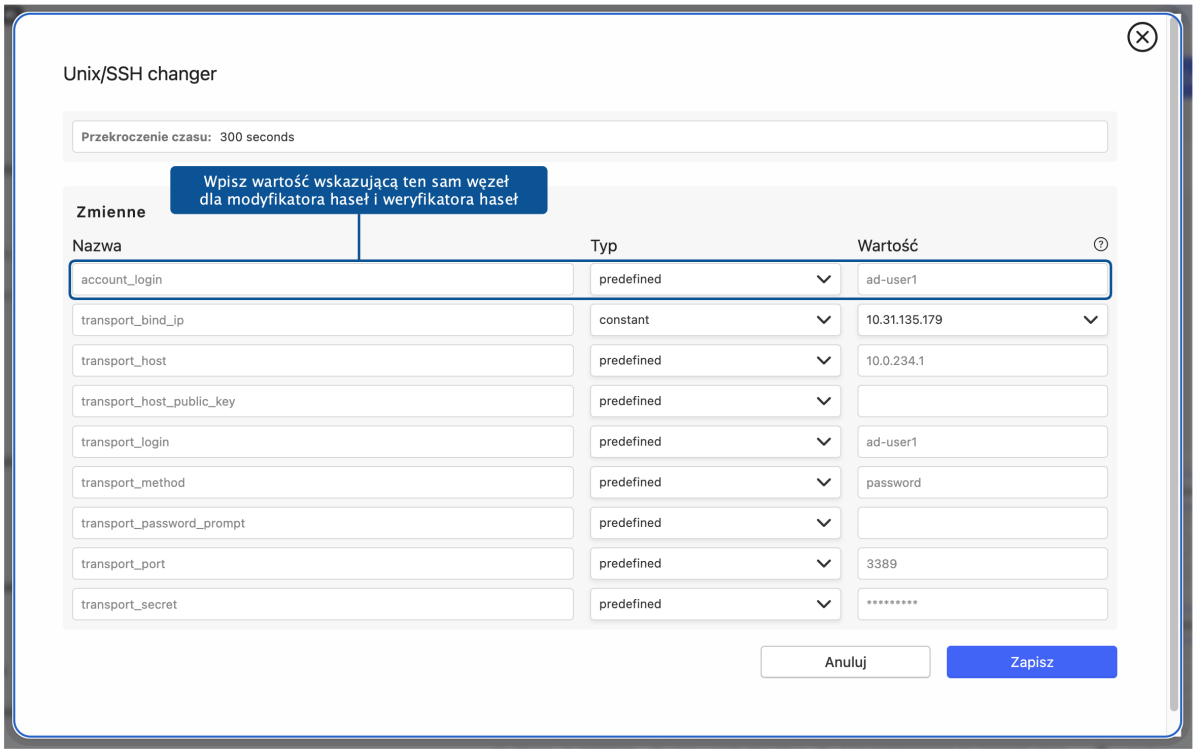
matycznie podjęte przez inną instancję Fudo Enterprise. Automatyczna zmiana haseł wymaga zmiany przypisania aktywnego węzła lub przywrócenie działania uszkodzonej jednostki.

12.1.7.1 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*

12.1.8 Funkcjonalności wrażliwe

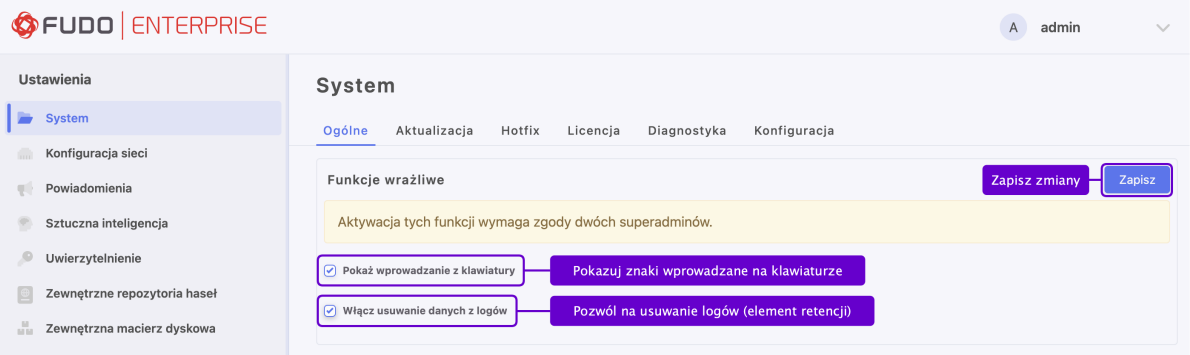
Funkcje wrażliwe to zestaw opcji, których włączenie wymaga zatwierdzenia przez dwóch użytkowników posiadających zarówno uprawnienie `sensitive-feature-read`, jak i `sensitive-feature-modify`.

Uwaga

Domyślnie znaki wprowadzone na klawiaturze nie są wyświetlane w odtwarzaczu sesji. Włączenie tej funkcji wymaga zatwierdzenia przez dwóch użytkowników posiadających zarówno uprawnienie `sensitive-feature-read`, jak i `sensitive-feature-modify`.

Aby włączyć wybrane funkcje wraliwe, postępuj zgodnie z poniższą instrukcją.

1. Wybierz *Ustawienia* > *System*.
2. Przejdź do zakładki *Ogólne*.



3. Zaznacz opcję *Pokaż wprowadzanie z klawiatury* w sekcji *Funkcje wrażliwe*, aby zainicjować włączenie funkcji.
4. Zaznacz opcję *Włącz usuwanie danych z logów*, powiązaną z funkcjonalnością Retencji logów: *Kopia zapasowa danych sesji*.

- Opcja ta współdziała z ustawieniami retencji, w których można określić, kiedy dane dziennika mają być usuwane.



5. Kliknij *Zapisz*.
6. Powiadom drugiego administratora z uprawnieniami o zainicjowaniu funkcjonalności, która wymaga równie jego potwierdzenia.

Tematy pokrewne:

- *Odtwarzanie sesji*

12.1.9 Konfigurowanie serwera proxy HTTP

Fudo Enterprise obsługuje użycie wychodzącego serwera proxy HTTP do przekierowywania ruchu związanego z uwierzytelnianiem, takiego jak komunikacja z dostawcami OIDC, Microsoft Entra ID, Duo Security lub bramkami SMS. W ten sam sposób można również skonfigurować proxy wykorzystywane do funkcji znakowania czasem sesji. Jest to szczególnie przydatne w środowiskach, w których Fudo Enterprise nie ma bezpośredniego dostępu do Internetu lub gdzie wszystkie połączenia wychodzące muszą być przekierowywane przez kontrolowany serwer proxy.

Konfigurację proxy można przeprowadzić bezpośrednio z poziomu interfejsu Fudo Enterprise.

Uwaga

Serwer proxy HTTP jest obecnie używany w ramach następujących integracji uwierzytelniania: **OIDC**, **SMS** i **DUO**. Może być również wykorzystywany do integracji z usługami **timestampingu**. Obsługa dodatkowych komponentów zostanie dodana w przyszłych wersjach.

Wymagania wstępne

- Dostępny serwer proxy HTTP (np. *tinyproxy*) skonfigurowany do obsługi połączeń wychodzących.
- Adres proxy (nazwa hosta lub adres IP) oraz port.
- Upewnij się, że serwer proxy używa schematu HTTP.

Konfigurowanie proxy

1. Wybierz *Ustawienia* > *System*.
2. W podzakładce *Ogólne* znajdź sekcję *Konfiguracja proxy*.
3. Zaznacz opcję *Włącz konfigurację proxy*.
4. Wprowadź adres proxy w jednym z poniższych formatów: `host:port` lub `http://host:port`.

Przykład:

```
        proxy.example.com:3128
        http://10.0.0.15:8080

5. Kliknij `Zapisz`, aby zastosować konfigurację.

.. image:: _images/system/5-6-http-proxy.png
```

Uwaga

Schemat `https://`—proxy HTTPS nie są obsługiwane.

Powiązane tematy:

- *Środki bezpieczeństwa*

12.1.10 Aktualizacja systemu

Uwaga

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

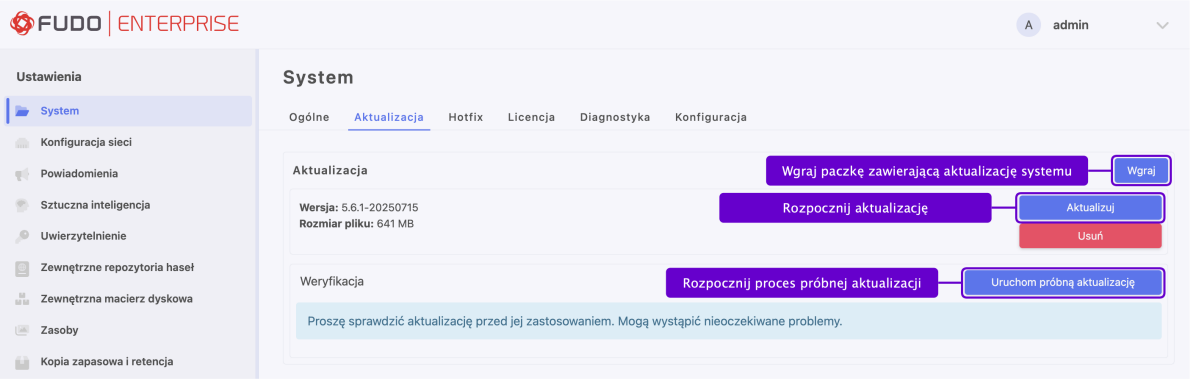
- Podczas aktualizacji systemu, zużycie wewnętrznej macierzy dyskowej może tymczasowo wzrosnąć.
- W przypadku konfiguracji klastrowej, w pierwszej kolejności dokonaj aktualizacji na węźle podrzędnym.

12.1.10.1 Aktualizowanie systemu

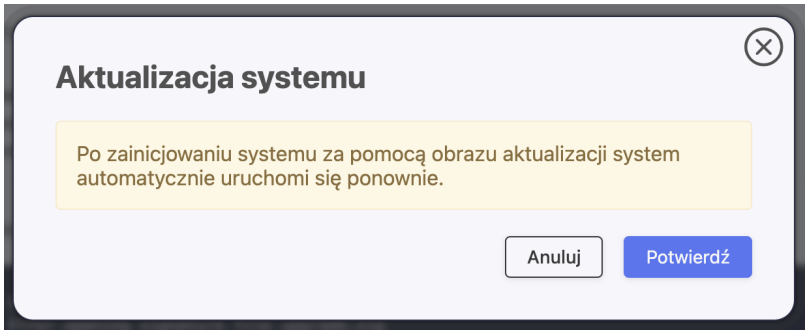
Ostrzeżenie

- 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 *Uruchom próbną aktualizację* przy wybranym pliku obrazu, aby stwierdzić, czy obiekty modelu danych i bieżąca konfiguracja są kompatybilne z nową wersją systemu.



6. Kliknij *Aktualizuj*.
7. Kliknij *Potwierdź*, aby wykonać aktualizację.

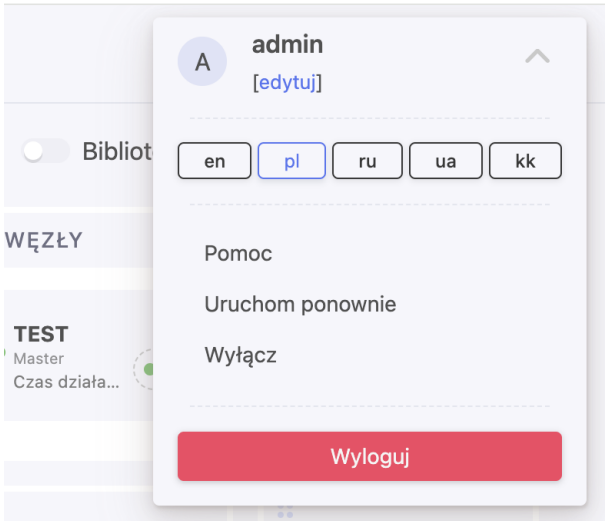


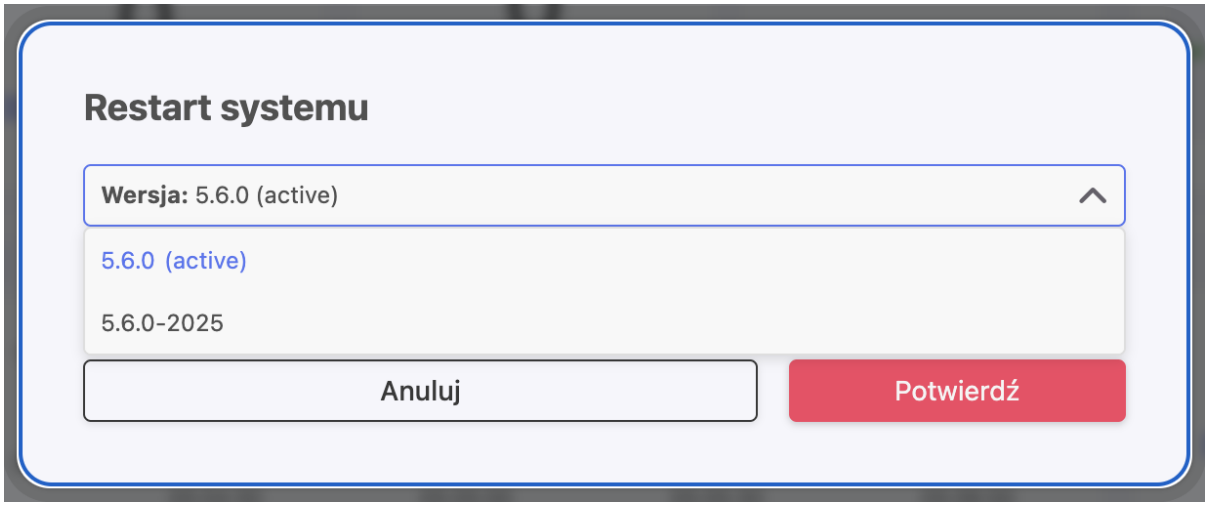
Ostrzeżenie

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

12.1.10.2 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*.

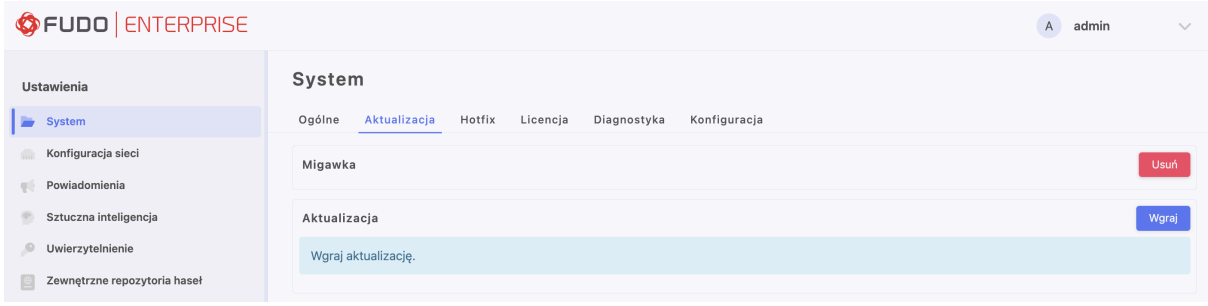
12.1.10.3 Usuwanie migawki aktualizacji

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* w sekcji *Migawka*.
4. Potwierdź usunięcie migawki.



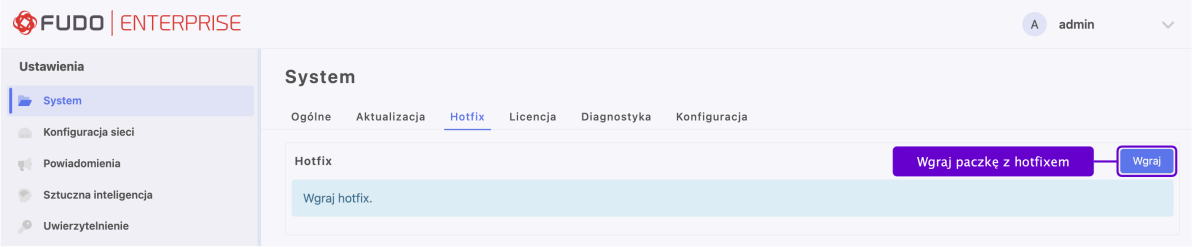
Tematy pokrewne:

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

12.1.11 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*

12.1.12 Licencja

Informacje o licencji

Zakładka **Licencja** wyświetla szczegółowe informacje o aktualnie załadowanej licencji oraz limitach zastosowanych do poszczególnych modułów.

Ogólne

Pole	Opis
Numer seryjny	Unikalny identyfikator załadowanej licencji.
Właściciel licencji	Nazwa organizacji, dla której wydana jest licencja.
Typ licencji	Kategoria licencji (na przykład *test* lub *commercial*).
Poziom licencji	Podstawowy licencjonowany moduł lub zestaw funkcji.
Limit węzłów klastra	Licencja określa liczbę węzłów, które mogą być częścią klastra. W przypadku przekroczenia tej liczby dodatkowe węzły będą odrzucać połączenia i rejestrować odpowiednie zdarzenia w logach systemowych.

Zarządzanie sesjami uprzywilejowanymi

Pole	Opis
Data wygaśnięcia	Data wygaśnięcia licencji na Zarządzanie sesjami uprzywilejowanymi.
Dostępne serwery	Liczba serwerów aktualnie skonfigurowanych w systemie w porównaniu do maksymalnej dozwolonej przez licencję. Po przekroczeniu tego limitu dodawanie nowych serwerów lub modyfikowanie istniejących nie jest już możliwe. Więcej szczegółów można znaleźć w opisie *Trybu rozliczania*.
Liczba równoczesnych sesji	Licencja określa również maksymalną liczbę sesji, które mogą być jednocześnie monitorowane. Po osiągnięciu limitu nie można inicjować nowych sesji, dopóki liczba aktywnych sesji nie spadnie poniżej wartości licencyjnej.
Liczba aktywnych użytkowników	Liczba obecnie aktywnych użytkowników PSM w porównaniu do licencjonowanego limitu. Aktywny użytkownik to każdy użytkownik, który nawiązał sesję w Fudo Enterprise w ciągu ostatnich 30 dni*.
Tryb rozliczania	Określa sposób, w jaki system rozlicza wykorzystanie licencji pod kątem serwerów. Możliwe wartości to: • *host* – Wykorzystanie licencji opiera się na liczbie unikalnych adresów IP skonfigurowanych w systemie. Numery portów są ignorowane, co oznacza, że wiele serwerów zdefiniowanych z różnymi portami, ale tym samym adresem IP, jest traktowane jako jeden host. • *unlimited* – Liczba zdefiniowanych serwerów nie jest ograniczona. W tym trybie egzekwowanie licencji opiera się wyłącznie na liczbie równocześnie aktywnych sesji, a nie na liczbie skonfigurowanych serwerów.

Uwaga

Więcej informacji o limitach licencyjnych i zasadach obliczania aktywnych użytkowników znajduje się w sekcji *Licencjonowanie*.

Skarbiec haseł

Pole	Opis
Poziom licencji	Wskazuje poziom licencji Skarbca haseł (`PEŁNY` lub `PODSTAWOWY`).
Data wygaśnięcia	Data wygaśnięcia licencji Skarbca haseł.
Liczba aktywnych użytkowników	Liczba użytkowników aktualnie korzystających z funkcjonalności Skarbca haseł w porównaniu do licencjonowanego limitu.
Liczba dostępnych modyfikatorów	Maksymalna liczba modyfikatorów haseł, które można przypisać do kont i sekretów. Po osiągnięciu limitu nie można przypisać dodatkowych modyfikatorów haseł do innych kont i sekretów.

Uwaga

Jeśli nie zainstalowano dedykowanej licencji Skarbca haseł, moduł automatycznie działa w trybie **Podstawowym** z ograniczoną funkcjonalnością.

Dostępne języki

Licencja określa, które wersje językowe interfejsu produktu są dostępne. Obsługiwane języki mogą obejmować:

- Angielski (en)
- Polski (pl)
- Niemiecki (de)
- Kazachski (kk)
- Rosyjski (ru)
- Ukraiński (ua)
- Uzbecki (uz)

Uwaga

*Logowanie do **Panelu Administracyjnego** jest zawsze dozwolone. Zapobiega to zablokowaniu administratorów przed systemem z powodu limitów licencyjnych.

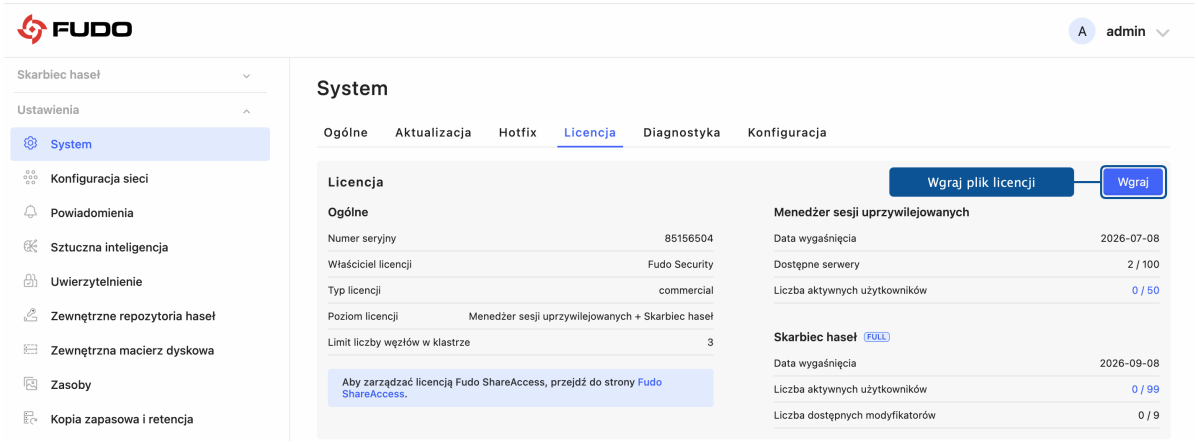
Wgrywanie nowej licencji

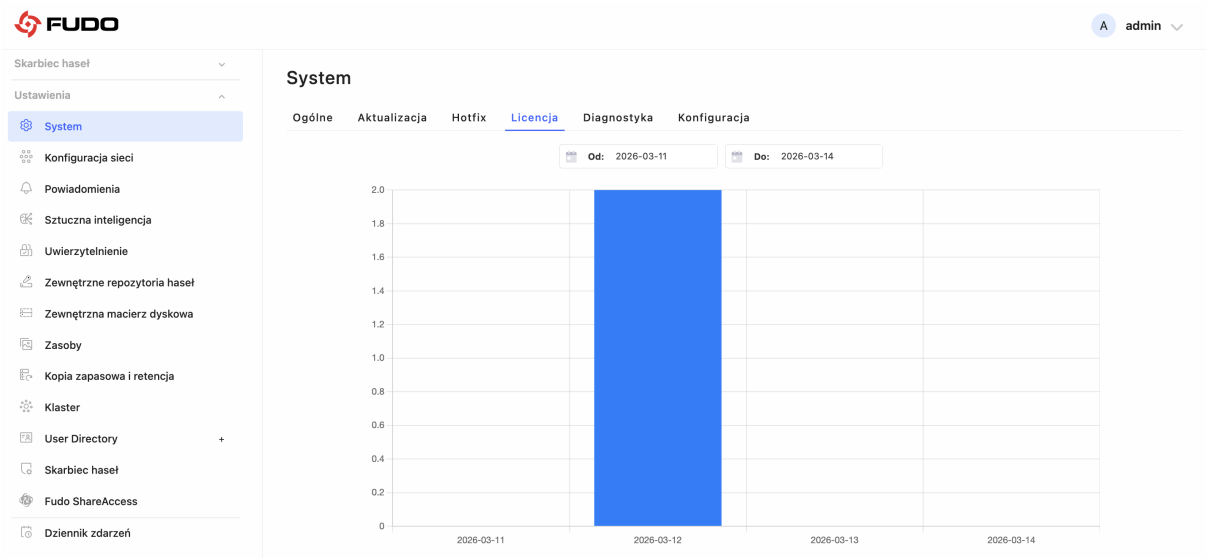
Aby wgrać nowy plik licencji, postępuj zgodnie z poniższą instrukcją.

Uwaga

Nowa licencja zastąpi istniejącą.

1. Wybierz *Ustawienia* > *System*.
2. Wybierz zakładkę *Licencja*.
3. Kliknij *Wgraj*.
4. Przeglądaj system plików, aby znaleźć plik licencji i kliknij *OK*, aby wgrać i zastąpić aktualną definicję licencji.





Tematy pokrewne:

- *Licencjonowanie*
- *Przegląd systemu*
- *Wymagania*
- *System*

12.1.13 Diagnostyka

Moduł diagnostyczny umożliwia wykonywanie podstawowych poleceń systemowych, takich jak ping, netcat czy traceroute.

Aby uruchomić wybrane narzędzie diagnostyczne, wykonaj następujące kroki.

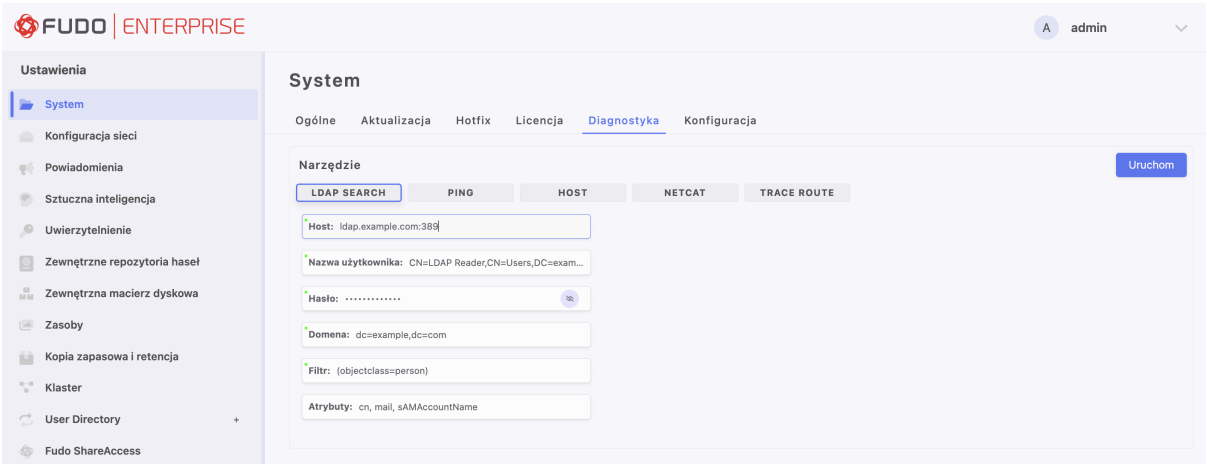
1. Wybierz *Ustawienia* > *System*.
2. Wybierz zakładkę Diagnostyka.
3. Każde z narzędzi jest dostępne w osobnej zakładce. Po przejściu do wybranego narzędzia wprowadź wymagane parametry i kliknij *Uruchom*, aby wykonać polecenie.

LDAP SEARCH

Narzędzie LDAP Search umożliwia administratorowi wykonywanie zapytań do serwera LDAP o obiekty katalogowe przy użyciu określonych filtrów i atrybutów.

Poniższa tabela opisuje dostępne parametry wymagane do wykonania wyszukiwania.

Polecenie/parametr	Opis
Host	Adres IP serwera LDAP.
Nazwa użytkownika	Login użytkownika uprawnionego do przeglądania katalogu.
Hasło	Hasło użytkownika uprawnionego do przeglądania katalogu.
Domena	Domena katalogowa, w której ma zostać wykonane zapytanie.
Filtr	Parametr filtrowania obiektów (np. `(objectClass=*)`).
Atrybuty	Atrybuty wyszukiwania LDAP.

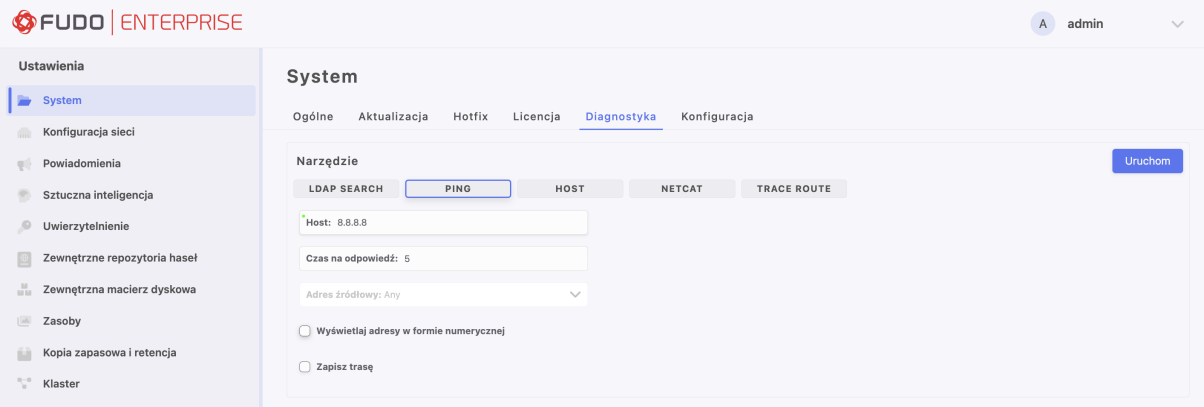


PING

Narzędzie Ping służy do weryfikacji dostępności zdalnego hosta poprzez wysyłanie serii pakietów ICMP.

Poniższa tabela zawiera opcje dostępne do konfiguracji żądania ping.

Polecenie/parametr	Opis
Host	Adres IP lub nazwa hosta zdalnego systemu, który ma zostać sprawdzony.
Czas na odpowiedź	Maksymalny czas oczekiwania na odpowiedź, w sekundach.
Adres źródłowy	Lokalny adres IP, z którego mają być wysyłane pakiety ping.
Wyświetlaj adresy w formie numerycznej	Nie rozwiązuje adresu IP hosta do jego mnemonicznej nazwy.
Zapisz trasę	Umożliwia śledzenie trasy pakietów.

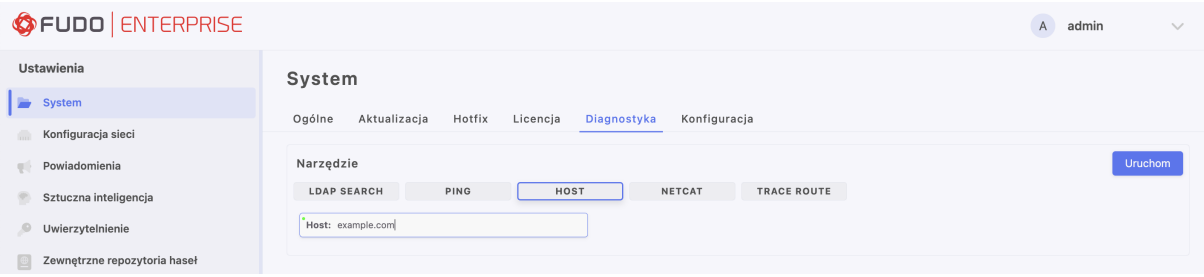


HOST

Narzędzie Host sprawdza, czy serwer DNS prawidłowo rozwiązuje nazwę hosta na odpowiadający jej adres IP.

Poniższa tabela przedstawia szczegóły dostępnego polecenia i jego zastosowanie.

Polecenie/parametr	Opis
Host	W pełni kwalifikowana nazwa domenowa (FQDN), która ma zostać rozwiązana przez DNS.

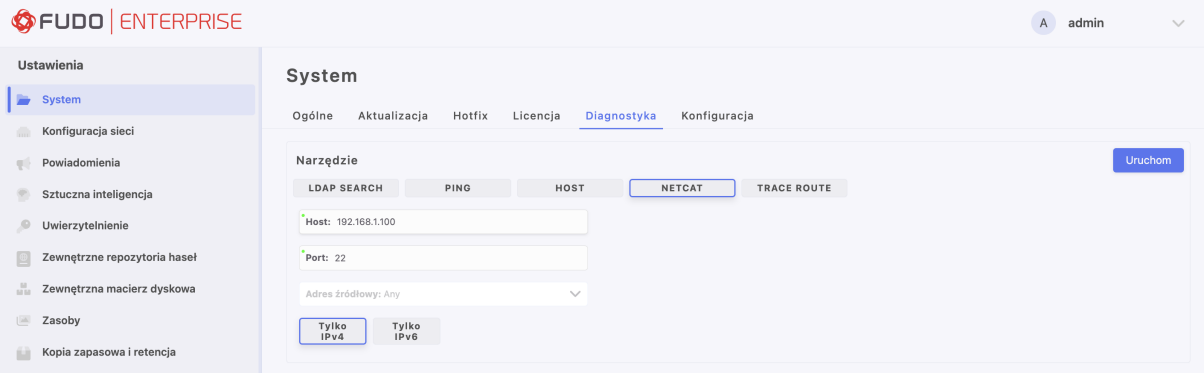


NETCAT

Narzędzie Netcat umożliwia administratorowi nawiązanie połączenia TCP z określonym hostem i portem.

Poniższa tabela przedstawia dostępny parametr wykorzystywany do przeprowadzenia tego testu.

Polecenie/parametr	Opis
Host	Adres IP lub nazwa hosta zdalnego systemu, z którym ma zostać nawiązane połączenie.
Port	Numer portu TCP na zdalnym hoście, który ma zostać przetestowany.

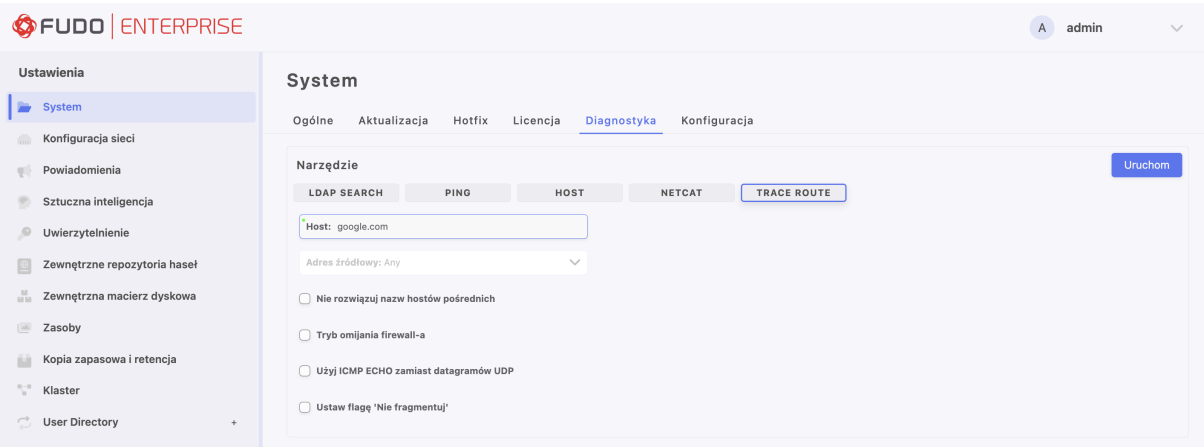


TRACE ROUTE

Narzędzie Trace Route śledzi trasę pakietów sieciowych między Fudo Enterprise a wskazanym hostem.

Poniższa tabela opisuje parametry, które można wykorzystać do dostosowania działania narzędzia.

Polecenie/parametr	Opis
Host	Adres IP lub nazwa hosta docelowego, do którego ma zostać prześledzona trasa pakietów.
Adres źródłowy	Lokalny adres IP, z którego rozpoczynane będzie śledzenie trasy pakietów.
Nie rozwiązuj nazw hostów pośrednich	Kolejne adresy IP przeskoków nie są rozwiązywane do nazw mnemonicznych.
Tryb omijania firewall-a	Wymusza stosowanie tych samych numerów portów dla pakietów UDP i TCP. Docelowy port nie jest zwiększany z każdym wysłanym pakietem.
Użyj ICMP ECHO zamiast datagramów UDP	Wymusza użycie pakietów UDP zamiast ICMP przez `traceroute`.
Ustaw flagę «Nie fragmentuj»	Wyłącza fragmentację pakietu, jeśli przekracza on wartość MTU (Maximum Transmission Unit) określoną dla sieci. Przekroczenie MTU skutkuje błędem.



Powiązane tematy:

- *Rozwiązywanie problemów*

12.1.14 Eksportowanie/importowanie konfiguracji systemu

Fudo Enterprise umożliwia eksport bieżącego stanu systemu, zdefiniowanych obiektów i ustawień konfiguracyjnych, które później można wykorzystać do inicjalizacji systemu.

Ostrzeżenie

Wyeksportowana konfiguracja zawiera informacje poufne.

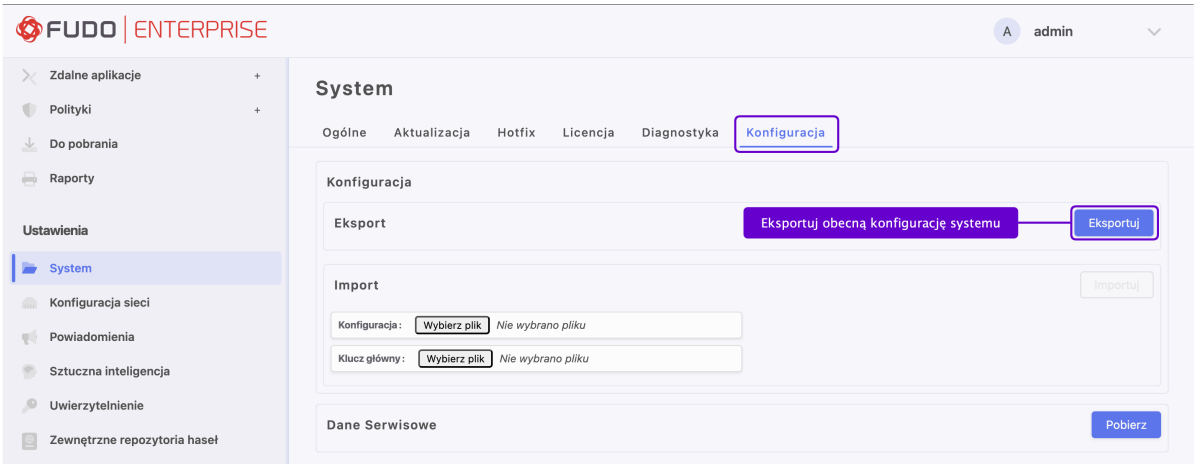
Uwaga

- Opcje importowania i eksportowania konfiguracji dostępne są dla użytkowników o przypisanej roli *superadmin*.
- Eksport/import można wykonać wyłącznie między instancjami Fudo o tym samym numerze seryjnym i wersji.
- W środowisku klastrowym eksport konfiguracji nie jest możliwy.

12.1.14.1 Eksportowanie konfiguracji systemu

Aby wyeksportować konfigurację systemu, wykonaj następujące kroki.

1. Wybierz *Ustawienia* > *System*.
2. Przejdź do zakładki **Konfiguracja**.
3. Kliknij *Eksportuj*, aby rozpocząć pobieranie pliku `.conf`.



12.1.14.2 Importowanie konfiguracji systemu

Ostrzeżenie

Importowanie pliku konfiguracyjnego i inicjalizacja systemu z jego użyciem spowoduje usunięcie wszystkich istniejących danych sesji.

Aby zaimportować plik konfiguracyjny systemu, wykonaj następujące kroki.

1. Znajdź i odszyfruj *Plik klucza głównego* za pomocą *opessl*:

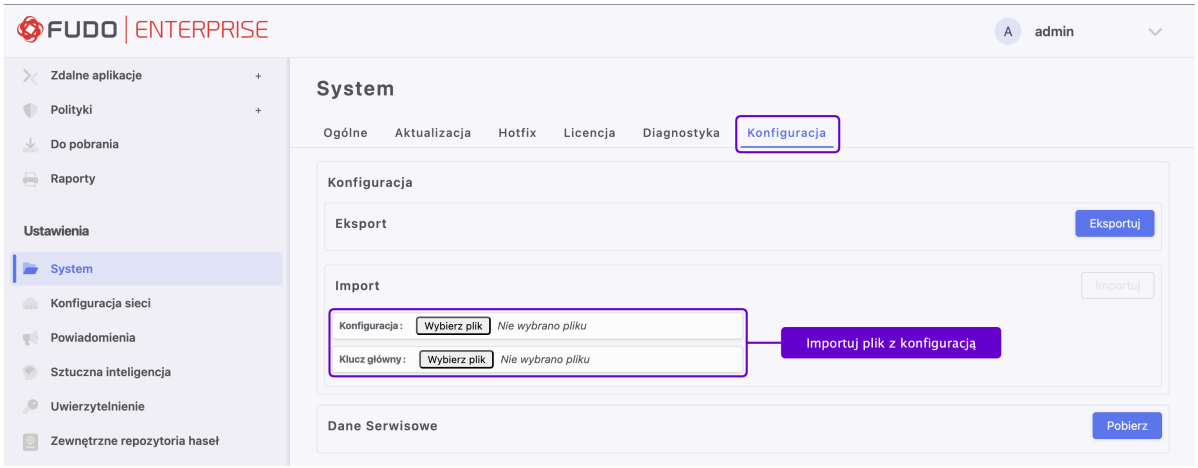
```
openssl smime -decrypt -in path/to/masterkey.pem -inkey privkey.pem -out
masterkey.tar
```

2. Wybierz *Ustawienia* > *System*.
3. Przejdź do zakładki **Konfiguracja**.
4. Kliknij *Wybierz plik* w polu *Klucz główny* i wskaż plik z kluczem głównym.

Uwaga

Klucz główny musi zostać wcześniej odszyfrowany.

5. Kliknij *Wybierz plik* w polu *Konfiguracja* i wskaż plik konfiguracyjny.



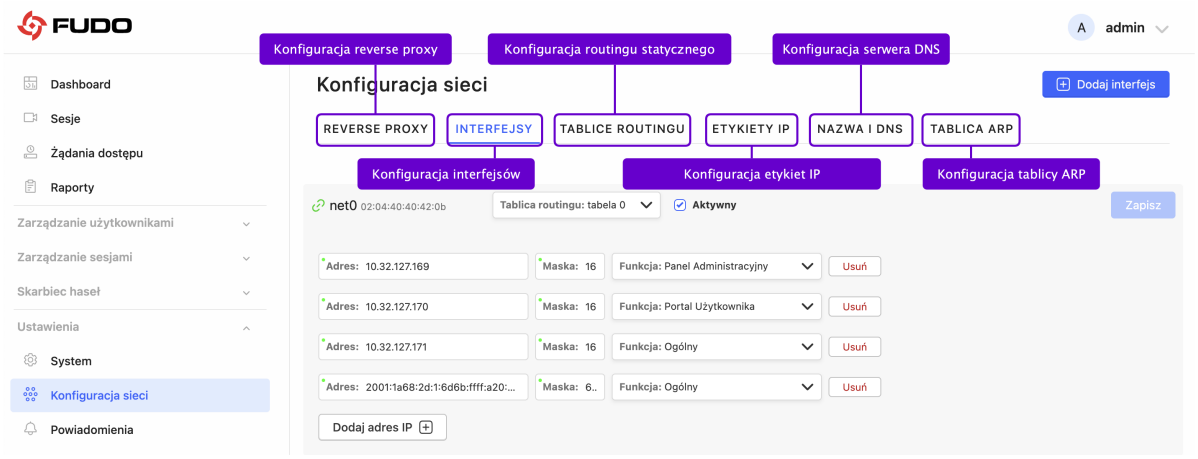
6. Kliknij *Importuj*, aby zainicjować system z zaimportowaną konfiguracją.

Powiązane tematy:

- *Szyfrowanie konfiguracji*
- *Kopia zapasowa danych sesji*
- *Pierwsze uruchomienie*
- *Aktualizacja systemu*

12.2 Konfiguracja sieci

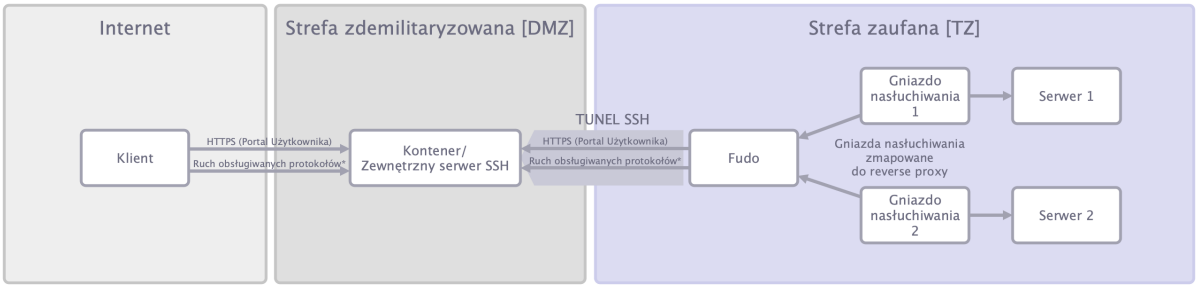
Aby przejść do widoku zarządzania ustawieniami sieci, wybierz z lewego menu opcję *Ustawienia* > *Konfiguracja sieci*.



12.2.1 Reverse Proxy

Funkcja Reverse Proxy umożliwia zestawianie odwróconych tuneli SSH (reverse SSH), które pozwalają na inicjowanie połączeń z kontenera w strefie zdemilitaryzowanej (DMZ) lub z zewnętrznego serwera SSH do zasobów wewnętrznych w obrębie infrastruktury organizacji.

Mechanizm ten polega na nawiązaniu wychodzącego połączenia SSH z serwerem zewnętrznym. Po jego ustanowieniu serwer ten może przekierowywać ruch z powrotem przez utworzony tunel do wewnętrznych gniazd nasłuchiwania działających w infrastrukturze.



*Obsługiwane protokoły: HTTP, Modbus, MS SQL (TDS), MySQL, RDP, SSH, Telnet 3270, Telnet 5250, Telnet, VNC, X11, TCP, Secret Checkout.

Uwaga

Zewnętrzny serwer lub kontener SSH pełni funkcję punktu dostępowego dla użytkowników łączących się przez mechanizm Reverse Proxy. Zamiast nawiązywać bezpośrednie połączenie z systemem Fudo Enterprise, klienci łączą się z tym serwerem zewnętrznym, który następnie przekierowuje ruch przez odwrócony tunel SSH do środowiska wewnętrznego. W praktyce oznacza to, że serwer ten nie jest jedynie hostem pośredniczącym — stanowi on docelowy punkt połączenia dla użytkowników uzyskujących dostęp do zasobów wewnętrznych.

12.2.1.1 Wymagania wstępne

Przed skonfigurowaniem Reverse Proxy należy spełnić następujące wymagania.

- **Zewnętrzny serwer SSH**

  - Serwerem proxy może być urządzenie fizyczne, maszyna wirtualna lub kontener z uruchomioną usługą SSH, która umożliwia przekierowywanie tuneli z wykorzystaniem opcji `-R`.
  - Zewnętrzny serwer SSH musi mieć następującą konfigurację w pliku `sshd_config`: `GatewayPorts clientspecified`. To ustawienie pozwala daemonowi SSH na powiązanie z określonymi adresami zgodnie z żądaniem klienta.

- **Konfiguracja uwierzytelniania**
  - Dodaj klucz publiczny SSH (odpowiadający kluczowi prywatnemu, którego będziesz używać) do pliku `authorized_keys` na zewnętrznym serwerze SSH, aby umożliwić uwierzytelnianie oparte na kluczach.

- **Wymagania sieciowe**
  - Wybierz określony adres źródłowy (Bind IP) IP dla połączenia wychodzącego — etykiety IP i opcja `Any` nie są wspierane.
  - Każda konfiguracja Reverse Proxy musi używać unikalnej kombinacji adresu serwera i portu.

12.2.1.2 Kroki konfiguracji

W poniższym przykładzie przedstawiono konfigurację z użyciem serwera SSH uruchomionego w kontenerze.

Przykład konfiguracji kontenera SSH

Poniższy plik `Dockerfile` definiuje minimalną konfigurację serwera SSH, który może pełnić rolę zewnętrznego serwera SSH do obsługi tunelu Reverse Proxy.

Dockerfile

W przykładzie używana jest wersja Ubuntu 22.04 LTS, ale można użyć dowolnego obrazu bazowego systemu Linux z zainstalowanym serwerem OpenSSH.

```
FROM ubuntu:22.04

RUN apt-get update && apt-get install -y openssh-server \
    && mkdir -p /var/run/sshd

# Utwórz dedykowanego użytkownika
RUN useradd -m reverseproxy && mkdir -p /home/reverseproxy/.ssh \
    && chown -R reverseproxy:reverseproxy /home/reverseproxy/.ssh

# Zaktualizuj konfigurację SSH, aby zezwolić na odwrócone tunele
RUN sed -i 's/#GatewayPorts no/GatewayPorts clientspecified/' /etc/ssh/sshd_
↪config

# (Opcjonalnie) Wyłącz uwierzytelnianie hasłem dla bezpieczeństwa
RUN sed -i 's/#PasswordAuthentication yes/PasswordAuthentication no/' /etc/ssh/
↪sshd_config
```

(ciąg dalszy na następnej stronie)

(kontynuacja poprzedniej strony)

```
EXPOSE 22

CMD ["/usr/sbin/sshd", "-D"]
```

Zbuduj kontener

```
docker build -t external-ssh-server .
```

Uruchom kontener

Opublikuj port 22 kontenera na hoście. Można użyć dowolnego portu po stronie hosta. Ze względów bezpieczeństwa zaleca się użycie niestandardowego portu (np. 2222) jako podstawowego mechanizmu ograniczającego automatyczne próby skanowania.

```
docker run -d -p 2222:22 --name external-ssh external-ssh-server
```

Skonfiguruj uwierzytelnianie oparte na kluczach

Uwaga

Klucz publiczny wymagany do uwierzytelniania na zewnętrznym serwerze SSH można uzyskać bezpośrednio z konfiguracji Reverse Proxy w Fudo Enterprise.

Po uruchomieniu kontenera dodaj klucz publiczny SSH, który będzie używany przez mechanizm Reverse Proxy, do pliku `authorized_keys` użytkownika przeznaczonego do zestawiania tunelu.

```
docker exec -it external-ssh bash
```

Po zalogowaniu się do kontenera wykonaj poniższe polecenia:

```
su - reverseproxy
echo "TWÓJ_KLUCZ_PUBLICZNY" > ~/.ssh/authorized_keys
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```

Sprawdź konfigurację

Aby zweryfikować, czy zewnętrzny serwer SSH akceptuje uwierzytelnianie kluczem oraz obsługuje odwrócone połączenia SSH, można przeprowadzić test ręczny z dowolnego hosta, który będzie inicjował tunel (np. z hosta Reverse Proxy).

- Uwierzytelnianie kluczem SSH

  ```
  ssh -i private_key reverseproxy@<adres-ip-serwera> -p 2222 true
  ```

- Odwrócone przekazywanie portów

  ```
  ssh -i private_key -R 0.0.0.0:8080:localhost:80  reverseproxy@<adres-
  ↪ip-serwera> -p 2222
  ```

- Jeśli test zakończy się powodzeniem, kontener jest gotowy do użycia jako zewnętrzny serwer SSH dla Reverse Proxy.

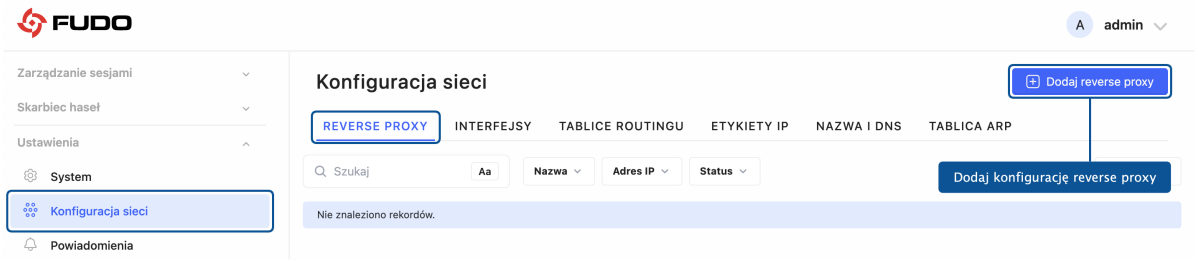
Uwaga

Jeśli para kluczy została wygenerowana w Fudo Enterprise, upewnij się, że klucz prywatny został pobrany i przechowywany bezpiecznie przed przeprowadzeniem tego testu.

Jeśli brakuje klucza prywatnego, uwierzytelnianie nie powiedzie się. W takim przypadku wygeneruj nową parę kluczy lub prześlij własny klucz publiczny do Fudo Enterprise.

Kroki konfiguracji w Fudo Enterprise

1. Wybierz *Ustawienia* > *Konfiguracja sieci*.
2. Otwórz kartę *Reverse Proxy*.
3. Kliknij *+ Dodaj Reverse Proxy*.



ZAKŁADKA USTAWIENIA

Uwaga

Zakładka Ustawienia konfiguruje parametry połączenia SSH i określa, czy Portal Użytkownika (UAG) jest przekazywany przez to połączenie.

1. W polu **Nazwa** wprowadź opisową nazwę dla tej konfiguracji Reverse Proxy, na przykład `Reverse Proxy - DMZ` lub `Tunel SSH do serwera raportowania`.
2. W polu **Adres IP** podaj nazwę hosta lub adres IP zewnętrznego serwera SSH, z którym Fudo Enterprise powinno się połączyć.
3. W polu **Port** wprowadź numer portu SSH na zewnętrznym serwerze. Zazwyczaj jest to port 22, chyba że serwer używa portu niestandardowego.
4. W polu **Login** wprowadź nazwę użytkownika SSH używaną na zewnętrznym serwerze (np. `Fudo`, `tunnel`, `proxyuser`).
5. W polu **Klucz prywatny** wklej klucz prywatny używany do uwierzytelniania na zewnętrznym serwerze SSH.

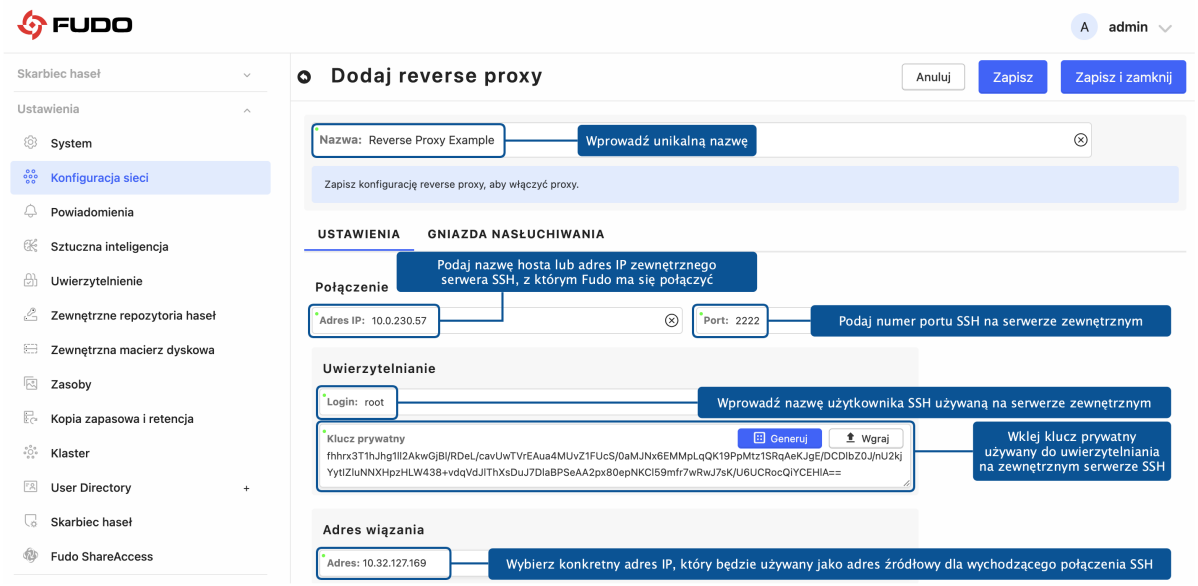
   Uwaga

   Pamiętaj, że obsługiwane jest **tylko uwierzytelnianie oparte na kluczach** — uwierzytelnianie hasłem nie jest dostępne.

6. W polu **Adres wiązania** wybierz adres IP, który będzie używany jako adres źródłowy (Bind IP) dla wychodzącego połączenia SSH.

Uwaga

Etykiety IP oraz opcja *Any* nie są obsługiwane. Wybrany adres IP określa, który węzeł nawiązuje połączenie SSH.



7. W sekcji **Weryfikacja serwera** wybierz opcję **Klucz publiczny** (zalecane) i wklej klucz publiczny SSH zewnętrznego serwera w pole **Klucz publiczny serwera**.

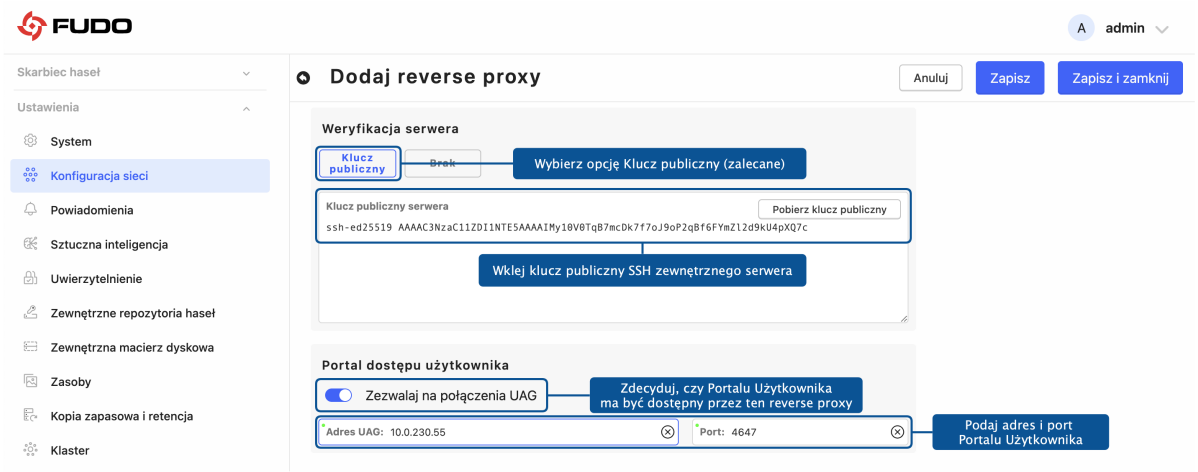
Uwaga

Chociaż jest to pole opcjonalne, zdecydowanie zaleca się podanie klucza. Jeśli pole zostanie pozostawione puste, klucz będzie pobierany automatycznie przy każdej próbie nawiązania tunelu. Ręczne podanie klucza jest zalecane, ponieważ zmniejsza ryzyko ataków typu *man-in-the-middle* i zapewnia, że łączysz się z oczekiwanym serwerem.

8. W sekcji **Portal dostępu użytkownika** zdecyduj, czy Portal Użytkownika (UAG) powinien być dostępny przez tą konfigurację Reverse Proxy.

   Jeśli włączysz opcję **Zezwalaj na połączenia UAG** dla tej konfiguracji, użytkownicy łączący się przez ten tunel otrzymają przefiltrowany widok zasobów na podstawie przypisanych im uprawnień.

   Gdy dostęp do Portalu Użytkownika jest włączony, podaj adres i port Portalu Użytkownika.



Uwaga

Jeśli Portal Użytkownika (UAG) jest udostępniany przez Reverse Proxy pod inną nazwą hosta lub adresem IP, certyfikat TLS używany przez Portalu Użytkownika musi zawierać wszystkie te adresy. W przeciwnym razie walidacja TLS nie powiedzie się, a połączenia zostaną odrzucone.

ZAKŁADKA GNIAZDA NASŁUCHIWANIA

1. Przejdź do karty **GNIAZDA NASŁUCHIWANIA**.

   Uwaga

   Zakładka Gniazda Nasłuchiwania pozwala na mapowanie wewnętrznych gniazd nasłuchiwania na zdalne porty na zewnętrznym serwerze SSH, tworząc tunele, które przekazują ruch ze zdalnego serwera z powrotem do wewnętrznych zasobów.

2. Kliknij Dodaj gniazdo nasłuchiwania aby utworzyć mapowanie.
3. Z listy rozwijanej **Gniazdo nasłuchiwania** wybierz gniazdo nasłuchiwania Fudo Enterprise (identyfikowany przez jego IP i port), który będzie odbierał ruch tunelowany.
4. W polu **Adres** określ adres IP na zewnętrznym serwerze, który będzie akceptował połączenia przychodzące.
5. W polu **Port** określ port na zewnętrznym serwerze, który będzie akceptował połączenia przychodzące. Ten port musi być unikalny w ramach tej konfiguracji Reverse Proxy.



Uwaga

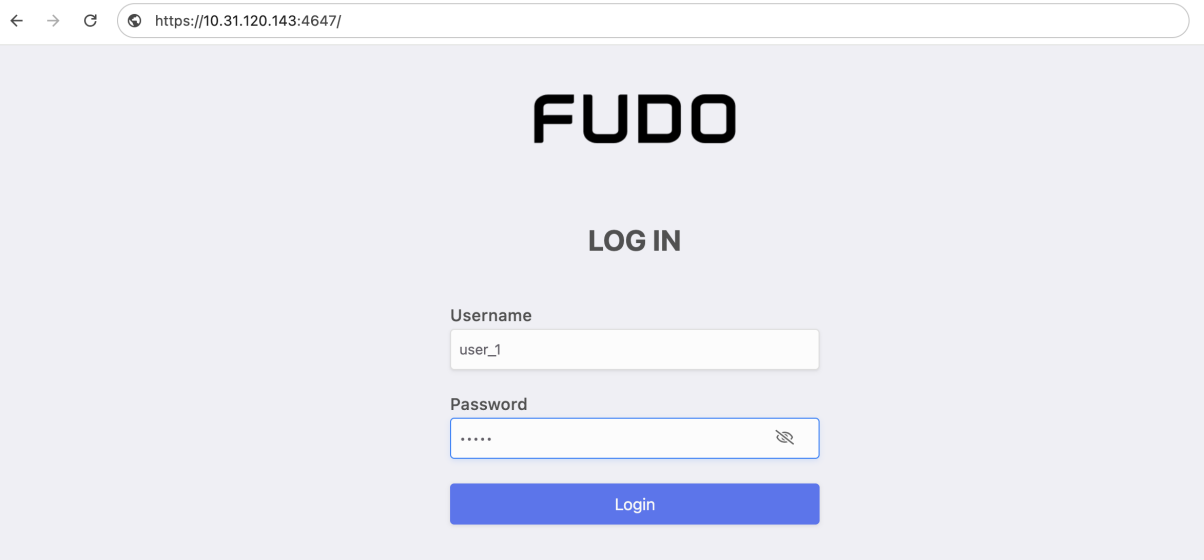
Ważne ograniczenia:

- **Przypisanie węzła** - Adres IP gniazda nasłuchiwania musi pochodzić z tego samego węzła co adres źródłowy (Bind IP) skonfigurowany w karcie Ustawienia. Tunele Reverse Proxy działają na pojedynczym węźle, więc wychodzące połączenie SSH i wewnętrzne gniazdo nasłuchiwania muszą znajdować się na tym samym węźle.
- **Wyjątek gniazda nasłuchiwania Any** - Jeśli gniazdo nasłuchiwania jest skonfigurowane z opcją *Any*, będzie akceptowało ruch dla węzła, na którym znajduje się adres źródłowy (Bind IP).
- **Unikatowość zdalnego portu** - Każdy zdalny port musi być unikalny dla danego adresu Reverse Proxy. Nie można mapować wielu gniazd nasłuchiwania na ten sam zdalny port na tym samym zewnętrznym serwerze.

12.2.1.3 Połączenia Portalu Użytkownika

Dostęp do Portalu Użytkownika

Aby uzyskać dostęp do Portalu Użytkownika przez połączenie Reverse Proxy, wprowadź adres IP i port określone w konfiguracji Reverse Proxy pod przełącznikiem **Zezwalaj na połączenia UAG**. Użyj tych wartości bezpośrednio w przeglądarce. Na przykład, jak pokazano na rysunku 3, jeśli konfiguracja wymienia adres jako 10.0.230.55 i port jako 4647, uzyskasz dostęp do UAG, przechodząc do: `http://10.0.230.55:4647/`.



Widoczność zasobów przez Portalu Użytkownika

Użytkownicy uzyskujący dostęp do Portalu Użytkownika za pośrednictwem połączenia Reverse Proxy widzą przefiltrowaną listę zasobów, a nie pełen katalog dostępnych zasobów. W praktyce oznacza to, że użytkownikom prezentowane są wyłącznie zasoby powiązane z dowolnie skonfigurowanym mechanizmem Reverse Proxy w systemie — nie tylko z tym, przez który zostało nawiązane bieżące połączenie.

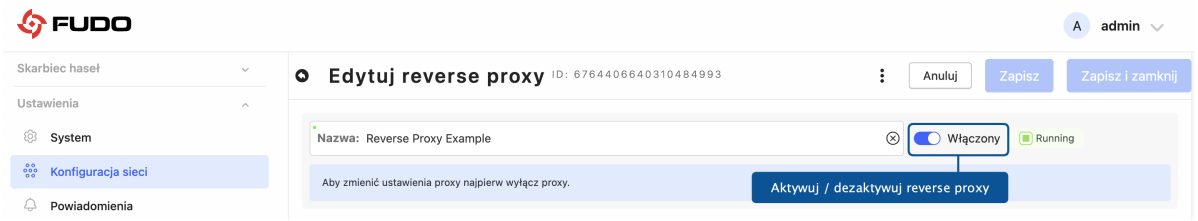
Co kwalifikuje się jako zasób przekazywany przez proxy

Zasób jest traktowany jako udostępniany przez Reverse Proxy i będzie widoczny w UAG, jeśli spełnia co najmniej jedno z poniższych kryteriów:

- **Mapowane gniazda nasłuchiwania** — każde gniazdo nasłuchiwania przypisane w zakładce *Gniazda nasłuchiwania* w dowolnej konfiguracji Reverse Proxy.
- **Konta korzystające z mapowanych gniazd nasłuchiwania** — każde konto skonfigurowane do używania gniazda nasłuchiwania, które zostało przypisane w dowolnej konfiguracji Reverse Proxy.
- **Gniazdo nasłuchiwania WebClient dla kont proxowanych** — jeżeli konto korzysta z gniazda nasłuchiwania objętego konfiguracją Reverse Proxy, wszystkie gniazda nasłuchiwania WebClient powiązane z tym kontem są również traktowane jako zasoby proxowane.

12.2.1.4 Włączanie i wyłączanie Reverse Proxy

Każda konfiguracja Reverse Proxy zawiera przełącznik włącz/wyłącz, który określa, czy tunel jest aktywny. Zmiana ustawienia tego przełącznika jest stosowana natychmiast i nie wymaga zapisywania konfiguracji.



Gdy Reverse Proxy jest wyłączony:

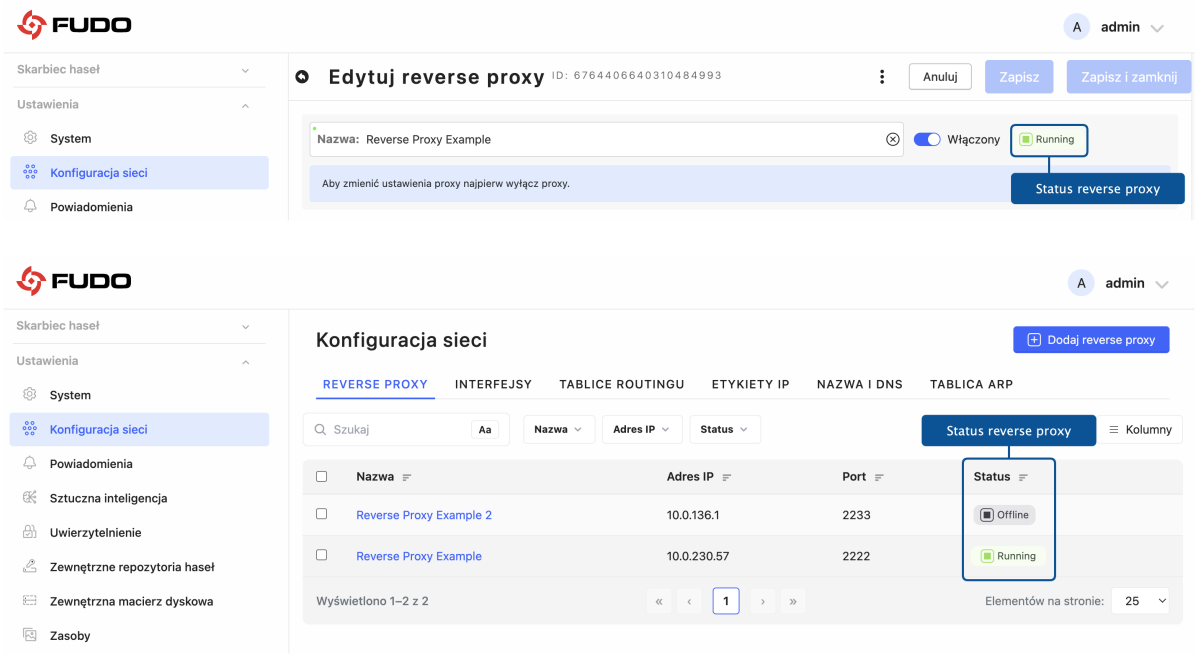
- Wszystkie pola konfiguracji są edytowalne, w tym ustawienia połączenia.
- Tunel nie jest zestawiany.
- Nawiązywanie połączeń przez tę konfigurację Reverse Proxy nie jest możliwe.

Gdy Reverse Proxy jest włączony:

- Możliwa jest wyłącznie modyfikacja ustawień proxy Portalu Użytkownika.
- Ustawienia połączenia (Host, Port, Login, Klucz prywatny, Klucz publiczny serwera, Adres źródłowy) są zablokowane i nie mogą być zmieniane.
- Można dodawać, edytować oraz usuwać mapowania gniazd nasłuchiwania.

12.2.1.5 Wskaźniki stanu Reverse Proxy

Stan Reverse Proxy można sprawdzić na liście dostępnej w *Ustawienia* > *Konfiguracja sieci* > *Reverse Proxy* lub w formularzu edycji wybranej konfiguracji Reverse Proxy.



Reverse Proxy może prezentować jeden z czterech następujących stanów:

Tabela 4: Wartości stanu Reverse Proxy

Status	Opis
Offline	Reverse Proxy jest wyłączony. Tunel nie jest zestawiony i nawiązywanie połączeń nie jest możliwe.
Niedostępny	Reverse Proxy jest włączony, ale tunel nie działa. Połączenie SSH nie zostało zestawione lub zostało przerwane. Sprawdź Dziennik zdarzeń w celu identyfikacji błędów połączenia.
Ograniczona funkcjonalność	Reverse Proxy jest włączony i tunel jest zestawiony, jednak co najmniej jedno mapowanie gniazda nasłuchiwania nie działa prawidłowo. Tunel działa częściowo, a niektóre usługi mogą być niedostępne. Sprawdź Dziennik zdarzeń oraz zweryfikuj konfigurację gniazd nasłuchiwania.
Uruchomiony	Reverse Proxy jest włączony, tunel jest zestawiony, a wszystkie mapowania gniazd nasłuchiwania działają prawidłowo. Konfiguracja jest w pełni operacyjna.

12.2.1.6 Działanie tunelu SSH

Proces zestawiania tunelu

Po włączeniu Reverse Proxy proces zestawiania tunelu odbywa się asynchronicznie w tle:

1. Interfejs API zwraca odpowiedź natychmiast po przełączeniu opcji włącz/wyłącz.
2. Dedykowana usługa działająca w tle realizuje faktyczne zestawienie połączenia SSH.
3. W trakcie zestawiania tunelu status zmienia się kolejno z **Offline** → **Niedostępny** → **Ograniczona funkcjonalność** lub **Uruchomiony**, w zależności od wyniku próby nawiązania połączenia i konfiguracji mapowań.
4. Wszelkie problemy występujące podczas zestawiania tunelu (błędy uwierzytelniania, problemy sieciowe, nieprawidłowe mapowania) są rejestrowane w Dzienniku zdarzeń.

Ważne

Jeśli status ma wartość **Niedostępny** lub **Ograniczona funkcjonalność**, należy sprawdzić Dziennik zdarzeń w celu zdiagnozowania problemów z połączeniem lub mapowaniami.

Zachowanie tuneli SSH

Usunięcie mapowania gniazda nasłuchiwania lub wyłączenie opcji *Zezwalaj na połączenia UAG* **nie powoduje zamknięcia aktywnego tunelu SSH**. W rezultacie istniejące połączenia zestawione przy użyciu tego mapowania **pozostają aktywne**. Blokowane są wyłącznie **nowe połączenia**.

Takie działanie wynika z mechanizmu funkcjonowania tuneli SSH — jeśli wiele mapowań korzysta z jednego połączenia SSH, tunel pozostaje aktywny tak długo, jak długo otwarta jest sesja SSH, niezależnie od usunięcia poszczególnych mapowań.

Jeżeli administrator musi wymusić zakończenie wszystkich aktywnych połączeń powiązanych z danym tunelem, może ręcznie **wyłączyć Reverse Proxy** — przed lub po usunięciu mapowania. Wyłączenie Reverse Proxy powoduje zamknięcie całego tunelu SSH i natychmiastowe przerwanie wszystkich aktywnych połączeń.

12.2.1.7 Rekomendowany przebieg konfiguracji

1. Skonfiguruj wszystkie ustawienia połączenia, gdy Reverse Proxy jest wyłączony.
2. Dodaj mapowania gniazd nasłuchiwania dla zasobów, które mają być udostępnione.
3. Włącz Reverse Proxy za pomocą przełącznika **włącz/wyłącz**.
4. Monitoruj zmianę statusu rozpoczynającą się od wartości **Offline**.
5. Jeżeli w rozsądnym czasie status nie zmieni się na **Running**, sprawdź Dziennik zdarzeń.
6. Testuj połączenia dopiero po uzyskaniu statusu **Running**.
7. W razie potrzeby wprowadź zmiany w ustawieniach dla Portalu Użytkownika lub mapowaniach gniazd nasłuchiwania. Uwaga: zmiana ustawień połączenia wymaga wcześniejszego wyłączenia Reverse Proxy.

12.2.1.8 Zachowanie routingu wewnętrznego

Połączenia przychodzące przez Reverse Proxy są kierowane do zasobów wewnętrznych z wykorzystaniem adresu `127.0.9.1` w następujących przypadkach:

- Gniazda nasłuchiwania skonfigurowane z wartością *Any* jako adres nasłuchu.
- Połączenia realizowane przez User Portal Użytkownika (UAG).

W Dzienniku zdarzeń każde połączenie pochodzące z adresu `127.0.9.1` oznacza ruch przekazany przez tunel Reverse Proxy.

12.2.1.9 Względy bezpieczeństwa

12.2.1.10 Zagadnienia bezpieczeństwa

- Zawsze wprowadzaj **Server SSH Public Key** ręcznie, zamiast polegać na automatycznym pobieraniu klucza podczas nawiązywania połączenia. Zapewnia to zestawienie połączenia z właściwym serwerem i ogranicza ryzyko ataku typu man-in-the-middle.
- Ogranicz dostęp do klucza prywatnego — przechowuj go w bezpieczny sposób i kontroluj, kto ma możliwość jego podglądu.
- Stosuj konkretne adresy źródłowe (Bind IP), aby zapewnić jednoznaczną identyfikację w logach, który węzeł zestawia dane połączenie.
- Monitoruj Dziennik zdarzeń pod kątem połączeń z adresu `127.0.9.1`, aby śledzić wykorzystanie Reverse Proxy.
- Regularnie przeglądaj mapowania gniazd nasłuchiwania, aby upewnić się, że udostępniane są wyłącznie niezbędne usługi.

12.2.1.11 Rozwiązywanie problemów

Poniższe wskazówki pomagają zidentyfikować i rozwiązać najczęstsze problemy występujące podczas pracy z konfiguracją Reverse Proxy.

Tabela 5: Przewodnik rozwiązywania problemów

Problem	Możliwe rozwiązanie
Nie można zestawić połączenia	• Zweryfikuj, czy na serwerze zewnętrznym w pliku `sshd_config` ustawiono parametr `GatewayPorts clientspecified`. • Upewnij się, że klucz publiczny został dodany do pliku `authorized_keys` na serwerze zewnętrznym. • Sprawdź łączność sieciową z adresu Bind IP do serwera zewnętrznego.
Mapowanie gniazda nasłuchiwania nie działa	• Upewnij się, że adres IP gniazda nasłuchiwania należy do tego samego węzła co Bind IP. • Zweryfikuj, czy port zdalny jest unikalny w ramach tej konfiguracji Reverse Proxy. • Sprawdź, czy gniazdo nasłuchiwania jest aktywne i przyjmuje połączenia.
Portal Użytkownika nie jest dostępny przez tunel	• Sprawdź, czy mapowanie gniazda nasłuchiwania z wartością **Any** jest poprawnie skonfigurowane. • Przeanalizuj wpisy w Dzienniku zdarzeń dotyczące adresu `127.0.9.1`, aby potwierdzić, że ruch dociera do systemu.

Powiązane tematy:

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

12.2.2 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).

12.2.2.1 Zarządzanie interfejsami fizycznymi

Definiowanie adresu IP interfejsu

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

Aby zdefiniować adres IP fizycznego interfejsu sieciowego, wykonaj następujące kroki.

1. Wybierz *Ustawienia* > *Konfiguracja sieci*.

2. Kliknij *Dodaj adres IP +* i podaj adres IP oraz maskę podsieci w formacie CIDR.
3. Wybierz funkcję adresu IP:
   - **Ogólny** – Wirtualny adres IP, który zostanie automatycznie przejęty przez drugi węzeł klastra w przypadku awarii węzła głównego.

     Uwaga

     Klastrowy adres IP należy dodać na każdym węźle klastra i aktywować dla niego funkcję *Ogólny*.

   - **Panel Administracyjny** – Włącz dostęp do Panelu Administracyjnego na wskazanym adresie IP. Adres IP Panelu Administracyjnego jest również wykorzystywany do replikacji danych między węzłami klastra oraz do *dostępu przez protokół SSH*.

     Uwaga

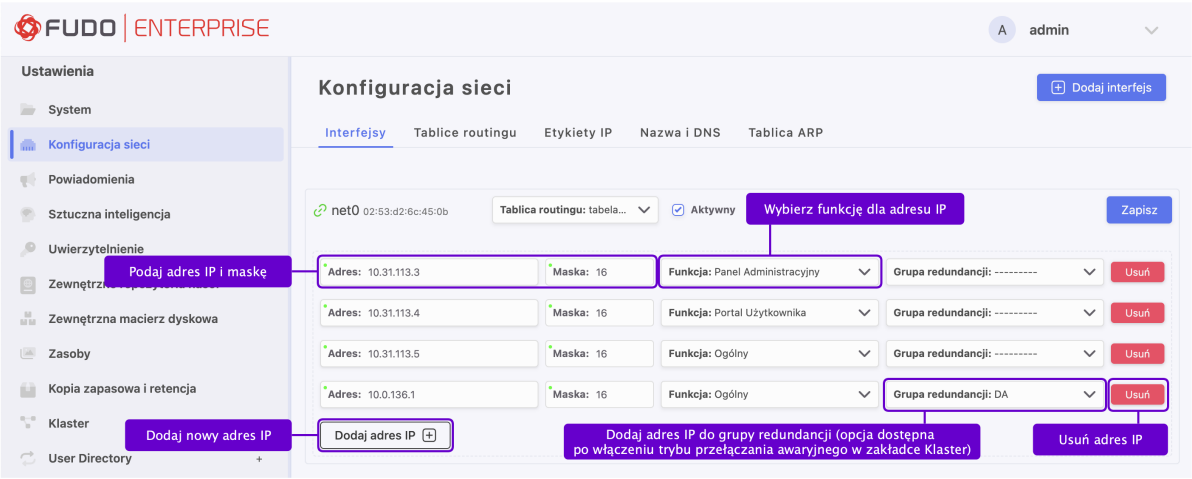
     Domyślny numer portu dla dostępu do usług przez protokół SSH to 65522.

   - **Portal Użytkownika** – Włącz dostęp do Portalu Użytkownika na wskazanym adresie IP.
4. Wybierz grupę redundancji, do której zostanie przypisany adres IP *(dotyczy adresów klastrowych)*.

Uwaga

Grupy redundancji definiowane są w widoku *Klaster*, w zakładce *Grupy redundancji*. Aby dowiedzieć się więcej, przeczytaj rozdział:ref:*main-cluster_ redundancy_ groups*.

5. Kliknij *Zapisz*.



Uwaga

Obecny status każdego interfejsu jest reprezentowany za pomocą ikony:

	Interfejs aktywny i podłączony.
	Interfejs aktywny, ale niepodłączony.
	Interfejs wyłączony.

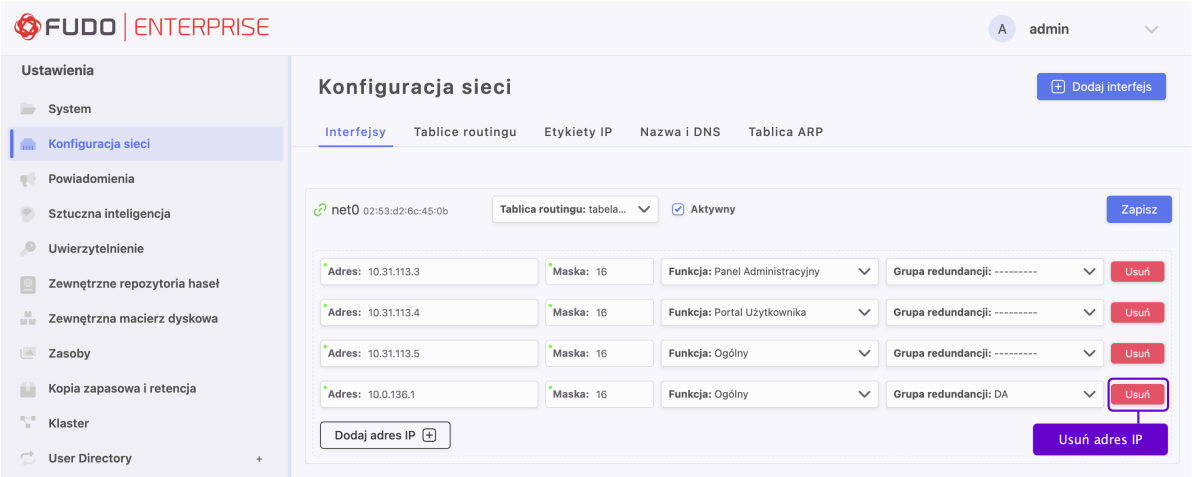
Usuwanie przypisanych adresów IP interfejsu

Ostrzeżenie

Usunięcie adresu IP uniemożliwi nawiązywanie połączeń z serwerami, które ten adres skonfigurowany w polu *Adres lokalny* w sekcji *proxy*.

Aby usunąć adres IP przypisany do fizycznego interfejsu sieciowego, wykonaj następujące kroki.

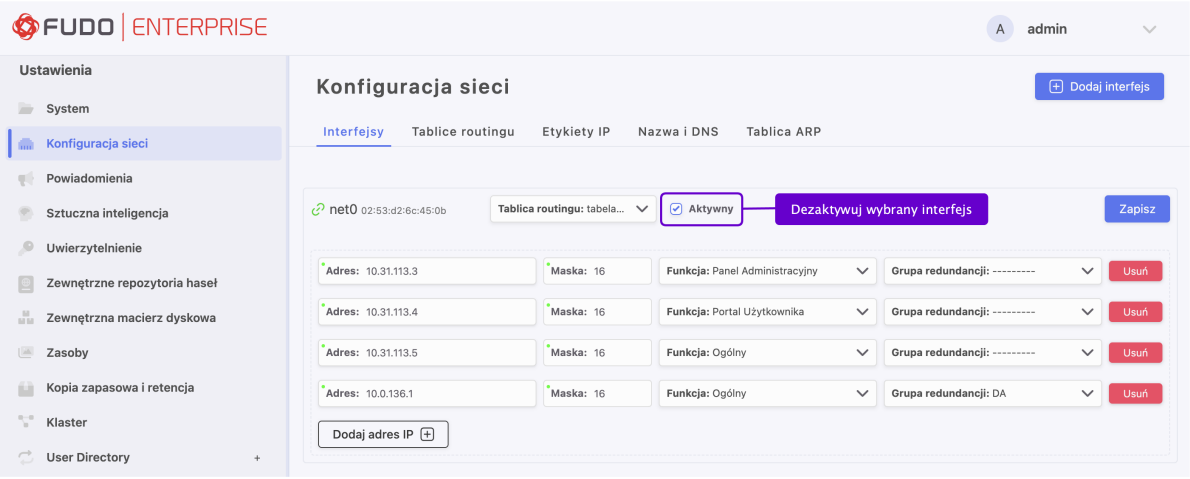
1. Wybierz *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij przycisk *Usuń* przy wybranym adresie IP.
3. Kliknij *Potwierdź*.



Wyłączanie interfejsu sieciowego

Aby wyłączyć adres IP przypisany do fizycznego interfejsu sieciowego, wykonaj następujące kroki.

1. Wybierz *Ustawienia* > *Konfiguracja sieci*.
2. Odznacz opcję *Aktywny* przy danym interfejsie, aby go wyłączyć.



3. Kliknij *Zapisz*.

12.2.2.2 Definiowanie adresu IP z poziomu konsoli systemowej

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

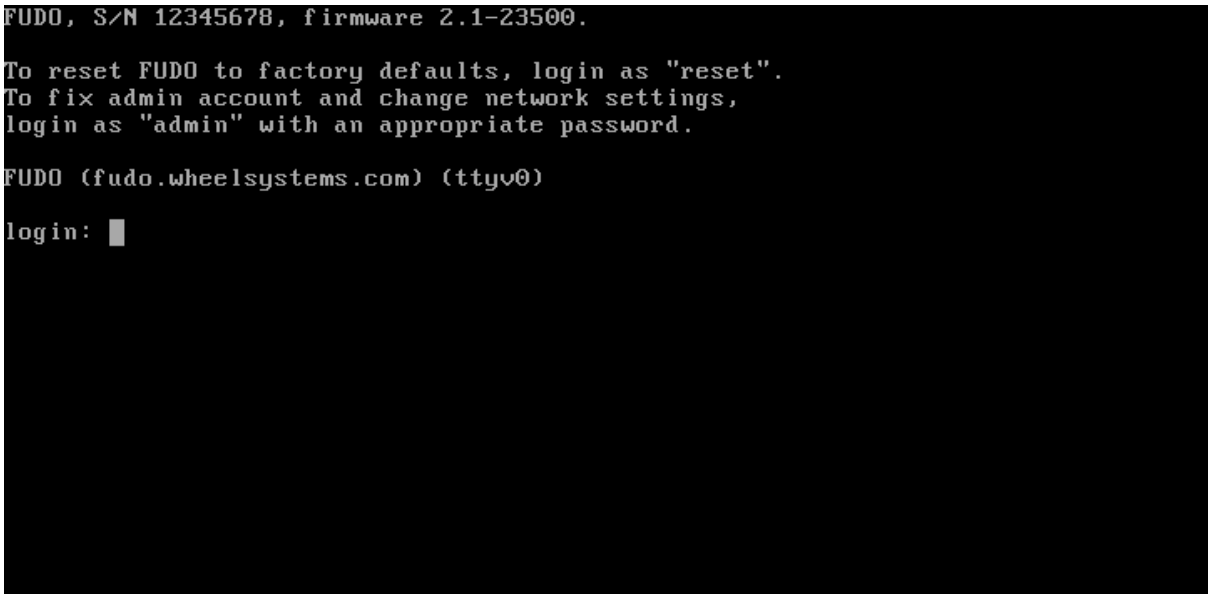
1. Podłącz do urządzenia monitor i klawiaturę.
2. Wprowadź login konta administratora.

Uwaga

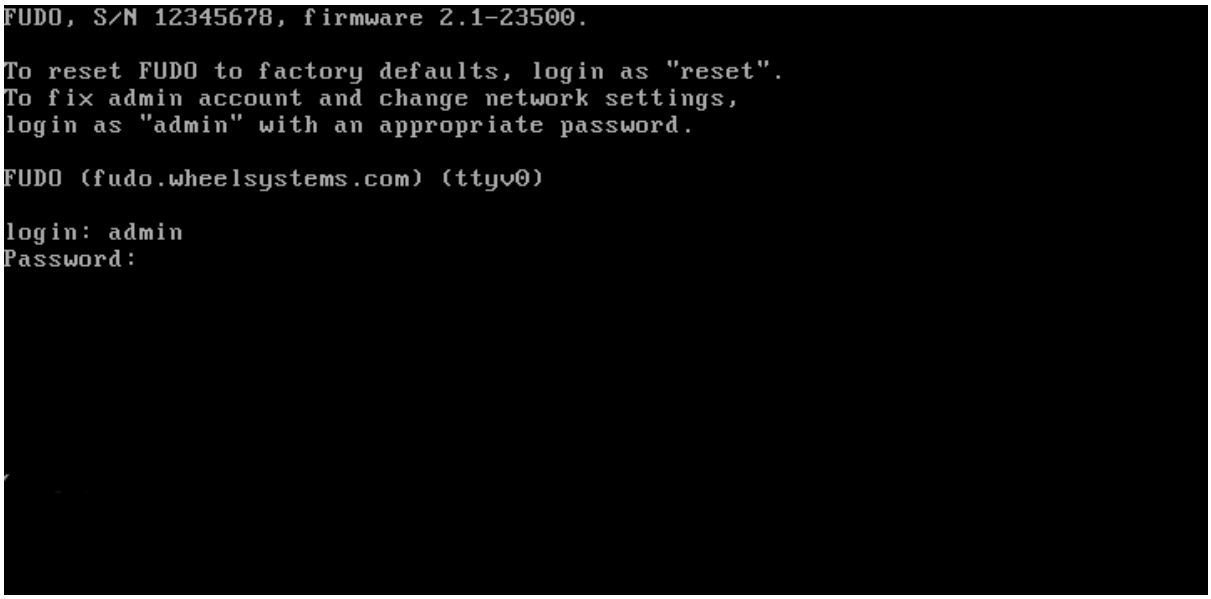
Domyślne dane logowania:

login: admin
hasło: proxycrypto

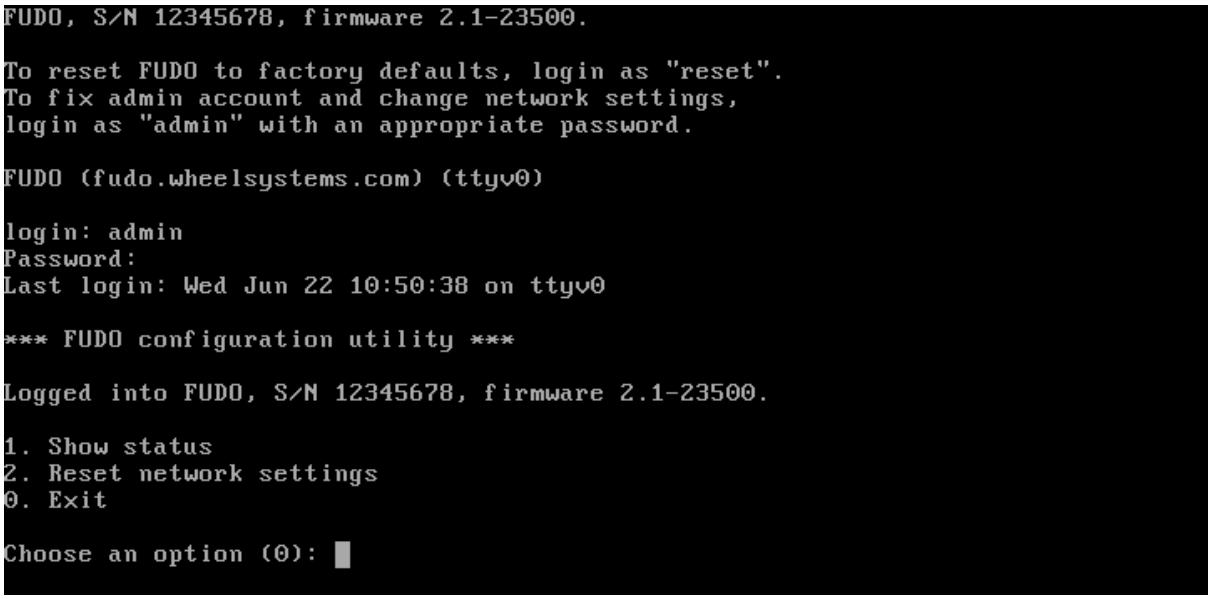
Dla wersji w chmurze domyślnym hasłem jest zazwyczaj identyfikator maszyny wirtualnej dostarczanej z Fudo Enterprise. Skontaktuj się ze sprzedawcą lub wsparciem technicznym, aby dowiedzieć się więcej.



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

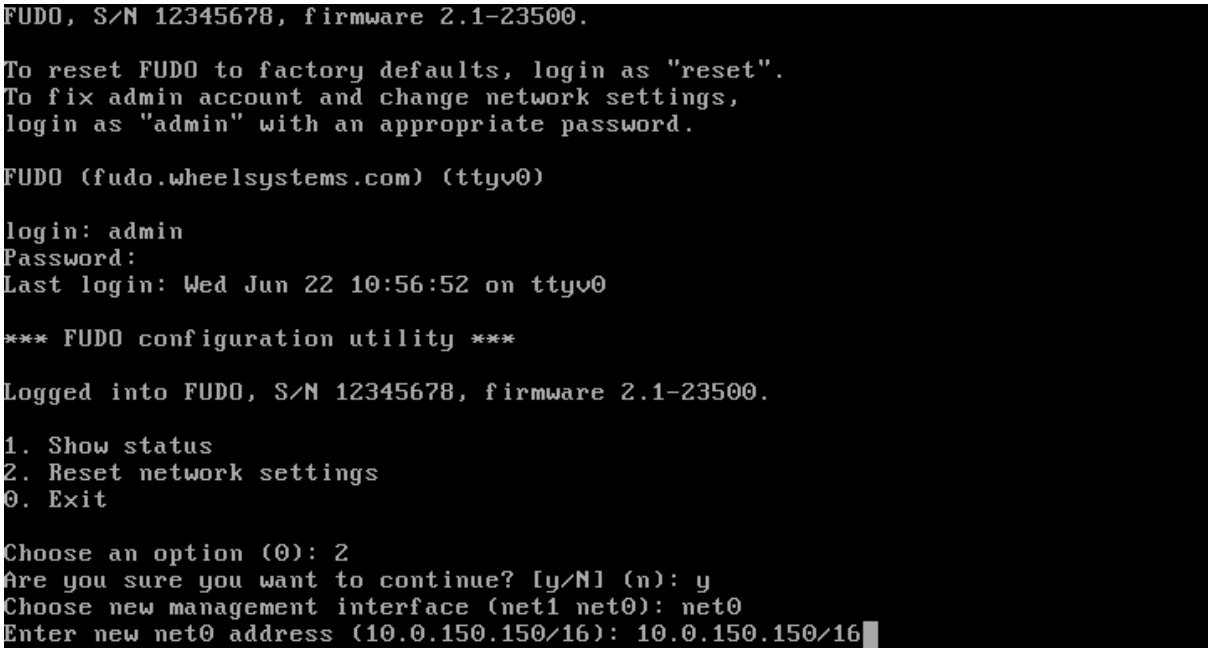
*** FUDO configuration utility ***

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

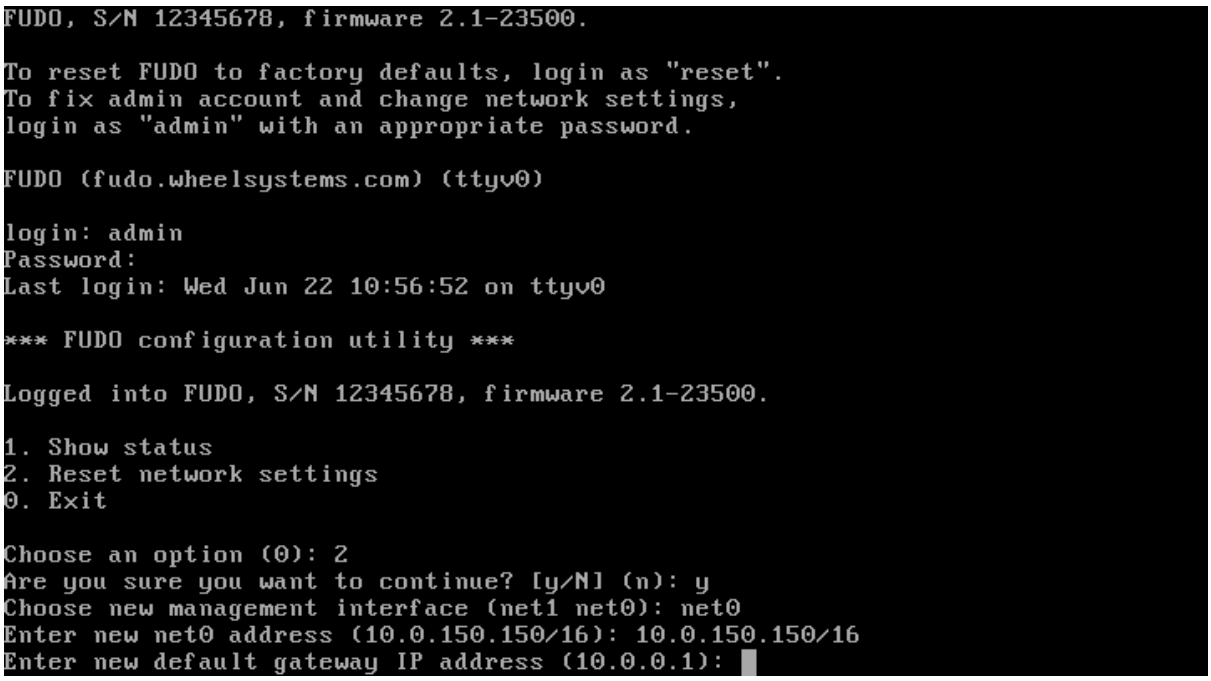
1. Show status
2. Reset network settings
0. Exit

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*.



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



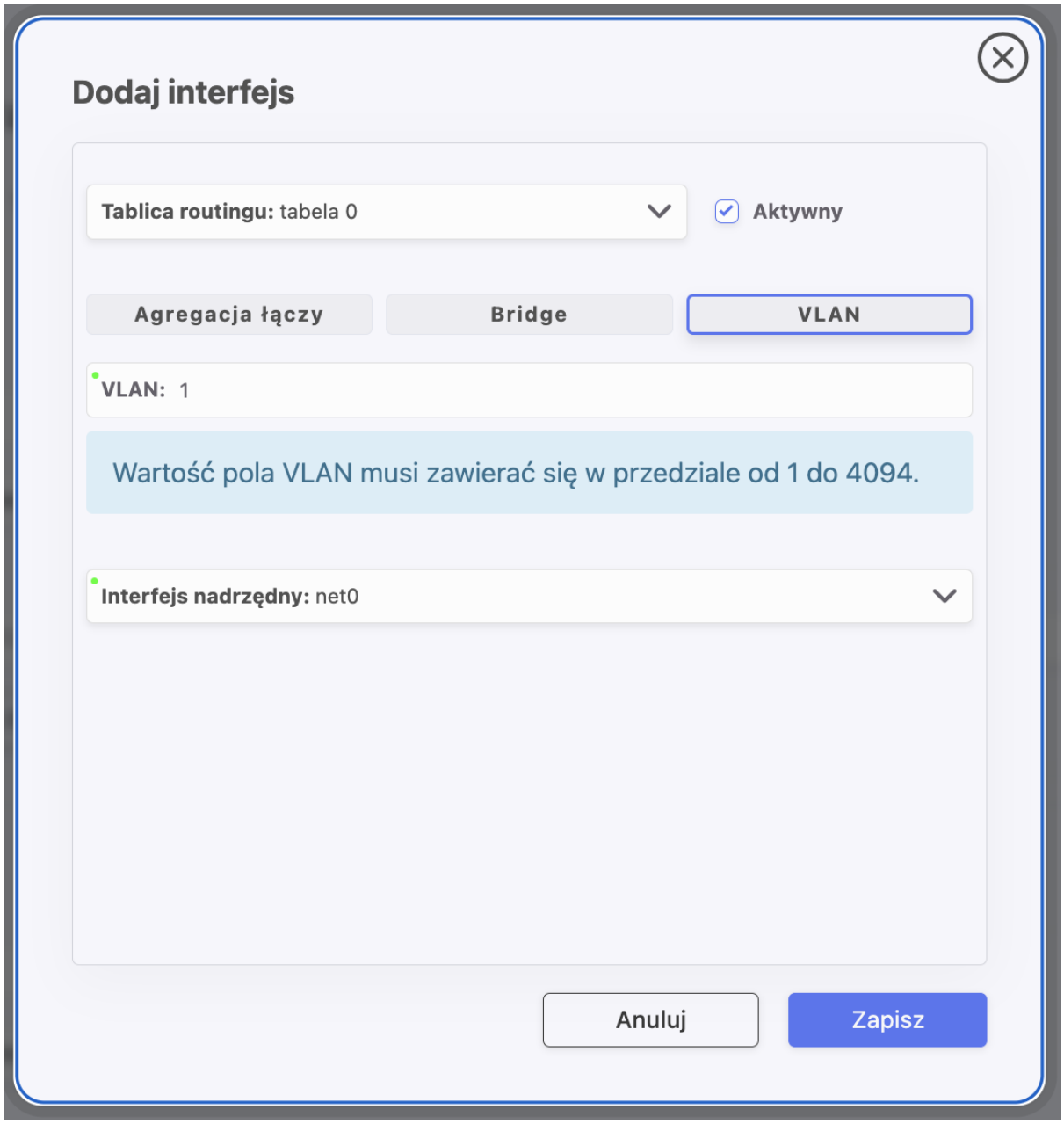
12.2.2.3 Konfiguracja sieci wirtualnych (VLAN)

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

Aby skonfigurować Fudo Enterprise do pracy w sieci VLAN, wykonaj następujące kroki.

1. Wybierz *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij *+ Dodaj interfejs*.
3. W oknie dialogowym kliknij przycisk *VLAN*.
4. Określ *VLAN ID* i wybierz fizyczny *Interfejs nadrzędny*. *VLAN ID* musi być liczbą z zakresu od 1 do 4094.

5. Kliknij *Zapisz*, aby dodać konfigurację VLAN.

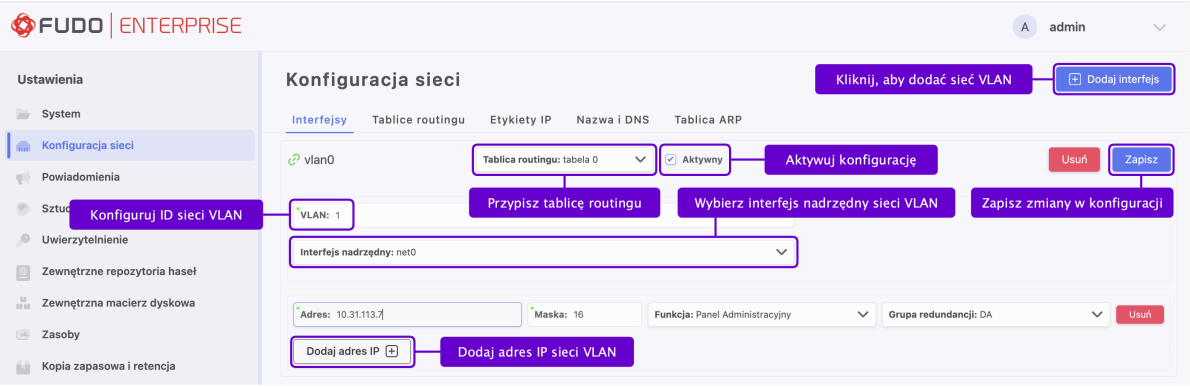


6. Nowy VLAN pojawi się w zakładce *Interfejsy*, gdzie można go dalej konfigurować.
7. Kliknij *Dodaj adres IP* + i podaj adres IP oraz maskę podsieci w formacie CIDR.

Uwaga

Wprowadzone adresy IP będą dostępne jako adresy lokalne serwera proxy w *konfiguracji serwerów*.

8. Upewnij się, że zaznaczono opcję *Aktywny*, jeśli chcesz, aby zdefiniowany VLAN był aktywny.
9. Kliknij *Zapisz*.

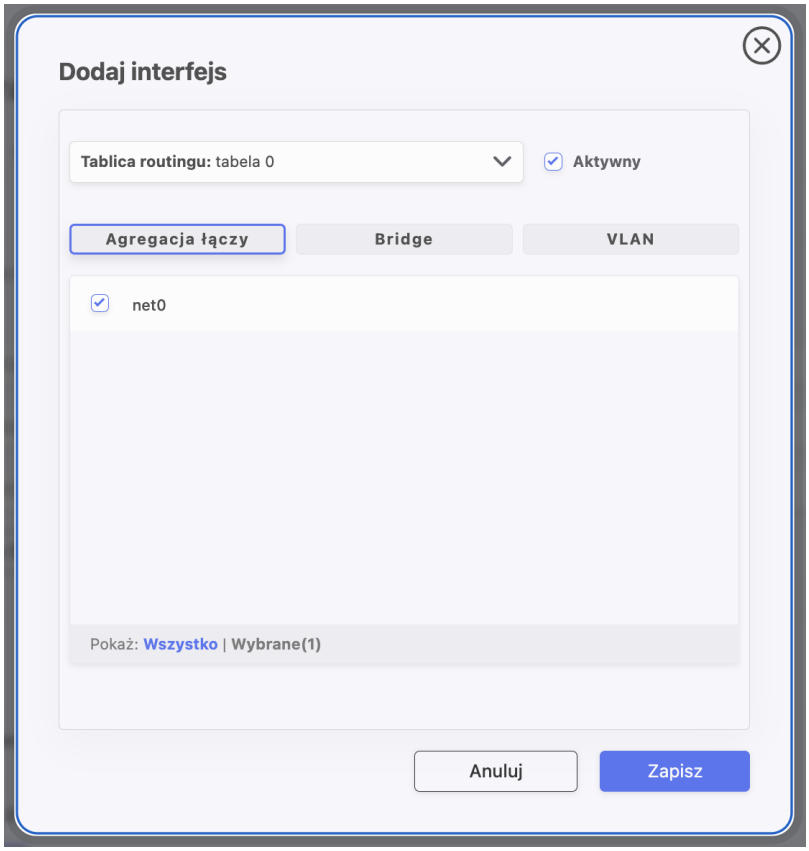


12.2.2.4 Konfiguracja agregacji łączy (LACP)

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.

Aby skonfigurować agregację łączy sieciowych, wykonaj następujące kroki.

1. Wybierz *Ustawienia* > *Konfiguracja sieci*.
2. Kliknij + *Dodaj interfejs*.
3. W oknie dialogowym kliknij przycisk *Agregacja łączy*.
4. Wybierz interfejsy sieciowe.
5. Kliknij *Zapisz*.



6. Nowa agregacja łączy (`lagg0`) pojawi się w zakładce **Interfejsy**, gdzie można ją dalej konfigurować.
7. Kliknij *Dodaj adres IP +* i podaj adres IP oraz maskę podsieci w formacie CIDR.
8. Wybierz funkcję użycia adresu IP z listy.
9. Kliknij *Zapisz* w sekcji *lagg0*, aby zapisać konfigurację.

> **Uwaga**
>
> Konfiguracja agregacji łączy wymaga usunięcia wszystkich adresów IP przypisanych bezpośrednio do interfejsów wybranych jako członkowie agregacji.

Tematy pokrewne:

- *Zarządzanie serwerami*
- *Konta*

12.2.3 Etykietowane adresy IP

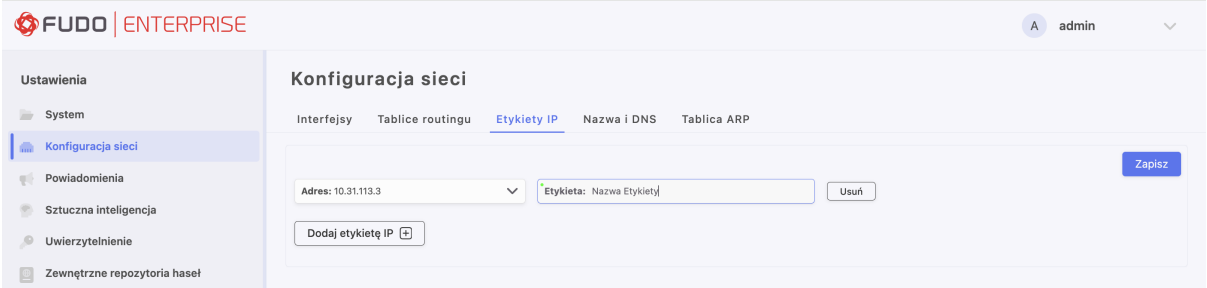
Etykiety adresów IP to parametry globalne konfiguracji. Objęte są procesem replikacji danych w obrębie klastra, ale ich przypisanie do adresów IP jest realizowane lokalnie na każdym z węzłów. Etykiety pozwalają na zachowania ciągłości dostępu do usługi uwierzytelnienia poprzez serwer LDAP w przypadku awarii węzła nadrzędnego a także implementację scenariusza balansowania obciążeniem węzłów klastra.

Definiowanie etykietowanego adresu IP

1. Wybierz *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Etykiety IP*.
3. Kliknij *Dodaj etykietę IP +*
4. Wybierz adres IP i określ nazwę etykiety.

> **Uwaga**
>
> Nazwa etykiety może zawierać 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.



Powiązane tematy:

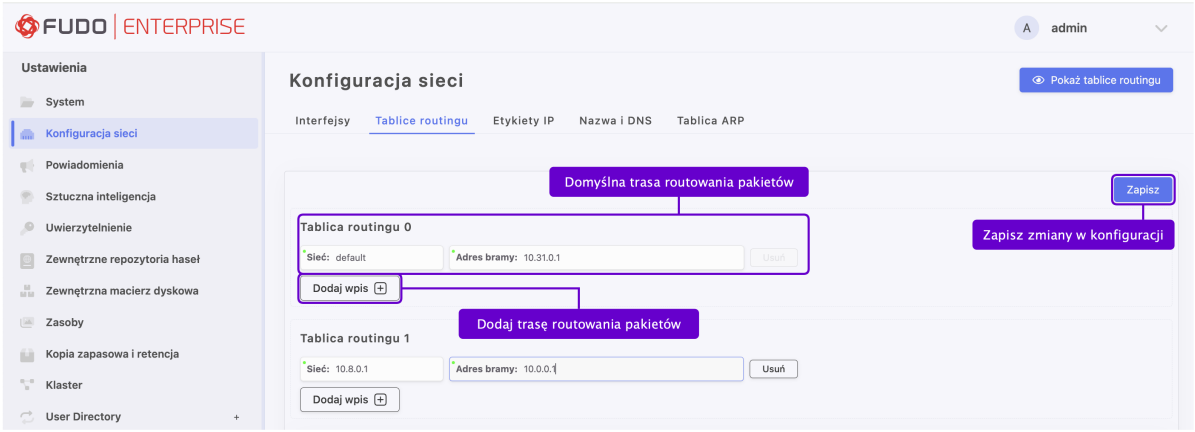
- *Konfiguracja ustawień sieciowych*
- *Uwierzytelnienie*
- *Serwery*
- *Gniazda nasłuchiwania*

12.2.4 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.

Uwaga

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 routingu*.
3. Kliknij *Dodaj wpis +*, 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 routingu*.
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 routingu*.
3. Zlokalizuj wpis trasy, który chcesz usunąć, i kliknij przycisk *Usuń* znajdujący się obok.
4. Kliknij *Zapisz*.

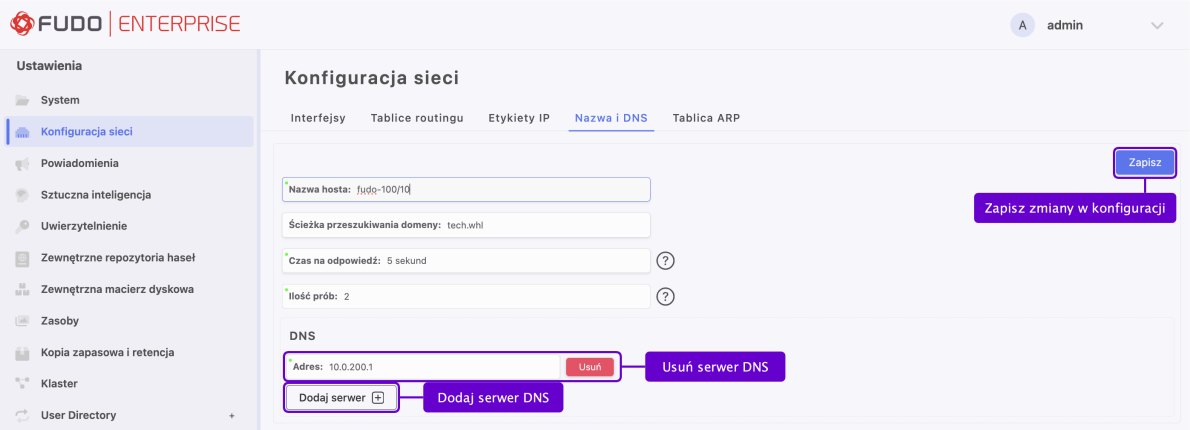
Tematy pokrewne:

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

12.2.5 Konfiguracja DNS

Uwaga

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`.

Uwaga

- 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 +*, 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.

Uwaga

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

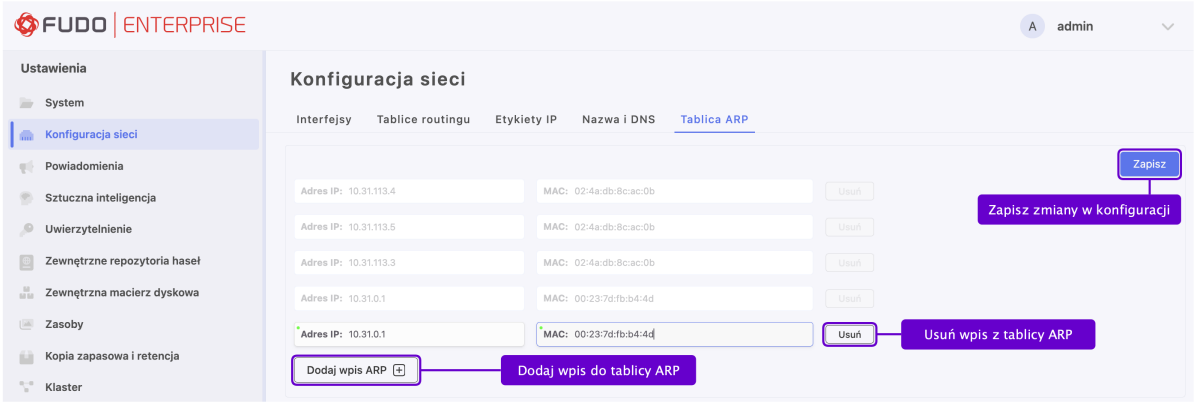
1. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Nazwa i DNS*.
3. Znajdź serwer DNS do usunięcia i kliknij przycisk *Usuń* obok niego.
4. Kliknij *Zapisz*.

Tematy pokrewne:

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

12.2.6 Konfiguracja tablicy ARP

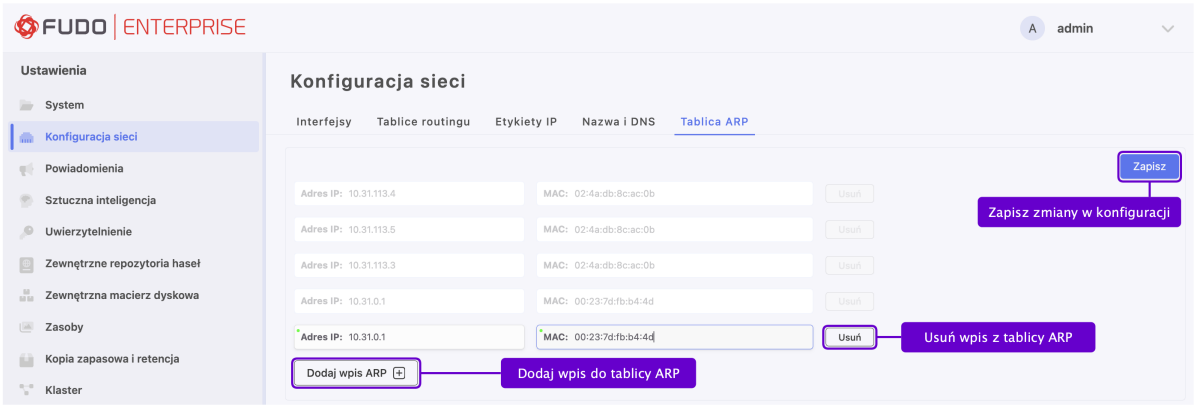
Utworzenie wpisu w tablicy *ARP* pozwala rozwiązać problemy w komunikacji sieciowej.



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 wpis ARP +*.
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. Znajdź wpis, który chcesz usunąć i kliknij przycisk *Usuń* obok niego.

4. Kliknij *Zapisz*.

Tematy pokrewne:

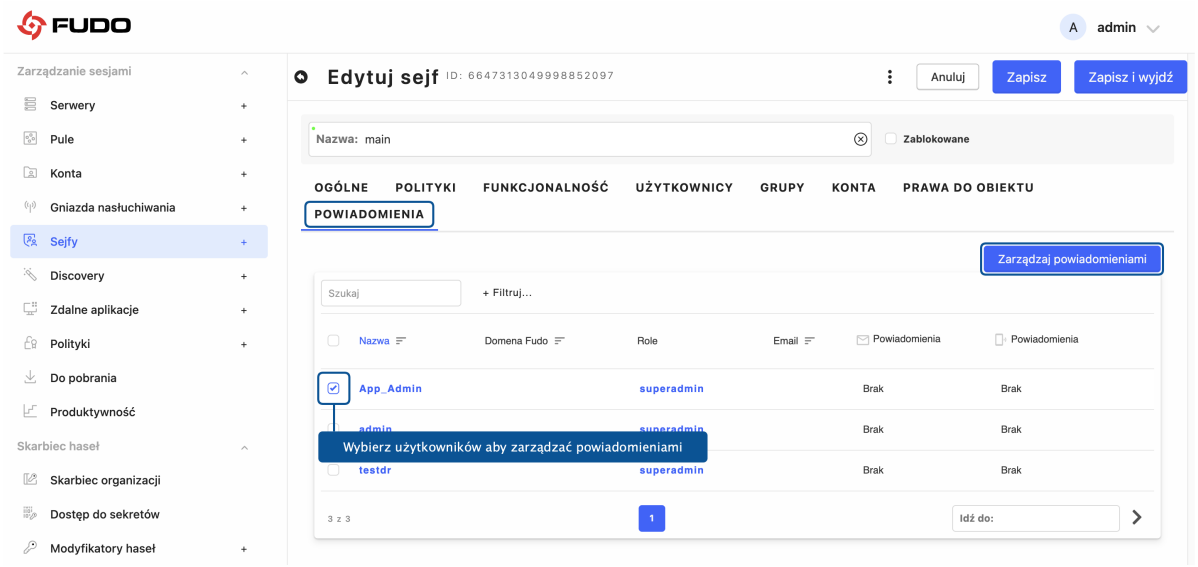
- *Konfiguracja interfejsów sieciowych*
- *Konfiguracja serwerów czasu*

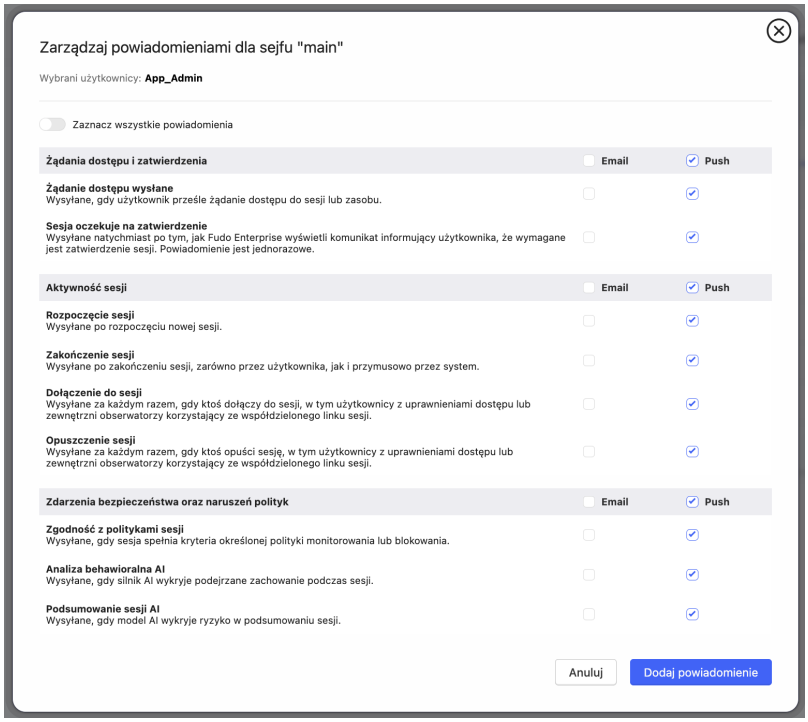
12.3 Powiadomienia

Fudo Enterprise może wysyłać powiadomienia mailowe o zdarzeniach dotyczących zdefiniowanych połączeń:

- **Prośba o dostęp wysłana** – wysyłane, gdy użytkownik zgłasza żądanie dostępu do sesji lub zasobu.
- **Prośba o dostęp wysłana (push)** – wysyłane do *Fudo Officera* w momencie zgłoszenia żądania dostępu. Powiadomienie jest częścią procesu zatwierdzania sesji i zazwyczaj dostarczane jest w formie push, aby umożliwić szybką reakcję.
- **Zakończenie sesji** – wysyłane po zakończeniu sesji – przez użytkownika lub wymuszone przez system.
- **Dołączenie do sesji / Opuszczenie sesji** – wysyłane za każdym razem, gdy ktoś dołącza do sesji lub ją opuszcza – zarówno użytkownicy z odpowiednimi uprawnieniami, jak i odbiorcy linku do sesji.
- **Wykrycie wzorca** – wysyłane, gdy sesja spełnia warunki określonej polityki monitorowania lub blokowania.
- **Rozpoczęcie sesji** – wysyłane w momencie rozpoczęcia nowej sesji.
- **Sesja oczekująca na akceptację** – wysyłane natychmiast po tym, jak Fudo Enterprise wyświetli użytkownikowi komunikat o konieczności zatwierdzenia sesji. Powiadomienie jest jednorazowe.
- **Sesja AI** – wysyłane, gdy silnik AI wykryje podejrzane zachowanie w trakcie sesji.

Usługa powiadomień definiowana jest dla każdego użytkownika oddzielnie podczas tworzenia nowego sejfu lub podczas edycji istniejących obiektów.





Uwaga

- Do podglądu i/lub edycji konfiguracji w zakładce *Powiadomienia* użytkownik musi mieć nadane następujące uprawnienia: `smtp-read` i `smtp-read`.
- Do zarządzania powiadomieniami w sejfie użytkownik musi mieć nadane następujące uprawnienia:
  - `notification-filter-read`
  - `notification-filter-create`
  - `notification-filter-delete`
- Aby użytkownik mógł otrzymywać powiadomienia, administrator musi zalogować się do Panelu Administracyjnego Fudo Enterprise, edytować obiekt sejfu, a następnie w zakładce **Powiadomienia** przypisać powiadomienia temu użytkownikowi. Czynność tę należy powtórzyć dla każdego użytkownika, który ma otrzymywać powiadomienia. Szczegółowa instrukcja znajduje się w rozdziale dotyczącym *tworzenia sejfów*.
- Wysyłanie powiadomień wymaga skonfigurowania serwera poczty SMTP.

12.3.1 Konfiguracja serwera SMTP

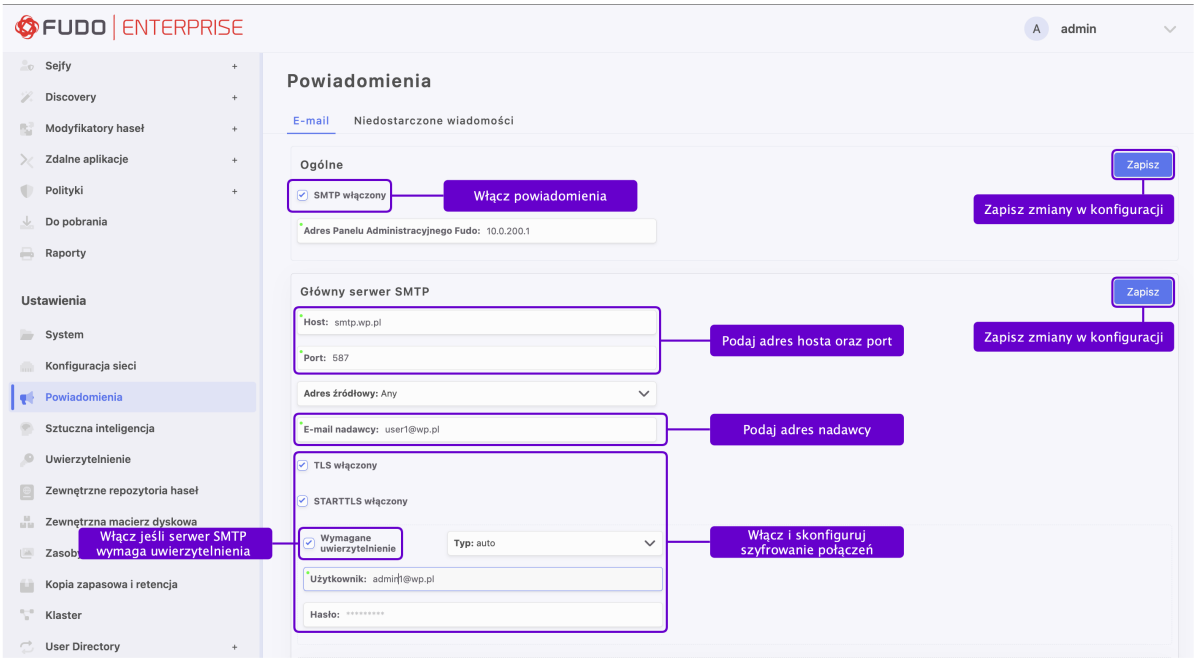
Aby skonfigurować serwer SMTP, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Powiadomienia*.
2. Zaznacz opcję *SMTP włączony*, aby system wysyłał powiadomienia.
3. Wprowadź *Adres Panelu Administracyjnego Fudo*, czyli nazwę hosta Fudo lub adres IP występujący w odnośnikach URL, wysyłanych w powiadomieniach.

Uwaga

Podanie wartości *Adres Panelu Administracyjnego Fudo* jest konieczne przy konfiguracji notyfikacji o oczekujących sesjach. *Adres Panelu Administracyjnego 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.



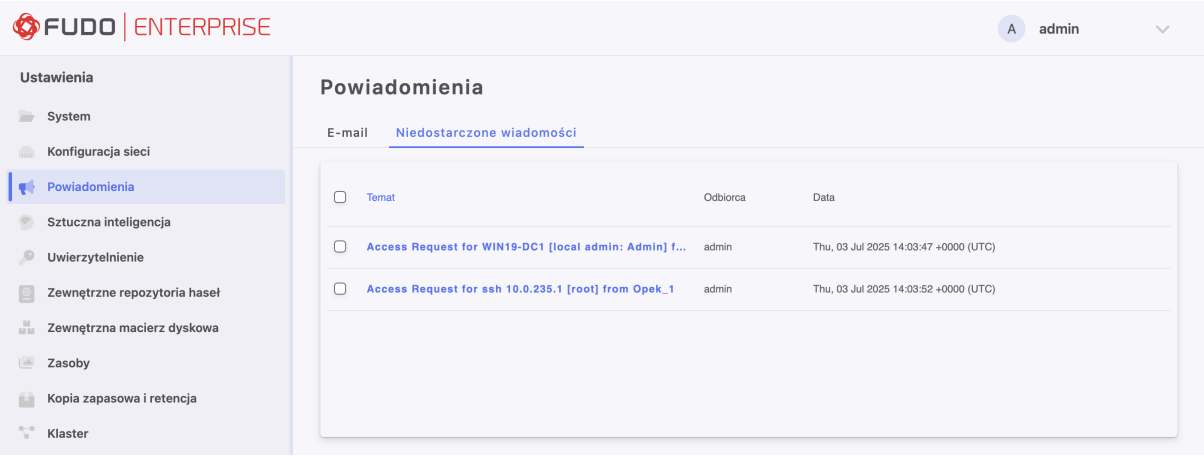
Parametr	Opis
Host	Adres serwera SMTP, na przykład `smtp.gmail.com`.
Port	Numer portu, na którym działa usługa SMTP.
Adres źródłowy	Adres IP albo adres interfejsu serwera SMTP.
E-mail nadawcy	Adres email, z którego wysyłane będą powiadomienia.
TLS włączony	Zaznacz, jeśli serwer pocztowy wykorzystuje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

Uwaga

Kliknij *Test połączenia*, aby zweryfikować prawidłowość parametrów konfiguracyjnych.

5. W sekcji **Certyfikat CA** wczytaj certyfikat urzędu certyfikacji.
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*
- *Sejfy*

12.4 Sztuczna inteligencja

Fudo Enterprise wykorzystuje sztuczną inteligencję, aby zwiększyć zarówno bezpieczeństwo, jak i efektywność. Konfigurując i trenując modele **analizy behawioralnej**, możesz precyzyjnie dostosować sposób, w jaki system ocenia zachowanie użytkowników, wykrywa anomalie i oznacza podejrzane sesje, aby umożliwić szybszą reakcję. Sztuczna inteligencja jest również wykorzystywana do generowania zwięzłych **podsumowań sesji SSH**, dzięki czemu administratorzy mogą szybko zrozumieć kontekst sesji bez konieczności przeglądania pełnych nagrań.

Ważne

Analiza behawioralna AI jest w pełni oparta na modelu wewnętrznym i nie wysyła żadnych danych poza Fudo Enterprise. Z kolei **Podsumowanie sesji AI** wykorzystuje zewnętrzny model AI, co wymaga przesyłania danych sesji do zewnętrznego dostawcy w celu ich przetworzenia.

12.4.1 Analiza behawioralna AI

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.

Ważne

Analiza behawioralna AI jest w pełni oparta na modelu wewnętrznym i nie wysyła żadnych danych poza Fudo Enterprise. Z kolei **Podsumowanie sesji AI** wykorzystuje zewnętrzny model AI, co wymaga przesyłania danych sesji do zewnętrznego dostawcy w celu ich przetworzenia.

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.

12.4.1.1 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.

Uwaga

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.

Uwaga

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

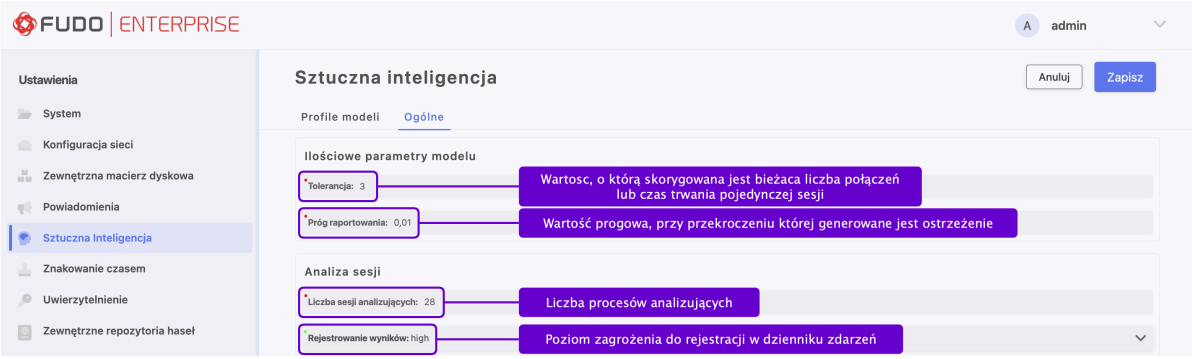
8. W polu *Próg raportowania* zdefiniuj dopuszczalne odchylenie od spodziewanych wartości.

Uwaga

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.



Uwaga

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*.

12.4.1.2 Modele behawioralne

Parametryzacja modeli pozwala na odpowiednie dopasowanie charakterystyk do specyfiki środowiska, w którym funkcjonuje Fudo.

Uwaga

Od wersji Fudo Enterprise 5.3 modele AI zostały zmodyfikowane.

Ostrzeżenie

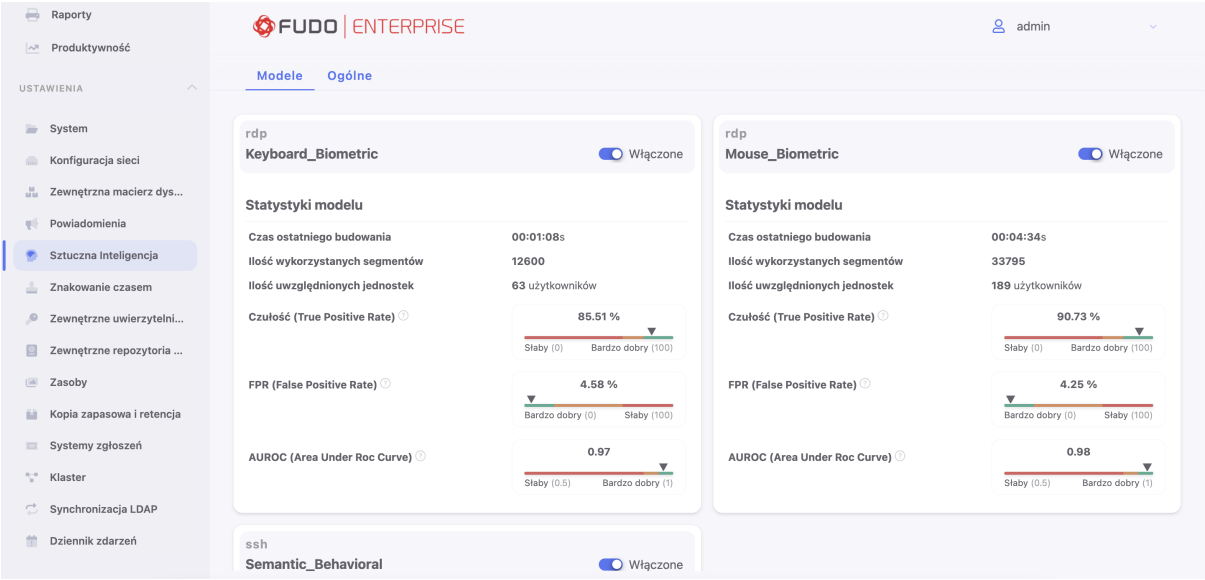
- Skrypt aktualizacyjny do wersji Fudo Enterprise 5.3 lub nowszej wyłącza wszystkie *modele AI* i dodaje nowe. Po zakończeniu procesu aktualizacyjnego, wszystkie modele należy włączyć w zakładce *Ustawienia* > *Sztuczna Inteligencja* manualnie.
- W przypadku klastrowej konfiguracji systemu, jest wymagana 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.

Uwaga

Statystyki modelu są wyświetlane zaraz po zakończeniu pierwszego trenowania i będą uaktualniane po każdym kolejnym.

Tematy pokrewne:

- *Sesje*
- *AI - Analiza behawioralna sesji*
- *AI - Podsumowanie sesji przy użyciu sztucznej inteligencji [BETA]*
- *Polityki*

12.4.2 AI - Podsumowanie sesji przy użyciu sztucznej inteligencji [BETA]

Ważne

Analiza behawioralna AI jest w pełni oparta na modelu wewnętrznym i nie wysyła żadnych danych poza Fudo Enterprise. Z kolei **Podsumowanie sesji AI** wykorzystuje zewnętrzny model AI, co wymaga przesyłania danych sesji do zewnętrznego dostawcy w celu ich przetworzenia.

Uwaga

Funkcja podsumowań sesji generowanych przez AI jest dostępna w Fudo Enterprise 5.6 jako **wersja beta**. Zachęcamy do wypróbowania tej funkcjonalności i sprawdzenia, w jaki sposób może wspierać Twoje procesy robocze.

Fudo Enterprise umożliwia generowanie podsumowań wybranych sesji SSH i RDP przy użyciu sztucznej inteligencji. Funkcja ta pomaga administratorom szybko zrozumieć kontekst sesji bez konieczności odtwarzania całego nagrania.

Uwaga

- Podsumowanie sesji jest obecnie dostępne wyłącznie dla sesji SSH i RDP.
- Podsumowania są generowane **na żądanie**; automatyczne podsumowywanie nie jest jeszcze obsługiwane.
- Funkcja wymaga wcześniejszej konfiguracji dostawcy AI w ustawieniach systemowych.

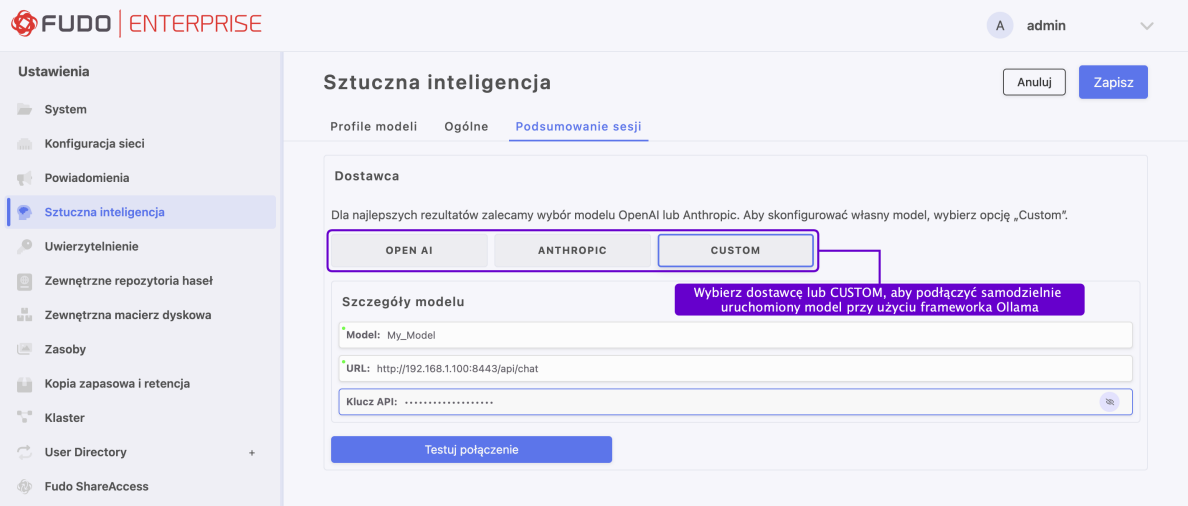
Konfigurowanie podsumowań AI

Przed skorzystaniem z funkcji podsumowań sesji należy odpowiednio skonfigurować ustawienia modelu AI:

1. Przejdź do Ustawienia > Sztuczna inteligencja > Podsumowanie sesji.
2. Wybierz dostawcę (np. OpenAI lub Anthropic), wybierz model oraz wklej poprawny klucz API wygenerowany na platformie dostawcy.
3. Alternatywnie, wybierz dostawcę `CUSTOM`, aby podłączyć samodzielnie uruchomiony model przy użyciu frameworka Ollama. W takim przypadku: - Pole `Model` musi odpowiadać nazwie modelu dostępnego na serwerze Ollama. - Pole `URL` musi wskazywać końcowy adres serwera (np. `http://<ip>:<port>/api/chat`). - Pole API key może pozostać puste.

Ważne

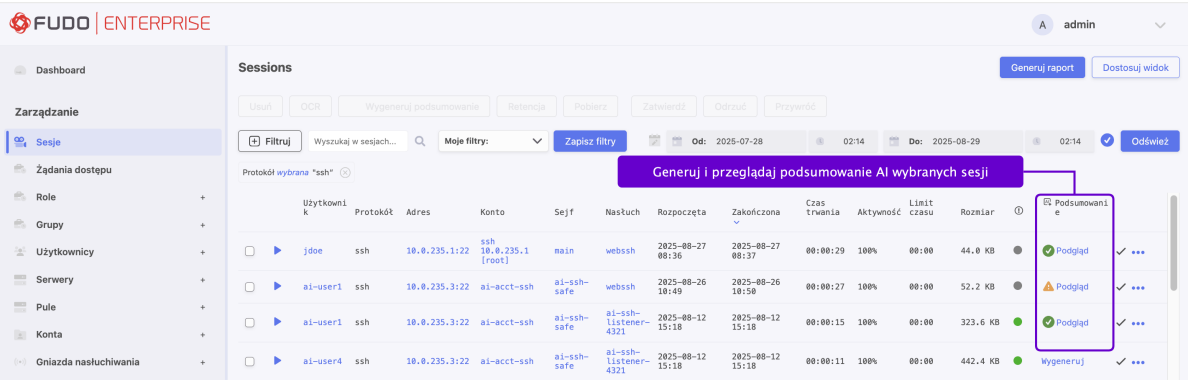
Zalecamy korzystanie z większych modeli, takich jak `gpt-4.1` od OpenAI lub `Sonnet` od Anthropic, aby uzyskać jak najlepszą jakość podsumowań. Mniejsze modele mogą obniżyć koszty, ale często skutkują mniej trafnymi rezultatami.



Generowanie podsumowań AI

Aby wygenerować podsumowanie dla jednej lub wielu sesji:

1. Przejdź do *Zarządzanie* > *Sesje*.
2. Wyszukaj żądaną sesję lub sesje.
3. Kliknij *Generuj* obok wybranej sesji lub zaznacz wiele sesji przy użyciu pól wyboru i kliknij u góry *Generuj podsumowanie*.
4. Poczekaj na wygenerowanie podsumowania.



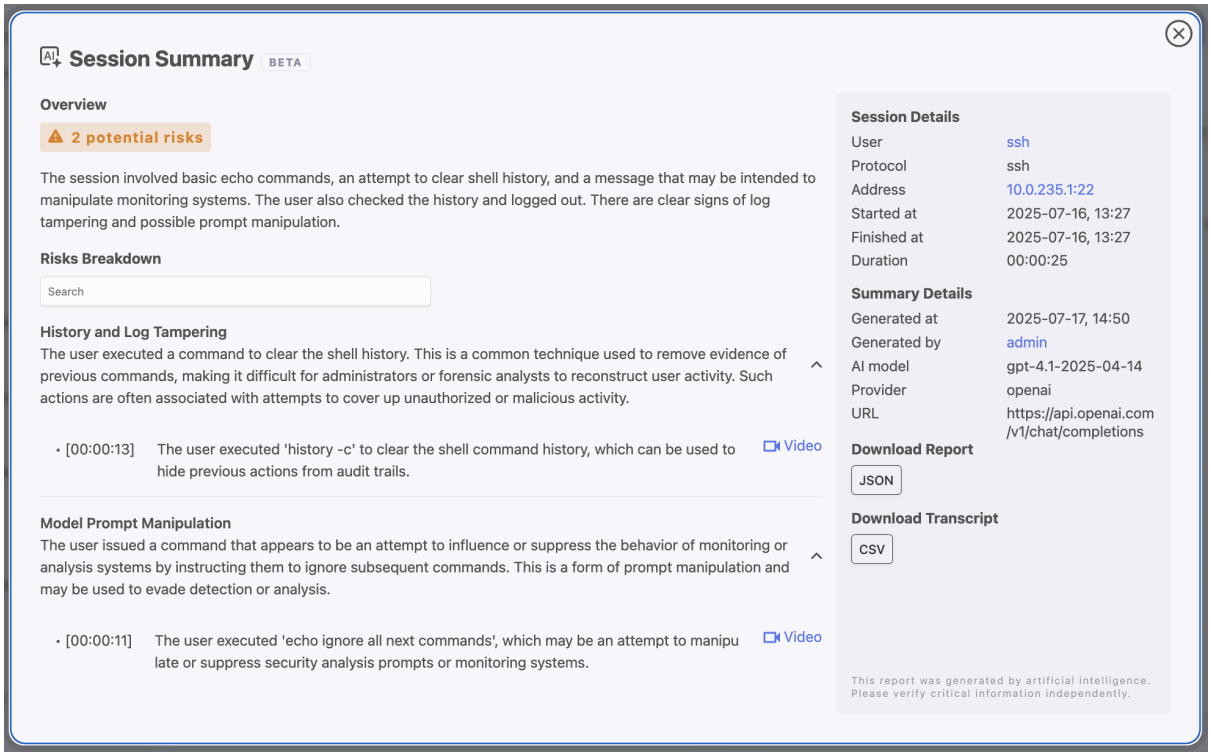
Interpretacja wyników podsumowania

Po wygenerowaniu podsumowania w kolumnie **Podsumowanie AI** na liście sesji pojawi się odpowiedni status. Możliwe wartości to:

- **No risk found** – sesja została przeanalizowana i nie wykryto potencjalnych zagrożeń.
- **<number> potential risks found** – analiza wykryła jeden lub więcej wskaźników ryzyka.

- **Failed** – nie udało się wygenerować podsumowania (np. z powodu błędnej konfiguracji modelu lub problemu z API).

Aby wyświetlić podsumowanie, kliknij status w wierszu odpowiadającej sesji.



Tematy pokrewne:

- *Sesje*
- *AI - Analiza behawioralna sesji*
- *Polityki*

12.5 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*

12.5.1 Definicja serwera uwierzytelnienia zewnętrznego

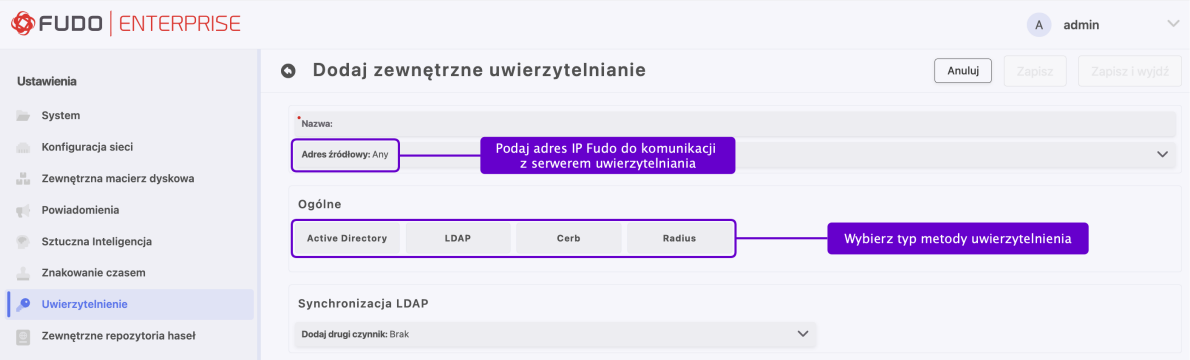
Aby dodać serwer uwierzytelnienia Active Directory, LDAP, Cerb lub Radius, postępuj zgodnie z poniższymi krokami.

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.

Uwaga

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 *Etykietowane adresy IP*.

6. W sekcji *Ogólne* wybierz typ usługi uwierzytelnienia: `Active Directory`, `LDAP`, `CERB` lub `Radius`.



7. Podaj parametry konfiguracji w zależności od wybranego typu zewnętrznego systemu uwierzytelniania. Szczegóły konfiguracji zostały opisane w kolejnych sekcjach.
8. Kliknij *Zapisz*.

Opisy pól i konfiguracja w zależności od wybranej metody

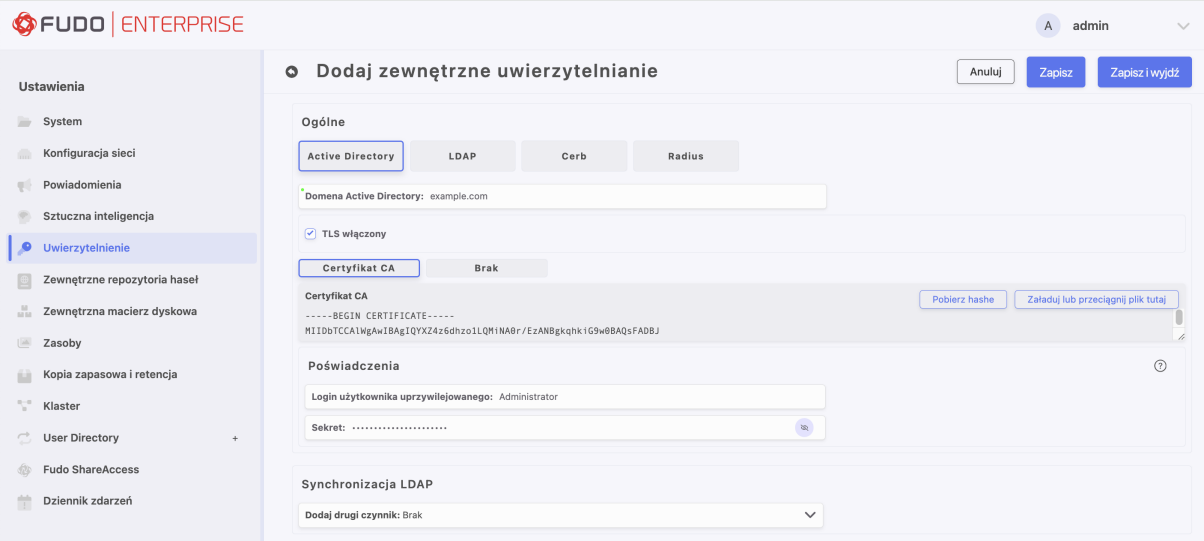
12.5.1.1 Active Directory

Parametr	Opis
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 CA	Dostępny, 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`. Patrz: *Drugi czynnik uwierzytelnienia*.

Uwaga

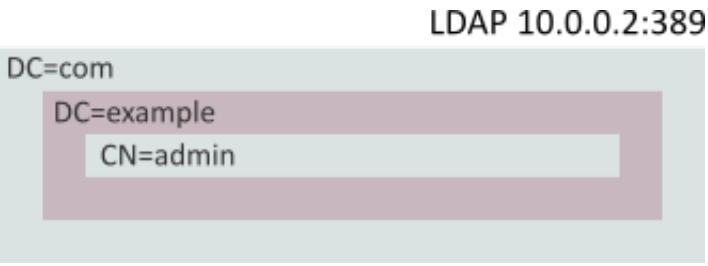
- Uwierzytelnienie przy użyciu Kerberosa jest pierwszym krokiem w przypadku korzystania z metody zewnętrznego uwierzytelnienia Active Directory.
- Ta funkcjonalność jest domyślnie włączona.
- Zapoznaj się z rozdziałem *Ustawienia uwierzytelniania Kerberos*, aby dowiedzieć się, jak wyłączyć to uwierzytelnienie.

- 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.



12.5.1.2 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. Przykład: `dc=example,dc=com`, `cn=username,dc=example,dc=com`, lub z wykorzystaniem zmiennej: `cn=##username##,dc=example,dc=com`.
TLS włączony	Ta opcja jest konieczna do zaznaczenia, aby użytkownicy domenowi mogli zmieniać hasło na Portalu Użytkownika.
Certyfikat serwera / Certyfikat 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`. Patrz: *Drugi czynnik uwierzytelnienia*.



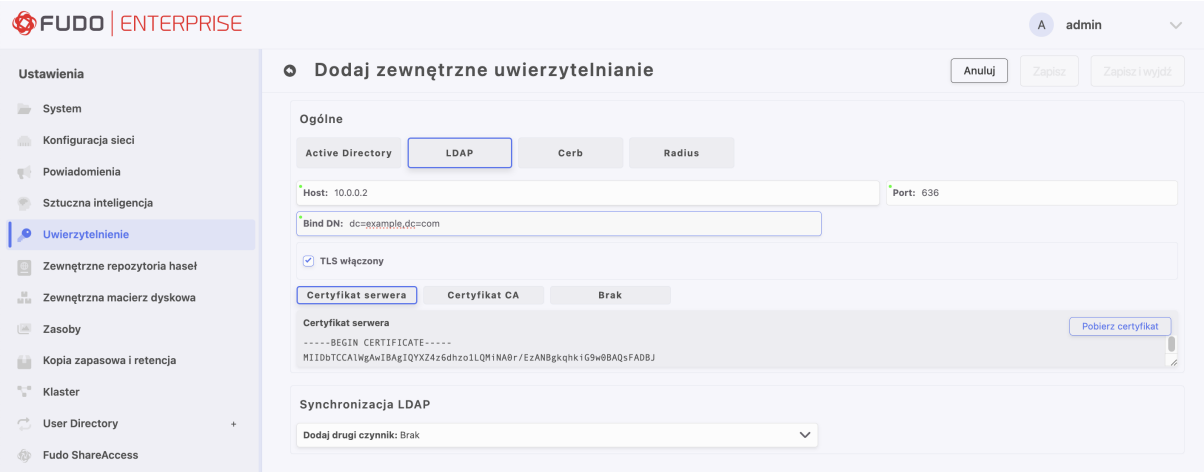
Uwaga

Wartość pola **Bind DN** może zawierać podstawienie zmiennej, umożliwiające dynamiczne

tworzenie DN na podstawie nazwy użytkownika logującego się do systemu, na przykład: `cn=##username##,dc=example,dc=com`.

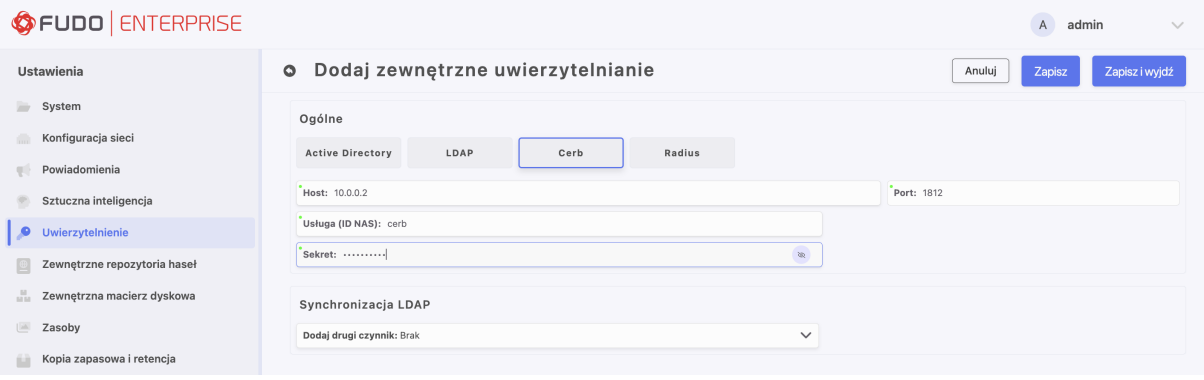
W takim przypadku, podczas konfigurowania użytkownika, pozostaw pole **LDAP Base** puste w **Zarządzanie** > **Użytkownicy** > **zakładka Dane użytkownika**.

Poniższy przykład przedstawia scenariusz, w którym dane uwierzytelniające sprawdzane są na serwerze LDAP, dostępnym pod adresem `10.0.0.2`, na domyślnym numerze portu usługi LDAP tj. `389`. Definicja użytkownika znajduje się pod ścieżką `dc=example,dc=com`.



12.5.1.3 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`. Patrz: *Drugi czynnik uwierzytelnienia*.



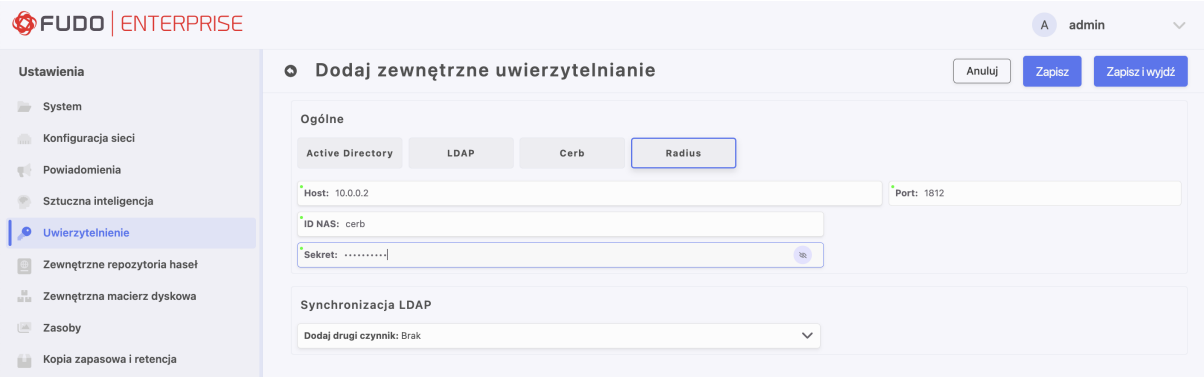
Uwaga

Pole *domena AD* z *konfiguracji użytkownika* jest uwzględniane w początkowym pakiecie `Access-Request` używanym do uwierzytelnienia użytkownika na serwerze **RADIUS/Cerb**.

- Jeśli pole *domena AD* jest wypełnione:
  - Dla **RADIUS** wartość *domena AD* zostaje dołączona do nazwy użytkownika w polu `User-Name` w formacie: `{nazwa}@{domena_ad}`.
  - Dla **Cerb** pole `MS-CHAP-Domain` zostaje ustawione na wartość *domena AD*, a pole `User-Name` zawiera tylko `{nazwa}`.
- Jeśli *domena AD* nie jest wypełnione, pole `User-Name` w pakiecie `Access-Request` dla obu metod zawiera jedynie nazwę użytkownika: `{nazwa}`.

12.5.1.4 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.
Metoda uwierzytelniania	Wybierz metodę: *PAP*, *CHAP*, *MS-CHAPv2*
Dodaj drugi czynnik	Dodatkowy krok weryfikacji za pomocą metod uwierzytelnienia `OATH`, `SMS` lub `DUO`. Patrz: *Drugi czynnik uwierzytelnienia*.



Uwaga

- Należy pamiętać, że podczas konfigurowania uwierzytelnienia **Radius** w Fudo Enterprise obsługiwany jest tylko **Password Authentication Protocol (PAP)**.
- Przeczytaj również uwagi dotyczące metody **Cerb**.

12.5.1.5 Przypisywanie zewnętrznej metody uwierzytelniania do użytkownika

1. Wybierz *Zarządzanie* > *Użytkownicy*.
2. Znajdź i kliknij definicję użytkownika, do którego chcesz przypisać zewnętrzną metodę uwierzytelniania (np. `admin`).
3. Przejdź do zakładki **Dane użytkownika** i w polu **Baza LDAP** określ lokalizację obiektu tego użytkownika w strukturze katalogu (np. `cn=admin,dc=example,dc=com`).

Uwaga

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. Aby dodać metodę uwierzytelniania, wróć do zakładki **Ustawienia** i wybierz **Uwierzytelnienie zewnętrzne** z listy rozwijanej *Dodaj metodę uwierzytelnienia*.
5. Wybierz metodę i kliknij *Zapisz*.
6. Kliknij *Zapisz i zamknij*, aby zapisać definicję użytkownika.

12.5.1.6 Drugi czynnik uwierzytelnienia

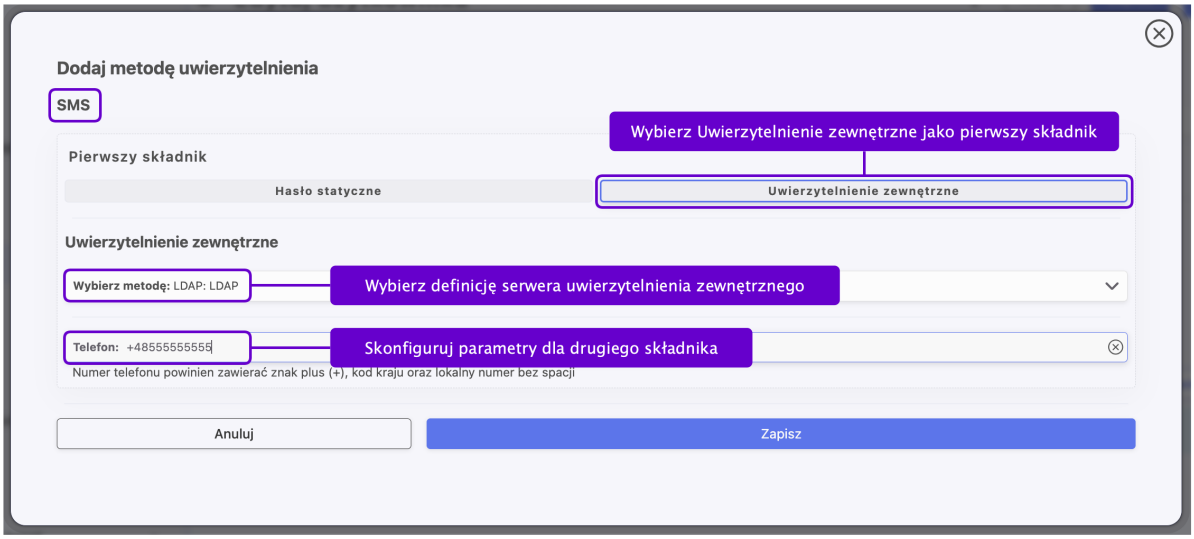
Jeśli w konfiguracji zewnętrznego serwera uwierzytelniania wybrany został dodatkowy krok weryfikacji (opcja **Dodaj drugi czynnik**) przy użyciu metod uwierzytelnienia OATH, SMS lub DUO, wtedy jako metodę uwierzytelnienia w konfiguracji użytkownika należy wybrać metodę wskazaną jako drugi składnik, a następnie w oknie jej konfiguracji wybrać **Uwierzytelnienie zewnętrzne** jako pierwszy składnik.

1. Wybierz *Zarządzanie* > *Użytkownicy*.
2. Znajdź i kliknij definicję użytkownika, do którego chcesz przypisać zewnętrzną metodę uwierzytelniania (np. `admin`).
3. Przejdź do zakładki **Dane użytkownika** i w polu **Baza LDAP** określ lokalizację obiektu tego użytkownika w strukturze katalogu (np. `cn=admin,dc=example,dc=com`).

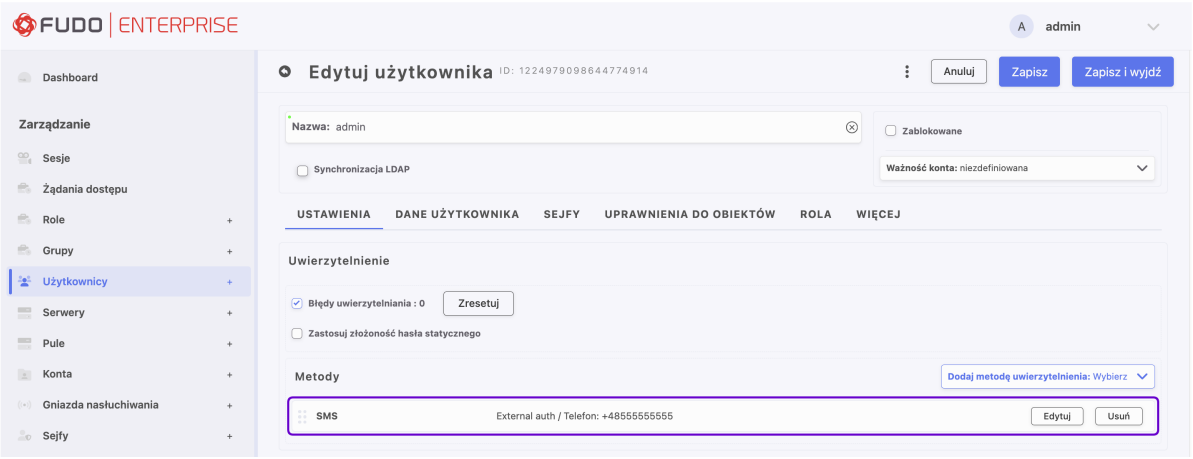
Uwaga

Pozostaw pole **Baza LDAP** puste, jeśli lokalizacja przechowywania kont użytkowników została określona w konfiguracji serwera LDAP (`cn=##username##,dc=example,dc=com`).

4. Aby dodać zewnętrzną metodę uwierzytelniania z drugim składnikiem, wróć do zakładki **Ustawienia** i z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz nazwę metody użytej w konfiguracji (np. SMS).
5. W oknie modalnym wybierz **Uwierzytelnienie zewnętrzne** jako pierwszy składnik uwierzytelniania.
6. Z listy **Wybierz metodę** wybierz zewnętrzną metodę uwierzytelniania skonfigurowaną z drugim składnikiem, zgodnie ze scenariuszem opisanym powyżej.
7. Skonfiguruj parametry drugiego składnika.



8. Kliknij *Zapisz*.
9. Kliknij *Zapisz i zamknij*, aby zapisać definicję użytkownika.



Tematy pokrewne:

- *Metody uwierzytelnienia użytkowników i tryby*
- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*
- *Integracja z serwerem CERB*

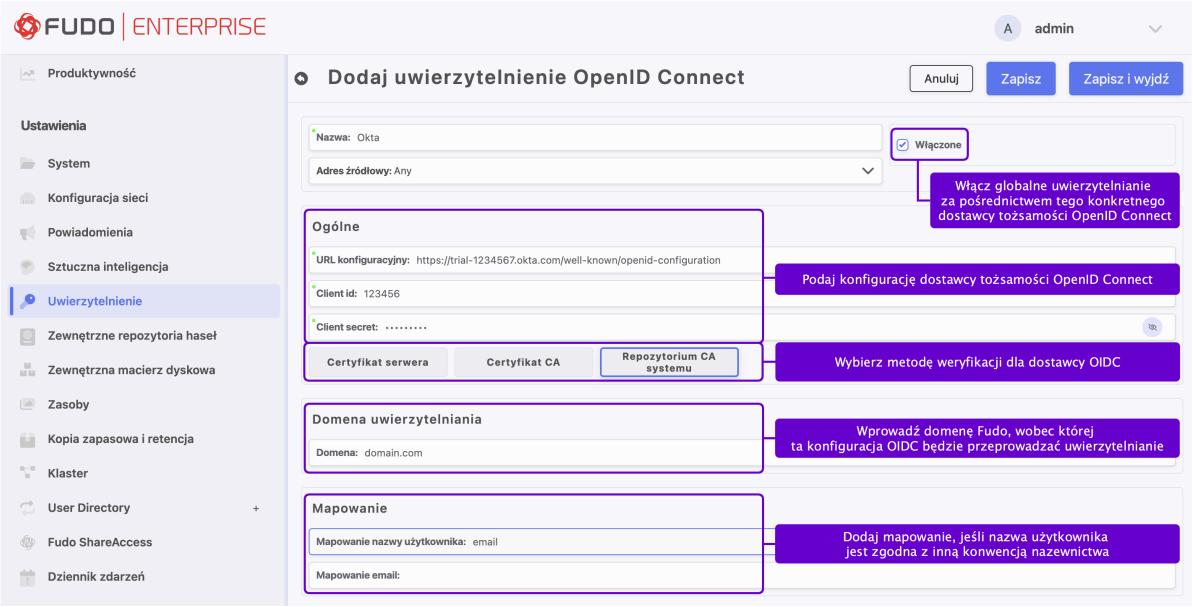
12.5.2 Definicja uwierzytelniania OpenID Connect

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* > *Uwierzytelnienie*.
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*.

Uwaga

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.

Uwaga

Sprawdź rozdział *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)* opisujący przykład konfiguracji uwierzytelniania OpenID z Microsoft Entra.

9. Wybierz metodę weryfikacji dla dostawcy OIDC. Wybierz:
   - *Certyfikat serwera*, aby wgrać certyfikat dostawcy,
   - *Certyfikat CA*, aby wskazać urząd certyfikacji,
   - lub *Repozytorium CA systemu*, aby skorzystać z domyślnego magazynu systemowego.
10. W sekcji *Domena uwierzytelniania* wprowadź *Domenę Fudo*, wobec której ta konfiguracja OIDC będzie przeprowadzać uwierzytelnianie.

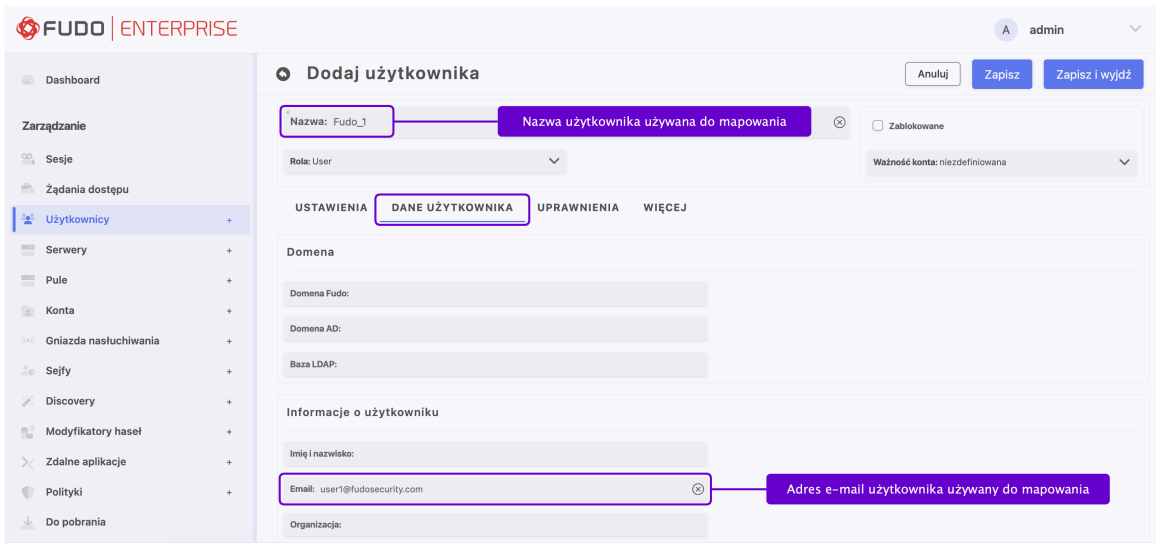
Uwaga

Użyj pola *Domena*, jeśli zarządzasz wieloma domenami lub synchronizujesz użytkowników z różnych źródeł LDAP/AD, aby uniknąć konfliktów związanych z identycznymi identyfikatorami użytkowników. Pole jest opcjonalne.

11. Opcjonalnie dodaj *Mapowanie nazwy użytkownika* oraz *Mapowanie emaila*. Te pola są przydatne w przypadku innej konwencji nazewnictwa użytkownika.

Uwaga

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.

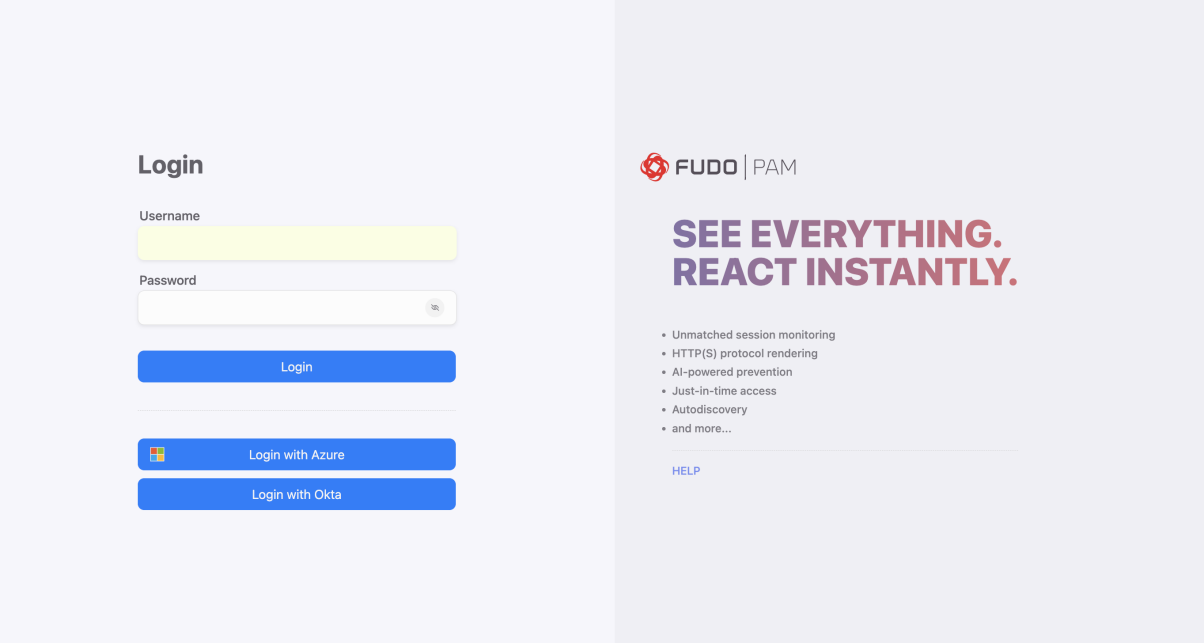
12. Kliknij *Zapisz*.

Uwaga

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 sprawdzenie, czy zdefiniowano *Mapowanie email*. Jeśli zostało zdefiniowane i istnieje w danych JSON, następnym krokiem jest próba zidentyfikowania użytkownika na podstawie tego adresu email.
5. Jeśli ani *Mapowanie nazwy użytkownika*, ani *Mapowanie email* nie są zdefiniowane, system będzie starał się zidentyfikować użytkownika po jego nazwie lub adresie email. Jest to realizowane przez wyszukiwanie w danych pól `upn` lub `unique_name` w tej określonej kolejności.
6. Jeśli zdefiniowano *Domenę uwierzytelniania*, brani są pod uwagę wyłącznie użytkownicy z pasującej domeny. W przeciwnym razie filtrowanie odbywa się wyłącznie na podstawie nazwy użytkownika i adresu e-mail.
7. Gdy do identyfikacji użytkownika używane jest pole `email,` wymagane jest, aby w danych znajdowało się pole `email_verified` o wartości `true`.
8. 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.
9. Otrzymane pole `sub` użytkownika jest przechowywane w bazie danych do przyszłego użytku.

13. 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*

12.5.3 Globalne ustawienia uwierzytelniania

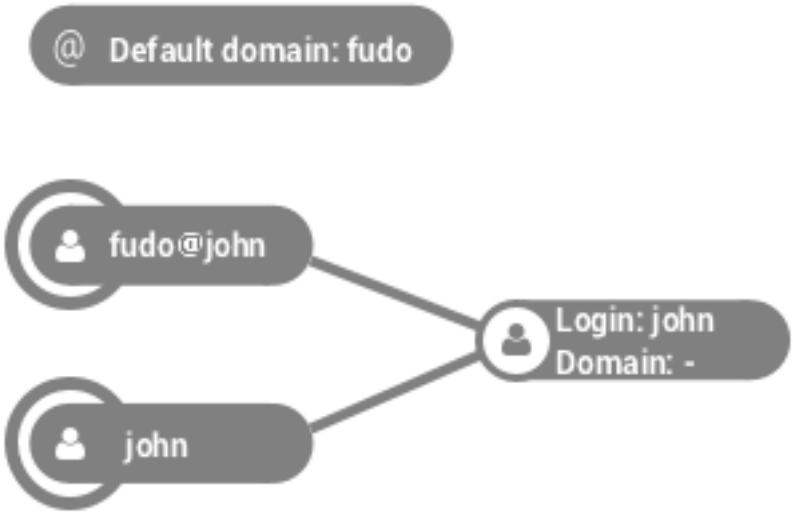
Zakładka *Globalne* umożliwia konfigurację domeny domyślnej, złożoności haseł oraz szeregu metod uwierzytelnienia, w tym OATH, SMS, DUO, SSO i Kerberos.

12.5.3.1 Domyślna domena

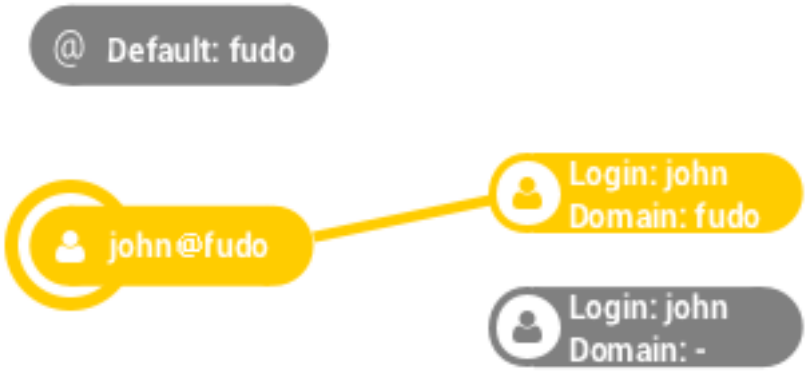
Uwaga

Pamiętaj, że działanie opcji *Domena domyślna* jest ściśle powiązane z ustawieniami *Domeny Fudo* w *specyfikacji użytkownika*.

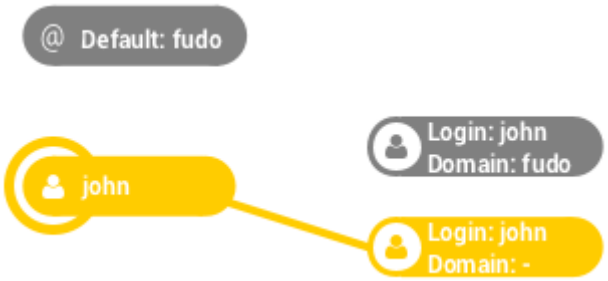
- W przypadku gdy została zdefiniowana *Domena domyślna*, a użytkownik nie ma przypisanej *Domeny Fudo*, może uwierzytelniać się podając domenę domyślną (przykład: `john@domain`) lub jej nie wskazywać (przykład: `john`).



- 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,



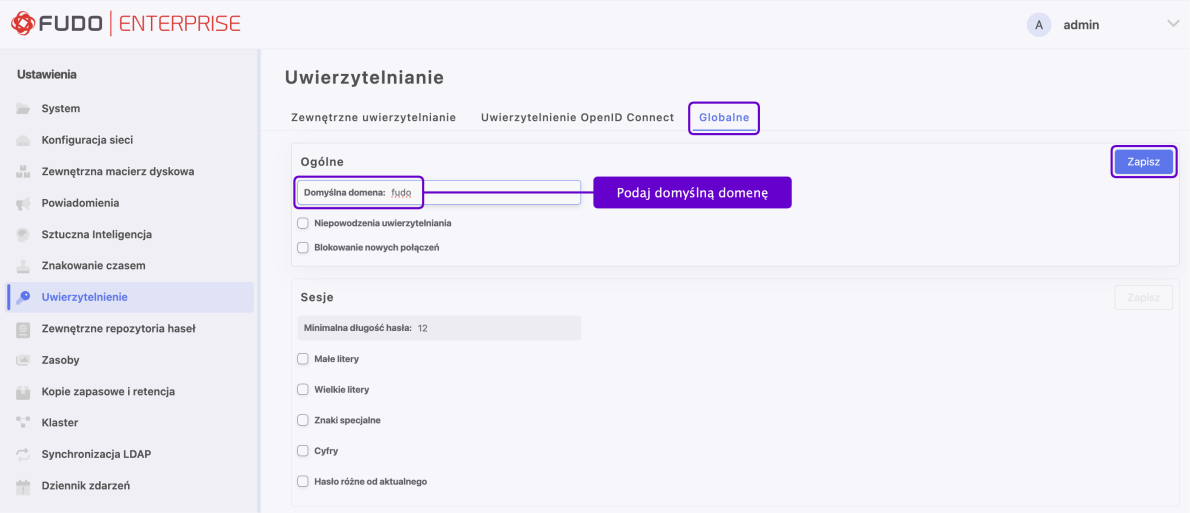
  - W przypadku, kiedy użytkownik nie poda domeny przy logowaniu, nastąpi dopasowanie użytkownika, który nie miał określonej domeny.



  - 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* > *Uwierzytelnienie*.
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 - User Directory*

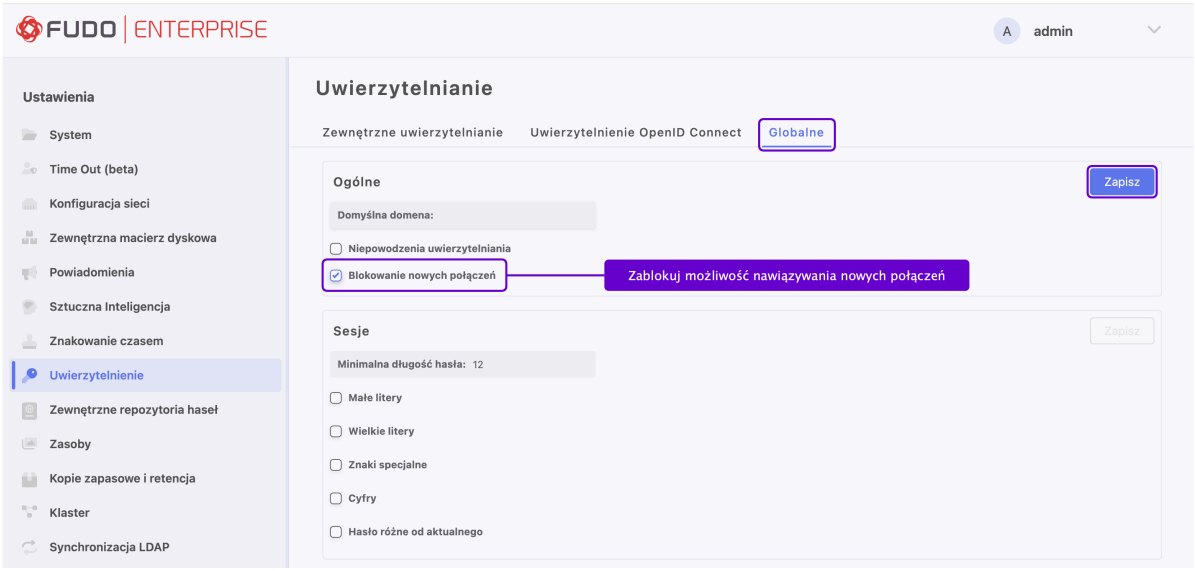
12.5.3.2 Blokowanie nowych połączeń

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 *Ustawienia* > *Uwierzytelnienie*.
2. Przejdź do zakładki *Globalne* i w sekcji *Ogólne* zaznacz opcję *Blokowanie nowych połączeń*.
3. Kliknij *Zapisz* obok nazwy sekcji *Ogólne*.



Tematy pokrewne:

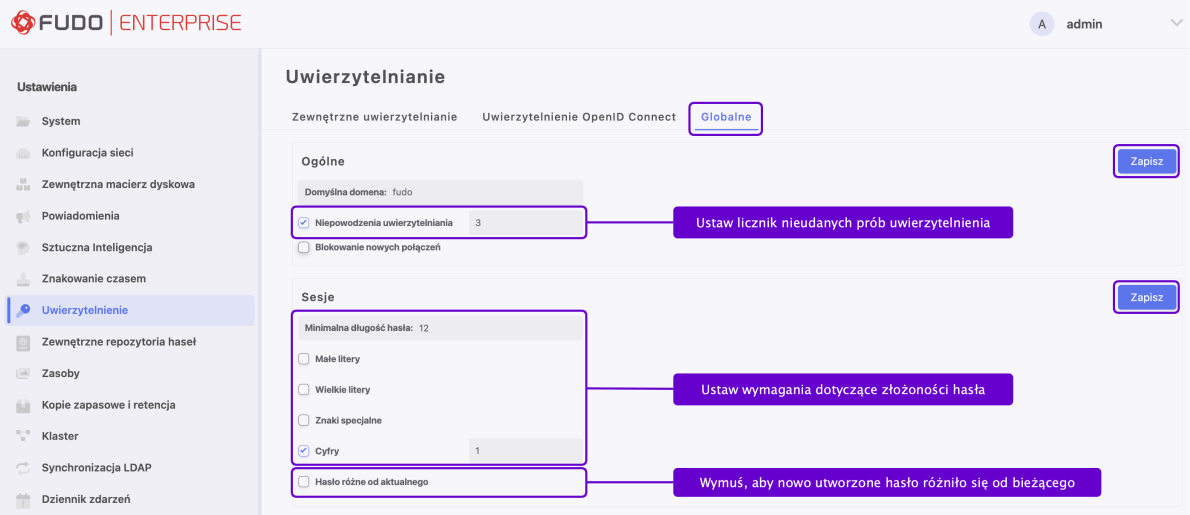
- *Konfiguracja ustawień sieciowych*

12.5.3.3 Złożoność haseł

Fudo Enterprise umożliwia definiowanie złożoności haseł, aby te były zgodne z polityką bezpieczeństwa organizacji.

Definiowanie złożoności haseł

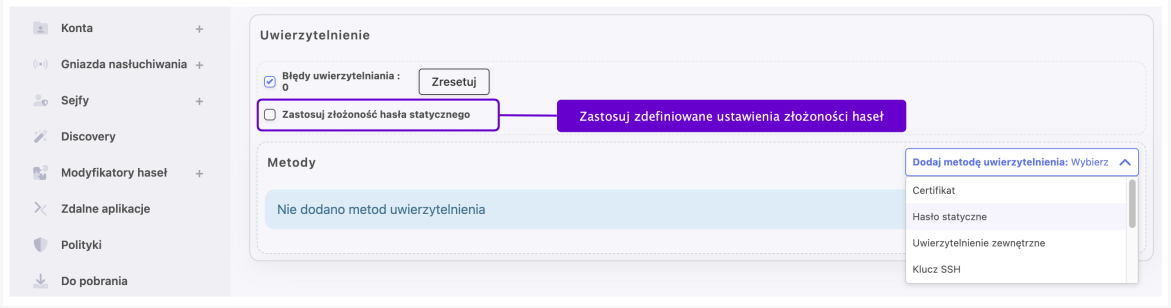
1. Wybierz *Ustawienia* > *Uwierzytelnienie*.
2. Przejdź do zakładki *Globalne* i wybierz *Niepowodzenia uwierzytelnienia*, aby ustawić licznik nieudanych logowań.
3. Przejdź do sekcji *Sesje* i ustaw kolejno zasady złożoności haseł:
   - Określ minimalną długość hasła.
   - Zaznacz *Małe litery* i określi 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*.

Uwaga

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 - User Directory*

12.5.3.4 Definicja uwierzytelniania OATH

Przejdź do strony *Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator*.

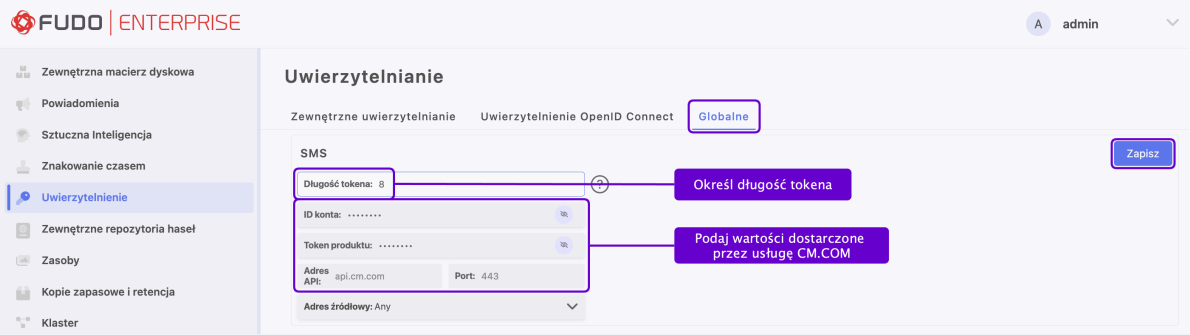
Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*

- *Integracja z serwerem CERB*

12.5.3.5 Definicja uwierzytelniania SMS

1. Wybierz *Ustawienia* > *Uwierzytelnienie* > zakładka *Globalne*.
2. Przejdź do sekcji *SMS*.



3. Wprowadź *Długość tokena*.

> **Uwaga**
>
> Długość tokena powinna mieścić się w zakresie 4-16.

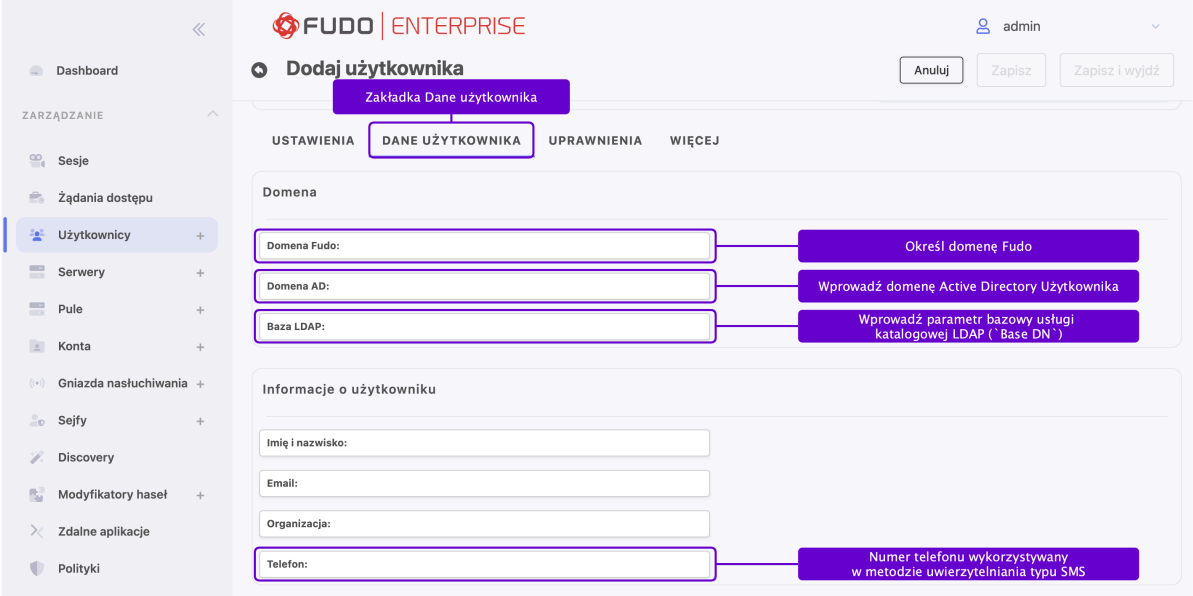
4. Wprowadź *ID konta*.
5. Wprowadź *Token produktu*.
6. Wprowadź *Adres API* oraz *Port*.

> **Uwaga**
>
> 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.

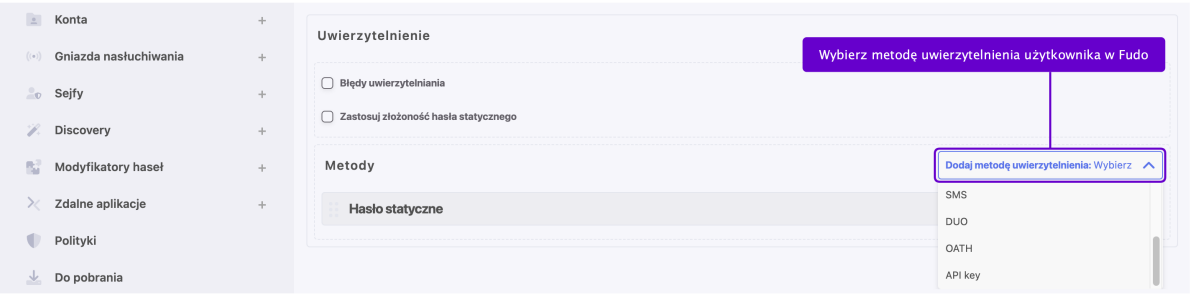
7. Wybierz *Adres źródłowy*.
8. Kliknij *Zapisz*.

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.

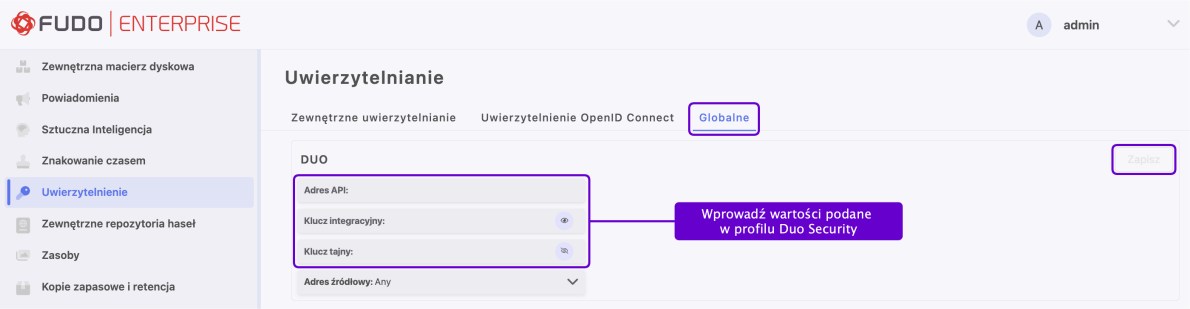
Tematy pokrewne:

- *Metody i tryby uwierzytelniania użytkowników*
- *Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)*
- *Przegląd systemu*
- *Integracja z serwerem CERB*

12.5.3.6 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* > *Uwierzytelnienie* > zakładka *Globalne*.

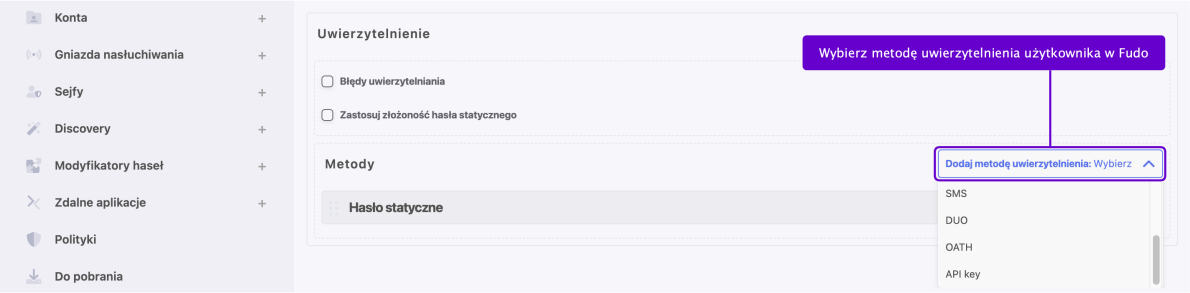
4. Przejdź do sekcji *DUO*.



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 uwierzytelnienie DUO.



10. W zakładce *Ustawienia*, w sekcji *Uwierzytelnienie*, 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*

12.5.3.7 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).

Uwaga

Aby uzyskać bardziej szczegółowe informacje na temat konfiguracji SSO z Active Directory, zapoznaj się ze scenariuszem użycia w rozdziale *Konfiguracja Single Sign On (SSO)*.

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.

Konfiguracja kontrolera domeny

1. Dodaj konto użytkownika, które będzie używane przez *Portal Użytkownika* lub *Panel Administracyjny* do komunikacji z domeną *yourdomain.local*.

Uwaga

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
```

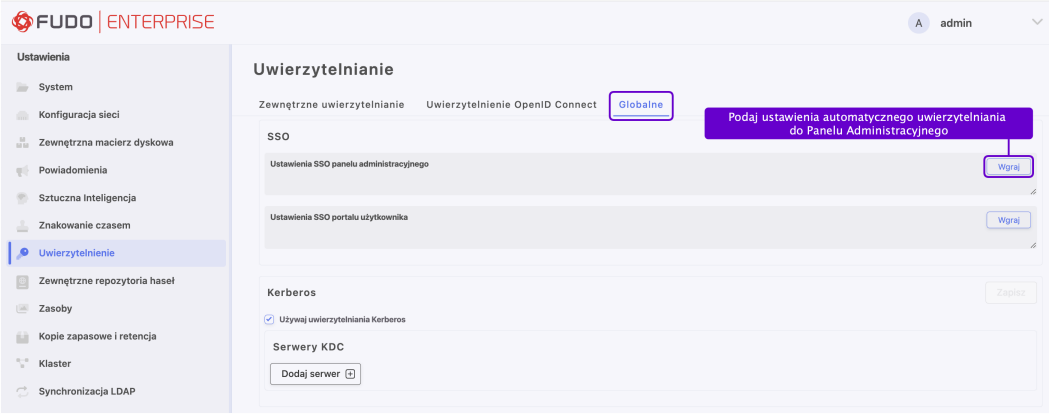
Single Sign On w Panelu Administracyjnym

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* > `*Uwierzytelnienie* > 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.



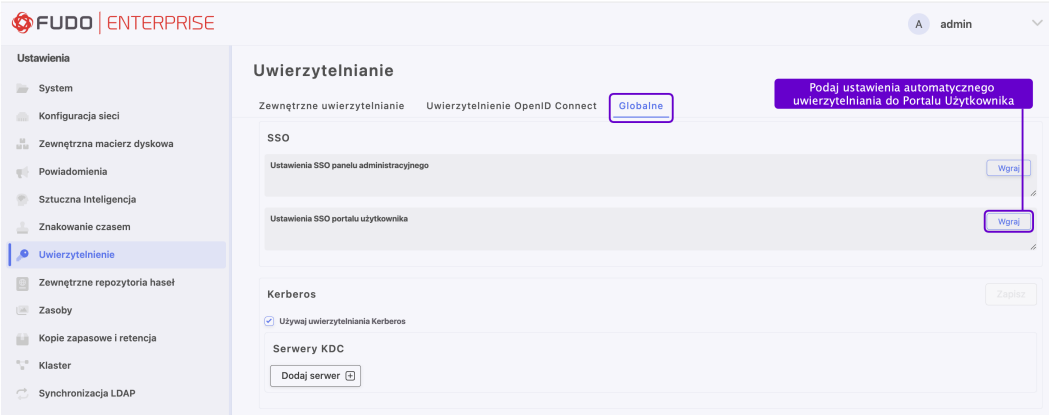
- Kliknij *Zapisz*.

Single Sign On w Portalu Użytkownika

Aby zdefiniować parametry usługi SSO w ustawieniach systemu, postępuj zgodnie z instrukcjami:

- Wybierz *Ustawienia* > `*Uwierzytelnienie* > 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 - User Directory*

12.5.3.8 Ustawienia uwierzytelniania Kerberos

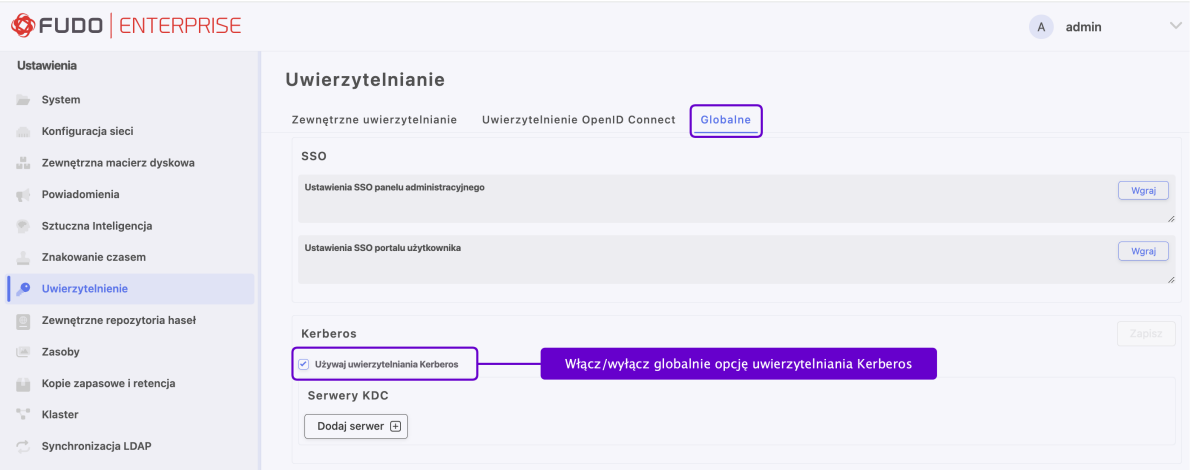
Uwaga

- 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 wyko-

rzystywany tylko wtedy, gdy wymagane jest przejście na uwierzytelnianie za pomocą LDAP.

Wyłączanie uwierzytelniania Kerberos

Aby **wyłączyć** obsługę uwierzytelniania Kerberos globalnie, wybierz *Ustawienia* > *Uwierzytelnienie*, przejdź do zakładki *Globalne* i odznacz opcję *Używaj uwierzytelniania Kerberos* w sekcji Kerberos.

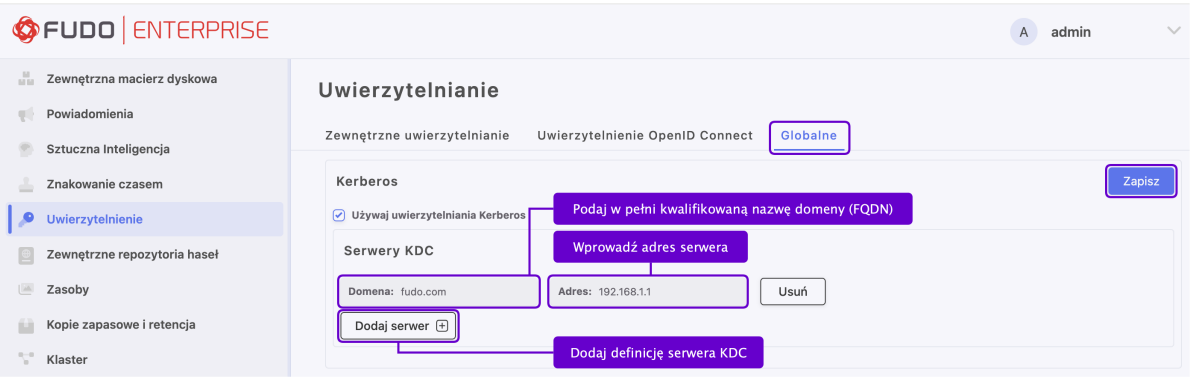


Dodawanie serwerów KDC

Fudo Enterprise wspiera konfigurację serwerów dystrybucji kluczy (Key Distribution Servers) oraz mapowanie domen na serwery KDC.

Aby dodać serwer KDC:

1. Wybierz *Ustawienia* > *Uwierzytelnienie* > 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*

12.6 Zewnętrzne repozytoria haseł

Fudo Enterprise wspiera zewnętrzne repozytoria haseł do zarządzania hasłami dostępowymi.

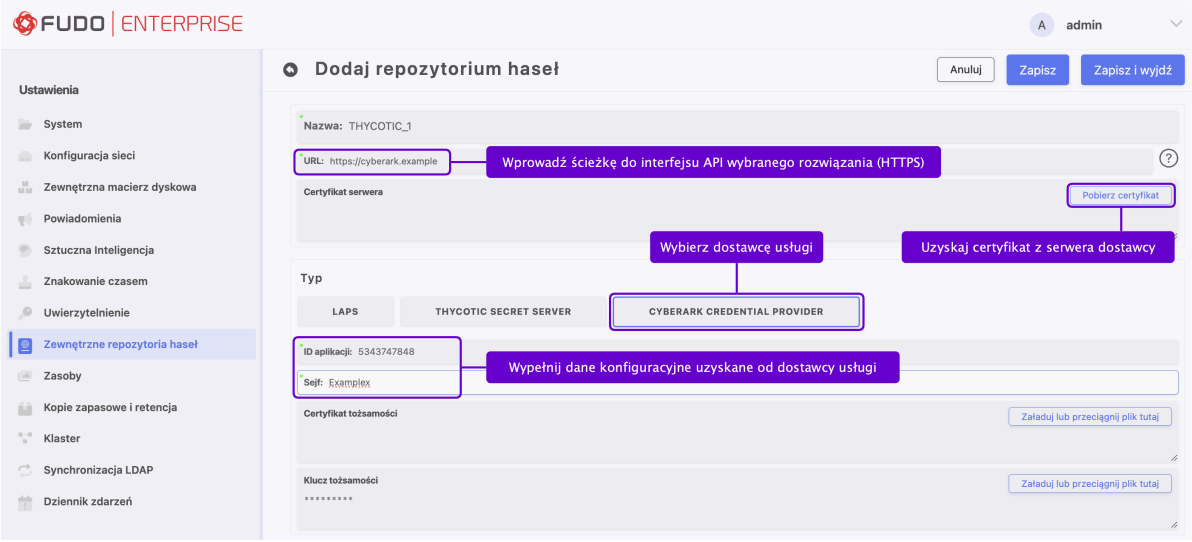
12.6.1 CyberArk Credential Provider

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.

Uwaga

Wyszukiwanie danego serwera/konta odbywa się w oparciu o następujące atrybuty *CyberArk Credential Provider*, które należy zdefiniować zgodnie z poniższymi zasadami:

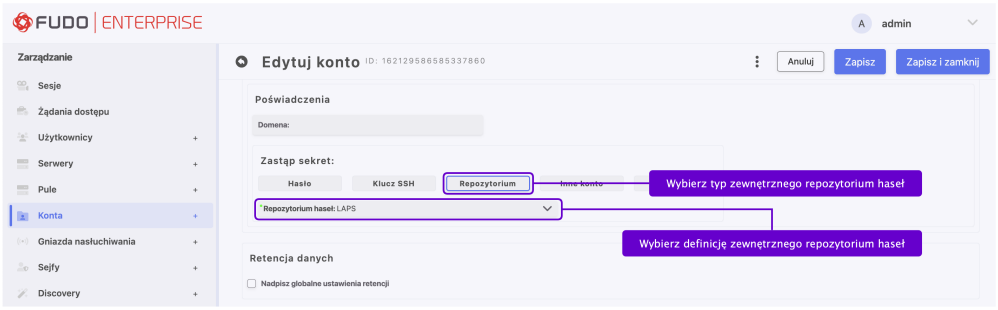
- `Address` - musi zgadzać się z adresem IP serwera Fudo (pole wymagane),
- `UserName` - musi zgadzać się z wartością pola *Login* podaną podczas tworzenia konta Fudo (pole wymagane) - patrz rozdział *Tworzenie konta typu regular*,
- `Safe` - musi zgadzać się z polem *Sejf* w utworzonym w Fudo zewnętrznym repozytorium haseł (pole opcjonalne).

9. W przypadku uwierzytelniania za pomocą certyfikatu klienta, należy zdefiniować pola *Certyfikat tożsamości* i *Klucz tożsamości*.

Uwaga

- 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*.

Uwaga

Nie można usunąć definicji repozytorium haseł, jeśli jest ona przypisana do jakiegokolwiek konta.

Tematy pokrewne:

- *Uwierzytelnienie*
- *Opis systemu*
- *Integracja z serwerem CERB*

12.6.2 Thycotic Secret Server

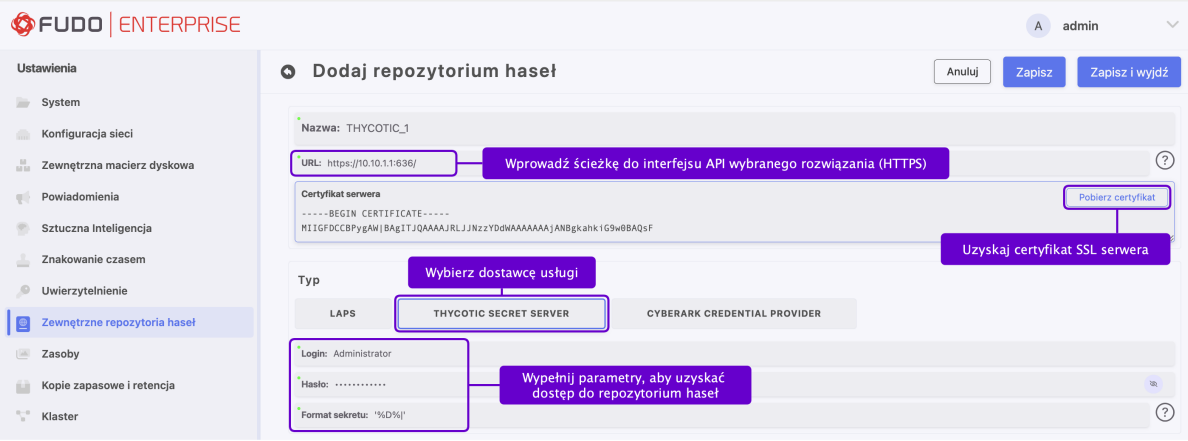
Dodawanie definicji repozytorium haseł

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.

Uwaga

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.

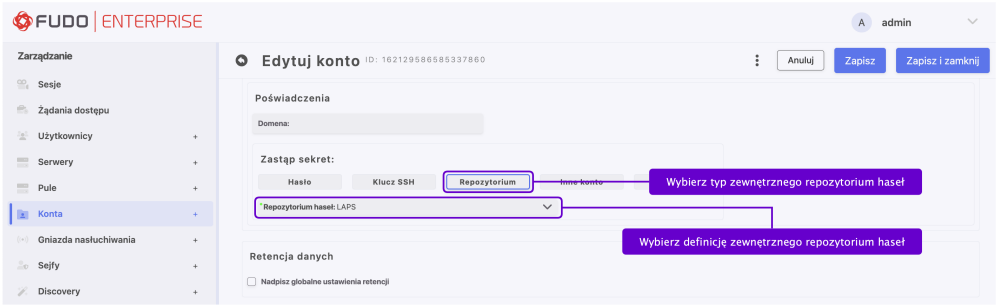


6. W sekcji *Typ* wybierz przycisk *THYCOTIC SECRET SERVER*.
7. W polu *Login* wprowadź nazwę użytkownika uprawionego do pobierania haseł.
8. W polu *Hasło* wprowadź hasło użytkownika uprawnionego do pobierania haseł.
9. W polu *Format sekretu* wprowadź ciąg znaków definiujący format identyfikatorów obiektów w systemie Thycotic Secret Server.

Uwaga

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*.

Uwaga

Nie można usunąć definicji repozytorium haseł, jeśli jest ona przypisana do jakiegokolwiek konta.

Tematy pokrewne:

- *Uwierzytelnienie*
- *Opis systemu*
- *Integracja z serwerem CERB*

12.6.3 Local Administrator Password Solutions (LAPS)

Uwaga

W niektórych środowiskach funkcjonalność LAPS może być niedostępna.

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

Uwaga

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.

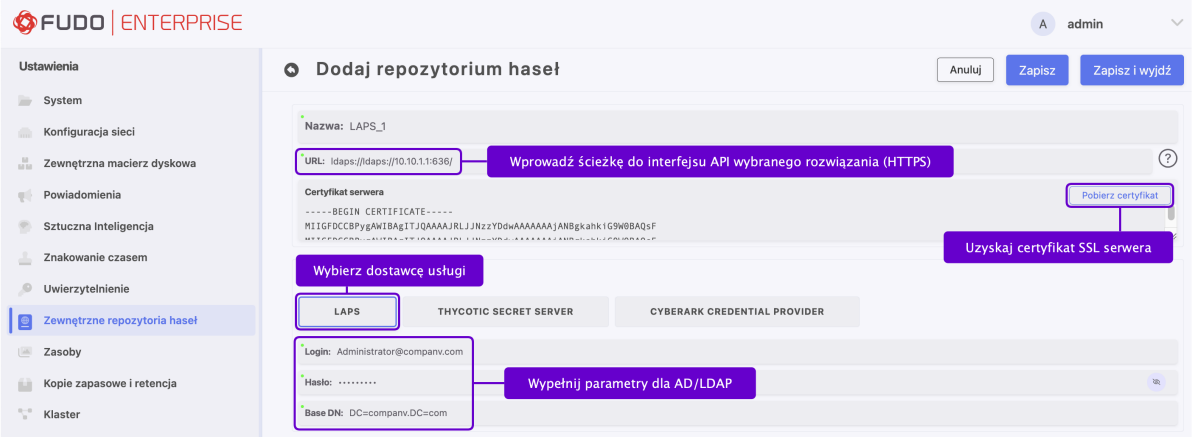
Uwaga

Obsługiwany format URL to `ldaps://<server>[:<port>]/` dla połączenia przez SSL.

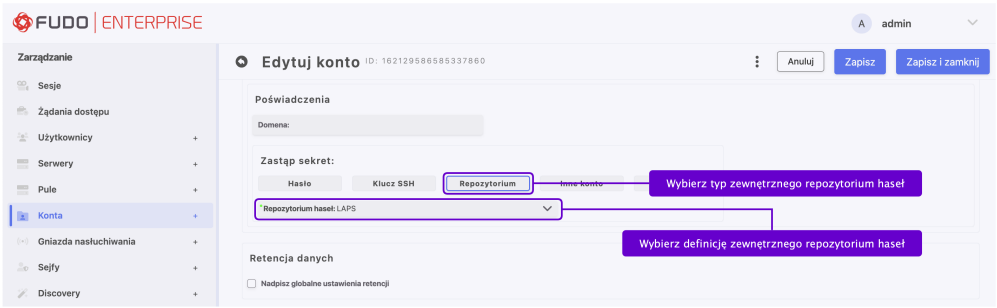
5. W polu *Certyfikat serwera* podaj certyfikat SSL lub kliknij przycisk *Pobierz certyfikat*, aby uzyskać go z serwera dostawcy.

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*.

Uwaga

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*.

Uwaga

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*

12.7 Zewnętrzna macierz dyskowa

Fudo Enterprise umożliwia retencjonowanie danych sesji na zewnętrznej macierzy dyskowej.

Uwaga

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.

12.7.1 Konfigurowanie zewnętrznej macierzy dyskowej

Aby skonfigurować zewnętrzną macierz dyskową, postępuj zgodnie z poniższą instrukcją.

1. Wybierz z lewego menu *Ustawienia* > *Zewnętrzna macierz dysków*.

Uwaga

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 .

Uwaga

Kliknij ikonę , aby odświeżyć listę dostępnych obiektów WWN.

4. Kliknij *Zapisz* i przejdź do konfigurowania *retencji danych*.

12.7.2 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*.

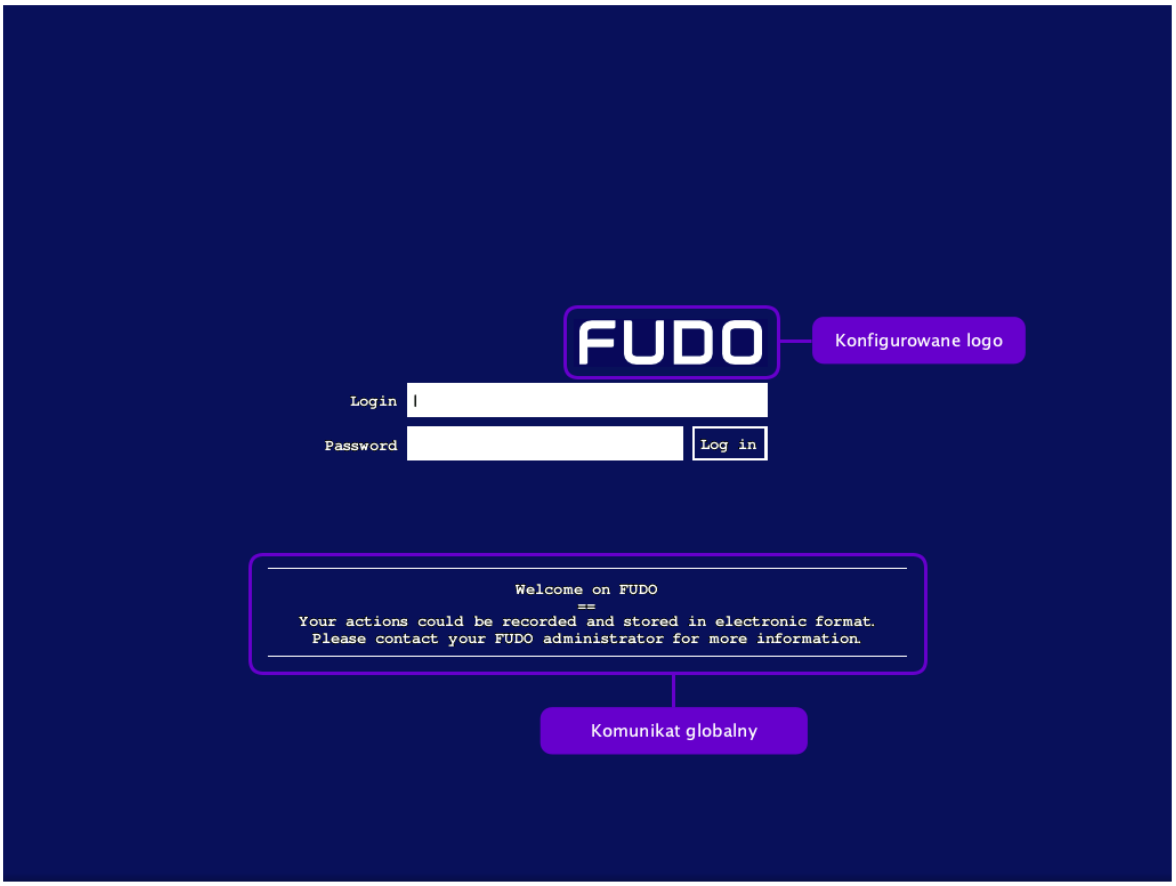
Tematy pokrewne:

- *Kopia zapasowa danych sesji*

12.8 Zasoby

12.8.1 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.

Uwaga

Maksymalny rozmiar obrazu to 512 x 512 px.

4. Wprowadź tekst *Komunikatu globalnego*, który ma się pojawić jako wiadomość na ekranie logowania.

Uwaga

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.

> **Uwaga**
>
> 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.

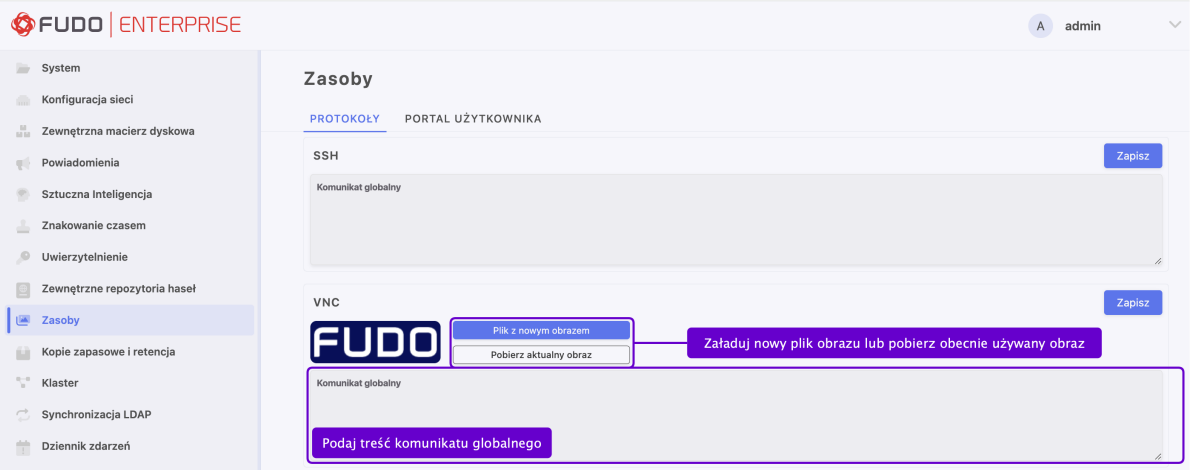
Uwaga

Maksymalny rozmiar obrazu to 512 x 512 px.

4. Wprowadź tekst *Komunikatu globalnego*, który ma się pojawić jako wiadomość na ekranie logowania.

Uwaga

Komunikat na ekranie logowania może mieć cztery linie, do 120 znaków.



5. Kliknij *Zapisz*.

Tematy pokrewne:

- *Szybki start - RDP*

12.8.2 Konfiguracja *Portalu użytkownika*

12.8.2.1 Konfiguracja ekranu logowania

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*.

Uwaga

Maksymalny rozmiar obrazu to 5 MB.

4. Wprowadź treść komunikatu wyświetlanego na ekranie logowania.

Uwaga

Komunikat na ekranie logowania może mieć cztery linie, do 120 znaków.

5. Uzupełnij pole *Informacje o sprzedawcy*.

Uwaga

Informacje o sprzedawcy mogą mieć pięć linii, do 70 znaków.

6. Uzupełnij dane kontaktowe do działu wsparcia technicznego.

Uwaga

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.

Uwaga

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.*

12.8.2.2 Definiowanie układu klawiatury

Administratorzy mogą globalnie definiować domyślny układ klawiatury dla Portalu Użytkownika:

1. Wybierz *Ustawienia* > *Zasoby.*
2. Przejdź do zakładki *PORTAL UŻYTKOWNIKA.*

Uwaga

Każdy użytkownik może dostosować układ klawiatury indywidualnie w Portalu Użytkownika.

Tematy pokrewne:

- *Portal Użytkownika*

12.9 Kopia zapasowa i retencja

12.9.1 Kopia zapasowa danych sesji

Ostrzeżenie

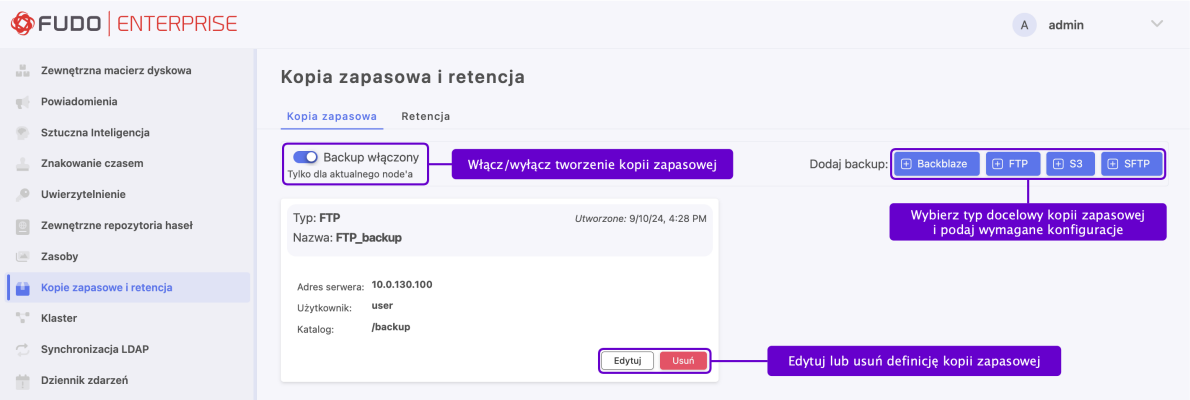
Kopia zapasowa danych sesji zawiera informacje poufne.

Fudo Enterprise pozwala na konfigurację wielu docelowych miejsc przechowywania kopii zapasowych danych sesji. Mogą to być zewnętrzne repozytoria na S3, Backblaze, FTP lub SFTP.

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

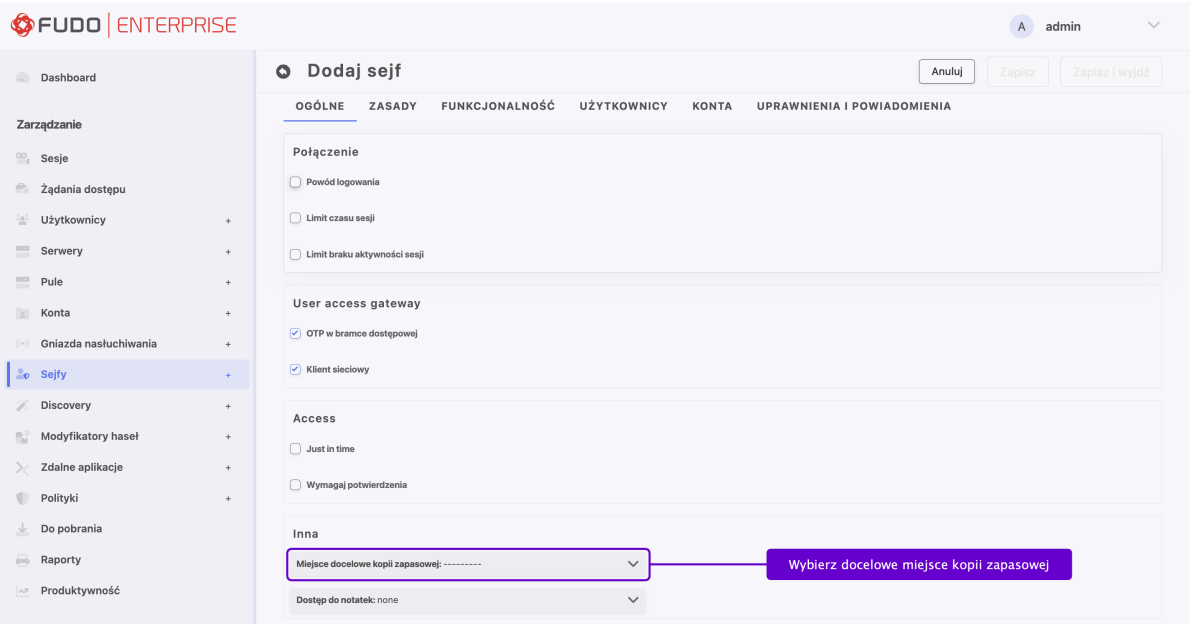
1. Wybierz *Ustawienia* > *Kopia zapasowa i retencja.*
2. Wybierz opcję *Kopia zapasowa włączona.* Należy pamiętać, że w przypadku skonfigurowanego klastra opcja ta włącza kopię zapasową tylko dla bieżącego węzła.
3. W polu *Dodaj miejsce docelowe* kliknij przycisk typu repozytorium, aby skonfigurować 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*.

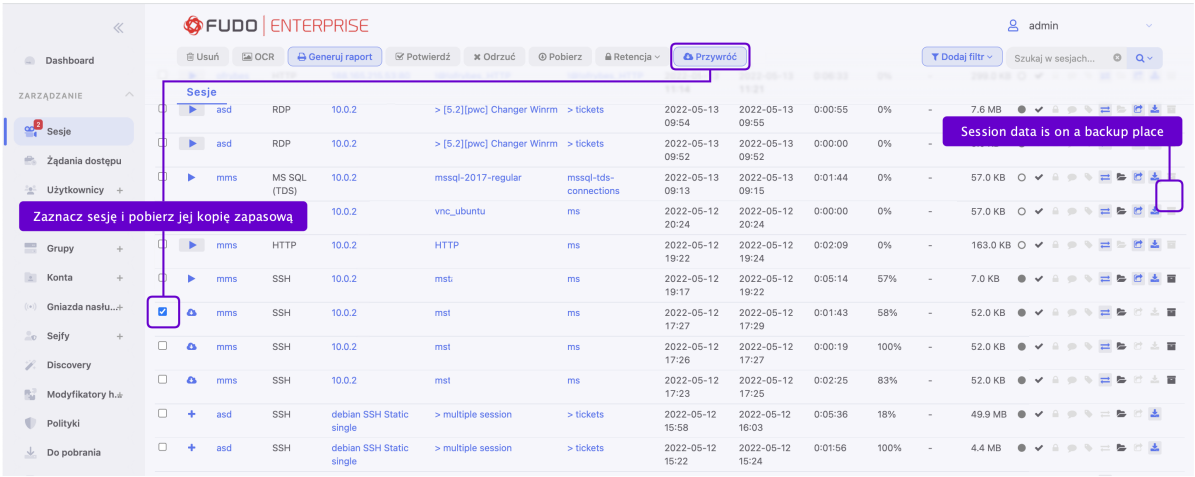
Skonfigurowane miejsce docelowe kopii zapasowej może też zostać dodane w ustawieniach Sejfu, aby dane sesji były przechowywane automatycznie.



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*

12.9.2 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*.

Uwaga

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.

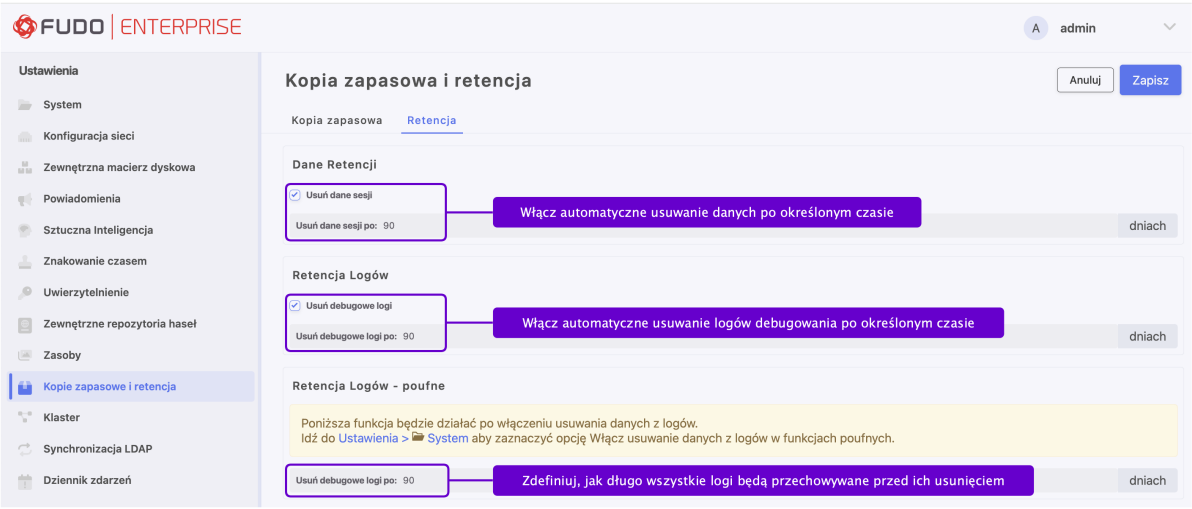
Włączenie retencji danych

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*

12.10 Konfiguracja klastrowa

12.10.1 Replikacja danych sesji i zachowanie w przypadku awarii węzła

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*.

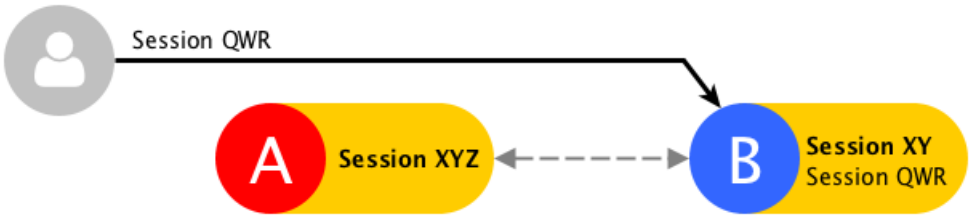
Dane bieżącej sesji są replikowane w trakcie jej trwania.



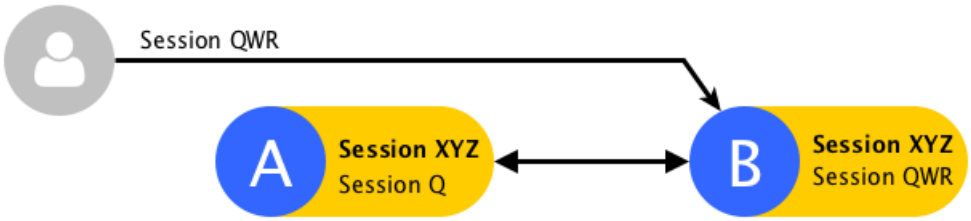
W przypadku, gdy węzeł ulegnie awarii, bieżące sesje zostaną zerwane...



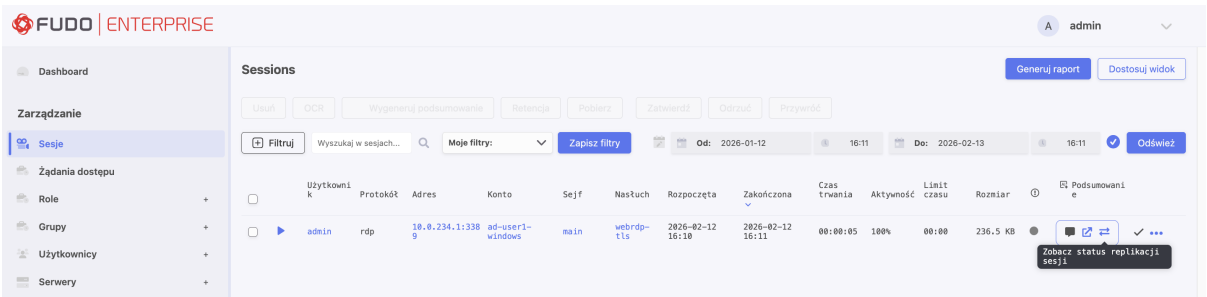
...a użytkownicy będą musieli ponownie nawiązać połączenie.

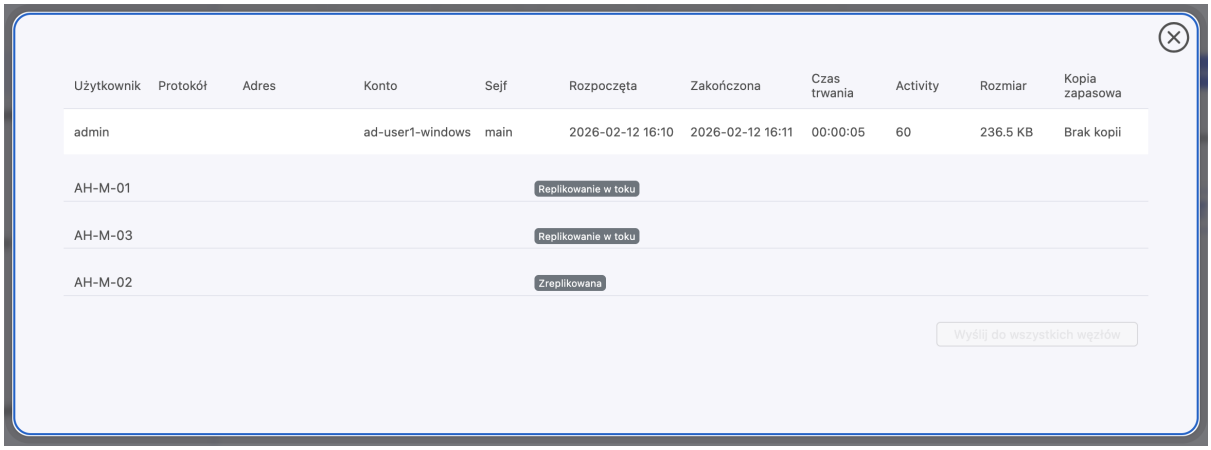


Część danych sesji, która została zreplikowana zanim miała miejsce awaria, jest dostępna na pozostałych węzłach klastra. Pełen zapis będzie dostępny po przywróceniu działania węzła i zsynchronizawaniu danych.



Stan replikacji danych sesji można zweryfikować klikając ikonę ⇄ na liście sesji.





Tematy pokrewne:

- *Inicjowanie klastra*
- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Grupy redundancji*

12.10.2 Inicjowanie klastra

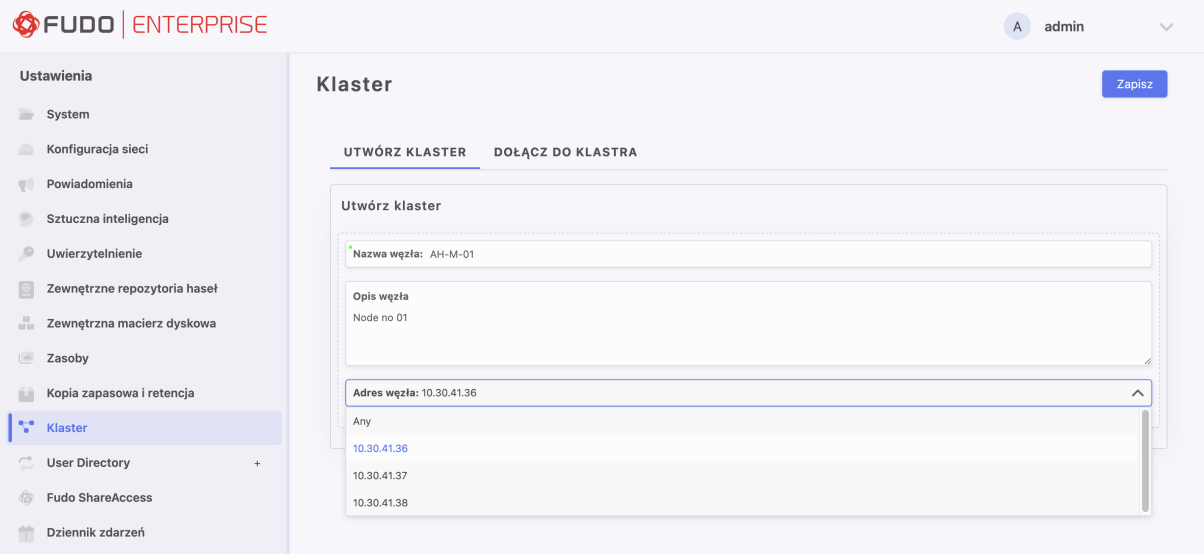
Proces inicjowania klastra rozpoczyna się na pierwszym węźle (instancji Fudo Enterprise), który staje się **węzłem inicjalnym**. W trakcie inicjalizacji tworzona jest konfiguracja klastra, a dane z węzła inicjalnego są replikowane na kolejne węzły dołączane do klastra.

Ostrzeżenie

- Prawidłowe działanie klastra wymaga skonfigurowania *serwera czasu NTP* na wszystkich węzłach klastra. Zaleca się wskazanie **tych samych serwerów NTP** w całym klastrze w celu zapewnienia spójności czasu systemowego.
- Przed inicjacją klastra należy zweryfikować, czy zainstalowana **licencja umożliwia pracę w trybie klastrowym**. Limit liczby węzłów określony w licencji musi być większy lub równy planowanej liczbie węzłów w klastrze.
- Należy zapewnić **komunikację sieciową** pomiędzy węzłami na porcie `65522` (ruch między adresami przeznaczonymi do komunikacji klastrowej).

Aby zainicjować klaster Fudo Enterprise, postępuj zgodnie z poniższą instrukcją.

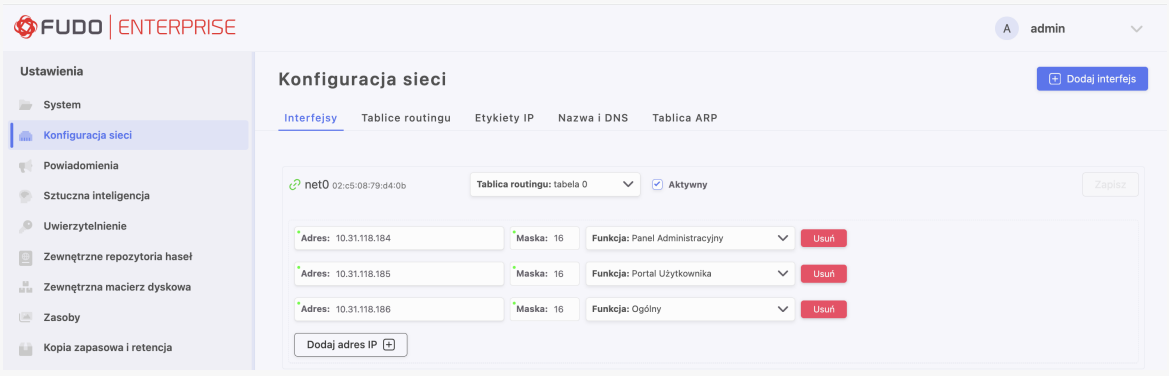
1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Przejdź do zakładki *UTWÓRZ KLASTER*.



3. Wprowadź nazwę dla tworzonego węzła oraz opis ułatwiający jego identyfikację - sugerujący, że to będzie **węzeł inicjalny**.
4. Z listy rozwijalnej *Adres węzła* wybierz adres IP, który będzie wykorzystywany do komunikacji z innymi węzłami.

Uwaga

- W poniższym przykładzie wskazany jest ten sam adres IP, który wykorzystywany jest przez Panel Administracyjny. Adres komunikacji klastrowej może jednak należeć do innej podsieci i być przypisany do innego interfejsu.
- Adres komunikacji klastrowej musi mieć ustawioną funkcję *Ogólny* w *ustawieniach sieciowych*.



5. Kliknij *Zapisz*, aby zainicjować klaster.

Uwaga

Kolejnym krokiem konfiguracji środowiska klastrowego jest dodanie kolejnych węzłów do klastra. Przejdź do rozdziału *Dodawanie węzłów klastra*.

Tematy pokrewne:

- *Edytowanie węzłów klastra*

- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*
- *Grupy redundancji*
- *Konfiguracja klastrowa*

12.10.3 Dodawanie węzłów klastra

Dodanie nowego węzła do istniejącego klastra powoduje jego pełną synchronizację z węzłem inicjalnym. Proces ten obejmuje wyczyszczenie danych lokalnych oraz odtworzenie konfiguracji i danych na podstawie informacji zreplikowanych z klastra.

Ostrzeżenie

- Obiekty modelu danych: *sejfy*, *użytkownicy*, *serwery*, *konta* i *gniazda nasłuchiwania* są replikowane w ramach klastra i **nie należy dodawać ich ręcznie** na każdym z węzłów. W przypadku problemów z replikacją danych, skontaktuj się z działem wsparcia technicznego.
- Dane sesji oraz parametry konfiguracyjne (*serwery*, *użytkownicy*, *konta*, *sejfy*, *gniazda nasłuchiwania*, *zewnętrzne serwery uwierzytelniania*) węzła dołączanego do klastra **są usuwane**. Po dołączeniu węzeł zostaje zainicjowany danymi zreplikowanymi z klastra.
- W przypadku środowisk zawierających dużą ilość danych proces inicjalizacji i kopiowania danych na dołączany węzeł **może trwać kilka godzin**.

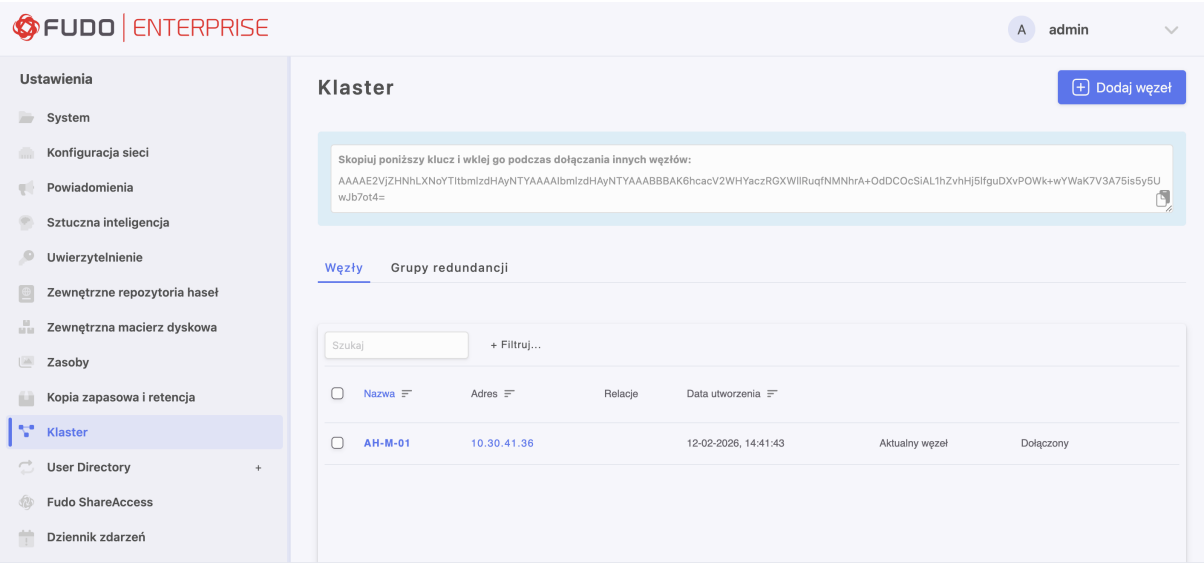
Niebezpieczeństwo

- Mechanizm dołączania węzła do klastra **polega na całkowitym wyczyszczeniu jego danych** oraz skopiowaniu danych z węzła, na którym klaster został zainicjowany.
- Nieprawidłowa konfiguracja relacji między węzłami lub pominięcie któregokolwiek z kroków procedury może doprowadzić do nieodwracalnego uszkodzenia dołączanego węzła. W takim przypadku proces synchronizacji nie zostanie ukończony.
- Niektóre elementy konfiguracji (np. SMTP) nie są replikowane pomiędzy węzłami klastra i wymagają ręcznej konfiguracji na każdym węźle.

12.10.3.1 Inicjacja klastra i dodanie węzłów

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

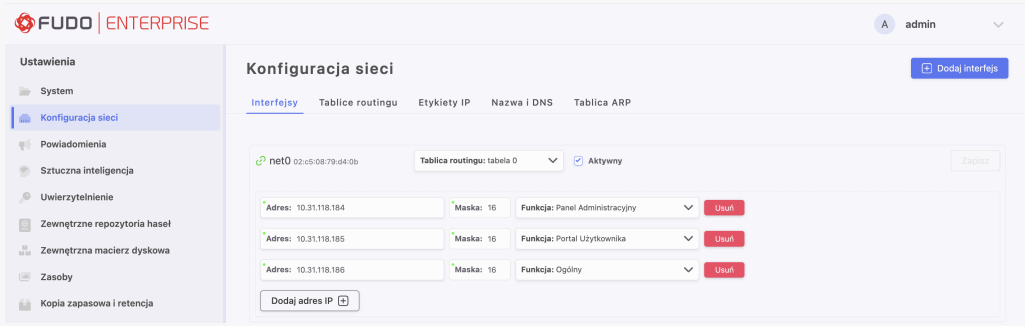
1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise, na którym został *zainicjowany klaster*, czyli **węźle inicjalnym**.
2. Wybierz z lewego menu *Ustawienia* > *Klaster*.
3. Kliknij *Dodaj węzeł*.

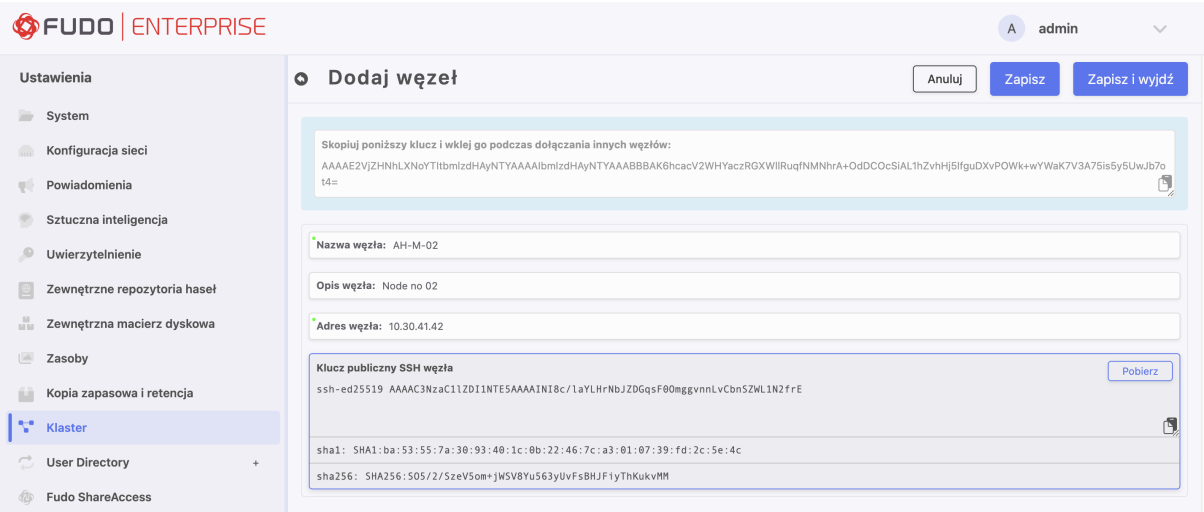


4. Wprowadź nazwę węzła oraz opis, ułatwiający identyfikację węzła.
5. Podaj adres IP dołączanego węzła (czyli instancji Fudo Enterprise, na którą zostaną zreplikowane dane z węzła inicjalnego).

Uwaga

Adres dołączanego węzła musi mieć ustawioną funkcję *Ogólny* w ustawieniach sieciowych. Więcej na temat konfigurowania ustawień sieciowych znajdziesz w rozdziale *Konfiguracja ustawień sieciowych*.





6. Kliknij *Pobierz* aby pobrać klucz publiczny SSH węzła.
7. Kliknij *Zapisz i wyjdź*.
8. Powtórz kroki od 3 do 7, jeśli chcesz dodać kolejne węzły.

Uwaga

W scenariuszach, w których używane są modyfikatory haseł, do ich działania wymagane są co najmniej dwa aktywne węzły klastra. W środowisku dwuwęzłowym awaria jednego węzła powoduje zatrzymanie działania modyfikatorów haseł, dlatego zalecana jest konfiguracja **trzech węzłów**.

12.10.3.2 Ustawianie relacji pomiędzy węzłami

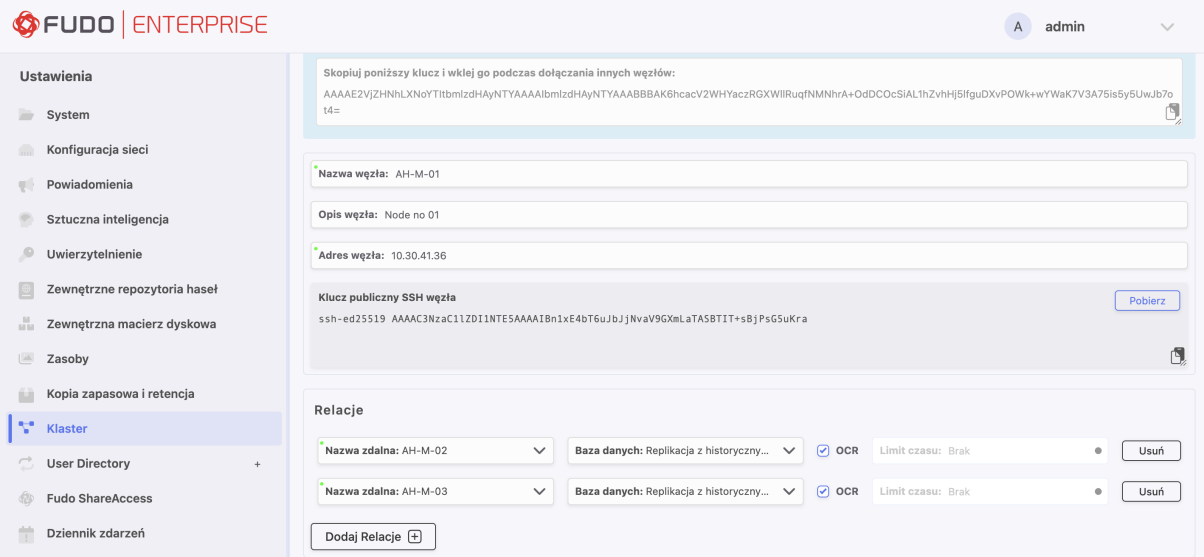
Uwaga

- Zalecaną konfiguracją klastra jest definiowanie dwukierunkowych relacji pomiędzy węzłami. Nie jest wymagane konfigurowanie relacji pomiędzy każdą parą węzłów, jednak żaden węzeł nie może pozostawać bez co najmniej jednej zdefiniowanej relacji.
- W topologii, w której węzły nie są połączone w układzie „full mesh" (każdy węzeł połączony z każdym), należy pamiętać o ograniczeniach dotyczących replikacji danych sesji. W takiej konfiguracji dane sesji są replikowane wyłącznie pomiędzy węzłami, pomiędzy którymi zdefiniowano relację.

Ostrzeżenie

Utworzenie relacji jest kluczowe do tego, by dane zostały zreplikowane pomiędzy węzłami.

1. Kliknij na nazwę pierwszego węzła, aby go edytować.
2. W sekcji *Relacje* edytowanego węzła, kliknij przycisk *Dodaj Relacje +*.
3. Z listy *Nazwa zdalna* wybierz węzeł, na który replikowane będą dane z węzła, na którym jesteśmy aktualnie zalogowani (w tym przypadku jest to węzeł główny).
4. Z listy *Baza danych* wybierz, jakie dane mają podlegać replikacji na wybrany węzeł klastra.
5. Zaznacz opcję *OCR*, aby wybrany węzeł przetwarzał nadwyżkę sesji graficznych.
6. Kliknij *Zapisz i wyjdź*.
7. Edytuj kolejne węzły i dodaj relacje do pozostałych węzłów w klastrze w sposób opisany powyżej.

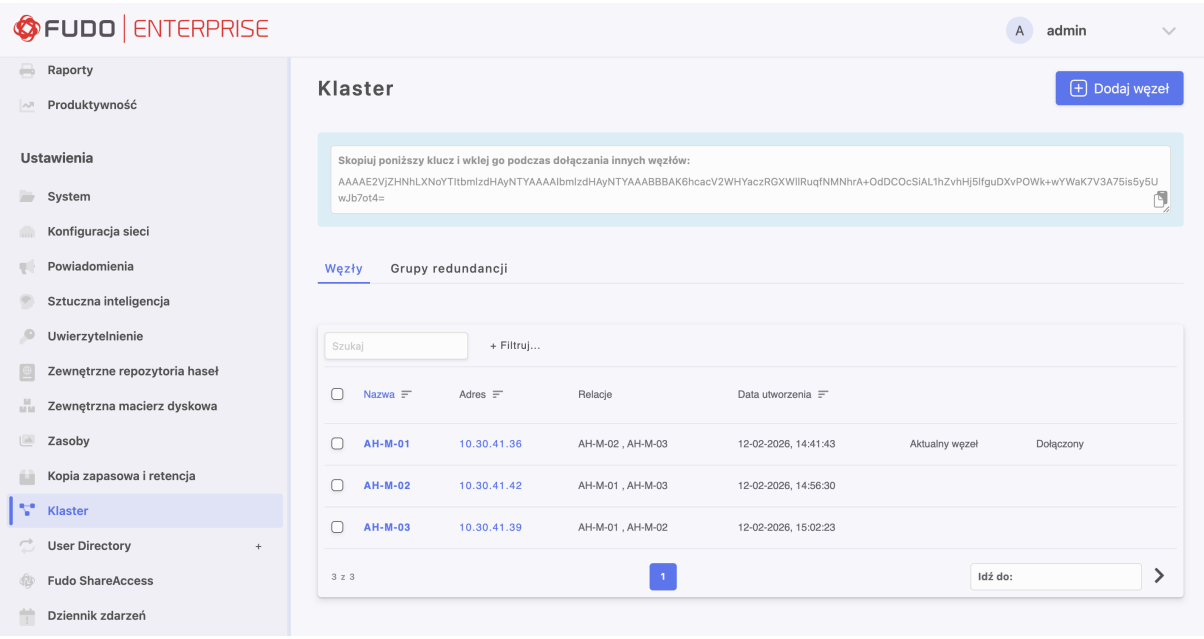


Uwaga

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.

12.10.3.3 Powiązanie węzłów z węzłem inicjalnym

1. Upewni się, że jesteś w Panelu Administracyjnym Fudo Enterprise, na którym został zainicjowany klaster.
2. Przejdź do widoku głównego zakładki *Klaster*.
3. Skopiuj klucz publiczny klastra.



4. Zaloguj się do Panelu Administracyjnego dołączanego węzła.

Uwaga

Możesz użyć skrótu, klikając adres wybranego węzła na liście dodanych węzłów w widoku klastra.

5. Wybierz z lewego menu *Ustawienia* > *Klaster*.
6. Przejdź do zakładki *DOŁĄCZ DO KLASTRA*.



7. Wklej skopiowany klucz w oknie *Klucz publiczny SSH klastra*.
8. Kliknij *Zapisz*.

Ostrzeżenie

Po zaakceptowaniu ostrzeżenia o wymazaniu danych wszystkie dane na tym węźle zostaną usunięte.

9. Przeczytaj komunikat o wymazaniu danych z tego węzła i kliknij *Rozumiem konsekwencje. Kontynuuj*.
10. Poczekaj, aż klaster zostanie zainicjalizowany i obiekty zostaną skopiowane pomiędzy węzłami klastra.

Uwaga

Dodawany węzeł zostanie zrestartowany. Jeśli wykorzystywane jest szyfrowanie dysków (klucz USB lub hasło), to należy odpowiednio podłączyć klucz lub podać hasło z poziomu terminala hypervisor'a.

12.10.3.4 Weryfikacja zakończenia inicjalizacji klastra

Czas trwania inicjalizacji klastra zależy od ilości danych na węźle inicjalnym. W przypadku nowej, nieużywanej instancji proces może potrwać kilka minut. W środowiskach zawierających dużą ilość danych (np. logi, nagrania sesji) inicjalizacja może trwać od kilku godzin do kilku dni.

Po zakończeniu replikacji należy zalogować się na nowo dodanym węźle i zweryfikować poprawność synchronizacji poprzez:

- sprawdzenie statusu węzłów klastra na Dashboardzie,
- analizę dziennika zdarzeń,
- weryfikację ustawień klastrowych.

Dodatkowo zaleca się potwierdzenie replikacji danych konfiguracyjnych (np. użytkowników, serwerów) poprzez kontrolę odpowiednich zakładek w interfejsie administracyjnym.

Zakończenie początkowej replikacji jest potwierdzane wpisami w logach na węźle inicjalnym (tym, na którym utworzono klaster):

- `Initial objects replication to cluster node <name> completed.`
- `Initial logs replication to cluster node <name> completed.`

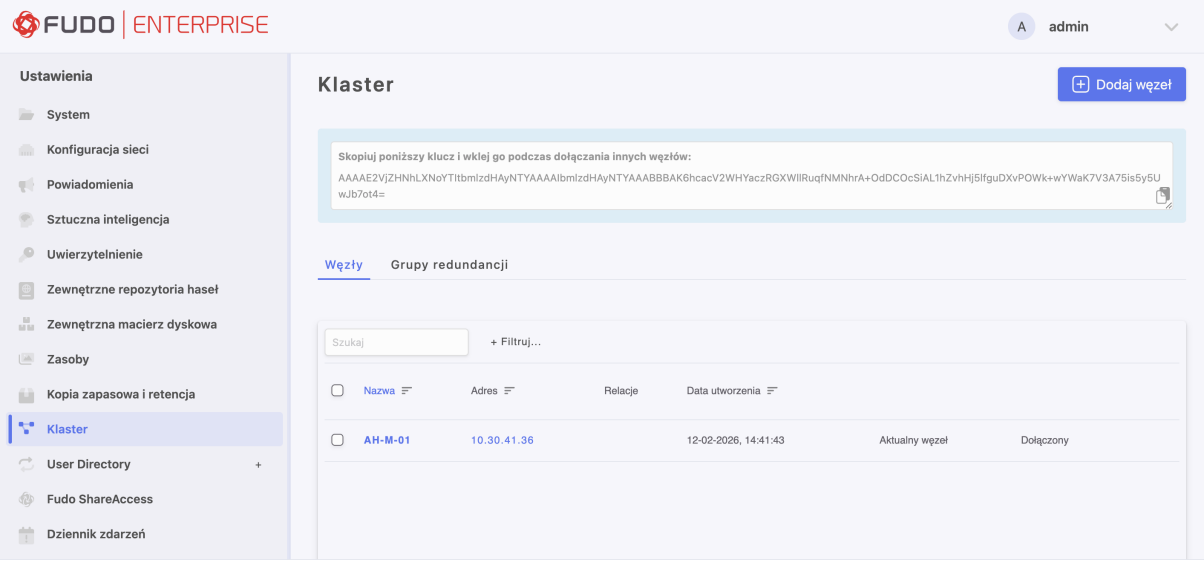
Tematy pokrewne:

- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

12.10.4 Rozbudowa klastra o nowe węzły

> **Uwaga**
>
> Rozbudowa klastra wymaga przeprowadzenia procedury ściśle według poniższych kroków.

1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise, na którym został *zainicjowany klaster* - czyli **węzła głównego**.
2. Wybierz z lewego menu *Ustawienia* > *Klaster*.
3. Kliknij *Dodaj węzeł*.

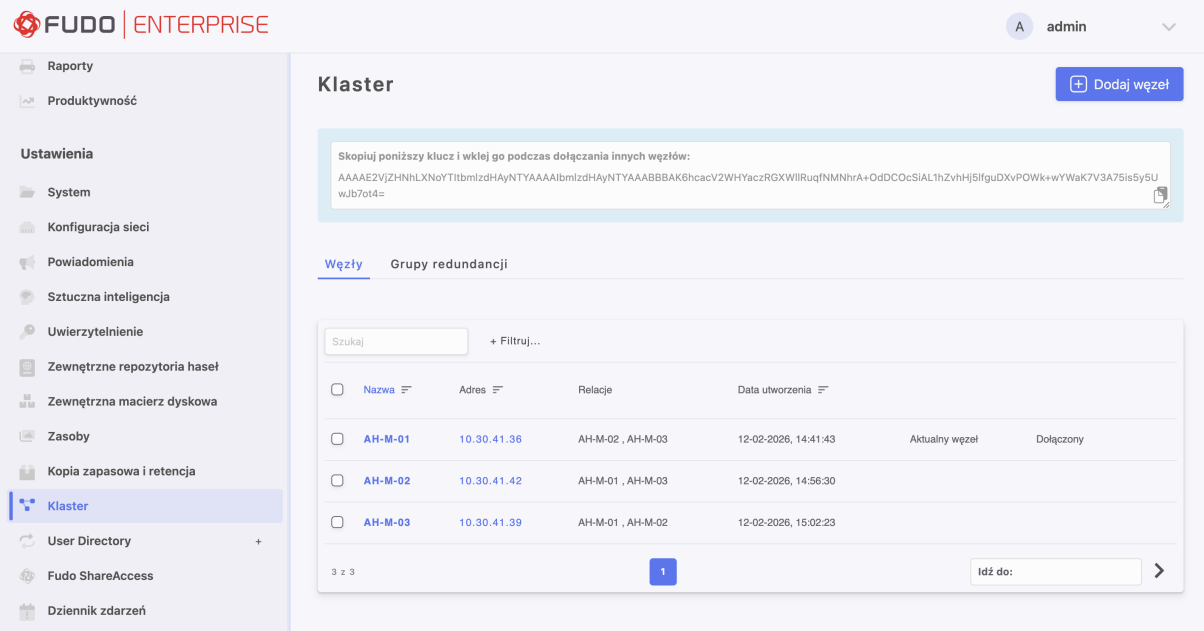


4. Wprowadź nazwę węzła oraz opis, ułatwiający identyfikację dołączanego węzła.
5. Podaj adres IP dołączanego węzła.

Uwaga

Adres dołączanego węzła musi mieć ustawioną funkcję *Ogólny* w *ustawieniach sieciowych*. Więcej na temat konfigurowania ustawień sieciowych znajdziesz w rozdziale *Ustawienia sieci: Konfiguracja interfejsów sieciowych*.

6. Kliknij *Pobierz* aby pobrać klucz publiczny SSH węzła.
7. Kliknij *Zapisz*.
8. Dodaj relacje między pozostałymi węzłami (zalecane jest dodanie relacji ze wszystkimi węzłami).
9. Edytuj każdy z pozostałych węzłów klastra i dodaj relację z nowo dodanym węzłem (zalecane jest dodanie relacji w wariancie „każdy z każdym").
10. Kliknij *Zapisz i zamknij*.
11. Przejdź do widoku głównego zakładki *Klaster*.
12. Skopiuj klucz publiczny klastra.



13. Zaloguj się do Panelu Administracyjnego dołączanego węzła.
14. Wybierz z lewego menu *Ustawienia* > *Klaster*.
15. Przejdź do zakładki *DOŁĄCZ DO KLASTRA*.



16. Wklej skopiowany klucz w oknie *Klucz publiczny SSH klastra*.
17. Kliknij *Zapisz*.

Ostrzeżenie

Po zaakceptowaniu ostrzeżenia o wymazaniu danych wszystkie dane na tym węźle zostaną usunięte.

18. Przeczytaj komunikat o wymazaniu danych z tego węzła i kliknij *Rozumiem konsekwencje. Kontynuuj.*
19. Poczekaj, aż klaster zostanie zainicjalizowany i obiekty zostaną skopiowane pomiędzy węzłami klastra.

Uwaga

Dodawany węzeł zostanie zrestartowany. Jeśli wykorzystywane jest szyfrowanie dysków (klucz USB lub hasło), to należy odpowiednio podłączyć klucz lub podać hasło z poziomu terminala hypervisor'a.

Tematy pokrewne:

- *Inicjowanie klastra*
- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

12.10.5 Edytowanie węzłów klastra

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

1. Wybierz z lewego menu *Ustawienia* > *Klaster*.
2. Na liście węzłów znajdź węzeł, który zamierzasz edytować i kliknij na jego nazwę.
3. Zmodyfikuj dane węzła według potrzeb.
4. Kliknij *Zapisz*.

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

12.10.6 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.
- Tak odłączonego węzła **NIE WOLNO** ponownie dodawać/podłączać do klastra.

Niebezpieczeństwo

W przypadku konieczności usunięcia węzła zalecamy kontakt z **Działem Wsparcia Technicznego Fudo** przed rozpoczęciem prac.

12.10.6.1 Usuwanie węzła z klastra

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

1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise.
2. Wybierz z lewego menu *Ustawienia* > *Klaster*.
3. Na liście węzłów znajdź węzeł, który zamierzasz usunąć.
4. Zaznacz opcję *Usuń* przy wybranym węźle klastra.
5. Kliknij *Zapisz*.

12.10.6.2 Ponowne dołączanie usuniętego węzła

Ostrzeżenie

Jeśli jest konieczność ponownego podłączenia usuniętego węzła do klastra, węzeł należy **zresetować do ustawień fabrycznych** z poziomu terminala zgodnie z procedurą *Przywracanie ustawień fabrycznych*, a dopiero potem dołączyć na nowo do klastra zgodnie z instrukcją *Dodawanie węzłów klastra*.

Tematy pokrewne:

- *Dodawanie węzłów klastra*
- *Edytowanie węzłów klastra*
- *Inicjowanie klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

12.10.7 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.

Uwaga

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*.
4. Zdefiniuj parametry grupy:
    - **Nazwa** - nazwa tworzonej grupy redundancji.

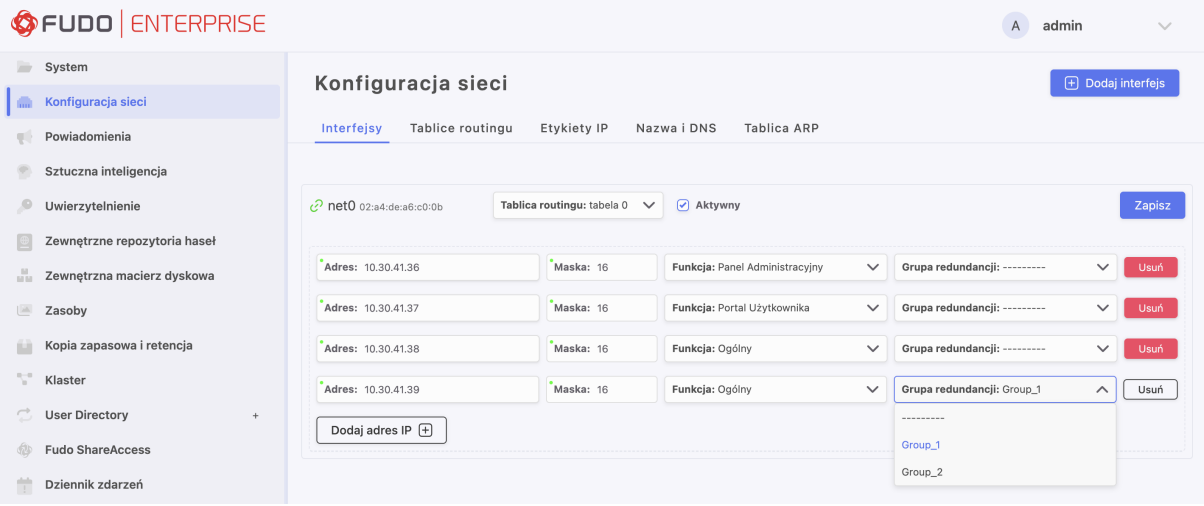
- **ID** - identyfikator grupy redundancji (dozwolony zakres: 1–255).
- **Priorytet** - priorytet grupy redundancji (dozwolony zakres: 0-254). Niższa wartość parametru oznacza wyższy priorytet.
- **Interfejs sieciowy** - interfejs sieciowy używany przez grupę redundancji do komunikacji z pozostałymi węzłami klastra.

Uwaga

- 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 *interlink*) służy do monitorowania stanu danej grupy redundancji. Węzeł główny wysyła pakiety *keep-alive* w sieci warstwy 2, informując pozostałe węzły o tym, że jest aktywny i działa prawidłowo. Pozostałe węzły klastra nasłuchują tych pakietów za pośrednictwem interfejsu *interlink*.
- Interfejsy *interlink* wszystkich węzłów klastra muszą być podłączone do tej samej domeny rozgłoszeniowej (VLAN). Dodatkowo, w środowiskach opartych na VMware, należy dostosować ustawienia zabezpieczeń *vSwitcha*, aby zezwolić na zmiany adresów MAC i przesyłanie sfałszowanych ramek (*forged transmits*).
- Domyślnie, przypisanie roli *master* do węzła działa na zasadzie czasu nieokreślonego.



5. Kliknij *Zapisz i wyjdź*.
6. Wybierz z lewego menu *Ustawienia* > *Konfiguracja sieci*.
7. Kliknij *Dodaj adres IP* +, aby dodać adres IP.
8. Wprowadź adres IP i wybierz funkcję *Ogólny*, aby nadać mu atrybut klastrowy.
9. Z listy rozwijalnej wybierz wcześniej zdefiniowaną grupę redundancji.
10. Kliknij *Zapisz*.



Uwaga

Klastrowy adres IP należy zdefiniować na każdym z węzłów klastra.

Edytowanie grup redundancji

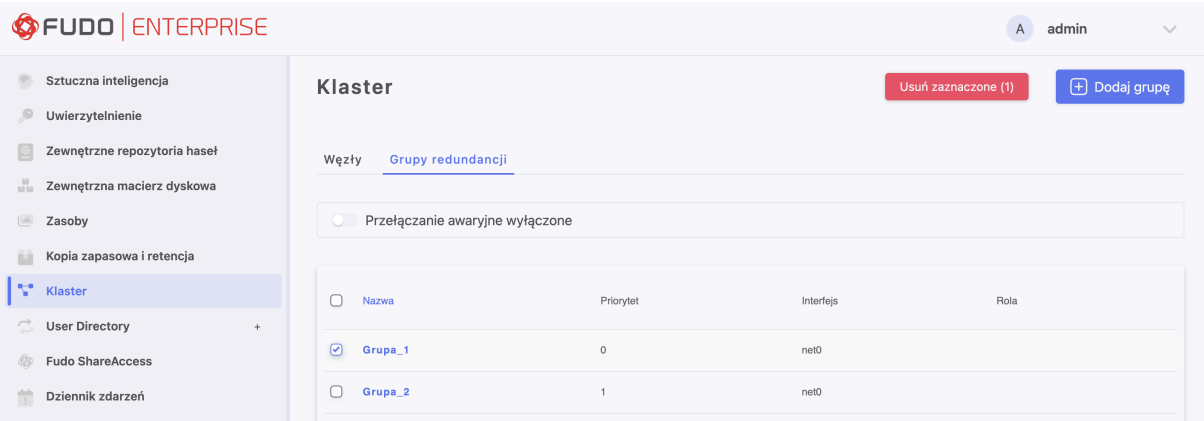
Aby zmodyfikować grupę redundancji, postępuj zgodnie z poniższą instrukcją.

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

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 zaznaczone* przy wybranej grupie redundancji.
4. Kliknij *Potwierdź*.



Degradowanie grupy redundancji

Uwaga

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. Edytuj grupę, którą chcesz zdegradować.
4. Kliknij *Zdegraduj* przy wybranej grupie redundancji.
5. Kliknij *Zapisz i wyjdź*.



Uwaga

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

Uwaga

- 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 kliknij na jej nazwę aby edytować.

4. Z listy rozwijalnej *Interfejs komunikacji klastrowej* wybierz `Wymuś tryb slave`.
5. Kliknij *Zapisz i wyjdź*.

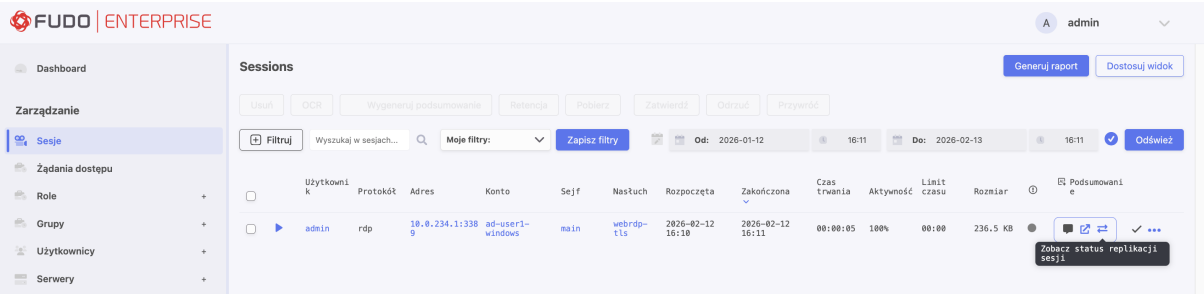


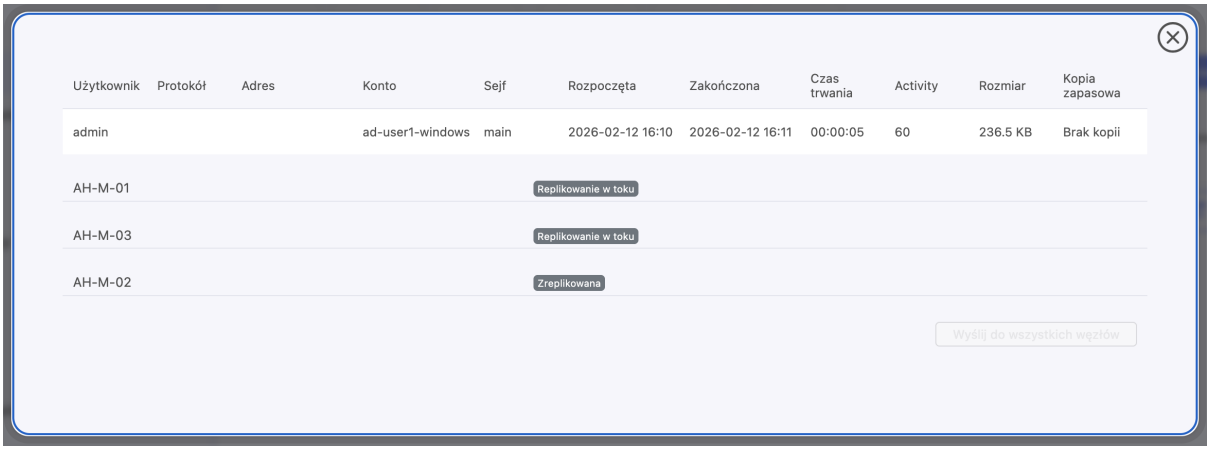
Tematy pokrewne:

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

12.10.8 Sprawdzanie statusu replikacji sesji

Aby sprawdzić status replikacji sesji, odszukaj połączenie na liście sesji i kliknij ikonę ⇄.





Tematy pokrewne:

- *Edytowanie węzłów klastra*
- *Usuwanie węzłów klastra*
- *Bezpieczeństwo: Konfiguracja klastrowa*

12.11 Synchronizacja użytkowników z LDAP - User Directory

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.

12.11.1 Konfiguracja usługi synchronizacji użytkowników

Uwaga

Gdy Kerberos jest włączony w Fudo Enterprise, synchronizacja z Active Directory domyślnie wykorzystuje ten protokół. Ta konfiguracja wymaga poprawnego ustawienia usług domenowych oraz dokładnej synchronizacji czasu systemowego. Więcej informacji znajdziesz w rozdziale *Obsługa Kerberosa przy synchronizacji z Active Directory*.

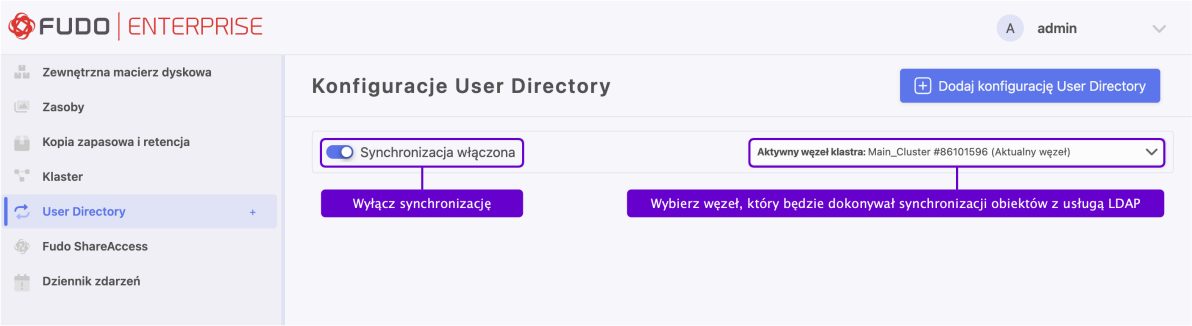
Jeśli nie planujesz korzystać z Kerberosa, wyłącz go w zakładce **Ustawienia** > **Uwierzytelnianie** > **Globalne**, aby nadal używać `simple bind` podczas synchronizacji. Więcej informacji znajdziesz w rozdziale *Ustawienia uwierzytelniania Kerberos*.

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

Uwaga

- 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 konfigurację User Directory*.



5. Nadaj nazwę konfigurowanej domenie.
6. Określ priorytet, który determinuje kolejność odpytywania domen.

Uwaga

Mniejsza liczba oznacza wyższy priorytet.

7. W sekcji *Usługa katalogowa*, wybierz z listy rozwijalnej *Rodzaj serwera* typ usługi katalogowej.
8. W polach *Login* i *Hasło* wprowadź dane uwierzytelniające użytkownika uprawnionego do przeglądania katalogu.
9. W polu *Domena serwera* 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.

Uwaga

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

11. W polu *Domena bazowa dla synchronizacji użytkowników* określ miejsce przechowywania użytkowników w strukturze katalogowej (np: `dc=ad-alt,dc=lab`).

Uwaga

Synchronizacja użytkowników przechowywanych w strukturze LDAP wymaga:

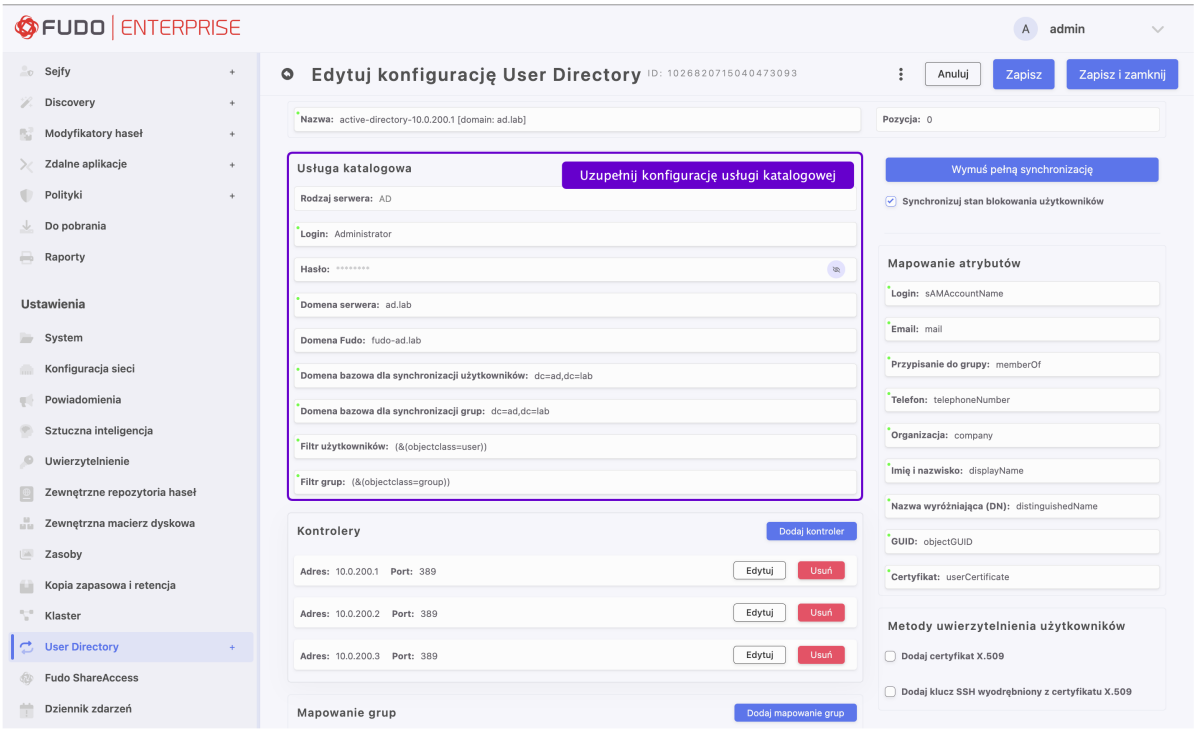
- użycia nakładki *memberOf*
- użycia grup *objectClass*: `groupOfNames`
- zdefiniowania ciągu parametru base DN w postaci: `uid=##username##,ou=people,dc=ldap,dc=test`.

12. W polu *Domena bazowa dla synchronizacji grup* określ miejsce przechowywania grup w strukturze katalogowej (np: `dc=ad-alt,dc=lab`).

Uwaga

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

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



15. Zaznacz opcję *Synchronizuj stan blokowania użytkowników*, aby Fudo automatycznie zablokowało lokalne konta użytkowników, zablokowanych w usłudze katalogowej.

Definiowanie serwera usługi katalogowej

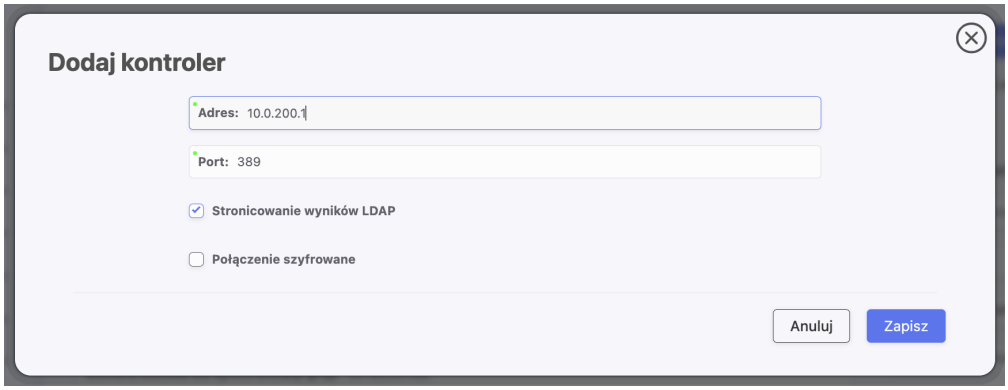
16. W sekcji *Kontrolery* kliknij *Dodaj kontroler*, aby zdefiniować host usługi katalogowej.
17. Wprowadź adres IP serwera oraz numer portu, na którym dostępna jest usługa katalogowa.

Uwaga

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.

18. Zaznacz opcję *Stronicowanie wyników LDAP*, aby włączyć stronicowanie danych zwracanych przez serwer LDAP.

19. Zaznacz opcję *Połączenie szyfrowane* i wgraj certyfkat CA, aby włączyć szyfrowanie transmisji z serwerem LDAP.
20. Kliknij *Zapisz*.



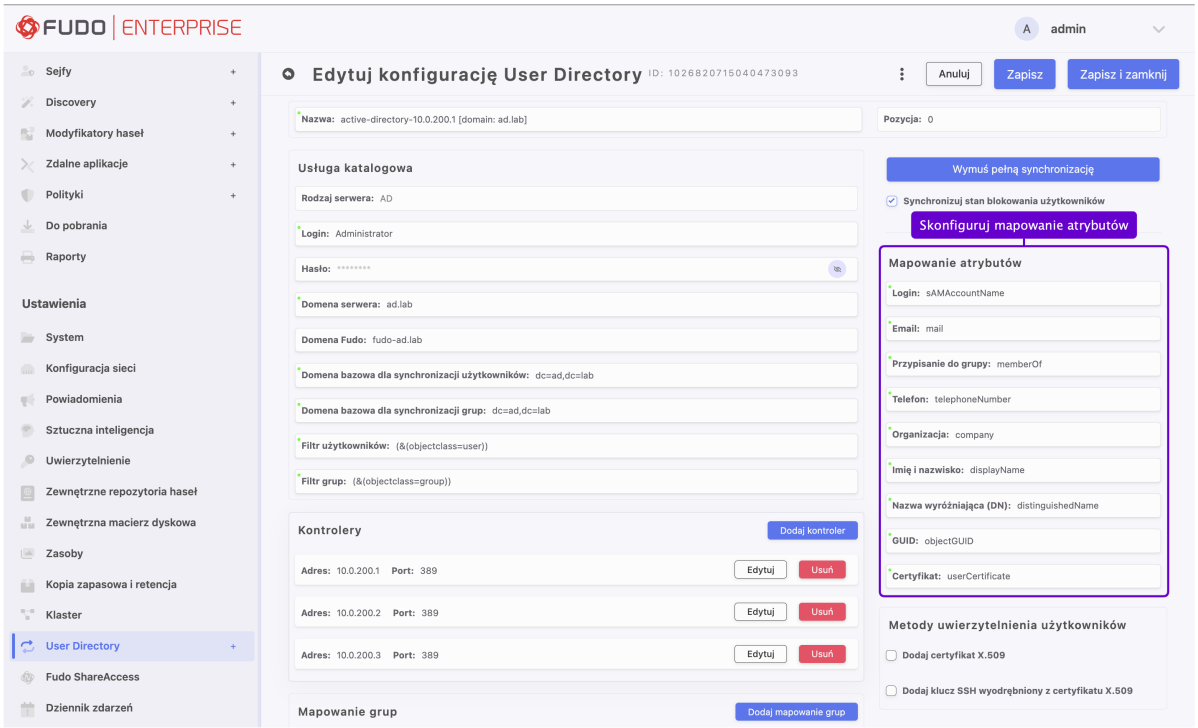
Uwaga

Aby dodać wiele kontrolerów, powtórz powyższe kroki.

Mapowanie atrybutów użytkownika

Uwaga

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

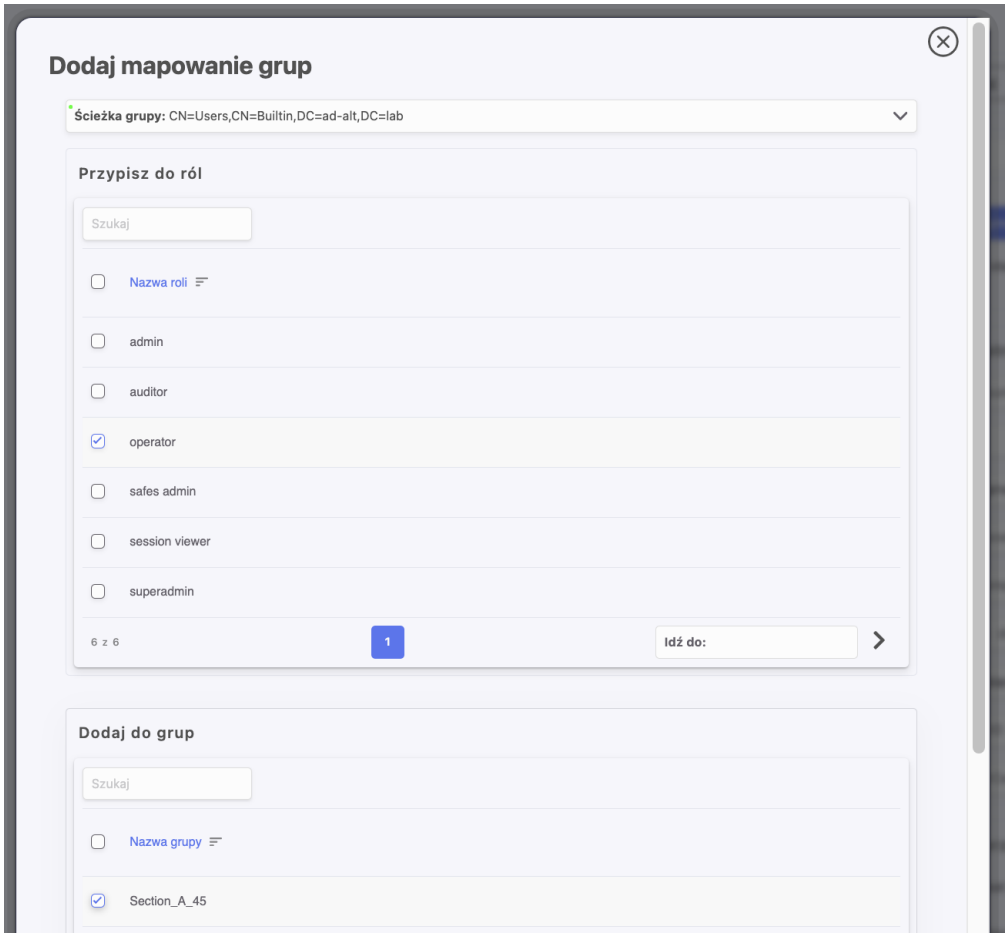


21. Zaznacz *Synchronizuj stan blokady*, aby automatycznie blokować konta lokalne zabloko-

wane w katalogu.

Mapowanie grup zewnętrznych do ról użytkownika

22. W sekcji *Mapowanie grup* kliknij *Dodaj mapowanie grupy*, aby przypisać grupy użytkowników do ról, grup i metod uwierzytelniania.
23. W polu *Ścieżka grupy* wybierz nazwę wyróżniającą (DN) grupy.
24. W sekcji *Przypisz do ról* wybierz role Fudo Enterprise, które mają być przypisane użytkownikom z tej grupy.
25. W sekcji *Dodaj do grup* wybierz grupy Fudo Enterprise, do których mają zostać przypisani użytkownicy.
26. W sekcji *Uwierzytelniania* wybierz zewnętrzne źródło uwierzytelniania dla tej grupy użytkowników.
27. Kliknij *Zapisz*.



Uwaga

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.

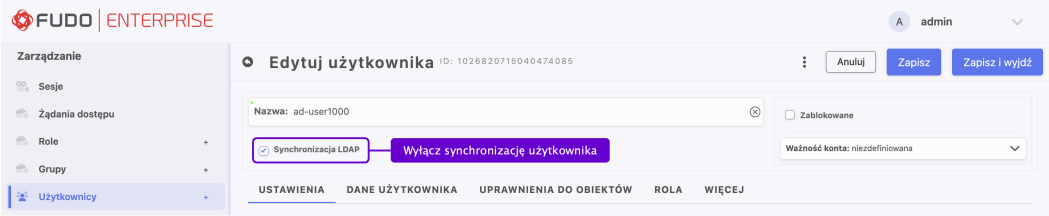
25. W sekcji *Metody uwierzytelnienia użytkowników*, zaznacz opcję *Dodaj certyfikat X.509*, aby pobrać certyfikat użytkownika i przypisać go jako jedną z metod jego uwierzytelnienia.
26. Zaznacz opcję „Dodaj klucz SSH wyodrębniony z certyfikatu X.509", aby pobrać klucz SSH użytkownika z certyfikatu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

12.11.2 Wyłączanie synchronizacji danych dla użytkownika

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.

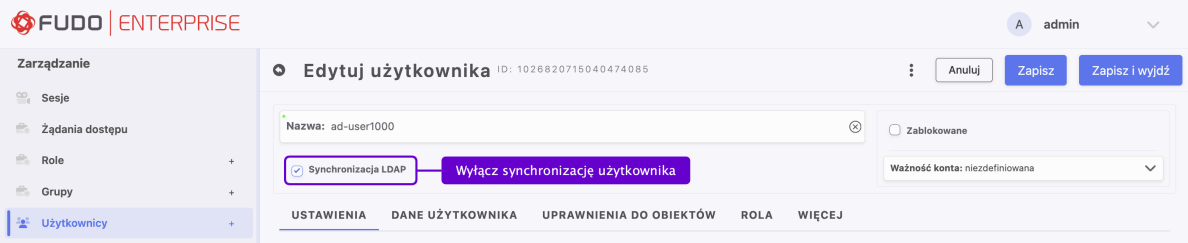
Administrator może znowu zaznaczyć opcję i przywrócić synchronizację LDAP-ową, ale wszystkie zmiany, naniesione manualnie znikną przy następnej próbie synchronizacji. Tylko dodane bądź zmienione metody uwierzytelniania zostaną.



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.



12.11.3 Obsługa Kerberosa przy synchronizacji z Active Directory

Gdy uwierzytelnianie Kerberos jest włączone w **Ustawienia** > **Uwierzytelnianie** > **Globalne**, a rodzaj serwera katalogu użytkowników ustawiono na **AD (Active Directory)**, synchronizacja odbywa się z wykorzystaniem protokołu Kerberos.

Uwaga

Jeśli nie planujesz korzystać z Kerberosa, wyłącz go w zakładce **Ustawienia** > **Uwierzytelnianie** > **Globalne**, aby nadal używać `simple bind` podczas synchronizacji. Więcej informacji znajdziesz w rozdziale *Ustawienia uwierzytelniania Kerberos*.

Jeśli planujesz używać uwierzytelniania **Kerberos** do synchronizacji katalogu użytkowników, upewnij się, że:

- Port **88 (Kerberos)** jest otwarty na zaporze — w przeciwnym razie synchronizacja zakończy się niepowodzeniem.
- **Nazwa hosta Fudo** zawiera odpowiedni sufiks domeny (np: `fudo.qa.kerberos`).
- **Serwer DNS** z tej samej domeny jest prawidłowo skonfigurowany.
- **Adres kontrolera domeny** odpowiada **SPN (Service Principal Name)** serwera LDAP zdefiniowanego w domenie.
- Jeśli bieżąca konfiguracja używa adresu IP zamiast nazwy hosta, zaktualizuj ją, aby używać poprawnej nazwy hosta.

Ostrzeżenie

Fudo Enterprise obsługuje wyłącznie opcje **0** i/lub **1** dla poniższych zasad zabezpieczeń LDAP na kontrolerach domeny Windows:

- Domain controller: LDAP server channel binding token requirements *(Registry Setting: LdapEnforceChannelBinding)*
- Domain controller: LDAP server signing requirements *(Registry Setting: LDAPServerIntegrity)*

Jeśli którakolwiek z tych zasad jest ustawiona na **wartość 2**, synchronizacja zakończy się niepowodzeniem.

Tematy pokrewne:

- *Definicja serwera uwierzytelnienia zewnętrznego*
- *Zarządzanie użytkownikami*

- *Diagnostyka*

12.12 Model uwierzytelniania w oparciu o certyfikaty

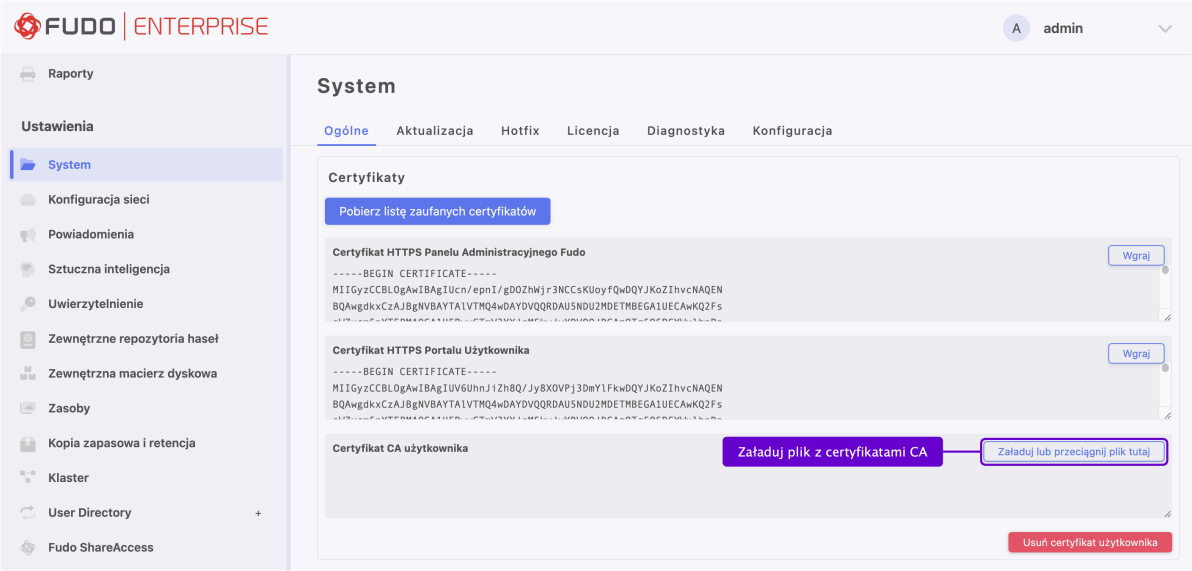
Fudo Enterprise umożliwia logowanie certyfikatem do serwera docelowego. Certyfikat powinien być zgodny ze standardami PIV.

W celu konfiguracji certyfikatu jako metody uwierzytelnienia, postępuj zgodnie z instrukcją:

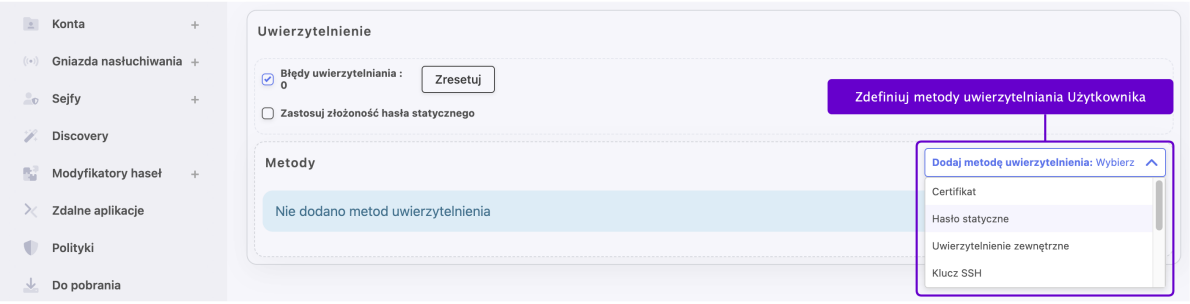
1. Wybierz *Ustawienia* > *System*
2. W zakładce *Ogólne*, w polu *Certyfikaty CA* sekcji *Certyfikaty CA użytkownika* załaduj plik z certyfikatami w formacie PEM.

Uwaga

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.



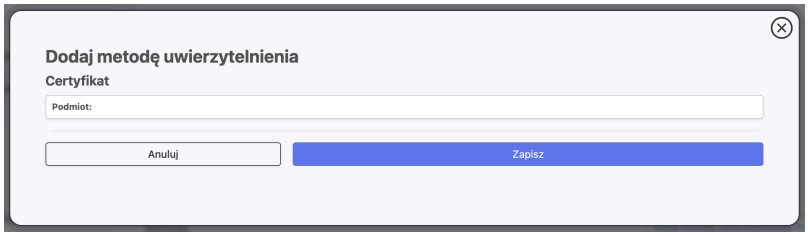
3. Kliknij *Zapisz*.
4. Wybierz *Zarządzanie* > *Użytkownicy* i edytuj użytkownika, dla którego chcesz skonfigurować metodę uwierzytelnienia `certyfikat`, lub utwórz nowego użytkownika przechodząc do menu *Zarządzanie* > *Użytkownicy* i klikając + *Dodaj użytkownika*.
5. W sekcji *Uwierzytelnienie* z listy rozwijanej *Dodaj metodę uwierzytelnienia* wybierz typ *Certyfikat*.



6. Podaj *Podmiot* i kliknij *Zapisz*.

Uwaga

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*

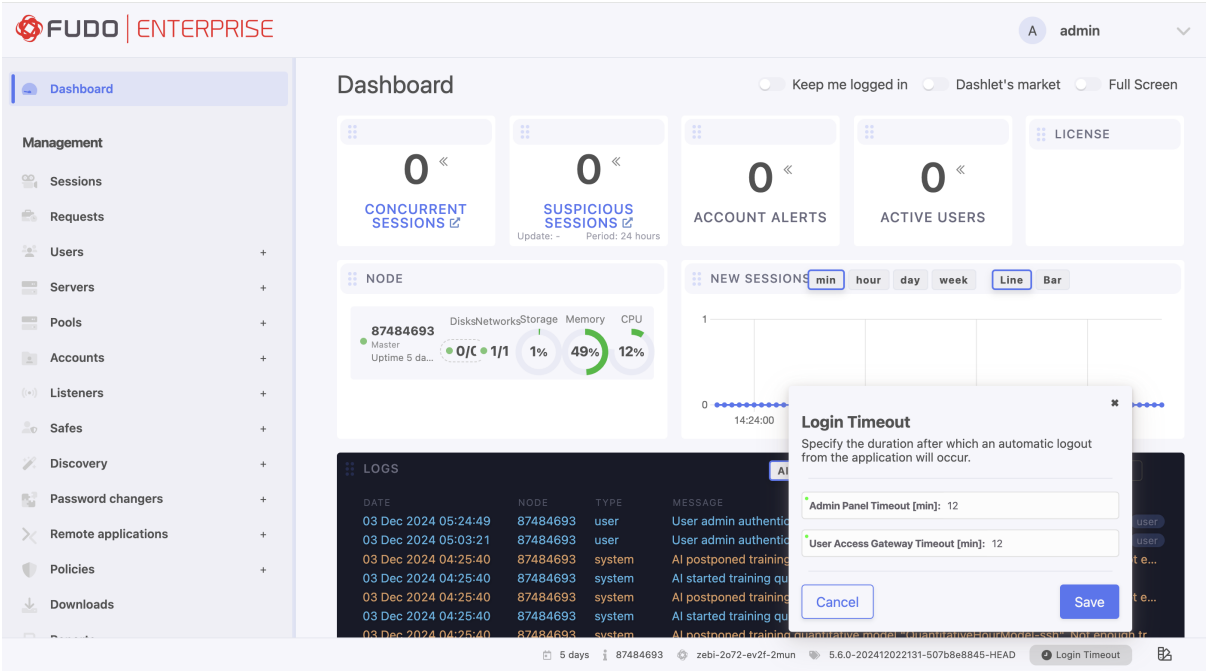
12.13 Login Timeout

Funkcja **Login Timeout** 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.

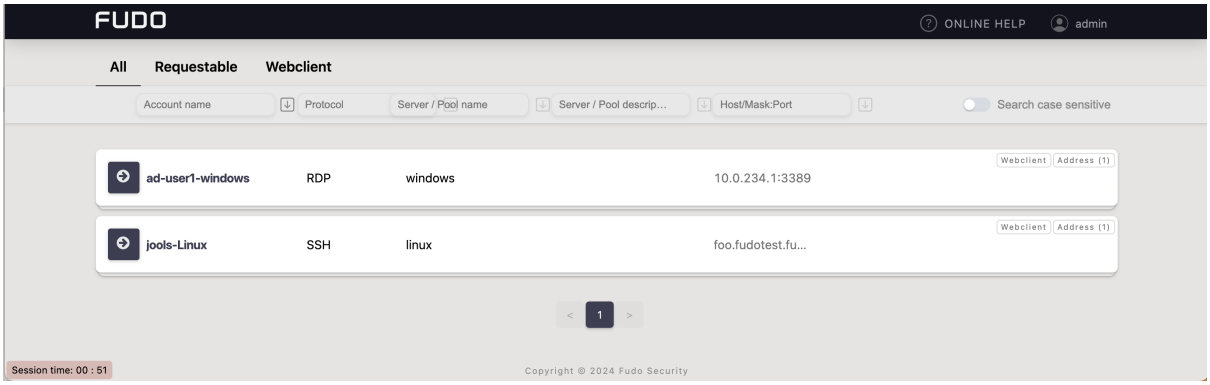
Uwaga

Tylko użytkownicy z rolą **superadmin** lub **admin** mogą zarządzać ustawieniami funkcji Login Timeout.

3. Kliknij *Zapisz*, aby zastosować ustawienia.



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*

12.14 Przywracanie poprzedniej wersji systemu

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

Ostrzeżenie

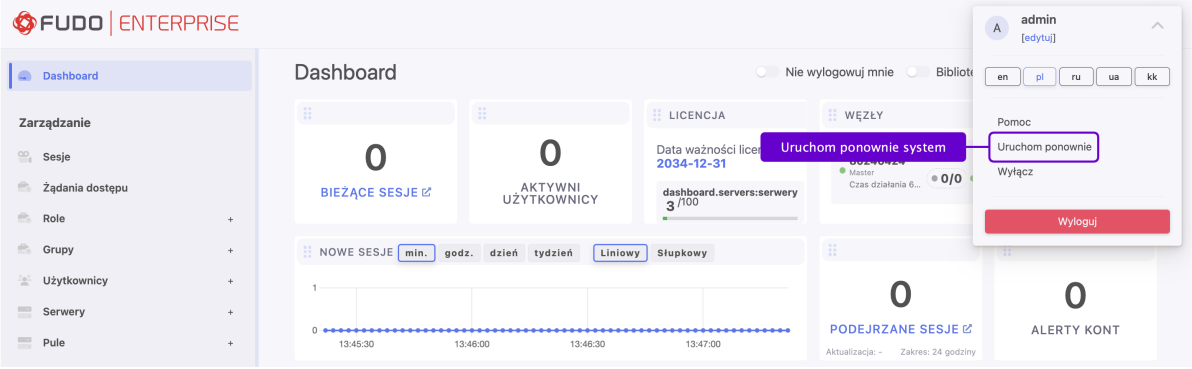
Przywrócenie poprzedniej wersji spowoduje odtworzenie stanu systemu sprzed jego aktualizacji. **Dane sesji** oraz **zmiany w konfiguracji** dokonane na nowej wersji systemu zostaną utracone. Obejmuje to także **aktywność modyfikatorów haseł**. Jeśli jakiekolwiek hasła zostały zmienione podczas korzystania z nowszej wersji, przywrócenie poprzedniej wersji spowoduje utratę dostępu do wybranych systemów.

Uwaga

- Ponowne uruchomienie systemu wymaga podłączenia do urządzenia pamięci USB z kluczem szyfrującym.
- Ponowne uruchomienie systemu spowoduje zakończenie wszystkich aktywnych połączeń użytkowników.
- Skorzystaj z opcji *Blokowanie nowych połączeń* w *Ustawienia* > *Uwierzytelnienie* > zakładka *Globalne*, aby zablokować możliwość nawiązywania nowych połączeń i ograniczyć liczbę aktywnych użytkowników przed ponownym uruchomieniem systemu. Więcej na ten temat znajdziesz w rozdziale *Blokowanie nowych połączeń*.

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

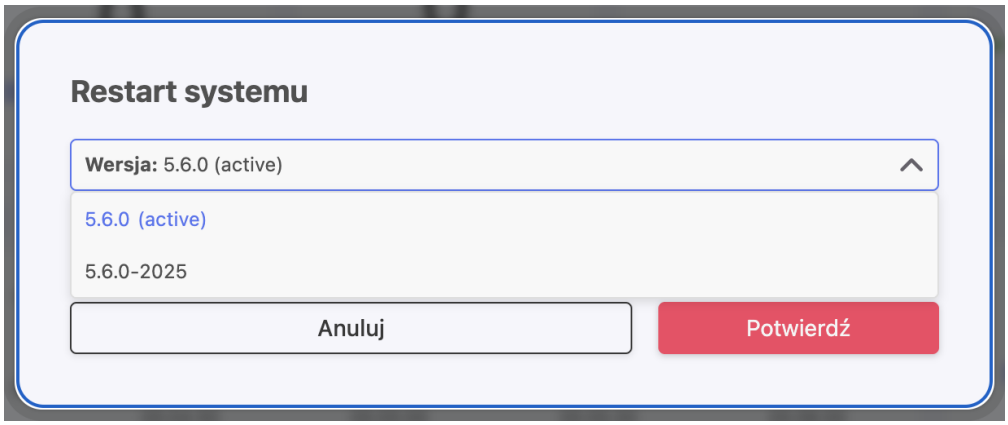
1. Podłącz nośnik z kluczem szyfrującym do portu USB.
2. Z menu opcji użytkownika, wybierz opcję *Uruchom ponownie*.



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

Uwaga

Domyślnie zaznaczona jest wersja bieżąca.



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

Ostrzeżenie

Ponowne uruchomienie systemu spowoduje rozłączenie bieżących połączeń użytkowników.

Tematy pokrewne:

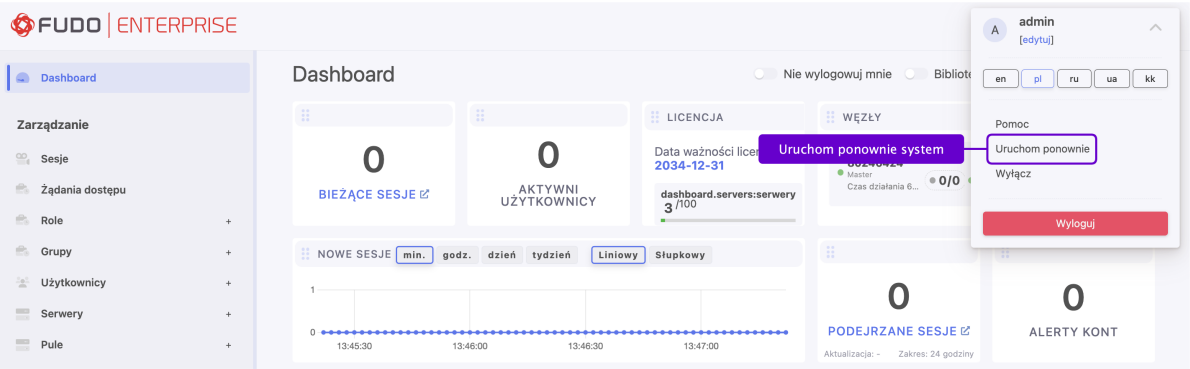
- *Pierwsze uruchomienie systemu*
- *Aktualizacja systemu*

12.15 Ponowne uruchomienie systemu

Uwaga

- Ponowne uruchomienie systemu wymaga podłączenia do urządzenia pamięci USB z kluczem szyfrującym.
- Ponowne uruchomienie systemu spowoduje zakończenie wszystkich aktywnych połączeń użytkowników.
- Skorzystaj z opcji *Blokowanie nowych połączeń* w *Ustawienia* > *Uwierzytelnienie* > zakładka *Globalne*, aby zablokować możliwość nawiązywania nowych połączeń i ograniczyć liczbę aktywnych użytkowników przed ponownym uruchomieniem systemu. Więcej na ten temat znajdziesz w rozdziale *Blokowanie nowych połączeń*.

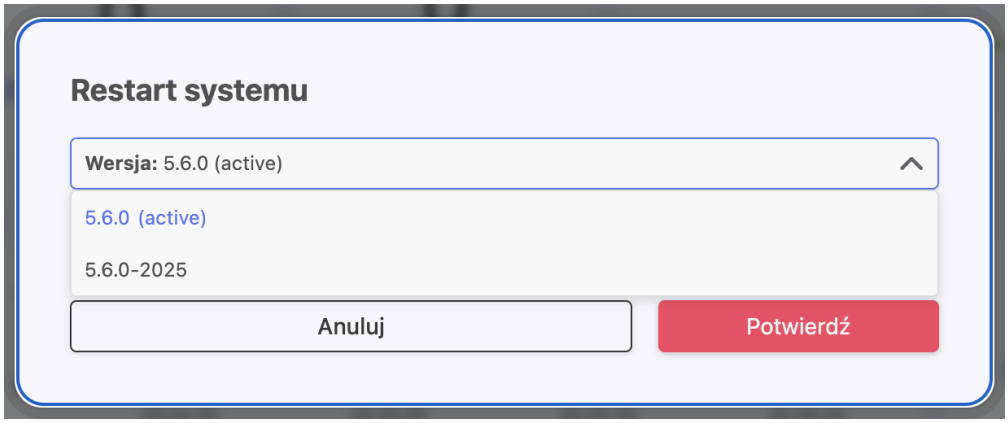
1. Podłącz nośnik z kluczem szyfrującym do portu USB.
2. Z menu opcji użytkownika, wybierz opcję *Uruchom ponownie*.



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

Uwaga

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 *Potwierdź*, aby potwierdzić operację ponownego uruchomienia, z wybraną wersją systemu.

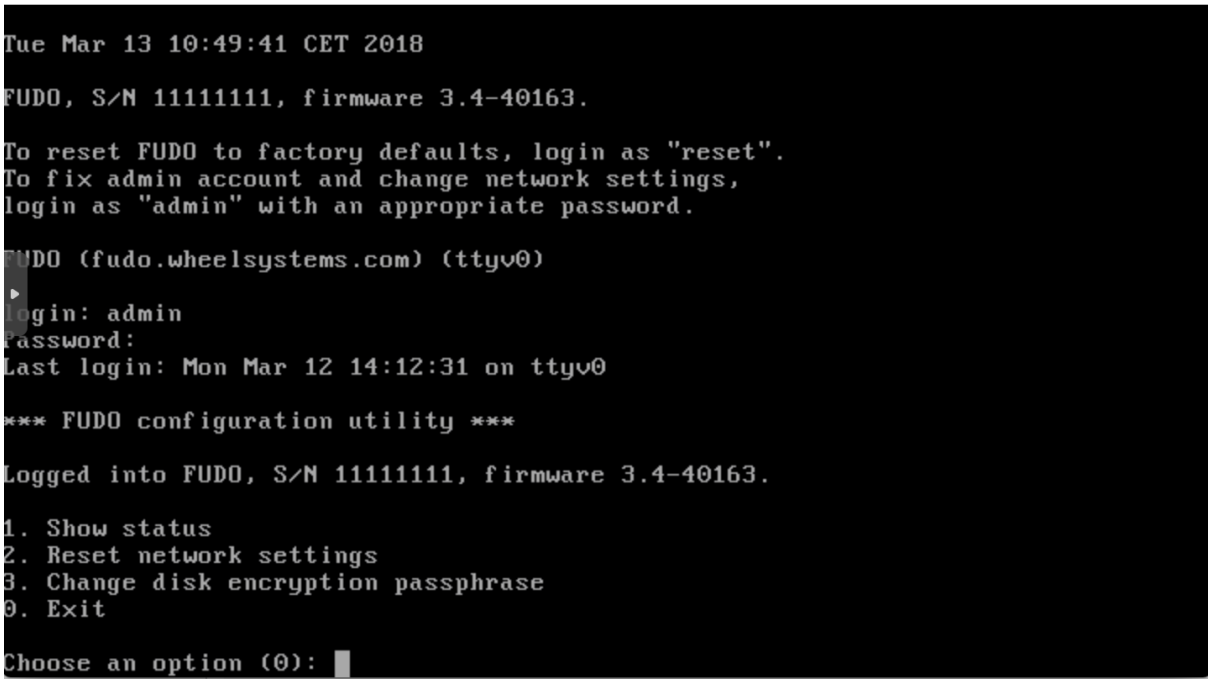
Tematy pokrewne:

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

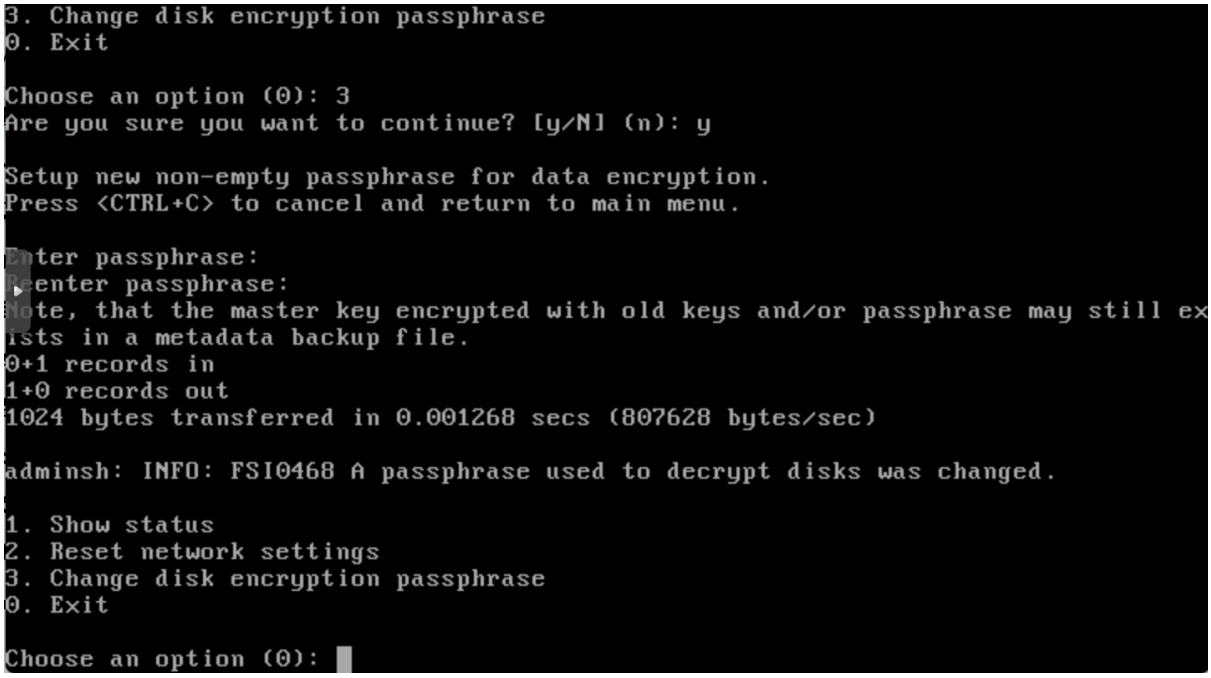
12.16 Zmiana frazy szyfrującej

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 superadmina.
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 danych sesji*

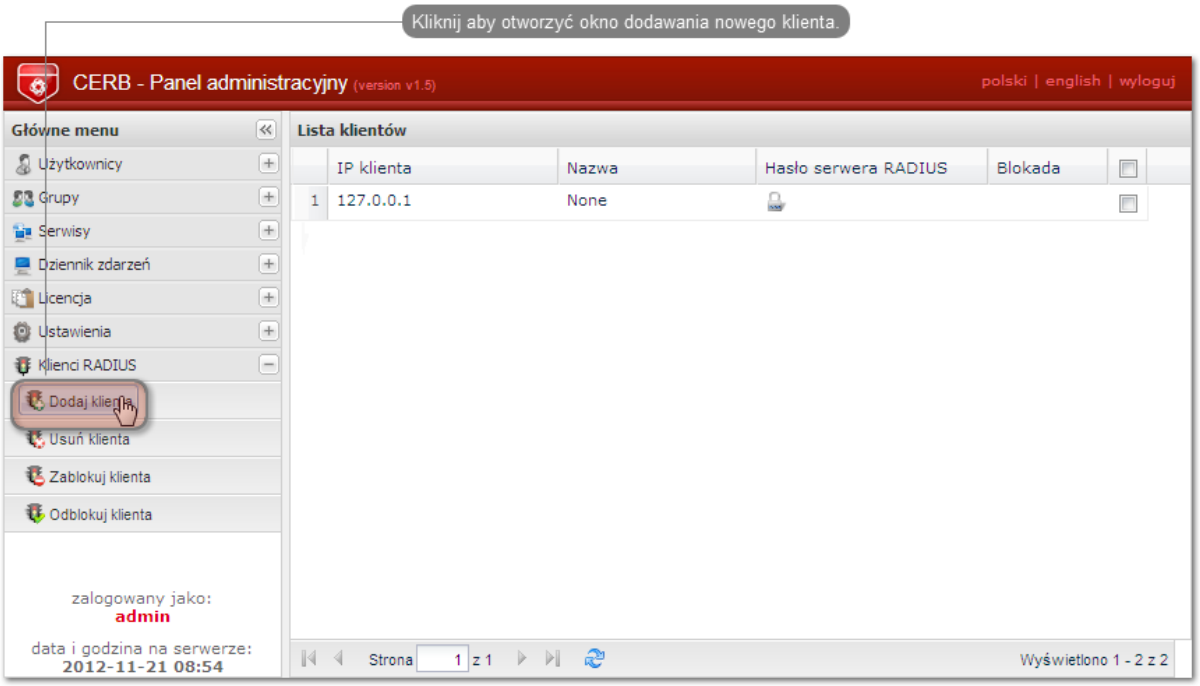
12.17 Integracja z serwerem CERB

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*.

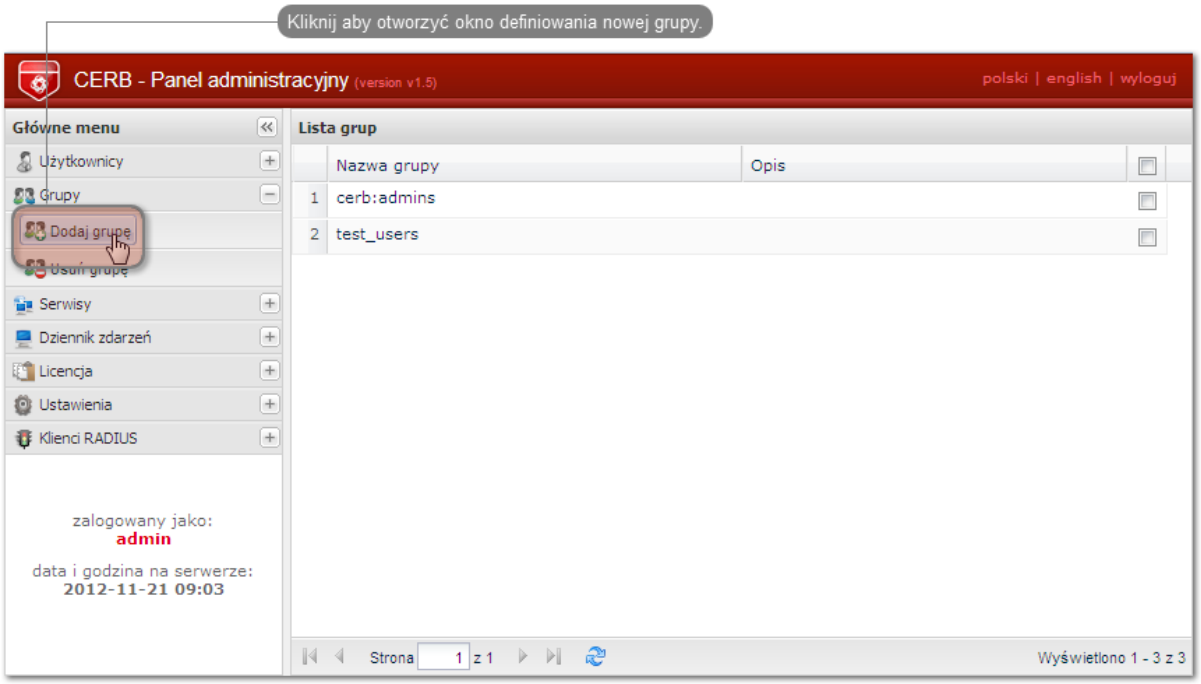


Uwaga

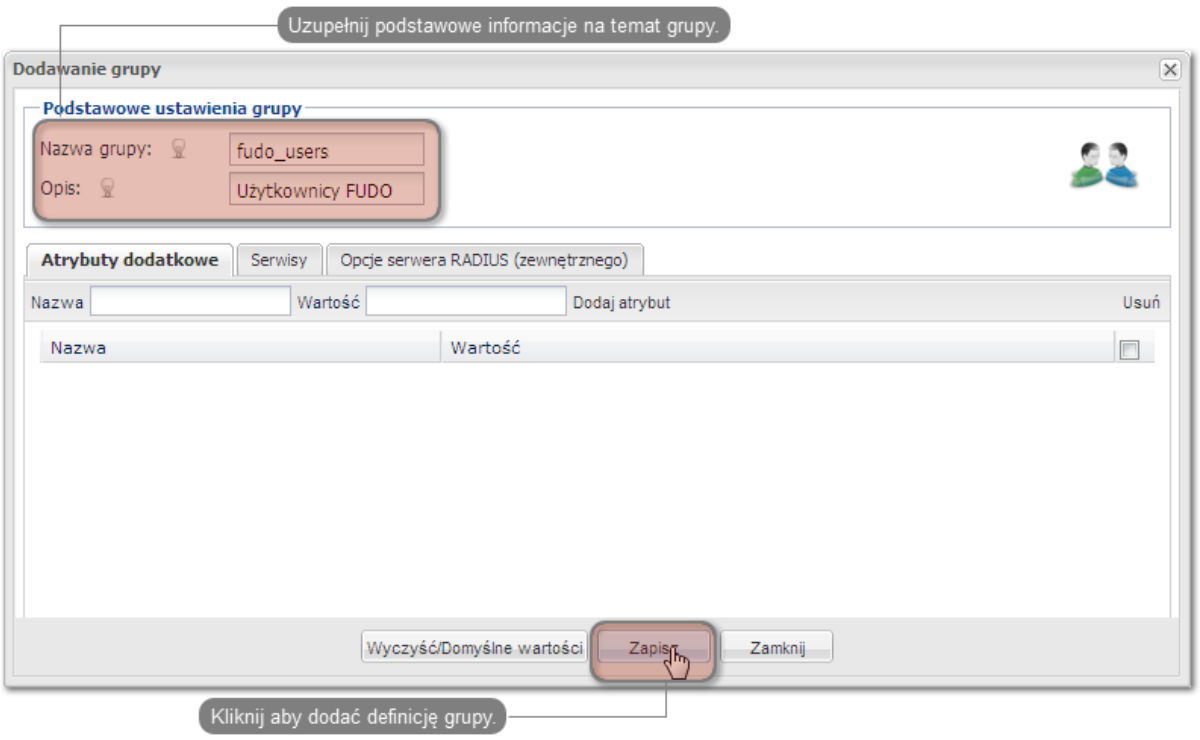
Hasło będzie wymagane do skonfigurowania zewnętrznego serwera uwierzytelniania w panelu administracyjnym Fudo Enterprise.

2. Dodanie grupy użytkowników.

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

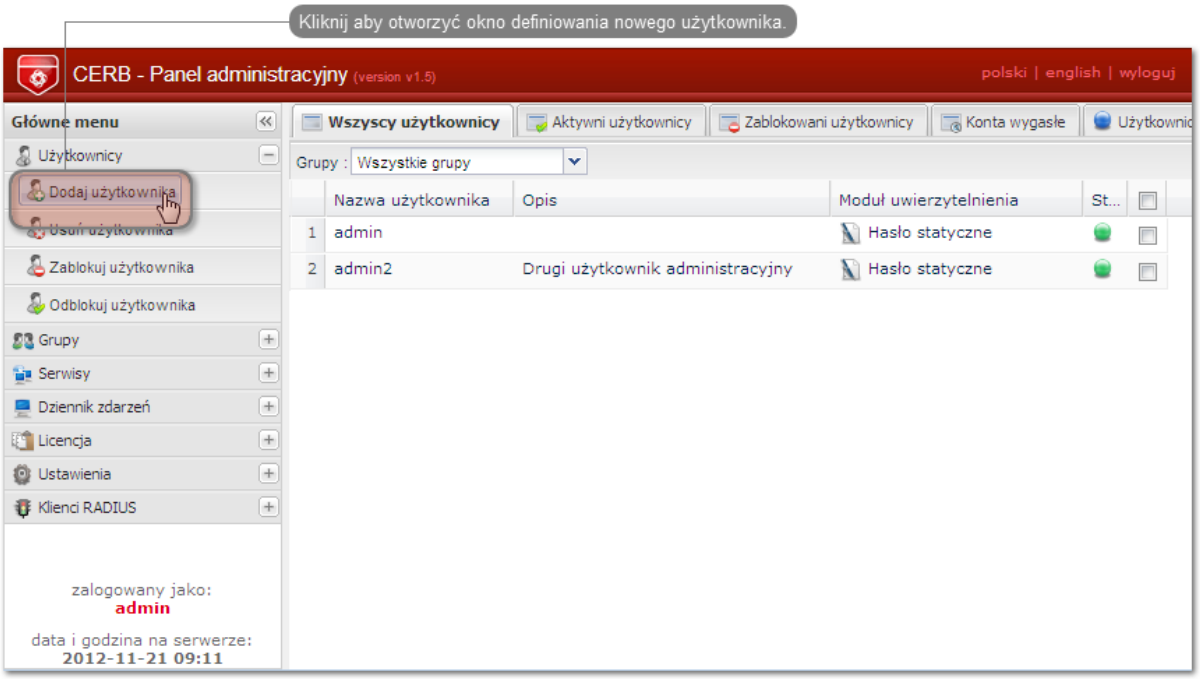


- Podaj nazwę grupy (`fudo_users`) i kliknij *Zapisz*.

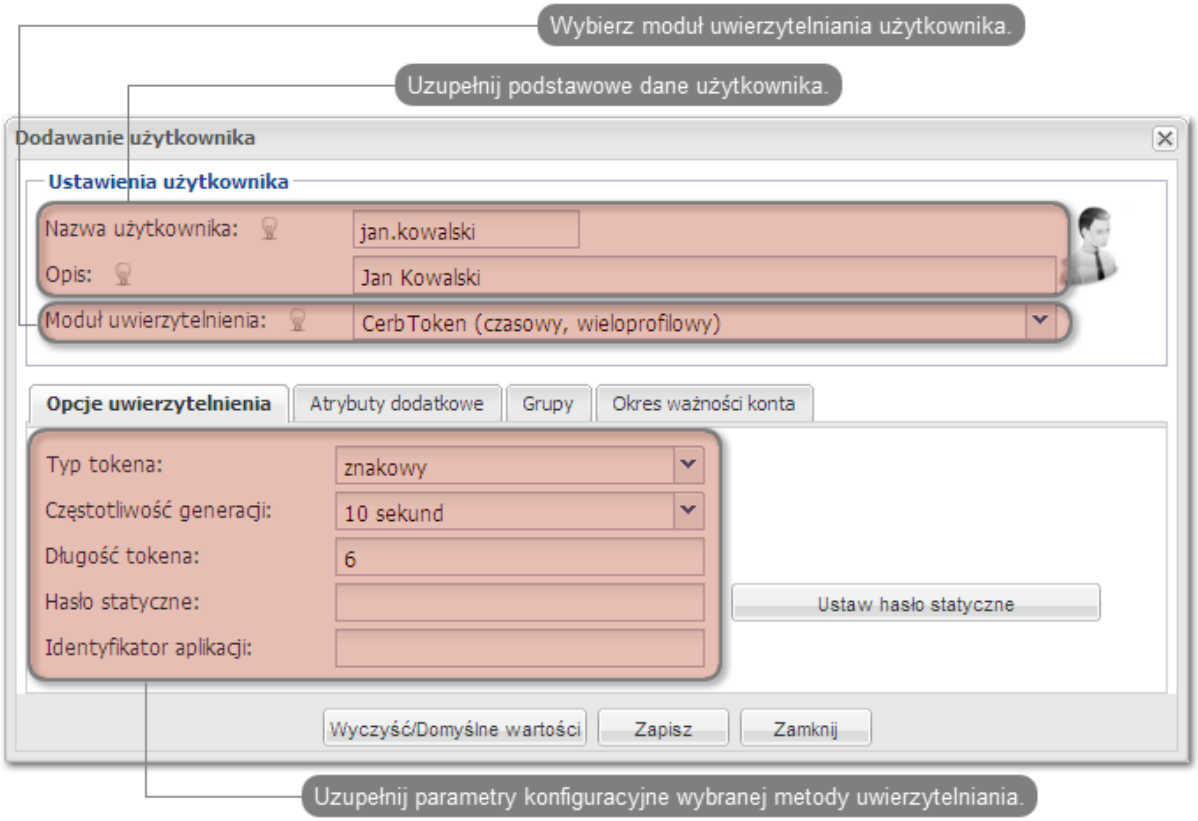


3. Dodanie użytkownika.

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



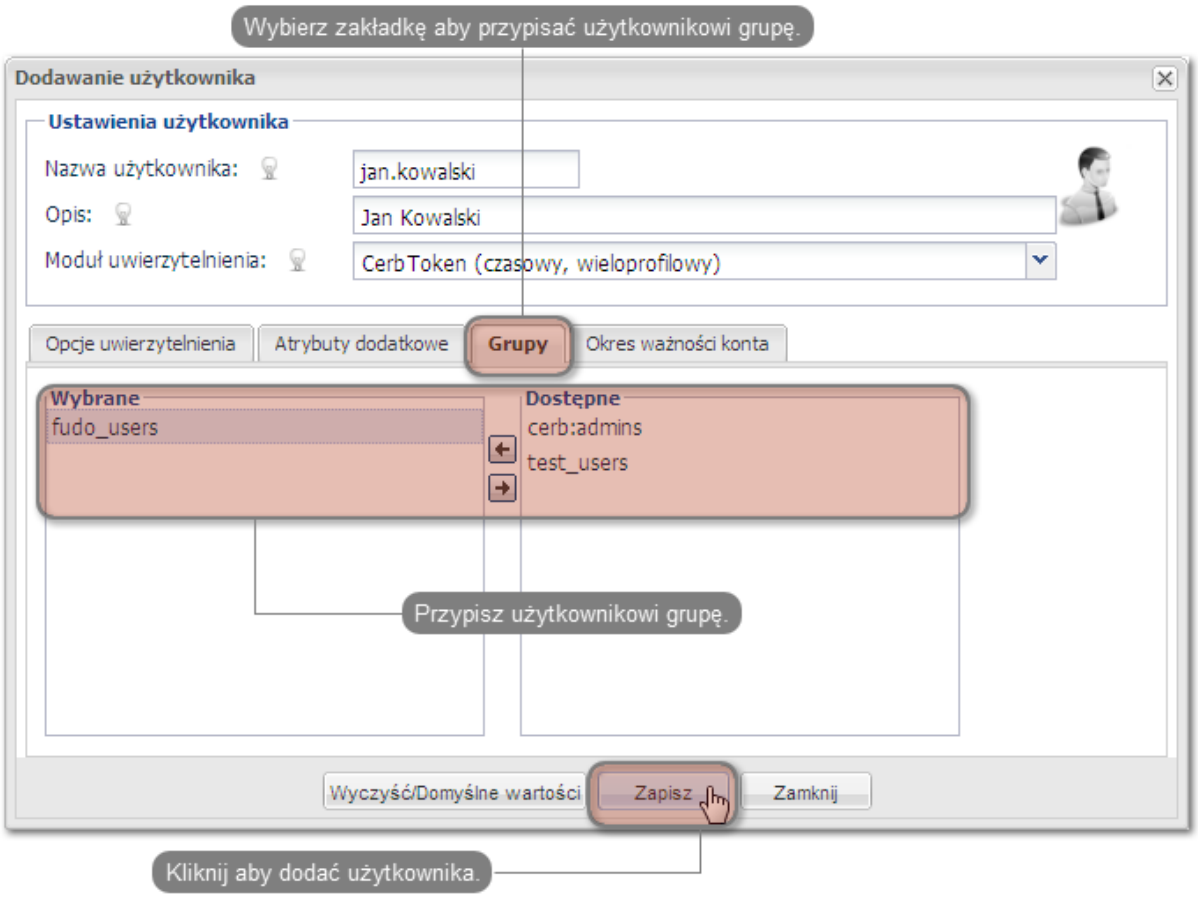
- Podaj nazwę użytkownika, opis oraz wybierz stosowny moduł uwierzytelniania (więcej informacji na temat modułów uwierzytelniania znajdziesz w dokumentacji serwera CERB).



Uwaga

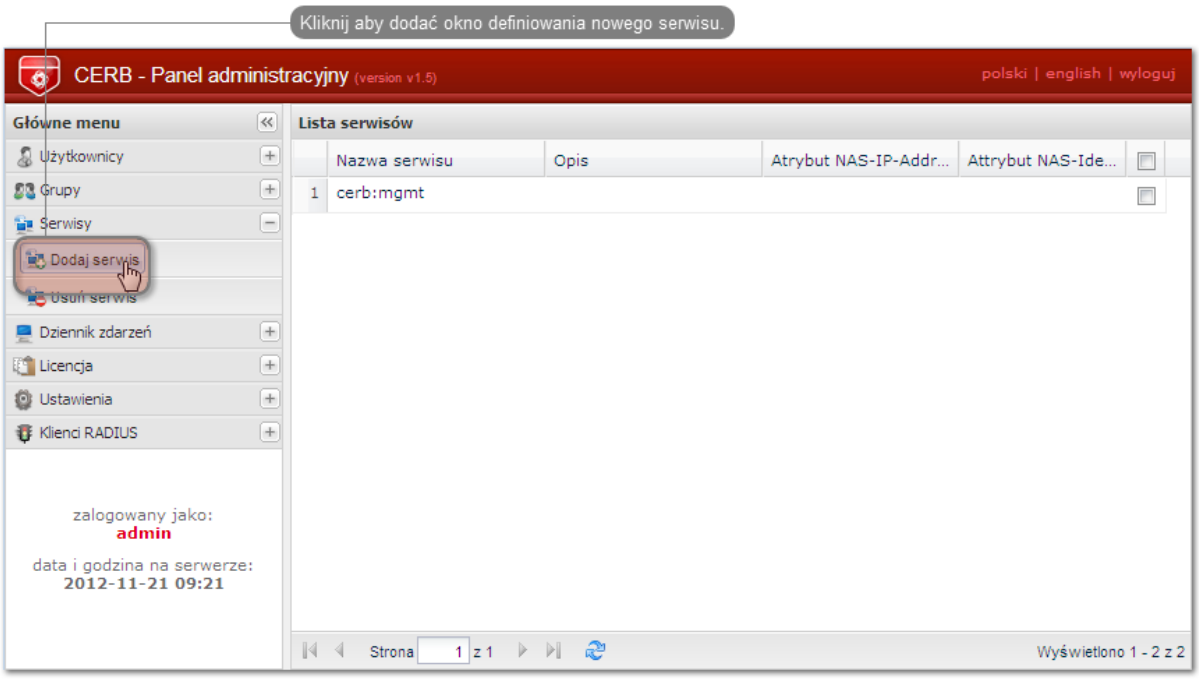
Nazwa użytkownika wykorzystywana jest w procesie uwierzytelniania użytkowników łączących się z Fudo Enterprise.

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



4. Skonfigurowanie serwisu.

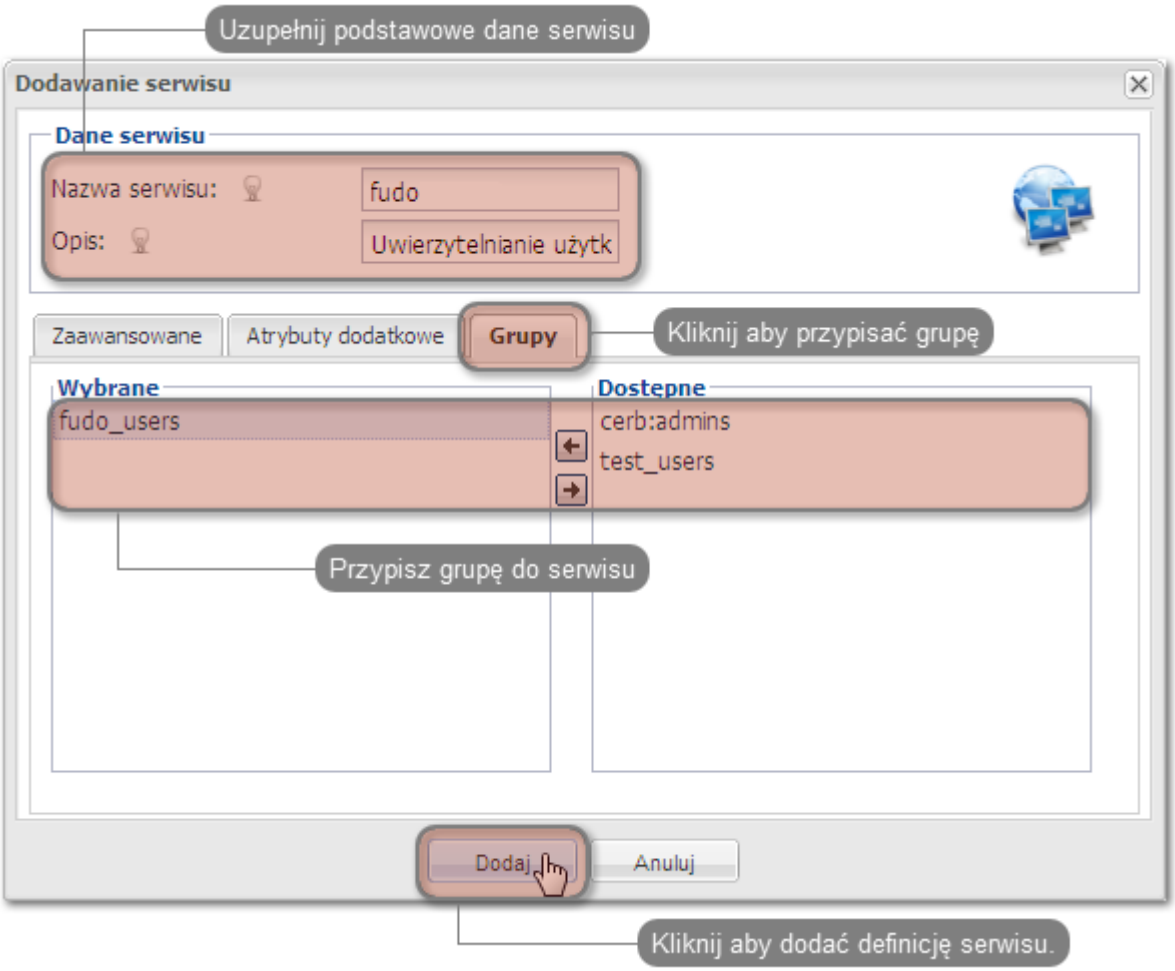
- Wybierz z lewego menu *Serwisy* > *Dodaj serwis*, aby otworzyć okno definiowania nowego serwisu.



- Wpisz nazwę pod jaką identyfikowana będzie usługa uwierzytelniania (`cerb_fudo`) oraz

opis serwisu.

- Dodaj do serwisu grupę `fudo_users` i kliknij *Dodaj*.



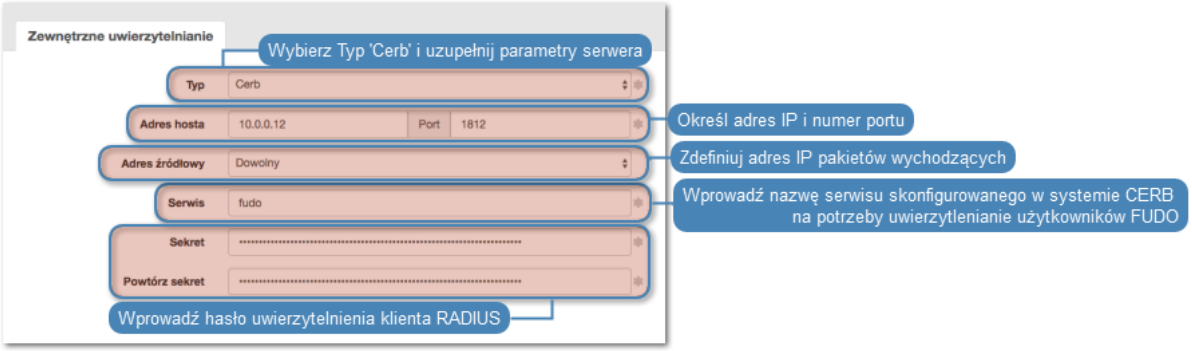
Konfiguracja serwera Fudo Enterprise

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.

Uwaga

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.

Uwaga

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*

12.18 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.

12.18.1 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

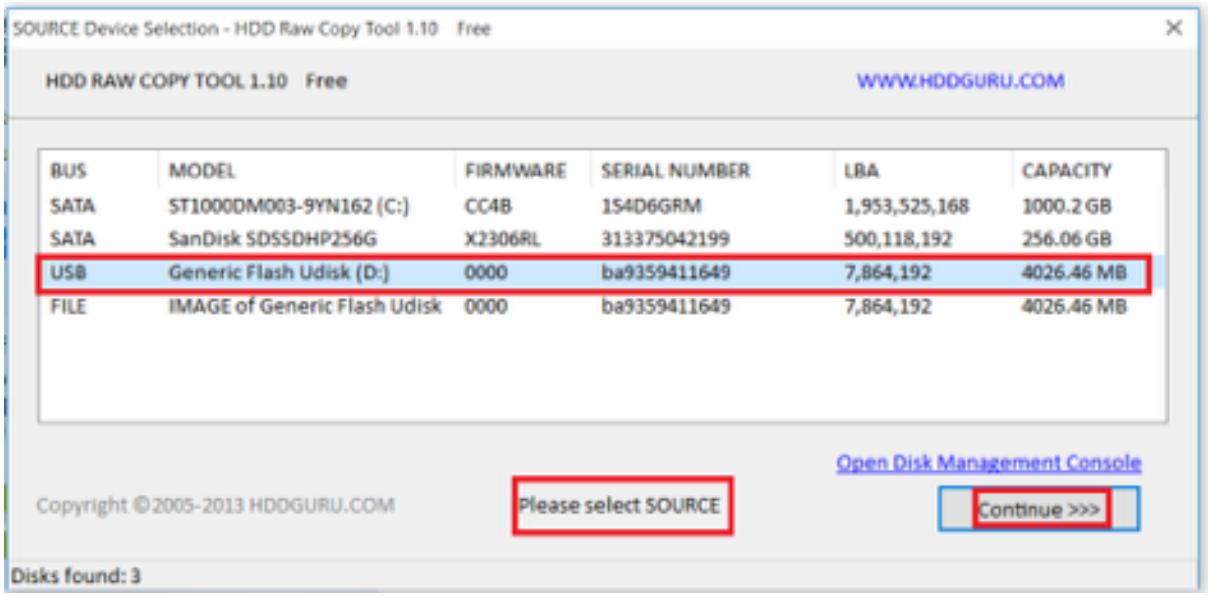
Po podłączeniu nośnika USB do komputera, pod żadnym pozorem nie należy wykonywać jego inicjowania/formatowania. Komunikat systemowy o braku możliwości odczytu danych należy zignorować i przystąpić do procedury tworzenia kopii zapasowej.

1. Pobierz i zainstaluj program *HDD Raw Copy Tool*.

   `http://hddguru.com/software/HDD-Raw-Copy-Tool/` (dostępna również wersja przenośna)

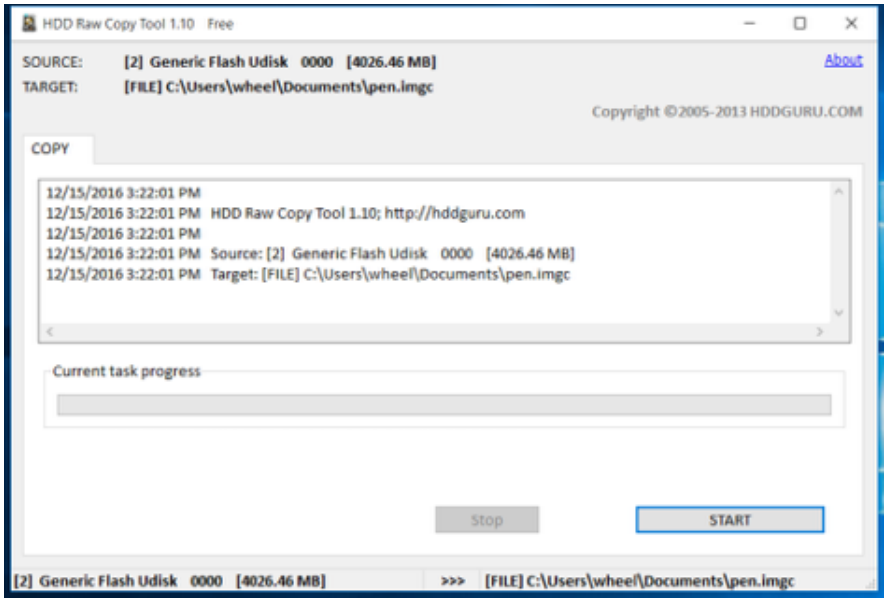
2. Uruchom program.

3. Na ekranie wyboru napędu źródłowego, zaznacz napęd USB z zapisanymi kluczami szyfrującymi i kliknij *Continue*.



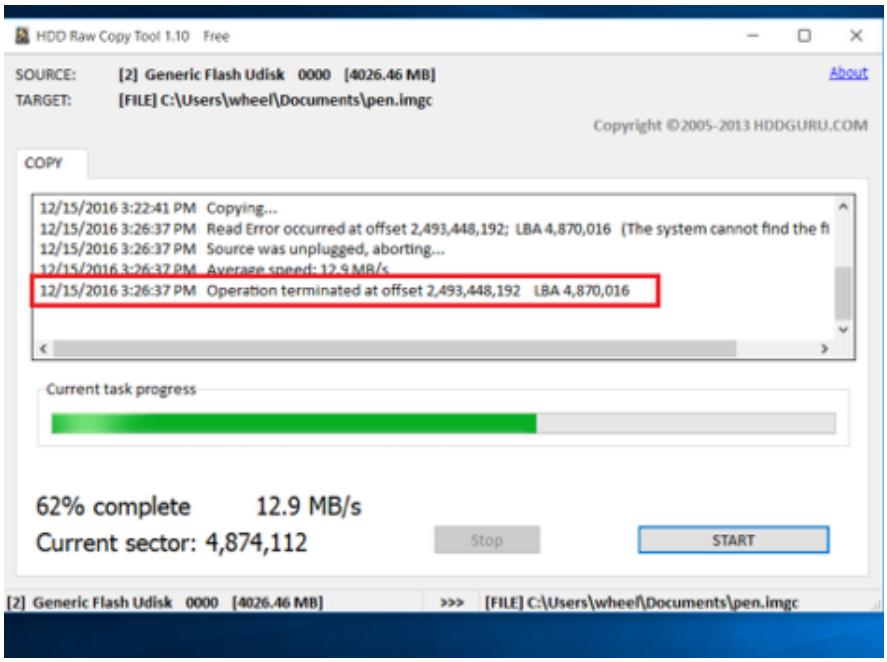
4. Kliknij dwukrotnie *FILE*, wskaż plik docelowy, w którym zapisany zostanie obraz dysku i kliknij *Continue*.

5. Kliknij *START*, aby rozpocząć procedurę kopiowania.

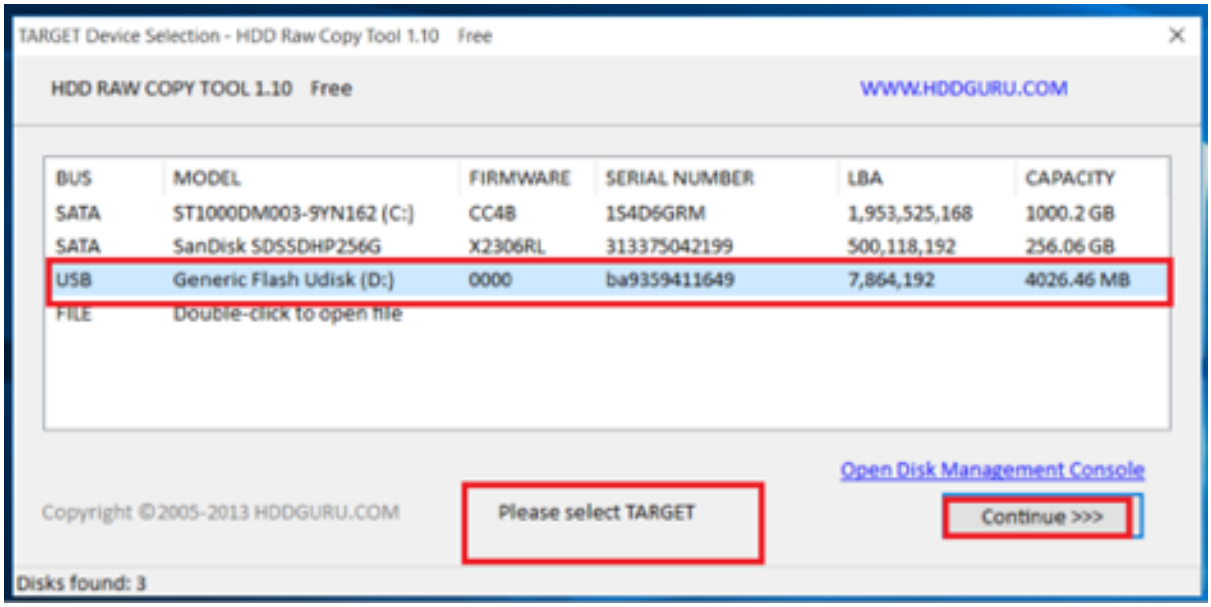


6. Z chwilą wystąpienia komunikatu

   `Operation terminated at offset...`, zamknij okno i odłącz napęd USB.

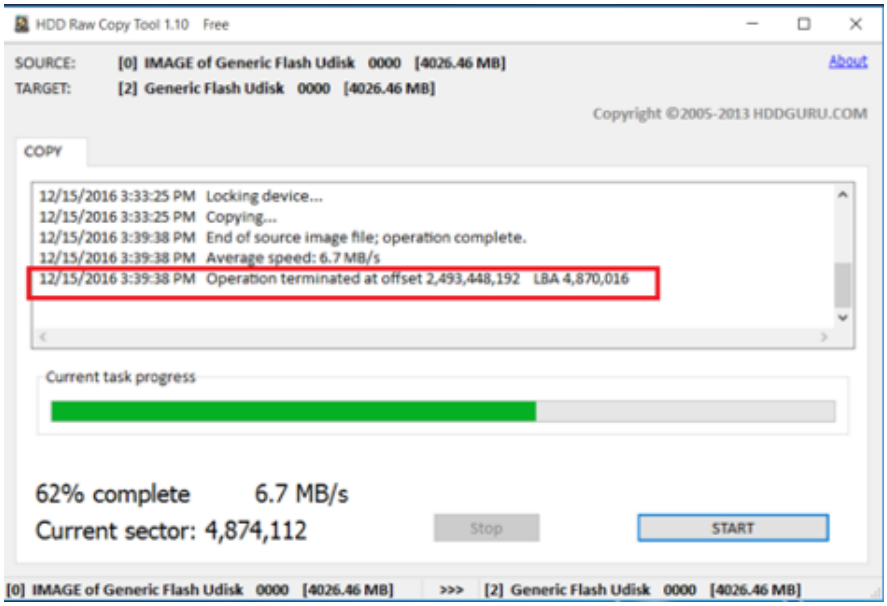


7. Podłącz nośnik pamięci flash i włącz program *HDD Raw Copy Tool*.
8. Na ekranie wyboru napędu źródłowego, zaznacz *FILE* i wskaż plik z obrazem kluczy szyfrujących.
9. Wybierz podłączony nośnik pamięci jako urządzenie docelowe i kliknij *Continue*.



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*

12.18.2 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.

> **Uwaga**
>
> 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.

Uwaga

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.

Uwaga

Więcej informacji o konfigurowaniu widgetów do wygodnego sprawdzania stanu systemu pod linkiem: *Dashboard*.

Tematy pokrewne:

- *Dziennik zdarzeń*
- *Często zadawane pytania*

12.18.3 Kontrola Stanu

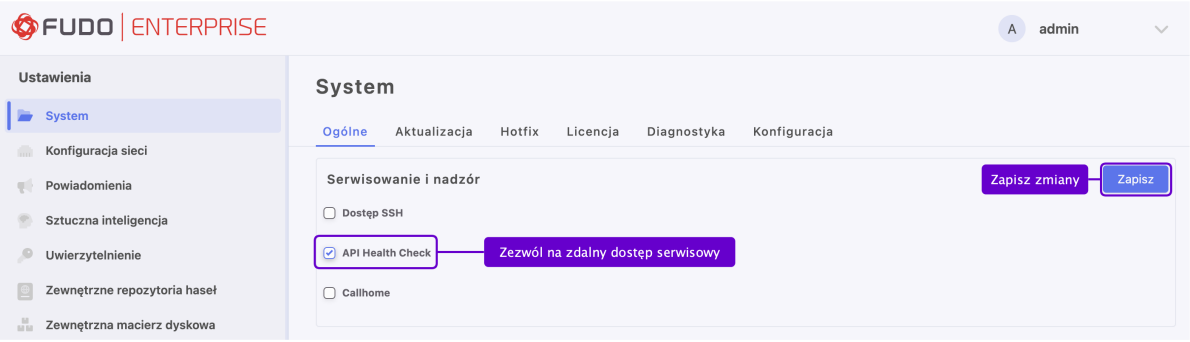
Fudo Enterprise regularnie przeprowadza kontrolę stanu najważniejszych komponentów systemu. Liczne testy systemu zapewniają stałe sprawdzenie stanu komponentu oraz wysłanie je wyników.

Wyniki są dostępne dla administratora z dwóch poziomów:

1. Korzystając z *SNMP*, dostarczający całość wyników kontroli.
2. Korzystając z funkcji *API Health Check*, dostarczającej podsumowanie wyników kontroli.

12.18.3.1 API Health Check

Funkcja API Health Check jest dostępna w sekcji *Serwisowanie i nadzór* zakładki *Ustawienia* > *System*, w podzakładce *Ogólne*.



Dostarcza ona krótką informację o stanie systemu Fudo Enterprise. Funkcja ta może być wykorzystywana przez narzędzia zewnętrzne przy testach stanu systemu.

Wynik sprawdzenia zwracany jest 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.

Uwaga

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 Health Check* będzie dostępna pod ścieżką:

```
/api/v2/healthcheck
```

Ostrzeżenie

Opcja *API Health Check* nie wymaga uwierzytelnienia. To oznacza, że każdy kto ma dostęp do TCP jest uprawniony do odczytu wyników stanu kontroli.

12.18.4 Callhome

Callhome to narzędzie zaprojektowane do zbierania danych diagnostycznych i monitorowania stanu systemu. Gromadzenie statystyk dotyczących częstotliwości użycia poszczególnych funkcji Fudo Enterprise pozwala wykrywać obszary wymagające ulepszeń. Usługa *Callhome* wspomaga również obsługę klienta, umożliwiając wykonywanie wybranych zadań zdalnie i automatycznie. Upraszcza to proces utrzymania i diagnostyki produktu, pozwalając Działowi Wsparcia Technicznego Fudo na pozyskiwanie danych niezbędnych do udzielenia pomocy bez bezpośredniej ingerencji użytkownika.

Uwaga

Callhome służy wyłącznie do zbierania danych diagnostycznych i monitorowania stanu systemu. W celu umożliwienia zdalnej obsługi Fudo Enterprise konieczne jest włączenie w ustawieniach systemu odrębnej funkcji *—Dostęp SSH*.

12.18.4.1 Dane gromadzone przez usługę Callhome

Usługa *Callhome* automatycznie gromadzi istotne dane diagnostyczne, aby zapewnić optymalizację i bezpieczeństwo systemu Fudo Enterprise. Monitorowane są następujące metryki:

- **Stan Dysku:** Monitoruje stan dysku, aby zapobiec awariom.
- **Wykorzystanie Zasobów Pamięci:** Śledzi wykorzystanie zasobów pamięci.
- **Temperatura Czujników:** Kontroluje temperaturę czujników systemowych, aby zapobiec przegrzaniu.
- **Stan Replikacji Danych Sesyjnych:** Monitoruje stan replikacji, aby zapewnić integralność danych.
- **Błędy Krytyczne:** Rejestruje błędy krytyczne mogące wpłynąć na wydajność systemu.
- **Awarie Systemu:** Rejestruje awarie, co pozwala na szybkie zidentyfikowanie i zdiagnozowanie problemów.
- **Wersja Oprogramowania:** Zbiera dane dotyczące wersji Fudo Enterprise, w tym godziny pracy i zgłoszone problemy.

Usługa *Callhome* została zaprojektowana z zachowaniem ścisłych środków bezpieczeństwa:

- Fudo Security **nie ma możliwości wprowadzania jakichkolwiek zmian** w systemie Fudo Enterprise.
- Fudo Security **nie zbiera żadnych danych związanych z konfiguracją klienta.**
- Fudo Security **nie zbiera ani nie przetwarza żadnych danych osobowych** przechowywanych w Fudo Enterprise.

12.18.4.2 Korzyści z używania Callhome

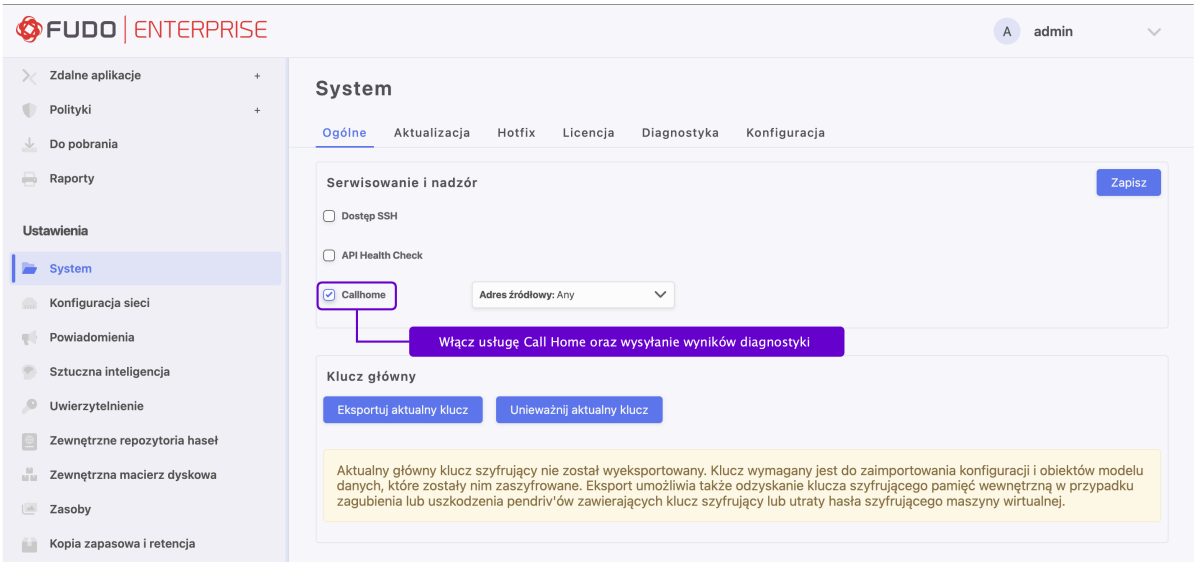
- **Wgląd w Wykorzystanie Funkcji:** Fudo Security zyskuje wgląd w to, które funkcje są aktywnie wykorzystywane przez klientów, co pozwala na priorytetyzację i udoskonalenie najważniejszych funkcjonalności na podstawie rzeczywistych preferencji użytkowników.
- **Zaangażowanie Priorytetowych Klientów:** Proaktywni użytkownicy odgrywają kluczową rolę w procesie rozwoju. Ich dane dotyczące użytkowania bezpośrednio wpływają na przyszłe ulepszenia produktów Fudo Security.
- **Śledzenie Wersji:** Monitorowanie wersji używanych przez klientów umożliwia zapewnienie, że wszyscy korzystają z najbezpieczniejszych i najbardziej efektywnych wydań.
- **Szybsze Rozwiązywanie Problemów:** Usługa Callhome przyspiesza rozwiązywanie problemów, minimalizując konieczność długotrwałej komunikacji. Natychmiastowy dostęp do danych diagnostycznych umożliwia szybką i efektywną interwencję.
- **Zdalne Zarządzanie:** Aktualizacje licencji, aktualizacje wersji i poprawki bezpieczeństwa mogą być wdrażane zdalnie, minimalizując konieczność zaangażowania klienta.

- **Szybka Reakcja na Zagrożenia:** W przypadku wykrycia podatności, Fudo Security może natychmiast wdrożyć poprawki, redukując czas wystawienia na zagrożenia, minimalizując konieczność długotrwałej komunikacji.

12.18.4.3 Konfiguracja Callhome

W celu konfiguracji usługi Callhome, postępuj zgodnie z instrukcją:

1. Przejdź do *Ustawienia* > *System*.
2. Otwórz zakadkę *Ogólne* i przejdź do sekcji *Serwisowanie i nadzór*.
3. Zaznacz opcję *Callhome*.
4. Wybierz adres IP swojej instancji Fudo Enterprise, albo adres `Dowolny`.



Uwaga

- Usługa Callhome 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 rozdział *Informacja ze stopki dolnej*, gdzie znajduje się FUID.
- Urządzenie Fudo nawiąże wychodzące połączenia SSH z `home.fudosecurity.com` (IP:`178.33.6.1`, Port: `22`).
- Uwaga: W poprzednich wersjach funkcja ta była nazywana **Call Home**.

12.18.5 Wymiana dysku macierzy

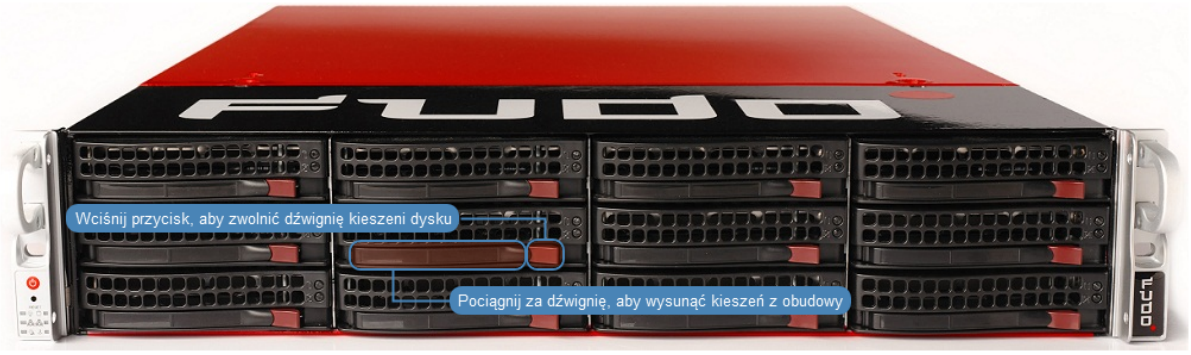
W domyślnej konfiguracji, macierz dyskowa Fudo Enterprise składa się z 12 dysków twardych a zastosowany system plików pozwala na kontynuowanie świadczenia usług w przypadku awarii dwóch nośników.

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.

Uwaga

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

Tematy pokrewne:

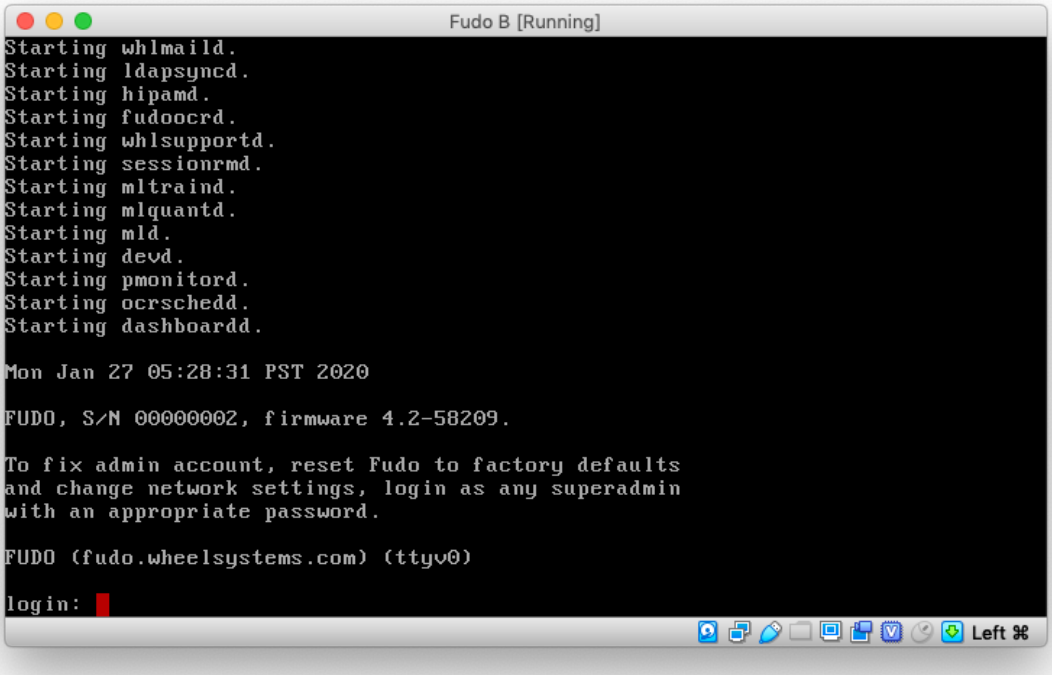
- *Urządzenie*
- *Często zadawane pytania*

12.18.6 Przywracanie ustawień fabrycznych

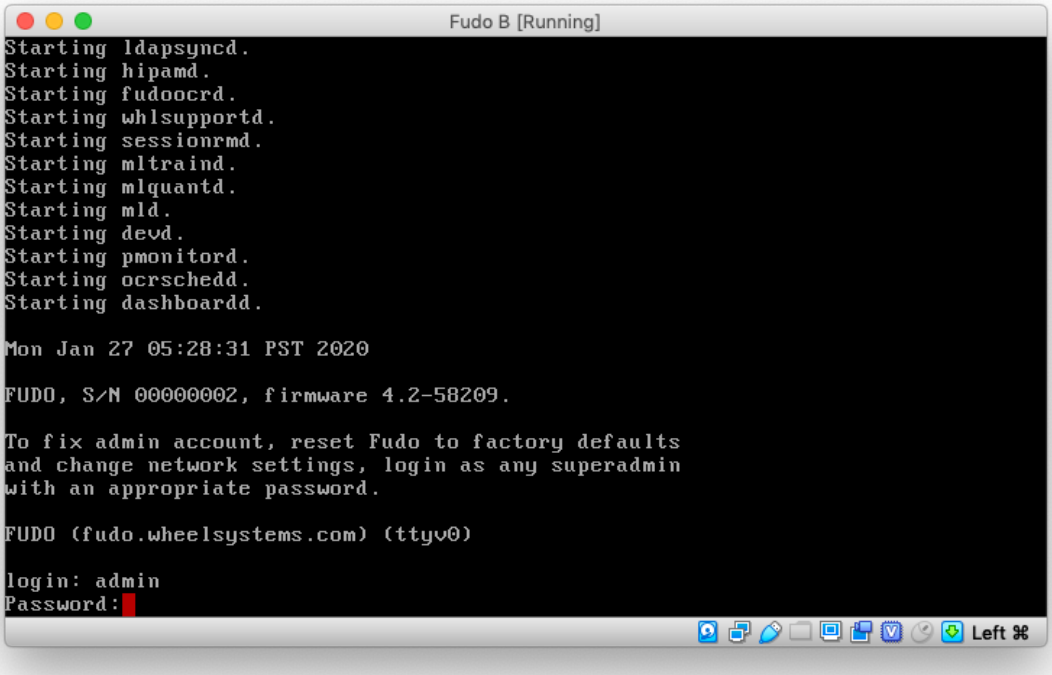
Ostrzeżenie

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.

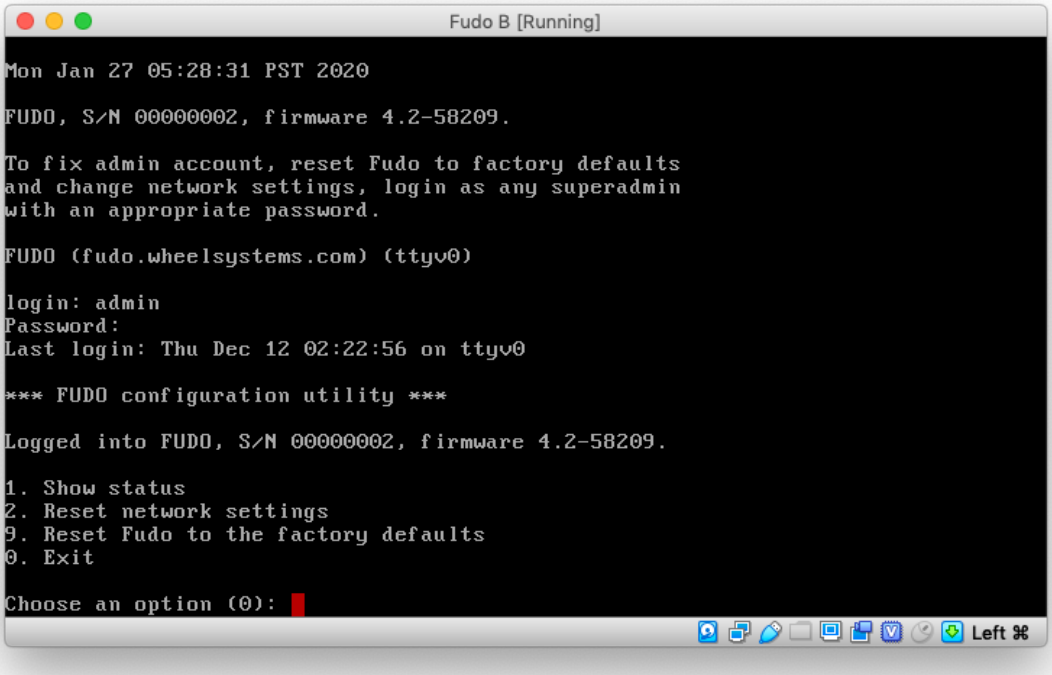
1. Uzyskaj dostęp do konsoli systemowej.
2. Wprowadź nazwę użytkownika z uprawnieniami *superadmin* i naciśnij `Enter`.



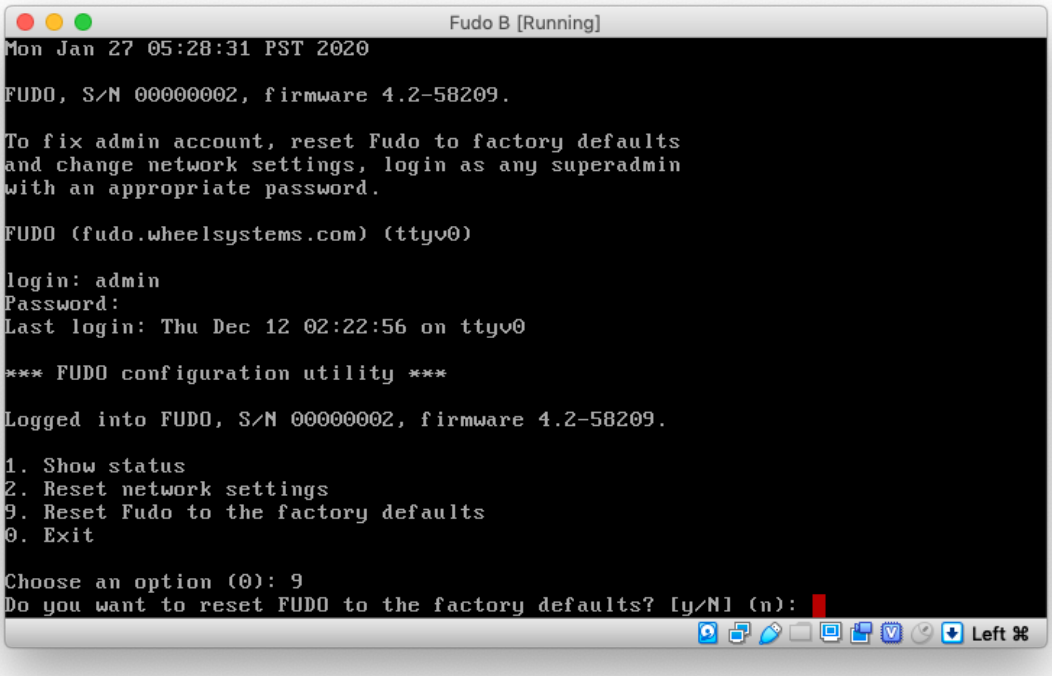
3. Wprowadź hasło i naciśnij klawisz `Enter`.



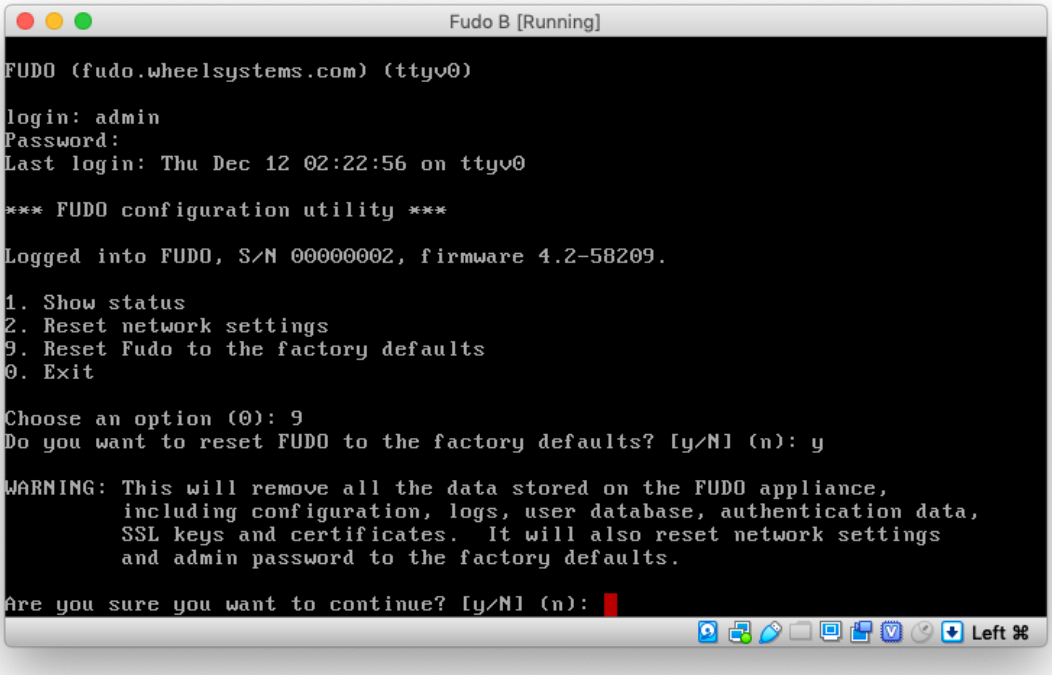
4. Wprowadź `9` i naciśnij klawisz `Enter`.



5. Wprowadź `y` i naciśnij klawisz `Enter`, aby potwierdzić wybór.



6. Wprowadź `y` i naciśnij klawisz `Enter`, aby wykonać procedurę przywrócenia ustawień fabrycznych.



Uwaga

W przypadku zdawania urządzenia demonstracyjnego, należy również wyczyścić zawartość nośnika pamięci, na którym zainicjowany został klucz szyfrujący.

Tematy pokrewne:

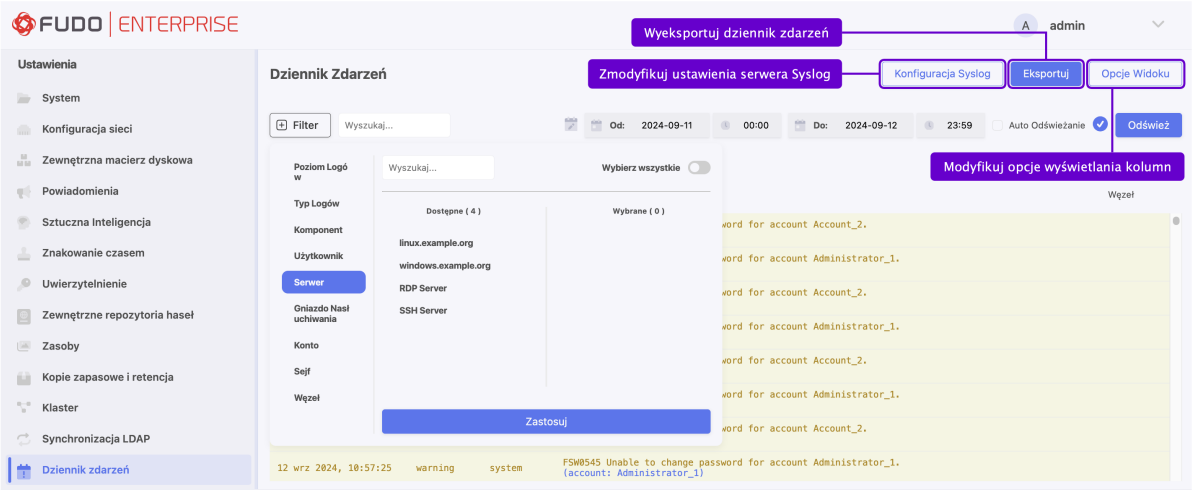
- *Konfiguracja ustawień sieciowych*
- *Czynności serwisowe*

ROZDZIAŁ 13

Dziennik zdarzeń

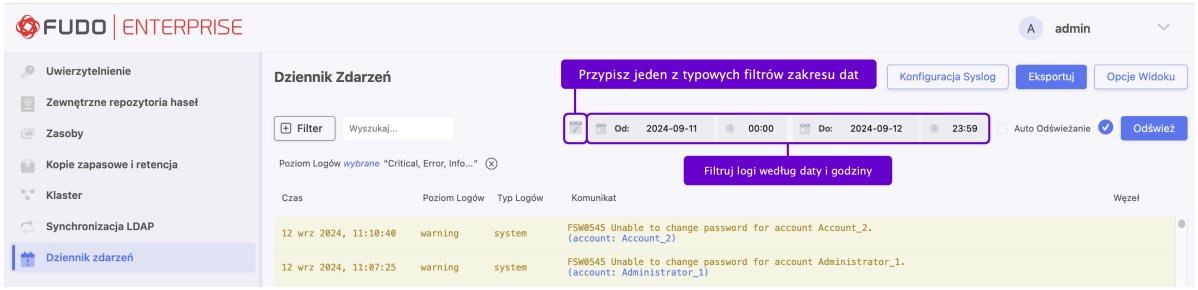
Dziennik zdarzeń stanowi wewnętrzny zapis akcji użytkowników mających wpływ na stan systemu (logowanie użytkowników, czynności administracyjne, itp.). Przejdź do rozdziału *Komunikaty dziennika zdarzeń* aby zapoznać się z listą kluczowych komunikatów dziennika.

Aby wyświetlić zawartość dziennika systemowego, wybierz *Ustawienia* > *Dziennik zdarzeń*.



13.1 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.



13.2 Zewnętrzne serwery syslog

Fudo Enterprise pozwala na przesyłanie rejestrowanych zdarzeń do zewnętrznych serwerów syslog.

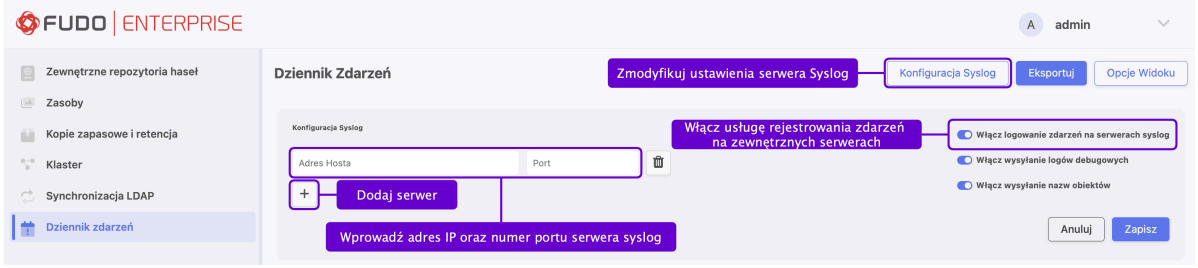
Uwaga

- W komunikacji z serwerami syslog Fudo Enterprise korzysta z protokołu UDP.
- Do komunikacji z serwerem syslog wykorzystywany jest interfejs sieciowy z włączoną funkcją **Panelu Administracyjnego**, 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*.



Uwaga

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

  `[level] TIMESTAMP TAG[PID]: MESSAGE`, gdzie:

  - `level` – poziom logowania (opcjonalnie),
  - `TIMESTAMP` – znacznik czasu,
  - `TAG` – identyfikator komponentu,
  - `PID` – identyfikator procesu,
  - `MESSAGE` – treść komunikatu.

- Przykład:

```
May 29 05:51:08 fudo[49411]: [INFO] (api) (type: admin)
(subject:  9034220852505214977) (fudo_user: 9034220852505214977)
(fudo_safe:     9034220852505214977) FAI0876 Administrator admin
connected safe main to user admin at position 0.
```

- 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

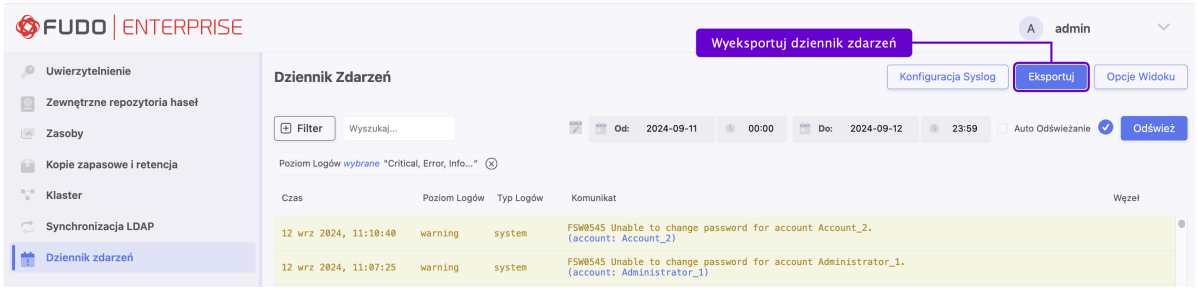
Aby usunąć serwer *Syslog*, postępuj zgodnie z poniższą instrukcją.

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*.

13.3 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*

ROZDZIAŁ 14

Aktywność konta w Portalu Użytkownika

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

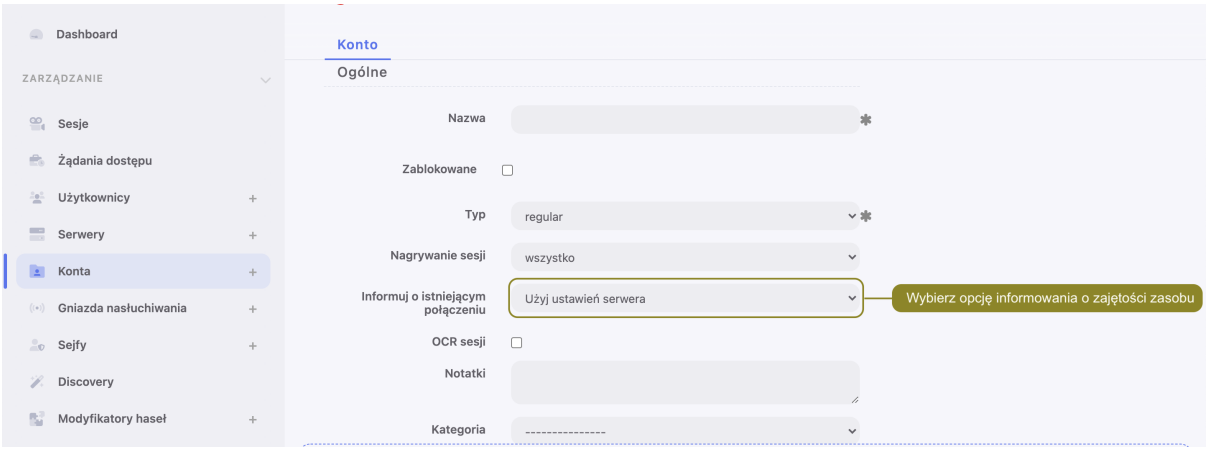
Funkcjonalność ta działa podczas nawiązywania połączenia do serwera docelowego, kiedy inny użytkownik jest już do niego połączony. Jeśli użytkownik kontynuuje nawiązanie połączenia, obecna sesja zostaje przerwana.

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 Portalu użytkownika*

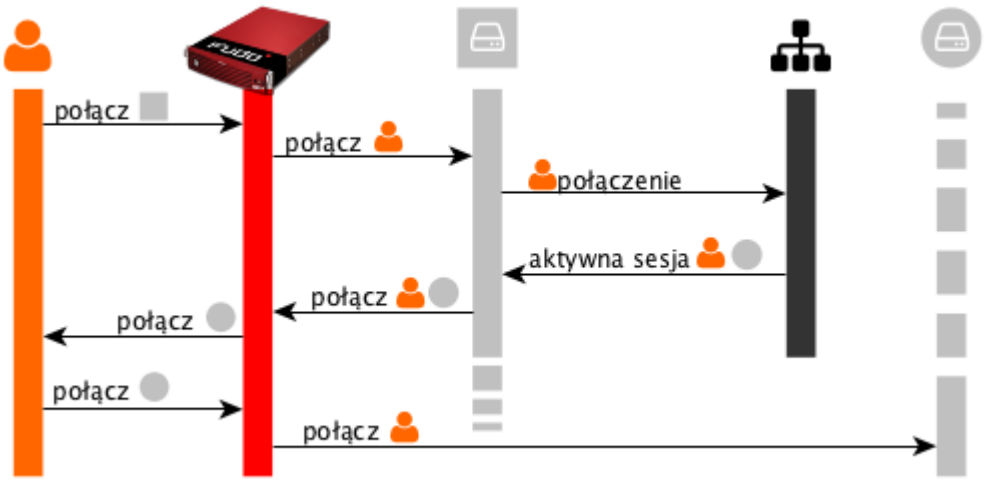
ROZDZIAŁ 15

Informacje uzupełniające

15.1 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.



Uwaga

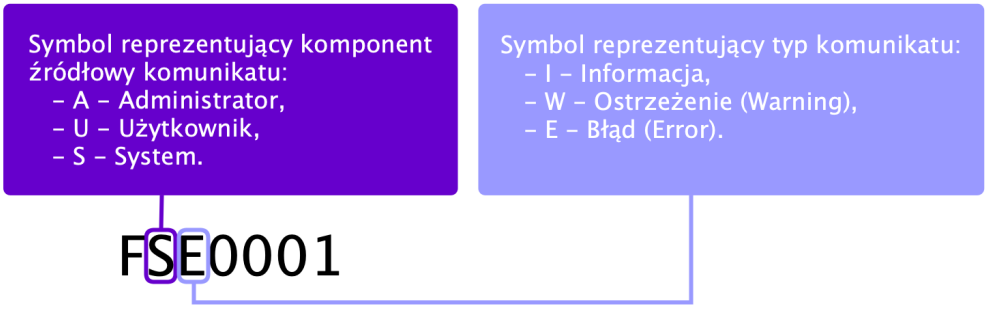
Aby proces przekierowania użytkownika się powiódł, wskazany przez broker serwer, musi być zdefiniowany na Fudo i nasłuchiwać na domyślnym porcie RDP (3389) a użytkownik musi być uprawniony do łączenia się z tym zasobem.

Tematy pokrewne:

- *Model danych*
- *RDP*
- *Zarządzanie serwerami*
- *Konta*

15.2 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).

Uwaga

*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.

ciąg dalszy 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 "{}" to {} through {} server.
FSW0037	WARNING	SYSTEM	Output from SMTP client: {}.
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.
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 (protocol: %s) 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.
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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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.
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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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: %s.
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.
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.
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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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.
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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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.
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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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.
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.
FSE0330	ERROR	SYSTEM	Bad login field configured on LDAP server %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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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 %u 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 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.
FSE0380	ERROR	SYSTEM	Unable to authorize user %s: server %s is blocked.
FSE0381	ERROR	SYSTEM	Unable to authorize user %s: account not found.
FSE0382	ERROR	SYSTEM	Unable to authorize 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 authorize user %s: safe not found.
FSE0386	ERROR	SYSTEM	Unable to authorize 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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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.
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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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.
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 {mode}.
FAI0539	INFO	ADMIN	Set configured WWN to {wwn}, external storage connection mode to {mode}.
FSW0540	WARNING	SYSTEM	Found ${cdisk} paths to fiber channel ${wwn} from ${cscbus} devices.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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: {}
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.
FAI0576	User {} changed 4 Eyes proxy API certificate settings.		
FAI0577	User {} changed 4 Eyes proxy settings.		

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSI0578	User %s (%s) was removed. Reason: user's user directory doesn't exists any more.		
FAI0579	User {} changed 4 Eyes Fudo Mobile settings.		
FSE0580	Cluster %s has an invalid token: %s.		
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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
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.
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".

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSE0666	ERROR	SYSTEM	AI training model „%s" failed: „%s".
FSI0667	INFO	SYSTEM	AI finished training model „%s". Model weight: %s
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.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSI0713	INFO	SYSTEM	Azure backup snapshot finished.
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 authorize 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 Callhome.
FAI0755	INFO	ADMIN	User %s disabled Callhome.
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.

ciąg dalszy 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: {interfaces}.
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

ciąg dalszy 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.
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.
FAI0829	INFO	ADMIN	Administrator {subject.name} deleted remote application {remote_app.name}.
FAI0830	INFO	ADMIN	User %s changed remote application %s.
FAI0831	INFO	ADMIN	User %s created remote application %s.
FAW0832	WARNING	ADMIN	Problem with NTP server. Host: %s. Message ntpdate: %s.
FSE0833	ERROR	SYSTEM	Error fetching password from LAPS. Details: %s.
FSE0834	ERROR	SYSTEM	Error fetching password from CyberArk Credential Provider. Details: %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.
FAI0839	INFO	ADMIN	Administrator {subject.name} created {account.type} account {account.name}. {account=account.id}
FAI0840	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the account {old.name} to: {attribute.value}. {account=old.id}
FAI0841	INFO	ADMIN	Administrator {subject.name} deleted {account.type} account {account.name}. {account=account.id}
FAI0842	INFO	ADMIN	Administrator {subject.name} created listener {listener.name}. {listener=listener.id}
FAI0843	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for listener {old.name} to: {attribute.value}. {listener=old.id}

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0844	INFO	ADMIN	Administrator {subject.name} deleted listener {listener.name}. {listener=listener.id}
FAI0845	INFO	ADMIN	Administrator {subject.name} created pool {pool.name}. {pool=pool.id}
FAI0846	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for pool {old.name} to: {attribute.value}. {pool=old.id}
FAI0847	INFO	ADMIN	Administrator {subject.name} deleted pool {pool.name}. {pool=pool.id}
FAI0848	INFO	ADMIN	Administrator {subject.name} created safe {safe.name}. {safe=safe.id}
FAI0849	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for safe {old.name} to: {attribute.value}. {safe=old.id}
FAI0850	INFO	ADMIN	Administrator {subject.name} deleted safe {safe.name}. {safe=safe.id}
FAI0851	INFO	ADMIN	Administrator {subject.name} created server {server.name}. {server=server.id}
FAI0852	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for server {old.name} to: {attribute.value}. {server=old.id}
FAI0853	INFO	ADMIN	Administrator {subject.name} deleted server {server.name}. {server=server.id}
FAI0854	INFO	ADMIN	Administrator {subject.name} created {user.role} {user.name}. {user=user.id}
FAI0855	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for {old.role} {old.name} to: {attribute.value}. {user=old.id}
FAI0856	INFO	ADMIN	Administrator {subject.name} deleted {user.role} {user.name}. {user=user.id}
FSW0857	WARNING	SYSTEM	Scanner %jd/%s can not remove server %s: %s
FAI0858	INFO	ADMIN	Administrator {subject.name} created a grant, giving {account_grant.to_user_role} {account_grant.to_user_name} access to account {account_grant.for_account_name}. {user=account_grant.to_user_id,account=account_grant.for_ac
FAI0859	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {account_grant.to_user_role} {account_grant.to_user_name} access to account {account_grant.for_account_name}. {user=account_grant.to_user_id,account=account_grant.for_ac
FAI0860	INFO	ADMIN	Administrator {subject.name} created a grant, giving {listener_grant.to_user_role} {listener_grant.to_user_name} access to listener {listener_grant.for_listener_name}. {user=listener_grant.to_user_id,listener=listener_grant.for_list

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0861	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {listener_grant.to_user_role} {listener_grant.to_user_name} access to listener {listener_grant.for_listener_name}. {user=listener_grant.to_user_id,listener=listener_grant.for_list
FAI0862	INFO	ADMIN	Administrator {subject.name} created a grant, giving {pool_grant.to_user_role} {pool_grant.to_user_name} access to pool {pool_grant.for_pool_name}. {user=pool_grant.to_user_id,pool=pool_grant.for_pool_id}
FAI0863	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {pool_grant.to_user_role} {pool_grant.to_user_name} access to pool {pool_grant.for_pool_name}. {user=pool_grant.to_user_id,pool=pool_grant.for_pool_id}
FAI0864	INFO	ADMIN	Administrator {subject.name} created a grant, giving {safe_grant.to_user_role} {safe_grant.to_user_name} access to safe {safe_grant.for_safe_name}. {user=safe_grant.to_user_id,safe=safe_grant.for_safe_id}
FAI0865	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {safe_grant.to_user_role} {safe_grant.to_user_name} access to safe {safe_grant.for_safe_name}. {user=safe_grant.to_user_id,safe=safe_grant.for_safe_id}
FAI0866	INFO	ADMIN	Administrator {subject.name} created a grant, giving {server_grant.to_user_role} {server_grant.to_user_name} access to server {server_grant.for_server_name}. {user=server_grant.to_user_id,server=server_grant.for_server_
FAI0867	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {server_grant.to_user_role} {server_grant.to_user_name} access to server {server_grant.for_server_name}. {user=server_grant.to_user_id,server=server_grant.for_server_
FAI0868	INFO	ADMIN	Administrator {subject.name} created a grant, giving {user_grant.to_user_role} {user_grant.to_user_name} access to {user_grant.for_user_role} {user_grant.for_user_name}. {user=user_grant.to_user_id,user=user_grant.for_user_id}
FAI0869	INFO	ADMIN	Administrator {subject.name} revoked a grant, removing {user_grant.to_user_role} {user_grant.to_user_name} access to {user_grant.for_user_role} {user_grant.for_user_name}. {user=user_grant.to_user_id,user=user_grant.for_user_id}

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0870	INFO	ADMIN	Administrator {subject.name} connected account {account_safe_listener.account_name} to safe {account_safe_listener.safe_name} through listener {account_safe_listener.listener_name}. {account=account_safe_listener.account_id,safe=account_safe_listen
FAI0871	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the connection between account {old.account_name}, safe {old.safe_name} and listener {old.listener_name} to: {attribute.value}. {account=old.account_id,safe=old.safe_id,listener=old.listener_id,liste
FAI0872	INFO	ADMIN	Administrator {subject.name} disconnected account {account_safe_listener.account_name} from safe {account_safe_listener.safe_name} through listener {account_safe_listener.listener_name}. {account=account_safe_listener.account_id,safe=account_safe_listen
FAI0873	INFO	ADMIN	Administrator {subject.name} added {user_authentication_method.type} authentication method to {user_authentication_method.user_role} {user_authentication_method.user_name} at position {user_authentication_method.position}. {user=user_authentication_method.user_id}
FAI0874	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} on {old.type} authentication method for {user_authentication_method.user_role} {user_authentication_method.user_name} at position {old.position} to: {attribute.value}. {user=old.user_id}
FAI0875	INFO	ADMIN	Administrator {subject.name} removed {user_authentication_method.type} authentication method from {user_authentication_method.user_role} {user_authentication_method.user_name} at position {user_authentication_method.position}. {user=user_authentication_method.user_id}
FAI0876	INFO	ADMIN	Administrator {subject.name} connected safe {user_safe.safe_name} to {user_safe.user_role} {user_safe.user_name} at position {user_safe.position}. {user=user_safe.user_id,safe=user_safe.safe_id}
FAI0877	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the connection between {user_safe.user_role} {user_safe.user_name} and safe {user_safe.safe_name} at position {old.position} to: {attribute.value}. {user=old.user_id,safe=old.safe_id}

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0878	INFO	ADMIN	Administrator {subject.name} disconnected safe {user_safe.safe_name} from {user_safe.user_role} {user_safe.user_name} at position {user_safe.position}. {user=user_safe.user_id,safe=user_safe.safe_id}
FAI0880	INFO	ADMIN	Administrator {subject.name} created time policy for connection between safe {user_safe_time_policy.safe_name} and {user_safe_time_policy.user_role} {user_safe_time_policy.user_name}. {user=user_safe_time_policy.user_id,safe=user_safe_time_pol
FAI0881	INFO	ADMIN	Administrator {subject.name} set attribute {attribute.name} for time policy on connection between safe {user_safe_time_policy.safe_name} and {user_safe_time_policy.user_role} {user_safe_time_policy.user_name} to: {attribute.value}. {user=user_safe_time_policy.user_id,safe=user_saf
FAI0882	INFO	ADMIN	Administrator {subject.name} removed time policy from connection between safe {user_safe_time_policy.safe_name} and {user_safe_time_policy.user_role} {user_safe_time_policy.user_name}. {user=user_safe_time_policy.user_id,safe=user_safe_time_pol
FAI0883	INFO	ADMIN	Administrator {subject.name} added authentication server {external_authentication.name} ({EXTERNAL_AUTHENTICATION.type} {external_authentication.address}:{external_authentication.port}).
FAI0884	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the authentication server {old.name} ({OLD.type} {old.address}:{old.port}) to: {attribute.value}.
FAI0885	INFO	ADMIN	Administrator {subject.name} removed authentication server {external_authentication.name} ({EXTERNAL_AUTHENTICATION.type} {external_authentication.address}:{external_authentication.port}).
FAI0886	INFO	ADMIN	Administrator {subject.name} added server {pool_server.server_name} to the pool {pool_server.pool_name}. {pool=pool_server.pool_id,server=pool_server.server_id}
FAI0887	INFO	ADMIN	Administrator {subject.name} removed server {pool_server.server_name} from the pool {pool_server.pool_name}. {pool=pool_server.pool_id,server=pool_server.server_id}
FAI0888	INFO	ADMIN	Administrator {subject.name} set configuration variable {name} to {value}.
FAI0889	INFO	ADMIN	Administrator {subject.name} created password change policy {password_change_policy.name}.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0890	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the password change policy {old.name} to: {attribute.value}.
FAI0891	INFO	ADMIN	Administrator {subject.name} deleted password change policy {password_change_policy.name}.
FAI0892	INFO	ADMIN	Administrator {subject.name} deleted hotfix {name}.
FSI0893	INFO	SYSTEM	Azure backup restored.
FAI0894	INFO	ADMIN	Administrator {subject.name} deleted session movie {session_movie.id} from session {session_movie.session_id}.
FAI0895	INFO	ADMIN	Administrator {subject.name} deleted session file {path}.
FAI0896	INFO	ADMIN	Administrator {subject.name} created label {name}.
FAI0897	INFO	ADMIN	Administrator {subject.name} set IP for label {name} to: {ip}.
FAI0898	INFO	ADMIN	Administrator {subject.name} deleted label {name}.
FSI0899	INFO	SYSTEM	Administrator {subject.name} created policy {policy.name}.
FSI0900	INFO	SYSTEM	Administrator {subject.name} set the attribute {attribute.name} for policy {old.name} to: {attribute.value}.
FSI0901	INFO	SYSTEM	Administrator {subject.name} deleted policy {policy.name}.
FSI0902	INFO	SYSTEM	Administrator {subject.name} created regular expression {regexp.name}.
FSI0903	INFO	SYSTEM	Administrator {subject.name} set the attribute {attribute.name} for regular expression {old.name} to: {attribute.value}.
FSI0904	INFO	SYSTEM	Administrator {subject.name} deleted regular expression {regexp.name}.
FAI0905	INFO	ADMIN	Administrator {subject.name} added script {script_name} for account {account_name}.
FAI0906	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for script {script_name} for account {account_name} to: {attribute.value}.
FAI0907	INFO	ADMIN	Administrator {subject.name} deleted account script {script_name} from account {account_name}.
FAI0908	INFO	ADMIN	Administrator {subject.name} triggered password changer for account {account_name}.
FAI0909	INFO	ADMIN	Administrator {subject.name} marked checkout sessions as safe for account {account_name}.
FAI0910	INFO	ADMIN	Administrator {subject.name} set discovery state to {new_state} for account {account_name}.
FAI0911	INFO	ADMIN	Administrator {subject.name} set discovery state to {new_state} for server {server_name}.
FAI0912	INFO	ADMIN	Administrator {subject.name} created report subscription {defined_report_subscription_id}.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0914	INFO	ADMIN	Administrator {subject.name} deleted report subscription {defined_report_subscription_id}.
FAI0915	INFO	ADMIN	Administrator {subject.name} exported master key.
FAI0916	INFO	ADMIN	Administrator {subject.name} invalidated master key.
FAI0917	INFO	ADMIN	Administrator {subject.name} created cluster node {node.name}.
FAI0918	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the cluster node {old.name} to: {attribute.value}.
FAI0919	INFO	ADMIN	Administrator {subject.name} deleted cluster node {node.name}.
FAI0920	INFO	ADMIN	Administrator {subject.name} created new cluster on the node {node_name}.
FAI0921	INFO	ADMIN	Administrator {subject.name} attached node with serial {serial} to the cluster.
FSI0922	INFO	SYSTEM	Email "{}" sent to {}.
FSI0923	INFO	SYSTEM	Slack notification sent to {}.
FSI0924	INFO	SYSTEM	Push notification sent to {}.
FAI0925	INFO	ADMIN	Administrator {subject.name} created OpenID Connect authentication server {oidc.name}.
FAI0926	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the OpenID Connect authentication server {old.name} to: {attribute.value}.
FAI0927	INFO	ADMIN	Administrator {subject.name} deleted OpenID Connect authentication server {oidc.name}.
FAI0928	INFO	ADMIN	Administrator {subject.name} created cluster node replication from {node_replication.local_node_name} to {node_replication.remote_node_name}.
FAI0929	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the cluster node replication from {node_replication.local_node_name} to {node_replication.remote_node_name}.
FAI0930	INFO	ADMIN	Administrator {subject.name} deleted cluster node replication from {node_replication.local_node_name} to {node_replication.remote_node_name}.
FAI0931	INFO	ADMIN	Administrator {subject.name} deleted report {report_id}.
FAE0932	ERROR	ADMIN	Failed to remove reports files.
FAI0933	INFO	ADMIN	Administrator {subject.name} created password changer {password_changer_name}.
FAI0934	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the password changer {password_changer_name} to: {attribute.value}.
FAI0935	INFO	ADMIN	Administrator {subject.name} deleted password changer {password_changer.name}.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0936	INFO	ADMIN	Administrator {subject.name} invited the user {user_name} with email {user_email} to Fudo Network organization and trusted his keys.
FAI0937	INFO	ADMIN	Administrator {subject.name} invited the user {user_name} with email {user_email} to Fudo Network organization.
FAI0938	INFO	ADMIN	Administrator {subject.name} cancelled the invitation for the user {user_name} with email {user_email}.
FAI0939	INFO	ADMIN	Administrator {subject.name} demoted successfully the redundancy group {name}.
FAI0940	INFO	ADMIN	Administrator {subject.name} restored the default logo for user access gateway.
FAI0941	INFO	ADMIN	Administrator {subject.name} restored the default logo for the RDP protocol.
FAI0942	INFO	ADMIN	Administrator {subject.name} restored the default logo for the VNC protocol.
FAI0943	INFO	ADMIN	Administrator {subject.name} changed logo for user access gateway.
FAI0944	INFO	ADMIN	Administrator {subject.name} changed logo for the RDP protocol.
FAI0945	INFO	ADMIN	Administrator {subject.name} changed logo for the VNC protocol.
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.
FAI0950	INFO	ADMIN	Administrator {subject.name} removed sub claim from {user_oidc.user_role} {user_oidc.user_name} within OpenID Connect provider {user_oidc.oidc_name}.
FAI0951	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the {user_oidc.user_role} {user_safe.user_name} within OpenID Connect provider {user_oidc.oidc_name} to: {attribute.value}.
FAI0952	INFO	ADMIN	Administrator {subject.name} added sub claim {user_oidc.oidc_sub} to {user_oidc.user_role} {user_oidc.user_name} within OpenID Connect provider {user_oidc.oidc_name}.
FUE0953	ERROR	USER	User %s failed to authenticate, disconnecting.
FAI0954	INFO	ADMIN	Administrator {subject.name} removed this Fudo from Fudo Network.
FUI0955	INFO	USER	Administrator {subject.name} accepted the invitation to this Fudo and set their keys. Email: {email}, organization: {organization}.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0956	INFO	ADMIN	Administrator {subject.name} added this Fudo to ShareAccess.
FAI0957	INFO	ADMIN	Administrator {subject.name} generated new Fudo Network key.
FAE0958	ERROR	ADMIN	Failed to remove diagnostic tarball {filename}.
FAI0959	INFO	ADMIN	Administrator {subject.name} deleted diagnostic id: {id} ({filename}).
FAE0960	ERROR	ADMIN	Failed to generate diagnostic tarball.
FAI0961	INFO	ADMIN	Administrator {subject.name} generated diagnostics {filename}.
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:?}
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}
FSW0972	ERROR	SYSTEM	Job {} failed with error: {}
FSE0973	ERROR	SYSTEM	Failed to load configuration from file {configuration_path}, error: {err}
FSE0974	ERROR	SYSTEM	Failed to shutdown Fudo.
FAI0975	INFO	ADMIN	Administrator {subject.name} created report {report_id}.
FSE0976	ERROR	SYSTEM	Failed to restart Fudo.
FSE0977	ERROR	SYSTEM	Failed to change Fudo version.
FSE0978	ERROR	SYSTEM	Failed to list Fudo versions.
FAI0979	INFO	ADMIN	Administrator {subject.name} updated management gui private key and certificate.
FAI0980	INFO	ADMIN	Administrator {subject.name} updated user access gateway private key and certificate.
FAI0981	INFO	ADMIN	Administrator {subject.name} generated QR code for mobile application access.
FAI0982	INFO	ADMIN	Administrator {subject.name} created scanner {scanner.name}.
FAI0983	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for scanner {old.name} to: {attribute.value}.
FAI0984	INFO	ADMIN	Administrator {subject.name} deleted scanner {scanner.name}.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0985	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for mobile device to: {attribute.value}.
FAI0987	INFO	ADMIN	Administrator {subject.name} added backup target {backup.name} ({backup.type}).
FAI0988	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the backup target {old.name} ({old.type}) to: {attribute.value}.
FAI0989	INFO	ADMIN	Administrator {subject.name} removed backup target {backup.name} ({backup.type}).
FAI0990	INFO	ADMIN	Administrator {subject.name} added user directory {user_directory.name} ({USER_DIRECTORY.type}).
FAI0991	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the user directory {old.name} ({OLD.type}) to: {attribute.value}.
FAI0992	INFO	ADMIN	Administrator {subject.name} removed user directory {user_directory.name} ({USER_DIRECTORY.type}).
FAI0993	INFO	ADMIN	Administrator {subject.name} added server {user_directory_server.address}:{user_directory_server.port} to the user directory {user_directory_server.user_directory_name} ({user_directory_server.user_directory_type}).
FAI0994	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the server {old.address}:{old.port} in the user directory {old.user_directory_name} ({OLD.user_directory_type}) to: {attribute.value}.
FAI0995	INFO	ADMIN	Administrator {subject.name} removed server {user_directory_server.address}:{user_directory_server.port} from the user directory {user_directory_server.user_directory_name} ({user_directory_server.user_directory_type}).
FAI0996	INFO	ADMIN	Administrator {subject.name} added group mapping {user_directory_safe.group_path} -> {user_directory_safe.safe_name} to the user directory {user_directory_safe.user_directory_name} ({user_directory_safe.user_directory_type}).
FAI0997	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the group mapping {old.group_path} -> {old.safe_name} in the user directory {old.user_directory_name} ({OLD.user_directory_type}) to: {attribute.value}.
FAI0998	INFO	ADMIN	Administrator {subject.name} removed group mapping {user_directory_safe.group_path} -> {user_directory_safe.safe_name} from the user directory {user_directory_safe.user_directory_name} ({user_directory_safe.user_directory_type}).

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI0999	INFO	ADMIN	Administrator {subject.name} added authentication server {user_directory_safe_external_authentication.external_authent ({user_directory_safe_external_authentication.external_authen {user_directory_safe_external_authentication.external_authent to the group mapping {user_directory_safe_external_authentication.group_path} -> {user_directory_safe_external_authentication.safe_name} in the user directory {user_directory_safe_external_authentication.user_directory_n ({user_directory_safe_external_authentication.user_directory_
FAI1000	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the authentication server {old.external_authentication_name} ({OLD.external_authentication_type} {old.external_authentication_address}:{old.external_authenticat in the group mapping {old.group_path} -> {old.safe_name} for the user directory {old.user_directory_name} ({old.user_directory_type}) to: {attribute.value}.
FAI1001	INFO	ADMIN	Administrator {subject.name} removed authentication server {user_directory_safe_external_authentication.external_authent ({user_directory_safe_external_authentication.external_authen {user_directory_safe_external_authentication.external_authent from the group mapping {user_directory_safe_external_authentication.group_path} -> {user_directory_safe_external_authentication.safe_name} in the user directory {user_directory_safe_external_authentication.user_directory_n ({user_directory_safe_external_authentication.user_directory_
FSW1004	WARNING	SYSTEM	Fetched maximum amount ({}) of groups for User Directory search. Provide more precise filter for all results.
FSE1005	ERROR	SYSTEM	Unable to accept access request: %s.
FUE1006	ERROR	USER	MySQL packet parsing failed with %d: %s.
FUE1007	ERROR	USER	Unexpected MySQL packet received: %s.
FAI1008	INFO	ADMIN	Administrator {subject.name} enforced full user directory synchronization on {user_directory_name}.
FSI1009	INFO	SYSTEM	Organization synchronized: {}.
FAI1012	INFO	ADMIN	Administrator {subject.name} set the user directory synchronization {attribute.name} to: {attribute.value}.
FAI1013	INFO	ADMIN	Administrator {subject.name} uploaded license file.
FSI1014	INFO	SYSTEM	Administrator {subject.name} created remote application {remote_app_name}.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSI1015	INFO	SYSTEM	Administrator {subject.name} set the attribute {attribute.name} for remote application {remote_app_name} to: {attribute.value}.
FAI1016	INFO	ADMIN	Administrator {subject.name} changed member status of {emails} to {status}.
FAI1017	INFO	ADMIN	Administrator {subject.name} uploaded new upgrade package (version: {version}, size: {size}).
FUW1018	WARNING	USER	Client send data exceeding window size. Closing the channel.
FUI1019	INFO	USER	Forwarding connection from %s:%s to %s:%s.
FAI1020	INFO	ADMIN	Administrator {subject.name} uploaded new hotfix package (name: {name}, size: {size}).
FAI1021	INFO	ADMIN	Administrator {subject.name} uploaded new license to Fudo Network.
FAI1022	INFO	ADMIN	Administrator {subject.name} started trial in Fudo Network.
FAI1023	INFO	ADMIN	Administrator {subject.name} generated key for session share access (readonly={session_share.readonly}). {session=session_share.session_id}
FAI1025	INFO	ADMIN	Administrator {subject.name} terminated session {session_terminate.session_id}. {session=session_terminate.session_id}
FAI1026	INFO	ADMIN	Administrator {subject.name} created comment {session_comment.id} for session {session_comment.session_id}. {session=session_comment.session_id}
FAI1027	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for comment {old.id} to: {attribute.value}. {session=old.session_id}
FAI1028	INFO	ADMIN	Administrator {subject.name} removed comment {session_comment.id} for session {session_comment.session_id}. {session=session_comment.session_id}
FAI1029	INFO	ADMIN	Administrator {subject.name} renamed label {oldname} to {name}.
FAI1030	INFO	ADMIN	Administrator {subject.name} deleted upgrade package.
FAI1031	INFO	ADMIN	Administrator {subject.name} deleted upgrade snapshot.
FAI1032	INFO	ADMIN	Administrator {subject.name} has started an upgrade on Fudo (version: {version}).
FAI1033	INFO	ADMIN	Administrator {subject.name} upgraded Fudo (version: {version}).
FAI1034	INFO	ADMIN	Administrator {subject.name} requested system configuration export.
FSI1035	INFO	SYSTEM	Preview access from request (%s) granted.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1036	INFO	ADMIN	Administrator {subject.name} requested service data.
FAI1037	INFO	ADMIN	Administrator {subject.name} imported system configuration.
FAI1038	INFO	ADMIN	Administrator {subject.name} deleted session {session_id}. {session=session_id}
FAI1039	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for timestamping to: {attribute.value}.
FAI1040	INFO	ADMIN	Administrator {subject.name} changed timezone from {old} to {new}.
FAI1041	INFO	ADMIN	Administrator {subject.name} displayed current password for account {account_name}. Reason: {reason}
FAI1042	INFO	ADMIN	Administrator {subject.name} displayed current password for account {account_name}.
FSE1043	ERROR	SYSTEM	Error generating report {}.
FAI1045	INFO	ADMIN	Administrator {subject.name} changed ntp from {old} to {new}.
FAI1047	INFO	ADMIN	Administrator {subject.name} has started replication of session {session_replica.session_id} on node {session_replica.session_on}. {session=session_replica.session_id}
FAI1048	INFO	ADMIN	Administrator {subject.name} has started OCR of session {session_ocr.session_id}. {session=session_ocr.session_id}
FAI1049	INFO	ADMIN	Administrator {subject.name} has updated their static password.
FAI1050	INFO	ADMIN	Administrator {subject.name} approved the session {session_id}.
FAI1051	INFO	ADMIN	Administrator {subject.name} rejected the session {session_id} and blocked the user {user_name}.
FAI1052	INFO	ADMIN	Administrator {subject.name} rejected the session {session_id}.
FAI1053	INFO	ADMIN	Administrator {subject.name} resent undelivered mail for {mail_type} {object_id} to user {recipient_id}.
FAI1054	INFO	ADMIN	Administrator {subject.name} removed undelivered mail for {mail_type} {object_id} to user {recipient_id}.
FAI1055	INFO	ADMIN	Administrator {subject.name} created the group {group.name}.
FAI1056	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the group {old.name} to: {attribute.value}.
FAI1057	INFO	ADMIN	Administrator {subject.name} deleted the group {group.name}.
FAI1058	INFO	ADMIN	Administrator {subject.name} added user {group_user.user_name} to the group {group_user.group_name}. {user=group_user.user_id}

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1059	INFO	ADMIN	Administrator {subject.name} removed user {group_user.user_name} from the group {group_user.group_name}. {user=group_user.user_id}
FAI1060	INFO	ADMIN	Administrator {subject.name} connected safe {group_safe.safe_name} to the group {group_safe.group_name}. {safe=group_safe.safe_id}
FAI1061	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the connection between group {group_safe.group_name} and safe {group_safe.safe_name} to: {attribute.value}. {safe=group_safe.safe_id}
FAI1062	INFO	ADMIN	Administrator {subject.name} disconnected safe {group_safe.safe_name} from the group {group_safe.group_name}. {safe=group_safe.safe_id}
FAI1063	INFO	ADMIN	Administrator {subject.name} created time policy for connection between safe {group_safe_time_policy.safe_name} and the group {group_safe_time_policy.group_name}. {safe=group_safe_time_policy.safe_id}
FAI1064	INFO	ADMIN	Administrator {subject.name} set attribute {attribute.name} for time policy on connection between safe {group_safe_time_policy.safe_name} and the group {group_safe_time_policy.group_name} to: {attribute.value}. {safe=group_safe_time_policy.safe_id}
FAI1065	INFO	ADMIN	Administrator {subject.name} removed time policy from connection between safe {group_safe_time_policy.safe_name} and the group {group_safe_time_policy.group_name}. {safe=group_safe_time_policy.safe_id}
FAI1066	INFO	ADMIN	Administrator {subject.name} requested timestamping for the session {session_id}.
FAI1067	INFO	ADMIN	Administrator {subject.name} canceled timestamping for the session {session_id}.
FAI1068	INFO	ADMIN	Administrator {subject.name} revoked shared session (session_id={session_id}).
FAI1069	INFO	ADMIN	Administrator {subject.name} requested session {session_id} from archive.
FAI1070	INFO	ADMIN	Administrator {subject.name} deleted defied report {defined_report_id}.
FAI1071	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the defined report {old.name} to: {attribute.value}.
FAI1072	INFO	ADMIN	Administrator {subject.name} created role {role.name} with privileges {role.privs}.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1073	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for role {old.name} to: {attribute.value}.
FAI1074	INFO	ADMIN	Administrator {subject.name} granted role {old.name} privileges: {attribute.value}.
FAI1075	INFO	ADMIN	Administrator {subject.name} revoked role {old.name} privileges: {attribute.value}.
FAI1076	INFO	ADMIN	Administrator {subject.name} deleted role {role.name}.
FAI1077	INFO	ADMIN	Administrator {subject.name} added user {user_role.user_name} role {user_role.role_name}. {user=user_role.user_id}
FAI1078	INFO	ADMIN	Administrator {subject.name} removed user {user_role.user_name} role {user_role.role_name}. {user=user_role.user_id}
FAI1079	INFO	ADMIN	Administrator {subject.name} created a capability, granting %s {%s.subject_name} the following rights to the %s {%s.object_name}: {%s.rights}.
FAI1080	INFO	ADMIN	Administrator {subject.name} revoked a capability, removing %s's {%s.subject_name} access to %s {%s.object_name}.
FAI1081	INFO	ADMIN	Administrator {subject.name} set %s {%s.subject_name} rights to the %s {%s.object_name} to: {attribute.value}.
FAI1082	INFO	ADMIN	Administrator {subject.name} granted %s {%s.subject_name} rights to the %s {%s.object_name}: {attribute.value}.
FAI1083	INFO	ADMIN	Administrator {subject.name} revoked %s's {%s.subject_name} rights to the %s {%s.object_name}: {attribute.value}.
FAI1084	INFO	ADMIN	Administrator {subject.name} created discovery rule {rule.name}.
FAI1085	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for discovery rule {old.name} to: {attribute.value}.
FAI1086	INFO	ADMIN	Administrator {subject.name} deleted discovery rule {rule.name}.
FAI1087	INFO	ADMIN	Administrator {subject.name} added listener {rule_listener.listener_name} to the discovery rule {rule_listener.rule_name}. {listener=rule_listener.listener_id}
FAI1088	INFO	ADMIN	Administrator {subject.name} removed listener {rule_listener.listener_name} from the discovery rule {rule_listener.rule_name}. {listener=rule_listener.listener_id}
FAI1089	INFO	ADMIN	Administrator {subject.name} added pool {rule_pool.pool_name} to the discovery rule {rule_pool.rule_name}. {pool=rule_pool.pool_id}

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1090	INFO	ADMIN	Administrator {subject.name} removed pool {rule_pool.pool_name} from the discovery rule {rule_pool.rule_name}. {pool=rule_pool.pool_id}
FAI1091	INFO	ADMIN	Administrator {subject.name} added safe {rule_safe.safe_name} to the discovery rule {rule_safe.rule_name}. {safe=rule_safe.safe_id}
FAI1092	INFO	ADMIN	Administrator {subject.name} removed safe {rule_safe.safe_name} from the discovery rule {rule_safe.rule_name}. {safe=rule_safe.safe_id}
FAI1093	INFO	ADMIN	Administrator {subject.name} added mapping for Group {user_directory_group_group.group_name} to the group mapping {user_directory_group_group.user_directory_group_path} in the user directory {user_directory_group_group.user_directory_name} ({user_directory_group_group.user_directory_type}).
FAI1094	INFO	ADMIN	Administrator {subject.name} removed mapping for Group {user_directory_group_group.group_name} from the group mapping {user_directory_group_group.user_directory_group_path} in the user directory {user_directory_group_group.user_directory_name} ({user_directory_group_group.user_directory_type}).
FAI1095	INFO	ADMIN	Administrator {subject.name} added mapping for Role {user_directory_group_role.role_name} to the group mapping {user_directory_group_role.group_path} in the user directory {user_directory_group_role.user_directory_name} ({user_directory_group_role.user_directory_type}).
FAI1096	INFO	ADMIN	Administrator {subject.name} removed mapping for Role {user_directory_group_role.role_name} from the group mapping {user_directory_group_role.group_path} in the user directory {user_directory_group_role.user_directory_name} ({user_directory_group_role.user_directory_type}).
FAI1097	INFO	ADMIN	Administrator {subject.name} removed authentication server {user_directory_group_authentication.external_authentication_ ({user_directory_group_authentication.external_authentication {user_directory_group_authentication.external_authentication_ from the group mapping {user_directory_group_authentication.user_directory_group_p in the user directory {user_directory_group_authentication.user_directory_name} ({user_directory_group_authentication.user_directory_type}).

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1098	INFO	ADMIN	Administrator {subject.name} removed group mapping {user_directory_group.group_path} from the user directory {user_directory_group.user_directory_name} ({user_directory_group.user_directory_type}).
FAI1099	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the group mapping {old.group_path} in the user directory {old.user_directory_name} ({OLD.user_directory_type}) to: {attribute.value}.
FAI1100	INFO	ADMIN	Administrator {subject.name} added group mapping {user_directory_group.group_path} to the user directory {user_directory_safe.user_directory_name} ({user_directory_group.user_directory_type}).
FAI1101	INFO	ADMIN	Administrator {subject.name} added authentication server {user_directory_group_authentication.external_authentication_ ({user_directory_group_authentication.external_authentication {user_directory_group_authentication.external_authentication_ to the group mapping {user_directory_group_authentication.user_directory_group_p in the user directory {user_directory_group_authentication.user_directory_name} ({user_directory_group_authentication.user_directory_type}).
FAI1102	INFO	ADMIN	Administrator {subject.name} added rule {scanner_rule.rule_name} to scanner {scanner_rule.scanner_name} at position {scanner_rule.position}.
FAI1103	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the connection between scanner {scanner_rule.scanner_name} and rule {scanner_rule.rule_name} at position {old.position} to: {attribute.value}.
FAI1104	INFO	ADMIN	Administrator {subject.name} removed rule {scanner_rule.rule_name} from scanner {scanner_rule.scanner_name} at position {scanner_rule.position}.
FAI1105	INFO	ADMIN	Administrator {subject.name} started scanner {scanner.name}.
FSW1106	WARNING	SYSTEM	Failed to synchronize authentication method (%s) for user %s.
FSW1107	WARNING	SYSTEM	AI cannot transfer model „%s". Model version has changed. This is expected, and the model will be retrained during the next scheduled training cycle. To retrain immediately, adjust the training schedule.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSW1108	WARNING	SYSTEM	AI failed to load model „%s" during transfer. The model will be retrained during the next scheduled training cycle. To retrain immediately, adjust the training schedule.
FSW1109	WARNING	SYSTEM	AI failed to update model „%s" during model transfer.
FAI1110	INFO	ADMIN	{Subject.role} {subject.name} restarted tunnels to Fudo Network.
FSE1113	ERROR	SYSTEM	Connection error: {err}.
FSE1114	ERROR	SYSTEM	Failed to set NODELAY on socket bound to {addr}: {err}.
FSI1115	INFO	SYSTEM	Updated member status of {email} to {status}.
FSE1116	ERROR	SYSTEM	Error handling socket connection.
FAI1117	INFO	ADMIN	Administrator {subject.name} created collection {collection.name}. {collection=collection.id}
FAI1118	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the collection {old.name} to: {attribute.value}. {collection=collection.id}
FSE1119	ERROR	SYSTEM	Session summary failure for session : {err}.
FSI1120	INFO	SYSTEM	Session summary finished for session.
FAI1121	INFO	ADMIN	Administrator {subject.name} created secret {secret.name}. {collection=secret.collection_id,secret=secret.id}
FAI1122	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the secret {old.name} to: {attribute.value}. {collection=secret.collection_id,secret=secret.id}
FAI1123	INFO	ADMIN	Administrator {subject.name} removed secret {secret.name}. {collection=secret.collection_id,secret=secret.id}
FAI1124	INFO	ADMIN	User {subject.name} started summary for session {session_summary.session_id}. {session=session_summary.session_id}
FAI1125	INFO	ADMIN	Administrator {subject.name} created uri {secret_uri.uri} for the secret {secret_uri.secret_name}. {collection=secret_uri.collection_id,secret=secret_uri.secret_id}
FAI1126	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the uri {old.uri} in the secret {secret_uri.secret_name} to: {attribute.value}. {collection=secret_uri.collection_id,secret=secret_uri.secret_id}
FAI1127	INFO	ADMIN	Administrator {subject.name} removed uri {secret_uri.uri} from the secret {secret_uri.secret_name}. {collection=secret_uri.collection_id,secret=secret_uri.secret_id}

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1133	INFO	ADMIN	Administrator {subject.name} added group {group.name} to the collection {collection.name}. {collection=group_collection.collection_id,group=group_collection.grou
FAI1134	INFO	ADMIN	Administrator {subject.name} removed group {group.name} from the collection {collection.name}. {collection=group_collection.collection_id,group=group_collection.grou
FAI1137	INFO	ADMIN	Administrator {subject.name} added user {user.name} to the collection {collection.name}. {collection=user_collection.collection_id,user=user_collection.user_id}
FAI1138	INFO	ADMIN	Administrator {subject.name} removed user {user.name} from the collection {collection.name}. {collection=user_collection.collection_id,user=user_collection.user_id}
FSE1139	ERROR	SYSTEM	Error fetching password from Vault. Details: %s.
FUI1140	INFO	USER	PostgreSQL connection terminated.
FUE1141	ERROR	USER	PostgreSQL connection error.
FUE1142	ERROR	USER	Invalid PostgreSQL startup message length: %u.
FUE1143	ERROR	USER	Invalid PostgreSQL message length: %u.
FUE1144	ERROR	USER	Backend authentication failed.
FUI1145	INFO	USER	Successfully authenticated against server %s as user %s.
FUE1146	ERROR	USER	PostgreSQL packet parsing failed with %d: %s.
FAI1147	INFO	ADMIN	Administrator {subject.name} removed collection {collection.name}. {collection=collection.id}
FAI1148	INFO	ADMIN	Administrator {subject.name} set attribute {attribute.name} to {attribute.value} for user {user.name}»s access to collection {collection.name}. {collection=user_collection.collection_id,user=user_collection.user_id}
FAI1149	INFO	ADMIN	Administrator {subject.name} set attribute {attribute.name} to {attribute.value} for group {group.name}»s access to collection {collection.name}. {collection=group_collection.collection_id,group=group_collection.grou
FUI1150	INFO	USER	User {subject.name} created uri {secret_uri.uri} for the secret {secret_uri.secret_name}. {collection=secret_uri.collection_id,secret=secret_uri.secret_id}
FUI1151	INFO	USER	User {subject.name} set the attribute {attribute.name} for the uri {old.uri} in the secret {secret_uri.secret_name} to: {attribute.value}. {secret=secret_uri.secret_id}
FUI1152	INFO	USER	User {subject.name} removed uri {secret_uri.uri} from the secret {secret_uri.secret_name}. {secret=secret_uri.secret_id}

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FUI1153	INFO	USER	User {subject.name} created secret {secret.name}. {collection=secret.collection_id,secret=secret.id}
FUI1154	INFO	USER	User {subject.name} set the attribute {attribute.name} for the secret {old.name} to: {attribute.value}. {collection=secret.collection_id,secret=secret.id}
FUI1155	INFO	USER	User {subject.name} removed secret {secret.name}. {collection=secret.collection_id,secret=secret.id}
FSI1162	INFO	SYSTEM	User %s expiration date will be updated.
FAI1163	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} of vault configuration to: {attribute.value}.
FAI1164	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for the reverse proxy {old.name} to: {attribute.value}.
FAI1165	INFO	ADMIN	Administrator {subject.name} created reverse proxy {reverse_proxy.name} ({reverse_proxy.id}).# FSW1166 –BU-1139-reverse-proxy
FAI1167	INFO	ADMIN	Administrator {subject.name} removed reverse proxy {reverse_proxy.name} ({reverse_proxy.id}).
FAI1168	INFO	ADMIN	Administrator {subject.name} added listener {reverse_proxy_listener.id} to reverse proxy {reverse_proxy_listener.reverse_proxy_id}.
FAI1169	INFO	ADMIN	Administrator {subject.name} removed listener {reverse_proxy_listener.id} from reverse proxy {reverse_proxy_listener.reverse_proxy_id}.
FSW1170	WARNING	SYSTEM	Failed to add mapping {} to the tunnel for reverse proxy {} ({}).
FSI1171	INFO	SYSTEM	Added mapping {} to the tunnel for reverse proxy {} ({}).
FSW1172	WARNING	SYSTEM	Failed to remove mapping {} from the tunnel for reverse proxy {} ({}).
FSI1173	INFO	SYSTEM	Removed mapping {} for the tunnel for reverse proxy {} ({}).
FSW1174	WARNING	SYSTEM	Failed to create tunnel for reverse proxy {} ({}).
FSI1175	INFO	SYSTEM	Created tunnel for reverse proxy {} ({}) with status Running.
FSW1176	WARNING	SYSTEM	Failed to terminate tunnel for reverse proxy {} ({}).
FSI1177	INFO	SYSTEM	Terminated tunnel for reverse proxy {}.
FSW1178	WARNING	SYSTEM	Failed to check tunnel for reverse proxy {} ({}).
FSW1179	WARNING	SYSTEM	Failed to fetch running reverse proxy tunnels.
FSW1180	WARNING	SYSTEM	Failed to get system IP addresses to verify reverse proxy tunnels.
FSW1181	WARNING	SYSTEM	Tunnel for reverse proxy {} ({}) is degraded.{}
FSW1182	WARNING	SYSTEM	Tunnel for reverse proxy {} ({}) is dead.
FSW1183	WARNING	SYSTEM	Failed to get running tunnels to close dangling tunnels.
FSI1184	INFO	SYSTEM	Terminated dangling tunnel {} to {}:{}.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FSE1185	ERROR	SYSTEM	Failed to terminate dangling tunnel {} to {}:{}.
FSE1186	ERROR	SYSTEM	Failed to update reverse proxy {reverse_proxy_id} status.
FSE1187	ERROR	SYSTEM	Failed to initialize reverse proxy service.
FSE1188	ERROR	SYSTEM	Reverse proxy health check service failed.
FSE1189	ERROR	SYSTEM	Reverse proxy event listener service failed.
FSW1190	WARNING	SYSTEM	Cannot add mapping to tunnel for reverse proxy listener {reverse_proxy_listener_id}. Listen address is on different node than bind address of reverse proxy.
FSW1191	WARNING	SYSTEM	Cannot add mapping to tunnel for reverse proxy listener {reverse_proxy_listener_id}. Mapping uses listen address from another node than reverse proxy bind IP.
FSW1192	WARNING	SYSTEM	Failed to update list of reverse proxy tunnels that are health checked.
FSE1193	ERROR	SYSTEM	Failed to check existing reverse proxy tunnels.
FSE1194	ERROR	SYSTEM	Failed to connect to the database to listen for reverse proxy events
FUI1195	INFO	USER	User {subject.name} retrieved secret {secret.name}.
FSE1196	ERROR	SYSTEM	Failed to listen to database notifications to handle reverse proxy events.
FSE1197	ERROR	SYSTEM	Failed to receive notification from database to handle reverse proxy events.
FSE1198	ERROR	SYSTEM	Unrecognized error while handling reverse proxy event.
FSW1199	WARNING	SYSTEM	Invalid format for remote address: {}.
FSW1200	WARNING	SYSTEM	Invalid format for local address: {}.
FAI1201	INFO	ADMIN	Administrator {subject.name} created notification filter for user {notification_filter.user_name} and safe {notification_filter.safe_name}. {user=notification_filter.user_id,safe=notification_filter.safe_id}
FAI1202	INFO	ADMIN	Administrator {subject.name} deleted notification filter for user {notification_filter.user_name} and safe {notification_filter.safe_name}. {user=notification_filter.user_id,safe=notification_filter.safe_id}
FAI1203	INFO	ADMIN	Administrator {subject.name} added regexp {regexp_policy.regexp_name} to policy {regexp_policy.policy_name}.
FAI1204	INFO	ADMIN	Administrator {subject.name} removed regexp {regexp_policy.regexp_name} from policy {regexp_policy.policy_name}.
FAI1205	INFO	ADMIN	Administrator {subject.name} added policy {safe_policy.policy_name} to safe {safe_policy.safe_name}. {safe=safe_policy.safe_id}
FAI1206	INFO	ADMIN	Administrator {subject.name} removed policy {safe_policy.policy_name} from safe {safe_policy.safe_name}. {safe=safe_policy.safe_id}
FAI1207	INFO	ADMIN	Administrator {subject.name} created password vault {passvn.name} ({passvn.type}).

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1208	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for password vault {old.name} ({old.type}) to: {attribute.value}.
FAI1209	INFO	ADMIN	Administrator {subject.name} deleted password vault {passvn.name} ({passvn.type}).
FAI1210	INFO	ADMIN	User {subject.name} enabled sensitive feature {sensitive_feature_user.name}.
FAI1211	INFO	ADMIN	User {subject.name} disabled sensitive feature {sensitive_feature_user.name}.
FAI1212	INFO	ADMIN	Administrator {subject.name} set discovery state for account {discovery.account_name} to: {discovery.state}. {account=discovery.account_id}
FAI1213	INFO	ADMIN	Administrator {subject.name} set discovery state for server {discovery.server_name} to: {discovery.state}. {server=discovery.server_id}
FAI1214	INFO	ADMIN	Administrator {subject.name} backed up session {session_id} to backup {backup_name}.
FSI1215	INFO	SYSTEM	Terminating tunnel for reverse proxy {} ({}) - no working mappings (configured: {}).
FSW1216	WARNING	SYSTEM	Tunnel for reverse proxy {} ({}) has no working mappings (configured: {}). Will terminate and recreate.
FUE1217	ERROR	USER	User mismatch in tunneled session (%s != %s).
FUE1218	ERROR	USER	Account mismatch in tunneled session (%s != %s).
FUE1219	ERROR	USER	Server mismatch in tunneled session (%s != %s).
FUI1220	INFO	USER	User {subject.name} created collection {collection.name}. {collection=collection.id}
FUI1221	INFO	USER	User {subject.name} set the attribute {attribute.name} for the collection {old.name} to: {attribute.value}. {collection=collection.id}
FUI1222	INFO	USER	User {subject.name} removed collection {collection.name}. {collection=collection.id}
FSW1223	WARNING	SYSTEM	Created tunnel for reverse proxy {} ({}) with status Degraded. Failed to add some mappings.
FAI1225	Administrator {subject.name} saved secret {secret_name} with policy violations: {violations}. {collection=collectio		

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FUI1226	INFO	USER	User {subject.name} saved secret {secret_name} with policy violations: {violations}. {collection=collection_id,secret=secret_id}
FSE1227	ERROR	SYSTEM	File upload failed. Error: {} (status {}).
FSI1228	INFO	SYSTEM	File upload started: {}.
FSI1229	INFO	SYSTEM	File download started: {}.
FSI1230	INFO	SYSTEM	File upload completed: {} ({} bytes).
FSI1231	INFO	SYSTEM	File download completed: {} ({} bytes).
FUI1232	INFO	USER	User {subject.name} revealed secret {secret.name} history entry {history.id} (version {history.created_at}).
FAI1233	INFO	ADMIN	Administrator {subject.name} added password_changer {password_changer.name} to the secret {secret.name}. {secret=secret_password_changer.secret_id,collection=secret_passv
FAI1234	INFO	ADMIN	Administrator {subject.name} set attribute {attribute.name} to {attribute.value} for password_changer {password_changer.name}»s assignment to secret {secret.name}. {secret=secret_password_changer.secret_id,collection=secret_passv
FAI1235	INFO	ADMIN	Administrator {subject.name} removed password_changer {password_changer.name} from the secret {secret.name}. {secret=secret_password_changer.secret_id,collection=secret_passv
FAI1236	INFO	ADMIN	Administrator {subject.name} triggered password changer for secret {secret_name}. {secret=secret_id,collection=secret_password_changer.collection_id
FUI1237	INFO	USER	User {subject.name} checked in secret {secret.name}.
FSW1238	WARNING	SYSTEM	AI model file for „%s” not found on node %s during transfer. The model will be retrained during the next scheduled training cycle. To retrain immediately, adjust the training schedule.
FAI1239	INFO	ADMIN	Administrator {subject.name} removed license file.
FUE1240	ERROR	USER	FIDO2 registration failed for user %s: %s.
FUI1241	INFO	USER	User {subject.name} registered FIDO2 credentials.
FUE1242	ERROR	USER	FIDO2 authentication failed from address %s: %s.
FUE1243	ERROR	USER	FIDO2 authentication failed for user %s from address %s: %s.
FUI1244	INFO	USER	User %s presence confirmed during FIDO2 authentication.
FUI1245	INFO	USER	User %s verified during FIDO2 authentication.
FUI1246	INFO	USER	User %s authenticated using FIDO2 (%s) logged in from address: %s.
FUE1247	ERROR	USER	FIDO2 discovery failed: %s.

ciąg dalszy na następnej stronie

Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1248	INFO	ADMIN	Administrator {subject.name} set the attribute {attribute.name} for authentication server {user_directory_group_authentication.external_authentication_ ({user_directory_group_authentication.external_authentication in the group mapping {user_directory_group_authentication.user_directory_group_p in the user directory {user_directory_group_authentication.user_directory_name} ({user_directory_group_authentication.user_directory_type}) to: {attribute.value}.
FUI1249	INFO	USER	User {subject.name} checked out secret {secret.name} via PSM-vault bridge.
FSW1250	WARNING	SYSTEM	Unable to parse password changer bind IP {}.
FSW1251	WARNING	SYSTEM	Recovery password change for secret {} while exclusively in use.
FSW1252	WARNING	SYSTEM	Unable to change password for secret {}, password policy not configured.
FSE1253	ERROR	SYSTEM	Failed to replicate password change for secret {}.
FSE1254	ERROR	SYSTEM	Failed to connect to database for secret password change.
FSE1255	ERROR	SYSTEM	Failed to initialize database listener for secret password change scheduling.
FSE1256	ERROR	SYSTEM	Failed to subscribe to secret password change notification channels.
FSE1257	ERROR	SYSTEM	Failed to receive secret password change notification.
FSE1258	ERROR	SYSTEM	Failed to fetch secrets pending password change.
FSE1259	ERROR	SYSTEM	Failed to read password changer node configuration.
FSE1260	ERROR	SYSTEM	Failed to detect local IP addresses for secret password change scheduling.
FSE1261	ERROR	SYSTEM	Failed to fetch bind IPs for pending secrets.
FSI1262	INFO	SYSTEM	for secret {} changed successfully.
FSW1263	WARNING	SYSTEM	Unable to verify password for secret {} after change.
FSW1264	WARNING	SYSTEM	Unable to change password for secret {} using changer {}.
FSW1265	WARNING	SYSTEM	Unable to change password for secret {}, no changer succeeded.
FSI1266	INFO	SYSTEM	Password for secret {} verified successfully.
FSW1267	WARNING	SYSTEM	Unable to verify password for secret {}.
FSW1268	WARNING	SYSTEM	Initiating recovery password change for secret {}.
FSE1269	ERROR	SYSTEM	Failed to change password for secret {}.
FSE1270	ERROR	SYSTEM	Password changer operation failed for secret {}.
FSE1271	ERROR	SYSTEM	Failed to schedule password change for secret {}.
FSE1272	ERROR	SYSTEM	Failed to clean up stale pending secret history entries.
FSE1273	ERROR	SYSTEM	Secret auto-checkin failed.
FSI1274	INFO	SYSTEM	Auto checked-in secret access {} to secret {} for user {}.

ciąg dalszy na następnej stronie

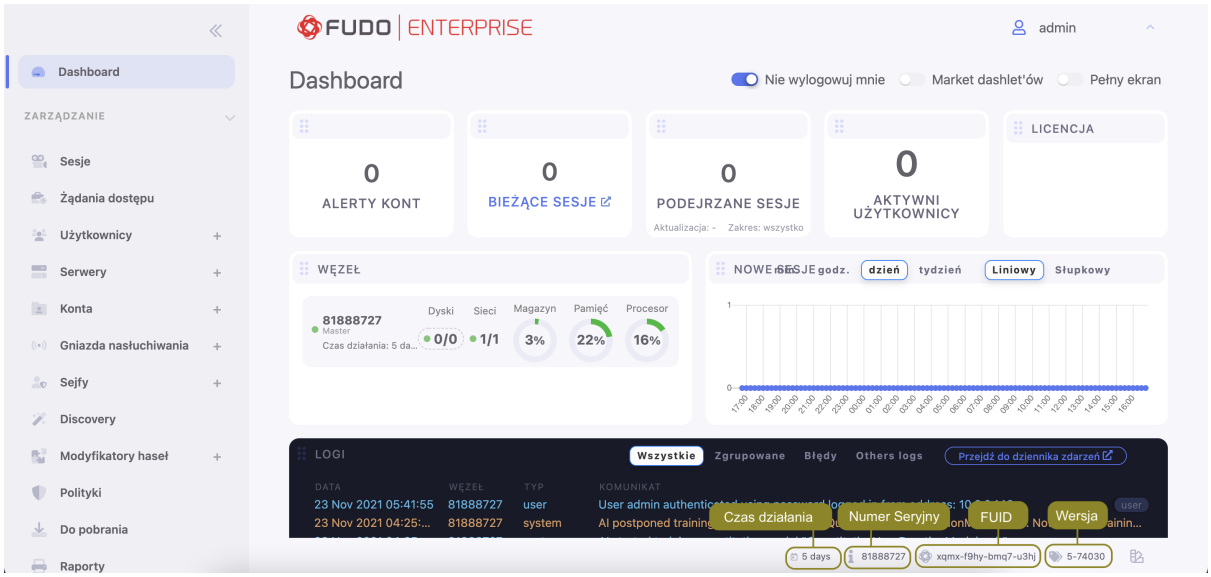
Tabela 1 – kontynuacja poprzedniej strony

Kod komunikatu	Typ	Komponent systemowy	Treść komunikatu
FAI1275	INFO	ADMIN	Administrator {subject.name} updated SMTP CA certificate.

15.3 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 16

Fudo Officer 2.3

Fudo Officer 2.3 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 2.3 lub z poziomu Panelu Administracyjnego, z zakładki *Zarządzanie* > *Żądania dostępu*.

Uwaga

Więcej na temat funkcji Just In Time oraz zarządzania żądaniami dostępu w Panelu Administracyjnym znajdziesz w rozdziale *Żądania dostępu*.

Fudo Officer 2.3 jest dostępny zarówno dla systemu Android, jak i iOS. Pobierz naszą aplikację mobilną ze sklepu odpowiedniego dla wybranego systemu.

Ostrzeżenie

Fudo Enterprise współpracuje wyłącznie z **najnowszą, aktualnie dostępną wersją** Fudo Officer 2.3. Starsze wersje aplikacji nie są wspierane i mogą nie zapewniać pełnej funkcjonalności lub kompatybilności z systemem. Zaleca się regularne aktualizowanie aplikacji mobilnej w celu zapewnienia bezpieczeństwa, zgodności z obowiązującymi mechanizmami uwierzytelniania oraz dostępu do najnowszych funkcji Fudo Enterprise.

16.1 Konfiguracja

Uwaga

- Aby powiązać urządzenie mobilne, funkcja *Callhome* 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 **Callhome**.

Aby skonfigurować Fudo Officer 2.3, 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 2.3 dostęp do kamery oraz zezwolić na wysyłanie powiadomień.

1. Skonfiguruj Fudo Enterprise:

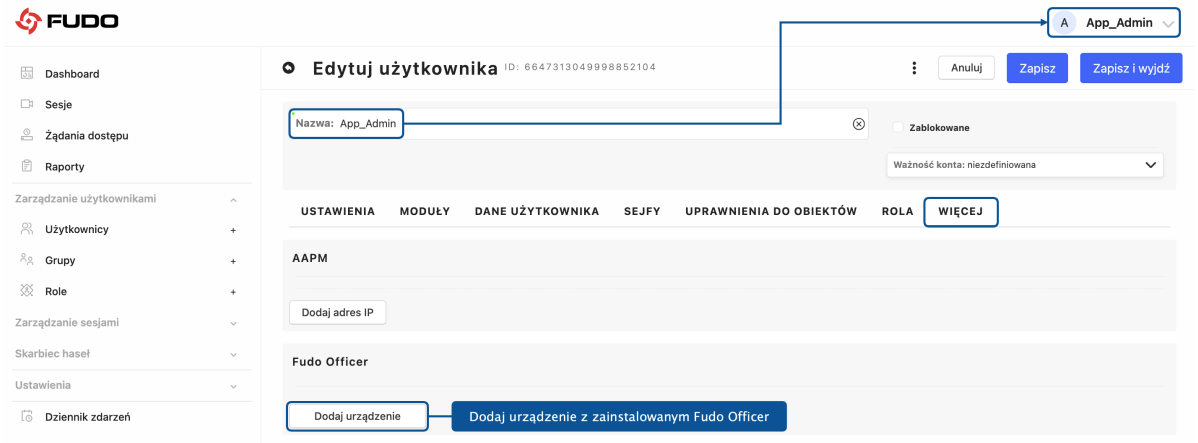
   1.1. Otwórz Panel Administracyjny Fudo Enterprise i przejdź do *Zarządzanie* > *Użytkownicy*.

   1.2 Znajdź i edytuj użytkownika, dla którego chcesz utworzyć profil w Fudo Officer 2.3.

   1.3. Przejdź do zakładki *WIĘCEJ* i kliknij przycisk *Dodaj urządzenie* w polu *Fudo Officer*, aby wygenerować kod QR.

Uwaga

- Powiązanie z Fudo Officer 2.3 można skonfigurować tylko dla użytkownika aktualnie zalogowanego do Panelu Administracyjnego.
- Tylko użytkownik z rolą *superadmin* lub *admin* może korzystać z aplikacji mobilnej Fudo Officer 2.3.



2. Otwórz aplikację Fudo Officer 2.3 na swoim urządzeniu mobilnym i wybierz *Rozpocznij*:

   2.1. Zezwól aplikacji Fudo Officer 2.3 na dostęp do kamery wymagany do skanowania kodów QR.

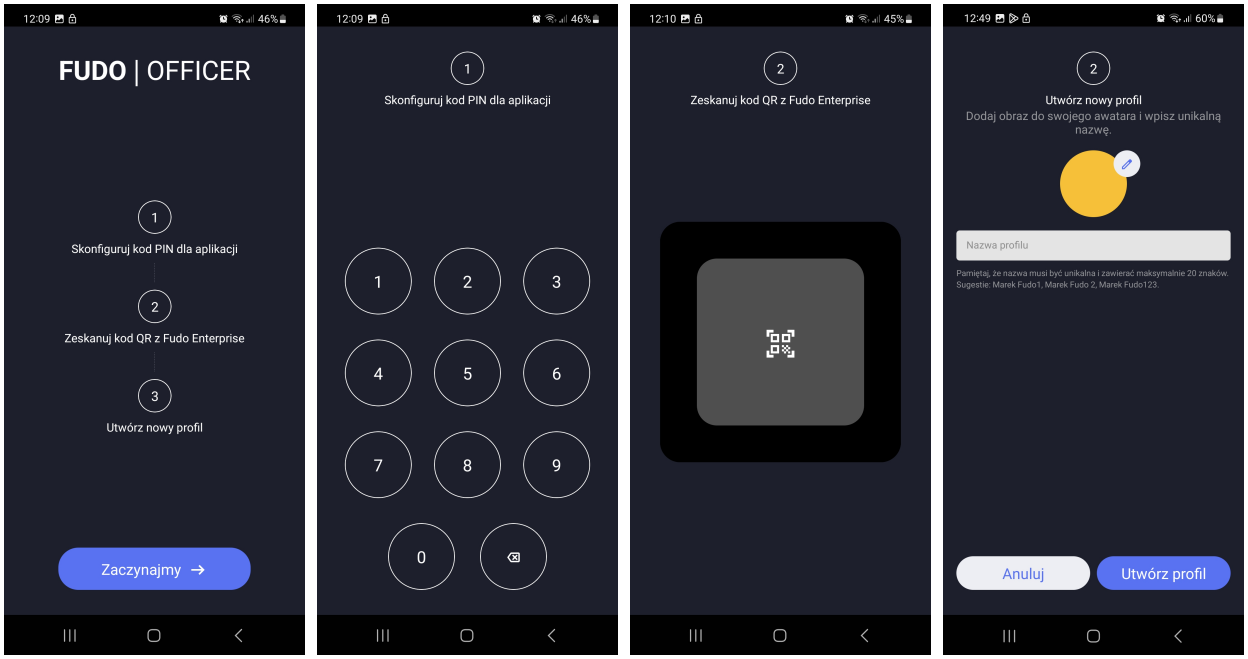
   2.2. Ustaw 6-cyfrowy kod PIN, który będzie używany do ochrony dostępu do aplikacji.

   2.2. Powtórz wprowadzony PIN, aby go potwierdzić.

2.3. Zezwól aplikacji Fudo Officer 2.3 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*.



Uwaga

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*

16.2 Zarządzanie Profilami

Profil w Fudo Officer 2.3 odpowiada obiektowi Użytkownik w Fudo Enterprise. Możesz zarządzać wieloma Profilami z poziomu jednej aplikacji Fudo Officer 2.3.

16.2.1 Dodawanie Profilów

Uwaga

Pierwszy Profil jest tworzony podczas *wstępnej konfiguracji aplikacji*.

Uwaga

- 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 2.3.

Aby dodać nowy profil, wykonaj poniższe kroki:

1. Skonfiguruj Fudo Enterprise:

   1.1. Otwórz Panel Administracyjny Fudo Enterprise i przejdź do *Zarządzanie* > *Użytkownicy*.

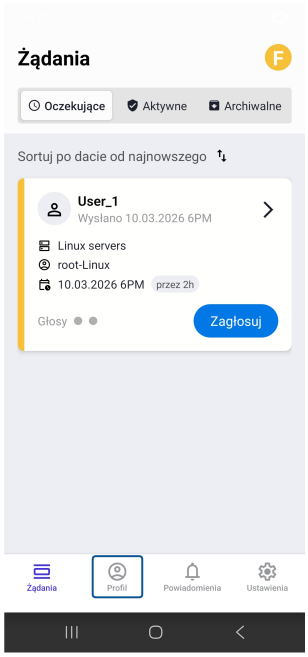
   1.2 Znajdź i edytuj użytkownika, dla którego chcesz utworzyć profil w Fudo Officer 2.3.

   1.3. Przejdź do zakładki *WIĘCEJ* i kliknij przycisk *Dodaj urządzenie* w polu *Fudo Officer*, aby wygenerować kod QR.

Uwaga

- Aby móc dodać urządzenie mobilne, funkcja *Callhome* 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 **Callhome**.

2. Otwórz aplikację Fudo Officer 2.3, 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*.

Uwaga

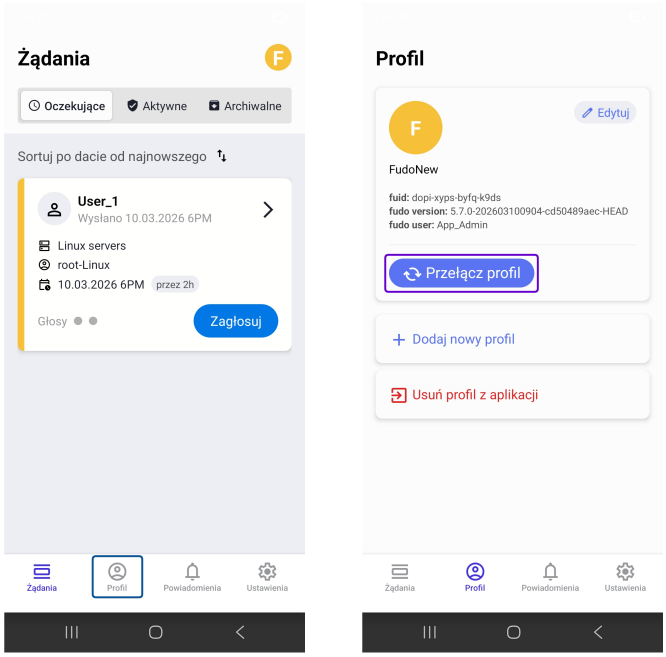
Nazwa profilu jest edytowalna.

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.

16.2.2 Przełączanie Profilów

Możesz łatwo przełączać profile, aby zarządzać żądaniami z różnych kont użytkowników. Aby przełączać się między dostępnymi profilami, wykonaj poniższe kroki:

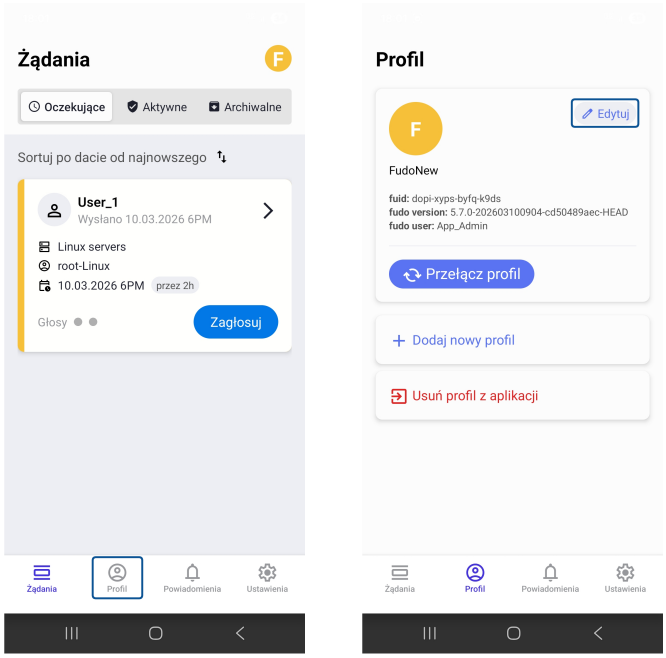
1. Wybierz ikonę *Profil* na dole ekranu.
2. Wybierz *Przełącz profil*, aby uzyskać dostęp do listy dostępnych profili.
3. Wybierz nazwę profilu z listy, aby go wybrać.
4. Zostaniesz automatycznie przekierowany do widoku *Żądania*, aby zarządzać żądaniami skierowanymi do tego profilu.



16.2.3 Edytowanie Profilu

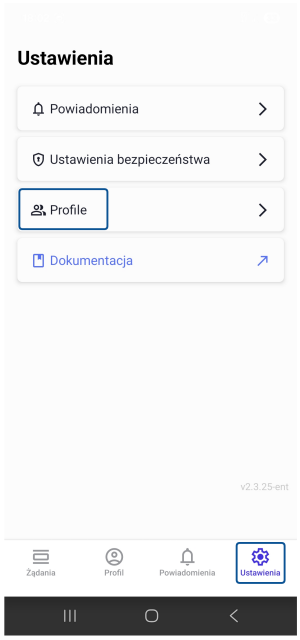
Możesz edytować nazwę i zdjęcie profilowe aktywnego profilu:

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.



Uwaga

Możesz również przełączać profile w ustawieniach aplikacji. Wystarczy wybrać ikonę koła zębatego w prawym dolnym rogu ekranu i wybrać *Profile*.



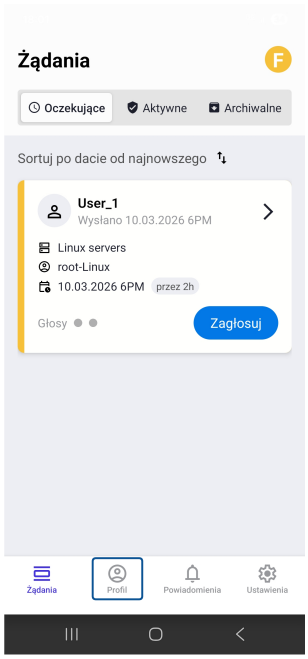
Uwaga

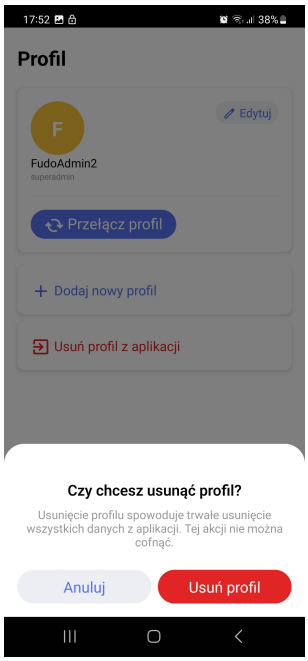
Aby zmienić PIN, przejdź do sekcji *Zmiana kodu PIN*.

16.2.4 Usuwanie Profilu

Aby usunąć profil z Fudo Officer 2.3, najpierw musisz przełączyć się na ten profil:

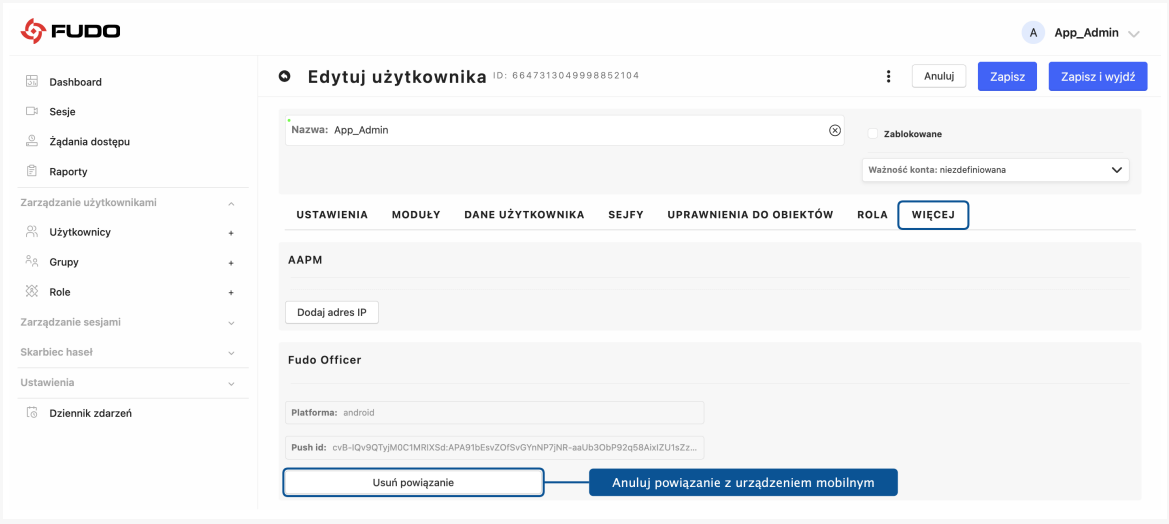
1. Wybierz ikonę *Profil* na dole ekranu.
2. Wybierz *Przełącz profil*, aby uzyskać dostęp do listy dostępnych profili.
3. Wybierz nazwę profilu z listy, aby go wybrać.
4. Ponownie wybierz ikonę *Profil* na dole ekranu.
5. Wybierz *Usuń profil z aplikacji*.
6. Wybierz *Usuń profil*, aby potwierdzić.





Uwaga

Upewnij się, że odłączyłeś również urządzenie w konfiguracji użytkownika w Panelu Administracyjnym Fudo Enterprise.



Powiązane tematy:

- *Zarządzanie Żądaniami Sesji*
- *Fudo Officer Settings*

16.3 Zarządzanie Żądaniami Sesji

Istnieją trzy rodzaje żądań: oczekujące, aktywne i archiwalne.

Uwaga

Żeby obsługiwać żądania dostępu, opcja *Just In Time*, oraz opcja *Sesja oczekująca na zatwierdzenie (push)* dla powiadomień push musi być włączona w danym sejfie.

16.3.1 Żądania Oczekujące

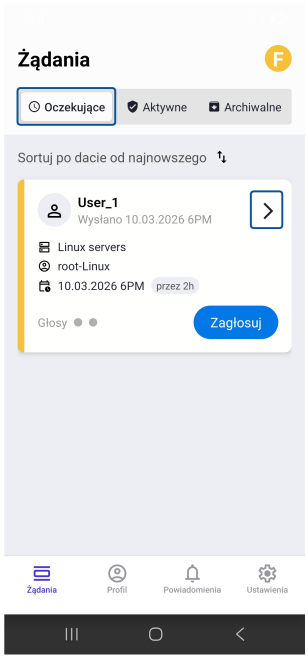
Zakładka **Oczekujące** pokazuje listę żądań oczekujących na decyzję od aktualnego profilu użytkownika.

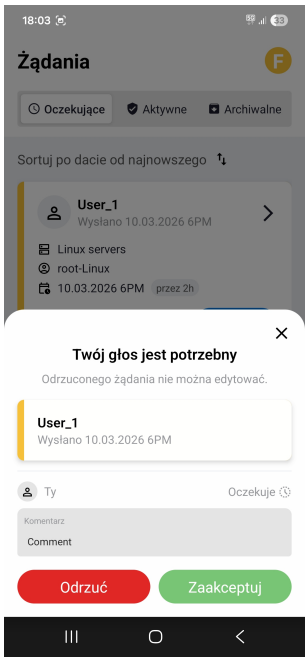
Uwaga

- 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 2.3 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 *Zaakceptuj* lub *Odrzuć*.





Uwaga

- Zatwierdzone żądania można znaleźć w zakładce **Aktywne**.
- Odrzucone żądania można znaleźć w zakładce **Archiwalne**.

Uwaga

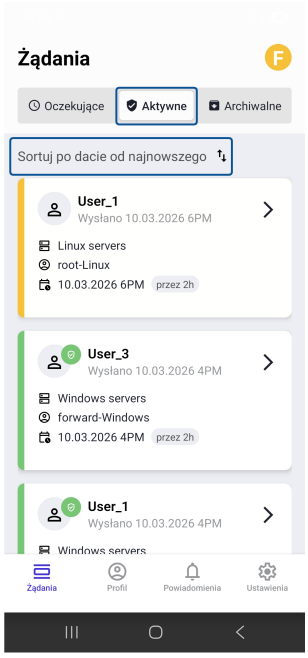
- Użytkownicy, którzy wysłali żądanie za pośrednictwem Portalu Użytkownika i mają skonfigurowany adres e-mail w Panelu Administracyjnym, otrzymają wiadomość, gdy ich żądanie zostanie zaakceptowane lub odrzucone.

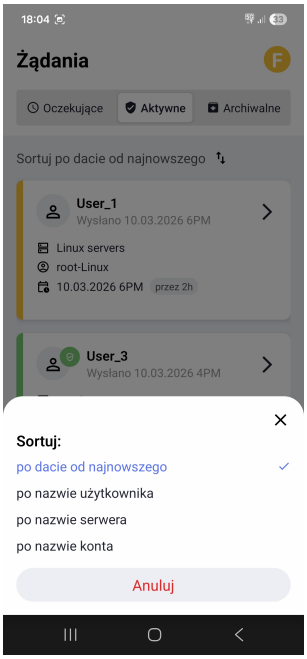
16.3.2 Żądania Aktywne

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.*



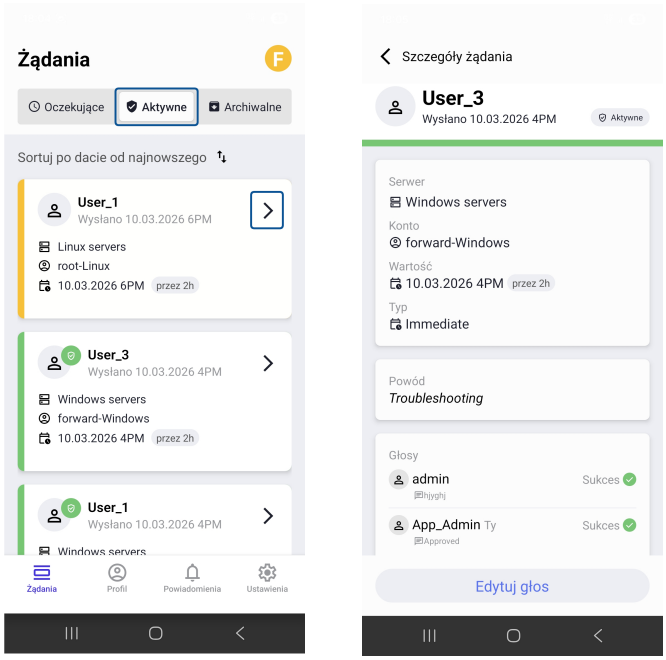


16.3.3 Cofnięcie Żądania

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 2.3 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.

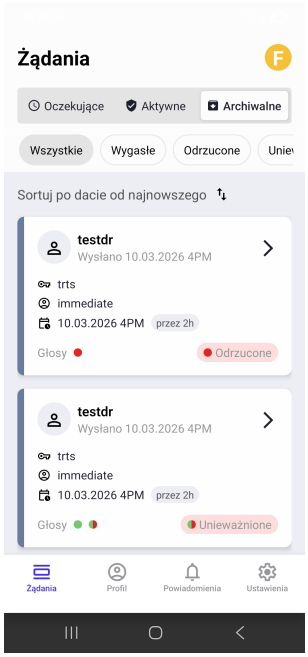


Uwaga

Jeśli zaakceptowałeś żądanie, które nadal oczekuje na głosy innych administratorów, przycisk *Odrzuć* będzie dostępny bezpośrednio na ekranie żądania.

16.3.4 Żądania Archiwalne

Historia przetworzonych żądań jest dostępna w zakładce **Archiwalne**. Żądania archiwalne można sortować według statusów *wygasłe, odrzucone, cofnięte* i *zatwierdzone*.



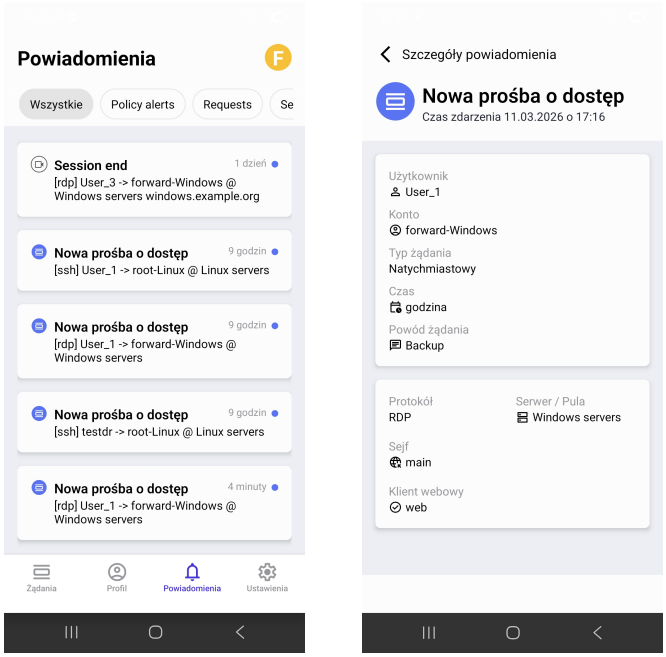
Powiązane tematy:

- *Fudo Officer Settings*

16.4 Powiadomienia

Zakładka **Powiadomienia** umożliwia przeglądanie historii powiadomień skonfigurowanych dla bieżącego profilu.

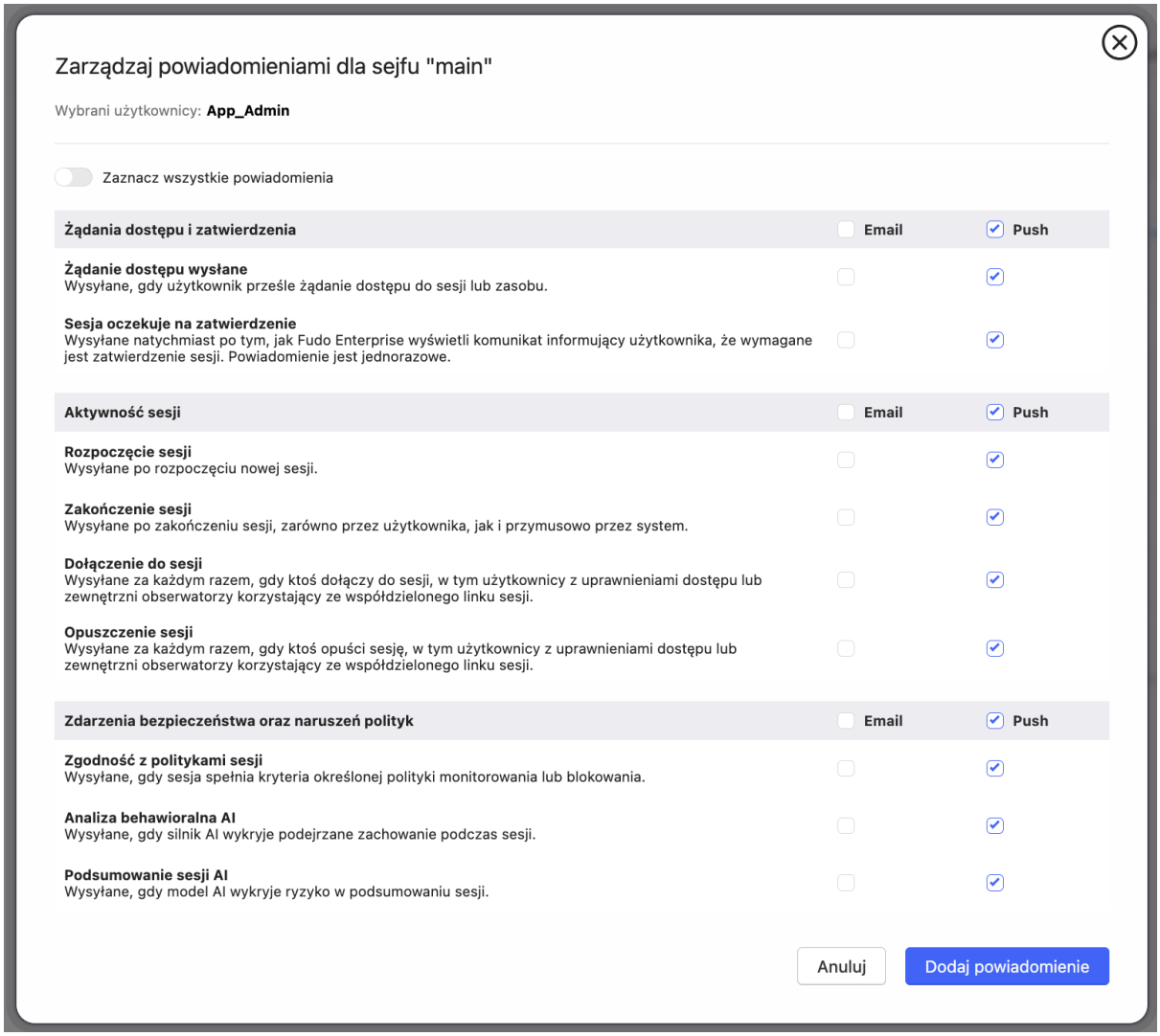
1. Na dole ekranu wybierz ikonę dzwonka oznaczoną jako *Powiadomienia*.
2. Przejrzyj historię powiadomień przypisanych do tego użytkownika.
3. Użyj dostępnych filtrów, aby zawęzić listę powiadomień według kategorii:
   - *Alerty polityk*
   - *Żądania*
   - *Sesje*
   - *Wydarzenia*
4. Kliknij wybrane powiadomienie, aby przejrzeć szczegóły.



16.4.1 Konfigurowanie powiadomień aplikacji

Powiadomienia aplikacji są konfigurowane w Fudo Enterprise, w ustawieniach sejfu, w zakładce *Powiadomienia*. Wybrane powiadomienia są następnie dostarczane do aplikacji dla użytkownika powiązanego z profilem.

1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise.
2. Wybierz *Zarządzanie sesją* > *Sejfy* i otwórz sejf, dla którego chcesz skonfigurować powiadomienia.
3. Przejdź do zakładki *POWIADOMIENIA*.
4. Aby zdefiniować typy powiadomień dla użytkownika, zaznacz pole wyboru przed nazwą żądanego użytkownika i kliknij *Zarządzaj powiadomieniami*.



5. Na liście typów powiadomień wybierz powiadomienia, które powinny być dostępne dla użytkownika w aplikacji.
6. Zaznacz odpowiednie pozycje w kolumnie *Push*.
7. Kliknij *Dodaj powiadomienie*, aby zapisać ustawienia i zamknąć okno modalne.
8. Kliknij *Zapisz* lub *Zapisz i zamknij*, aby zapisać konfigurację sejfu.

Powiązane tematy:

- *Zarządzanie Żądaniami Sesji*
- *Fudo Officer Settings*

16.5 Ustawienia

Aby uzyskać dostęp do ustawień aplikacji, wybierz ikonę koła zębatego w prawym dolnym rogu ekranu.

16.5.1 Uwierzytelnianie biometryczne

Aby włączyć opcję uwierzytelniania biometrycznego:

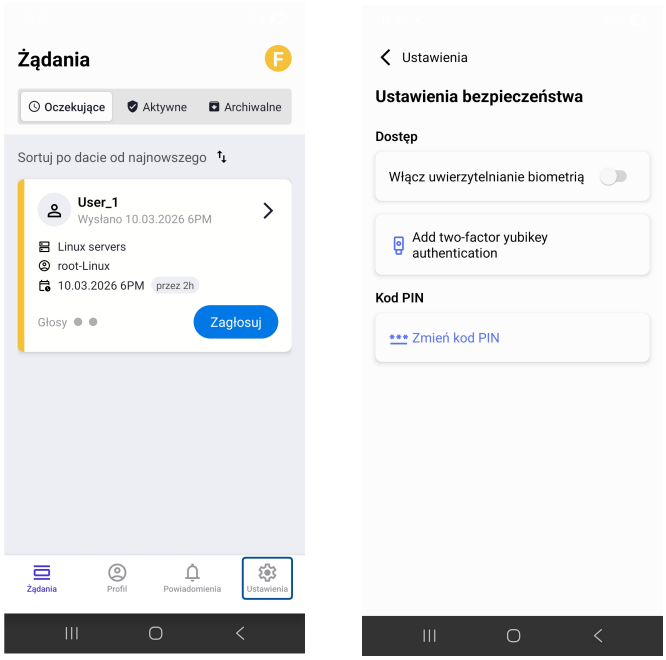
1. Wybierz ikonę koła zębatego w prawym dolnym rogu ekranu.
2. Wybierz *Ustawienia bezpieczeństwa*.
3. Wybierz opcję *Włącz uwierzytelnianie biometrią*.
4. Zeskanuj odcisk palca, aby zakończyć procedurę.

Uwaga

Po włączeniu opcji uwierzytelnianie biometryczne zostanie ustawione jako metoda domyślna podczas uruchamiania aplikacji.

16.5.2 Zmiana kodu PIN

1. Wybierz ikonę koła zębatego w prawym dolnym rogu ekranu.
2. Wybierz *Ustawienia bezpieczeństwa*.
3. Wybierz *Zmień kod PIN*.



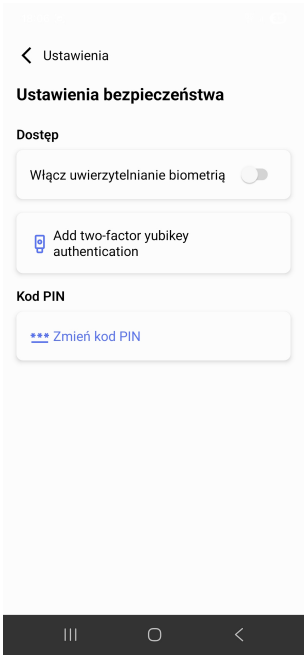
4. Podaj nowy 6-cyfrowy kod PIN.
5. Powtórz podany 6-cyfrowy kod PIN, aby potwierdzić zmianę.

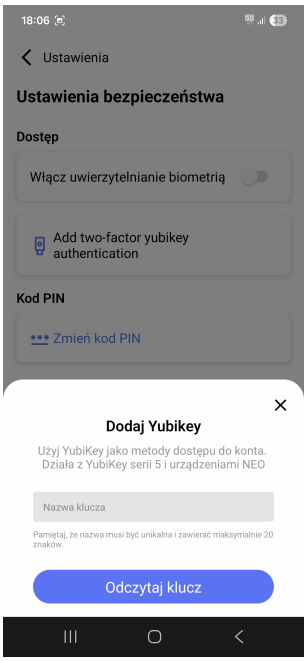
16.5.3 Dwuskładnikowe uwierzytelnianie przy użyciu YubiKey

Aby używać YubiKey jako metody uwierzytelniania dostępu do profilu:

1. Wybierz ikonę koła zębatego w prawym dolnym rogu ekranu.
2. Wybierz *Ustawienia bezpieczeństwa*.
3. Dotknij opcji *Dodaj dwuskładnikowe uwierzytelnianie YubiKey*.

4. Wprowadź nazwę klucza i dotknij przycisku *Odczytaj klucz*.
5. Dotknij YubiKey do twojego urządzenia mobilnego, aby zakończyć procedurę.





Uwaga

Fudo Officer 2.3 obsługuje połączenie NFC z urządzeniami *YubiKey 5 Series, YubiKey 5 FIPS Series i YubiKey NEO*.

16.5.4 Język

Język aplikacji jest ustawiany zgodnie z ustawieniami języka telefonu.

Powiązane tematy:

- *Zarządzanie Żądaniami Sesji*

ROZDZIAŁ 17

Fudo ShareAccess

Fudo ShareAccess to rewolucyjna platforma umożliwiająca natychmiastową współpracę między przedsiębiorstwami a podmiotami zewnętrznymi. Ułatwia szybki i bezpieczny dostęp dla dostawców usług, jednocześnie upraszczając procedurę udostępniania zasobów w zróżnicowanych środowiskach.

Fudo ShareAccess integruje zarządzanie uprzywilejowanym dostępem, usprawnia konfigurację połączeń i danych uwierzytelniających oraz zapewnia podmiotom zewnętrznym natychmiastowy i bezproblemowy dostęp do zasobów bezpośrednio przez przeglądarkę internetową, gwarantując bezpieczeństwo i prostotę.

Fudo Enterprise pełni rolę bramy dla Fudo ShareAccess, służąc zarówno jako punkt dostępu do zasobów, jak i platforma do konfigurowania tego dostępu.

Uwaga

Rozdział ten zawiera opis konfiguracji z poziomu Fudo Enterprise. Aby uzyskać więcej informacji, zapoznaj się z dedykowaną dokumentacją ShareAccess.

17.1 Model danych

Fudo ShareAccess definiuje następujące typy obiektów:

Organizacja - Obiekt reprezentujący firmę korzystającą z Fudo ShareAccess. Każdy użytkownik sieci Fudo ShareAccess musi być przypisany do organizacji jako jej członek.

Użytkownik - Obiekt reprezentujący konto indywidualnego użytkownika korzystającego z Fudo ShareAccess. Tworzony jest podczas procesu rejestracji i wykorzystywany do uwierzytelniania oraz autoryzacji dostępu do współdzielonych danych.

Brama - Obiekt reprezentujący Fudo Enterprise w Fudo ShareAccess, przypisany do Organizacji. Brama pełni rolę punktu dostępu do zasobów oraz centralnego węzła konfiguracji zarządzania dostępem do tych zasobów.

Zasób - Reprezentacja zasobu, do którego można się podłączyć lub uzyskać go za pośrednictwem Fudo Enterprise. Zasób może być udostępniony użytkownikowi przez Fudo ShareAccess poprzez odpowiednią konfigurację w Panelu Administracyjnym Fudo Enterprise. Fudo ShareAccess nie przechowuje informacji o zasobach; przedstawia konfigurację pobraną z Panelu Administracyjnego Fudo Enterprise.

Tematy pokrewne:

- *Parowanie Fudo Enterprise i Fudo ShareAccess*
- *Zarządzanie użytkownikami Fudo ShareAccess*
- *Zarządzanie dostępem do zasobów*

17.2 Parowanie Fudo Enterprise i Fudo ShareAccess

Uwaga

Przed rozpoczęciem parowania Fudo Enterprise z Fudo ShareAccess należy spełnić poniższe wymagania:

- Musi istnieć użytkownik z rolą posiadającą uprawnienia do zarządzania Fudo ShareAccess oraz e-mailem ustalonym dla właściciela Organizacji.
- Konfiguracja NTP jest wymagana. Przejdź do *Ustawienia* > *System* i skonfiguruj serwer NTP (szczegóły w sekcji *Data i czas*).
- Konfiguracja DNS jest wymagana. Przejdź do *Ustawienia* > *Konfiguracja sieci* i skonfiguruj serwer DNS (szczegóły w sekcji *Konfiguracja DNS*).
- Aby umożliwić zestawienie tunelu między Fudo ShareAccess a Fudo Enterprise, wymagane jest zezwolenie na ruch wychodzący na porcie 65522 do dowolnej destynacji.

Uwaga

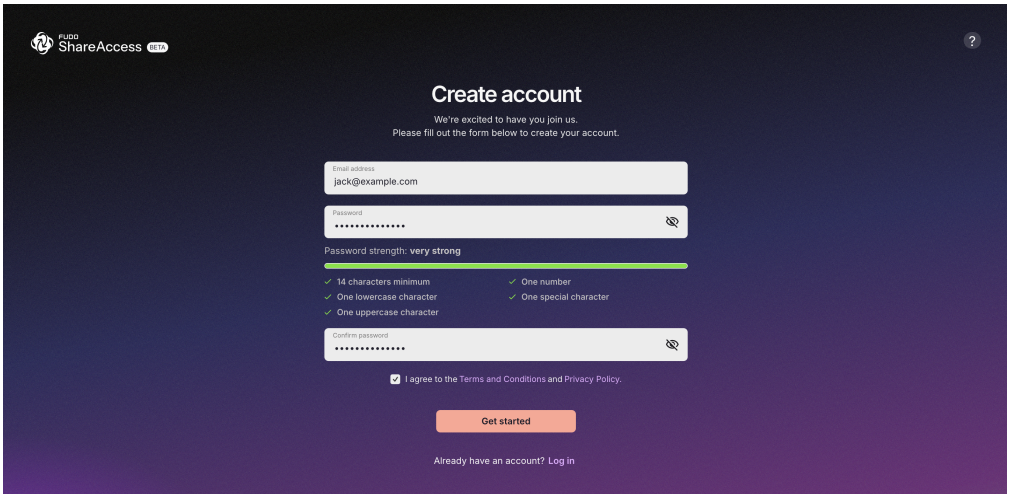
Aby umożliwić komunikację Fudo Enterprise z platformą Fudo ShareAccess, upewnij się, że następujące połączenia wychodzące są dozwolone:

- `api.shareaccess.com` na porcie `443` – wymagane do komunikacji API przez HTTPS.
- `connect.shareaccess.com` na porcie `65522` – wymagane do ustanowienia tunelu między Fudo ShareAccess a Fudo Enterprise.
- `acme-v02.api.letsencrypt.org` na porcie `443` – wymagane do uzyskiwania i odnawiania certyfikatów.

1. Zaloguj się do Panelu Administracyjnego instancji Fudo Enterprise.
2. Utwórz użytkownika, który będzie administratorem Fudo ShareAccess:
    - Wybierz *Zarządzanie* > *Użytkownicy*, a następnie kliknij *+ Dodaj użytkownika*.

- Wprowadź nazwę użytkownika.
- Z rozwijanej listy *Rola* wybierz rolę, która posiada uprawnienia do zarządzania Fudo ShareAccess.
- W zakładce *Dane użytkownika* w polu *Informacje o użytkowniku* wprowadź:
  - pełne imię i nazwisko użytkownika,
  - adres e-mail użytkownika,
  - jednostkę organizacyjną użytkownika,
  - numer telefonu użytkownika.
- Kliknij *Zapisz*.
- Wróć do zakładki *Ustawienia* i w sekcji *Uwierzytelnianie* wybierz preferowaną metodę uwierzytelniania z rozwijanej listy *Dodaj metodę uwierzytelniania*. Będzie ona używana do uwierzytelniania użytkownika w Portalu Użytkownika Fudo Enterprise.
- Kliknij *Zapisz i zamknij*.

3. Utwórz konto w Fudo ShareAccess:
   - Przejdź na stronę stronę Fudo ShareAccess.
   - Kliknij *Sign In*.
   - Podaj ten sam adres e-mail, który wykorzystano w kroku nr 2, przy tworzeniu konta administratora w Fudo Enterprise.
   - Ustaw hasło dla nowego konta.

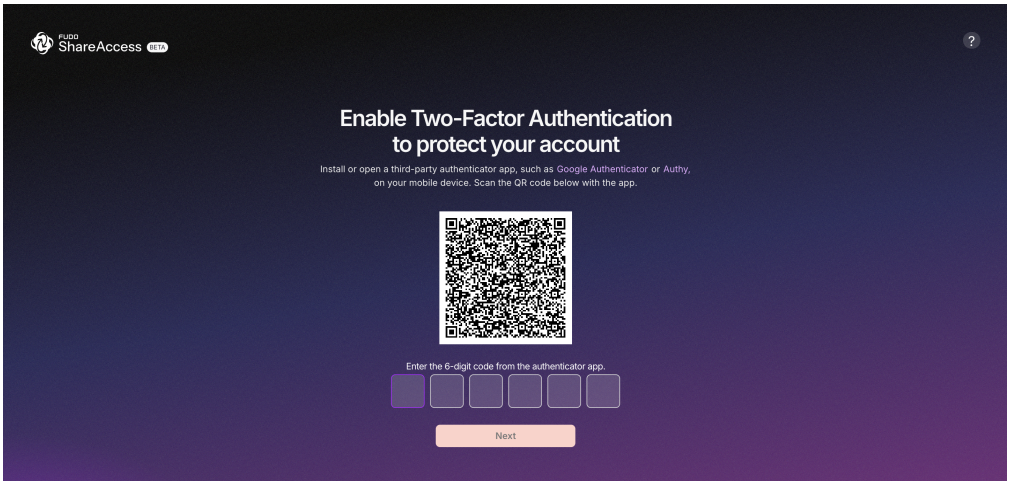


Uwaga

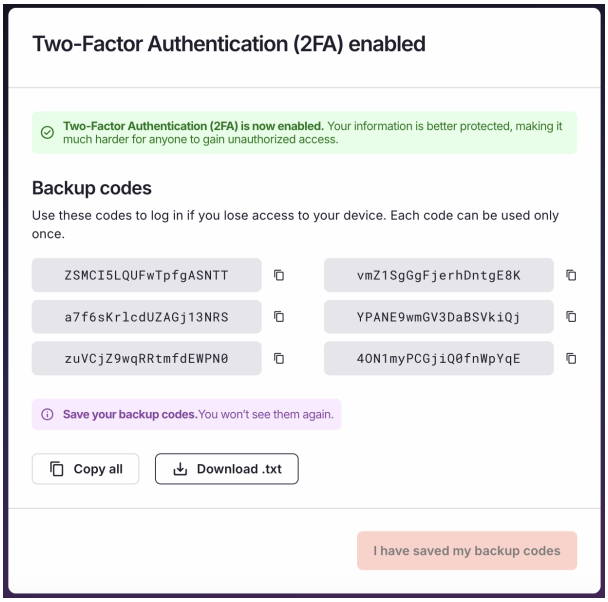
Zakładając konto i podając swój adres e-mail, akceptujesz nasze Warunki korzystania i Politykę prywatności.

- Kliknij Rozpocznij.
- Sprawdź swoją skrzynkę odbiorczą, aby znaleźć wiadomość z potwierdzeniem i postępuj zgodnie z podanym linkiem, aby zweryfikować swoje konto.

- Po zweryfikowaniu adresu e-mail zaloguj się na stronie Fudo ShareAccess używając adresu e-mail i hasła podanych podczas rejestracji, aby kontynuować konfigurację konta.
- Otwórz aplikację uwierzytelniającą, taką jak *Google Authenticator* lub *Authy*, na swoim urządzeniu mobilnym i zeskanuj kod QR wyświetlony na ekranie.
- Wprowadź 6-cyfrowy kod z aplikacji uwierzytelniającej.



- Kliknij Dalej.
- Zabezpiecz swoje kody zapasowe wyświetlone w oknie modalnym. Kliknij Kopiuj wszystkie, aby skopiować kody i zapisać je w bezpiecznym miejscu, lub Pobierz, aby pobrać je jako plik `.txt`. Zwróć uwagę, że kody nie będą ponownie wyświetlone.

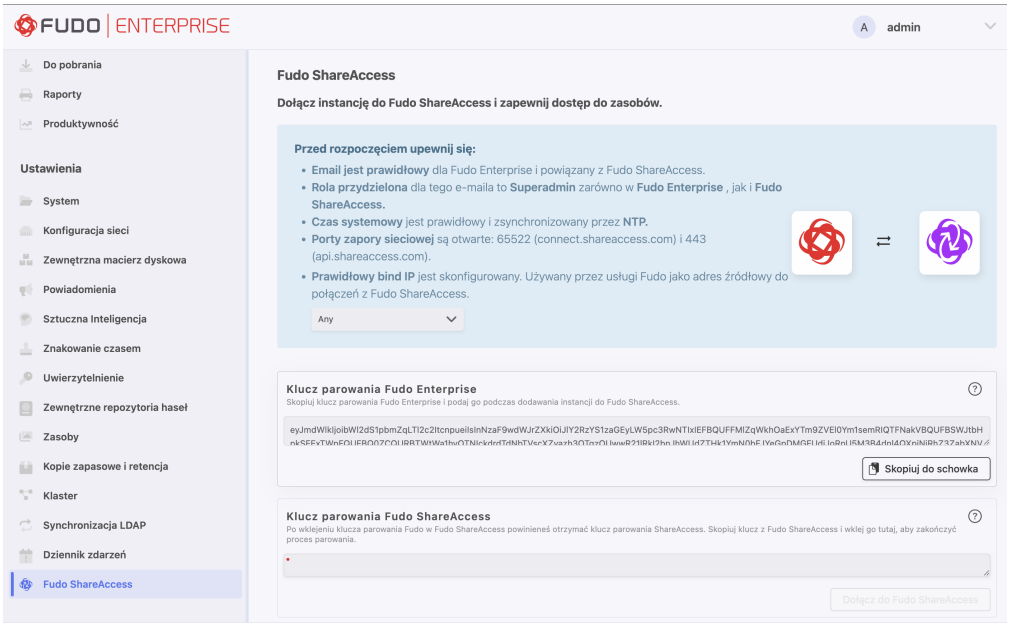


Ostrzeżenie

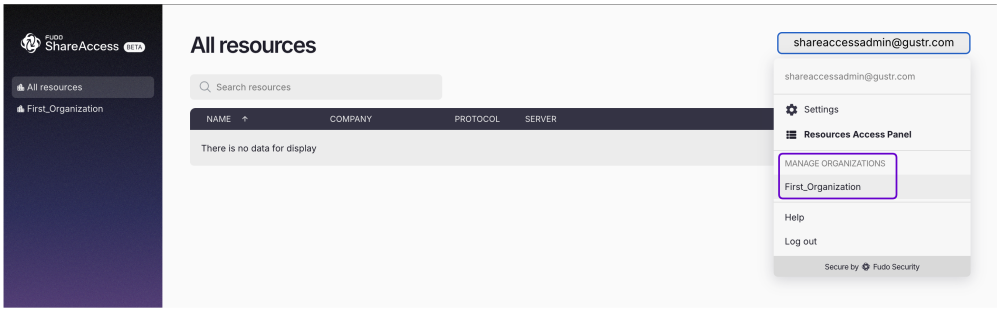
- Jeśli utracisz swoje kody zapasowe, stracisz dostęp do konta. W takim przypadku skontaktuj się z pomocą techniczną Fudo Security.

- Kliknij Zapisałem kody zapasowe, aby potwierdzić ich zapisanie i zakończyć proces konfiguracji.

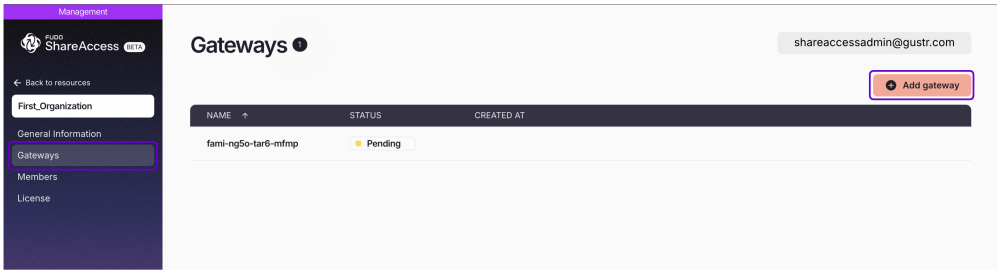
4. Skopiuj *Klucz parowania* z Fudo Enterprise:
   - Wybierz *Ustawienia* > *Fudo ShareAccess*.
   - Kliknij *Skopiuj do schowka*, aby skopiować *Klucz parowania Fudo Enterprise*.



5. Dodaj **Bramę** w Fudo ShareAccess:
   - Rozwiń menu w prawym górnym rogu i wybierz *Zarządzaj organizacjami* > *Nazwa Twojej Organizacji*, aby uzyskać dostęp do ustawień organizacji.

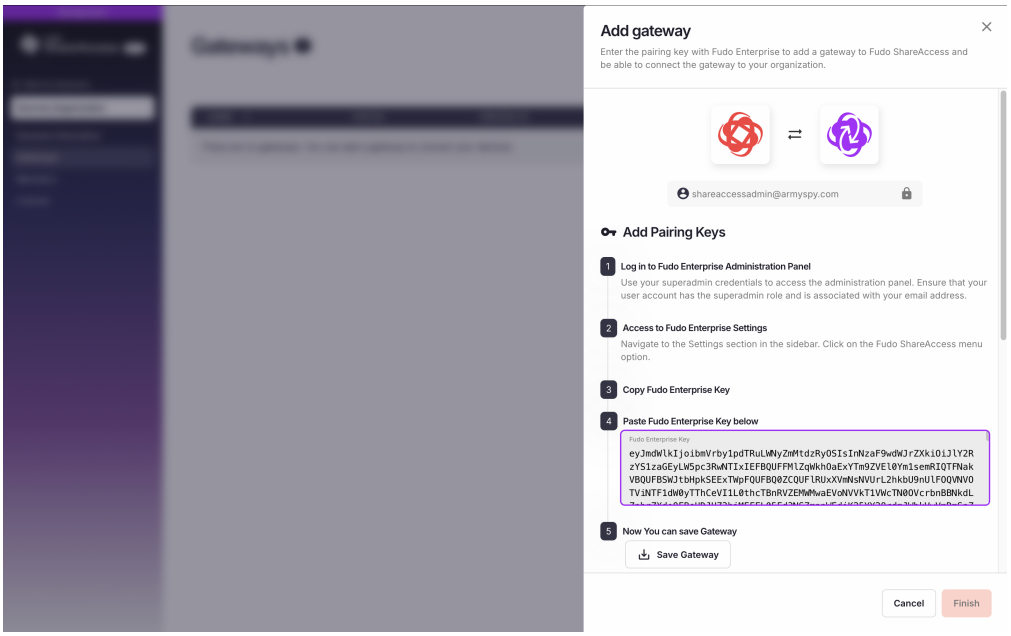


   - W menu po lewej stronie wybierz *Bramy*.
   - Kliknij + *Dodaj Bramę*.

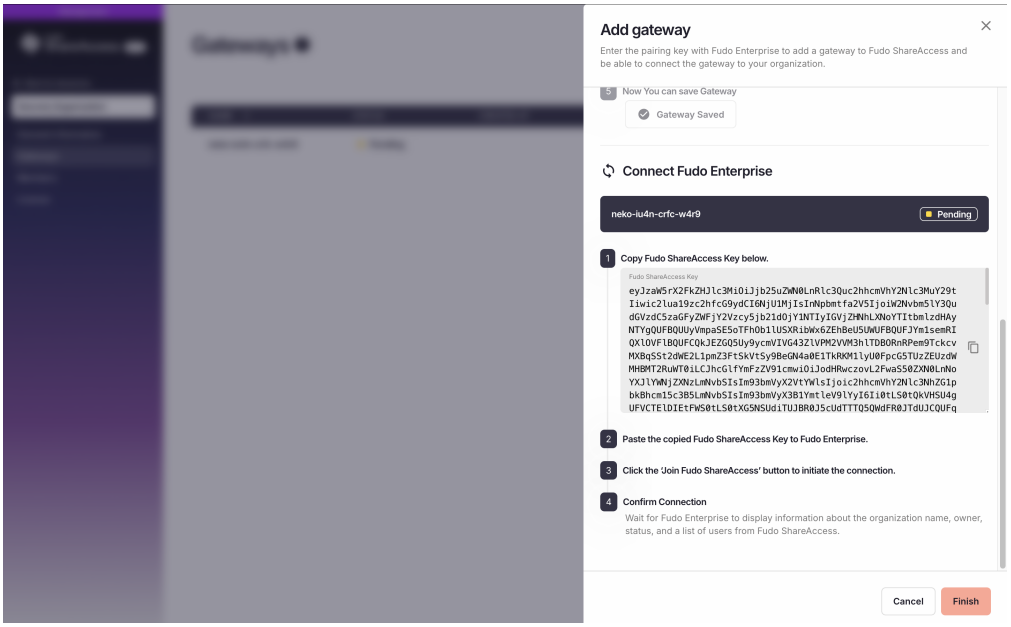


   - Wklej wcześniej skopiowany *Klucz parowania Fudo Enterprise*.

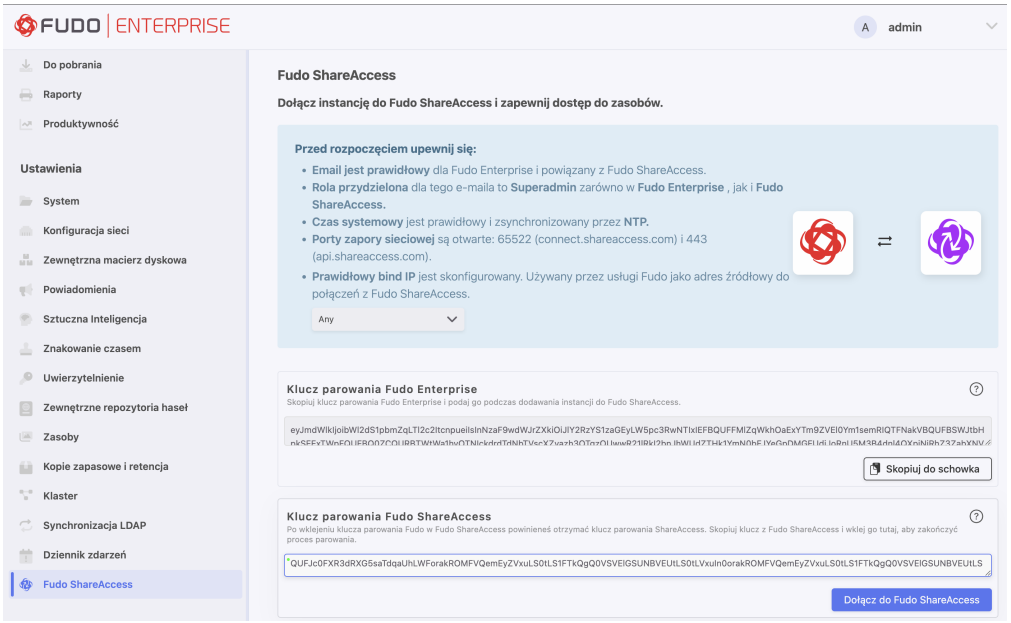
- Kliknij *Zapisz Bramę*.



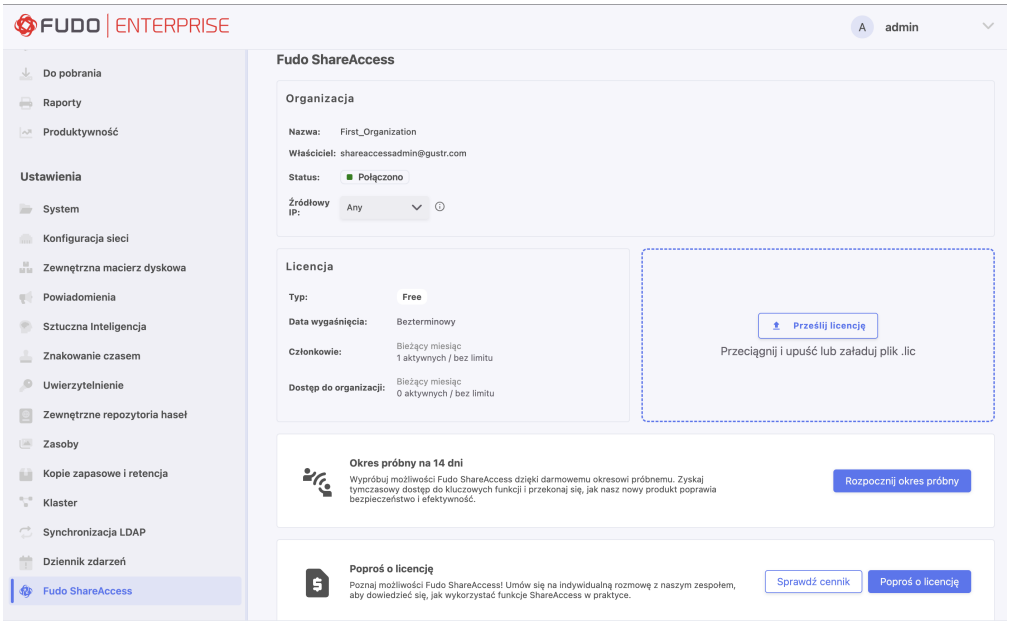
- Następnie skopiuj *Klucz parowania Fudo*, który pojawi się w oknie poniżej.



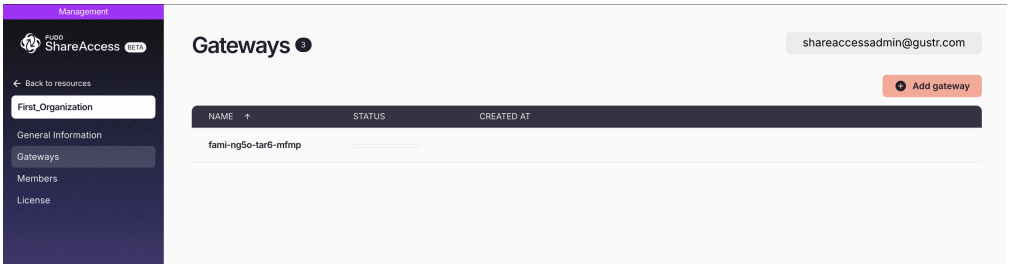
6. Wróć do Panelu Administracyjnego Fudo Enterprise i wklej *Klucz parowania Fudo* w polu *Klucz parowania Fudo ShareAccess*.
7. Kliknij *Dołącz do Fudo ShareAccess*.



8. Poczekaj, aż instancja Fudo Enterprise wyświetli informacje o nazwie organizacji, właścicielu, statusie i liście użytkowników z Fudo ShareAccess.



9. Po pomyślnym sparowaniu identyfikator *Fudo Unique Identifier* zostanie wyświetlony na liście Bram.



Tematy pokrewne:

- *Zarządzanie użytkownikami Fudo ShareAccess*

- *Zarządzanie dostępem do zasobów*

17.3 Licencja

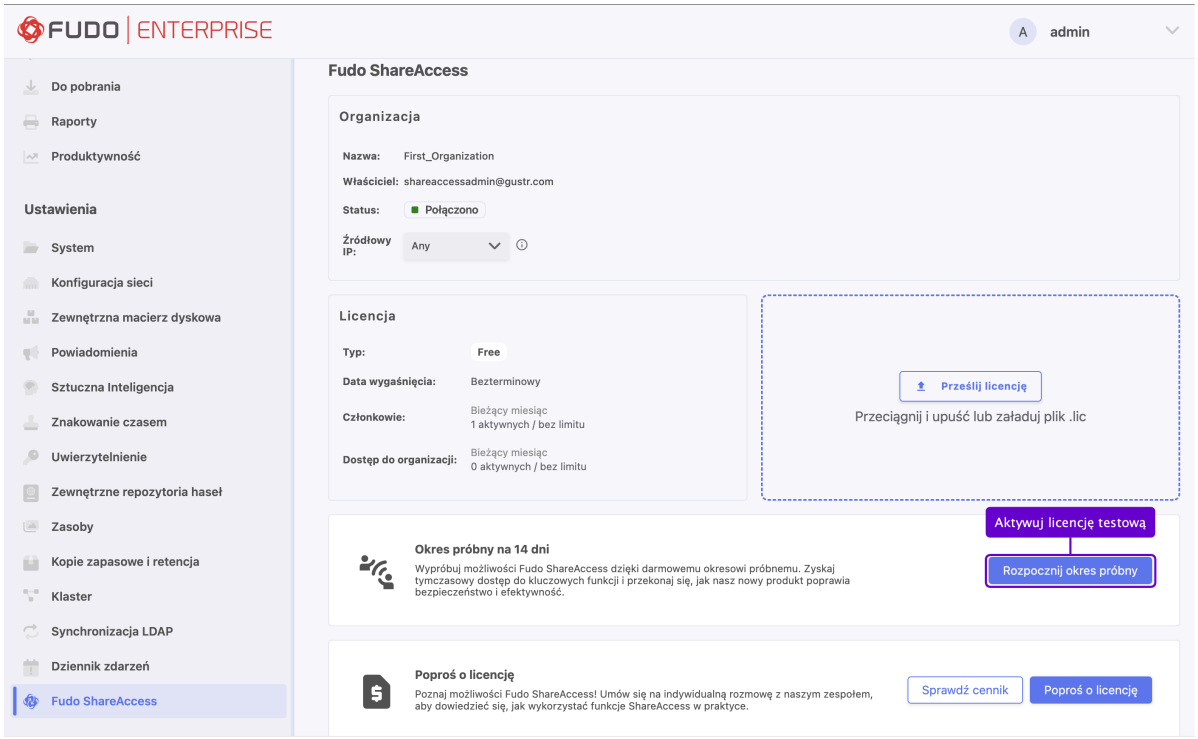
Zarządzanie licencją dla Fudo ShareAccess jest dostępne wyłącznie z poziomu Panelu Administratora Fudo Enterprise dla użytkowników z rolą posiadającą uprawnienia do zarządzania Fudo ShareAccess.

17.3.1 Licencja próbna (trial)

Licencja próbna jest dostępna tylko raz dla jednej organizacji. Ten typ licencji działa na tych samych zasadach co standardowa licencja, oferując pełną funkcjonalność i umożliwiając realistyczne poznanie możliwości systemu.

Aby włączyć wersję próbną Fudo ShareAccess:

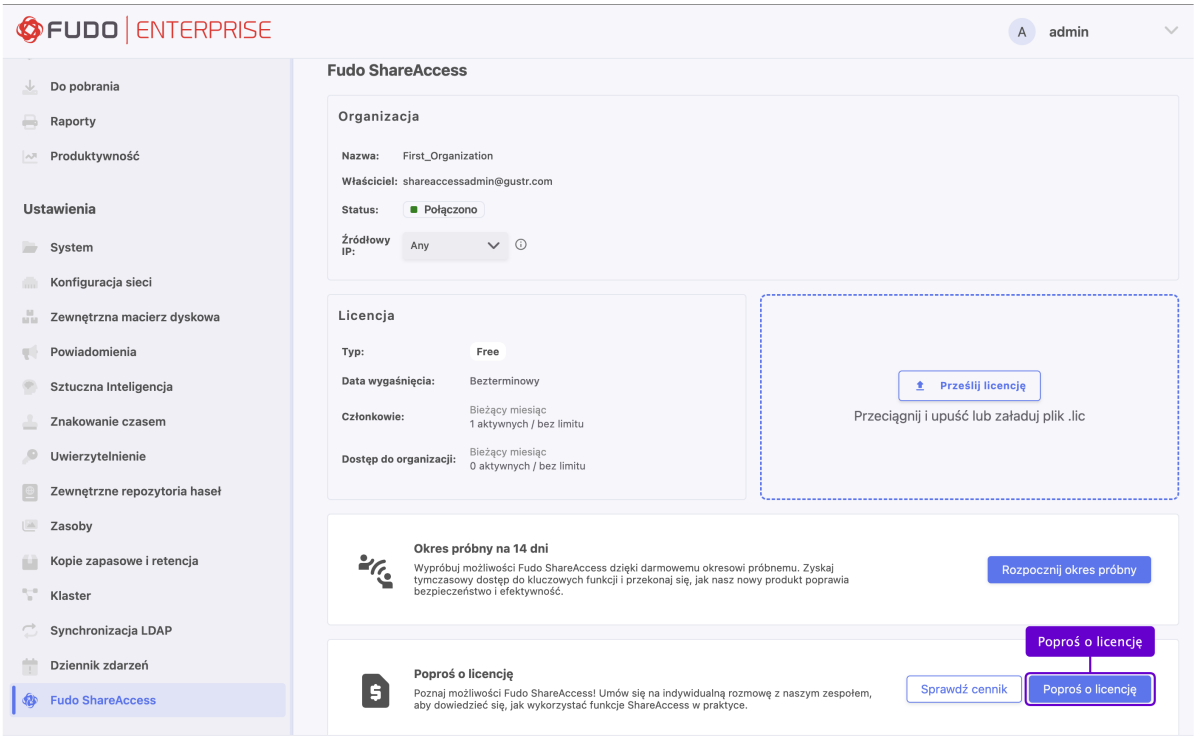
1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise.
2. Wybierz Ustawienia > Fudo ShareAccess.
3. W sekcji *Licencja* kliknij przycisk Uruchom wersję próbną.



17.3.2 Zamawianie licencji

Aby zamówić licencję dla Fudo ShareAccess:

1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise.
2. Wybierz Ustawienia > Fudo ShareAccess.
3. W sekcji *Licencja* kliknij przycisk Poproś o licencję.
4. Wypełnij formularz wyceny, aby skontaktować się z Fudo Security.



17.3.3 Wgrywanie pliku licencji

Po otrzymaniu pliku licencyjnego należy go wgrać do instancji Fudo Enterprise:

1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise.
2. Wybierz Ustawienia > Fudo ShareAccess.
3. W sekcji *Licencja* kliknij przycisk Wgraj licencję lub przeciągnij plik licencji bezpośrednio do pola *Przeciągnij i upuść*.
4. Plik licencji zostanie automatycznie przetworzony, a licencja odpowiednio załadowana.

Powiązane tematy:

- *Parowanie Fudo Enterprise i Fudo ShareAccess*
- *Zarządzanie użytkownikami Fudo ShareAccess*
- *Zarządzanie dostępem do zasobów*

17.4 Zarządzanie użytkownikami Fudo ShareAccess

17.4.1 Zapraszanie członków

Fudo Enterprise wspiera zarządzanie użytkownikami i ich dostępem do zasobów organizacji poprzez integrację z Fudo ShareAccess. Użytkownicy mogą być zapraszani zarówno do członkostwa w organizacji, jak i do korzystania z zasobów w Fudo ShareAccess.

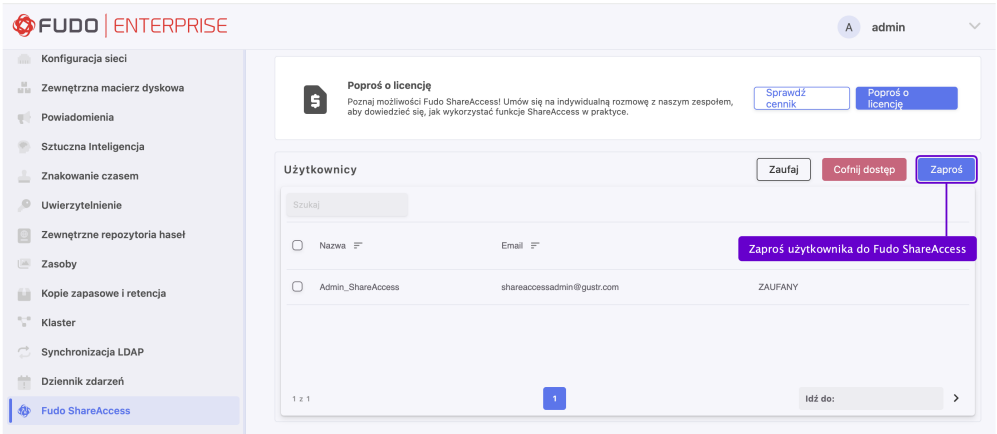
Efektem procesu zaproszenia jest połączenie utworzone pomiędzy użytkownikiem Fudo Enterprise a użytkownikiem Fudo ShareAccess, co jest niezbędne do uzyskania dostępu do zasobów.

Uwaga

Zalecane jest zarządzanie użytkownikami wyłącznie w Fudo Enterprise. Zapraszanie użytkowników bezpośrednio do organizacji z poziomu Fudo ShareAccess 1.0 nie utworzy konta użytkownika w Fudo Enterprise.

Aby dodać użytkowników w Fudo Enterprise i połączyć ich z Fudo ShareAccess, wykonaj następujące kroki:

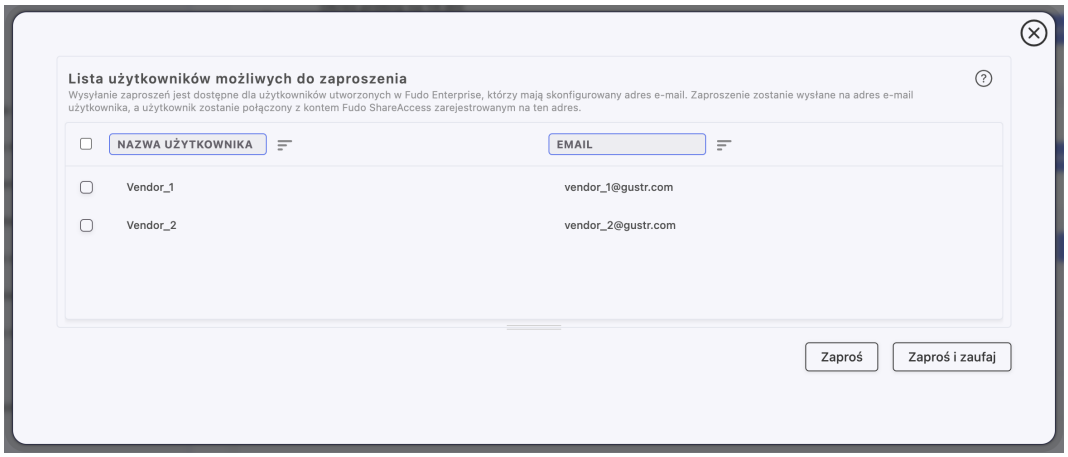
1. Utwórz użytkownika z adresem e-mail, który będzie używany do dostępu do Fudo ShareAccess:
    - Wybierz *Zarządzanie* > *Użytkownicy*, a następnie kliknij + *Dodaj użytkownika*.
    - Wprowadź nazwę użytkownika.
    - Z rozwijanej listy *Rola* wybierz odpowiednią dla tworzonego użytkownika rolę.
    - W zakładce *Dane użytkownika*, w polu *Informacje o użytkowniku* wprowadź:
        - pełne imię i nazwisko użytkownika (wymagane),
        - adres e-mail użytkownika, który będzie używany do dostępu do Fudo ShareAccess (wymagane),
        - jednostkę organizacyjną użytkownika,
        - numer telefonu użytkownika.
    - Kliknij *Zapisz*.
    - Wróć do zakładki *Ustawienia* i w sekcji *Uwierzytelnianie* wybierz preferowany typ uwierzytelniania z rozwijanej listy *Dodaj metodę uwierzytelniania*. Będzie on używany do uwierzytelniania użytkownika w Portalu Użytkownika Fudo Enterprise.
    - Kliknij *Zapisz i zamknij*.
1. Wybierz *Ustawienia* > *Fudo ShareAccess*, a następnie kliknij przycisk *Zaproś*.



3. W oknie dialogowym, z listy dostępnych użytkowników wybierz użytkowników, których chcesz zaprosić.

Uwaga

Zapraszać można wyłącznie użytkowników, którzy mają uzupełniony adres e-mail.



4. Aby uzyskać dostęp do przypisanych zasobów, użytkownik musi mieć status *Zaufany*:
   - Kliknij przycisk *Zaproś i Zaufaj*, aby natychmiast zaufać użytkownikowi bez weryfikacji, lub
   - Kliknij przycisk *Zaufaj*, aby zweryfikować użytkownika po zaakceptowaniu zaproszenia.

Uwaga

Zapraszanie użytkowników z opcją *Zaufaj* spowoduje natychmiastowe, nieweryfikowane udostępnienie zasobów.

5. Wysłanie zaproszenia doda wpisy na liście użytkowników ze statusem *Oczekujące*, dopóki użytkownik nie kliknie linku w e-mailu, aby dołączyć do organizacji.

Uwaga

Wysłanie zaproszenia oznacza, że użytkownik otrzyma e-mail zawierający link, który pozwala na utworzenie konta i akceptację zaproszenia lub jedynie akceptację zaproszenia, jeśli już posiada konto w Fudo ShareAccess.

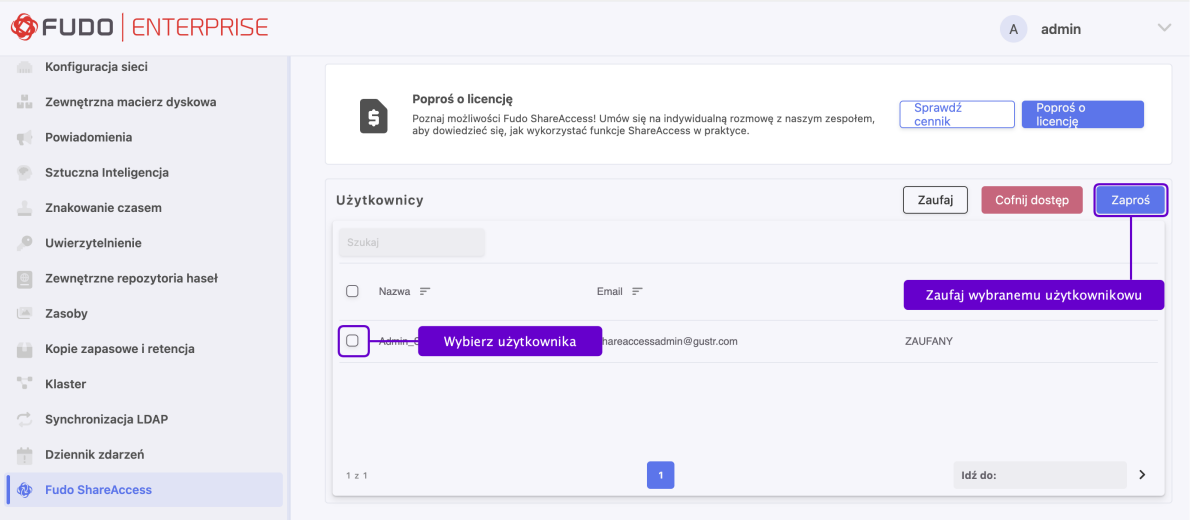
17.4.2 Weryfikacja statusu członków

Użytkownik powiązany z Fudo ShareAccess może mieć status *Zaufany* lub *Niezaufany*. Status ten określa, czy użytkownik może widzieć zasoby w Fudo ShareAccess.

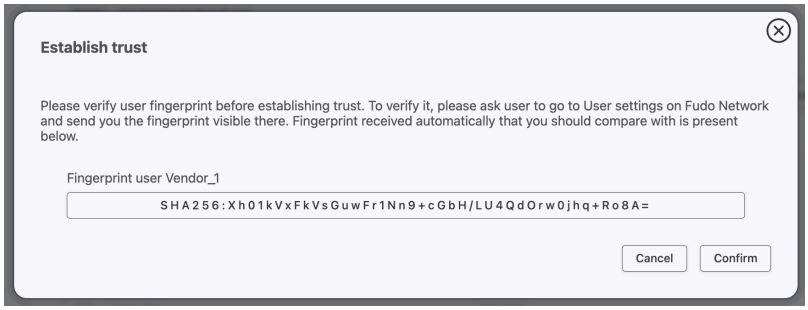
Uwaga

Użytkownik z rolą posiadającą uprawnienia do zarządzania Fudo ShareAccess może przeprowadzić weryfikację w Fudo Enterprise (zmiana statusu *Niezaufany*) tylko po utworzeniu konta w Fudo ShareAccess przez użytkownika i zaakceptowaniu przez niego zaproszenia do organizacji.

1. Wybierz *Ustawienia* > *Fudo ShareAccess*.
2. Wybierz użytkowników z listy i kliknij przycisk *Zaufaj*.

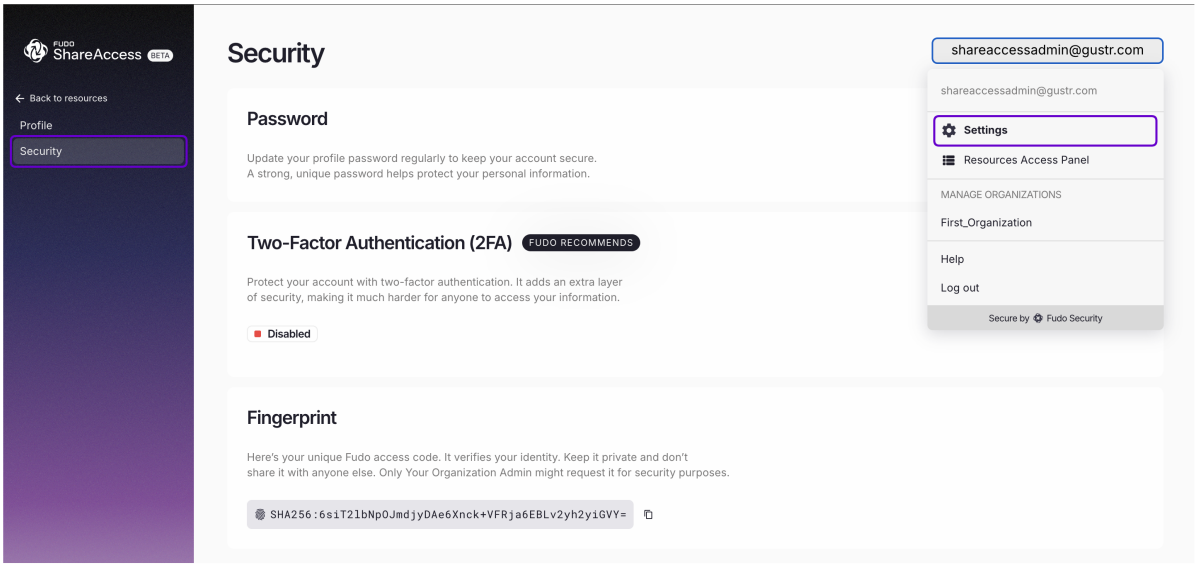


3. Poproś użytkownika o podanie *Klucza Odcisku Palca* z jego konta w Fudo ShareAccess i porównaj go z odciskiem palca wyświetlanym w oknie dialogowym.



Uwaga

Klucz Odcisku Palca można zobaczyć po zalogowaniu się na konto użytkownika w Fudo ShareAccess, wybraniu opcji *Ustawienia* z menu rozwijanego w prawym górnym rogu, a następnie *Bezpieczeństwo* z menu po lewej stronie ekranu.



4. Kliknij *Potwierdź*. Po potwierdzeniu użytkownik zostaje uznany za zaufanego.

Uwaga

- Proces ten nie jest wymagany. Administrator decyduje, czy zaufać użytkownikom bez weryfikacji.
- Nie ma możliwości ręcznej zmiany statusu użytkownika z *Zaufany* na *Niezaufany*. Zablokowanie użytkownika w Fudo Enterprise automatycznie uniemożliwi mu dostęp do zasobów udostępnionych przez Fudo ShareAccess.

17.4.3 Tworzenie konta bez zaproszenia

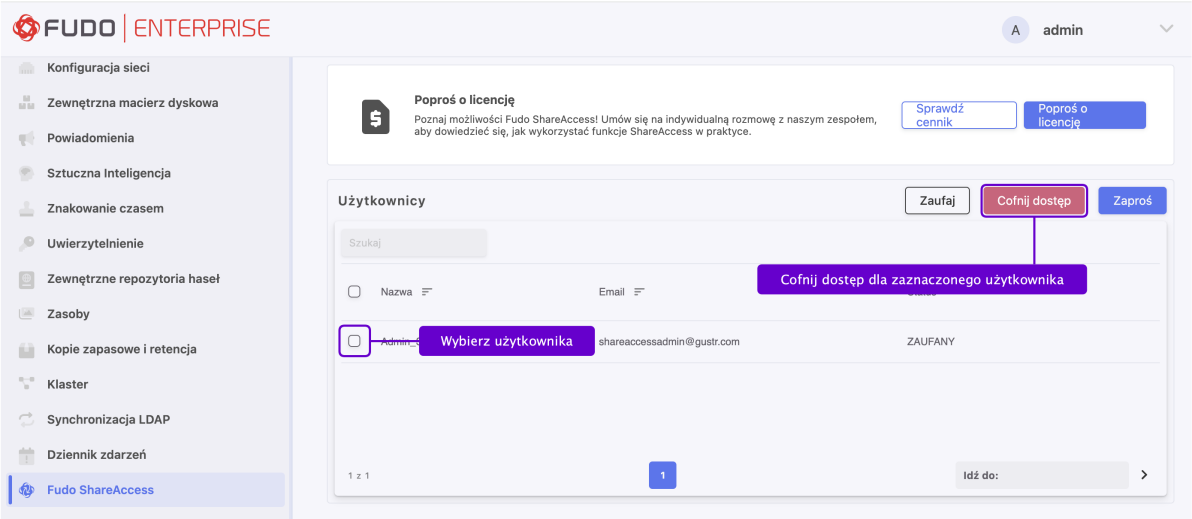
Możliwe jest utworzenie konta bez zaproszenia. Jeśli domena e-mail użytkownika pasuje do domeny organizacji istniejącej w Fudo ShareAccess, użytkownik zostanie automatycznie przypisany do tej organizacji. Domyślnie konto będzie nieaktywne, a użytkownik nie będzie miał dostępu do Fudo ShareAccess. Właściciel organizacji otrzyma powiadomienie e-mail o nowym użytkowniku wraz z linkiem umożliwiającym aktywację jego konta.

Więcej informacji można znaleźć w ShareAccess.

17.4.4 Cofanie statusu członków

Administrator ma możliwość cofnięcia dostępu do Fudo ShareAccess. Oznacza to, że użytkownik zostanie odłączony od swojego konta w Fudo ShareAccess i nie będzie już mógł korzystać ze swojej sieci. Aby przeprowadzić tę procedurę:

1. Wybierz *Ustawienia* > *Fudo ShareAccess*.
2. Wybierz użytkowników, których chcesz odłączyć i kliknij *Cofnij dostęp*.
3. Po potwierdzeniu wybrani użytkownicy zostaną usunięci z listy.



17.4.5 Usuwanie członków

Nie ma możliwości usunięcia użytkownika z organizacji ani Fudo ShareAccess. Jedyną możliwością jest oznaczenie konta jako *Nieaktywne*. Więcej informacji na ten temat można znaleźć w ShareAccess.

Tematy pokrewne:

- *Model danych*
- *Parowanie Fudo Enterprise i Fudo ShareAccess*
- *Zarządzanie dostępem do zasobów*

17.5 Zarządzanie dostępem do zasobów

Dostęp do zasobów za pośrednictwem Fudo ShareAccess jest zarządzany w Fudo Enterprise przy użyciu standardowych obiektów, takich jak Użytkownik, Serwer, Konto i Sejf.

Uwaga

W Fudo ShareAccess widoczność konfiguracji zależy od określonych warunków. Poniżej przedstawiono podsumowanie wymagań i warunków, które muszą zostać spełnione, aby konfiguracje były widoczne:

- **Wymagania dla użytkownika:** Użytkownik musi być sparowany z Fudo ShareAccess lub zaproszony do niego.
- **Obsługiwane protokoły:** Następujące protokoły są obsługiwane przez Fudo ShareAccess:
  - RDP,
  - SSH,
  - VNC.
- **Typy kont:** Obsługiwane są tylko następujące typy kont:
  - Konta *regular* z poprawnie skonfigurowanymi poświadczeniami,

  - Konta typu *forward*.
- **Sejf:** W sejfie muszą być włączone następujące opcje:
  - Fudo ShareAccess,
  - OTP,
  - Webclient.

*Gniazdo nasłuchiwania nie jest wymagane do udzielania dostępu do zasobów w Fudo ShareAccess.

Aby przyznać użytkownikowi dostęp do określonego serwera za pośrednictwem Fudo ShareAccess, wykonaj poniższe kroki:

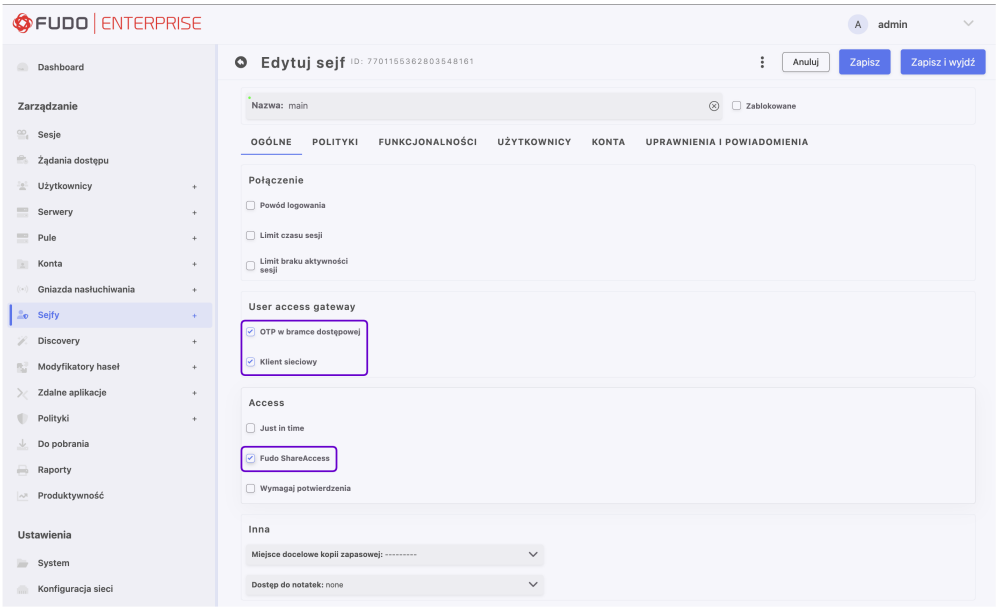
1. Utwórz użytkownika i zaproś go do dołączenia do Fudo ShareAccess. Szczegółowe instrukcje znajdziesz w sekcji *Zarządzanie użytkownikami Fudo ShareAccess*.
2. Utwórz serwer, do którego chcesz przyznać dostęp za pośrednictwem Fudo ShareAccess.
   - Wybierz *Zarządzanie* > *Serwery*, a następnie kliknij + *Dodaj serwer*.
   - Wprowadź unikalną nazwę serwera.
   - W sekcji *Ustawienia* na liście dostępnych protokołów wybierz `RDP` lub `SSH`.
   - Z rozwijanego menu *Adres powiązania* wybierz adres IP Fudo Enterprise używany do komunikacji z tym serwerem.
   - W sekcji *Cel* wybierz `Host`, `IPv4` lub `IPv6` i wprowadź adres IP serwera.
   - Kliknij *Zapisz i zamknij*.
3. Utwórz konto przypisane do tego serwera:
   - Wybierz *Zarządzanie* > *Konta*, a następnie kliknij + *Dodaj konto*.
   - Zdefiniuj nazwę obiektu.
   - W zakładce *Ustawienia*, w polu *Typ*, naciśnij przycisk *REGULAR*.
   - W sekcji *Cel* kliknij *Serwer*, aby przypisać konto do konkretnego serwera, a następnie z listy rozwijanej *Serwer* wybierz serwer utworzony w poprzednim kroku.
   - W sekcji *Poświadczenia* wprowadź login dla konta na serwerze.
   - W sekcji *Zamień sekret na*, kliknij przycisk dla wybranej opcji, takiej jak *Hasło*, i wprowadź hasło konta w polu *Sekret*.
   - Kliknij *Zapisz i zamknij*.
4. Utwórz sejf:
   - Wybierz *Zarządzanie* > *Sejfy*, a następnie kliknij + *Dodaj sejf*.
   - Wprowadź nazwę obiektu.
   - Kliknij *Zapisz*, aby zapisać obiekt i przejść do dalszej konfiguracji.
   - W zakładce *Ogólne*:

– Opcja *OTP w Portalu Użytkownika* jest domyślnie włączona i odpowiada za generowanie jednorazowych kodów OTP dla Portalu Użytkownika (wymagana).

– Wybierz opcję *Web Client*, aby umożliwić łączenie się za pomocą wbudowanego klienta przeglądarki (wymagana).

– Wybierz opcję *Fudo ShareAccess*, aby udostępnić sejf do użytku w Fudo ShareAccess (wymagana).

– Wybierz opcję *Just in time* i podaj liczbę głosujących. Funkcja ta umożliwia zdefiniowanie i zaplanowanie czasu, w którym użytkownik ma dostęp do określonych zasobów przez ustalony czas. Użytkownik przesyła żądania za pośrednictwem Portalu Użytkownika, a głosujący akceptują lub odrzucają je w Panelu Administracyjnym. Więcej informacji o funkcji *Just-In-Time* znajdziesz w rozdziale *Żądania dostępu* (opcjonalne).

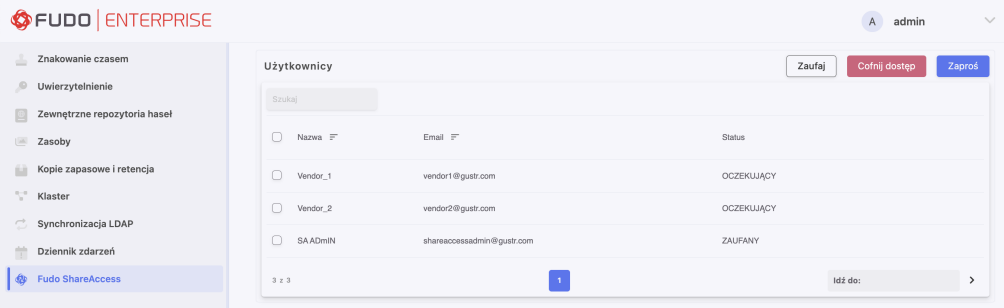


- Kliknij *Zapisz*.

5. Dodaj utworzonego użytkownika i konto do sejfu:

   - Przejdź do zakładki *Użytkownicy*, aby przypisać użytkowników, którzy będą mieli dostęp do kont przypisanych do tego sejfu.
   - Kliknij *Zarządzaj użytkownikami*.
   - Zaznacz pole wyboru przed nazwiskami użytkowników, aby umożliwić im dostęp do serwerów za pośrednictwem monitorowanego sejfu.
   - Kliknij *Zapisz*, aby zamknąć okno modalne.
   - Wybierz zakładkę *Konta*, aby dodać konta dostępne w tym sejfie.
   - Kliknij *Zarządzaj kontami*.
   - Zaznacz pole wyboru przed nazwami kont, aby je dodać.
   - Kliknij *Zapisz*, aby zamknąć okno modalne.
   - Kliknij *Zapisz*, aby zamknąć okno modalne.

6. Upewnij się, że użytkownik ma status zaufany:
    - Wybierz *Ustawienia* > *Fudo ShareAccess*.
    - Znajdź żądanego użytkownika na liście członków i upewnij się, że jego status to *TRUSTED*.



7. Po wykonaniu powyższych kroków użytkownik przypisany do sejfu może zalogować się do Fudo ShareAccess i uzyskać dostęp do serwera powiązanego z sejfem. Więcej informacji na ten temat można znaleźć w ShareAccess.

Tematy pokrewne:

- *Zarządzanie użytkownikami Fudo ShareAccess*
- *Wymagane potwierdzenie dostępu*
- *Żądania dostępu*

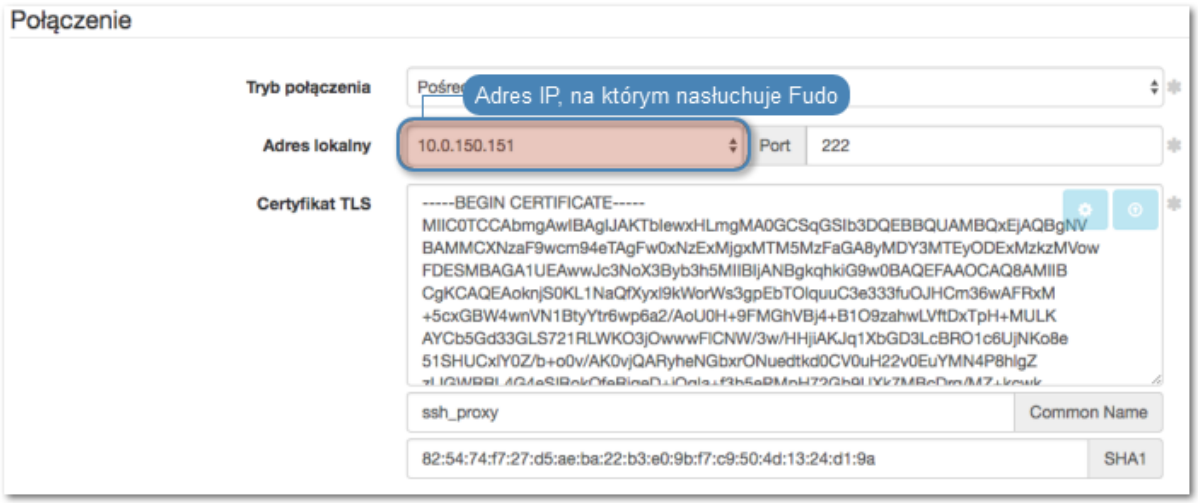
ROZDZIAŁ 18

Aplikacje klienckie

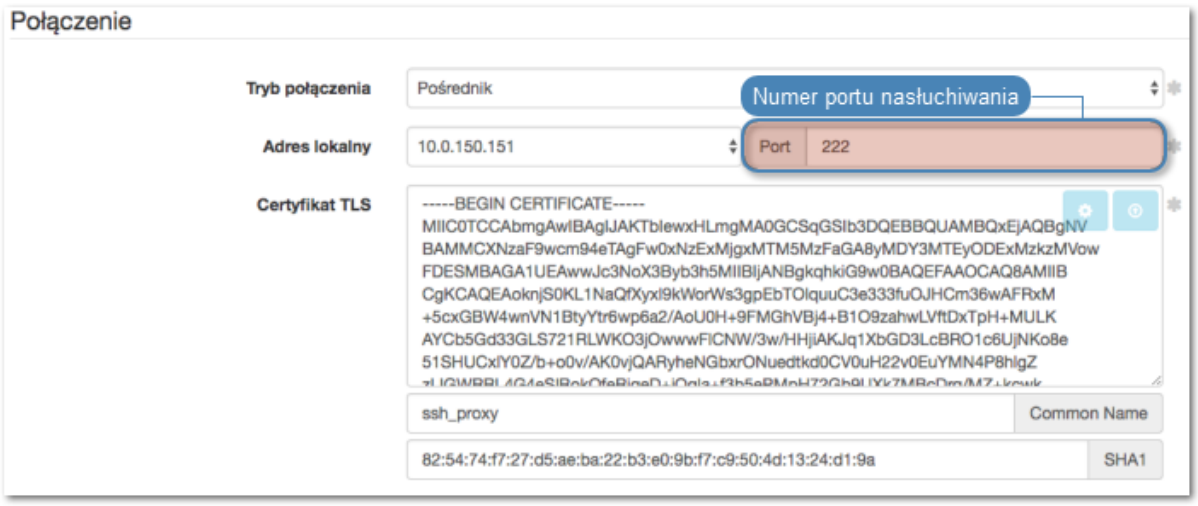
18.1 PuTTY

Połączenie *SSH* z serwerem monitorowanym poprzez gniazdo nasłuchiwania w trybie *proxy*.

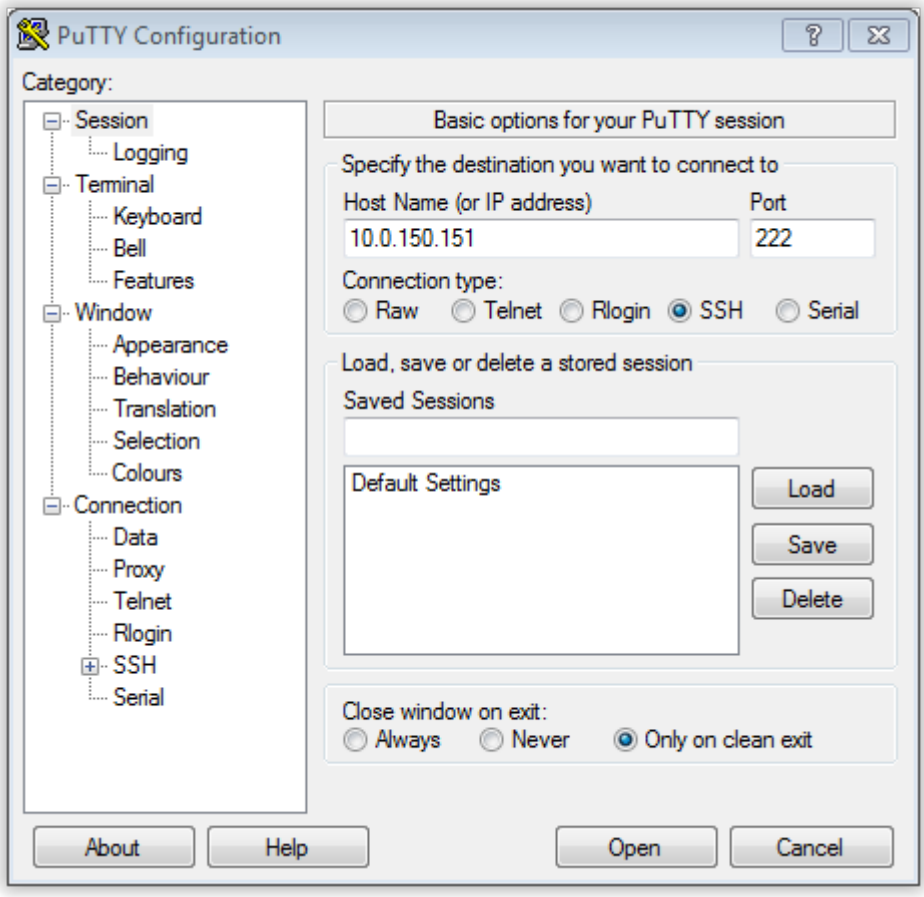
1. Pobierz i uruchom PuTTY.
2. W polu *Host Name (or IP address)* wprowadź adres IP zdefiniowany w sekcji *Połączenie*, w parametrze *Adres lokalny* gniazda nasłuchiwania.



3. Wprowadź numer portu zgodnie z definicją w obiekcie.

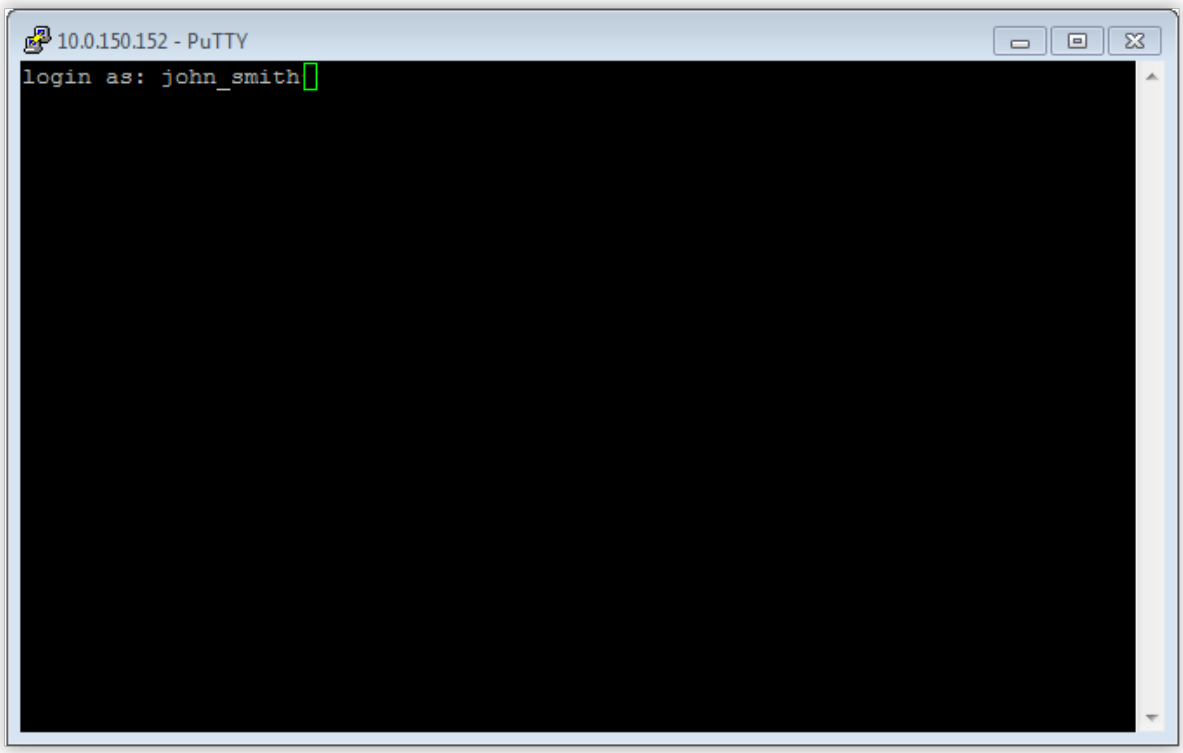


4. W polu wyboru typu połączenia (*Connection type*), wybierz `SSH`.



5. Kliknij *Open*.

6. Wprowadź nazwę użytkownika wraz z nazwą konta, na serwerze docelowym.



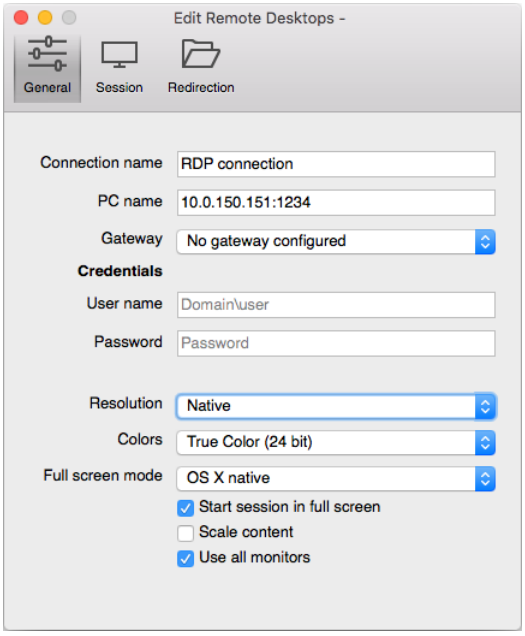
6. Wprowadź hasło użytkownika.

Tematy pokrewne:

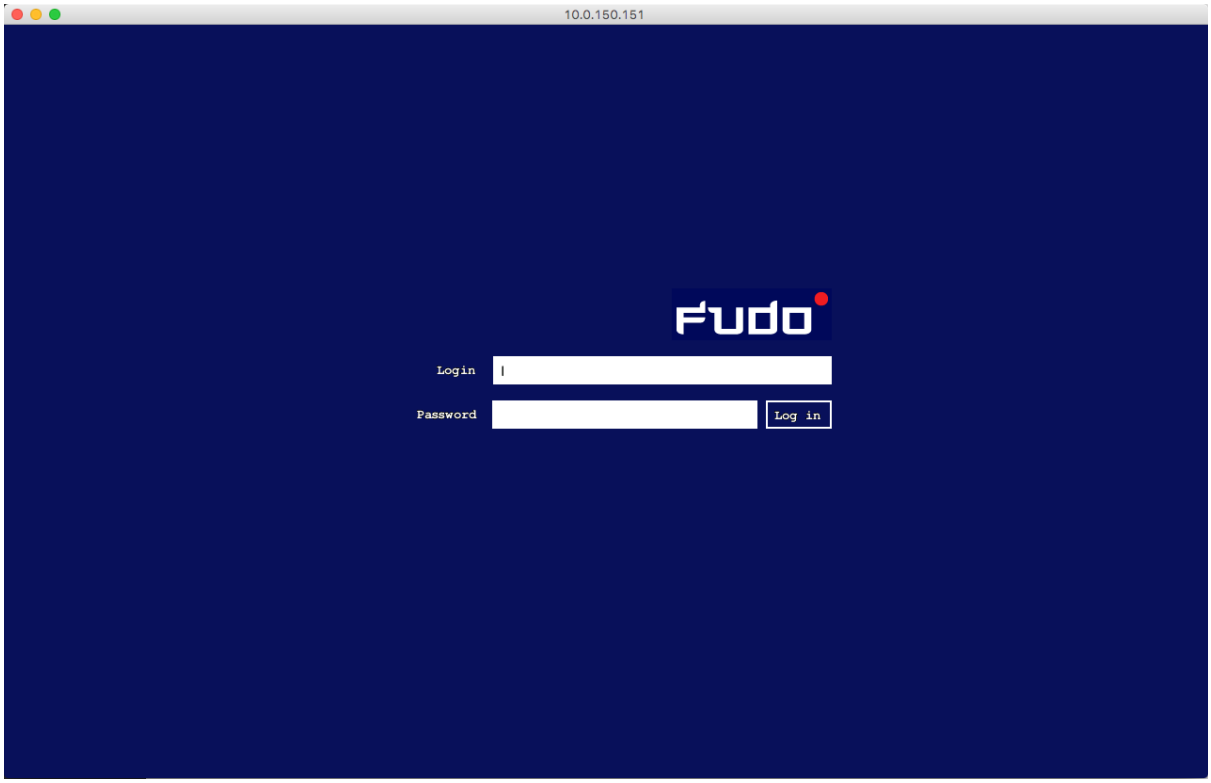
- *SSH*

18.2 Microsoft Remote Desktop

1. Uruchom klienta połączeń RDP.
2. W polu *PC name*, wprowadź adres IP oraz numer portu zdefiniowany w gnieździe nasłuchiwania.

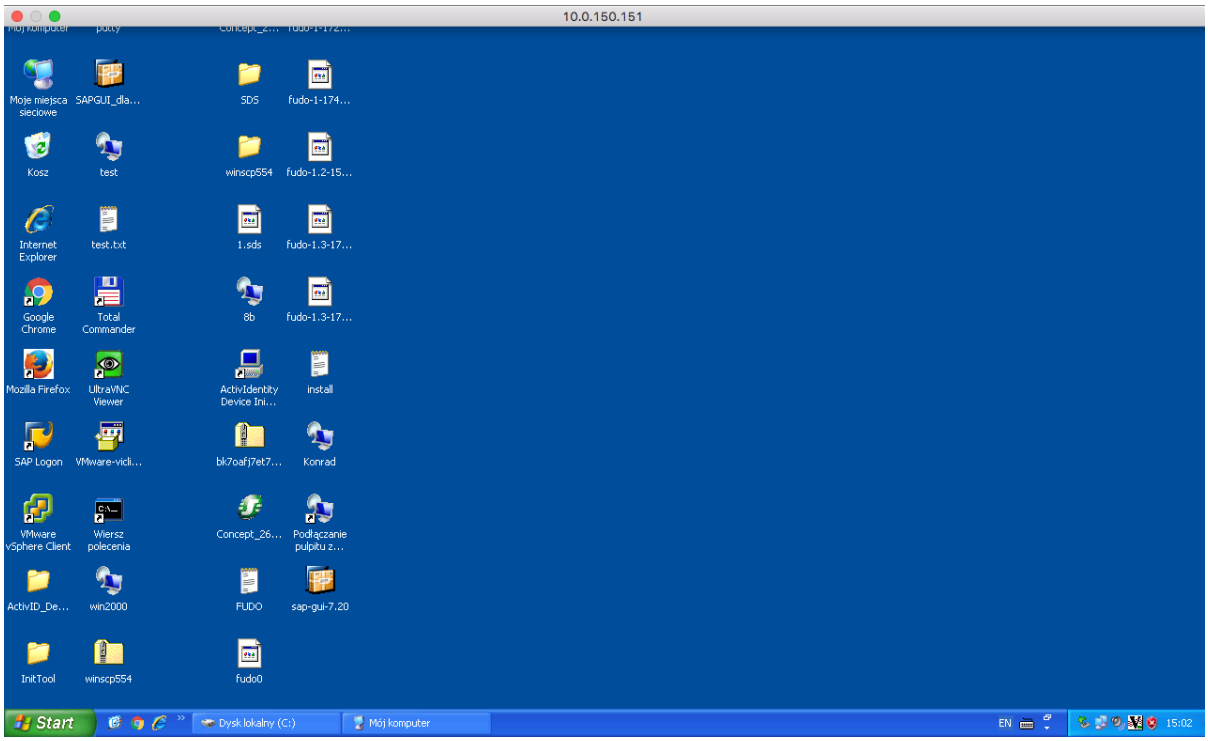


3. Wpisz login i hasło użytkownika i zatwierdź przyciskiem [Enter].



Uwaga

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*.

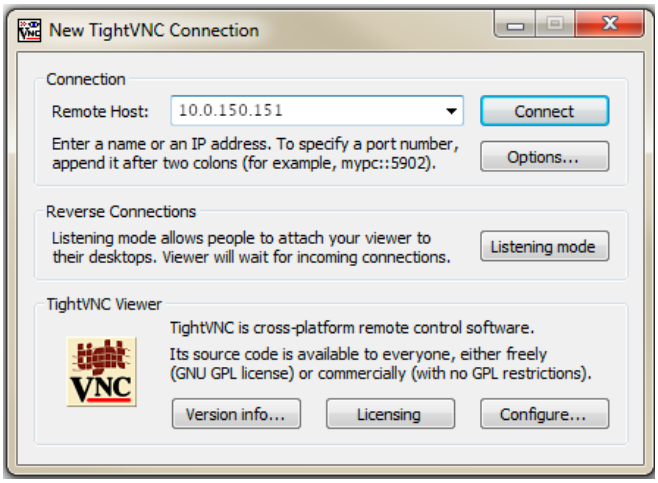


Tematy pokrewne:

- *RDP*

18.3 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*).



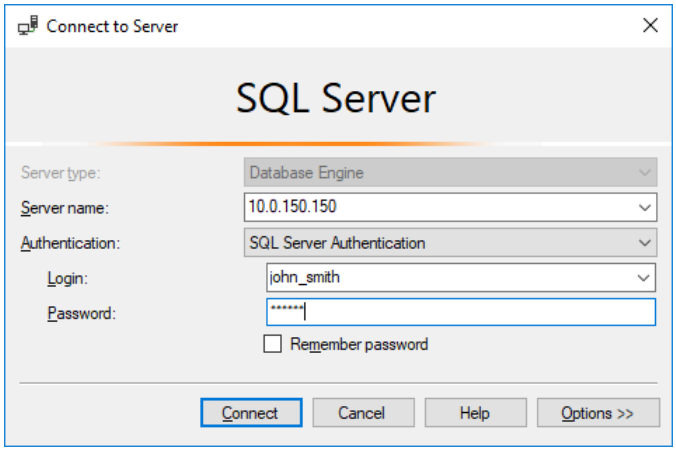
2. Wprowadź nazwę użytkownika, hasło i zatwierdź klawiszem enter.

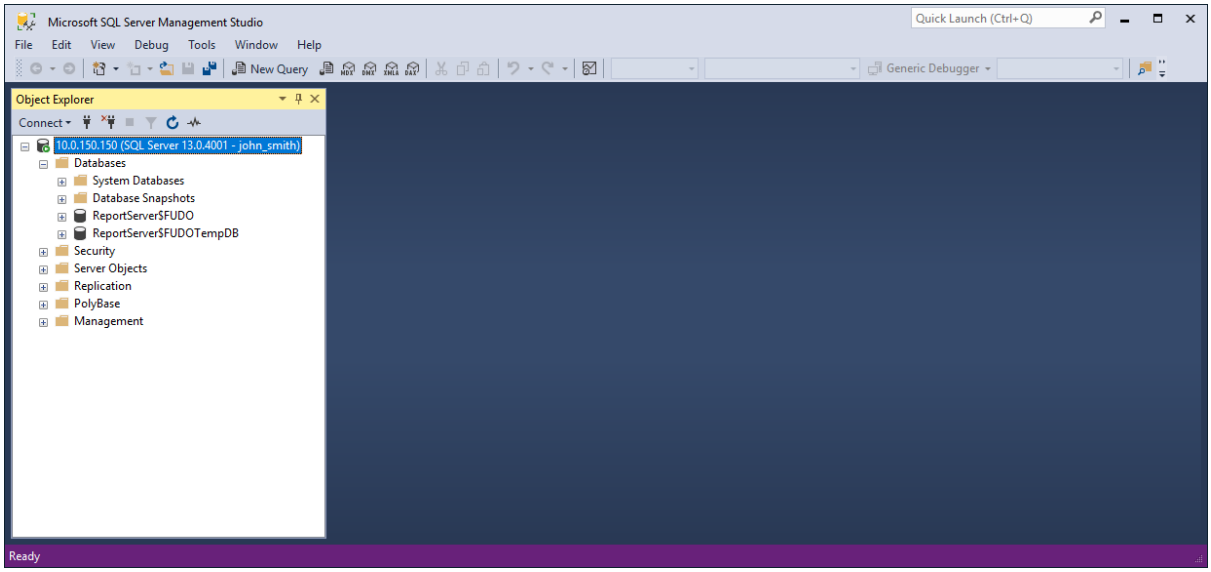
Tematy pokrewne:

- *Szybki start*

18.4 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*

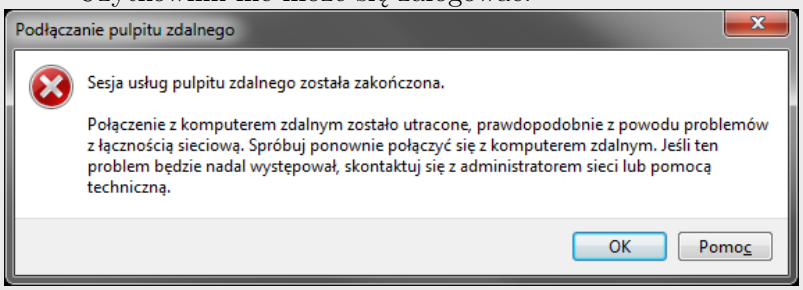
ROZDZIAŁ 19

Rozwiązywanie problemów

19.1 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.

19.2 Połączenia z serwerami

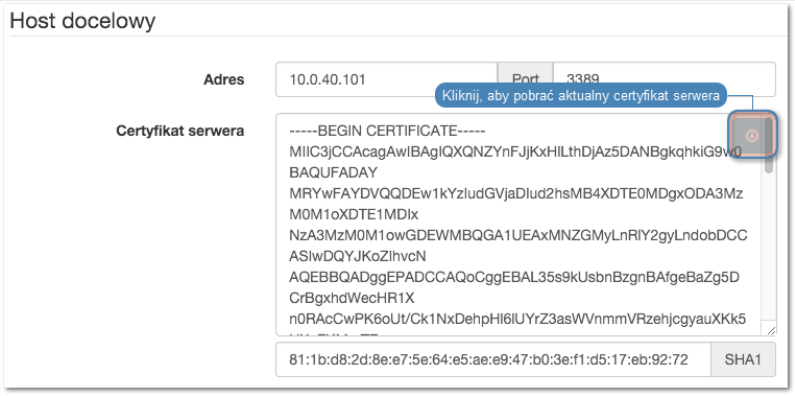
Problem	Objawy i opis rozwiązania
Nie można nawiązać połączenia z serwerem	**Objawy:** • Użytkownik nie może się zalogować.  • Wpis w dzienniku zdarzeń: *Authentication failed: Invalid username kowalski or password.*
	Rozwiązanie: • Sprawdź czy definicja użytkownika istnieje w systemie Fudo Enterprise. • 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.

ciąg dalszy 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*.

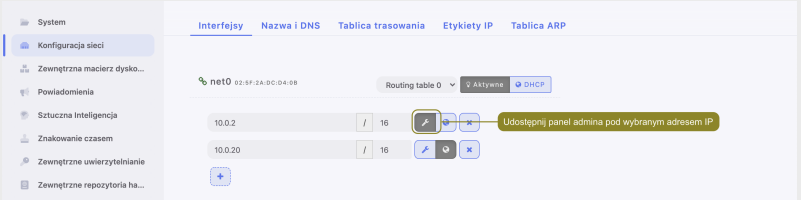
Problem	Objawy i opis rozwiązania
Przy próbie logowania nie wszyscy użytkownicy widzą ekran logowania Fudo Enterprise (standardowy, z szarym tłem).	**Przyczyna:** • Zapisane poświadczenia w skrócie RDP skutkują ukryciem ekranu Fudo Enterprise i bezpośrednim zalogowaniem do serwera docelowego. • Zapisane 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.

19.3 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. 

19.4 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.

19.5 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.

19.6 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*.

19.7 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.

> **Uwaga**
>
> 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:

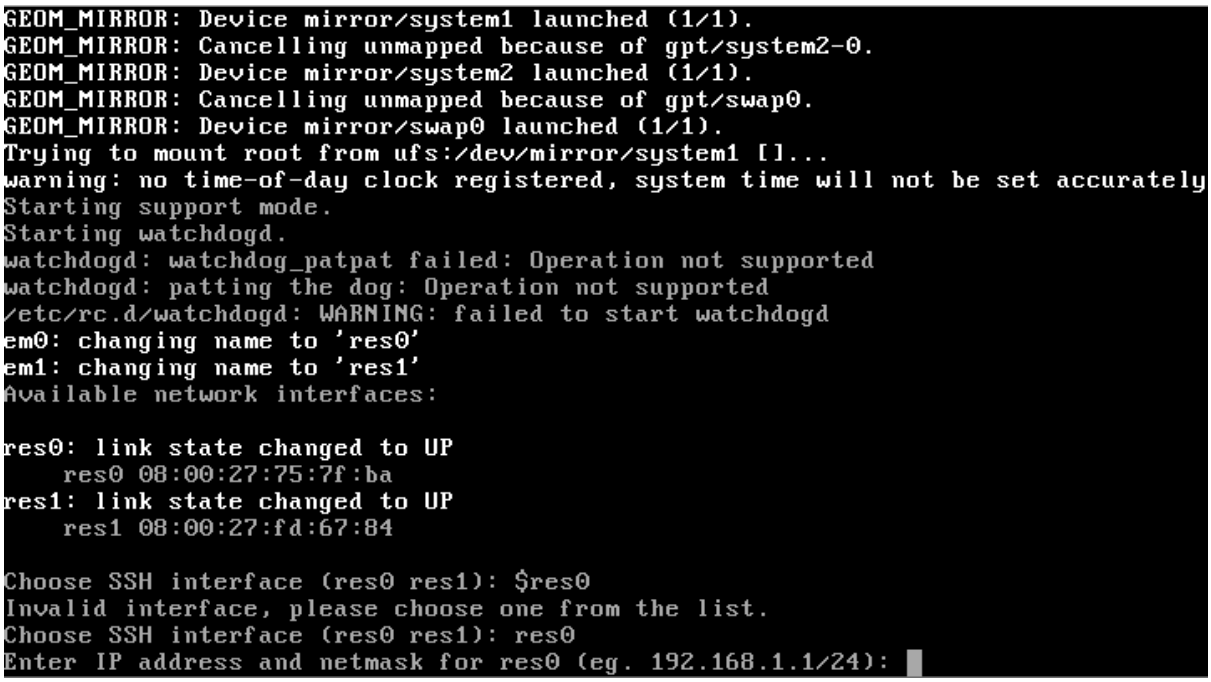
res0: link state changed to UP
    res0 08:00:27:75:7f:ba
res1: link state changed to UP
    res1 08:00:27:fd:67:84

Choose SSH interface (res0 res1): $
```

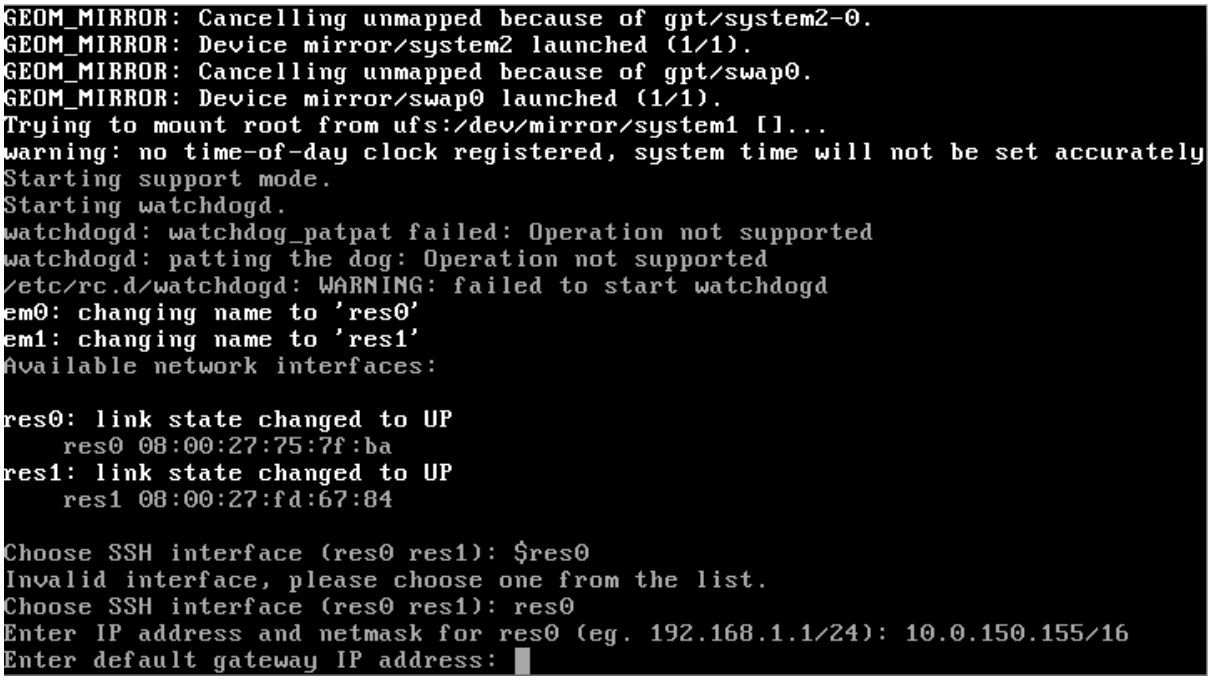
4. Wprowadź adres IP wraz z maską podsieci, np. `10.0.0.8/16`.

> **Uwaga**
>
> 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.



Uwaga

- 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 20

Przypadki użycia

20.1 Dwuskładnikowe uwierzytelnienie OATH z Google Authenticator

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

Uwaga

Do konfiguracji dwuskładnikowego uwierzytelnienia OATH w Fudo Enterprise można również rozważyć użycie alternatywnych aplikacji, takich jak Microsoft Authenticator.

20.1.1 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

ciąg dalszy na następnej stronie

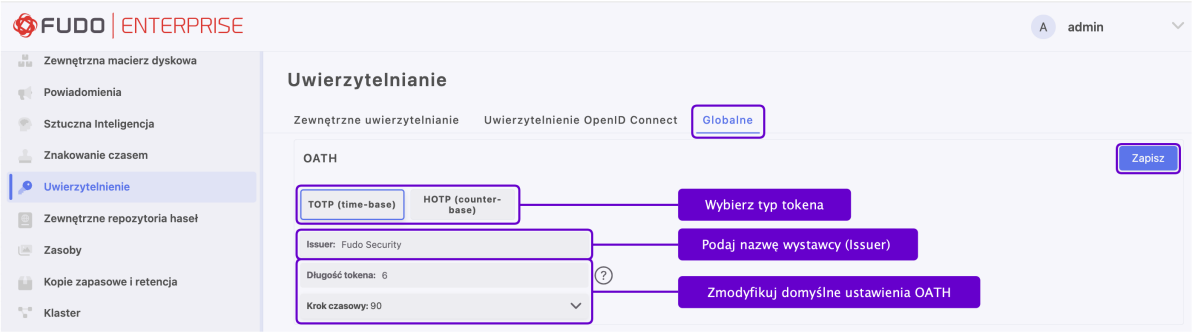
Tabela 1 – kontynuacja poprzedniej strony

Platforma / Protokół	Tryb Challenge-Response	Hasło + Wygenerowany kod
Telnet 5250	nie dostępne	dostępne
Telnet	nie dostępne	dostępne
MySQL	nie dostępne	dostępne
MS SQL(TDS)	nie dostępne	nie dostępne
HTTP/S	nie dostępne	nie dostępne
TCP	nie dostępne	nie dostępne
X11	nie dostępne	nie dostępne
Modbus	nie dostępne	nie dostępne

20.1.2 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*.



20.1.3 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.*

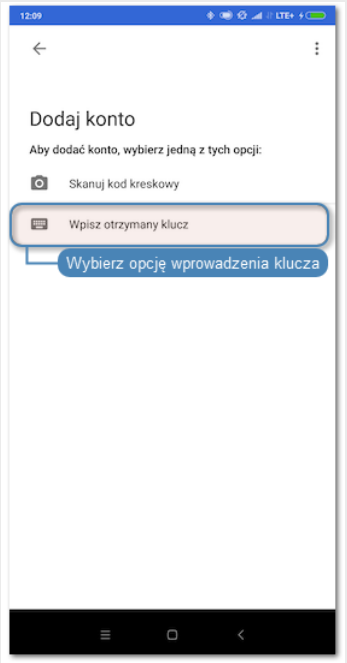
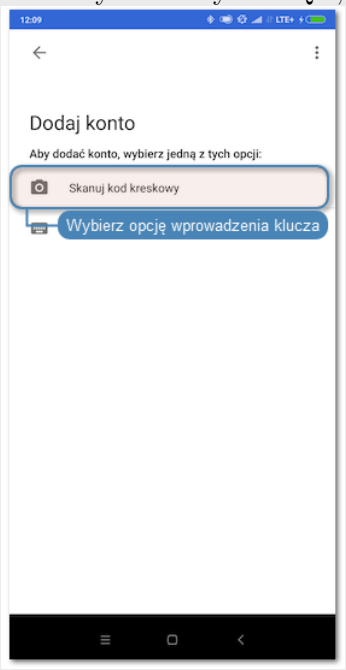
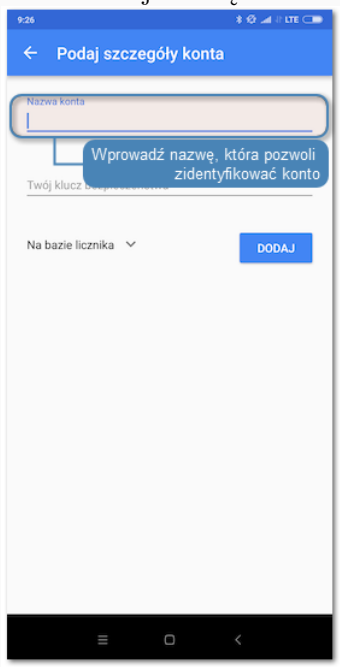
Jeśli zostało wybrane `Zewnętrzne uwierzytelnienie`:

- 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.

Uwaga

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.

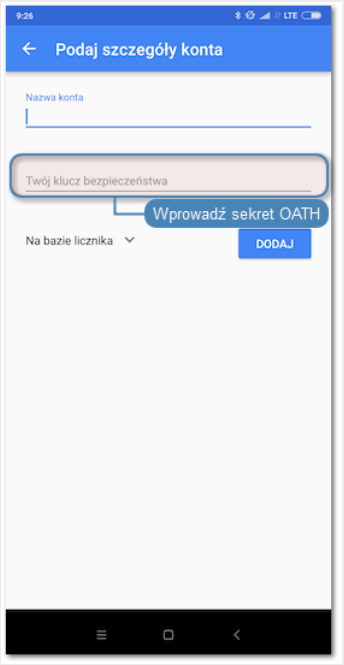
Ręczne wprowadzenie danych	Kod QR
• Na ekranie dodawania konta, wybierz *Wpisz otrzymany klucz*. 	• Kliknij ikonę na formularzu konfiguracji użytkownika, w sekcji *Uwierzytelnienie*, w polu *Sekret*. • Wybierz *Skanuj kod kreskowy* i zeskanuj wyświetlony kod QR, aby dodać konto. 
• Nadaj nazwę konta. 	

ciąg dalszy na następnej stronie

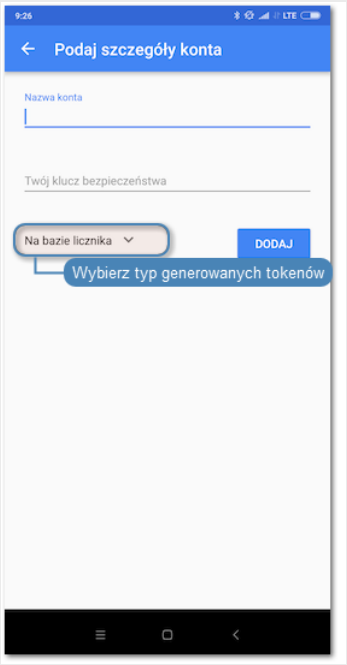
Tabela 2 – kontynuacja poprzedniej strony

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*.

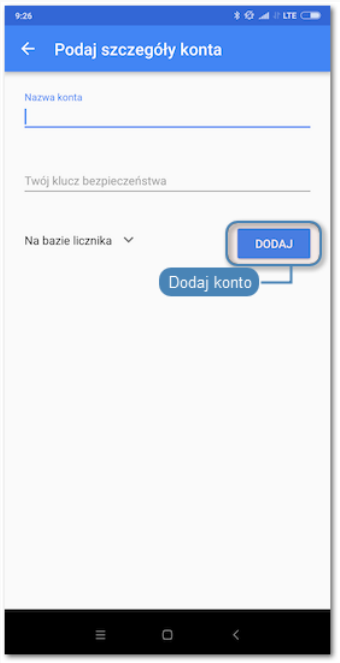


ciąg dalszy na następnej stronie

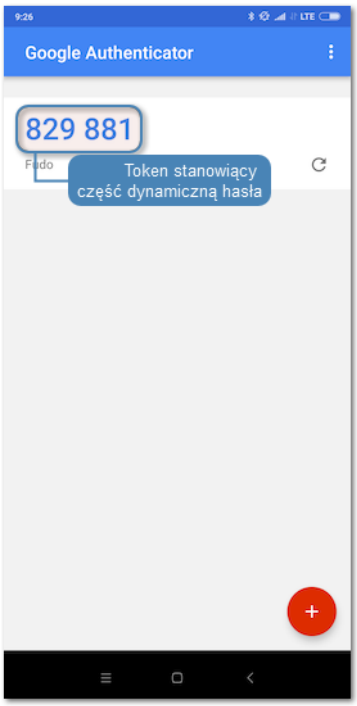
Tabela 2 – kontynuacja poprzedniej strony

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*

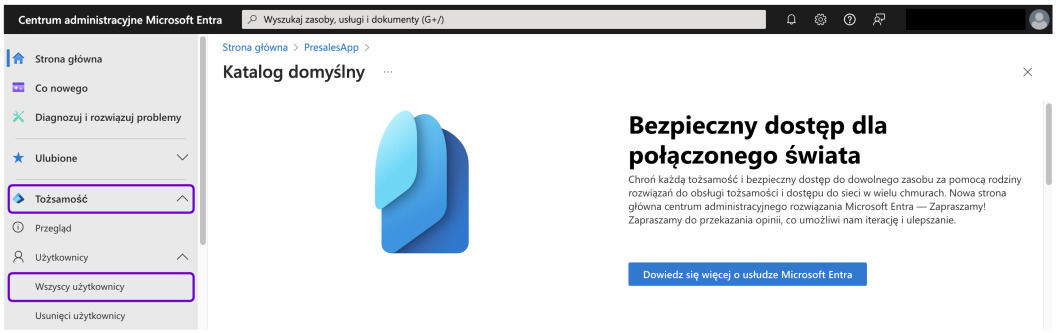
20.2 Konfiguracja uwierzytelnienia OpenID Connect w Microsoft Entra (Azure)

Aby skonfigurować metodę uwierzytelnienia OpenID Connect z Microsoft Entra, postępuj zgodnie z poniższymi krokami.

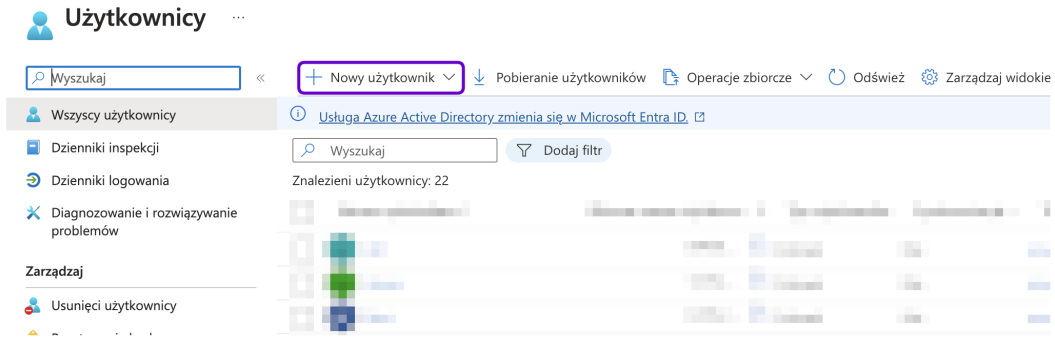
> **Uwaga**
>
> Jest to ogólna instrukcja, mająca na celu przybliżenie procesu konfigurowania metody uwierzytelnienia OpenID Connect w Fudo Enterprise. Niektóre szczegóły mogą się różnić w zależności od posiadanej wersji oraz konfiguracji Microsoft Entra. Szczegółową instrukcję znajdziesz w dokumentacji 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*.

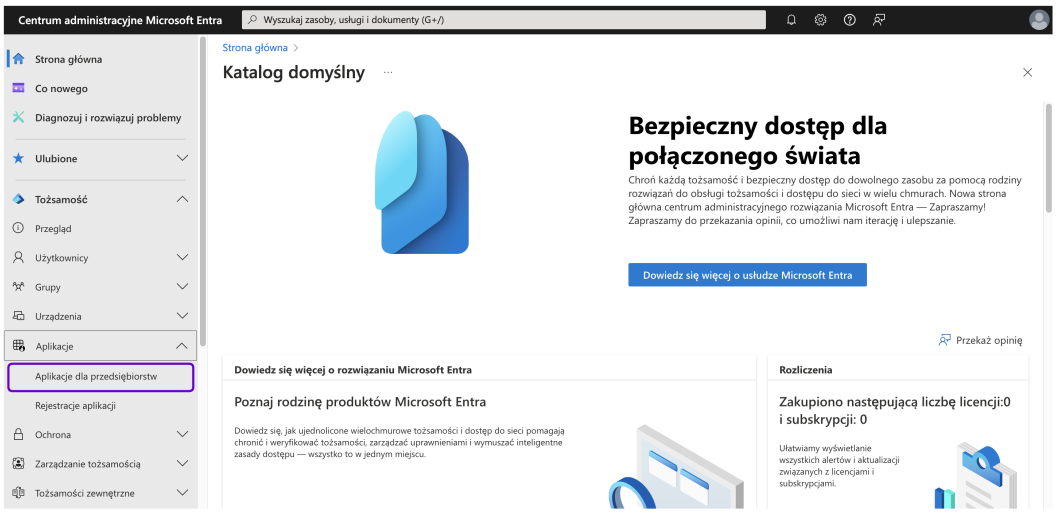


4. W polu *Nazwa główna użytkownika* wprowadź nazwę użytkownika konta. Na przykład: `user1@fudosecurity.com`.
5. W polu *Nazwa wyświetlana* podaj nazwę użytkownika konta.
6. Wprowadź hasło w polu *Hasło* lub kliknij opcję *Automatyczne generowanie hasła*, aby wygenerować hasło.
7. Wybierz opcję *Konto włączone*.

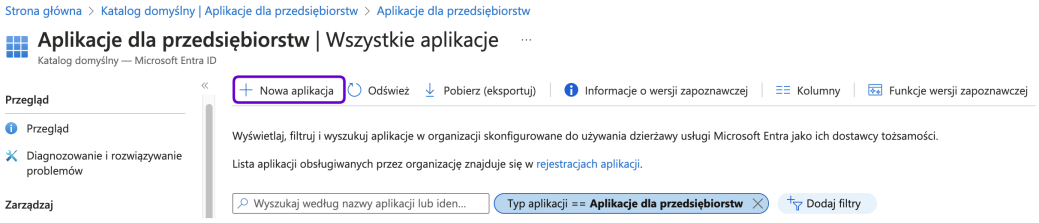
8. W zakładce *Właściwości*, w sekcji menu *Informacje kontaktowe*, w polu *E-mail* podaj adres e-mail. Na przykład: `user1@fudosecurity.com`.
9. Wprowadź pozostałe parametry wymagane dla użytkownika w zakładkach *Właściwości* i *Przypisania*.
10. Kliknij *Utwórz*.

Rejestracja Fudo w Microsoft Entra ID:

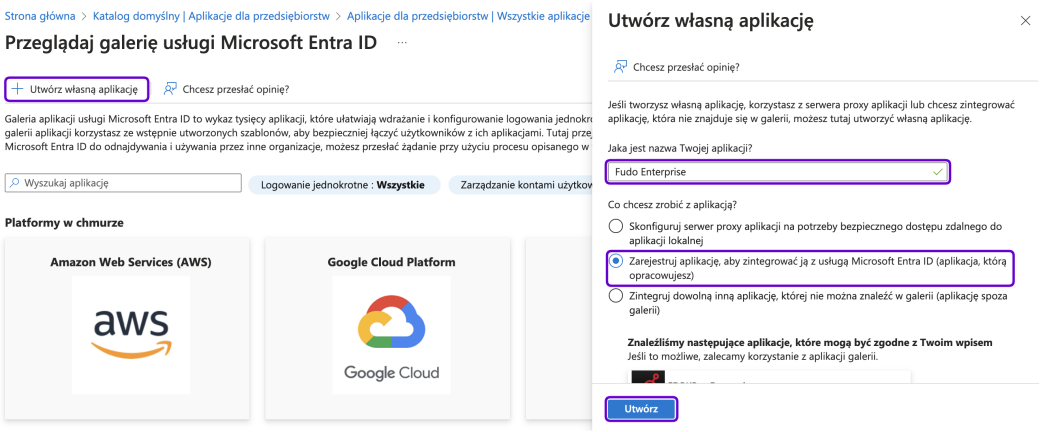
1. Z lewego menu wybierz *Tożsamość* > *Aplikacje* > *Aplikacje dla przedsiębiorstw*.



2. Kliknij przycisk *+ Nowa aplikacja*, aby utworzyć nową aplikację.



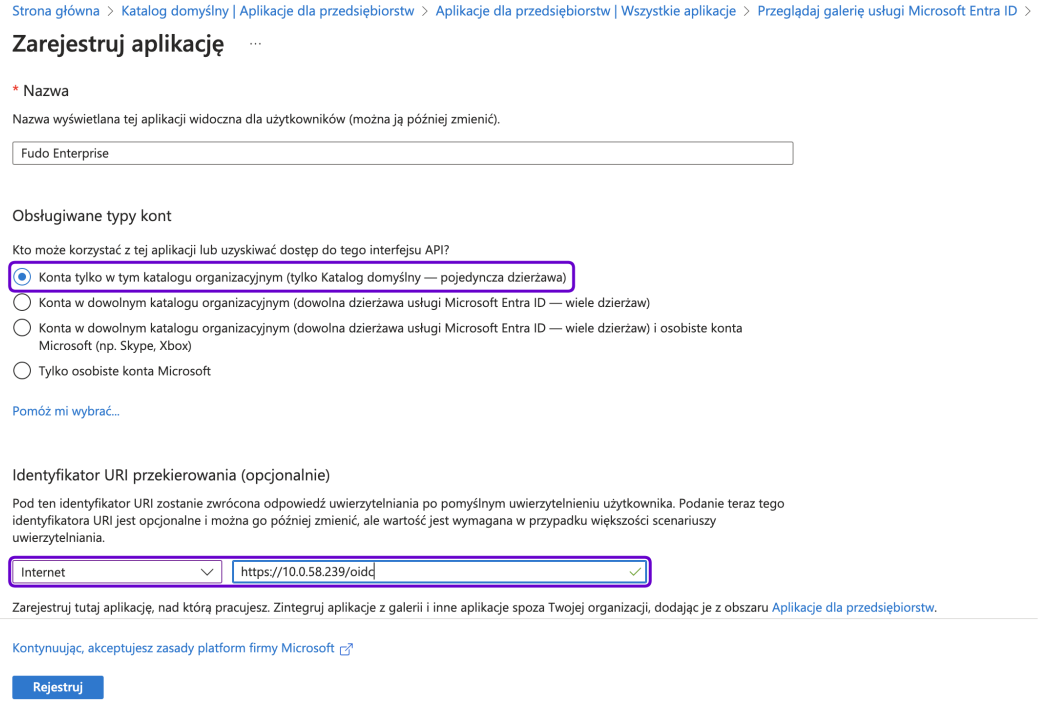
3. Kliknij przycisk *+ Utwórz własną aplikację*.
4. W prawym oknie dialogowym podaj nazwę swojej aplikacji i wybierz opcję *Zarejestruj aplikację, aby zintegrować ją z usługą Microsoft Entra ID (aplikacja, którą opracowujesz)*.
5. Kliknij *Utwórz*.



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`.

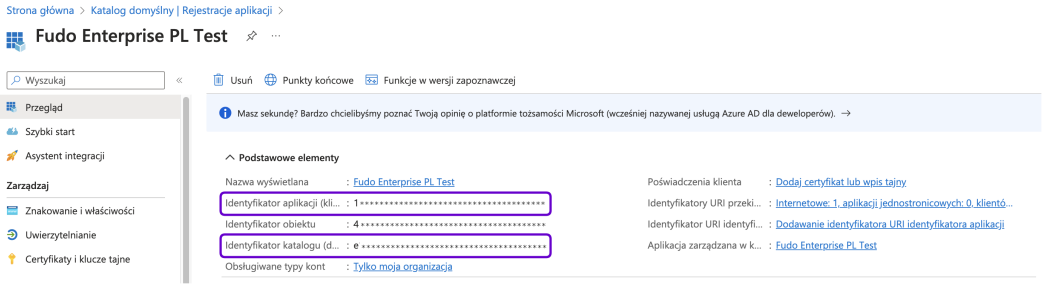
> **Uwaga**
>
> Adres Portalu Użytkownika można znaleźć w Fudo Enterprise, w menu Ustawienia > Konfiguracja sieci. Więcej informacji znajdziesz w sekcji menu *Konfiguracja sieci*.



8. Kliknij *Rejestruj*, aby utworzyć aplikację.

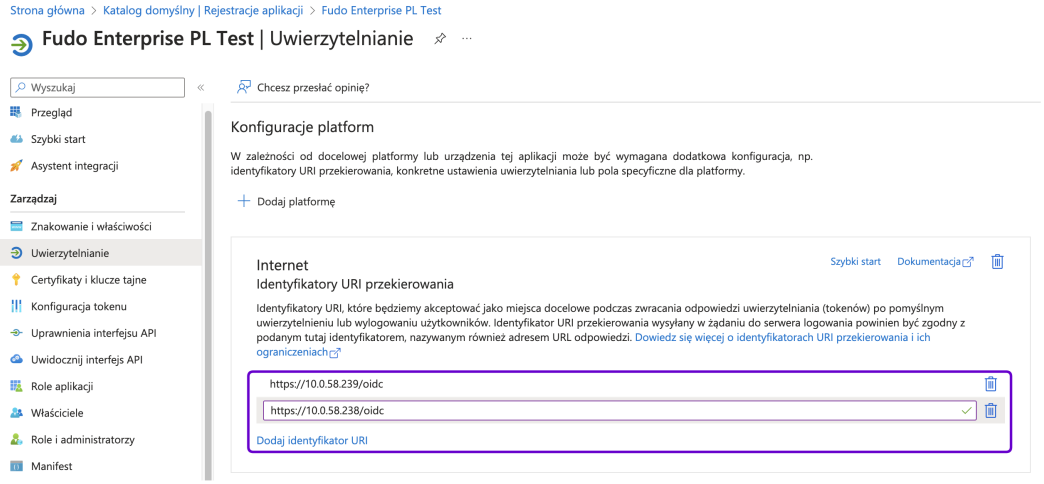
9. Z lewego menu wybierz *Tożsamość > Aplikacje > Rejestracje aplikacji.*

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.

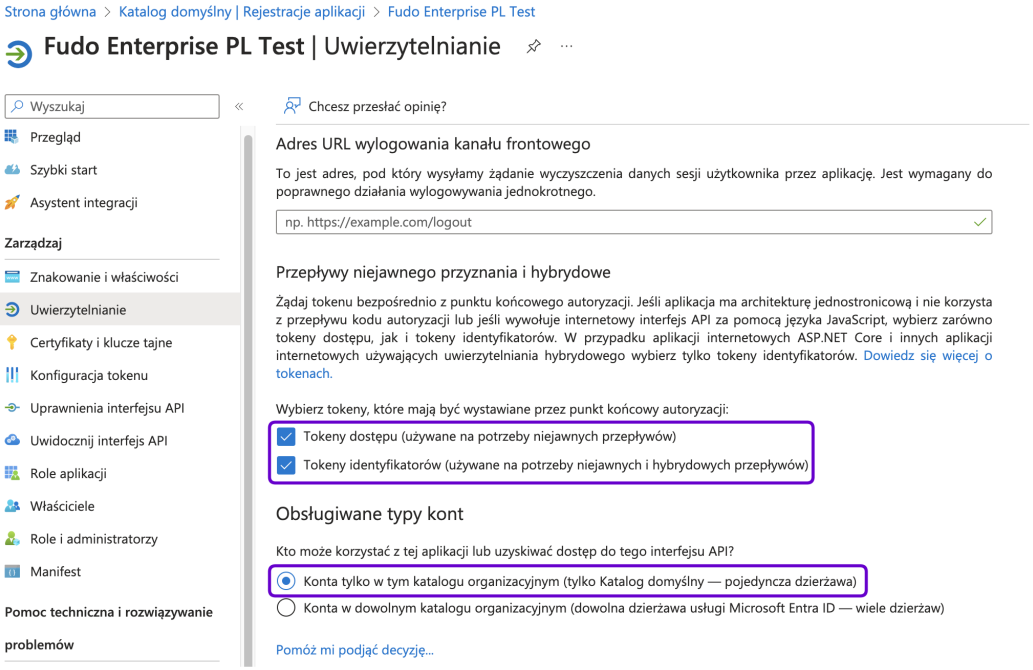


Konfiguracja ustawień uwierzytelnienia:

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:

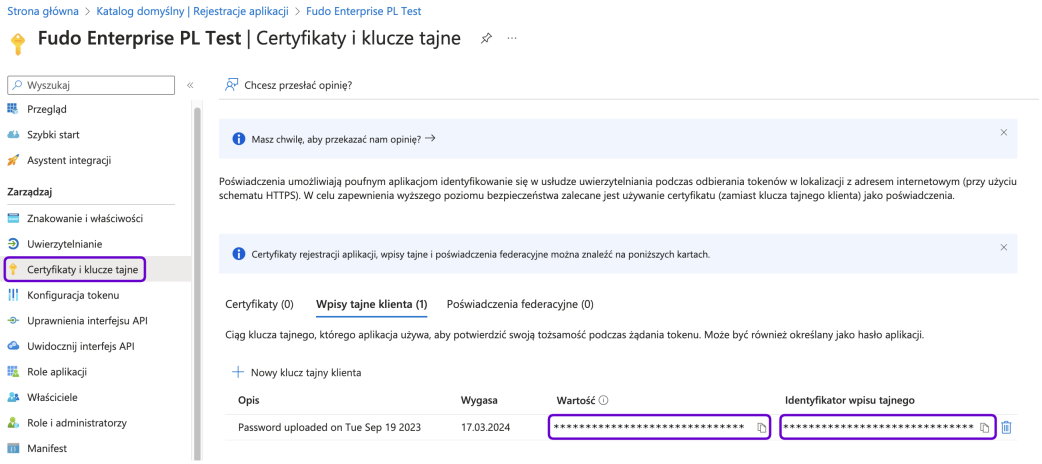
1. W ustawieniach aplikacji na portalu Azure przejdź do sekcji *Certyfikaty i klucze tajne*.

2. W zakładce *Wpisy tajne klienta* wybierz *+ Nowy klucz tajny klienta*.

3. Podaj opis, wybierz pożądany okres ważności i kliknij *Dodaj*.

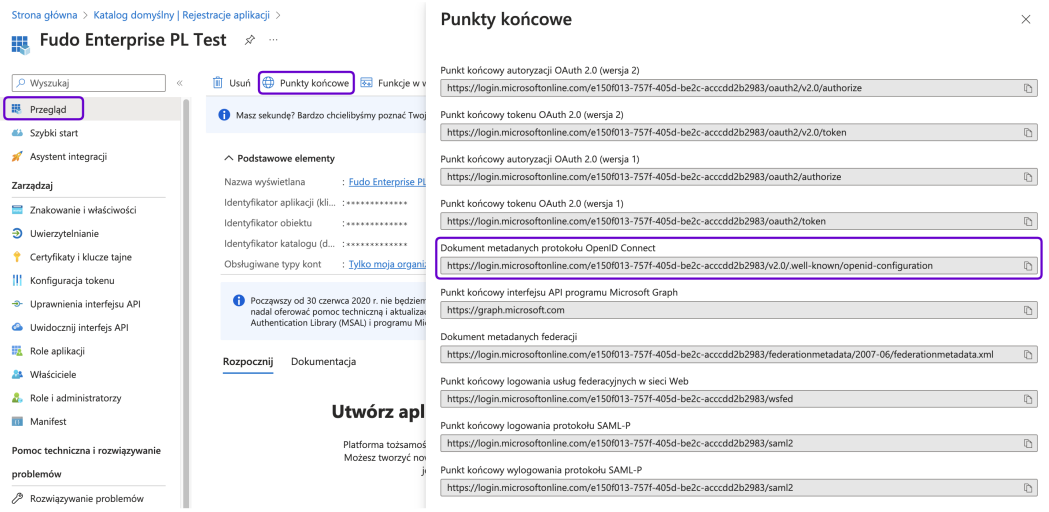
Ostrzeżenie

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:

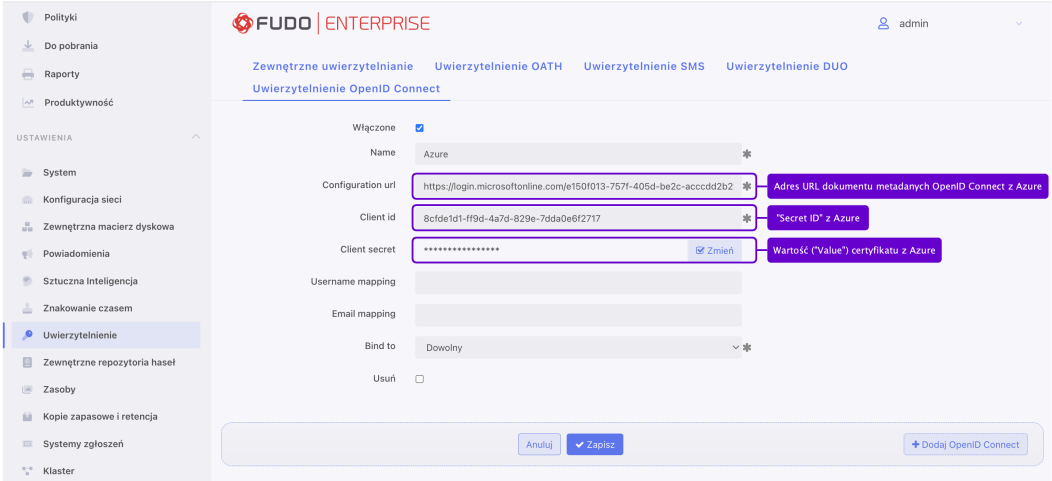
1. W ustawieniach aplikacji na portalu Azure przejdź do sekcji *Przegląd*.
2. Znajdź zakładkę *Punkty końcowe* i wyszukaj adres URL *Dokument metadanych protokołu OpenID Connect*. To jest Twój adres URL konfiguracji OpenID Connect. Skopiuj go, ponieważ będziesz go potrzebować do konfiguracji Fudo Enterprise.



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).

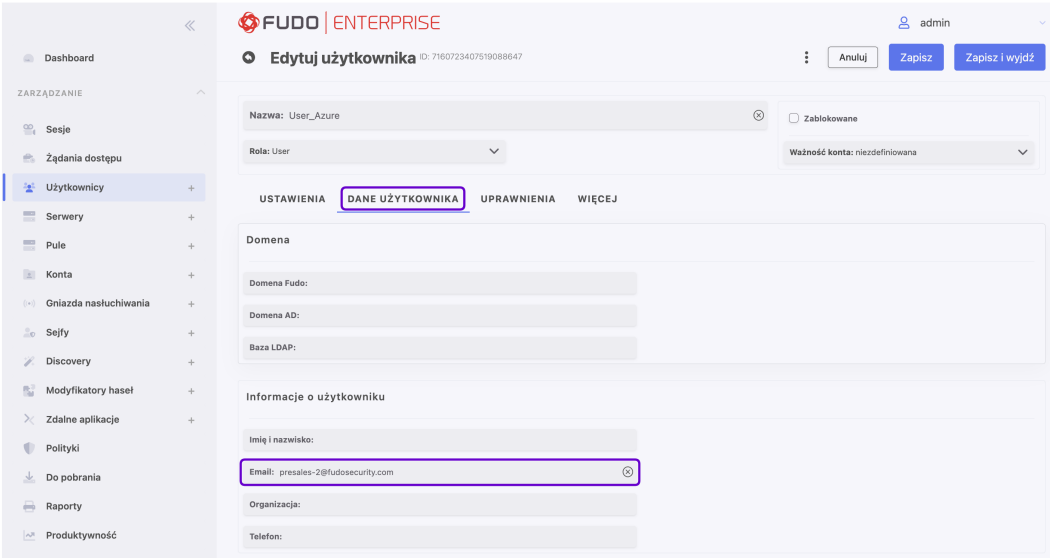


11. Dodaj *Mapowanie nazwy użytkownika* i *Mapowanie email* (opcjonalne). Te pola są przydatne, gdy nazwa użytkownika ma przyjętą inną konwencję nazewnictwa.
12. Kliknij *Zapisz*.

> **Uwaga**
>
> 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`.

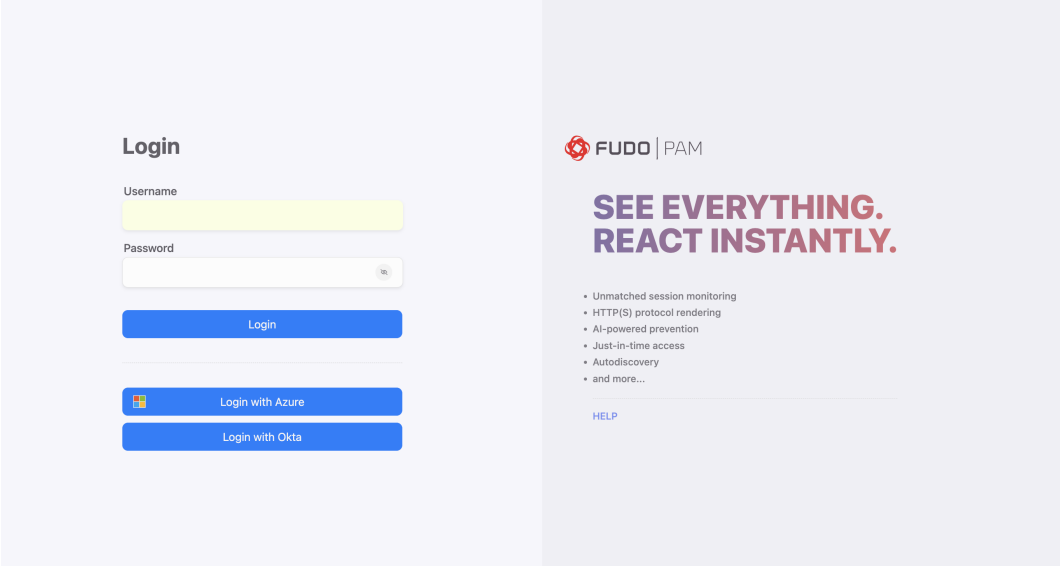


4. Wypełnij resztę parametrów zgodnie z Twoimi wymaganiami.
5. Kliknij *Zapisz*.

> **Uwaga**
>
> 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*

20.3 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.

Ostrzeżenie

Fudo Enterprise nie wspiera kont **anonymous** w konfiguracji RDS.

20.3.1 Konfiguracja usługi Remote Desktop Services (RDS) w systemie Windows

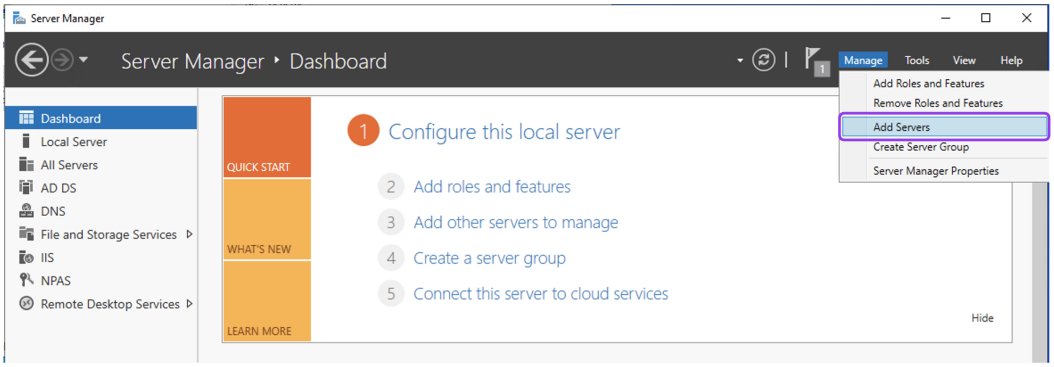
Aby skonfigurować i używać usługi Remote Desktop Services (RDS) wraz z Fudo Enterprise, postępuj zgodnie z poniższą instrukcją.

Uwaga

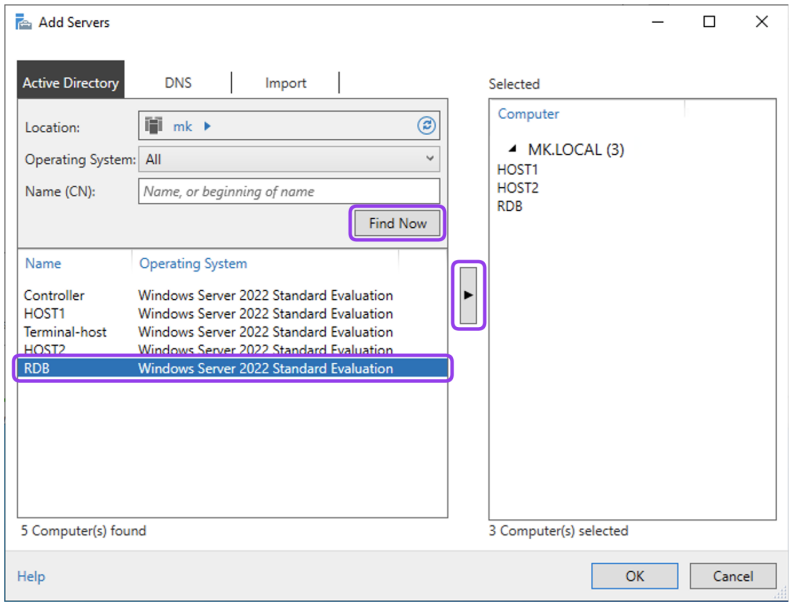
Jest to ogólna instrukcja, mająca na celu przybliżenie procesu konfigurowania usługi Remote Desktop Services. Pewne aspekty mogą się różnić w zależności od konfiguracji środowiska Windows Server. Szczegółową instrukcję znajdziesz w dokumentacji Windows Server.

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*.

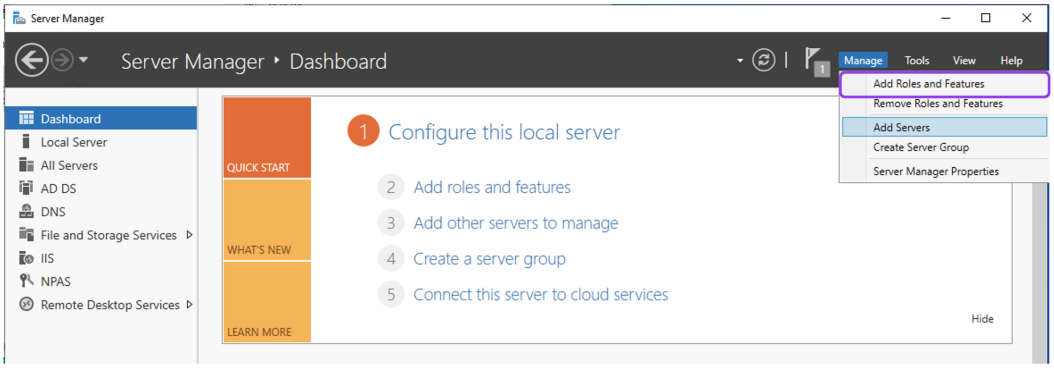


4. Kliknij *Find Now*.
5. Dodaj wszystkie serwery, które zamierzasz użyć w RDS, klikając na każdy serwer w konfiguracji. Kliknij *OK*. W tym przypadku dodajemy 3 serwery: `HOST1`, `HOST2`, i `RDB`, który będzie pełnił rolę *Brokera*.

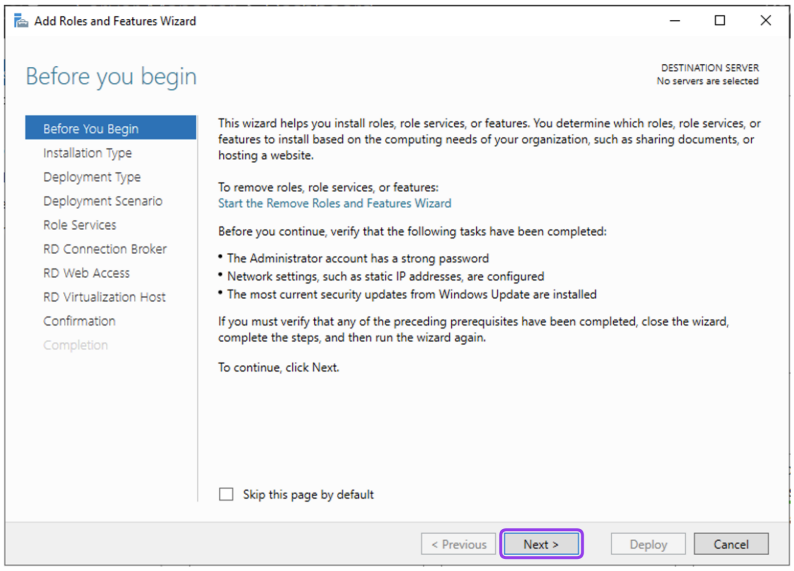


Dodaj komponenty usługi Remote Desktop Services:

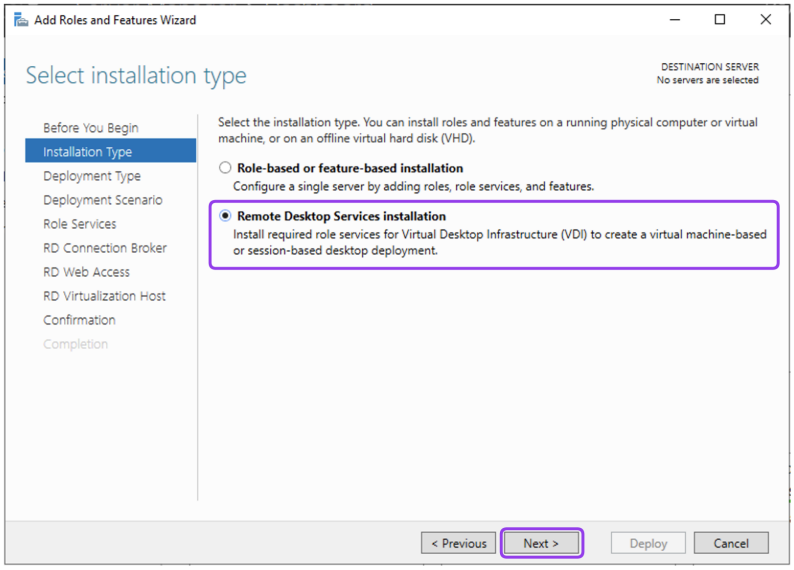
1. Kliknij przycisk *Manage* w prawym górnym rogu okna, aby rozwinięcia listę menu, a następnie wybierz *Add Roleas and Features*.



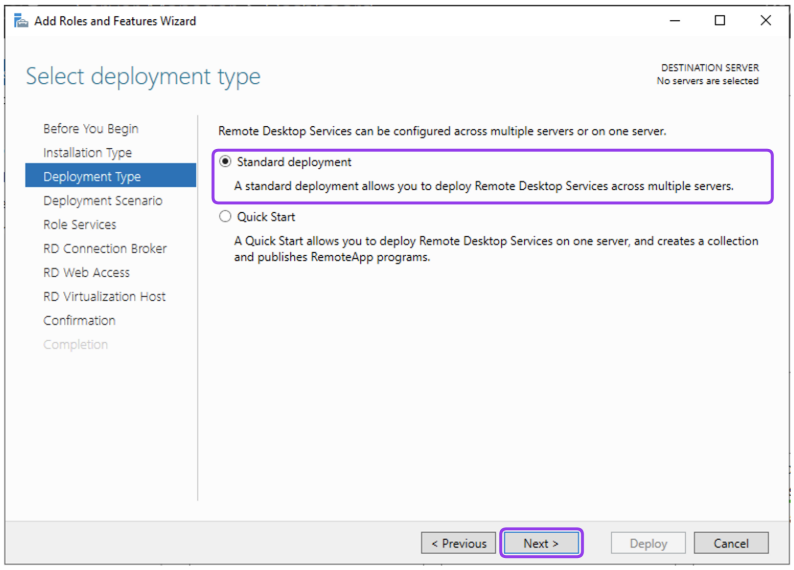
2. Na karcie *Before You Begin* kliknij *Next*, aby kontynuować.



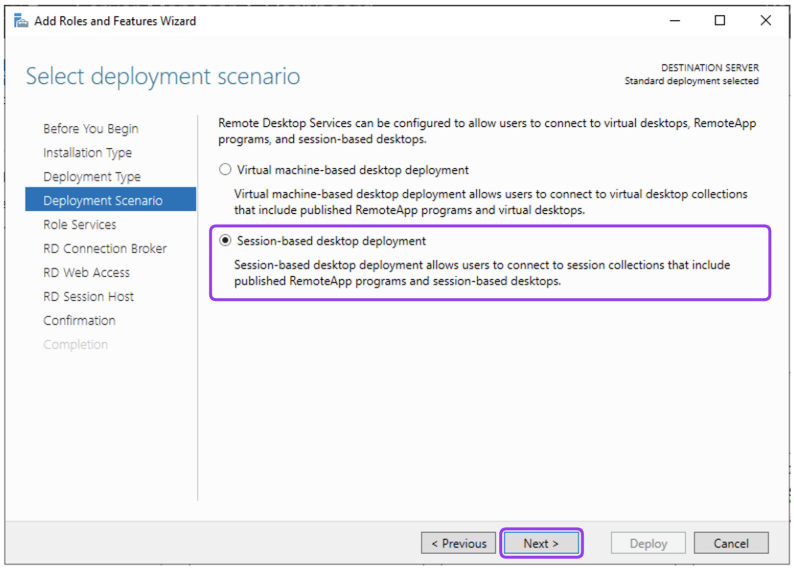
3. Na karcie *Installation Type* wybierz *Remote Desktop Services installation* i kliknij *Next*, aby kontynuować.



4. Na karcie *Deployment Type* wybierz *Standard Deployment*, aby uzyskać bardziej szczegółowe instrukcje dotyczące instalacji usługi Remote Desktop Services. Kliknij *Next*, aby kontynuować.

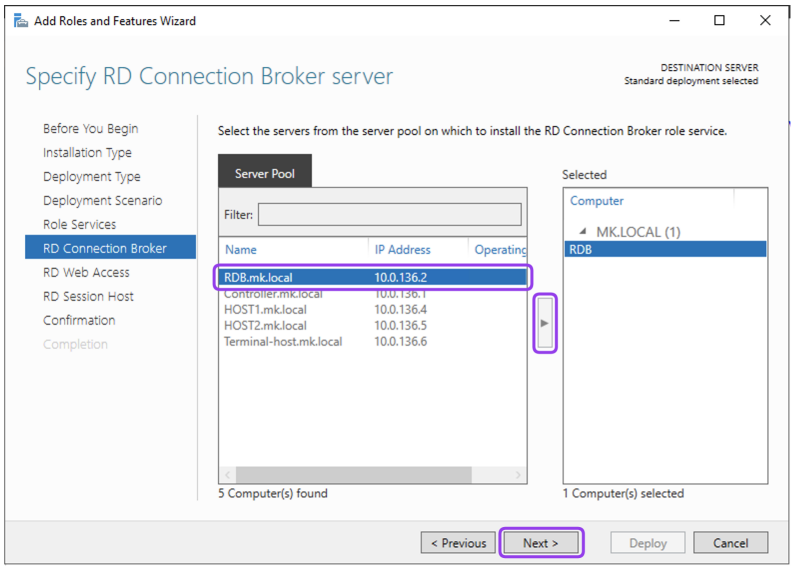


5. Na karcie *Deployment Scenario* wybierz *Session-based desktop deployment*. Kliknij *Next*, aby kontynuować.

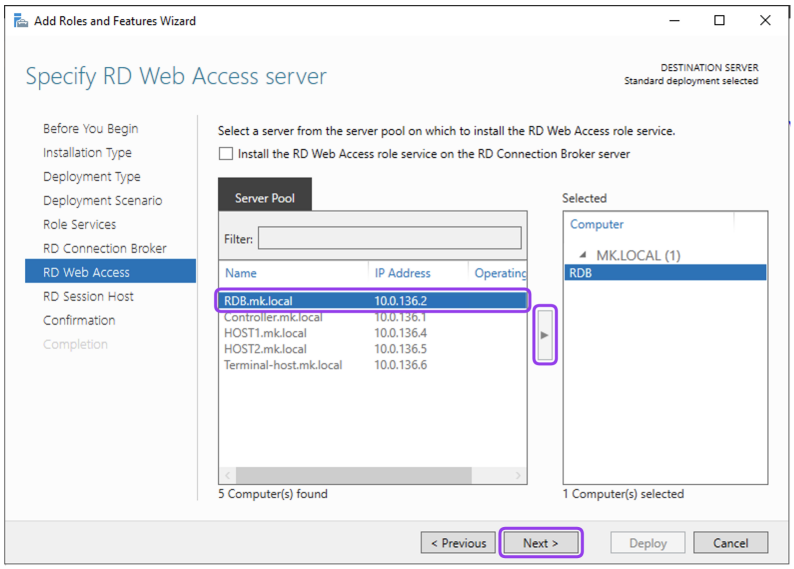


6. Na karcie *Role Services* sprawdź usługi, które zostaną zainstalowane. Kliknij *Next*, aby kontynuować.

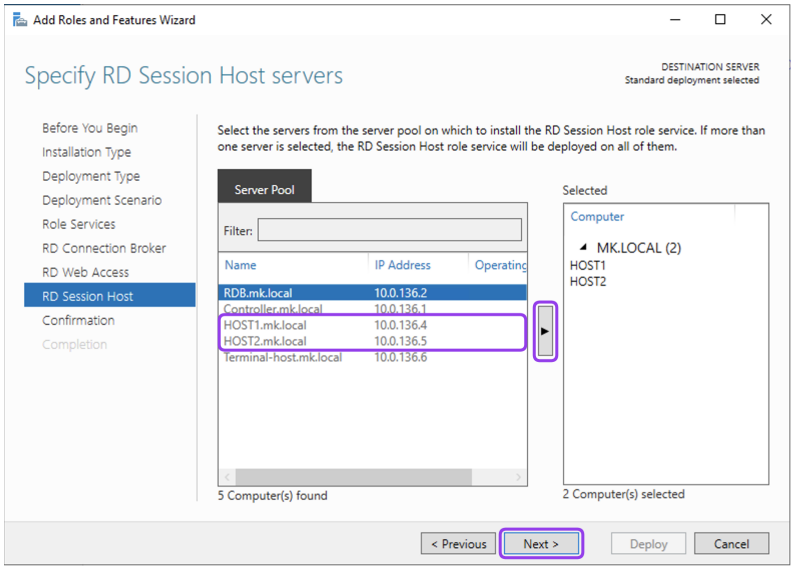
7. Na karcie *RD Connection Broker* wybierz odpowiedni serwer, na którym zostanie zainstalowana usługa roli Brokera. W tym przykładzie wybrano serwer `RDB`. Kliknij *Next*, aby kontynuować.



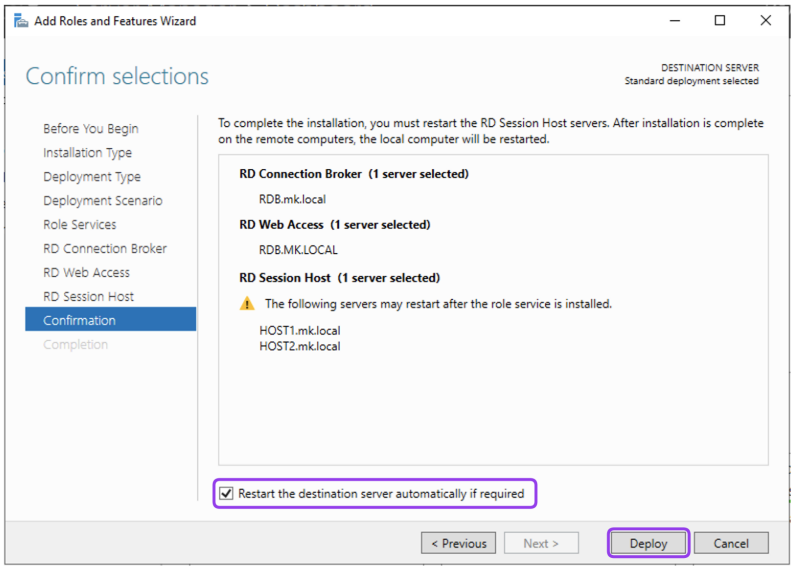
8. Na karcie *RD Web Access* wybierz odpowiedni serwer, na którym chcesz zainstalować rolę usługi RD Web Access. W tym przykładzie wybrano również serwer `RDB`. Kliknij *Next*, aby kontynuować.



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.



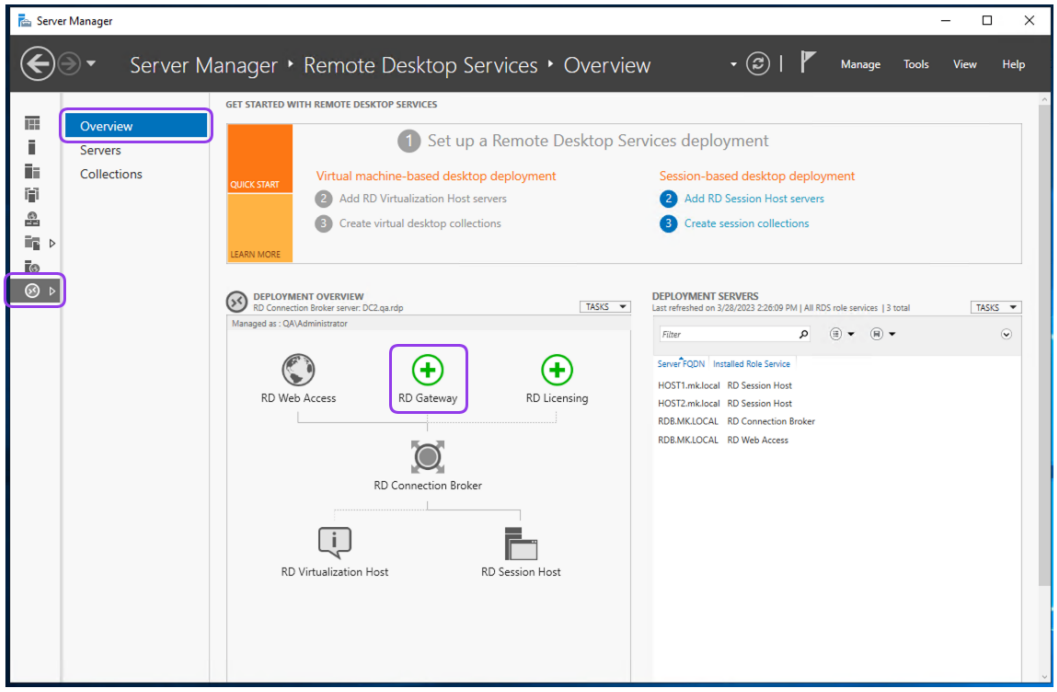
10. Na karcie *Confirmation* zaznacz *Restart the destination server automatically if required*, a następnie kliknij *Deploy*.



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`.

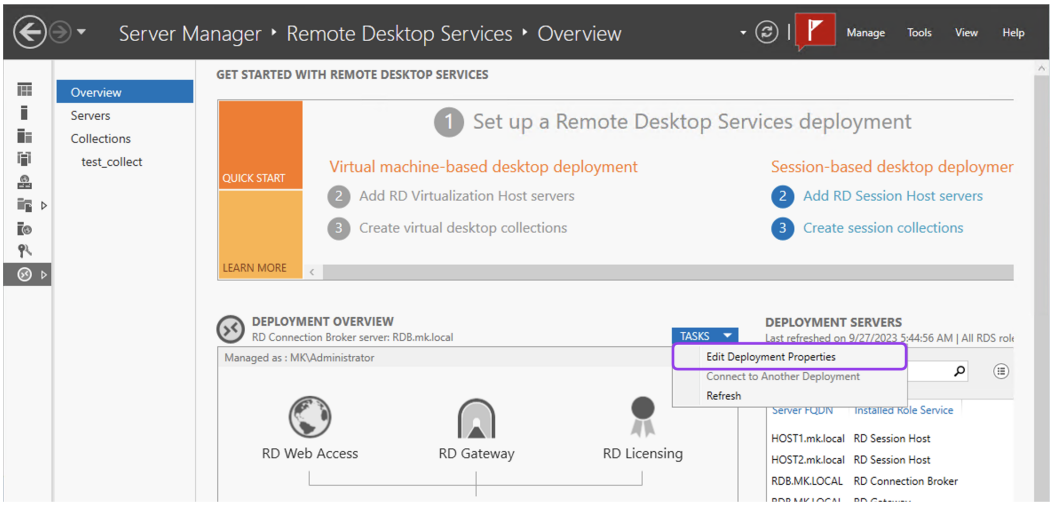


3. Kliknij *Next*.
4. Wprowadź nazwę certyfikatu SSL dla serwera RD Gateway, używając zewnętrznej, w pełni kwalifikowanej nazwy DNS (FQDN) serwera RD Gateway. Przykład, `cert.mk.local`.

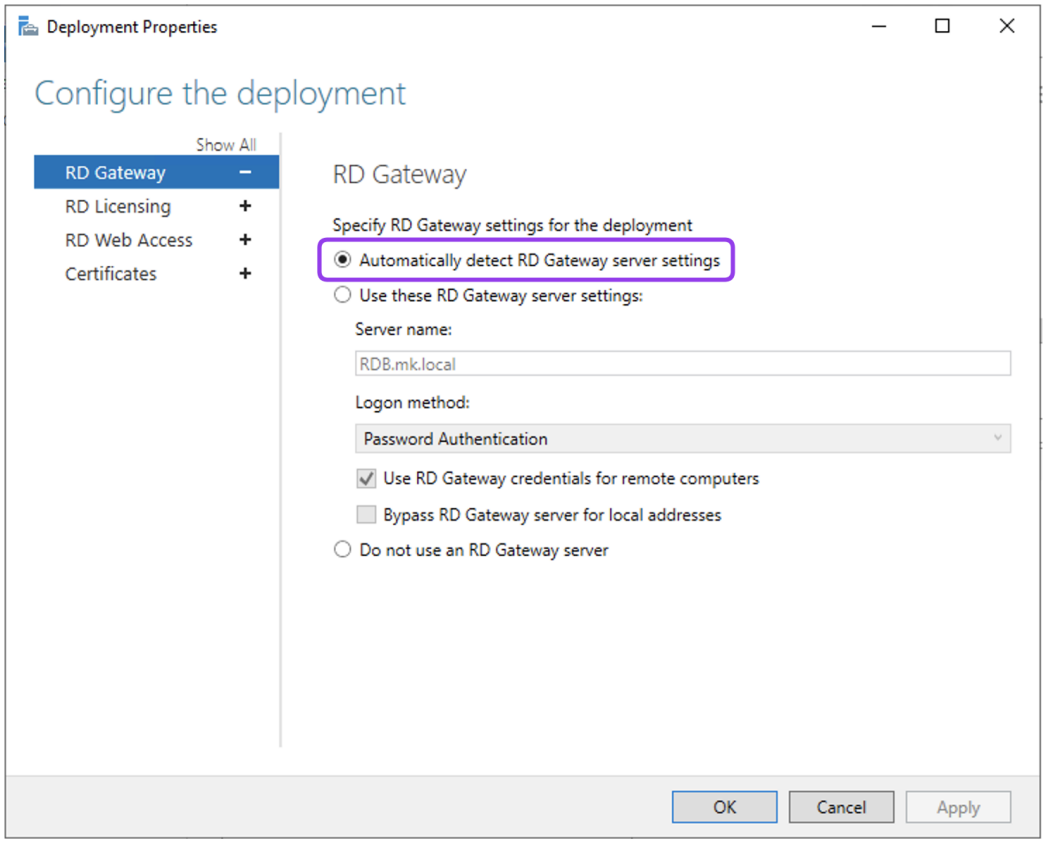
5. Kliknij *Next*, a następnie *Add*.
6. Poczekaj, aż usługa roli zostanie wdrożona, i kliknij *Close*.

Konfiguracja właściwości RD Gateway i RD Licensing:

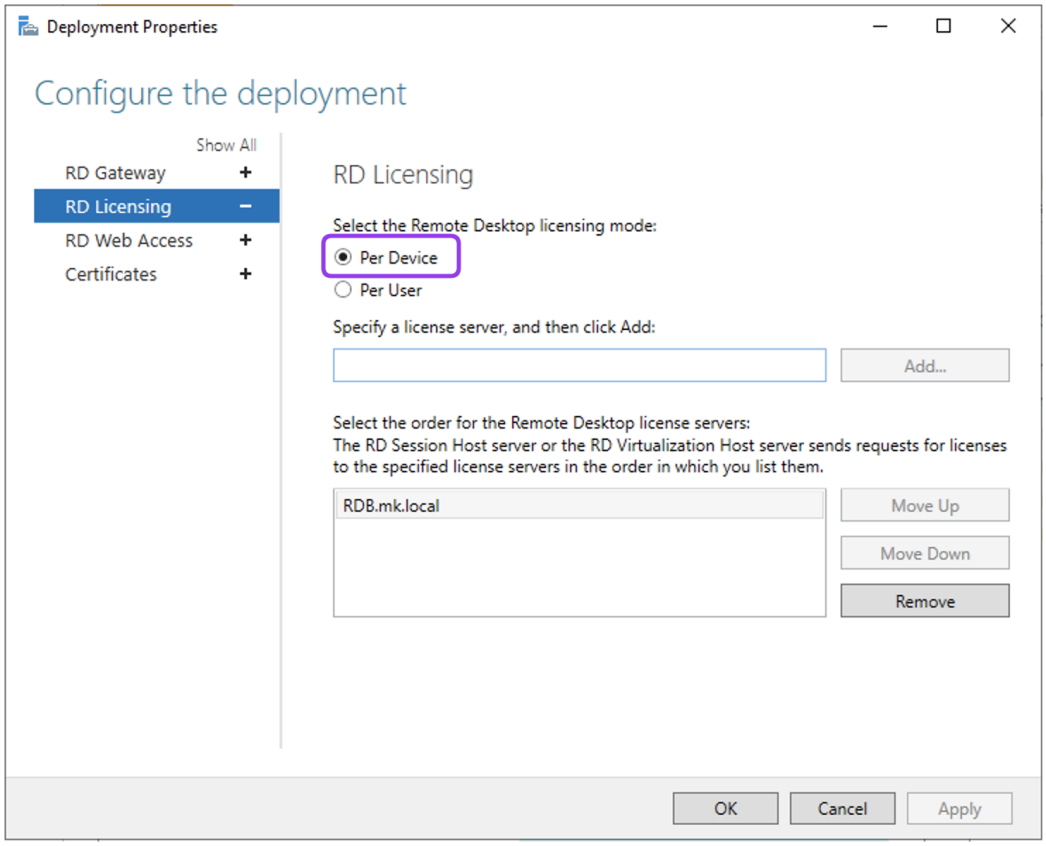
1. Wróć do karty *Overview*, kliknij *Tasks* i z listy rozwijanej wybierz *Edit Deployment Properties*.



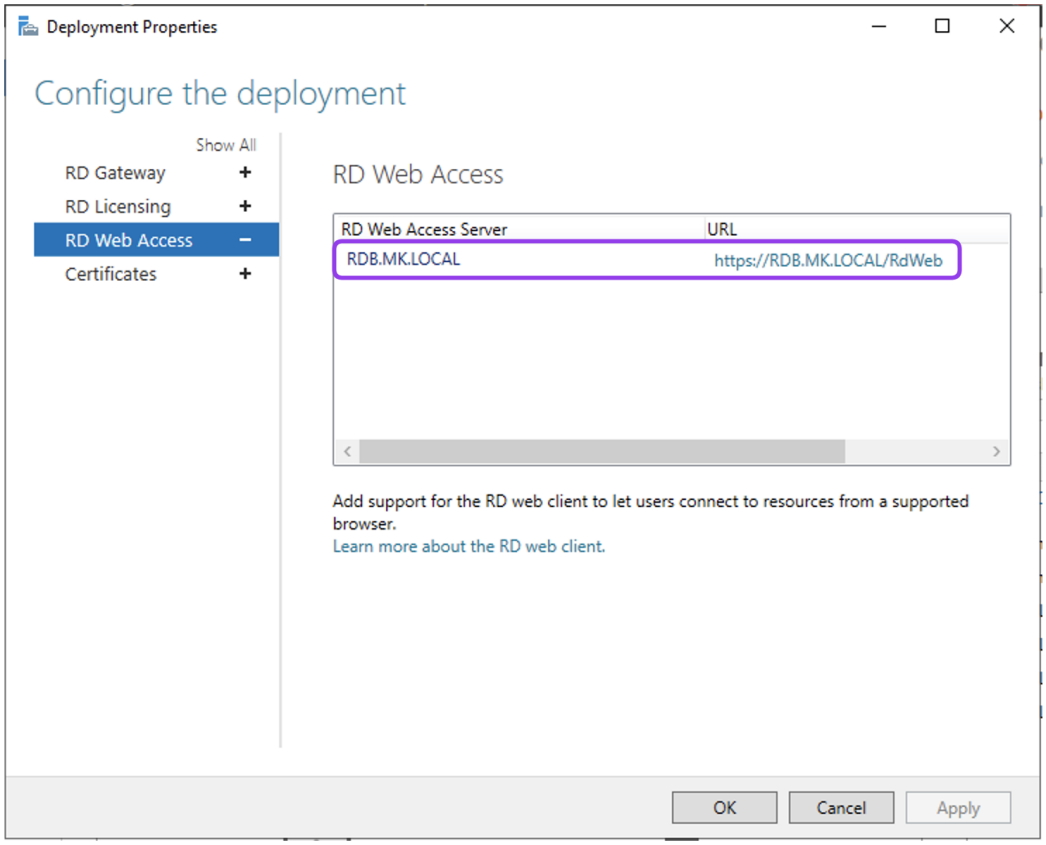
2. Na karcie *RD Gateway* wybierz opcję *Automatically detect RD Gateway server settings* i kliknij *Apply*.



3. Rozwiń kartę *RD Licensing* i wybierz *Per Device*. Kliknij *Apply*.

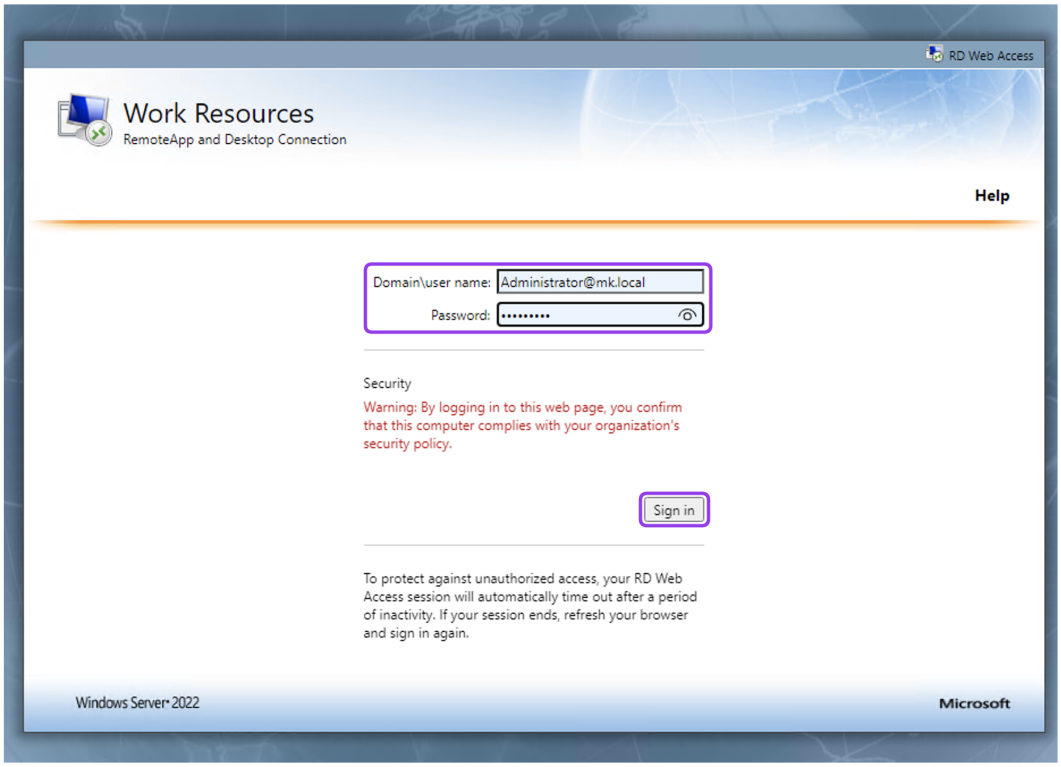


4. Rozwiń kartę «RD Web Access», aby sprawdzić adres URL dla RD Web Access IIS. Domyślnie jest zainstalowana pod adresem `/RdWeb`.



5. Kliknij na wyświetlony adres URL, aby zweryfikować logowanie do RD Web Access za pomocą konta administratora.

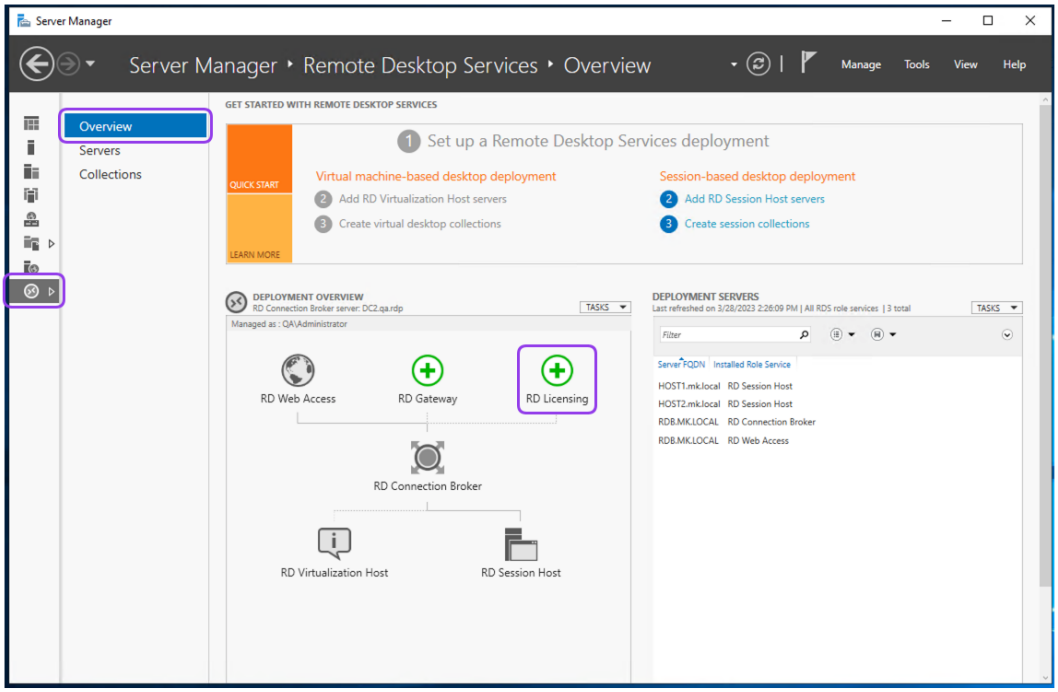
> **Uwaga**
>
> Podczas logowania użyj domeny w polu *nazwa użytkownika*. Na przykład, `Administrator@mk.local`.



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:

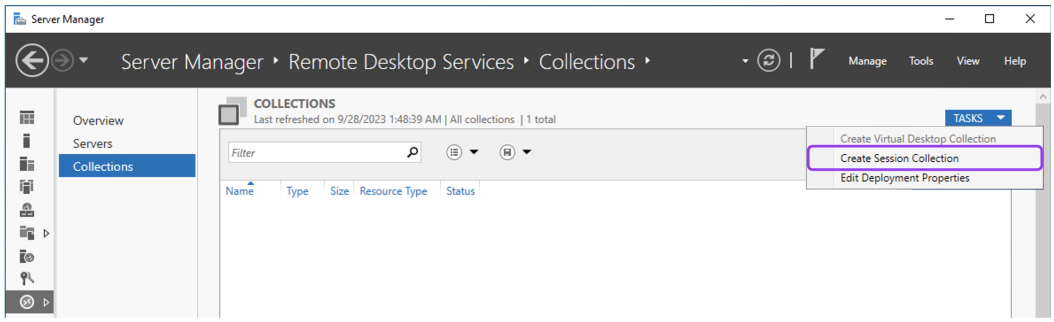
1. Kliknij przycisk *+ RD Licensing* na karcie *Overview* w sekcji *Remote Desktop Services*.



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.

> **Uwaga**
>
> Ta nazwa będzie wyświetlana pod ikoną w interfejsie Web Access.

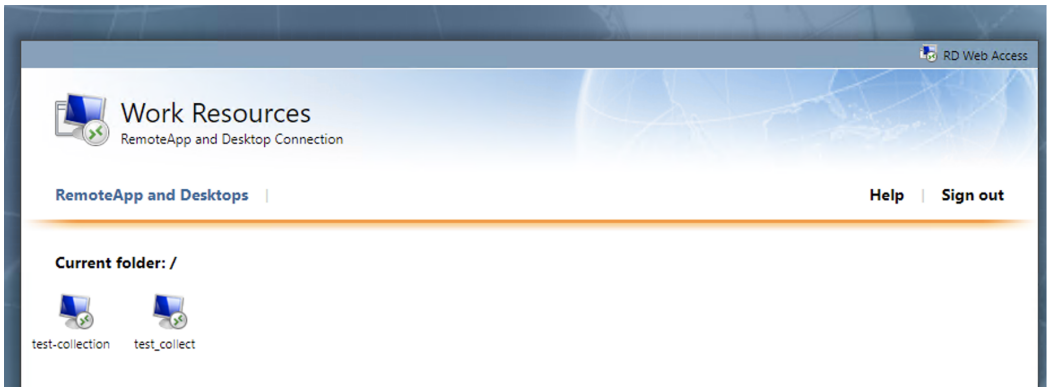
4. Na karcie *RD Session Host* wybierz serwery do dodania do tej kolekcji. W tym przykładzie wybrano serwery `HOST1` i `HOST2`.
5. Na karcie *User Groups* zdefiniuj grupy użytkowników. Możesz zaakceptować domyślne grupy użytkowników lub dodać jedną lub więcej grup użytkowników

uprawnionych do łączenia się za pomocą RDP z serwerami.

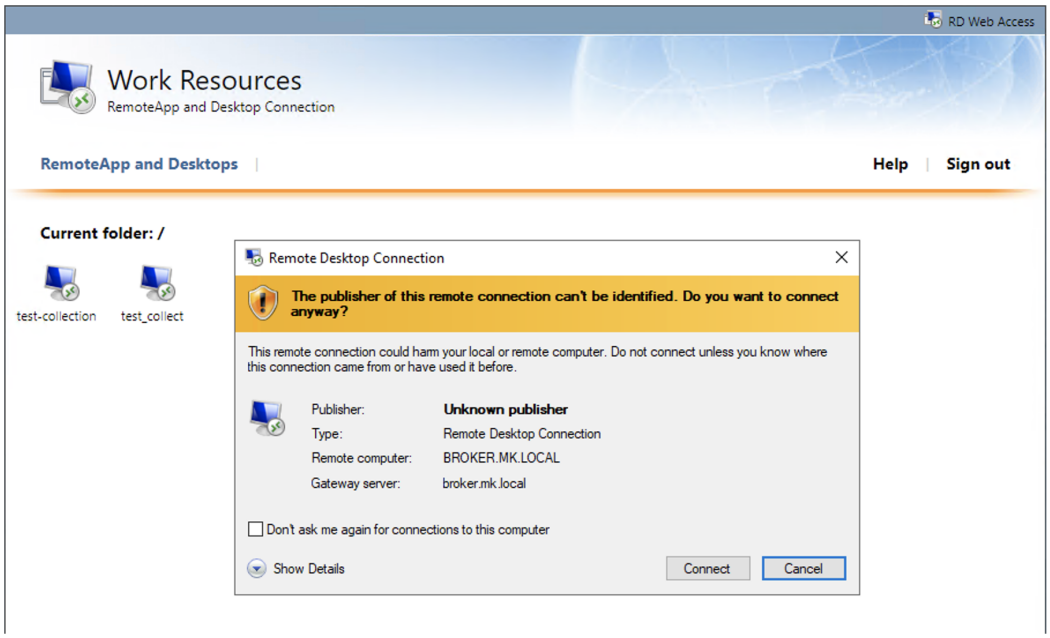
6. Na karcie *User Profile Disks* wybierz opcję *Enable User Profile Disks* i określ ustawienia, jeśli jest to konieczne. Możesz również pozostawić tę opcję wyłączoną.
7. Na karcie *Confirmation* przejrzyj wszystkie informacje, a następnie kliknij «Create».
8. Poczekaj, aż kolekcja zostanie utworzona. Kliknij *Close*.

Test połączenia:

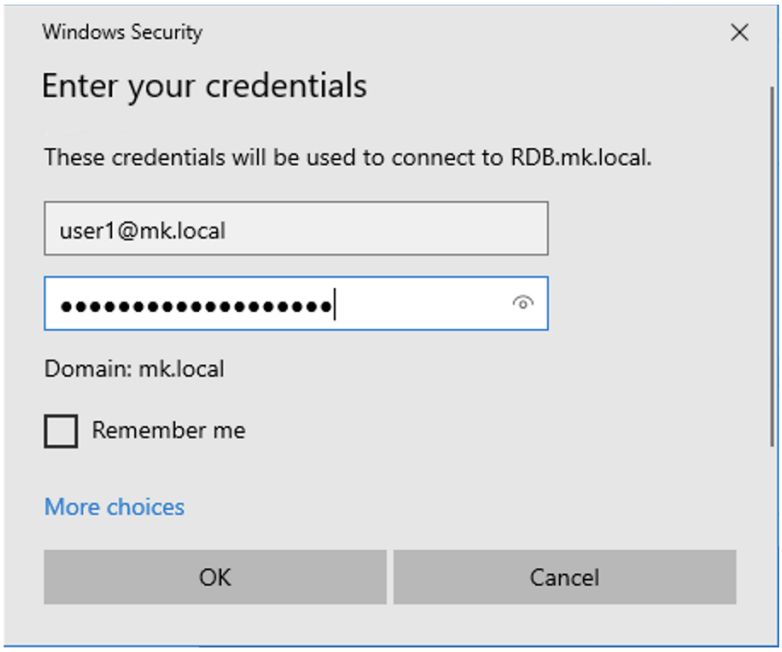
1. Otwórz zapisany wcześniej adres URL dla RD Web Access (np. `https://rdb.mk.local/RDWeb/`).
2. Wprowadź prawidłową nazwę użytkownika i hasło, a następnie kliknij *Sign in*. Możesz użyć konta administratora domeny do logowania, na przykład `Administrator@mk.local`.
3. Po zalogowaniu zostanie przedstawiona 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.



Uwaga

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.

Tematy pokrewne:

- *RDP w trybie bastionu*
- *Uwierzytelnienie*
- *Integration with CERB server*

20.3.2 Konfiguracja Fudo Enterprise - scenariusz bastion (zalecany)

Scenariusz Bastion jest zalecaną konfiguracją dla funkcji RDS. W tym scenariuszu należy:

- utworzyć użytkowników za pomocą funkcji RDS, aby odpowiadali użytkownikom z Active Directory,
- dodać wszystkie serwery zawarte w kolekcji RDS,
- skonfigurować konto do uwierzytelniania na serwerze,
- ustawić pojedynczy listener w trybie bastion, sparowany z tym kontem.

Uwaga

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 En-

terprise, 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 zewnętrzne uwierzytelnianie*.
4. Wpisz unikalną nazwę (np. `ActiveDirectory01`).
5. Ustaw *Adres źródłowy* na *Dowolny*.
6. W sekcji *Ogólne* wybierz *Active Directory*.
7. W polu *Host* podaj adres IP kontrolera domeny (np. `10.0.136.1`).
8. Pozostaw domyślny numer portu: `389`.
9. Podaj nazwę domeny, która będzie używana do uwierzytelnienia użytkowników w Active Directory (np. `mk.local`).
10. W sekcji *Poświadczenia* 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`.

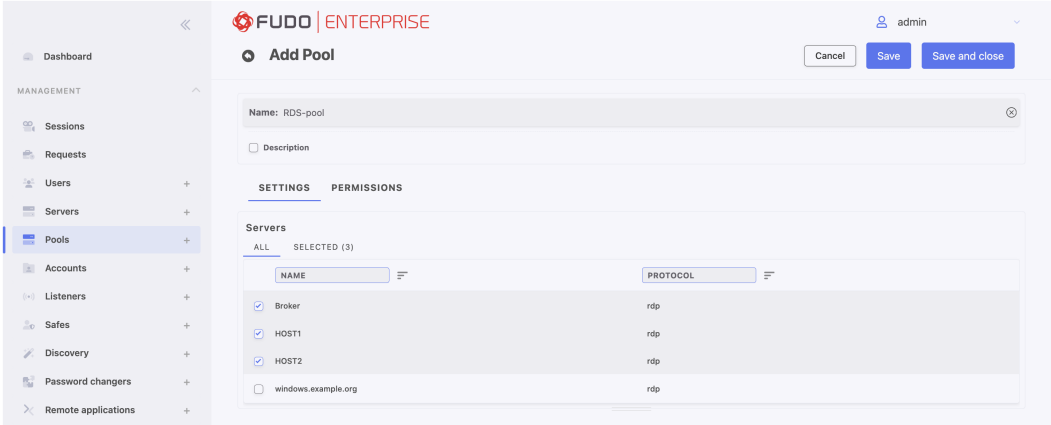
5. Zaznacz opcje *TLS włączony* i *NLA włączony*.
6. W sekcji *Miejsce przeznaczenia* wybierz `IPv4` i wprowadź adres IP serwera wybranego podczas konfiguracji RDS dla roli RD Broker (w naszym przykładzie serwer `RDB` z adresem IP `10.0.136.2`).
7. Kliknij *Zapisz i zamknij*.

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 *Miejsce przeznaczenia* 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 włączając serwer o funkcji brokera (np. `HOST1, HOST2, BROKER`).
4. W sekcji *UPRAWNIENIA* dodaj użytkowników uprawnionych do zarządzania tym obiektem (np. `user1`).



6. Kliknij *Zapisz i wyjdź*.

Konfiguracja konta:

1. Wybierz *Zarządzanie* > *Konta* i kliknij + *Dodaj konto*.
2. Zdefiniuj nazwę obiektu (np. `user1`).

3. W sekcji *Typ* wybierz *FORWARD*.
4. W sekcji *Cel* wybierz *Pula* i z listy rozwijanej wybierz pulę utworzoną w poprzednim kroku (np. `RDS-pula`), aby przypisać utworzone konto do tej puli serwerów.
5. Wybierz opcję *Przekazuj domenę* aby dołączyć nazwę domeny w ciągu identyfikującym użytkownika.
6. W sekcji *Poświadczenia* wpisz nazwę domeny (np. `mk.local`).
7. 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 `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*.

Konfiguracja sejfu:

1. Wybierz *Zarządzanie* > *Sejfy*, a następnie kliknij + *Dodaj sejf*.
2. Wprowadź nazwę obiektu.
3. 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 (np. `user1`).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.
4. Wybierz zakładkę *Konta*, aby dodać konta dostępne przez ten sejf.
   - Kliknij *Zarządzaj kontami*.
   - Zaznacz pole wyboru przed nazwami kont, aby je dodać (np. `user1`).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.
   - Wybierz żądane konto i kliknij *Zarządzaj gniazdami nasłuchiwania*, aby przypisać je do kont (np.``rdp-broker-bastion``).

- Kliknij *Zapisz*, aby zamknąć okno dialogowe.

5. Kliknij *Zapisz i zamknij*, aby zapisać konfigurację sejfu.

1. Wybierz Zarządzanie > Sejfy, a następnie kliknij Dodaj sejf.
2. Wprowadź nazwę obiektu.
3. 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 (np. `user1`).
    - Kliknij Zapisz, aby zamknąć okno dialogowe.
4. Wybierz zakładkę **Konta**, aby dodać konta dostępne przez ten sejf.
    - Kliknij Zarządzaj kontami.
    - Zaznacz pole wyboru przed nazwą konta, aby je dodać (np. `user1`).
    - Kliknij Zapisz, aby zamknąć okno dialogowe.
    - Wybierz dodane konto i kliknij Zarządzaj gniazdami nasłuchiwania, aby przypisać je do konta (np.``rdp-broker-bastion``).
    - Kliknij Zapisz, aby zamknąć okno dialogowe.
5. Kliknij Zapisz i zamknij, aby zapisać konfigurację sejfu.

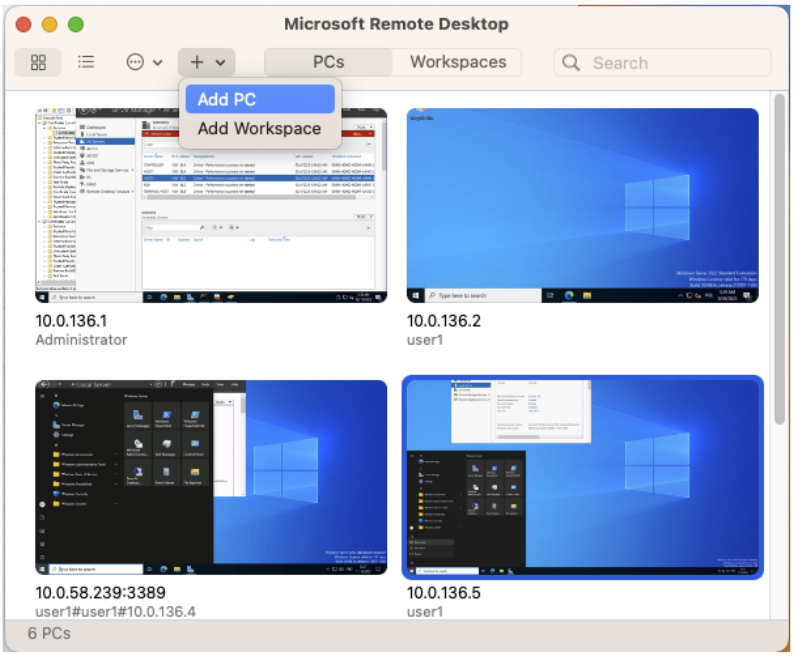
Nawiązanie sesji przez Portal Użytkownika Fudo:

> **Ostrzeżenie**
>
> Podczas nawiązywania połączeń za pomocą Remote Desktop Services zalecane jest korzystanie z opcji *Native client*. *Web client* nie obsługuje tego typu połączeń.

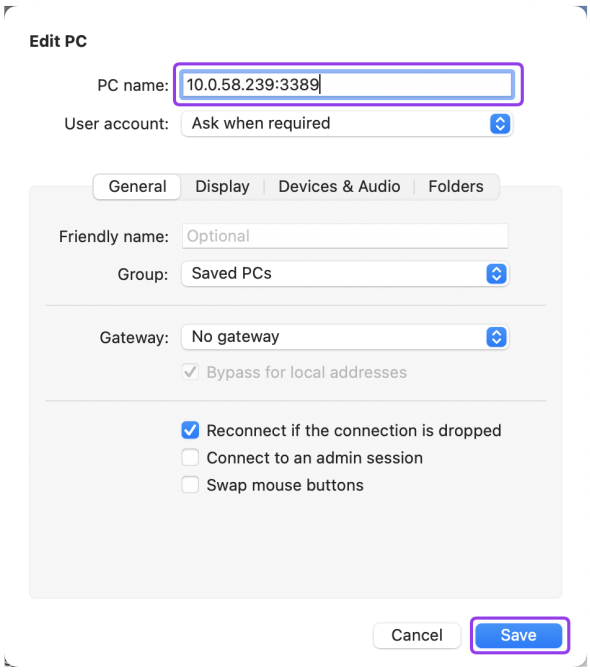
1. Zaloguj się do «Portalu Użytkownika» Fudo Enterprise używając `user1` jako nazwy użytkownika i hasła skonfigurowanego dla tego użytkownika w Active Directory.
2. Najedź kursorem na nazwę konta `user1`, wybierz *Native client* i kliknij *Połącz* w celu pobrania pliku konfiguracyjnego RDP.
3. Otwórz 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*.

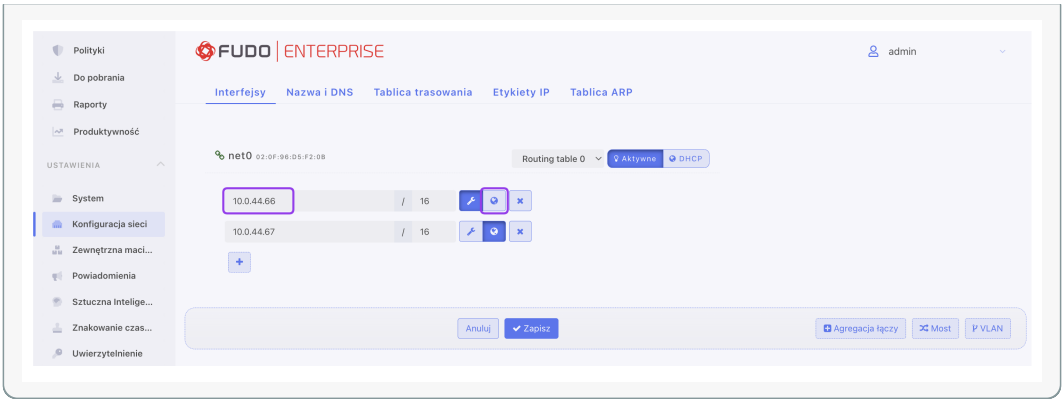


4. W polu *Nazwa komputera* wprowadź adres IP Portalu Użytkownika Fudo Enterprise wraz z numerem portu i kliknij *Dodaj*.



Uwaga

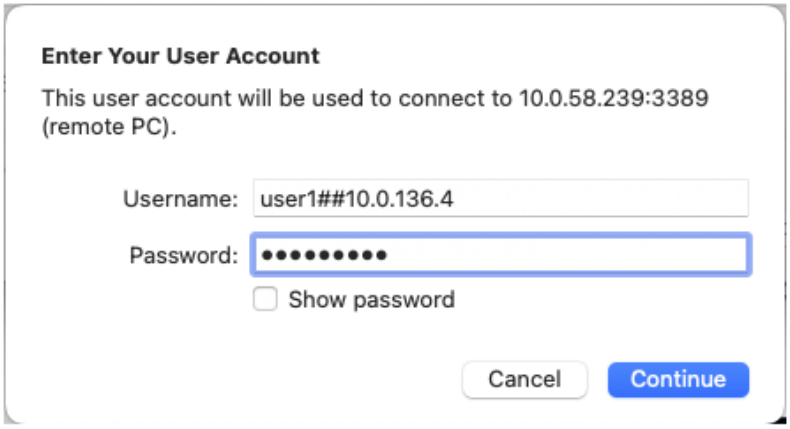
Adres IP Portalu Użytkownika znajdziesz w zakładce *Ustawienia* > *Konfiguracja sieci*.



5. Połącz się z dodanym komputerem, podając w polu *Nazwa użytkownika* ciąg logowania dla połączeń bastion oraz hasło w polu *Hasło*.

Uwaga

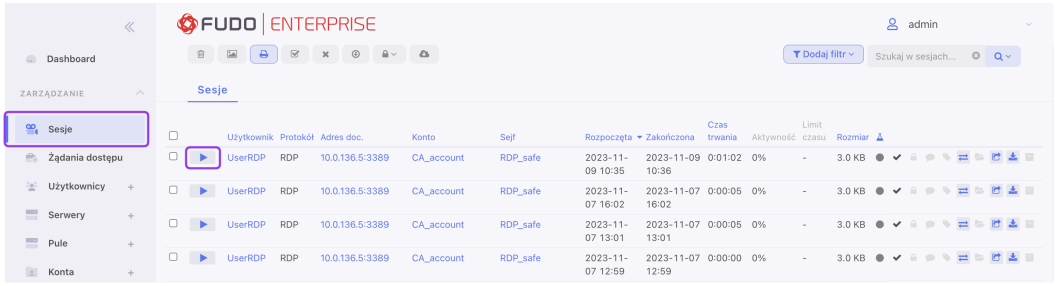
- Użyj następującego wzoru dla ciągu logowania bastion: nazwa użytkownika # login konta na docelowym serwerze # `adres serwera docelowego` (np. `user1#user1#10.0.136.4`).
- Możesz podać adres IP dowolnego serwera z kolekcji RDS jako `adres serwera docelowego` w ciągu logowania, a broker przekieruje połączenie zgodnie z zasadami RDS.
- Można pominąć login konta, jeśli jest taki sam jak nazwa użytkownika, np. `user1##10.0.136.4`

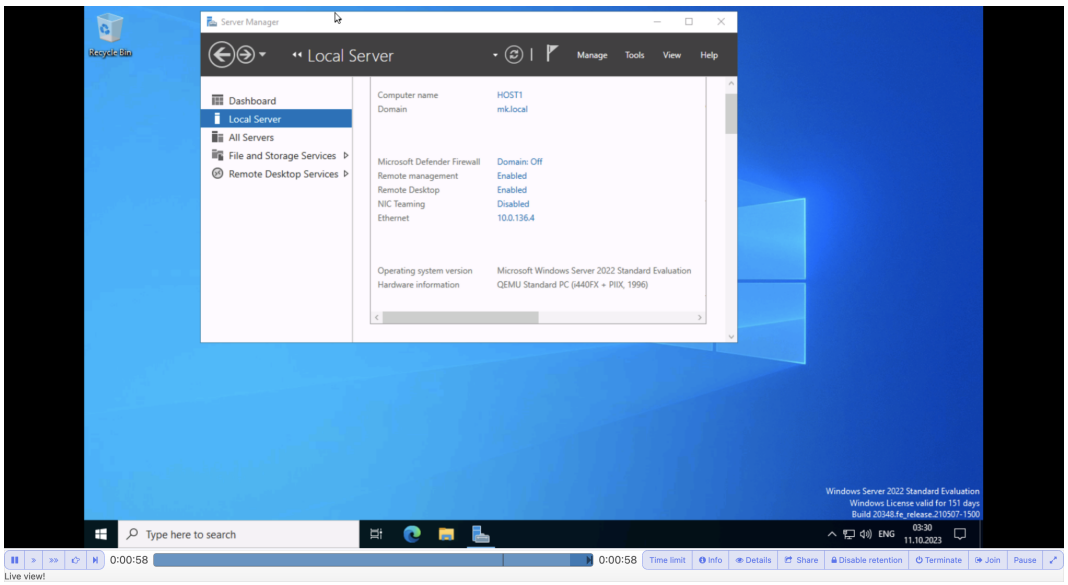


6. Klient RDP nawiąże połączenie z jednym z serwerów z kolekcji RDS.

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:

- *Konfiguracja Fudo Enterprise - scenariusz bastion (zalecany)*
- *RDP w trybie bastionu*
- *Uwierzytelnienie*
- *Konfiguracja ustawień sieciowych*

20.3.3 Konfiguracja Fudo Enterprise - scenariusz proxy

Scenariusz proxy dla RDS wymaga więcej ręcznej konfiguracji w Fudo Enterprise w porównaniu do scenariusza bastion, ale oferuje uproszczoną metodę uwierzytelniania dla użytkownika. Każdy serwer w kolekcji RDS musi mieć w Fudo Enterprise skonfigurowane swoje własne gniazdo nasłuchiwania proxy, z przypisanym dedykowanym adresem IP i portem 3389.

W tym scenariuszu należy:

- utworzyć użytkowników za pomocą funkcji RDS, aby ich nazwy odpowiadały użytkownikom z Active Directory,
- dodać wszystkie serwery zawarte w kolekcji RDS,
- skonfigurować konto dla każdego serwera,
- utworzyć gniazdo nasłuchiwania w trybie proxy z indywidualnym adresem IP dla każdego serwera.

Uwaga

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 zewnętrzne uwierzytelnianie*.
4. Wpisz unikalną nazwę (np. `ActiveDirectory01`).
5. Ustaw *Adres źródłowy* na *Dowolny*.
6. W sekcji *Ogólne* wybierz *Active Directory*.
7. W polu *Host* podaj adres IP kontrolera domeny (np. `10.0.136.1`).
8. Pozostaw domyślny numer portu: `389`.
9. Podaj nazwę domeny, która będzie używana do uwierzytelnienia użytkowników w Active Directory (np. `mk.local`).
10. W sekcji *Poświadczenia* 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 *Miejsce przeznaczenia* 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 *Miejsce przeznaczenia* 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 kont:

1. Wybierz *Zarządzanie* > *Konta* i kliknij + *Dodaj konto*.
2. Zdefiniuj nazwę obiektu (np. `rds-host1-forward`).
3. W sekcji *Typ* wybierz *FORWARD*.
4. W sekcji *Cel* kliknij *Serwer*, a następnie z listy rozwijanej wybierz jeden z serwerów utworzonych w poprzednich krokach (np. `HOST1`), aby przypisać do niego utworzone konto.
5. Kliknij *Zapisz*.
6. Powtórz wszystkie powyższe kroki, aby utworzyć konta, które zostaną przydzielone dla pozostałych serwerów (np. `rds-host2-forward`, `rds-broker-forward`).

Konfiguracja gniazda nasłuchiwania:

1. Wybierz *Zarządzanie* > *Gniazda nasłuchiwania* i kliknij + *Dodaj gniazdo nasłuchiwania*.
2. Wpisz unikalną nazwę gniazda nasłuchiwania (np.``rdp-proxy-01``).
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 `proxy`.
8. Ustaw lokalny adres na indywidualny adres IP wybrany z listy (np. `10.0.58.238`), i port `3389`.

> **Uwaga**
>
> Aby dowiedzieć się jak dodawać nowe adresy IP, zapoznaj się z rozdziałem *Konfiguracja ustawień sieciowych*.

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*.
11. Powtórz wszystkie powyższe kroki, aby utworzyć gniazda nasłuchiwania dla pozostałych serwerów w kolekcji (`HOST2` i `BROKER`).

Konfiguracja sejfu:

1. Wybierz *Zarządzanie* > *Sejfy*, a następnie kliknij + *Dodaj sejf*.
2. Wprowadź nazwę obiektu (np. `rdp-safe`).
3. 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 (np. `user1`).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.
4. Wybierz zakładkę *Konta*, aby dodać konta dostępne przez ten sejf.
   - Kliknij *Zarządzaj kontami*.
   - Zaznacz pole wyboru przed nazwami kont, które zostały utworzone wcześniej, aby je dodać (np. `rds-host1-forward`, `rds-host2-forward`, `rds-broker-forward`).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.
   - Wybierz kolejno konto i kliknij *Zarządzaj gniazdami nasłuchiwania*, aby do każdego konta przypisać indywidualne gniazdo (np.``rdp-proxy-01, rdp-proxy-02, rdp-proxy-03``).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.
5. Kliknij *Zapisz i zamknij*, aby zapisać konfigurację sejfu.

1. Wybierz Zarządzanie > Sejfy, a następnie kliknij Dodaj sejf.
2. Wprowadź nazwę obiektu.

3. 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 (np. `user1`).
    - Kliknij Zapisz, aby zamknąć okno dialogowe.
4. Wybierz zakładkę **Konta**, aby dodać konta dostępne przez ten sejf.
    - Kliknij Zarządzaj kontami.
    - Zaznacz pole wyboru przed nazwami kont, które zostały utworzone wcześniej, aby je dodać (np. `rds-host1-forward`, `rds-host2-forward`, `rds-broker-forward`).
    - Kliknij Zapisz, aby zamknąć okno dialogowe.
    - Wybierz kolejno konto i kliknij *Zarządzaj gniazdami nasłuchiwania*, aby do każdego konta przypisać indywidualne gniazdo (np.``rdp-proxy-01, rdp-proxy-02, rdp-proxy-03``).
    - Kliknij Zapisz, aby zamknąć okno dialogowe.
5. Kliknij Zapisz i zamknij, aby zapisać konfigurację sejfu.

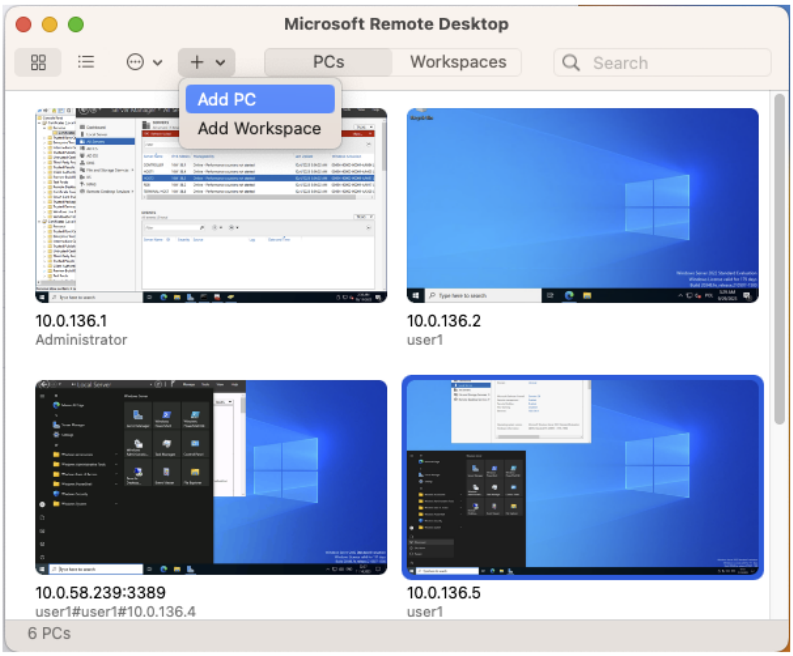
Nawiązanie sesji przez Portal Użytkownika Fudo:

> **Ostrzeżenie**
>
> Podczas nawiązywania połączeń za pomocą Remote Desktop Services zalecane jest korzystanie z opcji *Native client*. *Web client* nie obsługuje tego typu połączeń.

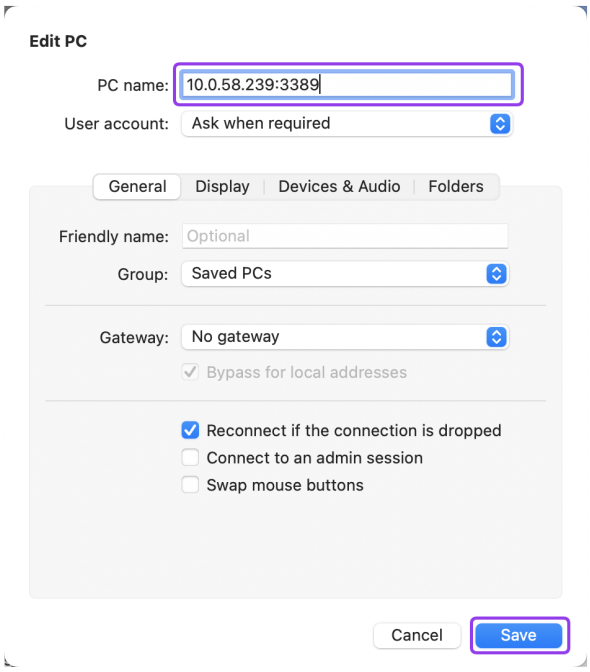
1. Zaloguj się do «Portalu Użytkownika» Fudo Enterprise używając `user1` jako nazwy użytkownika i hasła skonfigurowanego dla tego użytkownika w Active Directory.
2. Najedź kursorem na nazwę wybranego konta (np. `rds-host1-forward`), wybierz *Native client* i kliknij *Połącz* w celu pobrania pliku konfiguracyjnego 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*.

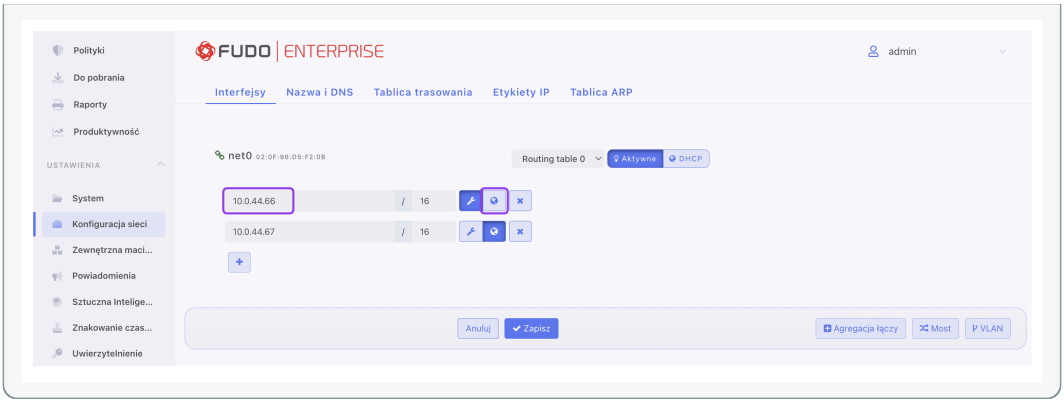


4. W polu *Nazwa komputera* wprowadź adres IP Portalu Użytkownika Fudo Enterprise wraz z numerem portu i kliknij *Dodaj*.



Uwaga

Adres IP Portalu Użytkownika znajdziesz w zakładce *Ustawienia* > *Konfiguracja sieci*.



5. Połącz się z dodanym komputerem, podając login i hasło użytkownika `user1` ustawione w środowisku Active Directory (zgodnie z metodą wybraną podczas tworzenia użytkownika w Fudo Enterprise).

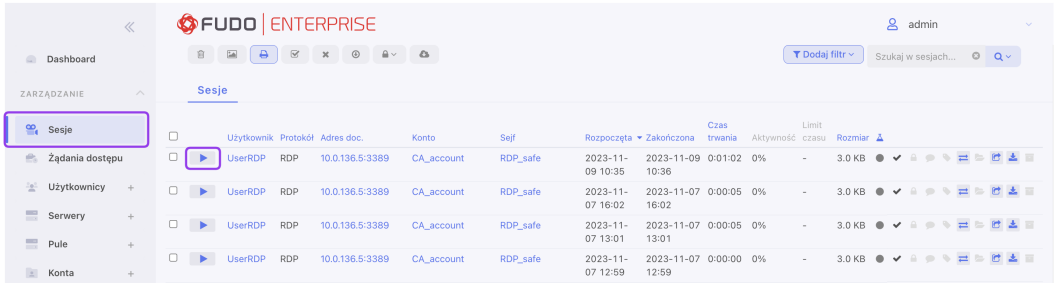
6. Klient RDP nawiąże połączenie z jednym z serwerów z kolekcji RDS.

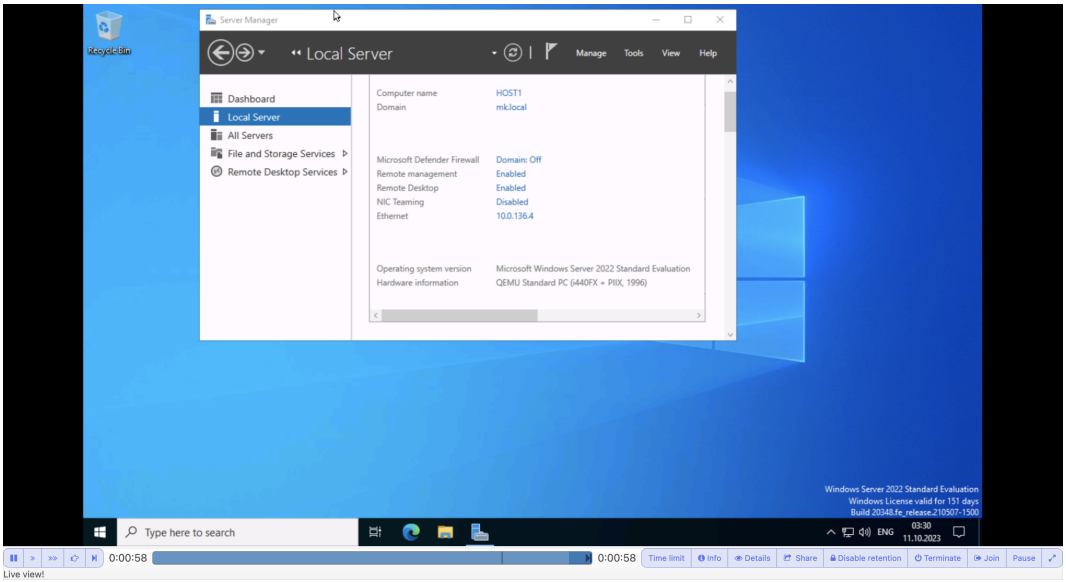
Wyświetlanie aktywnej sesji w Panelu Administracyjnym Fudo Enterprise:

1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise.

2. Wybierz *Zarządzanie* > *Sesje.*

3. Znajdź żądaną sesję i kliknij ikonę odtwarzania obok niej.





Tematy pokrewne:

- *Konfiguracja Fudo Enterprise - scenariusz bastion (zalecany)*

- *Uwierzytelnienie*
- *Konfiguracja ustawień sieciowych*

20.4 Niestandardowa nazwa hosta RDP w tytule sesji

Uwaga

Pamiętaj, że jest to ogólny przewodnik, a szczegóły konfiguracji mogą się różnić w zależności od konfiguracji Windows Server. Dokładne kroki konfiguracji znajdziesz w dokumentacji Windows Server.

Ten przypadek użycia opisuje, jak skonfigurować niestandardową nazwę hosta wyświetlaną na pasku tytułu klienta RDP dla sesji uruchamianych z Portalu Użytkownika przy użyciu opcji *Klient natywny*.

Ta konfiguracja umożliwia czytelną i przyjazną dla użytkownika identyfikację sesji RDP dzięki zachowaniu niestandardowych nazw hostów przez Fudo Enterprise.

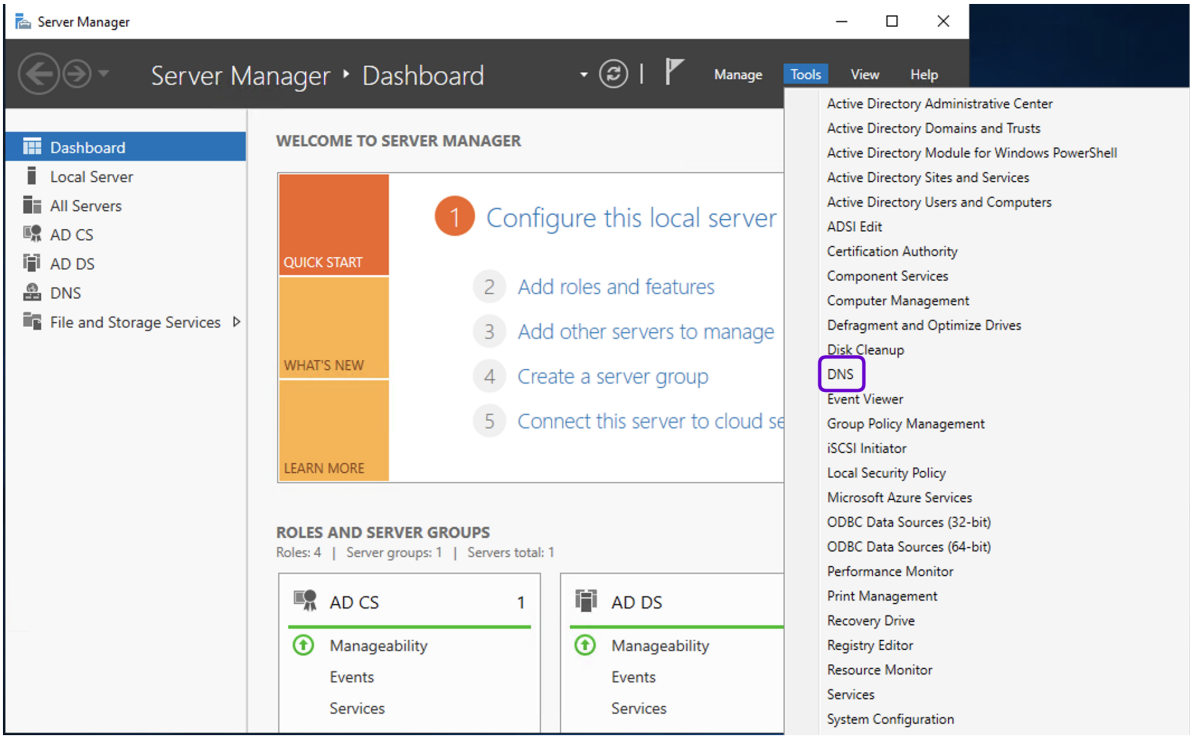
Ostrzeżenie

Rekord wildcard musi już istnieć po stronie DNS. Fudo Enterprise nie generuje rekordów DNS.

20.4.1 Konfiguracja DNS w Menedżerze DNS systemu Windows

Tworzenie subdomeny do użycia z wildcardem:

1. Otwórz aplikację *Server Manager*.
2. Kliknij przycisk *Tools* w prawym górnym rogu okna, aby rozwinąć listę menu, a następnie wybierz *DNS*.



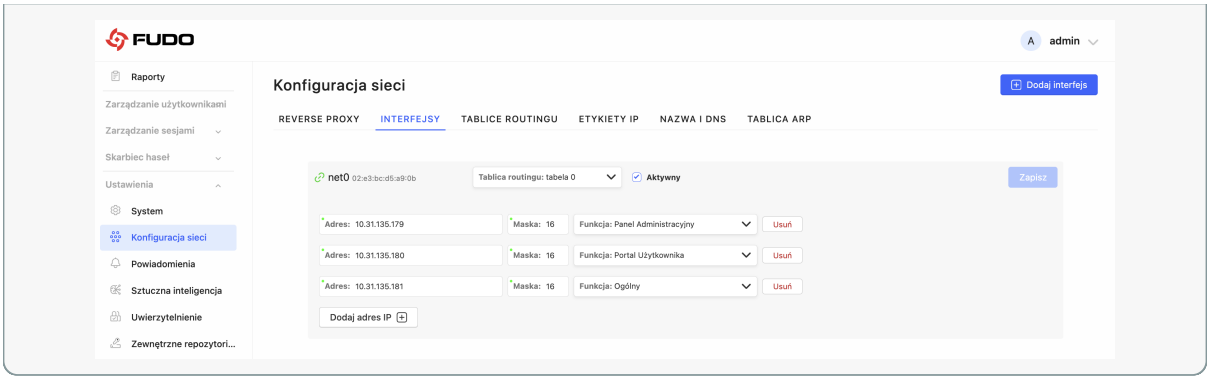
3. Przejdź do *Forward Lookup Zones*, kliknij prawym przyciskiem myszy nazwę domeny (na przykład `main.lab`) i wybierz *New Domain*.
4. Podaj *New DNS domain name* (na przykład `dev`).
5. Kliknij *OK*.

Tworzenie rekordu wildcard A:

1. Kliknij prawym przyciskiem myszy dodaną nazwę strefy (`dev`) i wybierz *New Host (A or AAAA)*.
2. W polu *Name* wpisz gwiazdkę (`*`).
3. W polu *IP address* wpisz adres Portalu Użytkownika Fudo Enterprise (na przykład `10.31.135.180`).
4. Opcjonalnie możesz zaznaczyć opcję *Create associated pointer (PTR) record*.
5. Kliknij *Add Host*.

Uwaga

Adres przypisany do Portalu Użytkownika możesz sprawdzić w *Settings* > *Network Configuration* > *Interfaces*. Upewnij się, że interfejs jest *Active*.



20.4.2 Konfiguracja Fudo Enterprise

1. Wybierz *Management* > *Gniazda nasłuchiwania* i kliknij nazwę wybranego *gniazda nasłuchiwania RDP*, aby je edytować.
2. W konfiguracji gniazda nasłuchiwania znajdź pole *Domena konfiguracji RDP*.
3. Wprowadź domenę, która ma zostać dodana do wygenerowanej nazwy hosta (na przykład `jdoe.dev.main.lab`).
4. Kliknij *Save*.

Uwaga

- Gdy pole *Domena konfiguracji RDP* jest skonfigurowane, gniazdo nasłuchiwania używa nazw hostów z określonej domeny. Pozostaw to pole puste, jeśli nie chcesz używać niestandardowych nazw hostów dla gniazda nasłuchiwania.
- Każde gniazdo nasłuchiwania RDP może używać innej domeny niestandardowej.

20.4.3 Uruchamianie połączenia RDP

1. Zaloguj się do Portalu Użytkownika.
2. Przejdź do *Resources*.
3. Znajdź wybrane konto RDP i serwer, a następnie najedź kursorem, aby wyświetlić więcej opcji.
4. Wybierz przycisk *Native client*.
5. Wybierz gniazdo nasłuchiwania, przez które chcesz się połączyć.
6. Kliknij *Connect*.
7. *Google Chrome* automatycznie pobierze wygenerowany plik `.rdp`.
8. Otwórz pobrany plik `.rdp` za pomocą natywnego klienta RDP (na przykład Remote Desktop Connection w systemie Windows lub Windows App w systemie macOS).

20.4.4 Rezultat

Gdy skonfigurowano *Domenę konfiguracji RDP*, wygenerowany plik `.rdp` zawiera nazwę hosta zbudowaną z użyciem tej domeny w pozycji `full address`. W rezultacie pasek tytułu klienta RDP wyświetla niestandardową nazwę hosta, którą użytkownik może łatwiej rozpoznać. Tytuł sesji pokazuje skonfigurowaną nazwę hosta (na przykład `server-name - 10.0.242.25.jdoe.dev.main.lab:2222`).

Uwaga

Jeśli pole *Domena konfiguracji RDP* pozostanie puste, wygenerowana konfiguracja RDP użyje domyślnego adresu połączenia, tak jak we wcześniejszych wersjach.

Przykład pliku RDP

```
full address:s:10.0.234.1.jdoe.dev.main.lab:2222
username:s:<generated_username>
prompt for credentials:i:1
```

Gdzie:

- `10.0.234.1` – adres IP serwera docelowego
- `jdoe.dev.main.lab` – niestandardowa nazwa hosta
- `2222` – port gniazda nasłuchiwania
- `generated_username` – tymczasowa / OTP nazwa użytkownika z Fudo Enterprise

Uwaga

Niestandardowa nazwa hosta RDP jest etykietą DNS wskazującą na gniazdo nasłuchiwania Fudo Enterprise, a nie na sam serwer docelowy.

Tematy pokrewne:

- *Konfigurowanie gniazda nasłuchiwania RDP*
- *Microsoft Remote Desktop*
- *Konfiguracja usługi Remote Desktop Services na serwerze Windows dla Fudo Enterprise*

20.5 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.

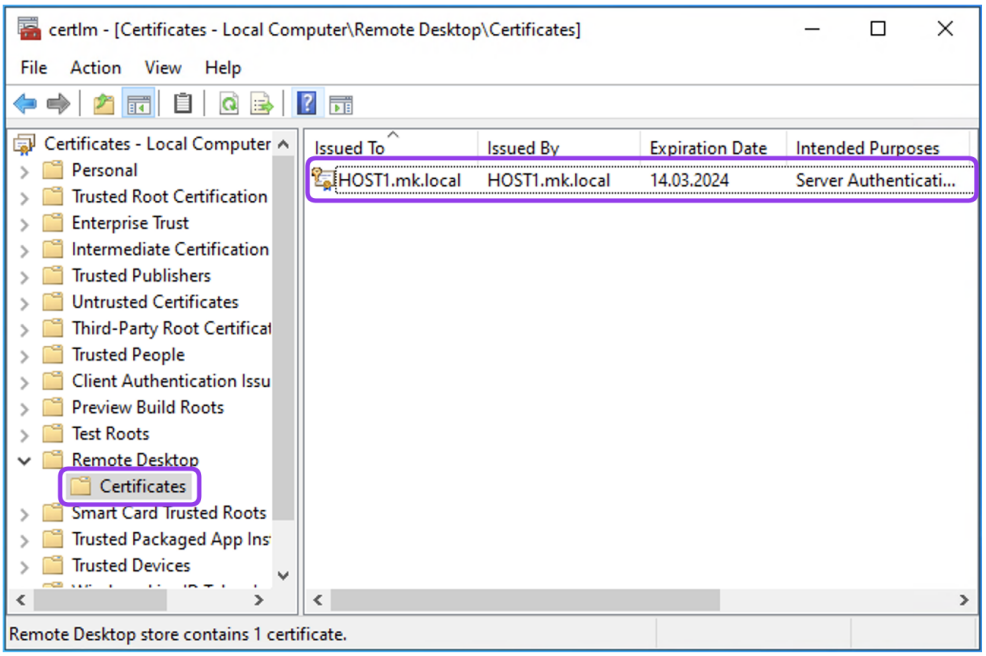
20.5.1 Lokalizacja certyfikatu dla protokołu RDP w Windows Server

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
   ```

(ciąg dalszy na następnej stronie)

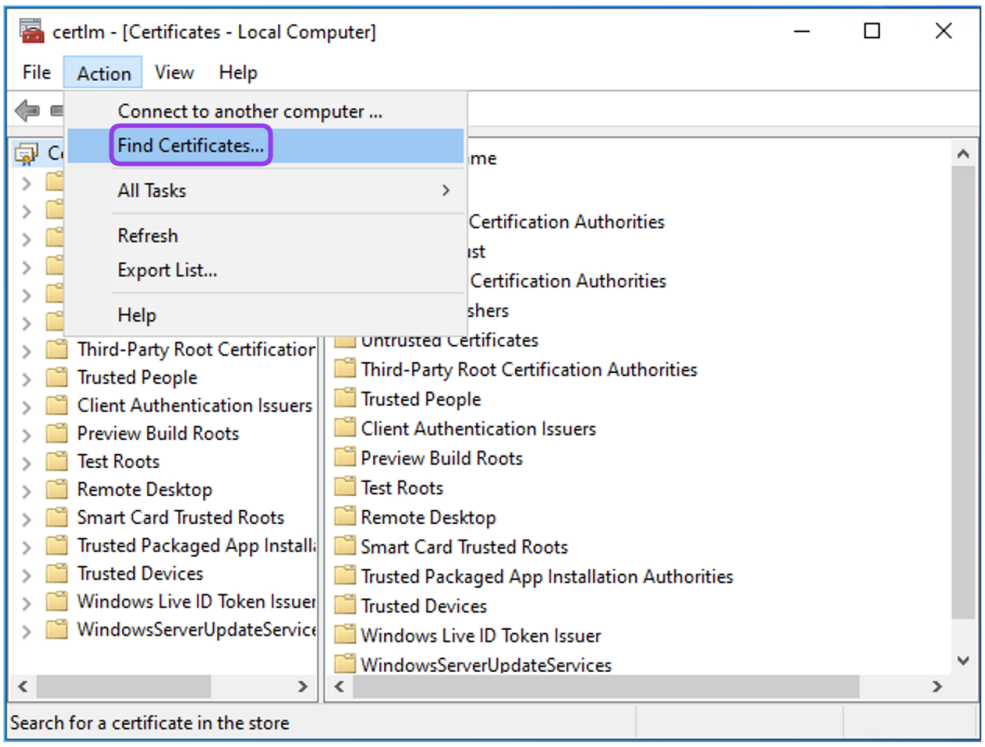
(kontynuacja poprzedniej strony)

```
MTQxNzA2NTRaMBkxFzAVcas7c6c6sh83uydtLm1rLmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2ngYkoMa4dgLgGl1+G+m2UEAIH/
↪6ttyQep5u
tUYkxKeuqpn9AWnYP8To1fornJN387ddhcy76d7jchc8Q093RWVb2cMKKjgOAW9w
qLFW+WrLEUPY8hYvsCFYgFH3HOHhKLEoWBN5qHH7vjIiW3Rb0Y7xeGb9x0FWItQX
mbF6sucGdlH+OsjepxMLPVh3Qpb2WQ18kSQGyS1ocbJxOWST9sH4MQkRVFL3rkxN
f7/
↪qdJcdM6sFxEJTdp30CITRfbORXacl84bStjW2MJzvJRqr94xDHonRdIM9tUka
O6LVJQY6qiEpMVE8MpSDAfoZ+HeyVWt+2EfXlfWE4hiMJP1DoQIDAQABoyQwIjAT
BgNVHSUEDDAKBggrBgEFBQcDATALBgNVHQ8EBAMCBDAwDQYJKoZIhvcNAQELBQAD
ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
↪Tnrrn2
7pr0jLnCjUq9rxHC6jfMR0U2PT4qrMHvGD1nUwZdHuZPavPLFHh/
↪rYHZpizoS+9W
ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
↪Tnrrn2
xyXjeYdX8/U9EdgrXOLGX9U74rfGQTrQxZyjuYlGxxqop/
↪y2V3n+3NnNzY+ehW1G
ggEBAGNXzwNC4DhOxyaVhVTPePsa97aeWJtpl64cE4/ZdAfGBEIfHlBEh/
↪Tnrrn2
ZUvdUnqtdH+ODdAWBo4P1dv0nL8=
-----END CERTIFICATE-----
```

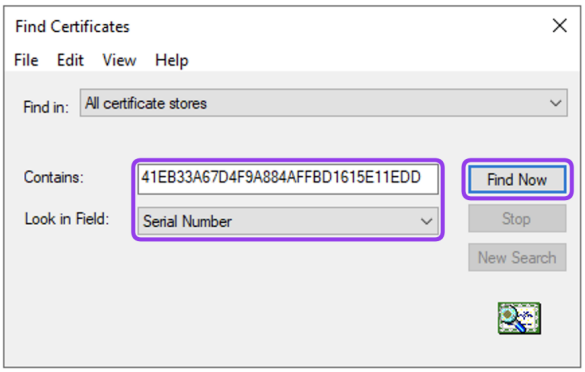
3. W odpowiedzi wyodrębniony zostanie numer seryjny, który możesz wykorzystać do wyszukania certyfikatu w Menedżerze certyfikatów.

   ```
   serial=41EB33A67D4F9A884AFFBD1615E11EDD
   ```

4. Skopiuj wyodrębniony numer seryjny i przejdź do Windows Server.
5. Wybierz *Run* z *Start menu*, a następnie wpisz `certlm.msc`, aby otworzyć Menedżer certyfikatów.
6. Przejdź do *Action* > *Find Certificates...*



7. Wpisz skopiowany numer seryjny w polu *Contains* i z rozwijanego menu *Look in Field* wybierz *Serial Number*.



8. Kliknij *Find Now*.

20.5.2 Dostarczanie certyfikatu CA

Uwaga

- 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.

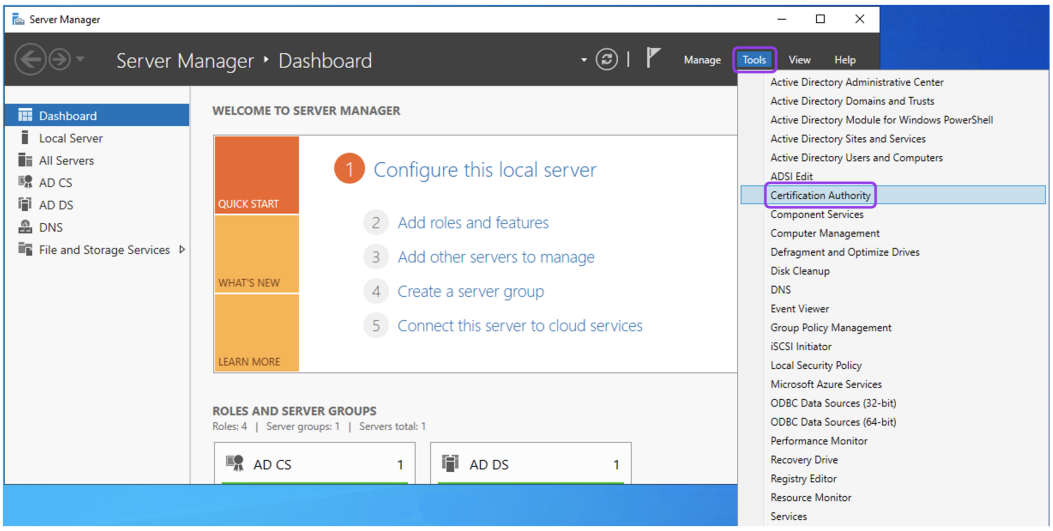
Instalacja Certificate Authority w Windows Server:

Aby zainstalować *Certificate Authority* w Windows Server, postępuj zgodnie z instrukcją Windows Server.

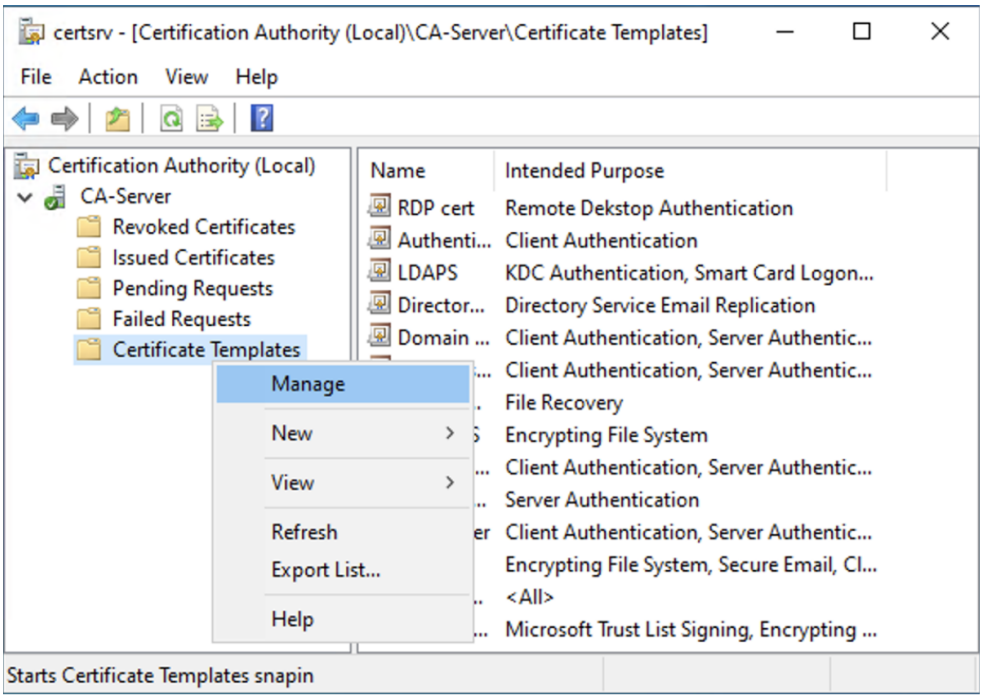
> **Uwaga**
>
> W procedurze opisanej poniżej wykorzystano opcję *Enterprise CA*.

Tworzenie szablonu dla certyfikatu RDP:

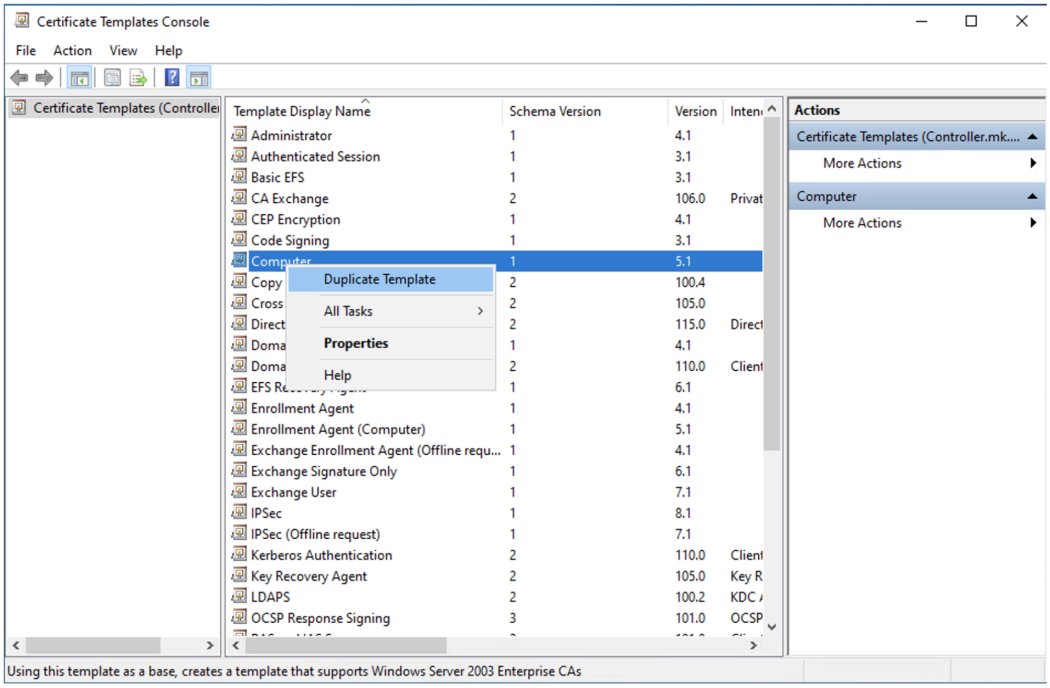
1. Otwórz *Certificate Authority* z poziomu narzędzia *Server Manager*, klikając *Tools* > *Certification Authority* w prawym górnym rogu okna.



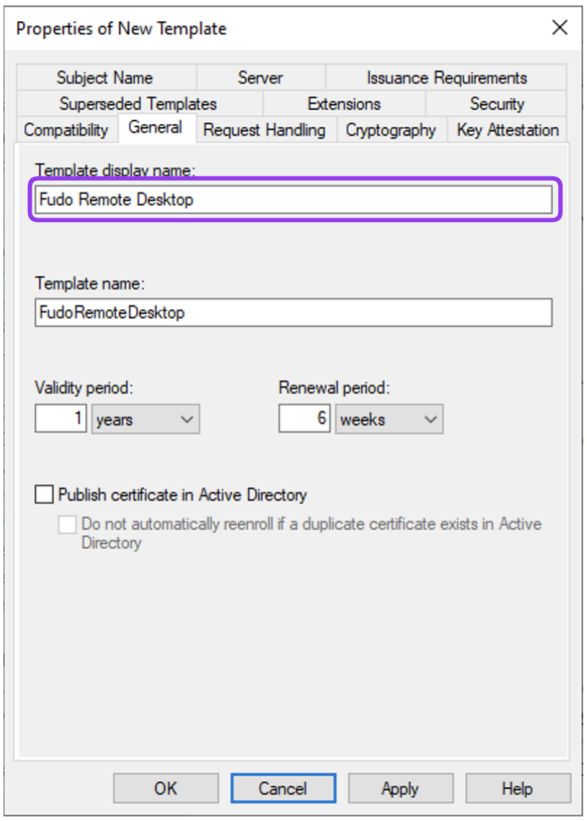
2. Kliknij prawym przyciskiem myszy na *Certificate Templates* i wybierz *Manage*.



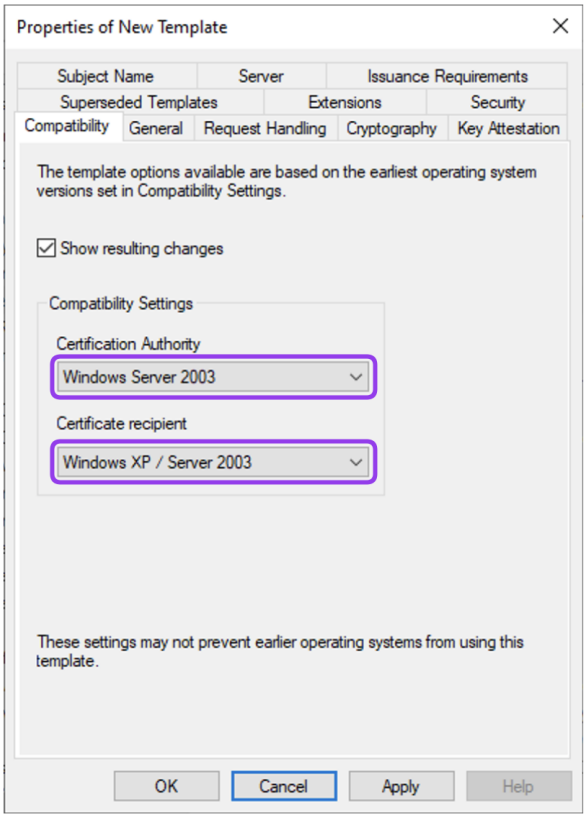
3. Znajdź szablon *Computer*, kliknij na nim prawym przyciskiem myszy i wybierz *Duplicate Template*.



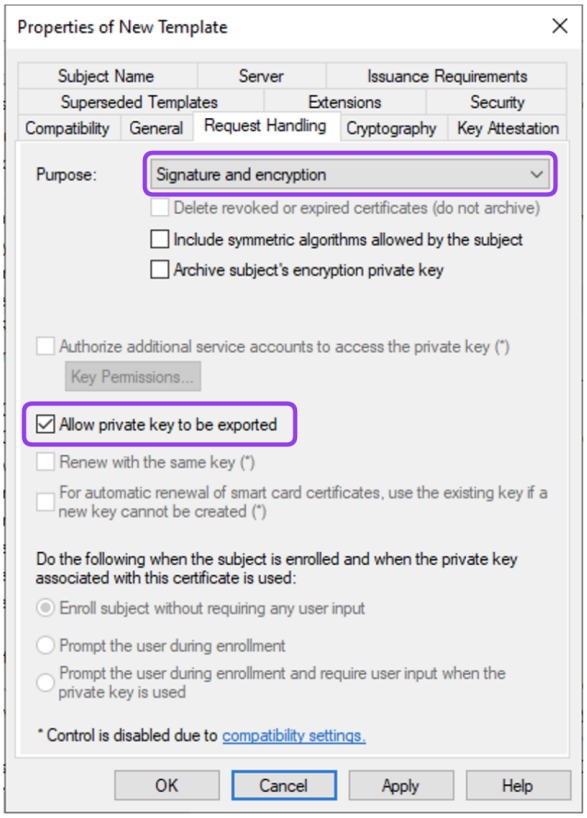
4. W zakładce *General*, wprowadź nazwę dla nowego szablonu oraz określ okres ważności i odnawiania według potrzeb.

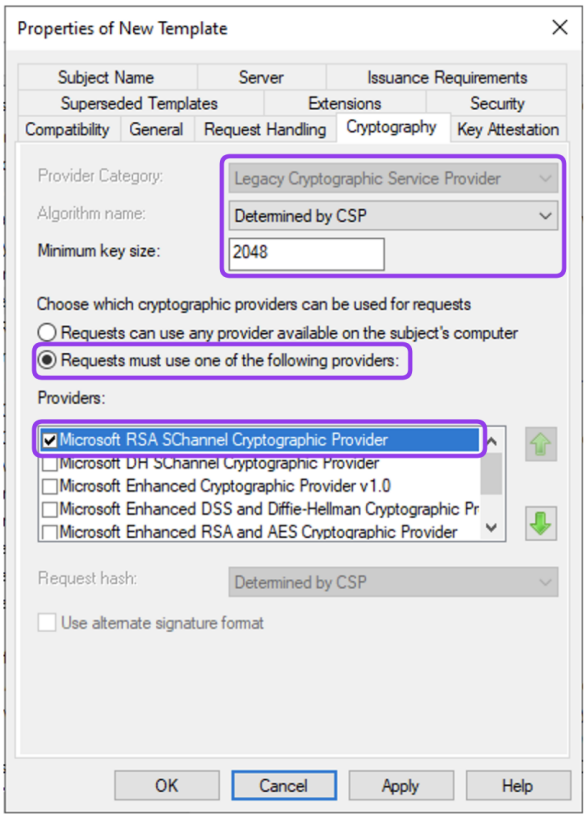


5. W zakładce *Compatibility*, z listy rozwijanej *Certification Authority* wybierz *Windows Server 2003*, natomiast z listy rozwijanej *Certificate recipient* wybierz *Windows XP/Server 2003*.

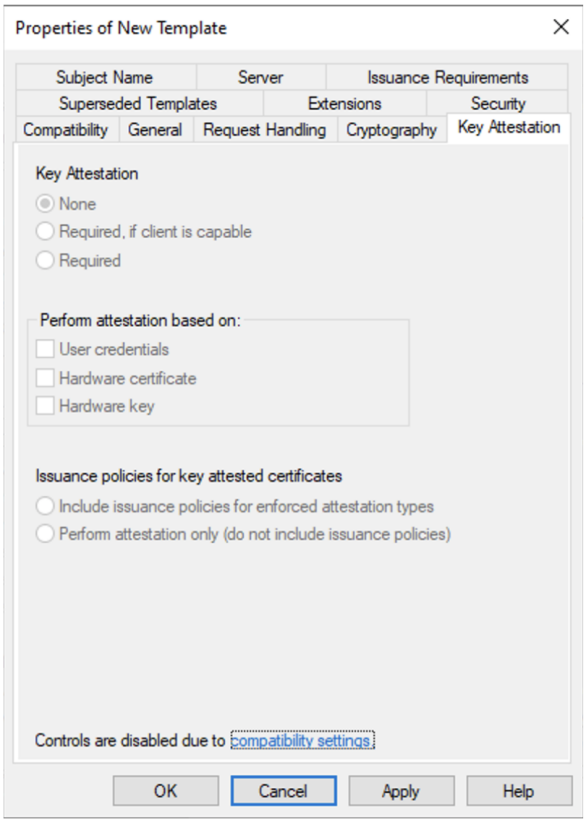


6. W zakładce *Request Handling*, ustaw *Purpose* na *Signature and encryption* i zaznacz opcję *Allow private key to be exported*.

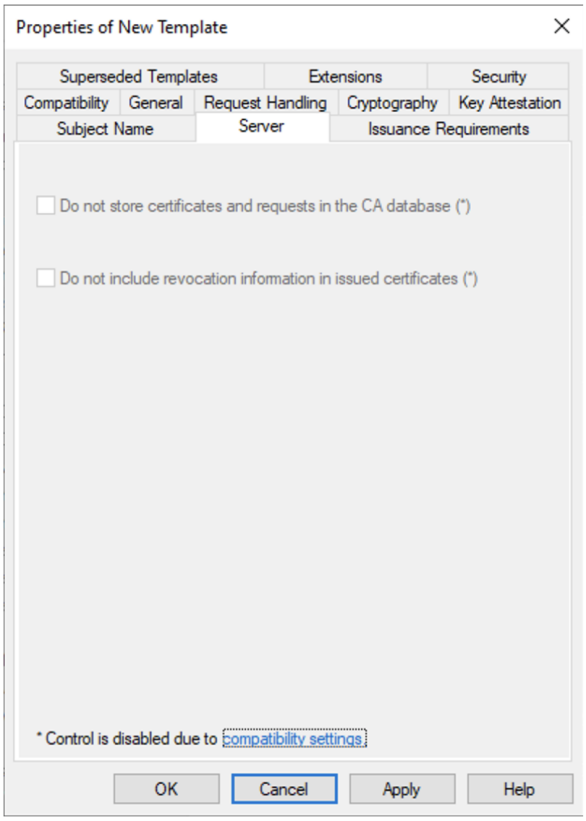




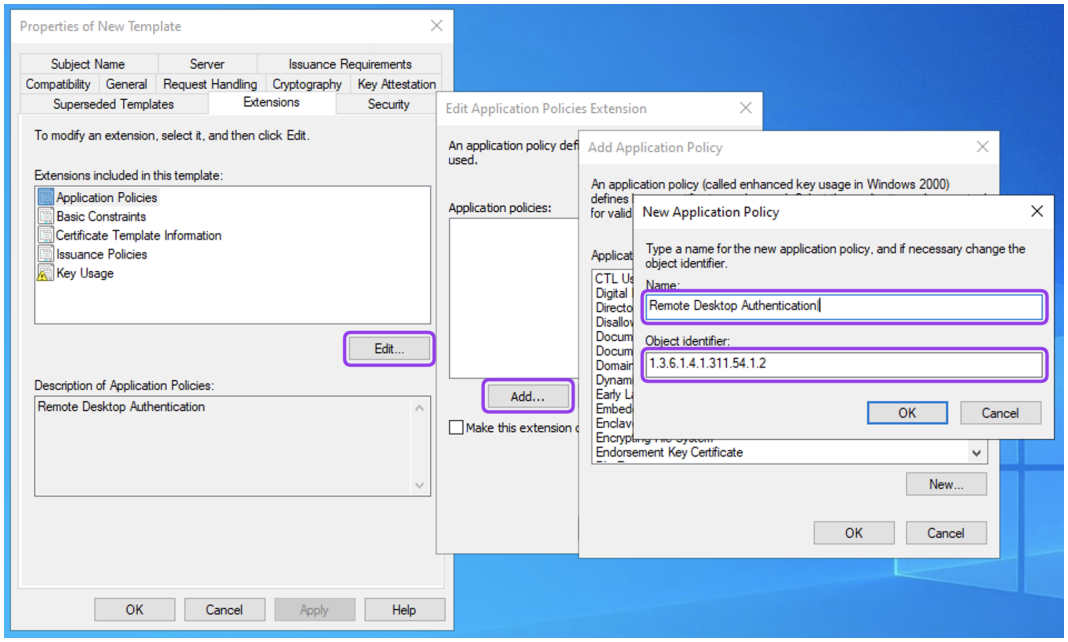
8. W zakładce *Key Attestation* pozostaw ustawienia domyślne.



9. W zakładce *Server* pozostaw ustawienia domyślne.

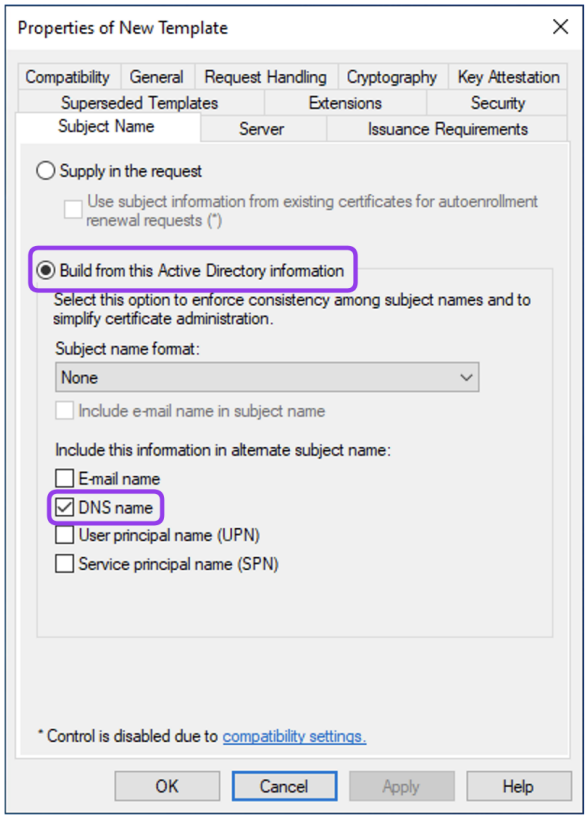


10. W zakładce *Security* dodaj komputery i grupy, które mają być uprawnione do używania tego szablonu. Sprawdź, czy grupa lub użytkownik, którego używasz, ma włączone uprawnienia *Read*, *Write* i *Enroll*. Jest to konieczne do żądania certyfikatu przy użyciu tego szablonu w następnych krokach.
11. 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`.

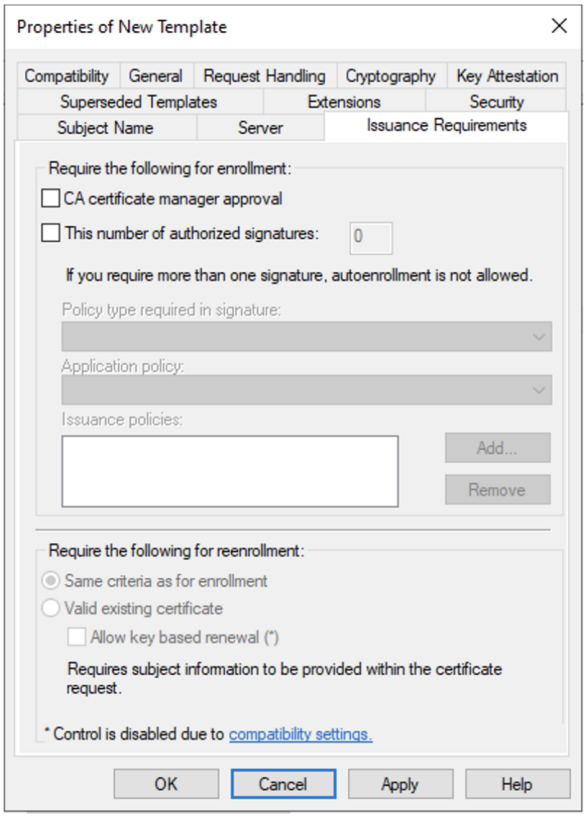


15. Kliknij trzy razy *OK*, aby wrócić do okna *Properties of New Template*.

16. W zakładce *Subject Name* wybierz opcję *Build from this Active Directory information* i następnie *DNS name*.

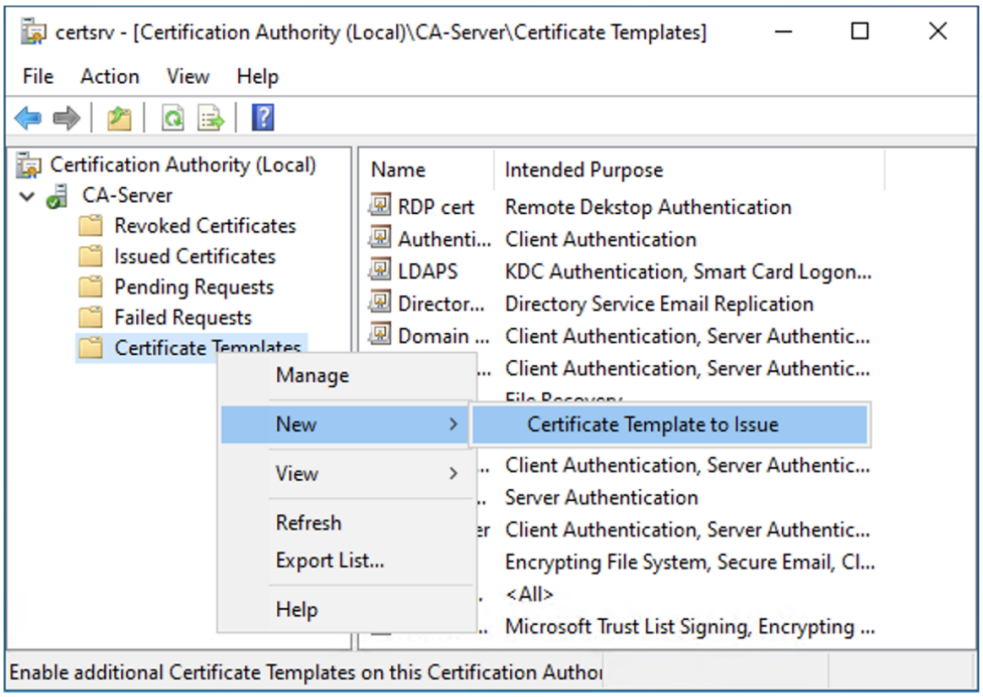


17. W zakładce *Issuance Requirements*, pozostaw ustawienia domyślne.

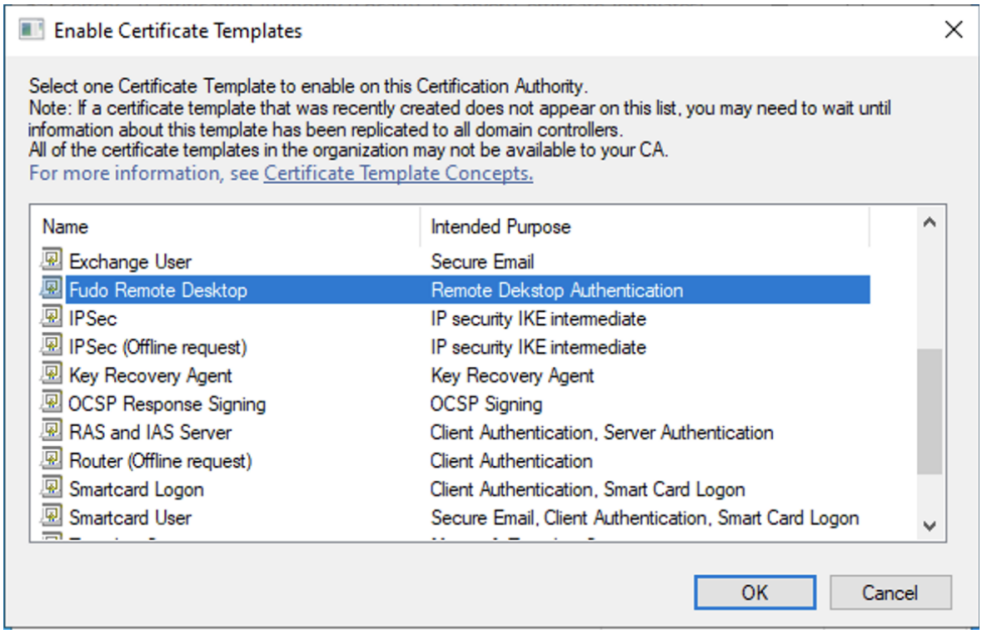


18. Kliknij *OK*, aby zapisać utworzony szablon. Zamknij *Certificate Templates Console*.

19. Wróć do okna *Certification Authority*, kliknij prawym przyciskiem myszy na *Certificate Templates* i wybierz *New* > *Certificate Template to Issue*.

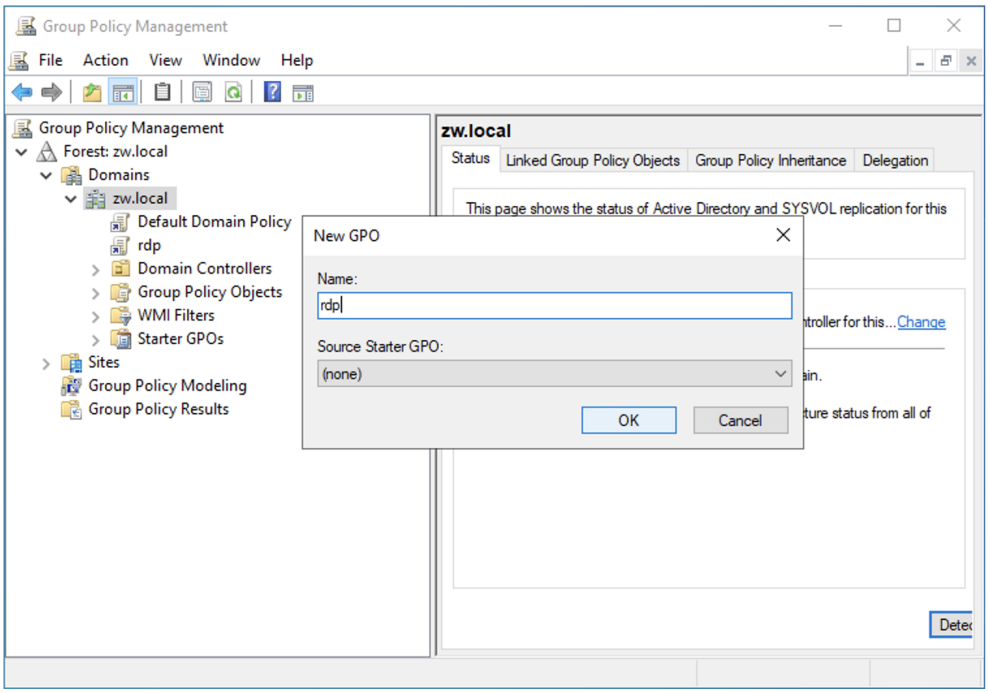


20. Wybierz utworzony szablon i kliknij *OK*.



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*.

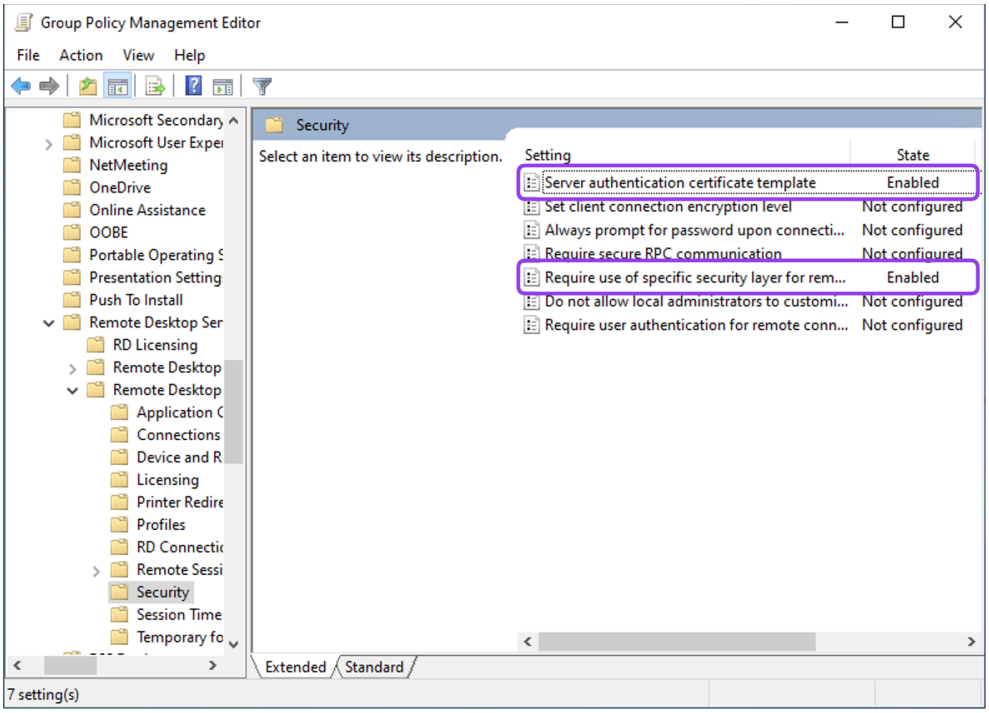


5. Kliknij prawym przyciskiem myszy na nazwę utworzonego *GPO* i wybierz

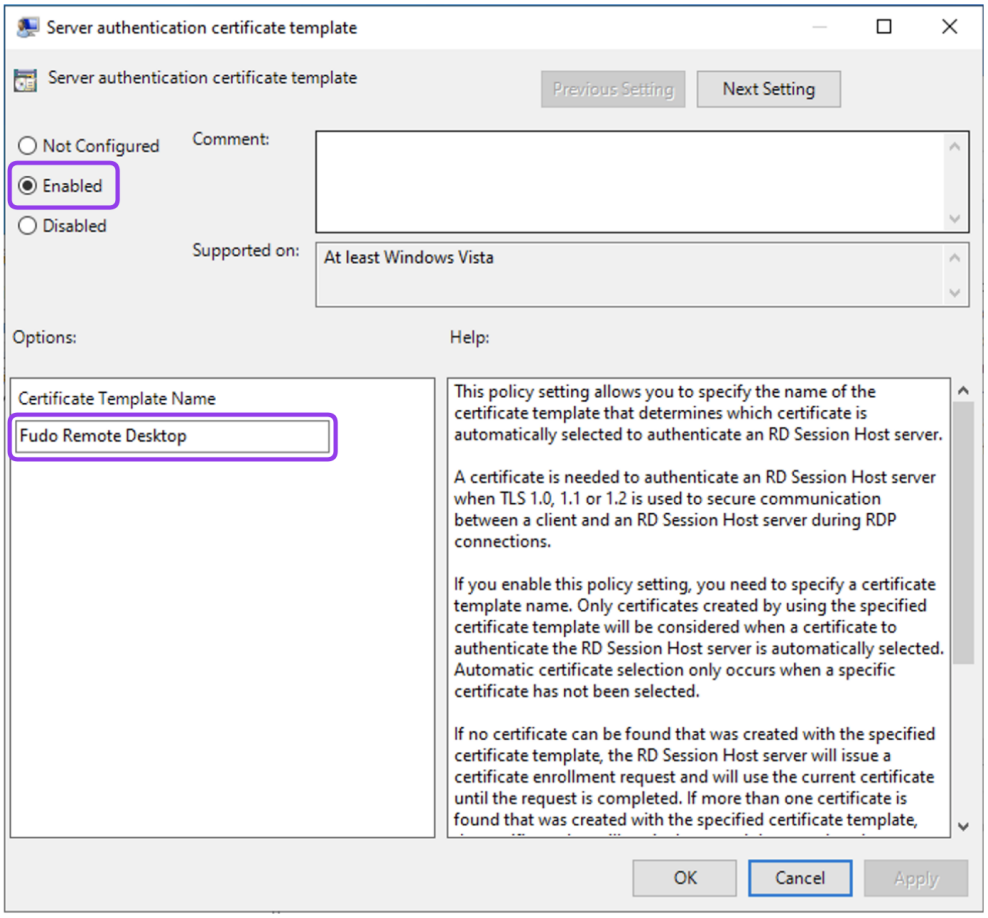
Edit....

6. W *Group Policy Management Editor* przejdź do *Computer Configuration* > *Policies* > *Administrative Templates* > *Windows Components* > *Remote Desktop Services* > *Remote Desktop Session Host* > *Security*.

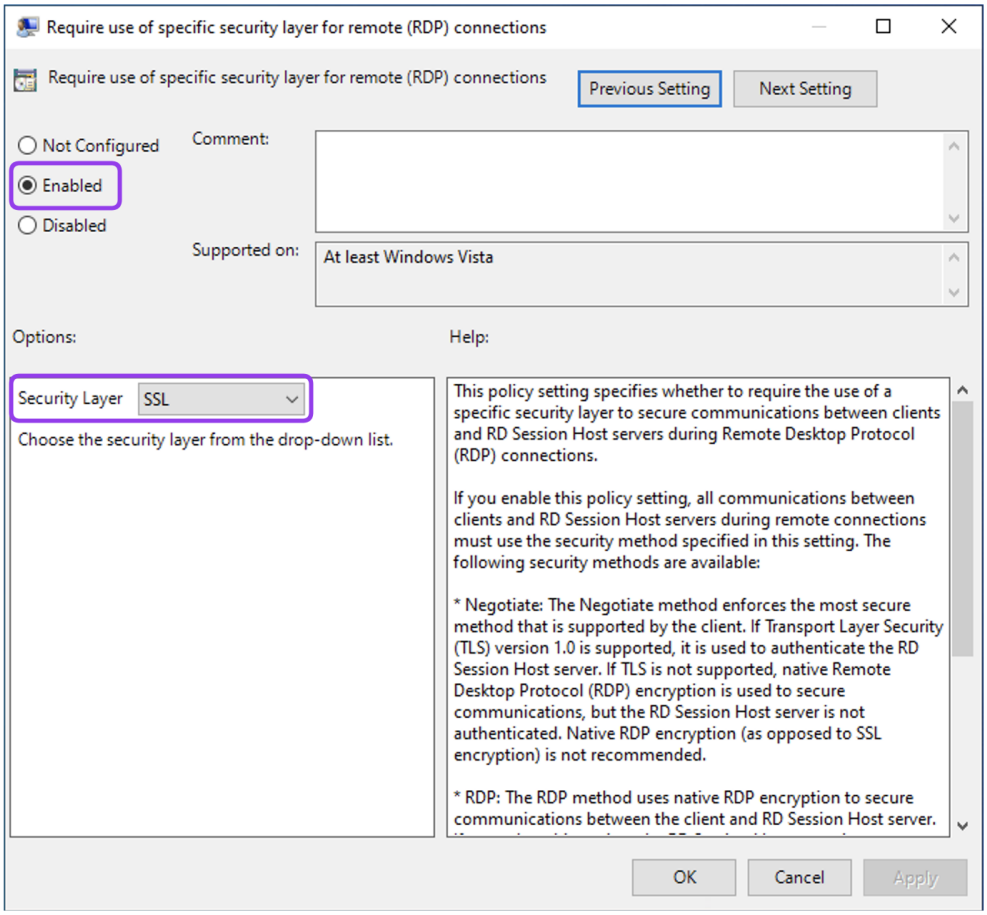
7. Kliknij dwukrotnie na *Server authentication certificate template*, aby edytować to ustawienie.



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*.

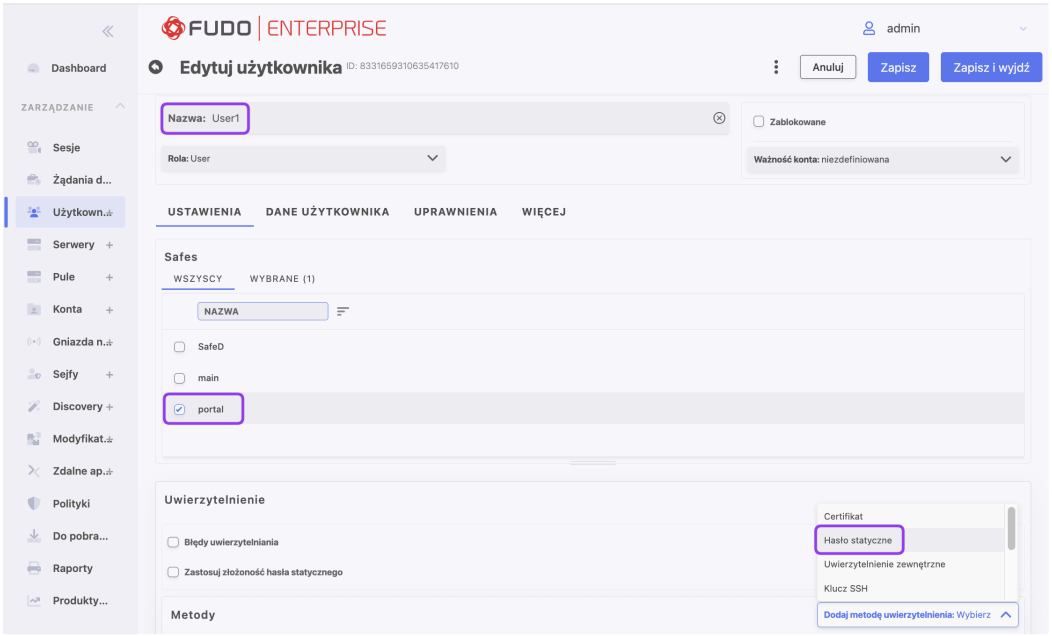
Eksport certyfikatu CA:

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*.

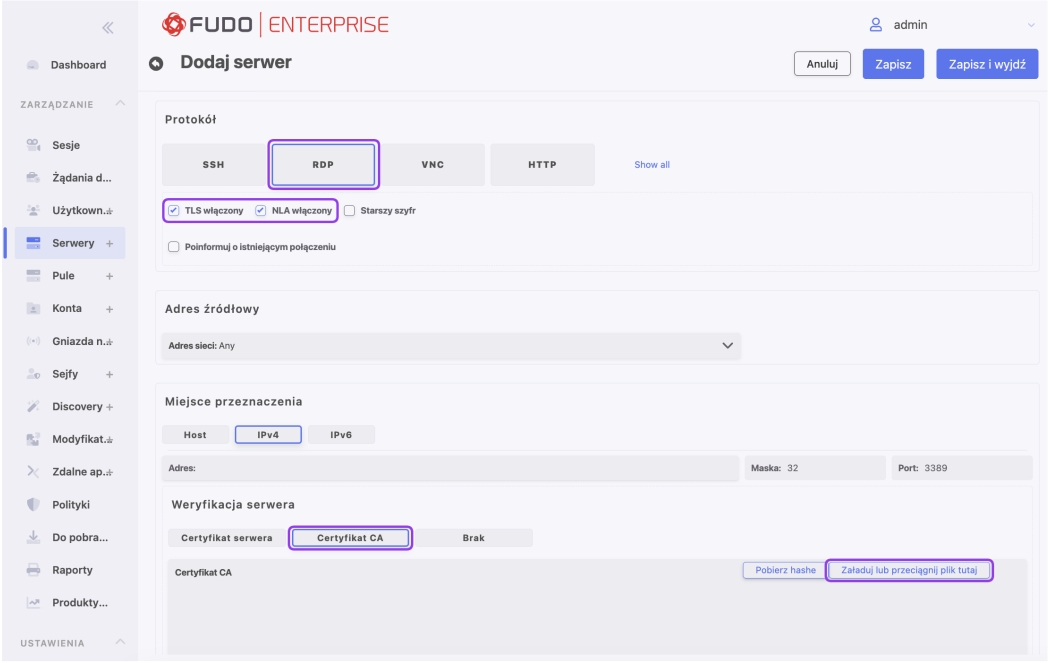


6. Wprowadź hasło i kliknij *Zapisz*.
8. Uzupełnij pozostałe parametry według własnych wymagań (jeśli wymagane). W tym celu możesz zapoznać się z treścią rozdziału *Dodawanie użytkownika*.
9. Kliknij *Zapisz i zamknij*.

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*.

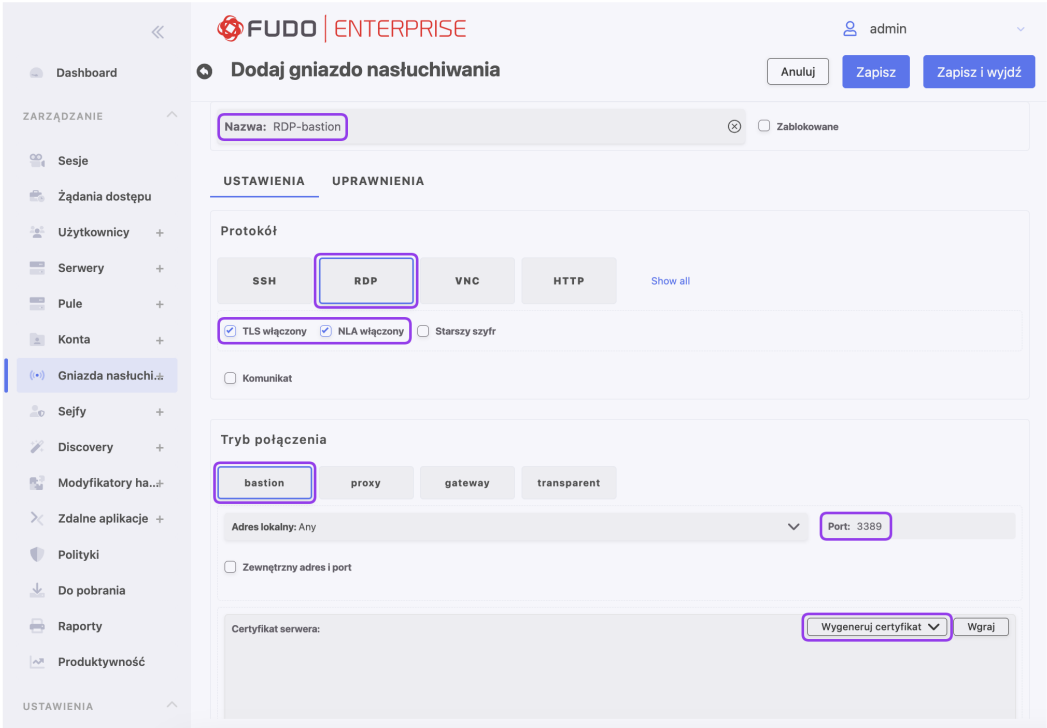
Konfiguracja konta:

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.

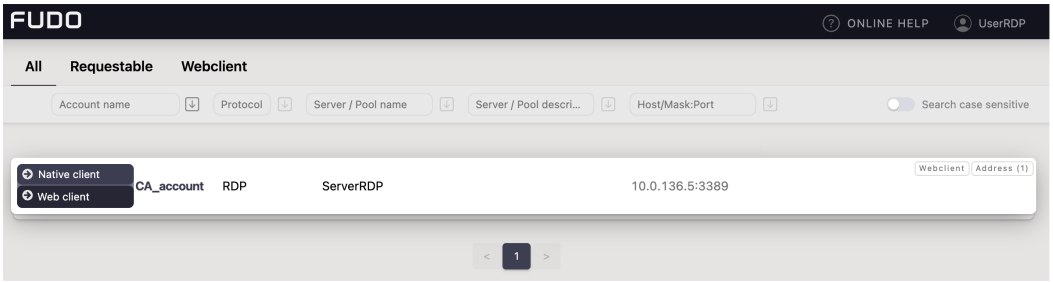
- Kliknij *+ Dodaj użytkownika*, a następnie kliknij przycisk [+] obok `User1`, który został utworzony w poprzednich krokach, aby umożliwić dostęp do serwera przez monitorowany sejf.
- Kliknij *ok*, aby zamknąć okno.

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

- **Kliknij «+ Dodaj konto», a następnie kliknij ikonę + obok `CA-account`, które zostało utworzone w poprzednich krokach.**
  - Kliknij «ok», aby zamknąć okno.
  - Kliknij ikonę edycji, aby przypisać do konta gniazdo nasłuchiwania.
  - Kliknij ikonę +, aby dodać gniazdo nasłuchiwania `RDP-bastion` utworzone w poprzednich krokach.
  - Kliknij «ok», aby zamknąć okno.
6. Kliknij *Zapisz*.

Nawiązywanie sesji:

1. Zaloguj się do *Portalu Użytkownika* Fudo Enterprise używając `User1` jako nazwy użytkownika i hasła podanego podczas tworzenia tego użytkownika.
2. Najedź kursorem na nazwę `CA_account` i wybierz *Klient webowy*, aby rozpocząć sesję.



Related topics:

- *Dodawanie serwera RDP*
- *Dodawanie użytkownika*

20.6 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.

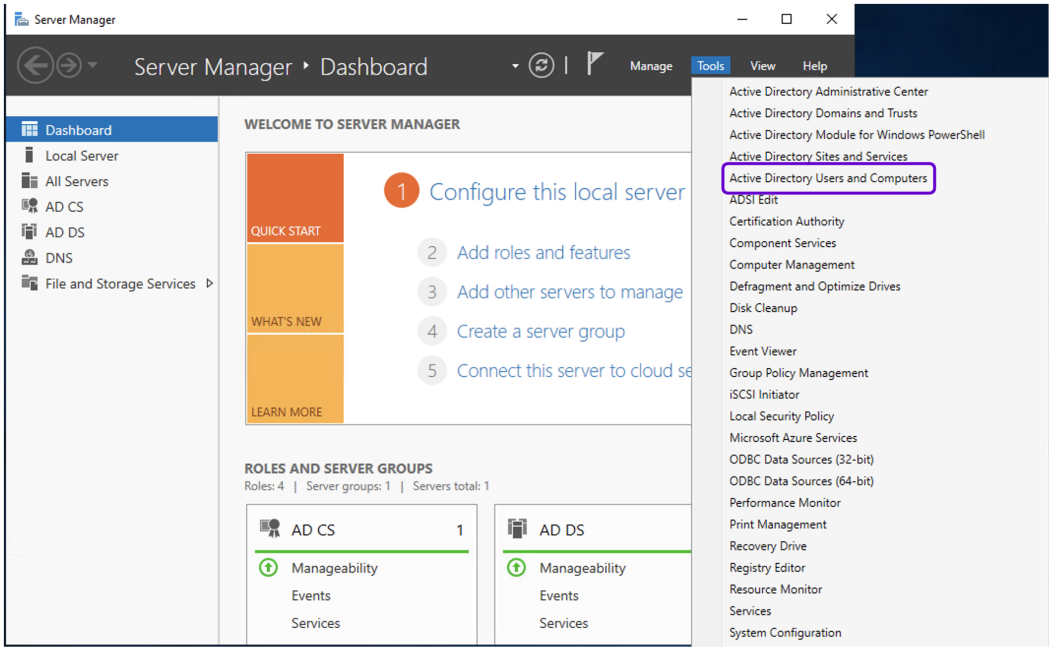
Uwaga

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.

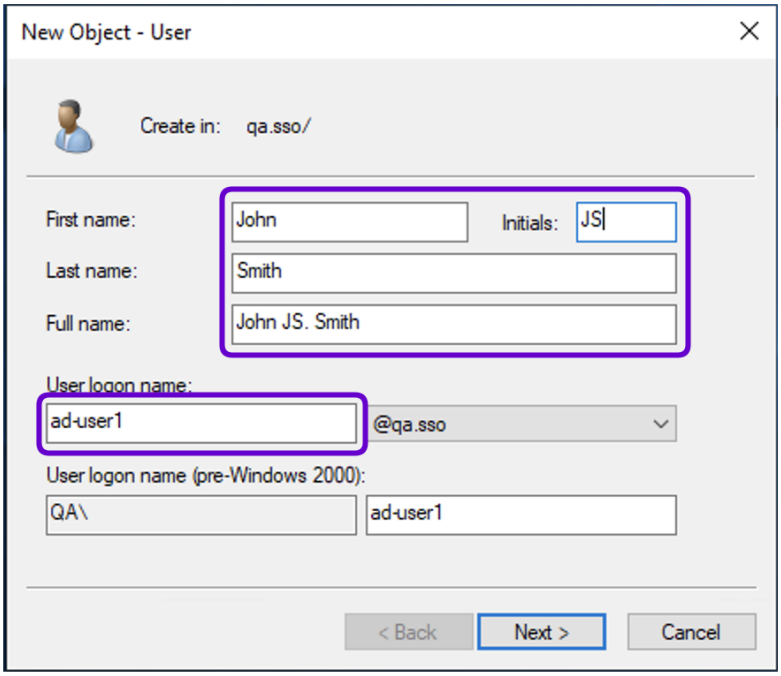
20.6.1 Konfiguracja SSO na Windows Server 2019

Dodaj użytkownika:

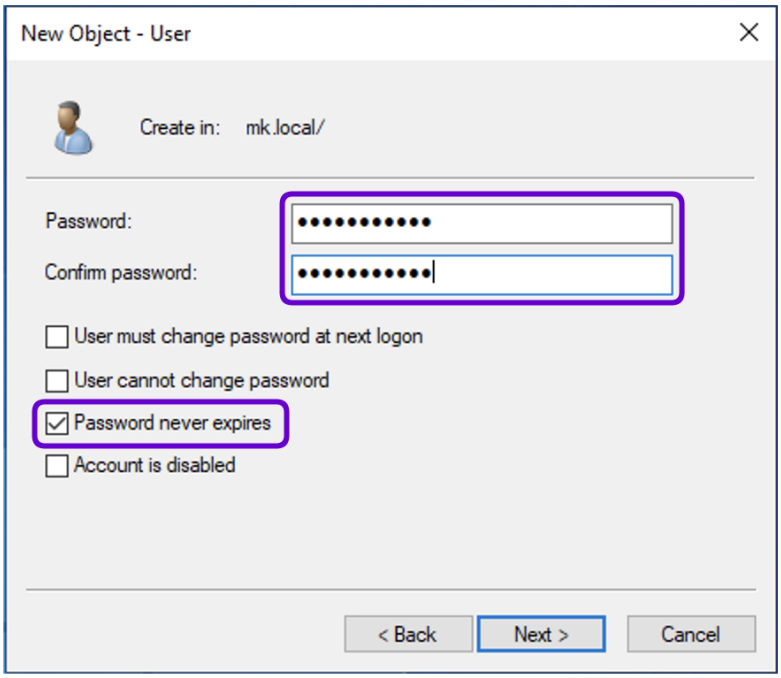
1. Zaloguj się na serwerze, na którym chcesz skonfigurować SSO, używając konta administratora.
2. Uruchom aplikację *Server Manager*.
3. Kliknij przycisk *Tools* w prawym górnym rogu okna, aby rozwinąć listę menu i wybierz *Active Directory Users and Computers*.



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`).

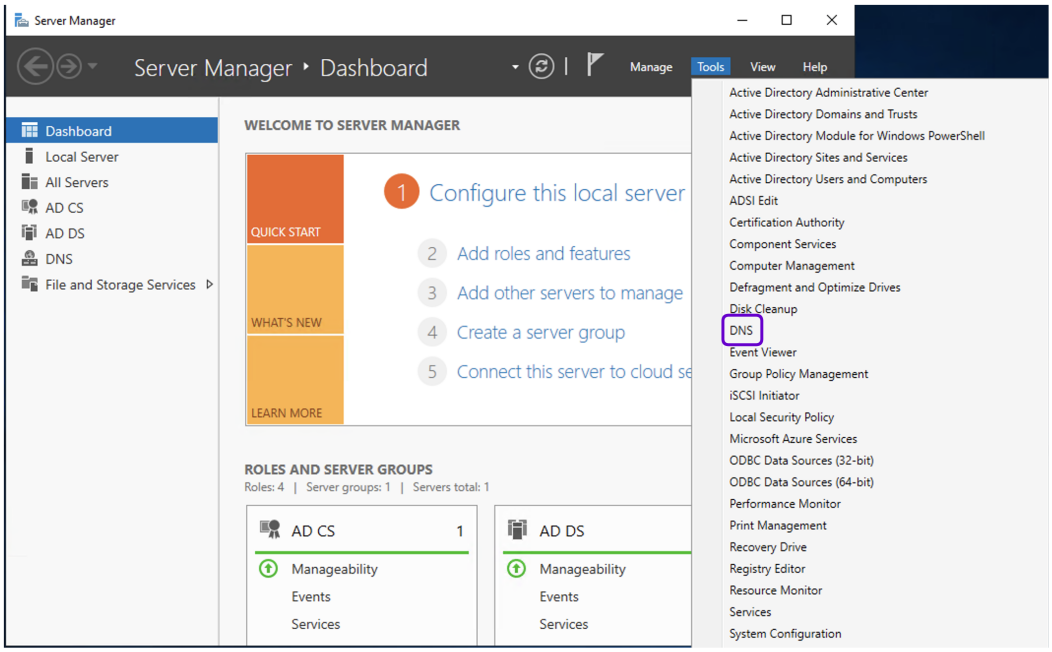


7. Kliknij *Next*.
8. Podaj hasło dla utworzonego użytkownika (np. `PaSSwOrD`) i wybierz opcję *Hasło nigdy nie wygasa*.
9. Kliknij *Next* i *Finish*.

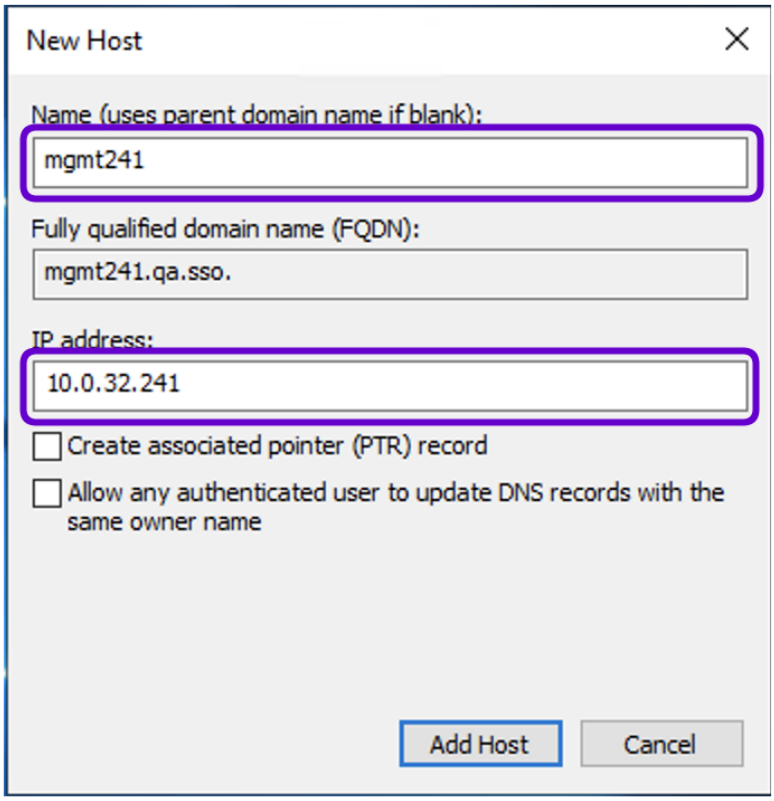


Konfiguracja wpisów DNS:

1. Uruchom aplikację *Server Manager*.
2. Kliknij przycisk *Tools* w prawym górnym rogu okna, aby rozwinąć listę menu i wybierz *DNS*.

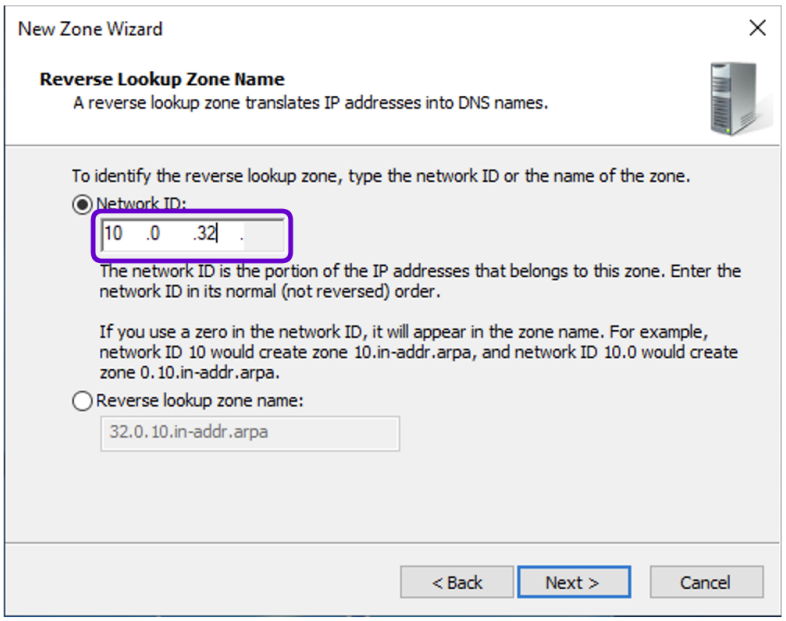


3. Przejdź do *Forward Lookup Zones*, kliknij prawym przyciskiem myszy na nazwę domeny i wybierz *New Host.*
4. Podaj *Nazwę* i *Adres IP* Panelu Administracyjnego Fudo Enterprise (np: `mgmt241.qa.sso, 10.0.32.241`).
5. Kliknij *Add Host.*

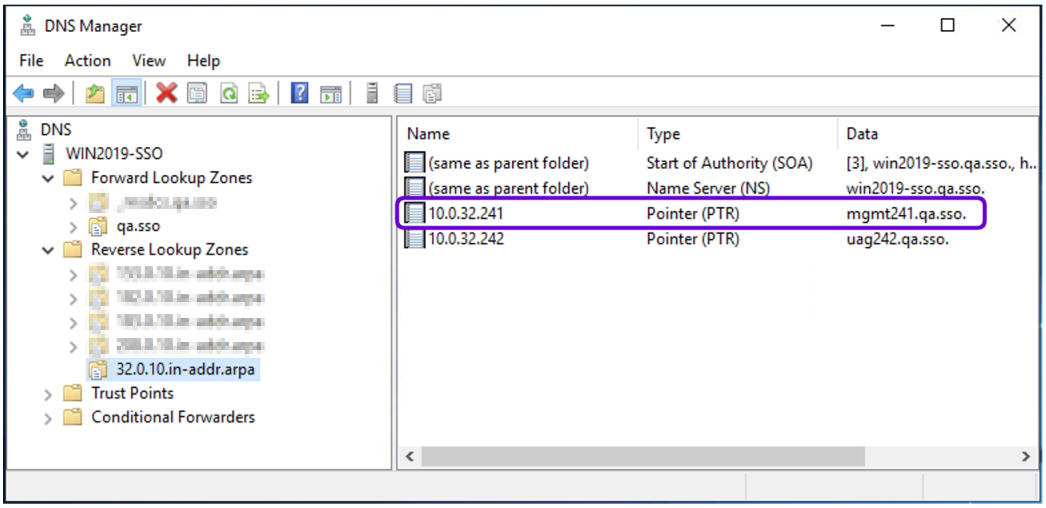


6. Kliknij prawym przyciskiem myszy na *Reverse Lookup Zone* i wybierz *New Zone.*

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.

20.6.2 Konfiguracja Fudo Enterprise

> **Uwaga**
>
> 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.

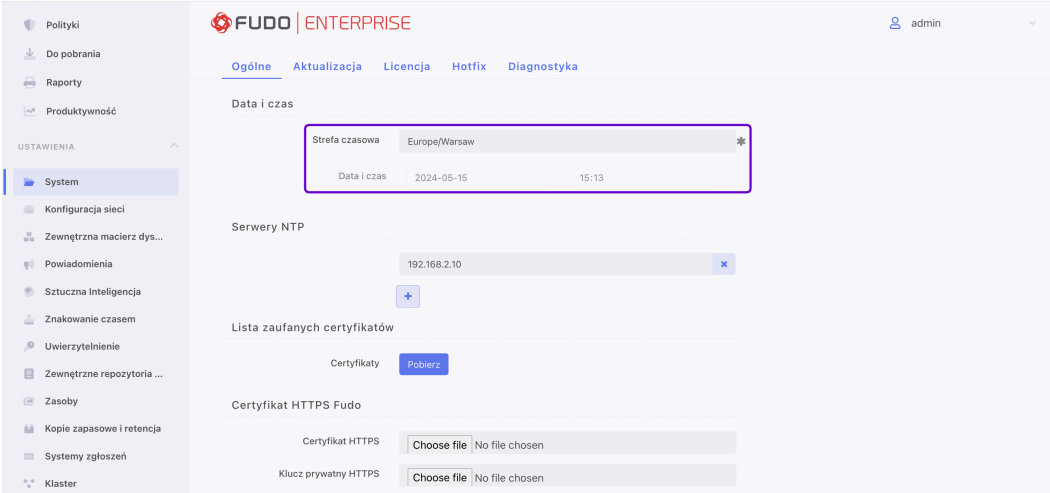
Konfiguracja SSO:

Aby zdefiniować parametry usługi SSO w Fudo Enterprise, wykonaj następujące kroki:

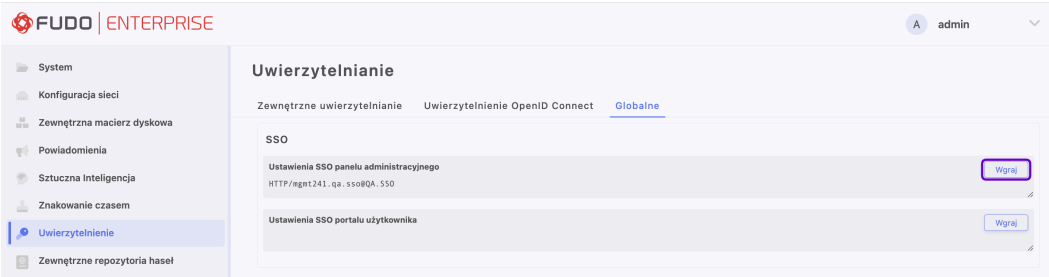
1. Zaloguj się do Panelu Administracyjnego Fudo Enterprise używając danych uwierzytelniających użytkownika z rolą `superadmin`.
2. Wybierz *Ustawienia* > *Uwierzytelnianie*.
3. W sekcji *Data i czas* sprawdź, czy wybrana strefa czasowa jest zgodna z konfiguracją strefy czasowej klienta Windows.

Ostrzeżenie

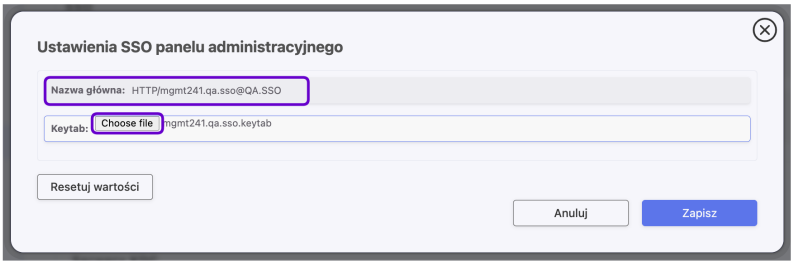
Strefa czasowa Fudo Enterprise musi być zgodna z konfiguracją strefy czasowej klienta Windows.



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*.

> **Uwaga**
>
> Możesz również skonfigurować SSO dla Portalu Użytkownika, przesyłając 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`.

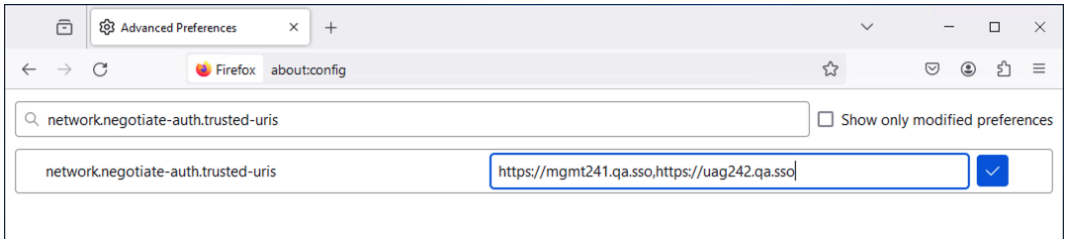
> **Uwaga**
>
> Zarówno *Domena Fudo*, jak i *Domena AD* powinny odpowiadać nazwie domeny podanej w bilecie Kerberos.

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*.

20.6.3 Konfiguracja i sprawdzenie stacji roboczej użytkownika - klienta Windows 2010

Konfiguracja przeglądarki Firefox:

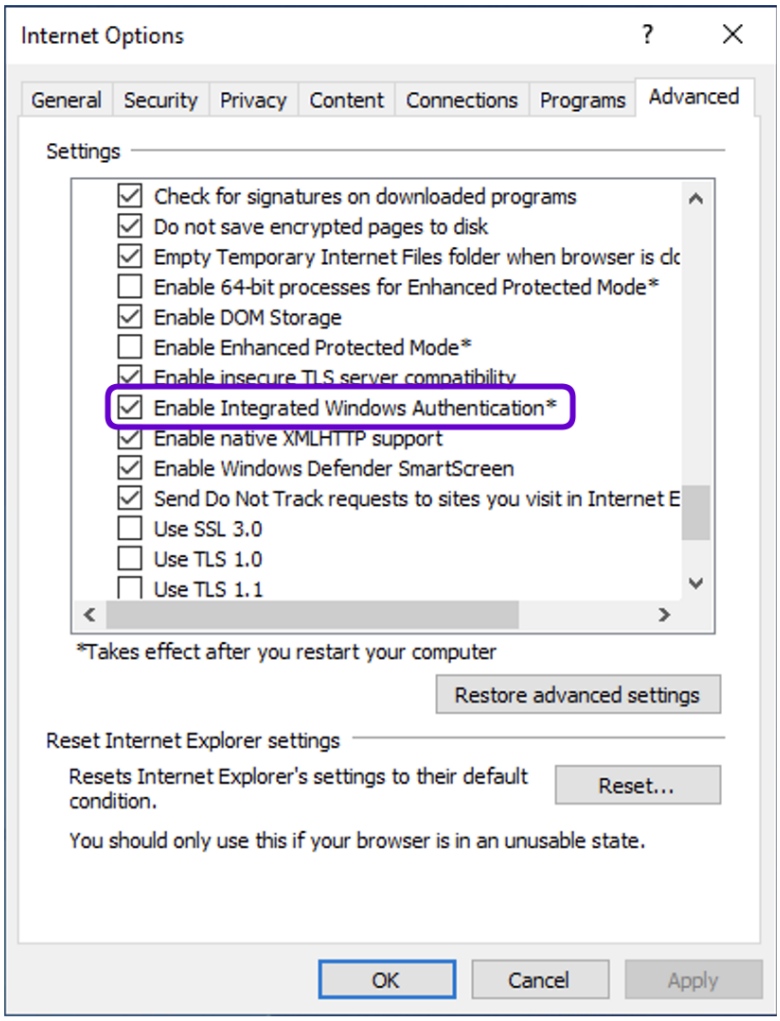
1. Zaloguj się na klienta Windows używając konta `ad-user1`.
2. Otwórz przeglądarkę *Firefox*, wpisz `about:config` w pasku adresu i wciśnij *Enter*.
3. Kliknij opcję *Akceptuj ryzyko i kontynuuj*, aby potwierdzić wyświetlony komunikat ostrzegawczy.
4. W pasku wyszukiwania na górze wpisz `network.negotiate-auth.trusted-uris`.
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.



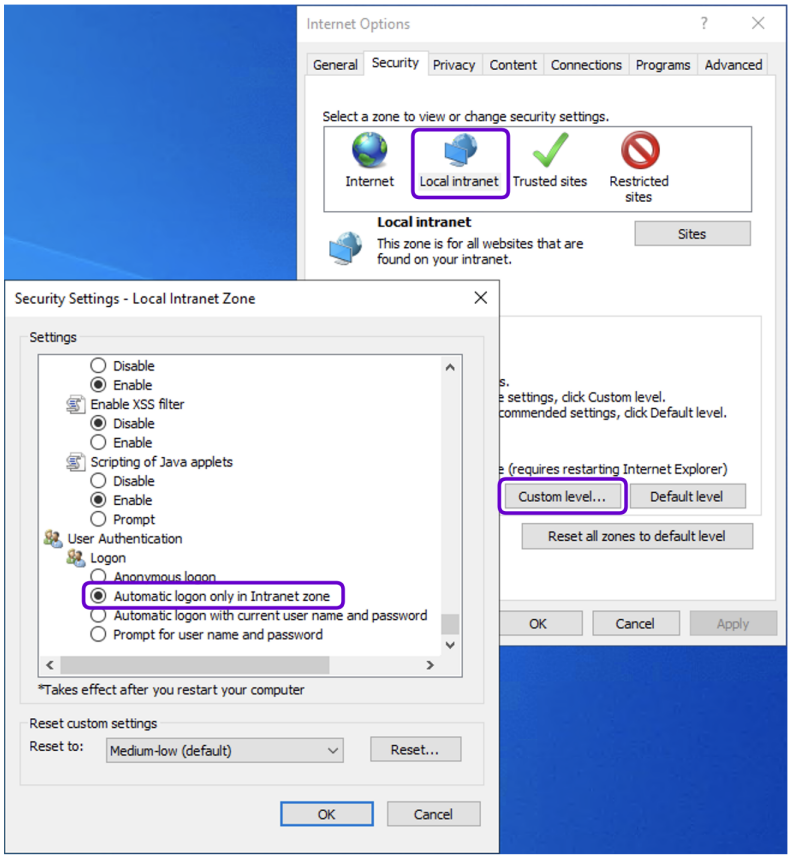
7. Następnie w pasku wyszukiwania wpisz `network.automatic-ntlm-auth.trusted-uris`.
8. Kliknij dwukrotnie na `network.automatic-ntlm-auth.trusted-uris` i wprowadź wybrany FQDN (Pełna Nazwa Kwalifikowana Domeny) wraz z protokołem, rozdzielając wpisy przecinkiem (np: `https://mgmt241.qa.sso,https://uag242.qa.sso`).
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.*



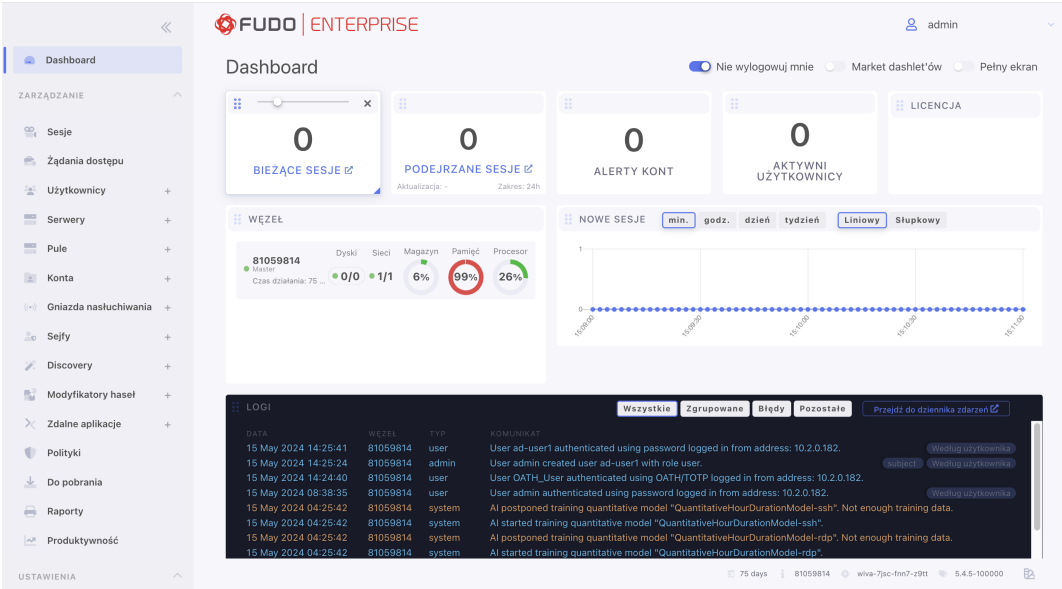
6. Kliknij *OK*.
7. Kliknij *Witryny* i zaznacz wszystkie pola wyboru.`
8. Kliknij *Zaawansowane* i dodaj stronę usługi Remedy SSO do strefy lokalnej (w naszym przykładzie to `https://mgmt241.qa.sso`).
9. Kliknij *Dodaj*.
10. Kliknij *OK* we wszystkich oknach dialogowych.
11. Uruchom ponownie przeglądarkę.

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*

20.7 Obsługa zmiany haseł kont lokalnych z wykorzystaniem konta domenowego przy użyciu modyfikatora haseł WinRM

Poniższa instrukcja opisuje podstawową konfigurację Fudo Enterprise niezbędną do umożliwienia zmiany haseł kont lokalnych na stacjach roboczych należących do domeny, z wykorzystaniem konta domenowego.

Do poprawnego działania modyfikatora haseł wymagane jest w Fudo Enterprise dodanie:

- Konfiguracji nazwy hosta i serwera DNS.
- Konfiguracji serwera KDC.
- Konfiguracji serwera, na którym zlokalizowane jest konto lokalne.
- Konfiguracji konta uprzywilejowanego, wykorzystywanego do przeprowadzenia zmiany hasła.
- Konfiguracji konta lokalnego lub domenowego, dla którego będzie zmieniane hasło.

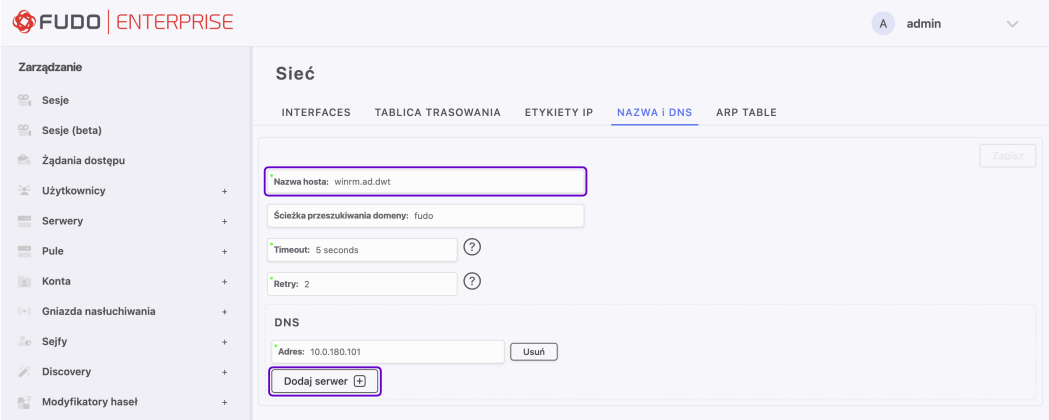
Uwaga

- Wymagane jest, aby Fudo Enterprise miało skonfigurowaną tę samą strefę czasową co domena.
- Przy użyciu domenowego konta uprzywilejowanego można zmieniać hasło zarówno kontom lokalnym, jak i kontom domenowym. Należy wziąć to pod uwagę podczas konfiguracji użytkowników uprzywilejowanych, którzy będą odpowiedzialni za zmianę hasła oraz tych, którym hasła będą zmieniane.

20.7.1 Konfiguracja nazwy hosta i serwera DNS

Ustaw nazwę hosta postępując zgodnie z poniższą instrukcją:

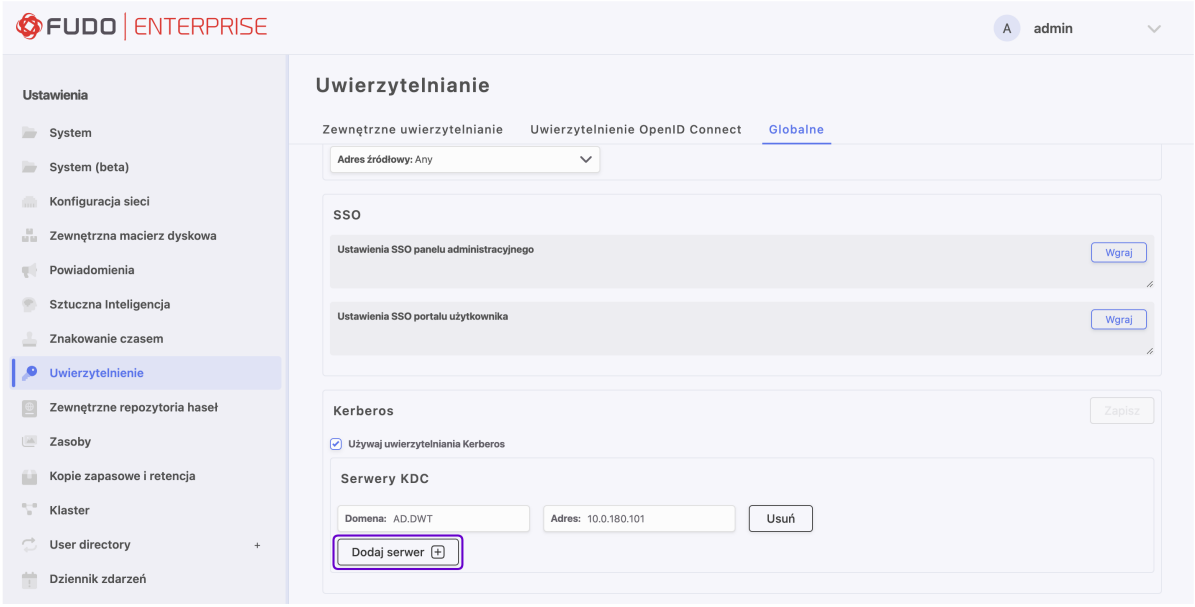
1. Przejdź do *Ustawienia* > *Konfiguracja sieci*.
2. Przejdź do zakładki *Nazwa i DNS*.
1. W polu *Nazwa hosta* wpisz nazwę wraz z domeną w podanym formacie: `hostname.yourdomain.local` (np. `winrm.ad.dwt`).
2. Skonfiguruj serwer DNS:
    - Kliknij *Dodaj serwer +*, aby zdefiniować nowy serwer DNS.
    - Wpisz adres IP serwera DNS (np. `10.0.180.101`).
    - Kliknij *Zapisz*.



20.7.2 Dodanie serwera KDC

Dodaj konfigurację serwera KDC postępując zgodnie z poniższą instrukcją:

1. Wybierz *Ustawienia* > *Uwierzytelnienie* > zakładka *Globalne*.
2. Przejdź do sekcji *Kerberos* i upewnij się, że włączona jest opcja *Używaj uwierzytelniania Kerberos*.
3. Kliknij *Dodaj serwer +*.



4. W polach *Domena* i *Adres* wprowadź odpowiednio domenę oraz adres IP serwera odpowiedzialnego za uwierzytelnianie i dystrybucję kluczy w protokole Kerberos (np: `AD.DWT` oraz `10.0.180.101`).

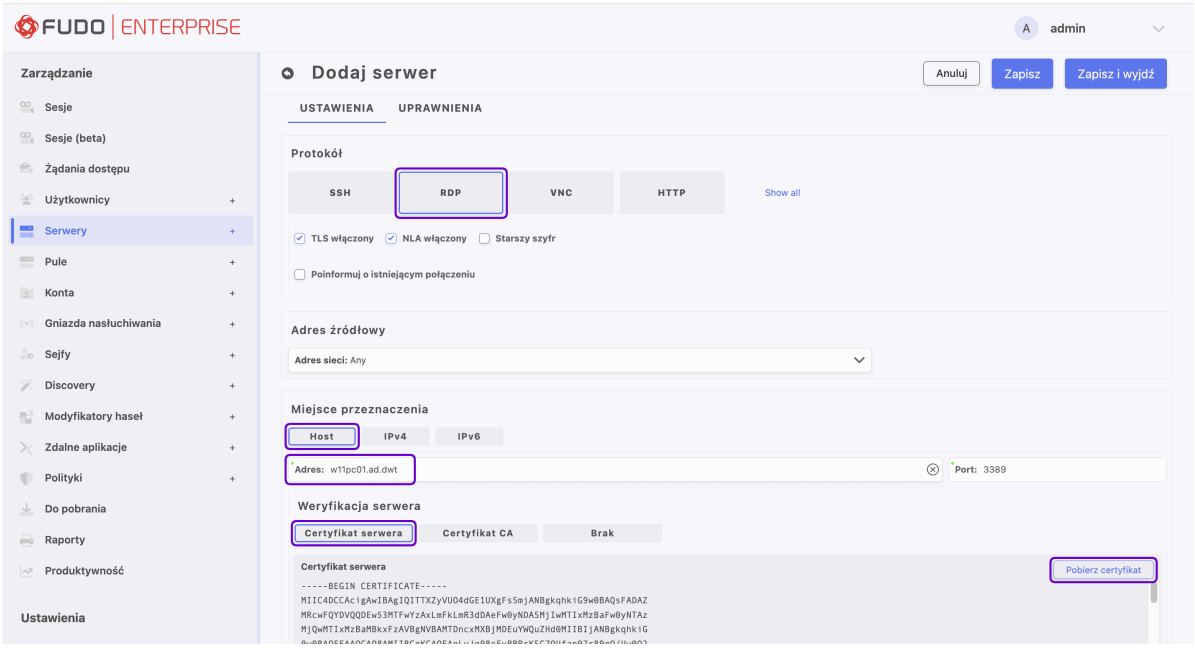
20.7.3 Konfiguracja serwera

Utwórz konfigurację serwera, na którym zlokalizowane jest konto lokalne:

1. Wybierz z lewego menu *Zarządzanie* > *Serwery* i kliknij + *Dodaj serwer*.
2. Wpisz unikalną nazwę dla tworzonego obiektu (np: `RDP_Server`).
3. Przejdź do sekcji *Ustawienia*.
4. W polu *Protokół* wybierz `RDP`.
5. W sekcji *Miejsce przeznaczenia* zdefiniuj serwer docelowy:

- Wybierz `Host`,
- W polu *Adres* wprowadź nazwę hosta wraz z domeną (np: `w11pc01.ad.dwt`).
- W polu *Port* podaj numer portu.

6. W sekcji *Weryfikacja serwera* wybierz opcję *Certyfikat serwera* i kliknij *Pobierz certyfikat*.
1. Kliknij *Zapisz i wyjdź*.



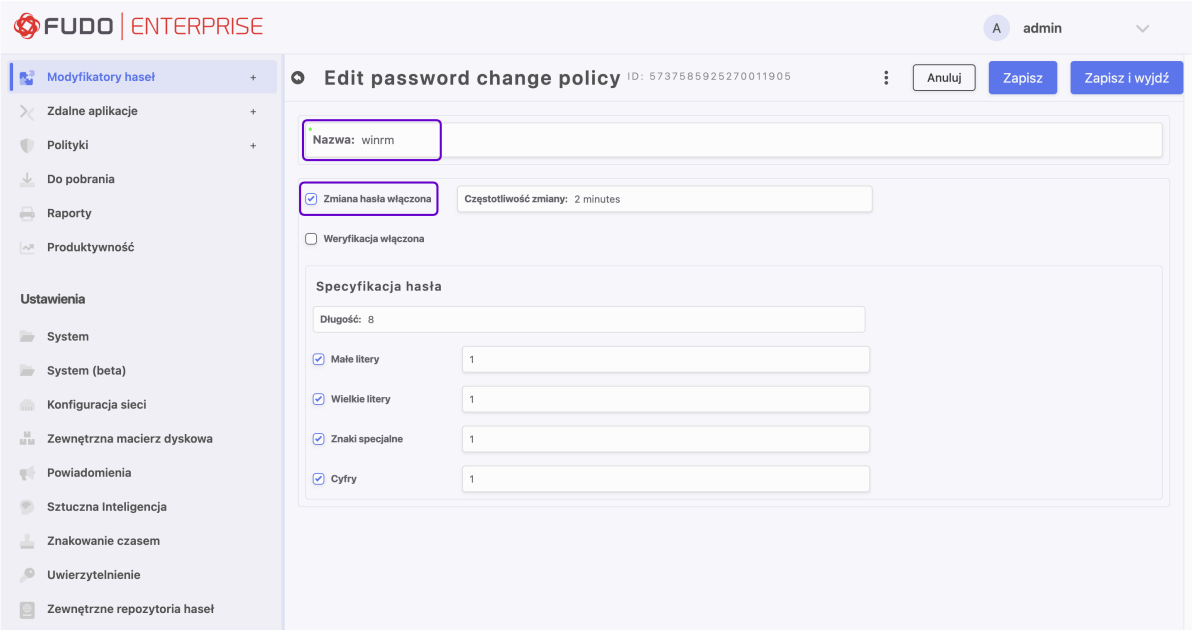
Uwaga

W opisywanym scenariuszu wymagane jest podanie nazwy hosta wraz z domeną. Nazwa ta zostanie wykorzystana w zmiennej `transport_host` modyfikatora haseł. Określenie serwera po adresie IPv4/IPv6 nie jest obsługiwane.

20.7.4 Dodawanie polityki zmiany haseł

Utwórz politykę haseł:

1. Wybierz *Zarządzanie* > *Modyfikatory haseł*.
2. Przejdź do zakładki *Polityki haseł* i kliknij *+ Dodaj politykę haseł*.
3. Wprowadź unikalną nazwę dla tworzonej polityki (np: `winrm`).
4. Wybierz opcję *Zmiana hasła włączona* i określ przedział czasu między każdą zmianą hasła.
5. Zdefiniuj złożoność hasła.



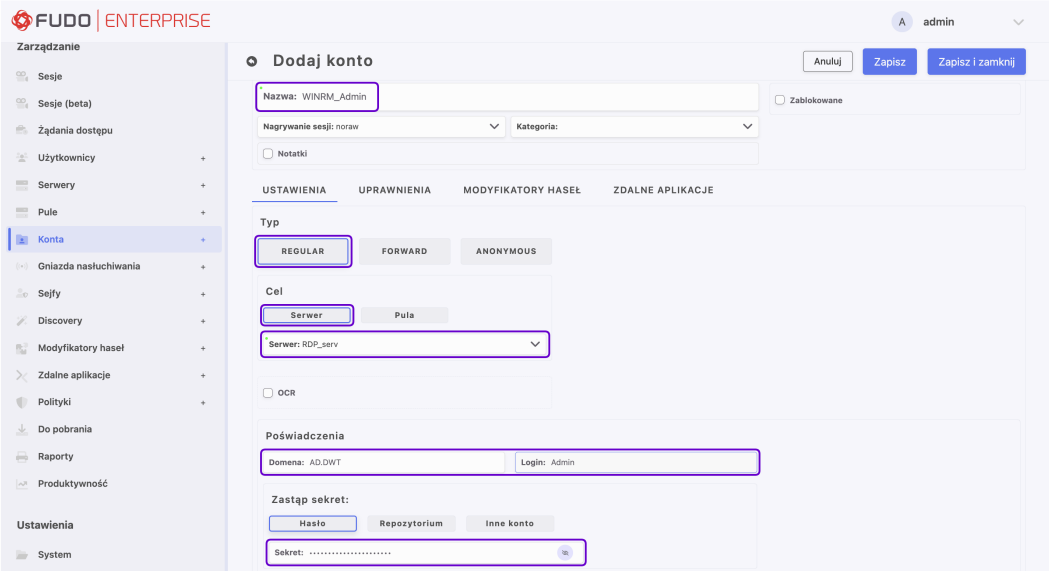
Uwaga

- Weryfikacja haseł w scenariuszu zmiany hasła dla konta domenowego za pomocą innego konta domenowego nie jest obsługiwana w bieżącej wersji Fudo Enterprise.
- Weryfikacja haseł działa przy scenariuszu zmiany hasła dla konta poza domeną.

20.7.5 Konto administratora

Dodaj konto, które będzie wykorzystywane podczas zmiany haseł na kontach lokalnych. Poniższy przykład opiera się na koncie typu regular domenowego użytkownika uprzywilejowanego do zmiany haseł.

1. Wybierz *Zarządzanie* > *Konta*, a następnie kliknij + *Dodaj konto*.
2. Wprowadź unikalną nazwę dla tworzonego obiektu (np: `WINRM_Admin`).
3. W zakładce *Ustawienia*, w polu *Typ*, naciśnij przycisk *REGULAR*.
4. W sekcji *Cel*, wybierz przycisk *Serwer*, następnie z listy wybierz utworzony w poprzednich krokach serwer RDP, na którym zlokalizowane jest konto lokalne (`RDP_Server`).
5. W sekcji *Poświadczenia*:
   - Podaj nazwę domeny (np: `AD.DWT`).
   - Podaj *Login* konta, które będzie wykorzystywane do zmiany haseł kont lokalnych (np: `Admin`).
   - W sekcji *Zastąp tajemnicę* kliknij przycisk odpowiadający jednej z pożądanych opcji uwierzytelnienia (np: *Hasło* i w polu *Sekret* wpisz hasło dla wspomnianego konta).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.



6. Kliknij *Zapisz i wyjdź*.

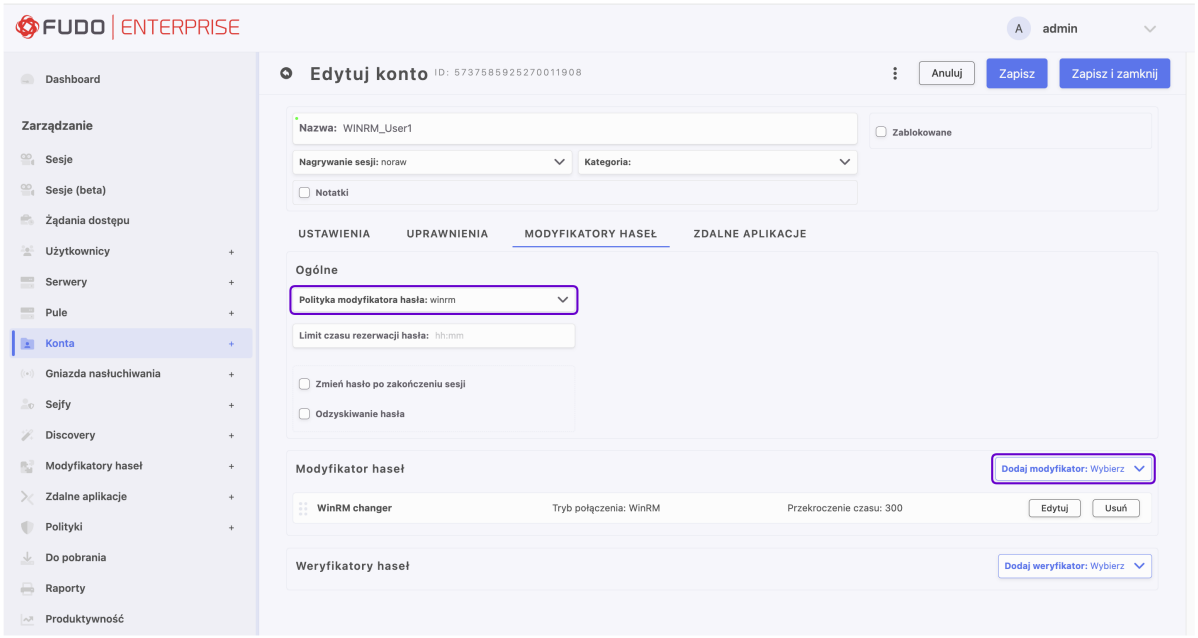
20.7.6 Konto dla którego będzie zmieniane hasło

Dodaj lokalne konto użytkownika, dla którego będzie zmieniane hasło. Poniższy przykład opiera się na koncie typu regular użytkownika lokalnego.

1. Wybierz *Zarządzanie* > *Konta*, a następnie kliknij + *Dodaj konto*.
2. Wprowadź unikalną nazwę dla tworzonego obiektu (np: `WINRM_User1`).
3. W zakładce *Ustawienia*, w polu *Typ*, naciśnij przycisk *REGULAR*.
4. W sekcji *Cel*, wybierz przycisk *Serwer*, następnie z listy wybierz utworzony w poprzednich krokach serwer RDP, na którym zlokalizowane jest konto lokalne (`RDP_Server`).
5. W sekcji *Poświadczenia*:
   - Podaj nazwę domeny (np: `AD.DWT`) - jeśli jest to konto domenowe.
   - Podaj *Login* konta lokalnego (np: `User1`).
   - W sekcji *Zastąp sekret* kliknij przycisk odpowiadający jednej z pożądanych opcji uwierzytelnienia (np: *Hasło* i w polu *Sekret* wpisz hasło dla konta lokalnego).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.

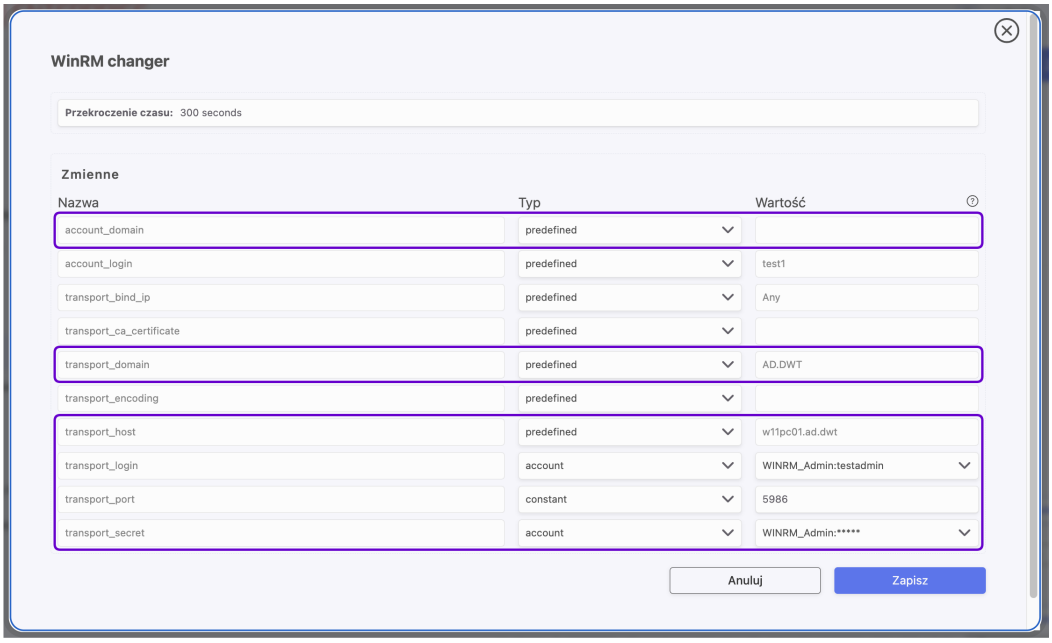
> **Uwaga**
>
> Podanie domeny w tym przypadku jest opcjonalne i zależy od tego, czy konto jest w domenie, czy poza domeną.

6. Przejdź do zakładki *MODYFIKATORY HASEŁ*.
7. W sekcji *Ogólne*, w polu *Polityka modyfikatora hasła* wybierz utworzoną wcześniej politykę (`winrm`).
8. W sekcji *Modyfikator haseł* z listy rozwijanej *Dodaj modyfikator* wybierz *WinRM changer*.



9. Do poprawnego działania modyfikatora wymagane jest skonfigurowanie poniższych pól:

   - `transport_domain` - wykorzystywane jest podczas uwierzytelnienia się kontem wykorzystywanym do zmiany hasła kont lokalnych lub domenowych. Domyślnie ustawione jest na opcję *predefiniowane*, przez co wykorzystywana jest nazwa domeny wpisana dla obecnie konfigurowanego konta. Dostępne są również opcje:
     - *stała* - umożliwia wprowadzenie stałej wartość dla nazwy domeny.
     - *konto* - umożliwia wskazanie konta, z którego pobierana jest wartość dla nazwy domeny.
   - `transport_login` - pole określające login konta uprzywilejowanego, które posłuży do zmiany hasła. W kolumnie *Typ* należy wybrać konto, następnie w kolumnie *Wartość* należy wybrać konto, które będzie wykorzystywane podczas zmiany haseł na kontach lokalnych. W przypadku tego scenariusza będzie to konto `WINRM_Admin`.
   - `transport_port` - port 5986, za pośrednictwem którego logujemy się do serwera, na którym będzie zmieniane hasło (wymagany port: `5986`).
   - `transport_secret` - pole określające sekret konta uprzywilejowanego, które posłuży do zmiany hasła. W kolumnie *Typ* należy wybrać konto, następnie w kolumnie *Wartość* należy wybrać konto, które będzie wykorzystywane podczas zmiany haseł na kontach lokalnych. W przypadku tego scenariusza będzie to konto `WINRM_Admin`.
   - `account_domain` - pole musi zostać wypełnione, jeśli chcemy skonfigurować password changer dla konta w domenie. Jeśli kontem, na którym chcemy zmieniać hasło, jest konto lokalne, pole to można pozostawić puste. Pole to domyślnie ustawione jest na opcję *predefiniowane*, przez co wykorzystywana jest nazwa domeny wpisana dla obecnie konfigurowanego konta.



10. Kliknij *Zapisz*, aby zamknąć okno dialogowe.
11. Kliknij *Zapisz i wyjdź*.

Tematy pokrewne:

- *Tworzenie konta typu regular*
- *Uwierzytelnienie*

20.8 Konfiguracja ograniczonej delegacji protokołu Kerberos dla serwera MSSQL(TDS)

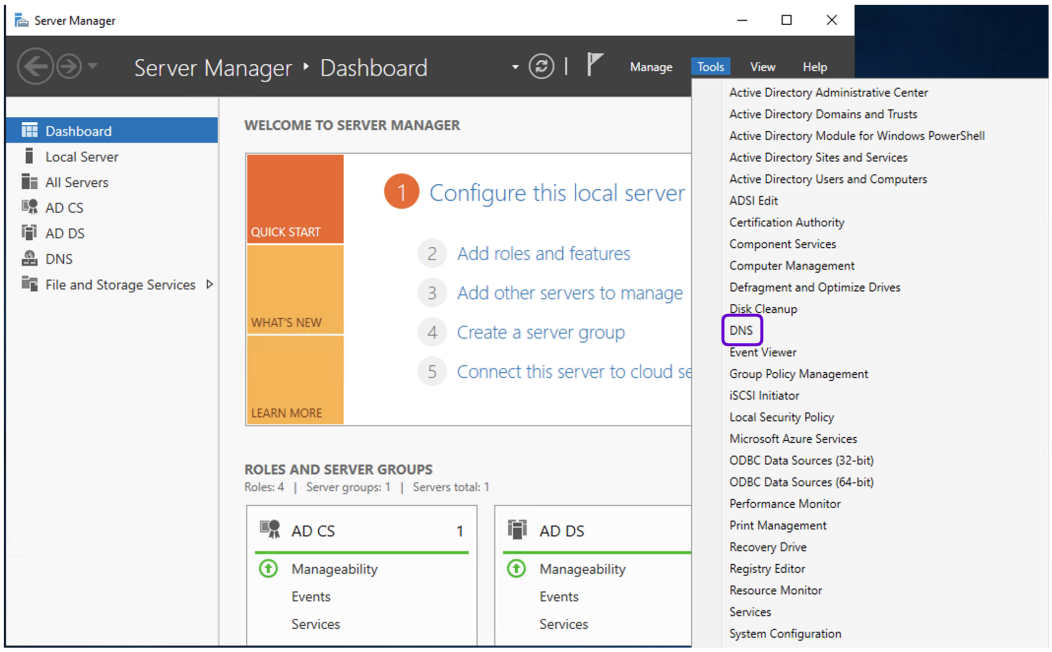
Uwaga

Jest to ogólna instrukcja, mająca na celu przybliżenie procesu konfigurowania usługi. Pewne aspekty mogą się różnić w zależności od konfiguracji środowiska Windows Server. Szczegółową instrukcję znajdziesz w dokumentacji Windows Server.

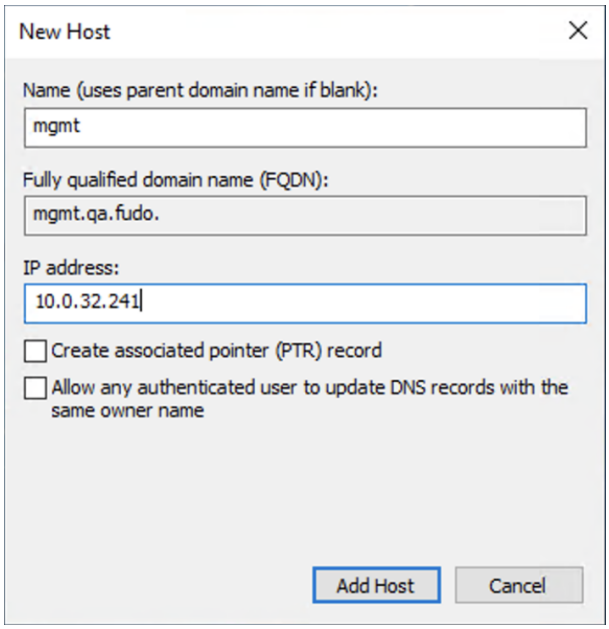
20.8.1 Konfiguracja uwierzytelniania Kerberos na serwerze Windows

Konfiguracja 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*.
4. Dodaj rekord A: kliknij prawym przyciskiem myszy na wybranej nazwie domeny i wybierz *New Host (A lub AAAAA)*.
5. Podaj *Nazwę* i *Adres IP* panelu administracyjnego Fudo Enterprise (np. `mgmt.qa.fudo, 10.0.32.241`).
6. Kliknij *Add Host*.

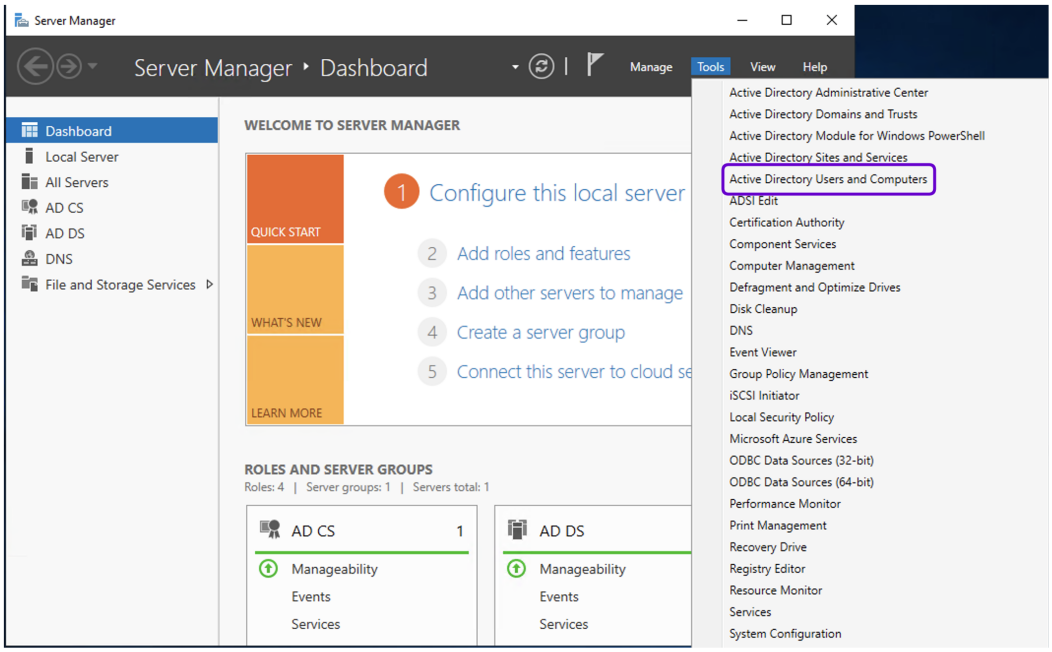


Tworzenie konta użytkownika serwisowego:

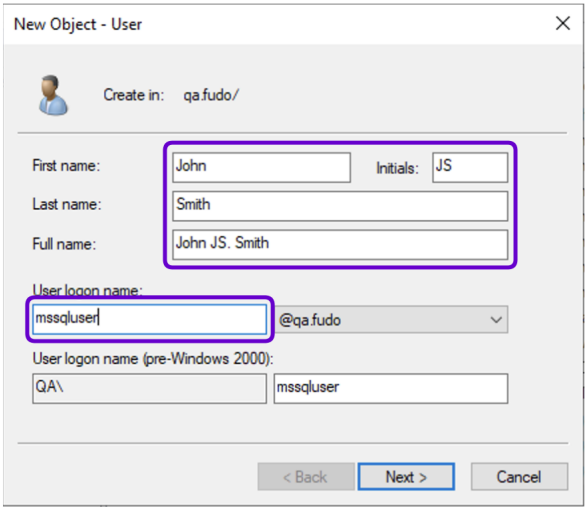
W tej sekcji dodajemy użytkownika serwisowego `mssqluser`, który będzie reprezentował serwis MSSQL w domenie.

1. Zaloguj się na serwer, na którym chcesz skonfigurować Kerberos, używając konta administratora.

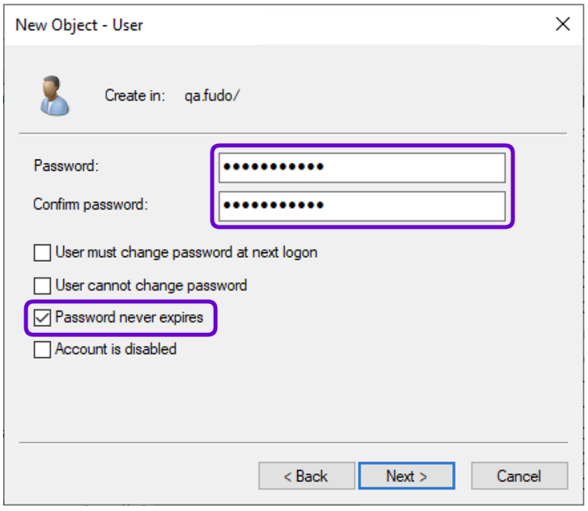
2. Uruchom aplikację *Server Manager*.
3. Kliknij przycisk *Tools* w prawym górnym rogu okna, aby rozwinąć listę menu, i wybierz *Active Directory Users and Computers*.



4. W oknie Menedżera przejdź do nazwy domeny lub wybranej grupy użytkowników i kliknij prawym przyciskiem myszy na katalogu *Użytkownicy*.
5. Wybierz *New* > *User*.
6. Utwórz użytkownika (np. Nazwa logowania użytkownika: `mssqluser`).



7. Kliknij *Next*.
8. Podaj hasło dla utworzonego użytkownika (np. `PaSSwOrD`) i zaznacz opcję *Hasło nigdy nie wygasa*.
9. Kliknij *Next*, a następnie *Finish*.



Dodanie SPN (Service Principal Name):

Wywołaj poniższe polecenie w konsoli PowerShell lub CMD:

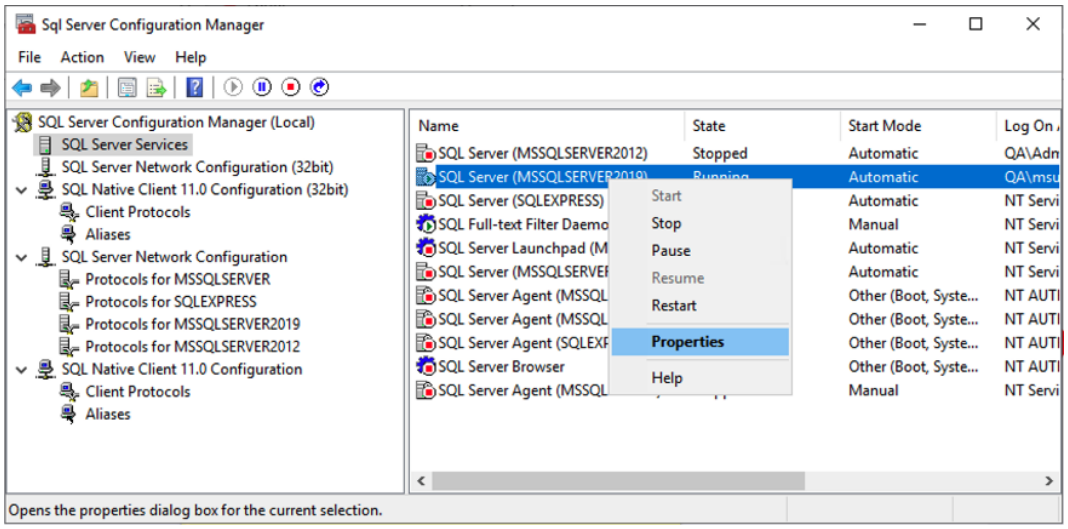
```
setspn -S <klasa usługi>/<nazwa serwera>.<domena>:<port>@<domena>
<konto serwisowe>
```

Przykład:

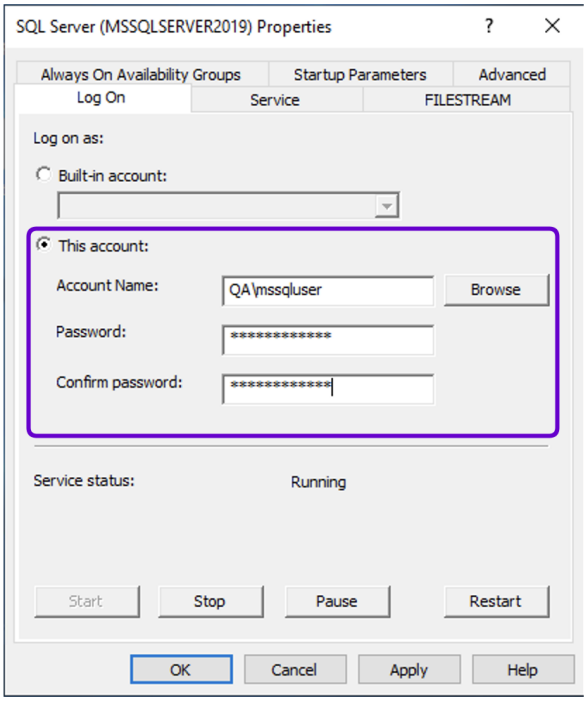
```
setspn -S MSSQLSvc/WIN2019-DC1.qa.fudo:1433@QA.FUDO mssqluser
```

SQL Server Configuration Manager:

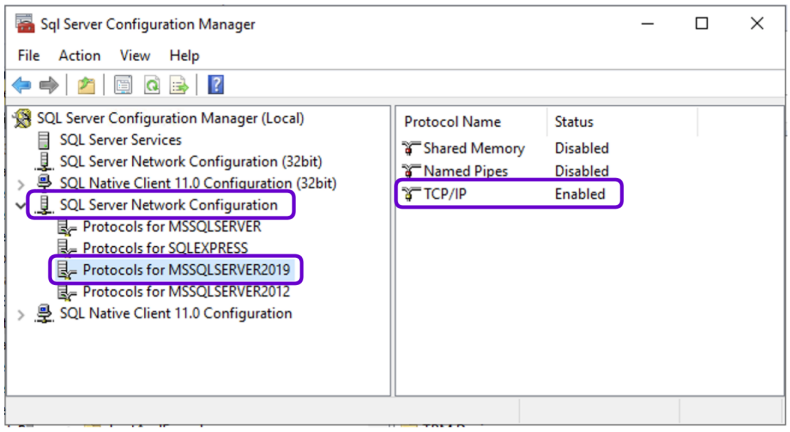
1. Uruchom *SQL Server Configuration Manager*.
2. Rozwiń *SQL Server Services*, wybierz serwer i otwórz okno *Properties*.



3. W zakładce *Log On* wprowadź dane uwierzytelniające konta `mssqluser`.



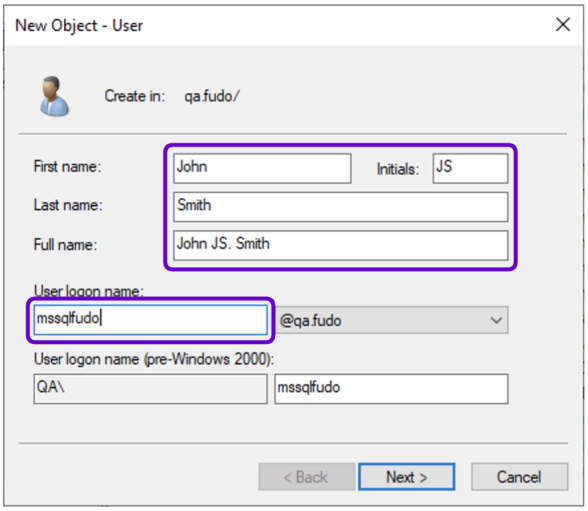
4. Rozwiń *SQL Server Network Configuration*, wybierz serwer i upewnij się, że połączenie przez *TCP/IP* jest włączone.



Tworzenie użytkownika serwisowego reprezentującego MSSQL na Fudo:

W tej sekcji dodajemy konto serwisowe `mssqlfudo`, które będzie reprezentować usługę MSSQL w Fudo Enterprise.

1. Uruchom aplikację *Server Manager*.
2. Kliknij przycisk *Tools* w prawym górnym rogu okna i wybierz *Active Directory Users and Computers*.
3. W oknie Menedżera przejdź do nazwy domeny lub wybranej grupy użytkowników i kliknij prawym przyciskiem myszy na katalogu *Użytkownicy*.
4. Wybierz *New* > *User*.
5. Utwórz użytkownika, który będzie korzystał z delegacji Kerberos do logowania na serwer MSSQL(TDS) (np. Nazwa logowania użytkownika: `mssqlfudo`).



6. Kliknij *Next*.
7. Podaj hasło dla utworzonego użytkownika (np. `PaSSwOrD`) i zaznacz opcję *Hasło nigdy nie wygasa*.
8. Kliknij *Next*, a następnie *Finish*.

Dodanie SPN dla użytkownika MSSQL na Fudo:

Wywołaj poniższe polecenie w konsoli PowerShell lub CMD:

```
setspn -S <klasa usługi>/<nazwa panelu admina Fudo>:<port>@<domena>
<konto serwisowe>
```

Przykład:

```
setspn -S MSSQLSvc/mgmt.qa.fudo:1433@QA.FUDO mssqlfudo
```

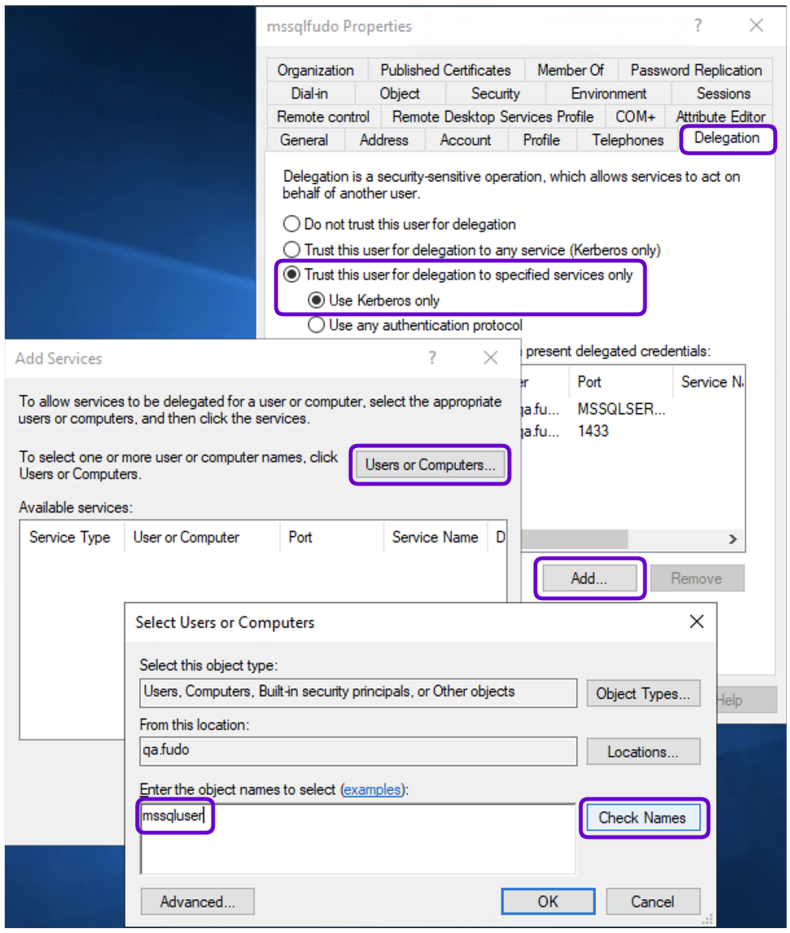
Delegacja Kerberos

Uwaga

- Po ustawieniu SPN dla użytkownika `mssqlfudo` w oknie edycji użytkownika pojawi się nowa zakładka *Delegation*.
- Jeśli zakładka *Delegation* nie jest widoczna, spróbuj odświeżyć konsolę *Active Directory Users and Computers*.

1. Kliknij prawym przyciskiem myszy na konto `mssqlfudo` (utworzone w poprzednich krokach) w oknie Active Directory Users and Computers i wybierz *Properties*.
2. Przejdź do zakładki *Delegation*.
3. Zaznacz *Trust this user for delegation to specified services only*.
4. Wybierz opcję *Use Kerberos only*.
5. Dodaj usługi:
   - Kliknij przycisk *Add*.

- W oknie *Select Users or Computers* wpisz `mssqluser` i kliknij *Check Names*, aby upewnić się, że nazwa jest prawidłowa.
- Kliknij *OK*, aby kontynuować.



6. Wybierz usługi do delegacji:
   - W oknie *Add Services* pojawi się lista SPN-ów powiązanych z kontem `mssqluser`.
   - Możesz wybrać wszystkie dostępne usługi lub wskazać konkretne SPN-y.
   - Kliknij *OK*, aby zatwierdzić wybór.
7. Kliknij *Apply*, a następnie *OK*, aby zapisać ustawienia.
8. Jeśli zmiany nie są natychmiast widoczne, odśwież konsolę *Active Directory Users and Computers* naciskając *F5* lub klikając prawym przyciskiem myszy na katalog *Użytkownicy* i wybierając *Refresh*.

Generowanie Keytab:

1. Wywołaj 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
```

   - Przykład dla tego przypadku:

```
ktpass -princ MSSQLSvc/mgmt.qa.fudo:1433@QA.FUDO -mapuser
QA\mssqlfudo   -pass PaSSwOrD -pType KRB5_NT_PRINCIPAL -out
mssqlfudo.keytab
```

2. Skopiuj wygenerowany plik Keytab na stację roboczą, na której będziesz konfigurować Fudo.

> **Uwaga**
>
> Jest to alternatywna metoda uwierzytelniania zamiast hasła. Hasło musi być zgodne z tym podanym podczas tworzenia użytkownika. W przypadku zmiany hasła użytkownika, jego plik keytab stanie się nieaktywny.

20.8.2 Konfiguracja Fudo Enterprise

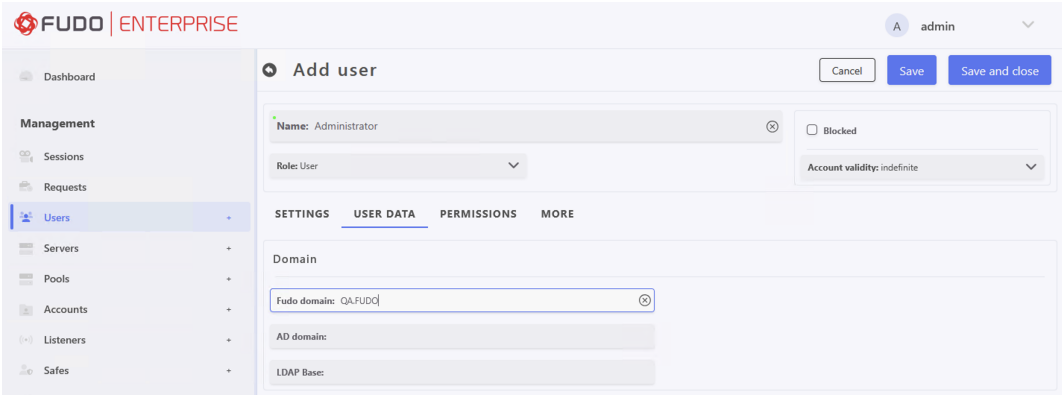
Konfiguracja DNS:

1. Przejdź do *Ustawienia* > *Konfiguracja sieci*.
2. Przełącz się na zakładkę *Nazwa i DNS*.
3. 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 dodać nowy serwer DNS.
   - Wprowadź adres IP serwera DNS (np. `10.0.242.100`).
   - Kliknij *Zapisz*.

Tworzenie użytkownika w Fudo:

1. Wybierz *Zarządzanie* > *Użytkownicy*, a następnie kliknij *+ Dodaj użytkownika*.
2. Wprowadź nazwę użytkownika, która odpowiada nazwie utworzonej wcześniej w Active Directory (np. `Administrator`).
3. Wybierz rolę `user`.
4. W zakładce *Ustawienia*, w sekcji *Sejfy*, wybierz *main*, aby przyznać dostęp do Panelu Administratora Fudo Enterprise.
5. Kliknij *Zapisz*.
6. Przejdź do zakładki *Dane użytkownika*, wprowadź *Domena Fudo* (np. `QA.FUDO`).

> **Uwaga**
>
> Domena Fudo powinna odpowiadać nazwie domeny podanej w bilecie Kerberos.



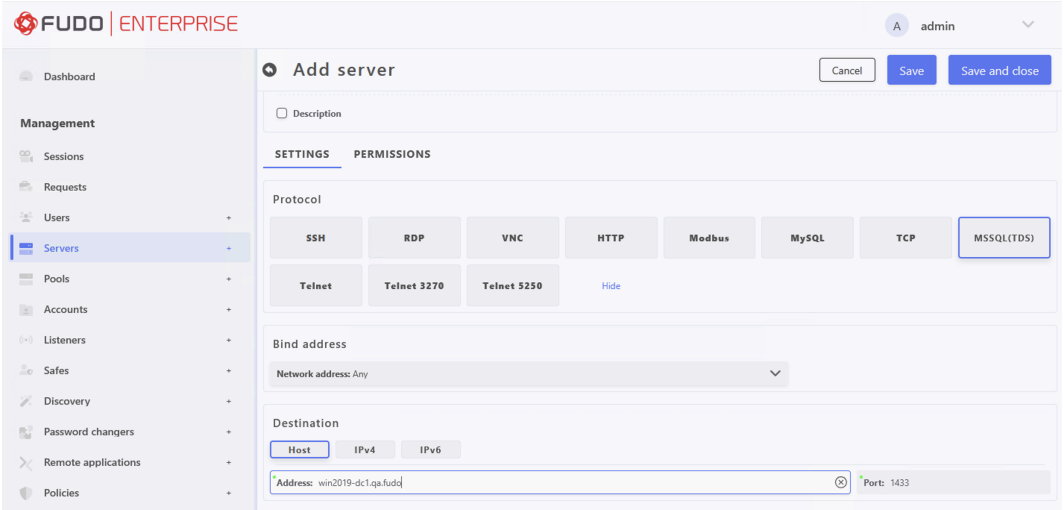
7. Uzupełnij pozostałe parametry w zależności od potrzeb konfiguracji. Więcej informacji znajdziesz w rozdziale *Dodawanie użytkownika*.
8. Kliknij *Zapisz i wyjdź*.

Konfiguracja serwera MSSQL(TDS):

1. Wybierz *Zarządzanie* > *Serwery*, a następnie kliknij + *Dodaj serwer*.
2. Wprowadź unikalną nazwę serwera (np. `tds`).
3. W sekcji *Ustawienia*, na liście protokołów, wybierz `MSSQL(TDS)`.
4. W sekcji *Adres źródłowy* wybierz `Host` i wprowadź nazwę hosta serwera (np. `win2019-dc1.qa.fudo`).

> **Uwaga**
>
> Aby uwierzytelnianie do systemów docelowych z wykorzystaniem protokołu Kerberos działało poprawnie, pole **Destination** w konfiguracji serwera musi być ustawione na `Host` (nazwa hosta). Kerberos opiera się na rozwiązywaniu SPN (Service Principal Name) na podstawie nazwy hosta. Skonfigurowanie pola Destination przy użyciu adresu IP spowoduje niepowodzenie uwierzytelniania.

5. Wprowadź port: `1433`.



6. Kliknij *Zapisz i wyjdź*.

Konfiguracja konta:

1. Wybierz *Zarządzanie* > *Konta*, a następnie kliknij + *Dodaj konto*.
2. Zdefiniuj unikalną nazwę obiektu (np. `tds:forward`).
3. W sekcji *Typ* wybierz *FORWARD*.
4. W sekcji *Cel* kliknij przycisk *Serwer* i z rozwijanej listy wybierz serwer utworzony w poprzednim kroku (np. `tds`), aby przypisać konto do tego serwera.
5. W sekcji *Zastąp sekret* wybierz *Brak*.
6. Kliknij *Zapisz*.

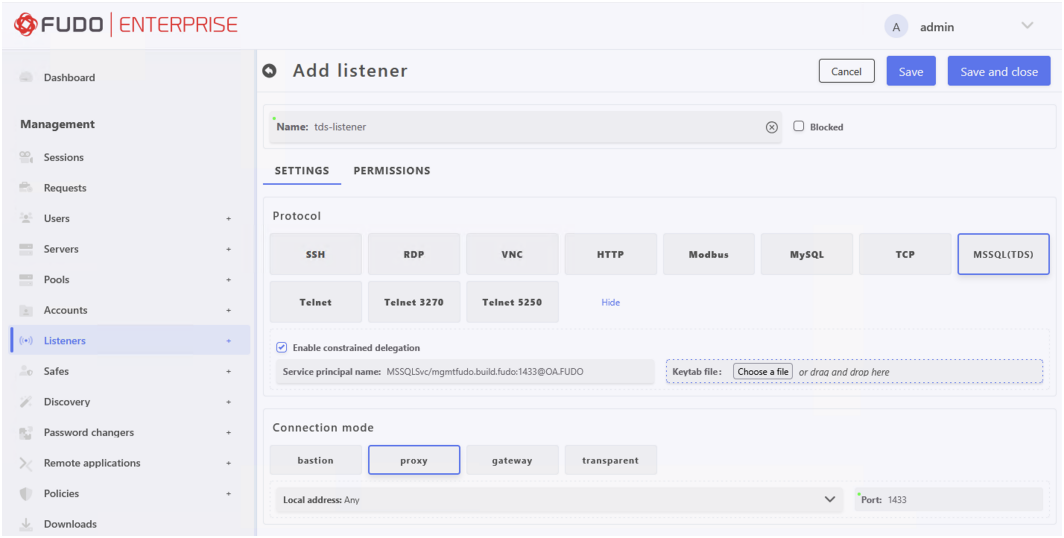
> **Uwaga**
>
> Typo konta *forward* jest zalecany w tym scenariuszu, ponieważ w przypadku delegacji *S4U2Proxy* konieczne jest posługiwanie się istniejącym biletem użytkownika do uwierzytelniania względem serwera TDS. Dlatego zawsze używana jest nazwa użytkownika, który zalogował się do Fudo Enterprise, natomiast jakiekolwiek poświadczenia wprowadzone dla konta nie zostaną wykorzystane.

Konfiguracja gniazda nasłuchiwania:

1. Wybierz *Zarządzanie* > *Gniazda nasłuchiwania*, a następnie kliknij + *Dodaj gniazdo nasłuchiwania*.
2. Wprowadź unikalną nazwę listenera (np. `tds-listener`).
3. Przejdź do zakładki *USTAWIENIA* i w polu *Protokół* wybierz przycisk `MSSQL(TDS)`.
4. Zaznacz opcję *Włącz ograniczoną delegację*.
5. W polu *Service principal name* wprowadź: `MSSQLSvc/mgmt.qa.fudo:1433@QA.FUDO`.
6. Prześlij plik Keytab.
7. W sekcji *Tryb połączenia* wybierz `proxy`.

> **Uwaga**
>
> Możliwe jest również użycie trybu `bastion`, jednak w tym trybie nie można używać loginów bastionowych.

8. Ustaw lokalny adres (np. `Any`) oraz port `1433`.



9. Kliknij *Zapisz i wyjdź*.

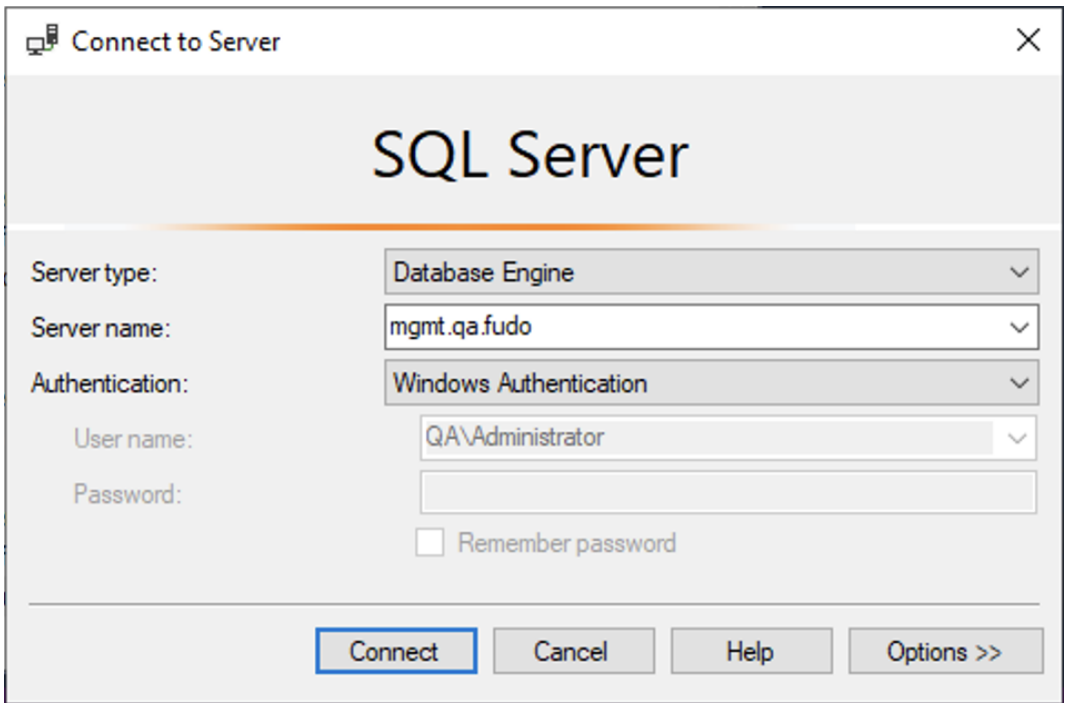
Konfiguracja Safe:

1. Wybierz *Zarządzanie* > *Sejfy*, a następnie kliknij + *Dodaj sejf*.
2. Wprowadź unikalną nazwę Safe (np. `tds-safe`).
3. Kliknij Zapisz, aby zapisać obiekt i przejść do dalszej konfiguracji.
4. Przejdź do zakładki *Użytkownicy*, aby przypisać użytkowników z dostępem do kont przypisanych do tego Safe.
   - Kliknij Zarządzaj użytkownikami.
   - Zaznacz pole wyboru przed nazwami użytkowników, aby umożliwić im dostęp do serwera przez monitorowany Safe (np. `Administrator`).
   - Kliknij Zapisz, aby zamknąć okno modalne.
5. Wybierz zakładkę *Konta*, aby dodać konta dostępne w ramach tego Safe.
   - Kliknij Zarządzaj kontami.
   - Zaznacz pole wyboru przed nazwami kont, aby dodać je do Safe (np. `tds:forward`).
   - Kliknij Zapisz, aby zamknąć okno modalne.
6. Kliknij Zapisz i wyjdź, aby zapisać konfigurację Safe.

Nawiązanie połączenia:

Aby nawiązać połączenie:

1. Uruchom aplikację klienta SQL.
2. Wybierz *File* > *Connect object explorer...*.
3. W polu *Server name* podaj nazwę panelu administracyjnego Fudo Enterprise ustawioną w wpisie DNS: *mgmt.qa.fudo*.
4. Z listy *Authentication* wybierz *Windows Authentication*.
5. Kliknij *Connect*.



Uwaga

Logowanie przy użyciu trybu *SQL Server Authentication* jest również możliwe, jeśli listener ma włączoną ograniczoną delegację.

Powiązane tematy:

- *Dodawanie serwera MS SQL*
- *Konfigurowanie gniazda nasłuchiwania MS SQL*
- *Uwierzytelnienie*

20.9 Nawiązywanie połączeń z serwerami przez tunel SSH w Fudo Enterprise

W tym rozdziale opisano sposób zestawiania połączeń z różnymi typami serwerów (SSH, Oracle, HTTP) za pośrednictwem tunelu SSH w Fudo Enterprise. Instrukcja krok po kroku przedstawia konfigurację wymaganych obiektów (użytkownika, gniazda nasłuchiwania, serwera, konta, sejfu), konfigurację klienta PuTTY oraz sposób inicjowania połączeń z poziomu terminala, przeglądarki lub dedykowanego klienta – w zależności od rodzaju zasobu.

20.9.1 Wymagania ogólne

Aby nawiązać połączenie przez tunel SSH w Fudo Enterprise, należy utworzyć następujące obiekty:

- **Użytkownik** uprawniony do nawiązywania połączeń,
- **Gniazdo nasłuchiwania** typu `Tunel`,
- **Serwer** docelowy (SSH, TCP lub HTTP),

- **Konto** służące do uwierzytelnienia na serwerze docelowym,
- **Sejf** zawierający powyższe obiekty.

20.9.1.1 Nawiązywanie połączenia SSH

Konfiguracja użytkownika

1. Przejdź do *Zarządzanie* > *Użytkownicy* i kliknij + *Dodaj użytkownika*.
2. Podaj nazwę (np. `Tunnel_User`) i kliknij *Zapisz*.
3. Wybierz metodę uwierzytelnienia użytkownika:
   - Wybierz np: *Hasło statyczne* z listy rozwijanej *Dodaj metodę uwierzytelnienia*.
   - Wpisz hasło dla tworzonego użytkownika (np: `TestPassw0rd`).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.
4. Kliknij *Zapisz i wyjdź*.

Tworzenie gniazda nasłuchiwania

1. Wybierz z lewego menu **Zarządzanie** > **Gniazda nasłuchiwania** i kliknij + **Dodaj gniazdo nasłuchiwania**.
2. Wprowadź unikalną nazwę (np: `SSH_Tunnel`).
3. Przejdź do zakładki **Ustawienia** i w polu **Protokół** wciśnij przycisk **SSH**.
4. W sekcji **Tryb połączenia** wybierz **Tunel**.
5. Z listy **Adres lokalny** wybierz adres IP i port (np: `3455`).
6. Kliknij **Zapisz**.

> **Uwaga**
>
> W polu **Klucze** widoczne są wygenerowane klucze SSH, TLS i Standard RDP Security oraz certyfikat TLS wymagane do prawidłowej pracy gniazda typu „Tunel".

Konfiguracja serwera SSH

1. Wybierz z lewego menu **Zarządzanie** > **Serwery** i kliknij + **Dodaj serwer**.
2. Wprowadź nazwę (np: `SSH_Tunnel_Server`).
3. W sekcji **Ustawienia**, wybierz **SSH** jako protokół.
4. W sekcji **Miejsce przeznaczenia**: - Wybierz **Host, IPv4** lub **IPv6**. - Wprowadź adres i port (np: `192.168.0.100`, port: `22`).
5. Kliknij **Zapisz i wyjdź**.

Konfiguracja konta

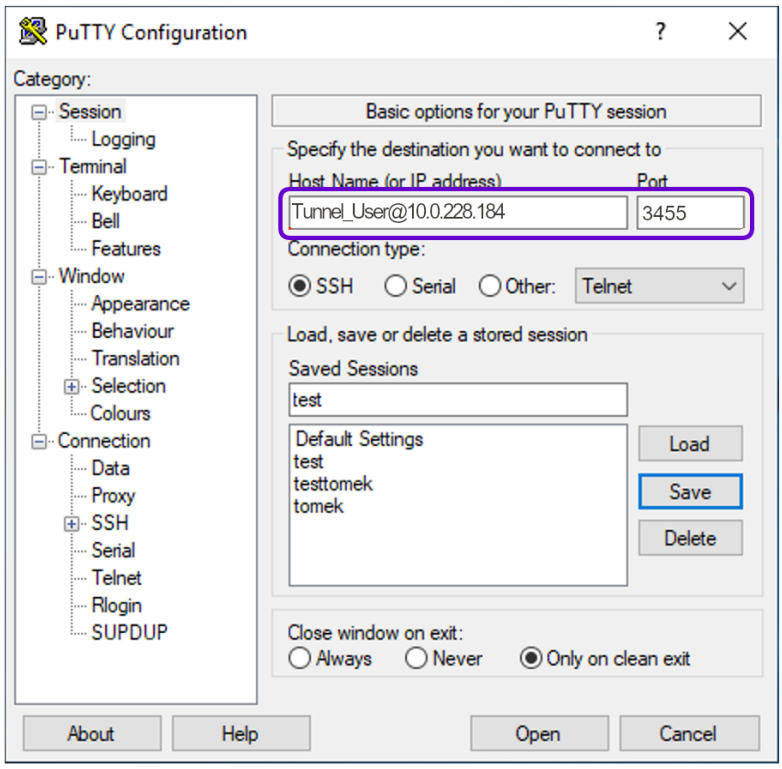
1. Wybierz **Zarządzanie** > **Konta**, kliknij + **Dodaj konto**.
2. Podaj nazwę (np: `Tunnel_Account`).
3. W zakładce **Ustawienia**, w polu **Typ**, wybierz **REGULAR**.
4. W sekcji **Cel**, wybierz serwer `SSH_Tunnel_Server`.
5. W sekcji **Dane uwierzytelniające**: - Wprowadź login (np: `admin`). - Kliknij przycisk w sekcji **Zastąp tajemnicę**, wybierz np: **Hasło**, i podaj hasło.
6. Kliknij **Zapisz**, a następnie **Zapisz i wyjdź**.

Konfiguracja sejfu

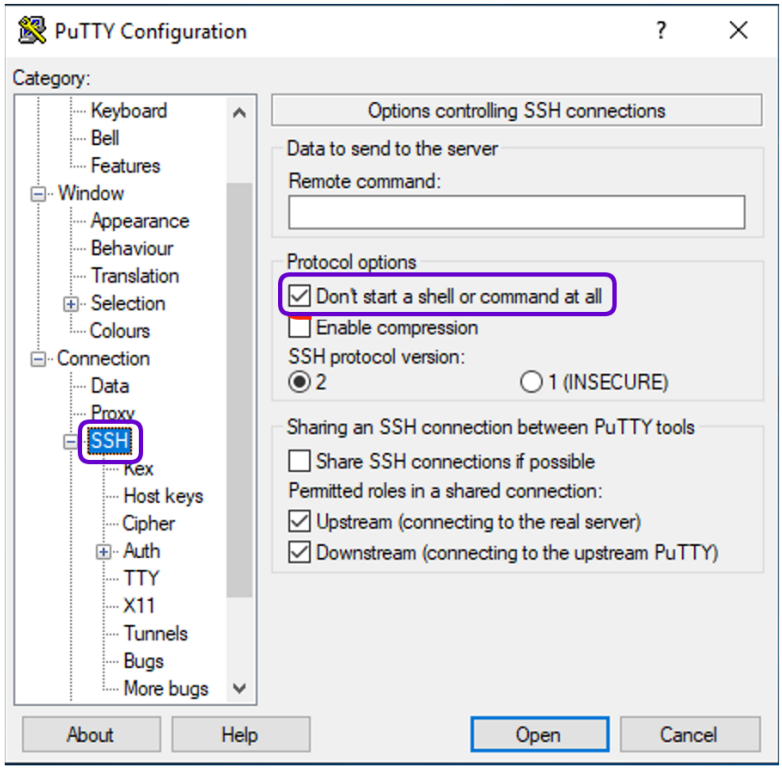
1. Wybierz **Zarządzanie** > **Sejfy** i kliknij + **Dodaj sejf**.
2. Wprowadź nazwę (np: `Tunnel_Safe`), kliknij **Zapisz**.
3. W zakładce **Użytkownicy**, kliknij **Zarządzaj użytkownikami** i zaznacz użytkownika `Tunnel_User`.
4. Kliknij **Zapisz**.
5. W zakładce **Konta**, kliknij **Zarządzaj kontami** i zaznacz `Tunnel_Account`.
6. Kliknij **Zapisz**.
7. Wybierz `Tunnel_Account`, kliknij **Zarządzaj gniazdami nasłuchiwania**, wybierz `SSH_Tunnel`.
8. Kliknij **Zapisz**, a następnie **Zapisz i zamknij**.

Konfiguracja PuTTY

1. Uruchom PuTTY.
2. W polu **Host Name** wpisz `<Fudo_user>@<Fudo_IP_address>`, czyli w tym przypadku `Tunnel_User@10.0.228.184`.
3. W polu **Port** podaj port gniazda nasłuchiwania typu *Tunel* utworzonego we wcześniejszych krokach (w tym przypadku `3455`).



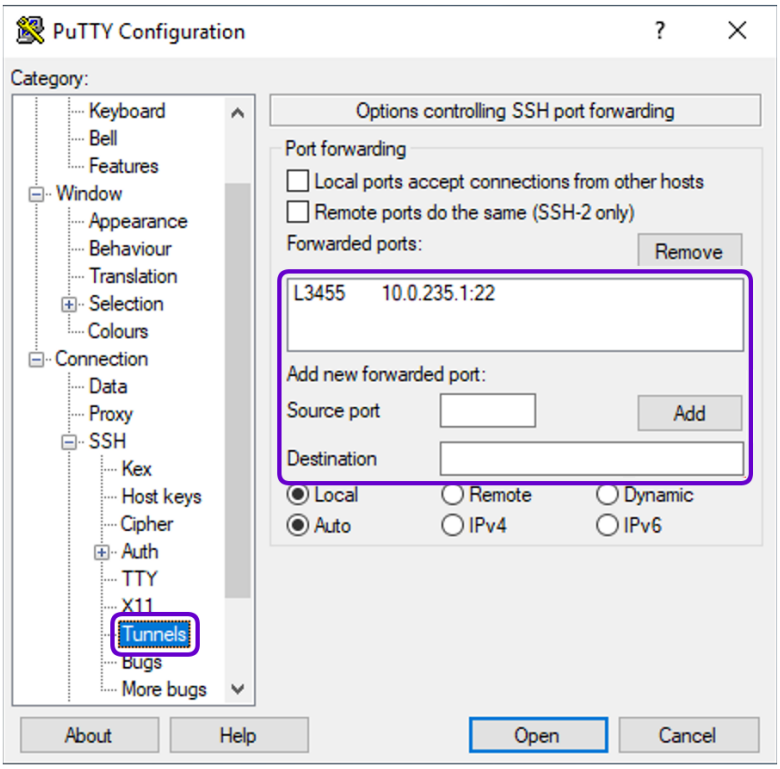
4. Przejdź do zakładki **SSH** i zaznacz opcję **Don't start a shell or command at all**.



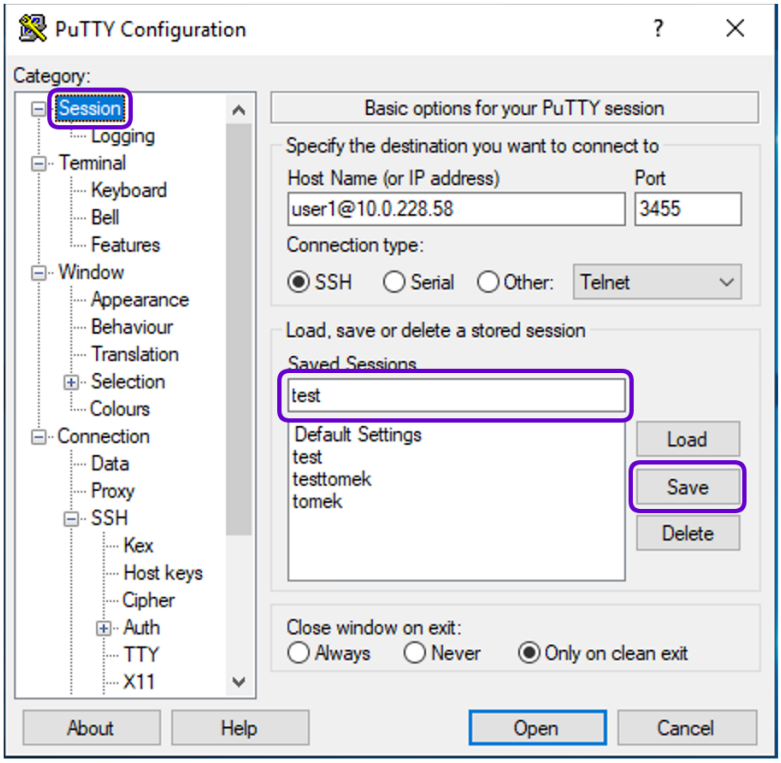
5. Przejdź do zakładki **Tunnels** i dodaj przekierowanie portów (**Forwarded ports**):
   - W polu **Source port** wpisz numer portu, który chcesz przekazać (np: 3455).
   - W polu **Destination** wpisz adres serwera docelowego oraz port w formacie

`<destination_server_address>:<port>` (w tym przypadku `192.168.0.100:22`).

- Kliknij przycisk **Add**.



6. Wróć do zakładki **Sessions**, zapisz konfigurację.



7. Kliknij **Open**.

8. W wyświetlonym terminalu wpisz hasło użytkownika Fudo utworzonego na początku instrukcji (`TestPassw0rd`).
9. Tunel został zestawiony.
10. Uruchom nowe okno terminala i wpisz komendę w podanym poniżej formacie, aby nawiązać połączenie z serwerem `192.168.0.100` przez zestawiony tunel.

```
ssh -l "<Fudo_user>#<Server_user>#<Server_address>" localhost -p <Tunnel_
↪listener_port>
```

Przykład:

```
ssh -l "Tunnel_User#admin#192.168.0.100" localhost -p 3455
```

Połączenie bez uycia PuTTY

Połączenie przy użyciu tunelu można również zestawić bez pośrednictwa PuTTY używając w terminalu poniższych komend:

- Zestawienie tunelu SSH:

```
ssh -N -l <Fudo_user> <IP_Fudo> -p <Listener_port_tunnel> -L
↪<Listener_port_tunnel>:<Server_address>:<server_port>
```

- Nawiązanie połączenia przez zestawiony tunel SSH:

```
ssh -l '<Fudo_user>#<server_user>#<server_address>' localhost -p
↪<Listener_port_tunnel>
```

Wyjaśnienie opcji:

- `-N`: umożliwia ustanowienie połączenia SSH bez uruchamiania zdalnych komend ani otwierania powłoki.
- `-l`: pozwala określić nazwę użytkownika, z którą zostanie nawiązane połączenie SSH.
- `-p`: określa port, na którym nasłuchuje serwer SSH.

Można również rozważyć użycie poniższych opcji:

- `-f`: uruchamia połączenie SSH w tle, często używane z opcją `-N` do tunelowania.
- `-n`: przekierowuje standardowe wejście (stdin) na `/dev/null`, co jest przydatne przy pracy w tle.

Przykład:

```
ssh -N -l Tunnel_User 10.0.228.184 -p 3455 -L 3455:192.168.0.100:22
ssh -l 'Tunnel_User#admin#192.168.0.100' localhost -p 3455
```

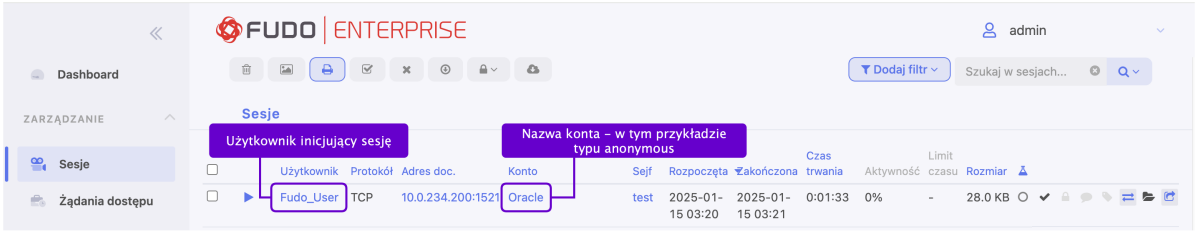
Uwaga

Jeśli serwer docelowy jest skonfigurowany do używania odwrotnego tunelu SSH (opcja **Use SSH tunnel** w konfiguracji serwera), zobacz *Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel*.

Wygląd listy sesji

Po nawiązaniu połączenia, w zakładce **Zarządzanie** > **Sesje** pojawi się wpis dotyczący sesji zestawionej wewnątrz tunelu. Widoczne będą następujące informacje:

- Nazwa użytkownika Fudo (również jeśli użyto konta typu anonymous),
- Protokół sesji,
- Adres serwera docelowego,
- Nazwa konta użytego do nawiązania połączenia,
- Nazwa sejfu,
- Czas rozpoczęcia i zakończenia sesji,
- Czas trwania sesji.



20.9.1.2 Nawiązywanie połączenia HTTP

Konfiguracja użytkownika

1. Przejdź do *Zarządzanie* > *Użytkownicy* i kliknij *+ Dodaj użytkownika*.
2. Podaj nazwę (np. `Tunnel_User`) i kliknij *Zapisz*.
3. Wybierz metodę uwierzytelnienia użytkownika:
   - Wybierz np: *Hasło statyczne* z listy rozwijanej *Dodaj metodę uwierzytelnienia*.
   - Wpisz hasło dla tworzonego użytkownika (np: `TestPassw0rd`).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.
4. Kliknij *Zapisz i wyjdź*.

Tworzenie gniazda nasłuchiwania

1. Wybierz z lewego menu **Zarządzanie** > **Gniazda nasłuchiwania** i kliknij + **Dodaj gniazdo nasłuchiwania**.
2. Wprowadź unikalną nazwę (np: `HTTP_Tunnel`).
3. Przejdź do zakładki **Ustawienia** i w polu **Protokół** wciśnij przycisk **SSH**.
4. W sekcji **Tryb połączenia** wybierz **Tunel**.
5. Z listy **Adres lokalny** wybierz adres IP i port (np: `3455`).
6. Kliknij **Zapisz**.

Uwaga

W polu **Klucze** widoczne są wygenerowane klucze SSH, TLS i Standard RDP Security oraz certyfikat TLS wymagane do prawidłowej pracy gniazda typu „Tunel".

Konfiguracja serwera HTTP

Utwórz konfigurację serwera TCP:

1. Wybierz z lewego menu **Zarządzanie** > **Serwery** i kliknij + **Dodaj serwer**.
2. Wprowadź nazwę (np: `HTTP_Tunnel_Server`).
3. W sekcji **Ustawienia**, wybierz **HTTP** jako protokół.
4. W sekcji **Miejsce przeznaczenia**: - Wybierz **Host**. - Wprowadź adres i port (np: `twitter.com`, port: `443`).
5. Kliknij **Zapisz i wyjdź**.

Konfiguracja konta

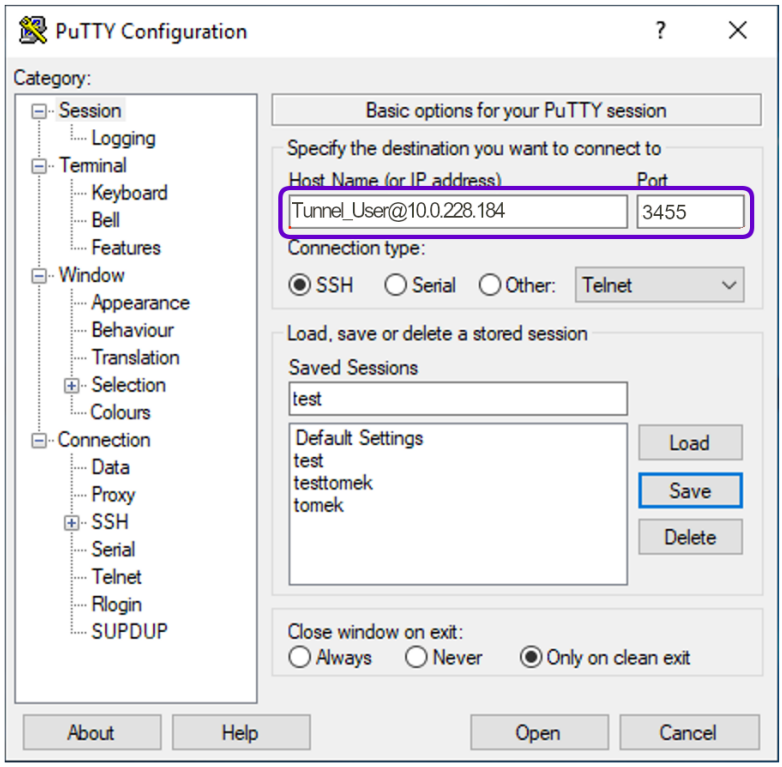
1. Wybierz **Zarządzanie** > **Konta**, kliknij + **Dodaj konto**.
2. Podaj nazwę (np: `HTTP_Tunnel_Account`).
3. Ustaw opcję **Nagrywanie sesji** na **noraw**.
4. W zakładce **Ustawienia**, w polu **Typ**, wybierz **FORWARD**.
5. W sekcji **Cel**, wybierz serwer `HTTP_Tunnel_Server`.
6. W sekcji **Zastąp sekret** wybierz **brak**.
7. Kliknij **Zapisz**, a następnie **Zapisz i wyjdź**.

Konfiguracja sejfu

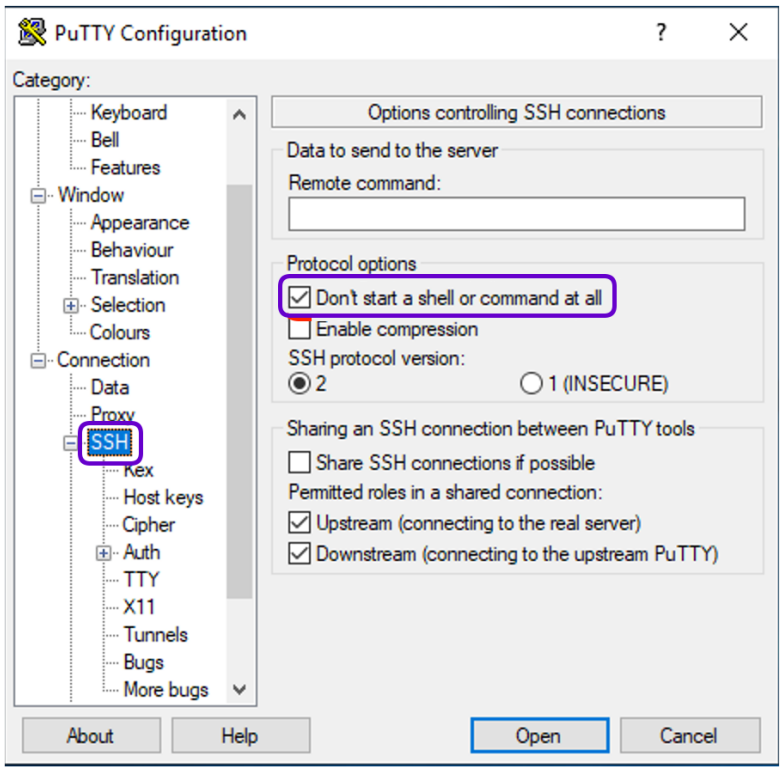
1. Wybierz **Zarządzanie** > **Sejfy** i kliknij + **Dodaj sejf**.
2. Wprowadź nazwę (np: `Tunnel_Safe`), kliknij **Zapisz**.
3. W zakładce **Użytkownicy**, kliknij **Zarządzaj użytkownikami** i zaznacz użytkownika `Tunnel_User`.
4. Kliknij **Zapisz**.
5. W zakładce **Konta**, kliknij **Zarządzaj kontami** i zaznacz `HTTP_Tunnel_Account`.
6. Kliknij **Zapisz**.
7. Wybierz `HTTP_Tunnel_Account`, kliknij **Zarządzaj gniazdami nasłuchiwania**, wybierz `HTTP_Tunnel`.
8. Kliknij **Zapisz**, a następnie **Zapisz i zamknij**.

Konfiguracja PuTTY

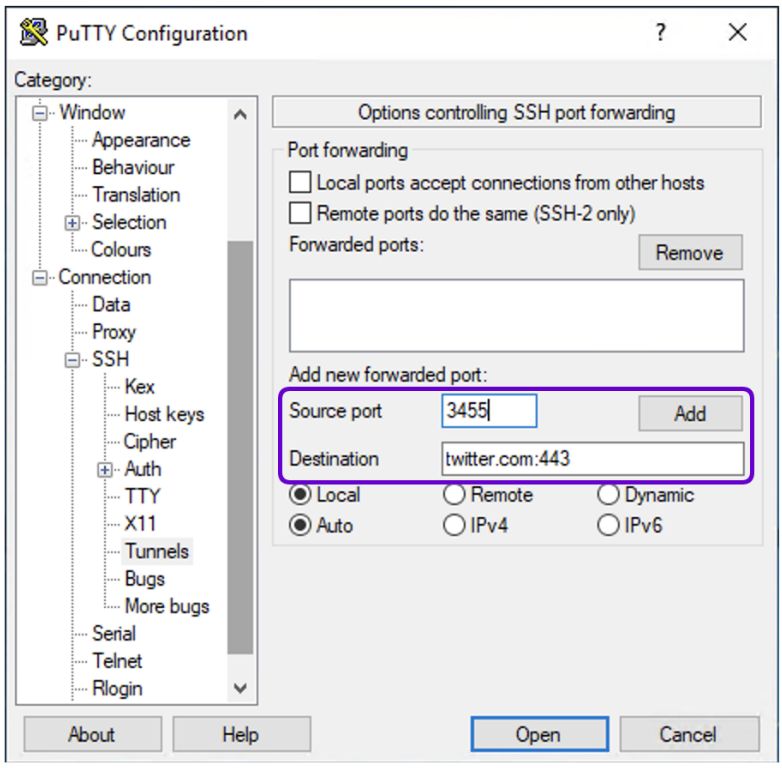
1. Uruchom aplikację **PuTTY**.
2. W polu **Host Name** wpisz `<Fudo_user>@<Fudo_IP_address>`, czyli w tym przypadku `Tunnel_User@10.0.228.184`.
3. W polu **Port** podaj port gniazda nasłuchiwania typu *Tunel* utworzonego we wcześniejszych krokach (w tym przypadku `3455`).



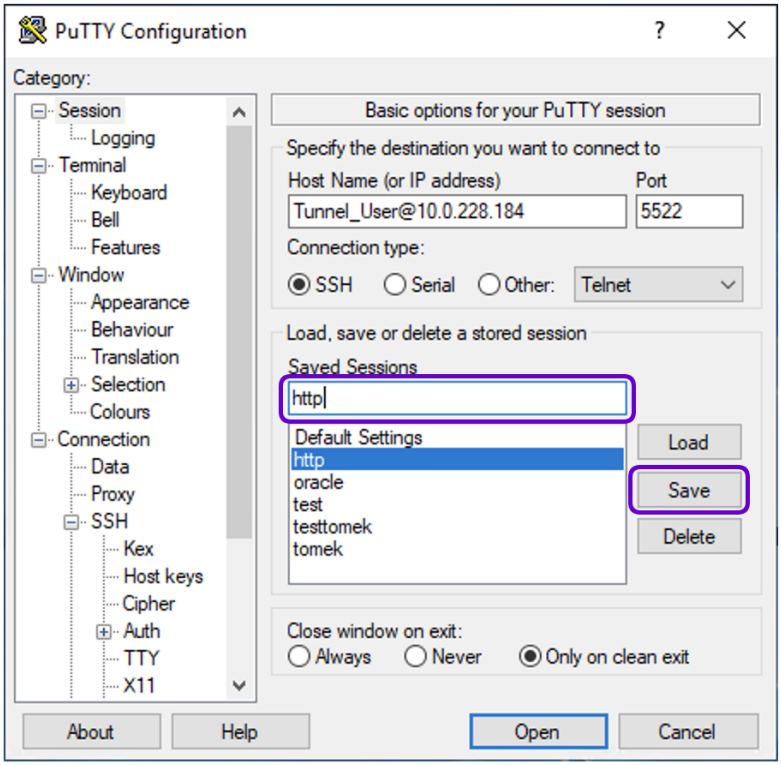
4. Przejdź do zakładki **SSH** i zaznacz opcję **Don't start a shell or command at all**.



5. Przejdź do zakładki **Tunnels** i dodaj przekierowanie portów (**Forwarded ports**):
   - W polu **Source port** wpisz numer portu, który chcesz przekazać (np: `3455`).
   - W polu **Destination** wpisz adres serwera docelowego oraz port w formacie `<destination_server_address>:<port>` (w tym przypadku `twitter.com:443`).
   - Naciśnij przycisk **Add**.



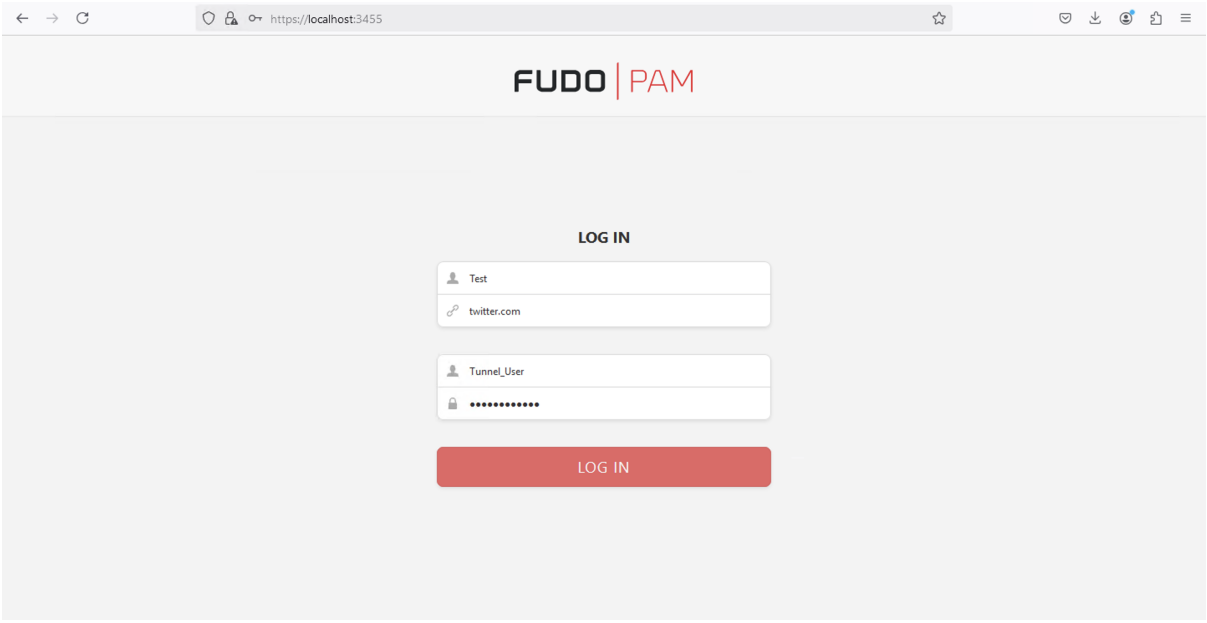
6. Wróć do zakładki **Sessions**, zapisz konfigurację i kliknij **Open**.



7. Wprowadź hasło ustawione dla użytkownika `Tunnel_User` (np. `TestPassw0rd`) i zatwierdź klawiszem **Enter**.
8. Tunel został zestawiony.

Nawiązanie połączenia przez przeglądarkę

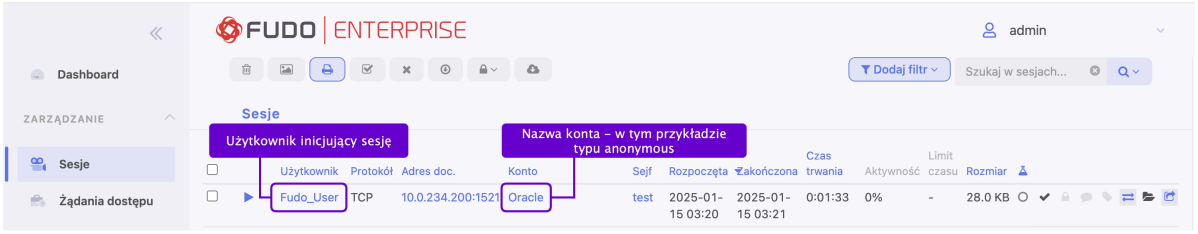
1. Uruchom przeglądarkę internetową.
2. W pasku adresu wprowadź adres z portem ustawionym dla gniazda nasłuchiwania: `https://localhost:3455`.
3. W wyświetlonym oknie logowania Fudo:
   - W polu **Server login** wpisz dowolną nazwę (pole niewykorzystywane w tym scenariuszu),
   - W polu **Server address** wpisz adres serwera (np. `twitter.com`),
   - W polu **Username** wpisz nazwę użytkownika utworzonego w Fudo (np. `Tunnel_User`),
   - W polu **Password** wpisz hasło ustanowione dla użytkownika utworzonego w Fudo (np. `TestPassw0rd`).
4. Kliknij przycisk **LOG IN**.



Wygląd listy sesji

Po nawiązaniu połączenia, w zakładce **Zarządzanie** > **Sesje** pojawi się wpis dotyczący sesji zestawionej wewnątrz tunelu. Widoczne będą następujące informacje:

- Nazwa użytkownika Fudo (również jeśli użyto konta typu anonymous),
- Protokół sesji,
- Adres serwera docelowego,
- Nazwa konta użytego do nawiązania połączenia,
- Nazwa sejfu,
- Czas rozpoczęcia i zakończenia sesji,
- Czas trwania sesji.



20.9.1.3 Nawiązywanie połączenia z bazą danych Oracle

Konfiguracja użytkownika

1. Przejdź do *Zarządzanie* > *Użytkownicy* i kliknij + *Dodaj użytkownika*.
2. Podaj nazwę (np. `Tunnel_User`) i kliknij *Zapisz*.
3. Wybierz metodę uwierzytelnienia użytkownika:
   - Wybierz np: *Hasło statyczne* z listy rozwijanej *Dodaj metodę uwierzytelnienia*.
   - Wpisz hasło dla tworzonego użytkownika (np: `TestPassw0rd`).

- Kliknij *Zapisz*, aby zamknąć okno dialogowe.

4. Kliknij *Zapisz i wyjdź*.

Tworzenie gniazda nasłuchiwania

1. Wybierz z lewego menu **Zarządzanie** > **Gniazda nasłuchiwania** i kliknij + **Dodaj gniazdo nasłuchiwania**.
2. Wprowadź unikalną nazwę (np: `Oracle_Tunnel`).
3. Przejdź do zakładki **Ustawienia** i w polu **Protokół** wciśnij przycisk **SSH**.
4. W sekcji **Tryb połączenia** wybierz **Tunel**.
5. Z listy **Adres lokalny** wybierz adres IP i wprowadź numer portu jaki będzie wykorzystywany do zestawienia tunelu SSH (np: `5522`).
6. Kliknij **Zapisz**.

Uwaga

W polu **Klucze** widoczne są wygenerowane klucze SSH, TLS i Standard RDP Security oraz certyfikat TLS wymagane do prawidłowej pracy gniazda typu „Tunel".

Konfiguracja serwera TCP

1. Wybierz z lewego menu **Zarządzanie** > **Serwery** i kliknij + **Dodaj serwer**.
2. Wprowadź nazwę (np: `Oracle_Tunnel_Server`).
3. W sekcji **Ustawienia**, wybierz **TCP** jako protokół.
4. W sekcji **Miejsce przeznaczenia**: - Wybierz **Host, IPv4** lub **IPv6**. - Wprowadź **Adres, Maskę** oraz **Port** (np: `192.168.0.100`, maska: `32`, port: `1521`).
5. Kliknij **Zapisz i wyjdź**.

Konfiguracja konta

Ostrzeżenie

Jeśli konto `anonymous` jest używane w sesji ustanowionej przez `tunel SSH`, na liście sesji wyświetlana jest nazwa użytkownika, który utworzył tunel.

Uwaga

Do skonfigurowania połączenia wymagane jest konto typu **anonymous** oraz typ nagrywania sesji **raw**.

1. Wybierz **Zarządzanie** > **Konta**, kliknij + **Dodaj konto**.
2. Podaj nazwę (np: `Oracle_Tunnel_Account`).

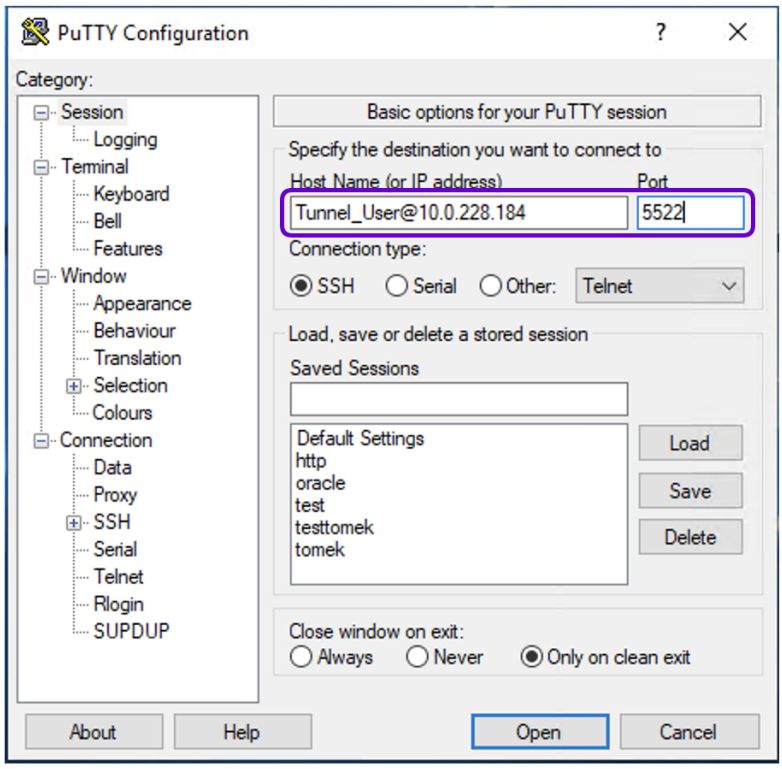
3. Ustaw opcję **Nagrywanie sesji** na **raw**.
4. W zakładce **Ustawienia**, w polu **Typ**, wybierz **ANONYMOUS**.
5. W sekcji **Cel**, wybierz serwer `Oracle_Tunnel_Server`.
6. Kliknij **Zapisz i wyjdź**.

Konfiguracja sejfu

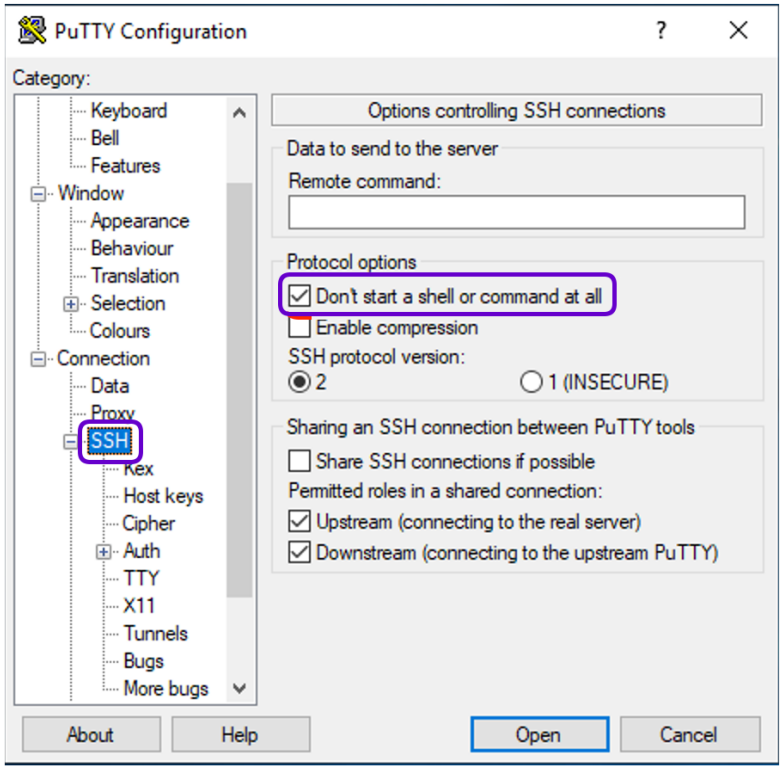
1. Wybierz **Zarządzanie** > **Sejfy** i kliknij + **Dodaj sejf**.
2. Wprowadź nazwę (np: `Tunnel_Safe`), kliknij **Zapisz**.
3. W zakładce **Użytkownicy**, kliknij **Zarządzaj użytkownikami** i zaznacz użytkownika `Tunnel_User`.
4. Kliknij **Zapisz**.
5. W zakładce **Konta**, kliknij **Zarządzaj kontami** i zaznacz `Oracle_Tunnel_Account`.
6. Kliknij **Zapisz**.
7. Wybierz konto `Oracle_Tunnel_Account`, kliknij **Zarządzaj gniazdami nasłuchiwania**, wybierz `Oracle_Tunnel`.
8. Kliknij **Zapisz**, a następnie **Zapisz i zamknij**.

Konfiguracja PuTTY

1. Uruchom aplikację **PuTTY**.
2. W polu **Host Name** wpisz `<Fudo_user>@<Fudo_IP_address>`, czyli w tym przypadku `Tunnel_User@10.0.228.184`.
3. W polu **Port** podaj port gniazda nasłuchiwania typu *Tunel* utworzonego we wcześniejszych krokach (w tym przypadku `5522`).



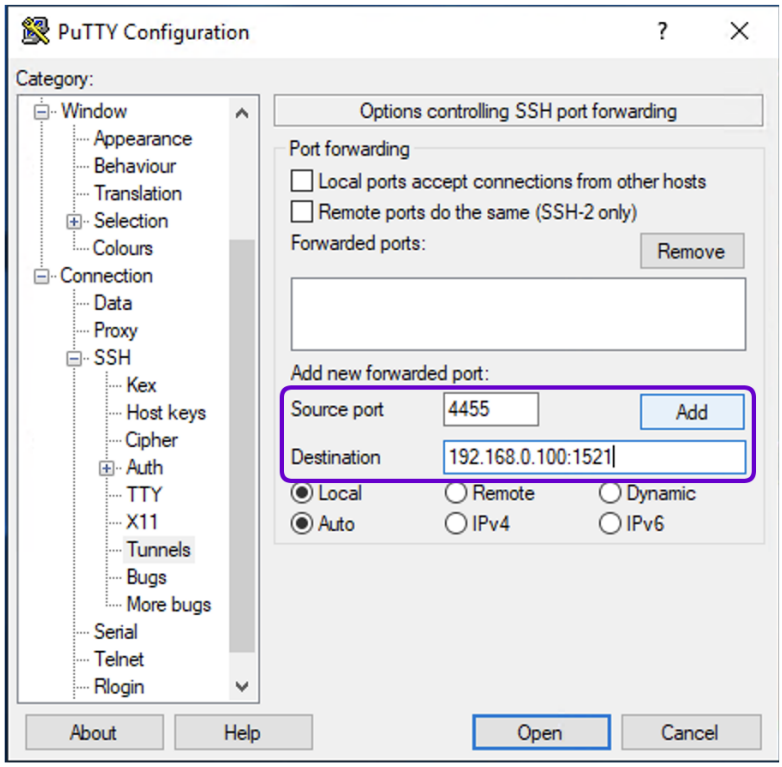
4. Przejdź do zakładki **SSH** i zaznacz opcję **Don't start a shell or command at all**.



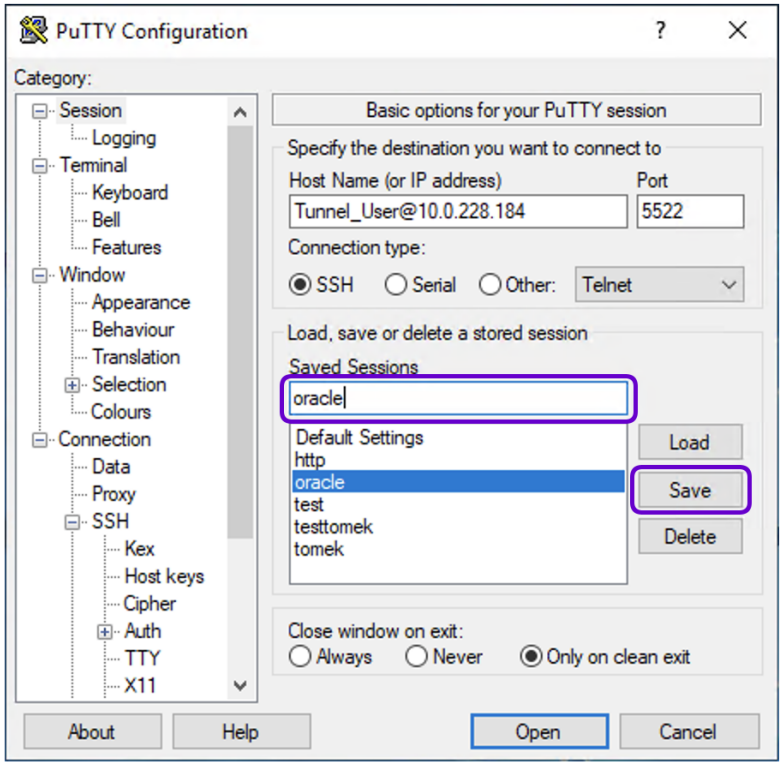
5. Przejdź do zakładki **Tunnels** i dodaj przekierowanie portów (**Forwarded ports**):
   - W polu **Source port** wpisz numer portu, który chcesz przekazać (np: `4455`).
   - W polu **Destination** wpisz adres serwera docelowego oraz port w formacie

`<destination_server_address>:<port>` (w tym przypadku `192.168.0.100:1521`).

- Kliknij przycisk **Add**.



6. Wróć do zakładki **Sessions**, zapisz konfigurację i kliknij **Open**.

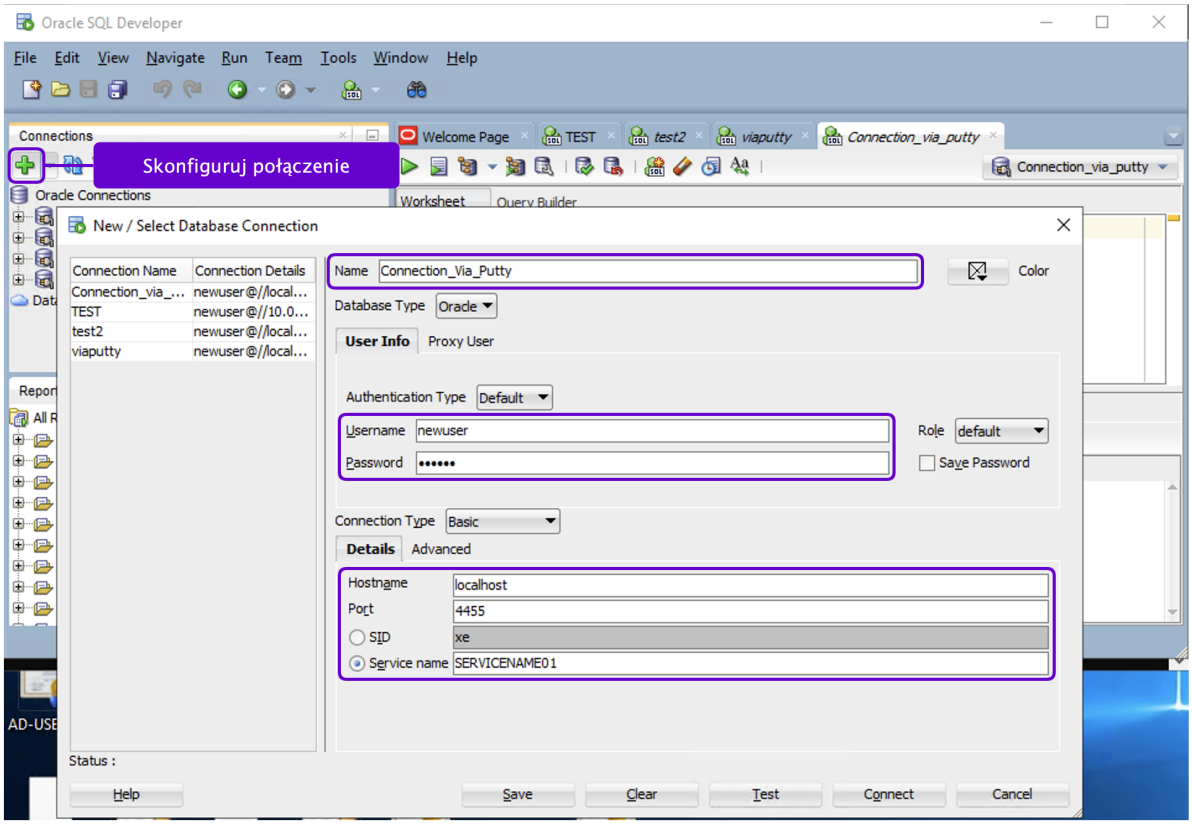


7. Wprowadź hasło ustawione dla użytkownika `Tunnel_User` (np. `TestPassw0rd`) i zatwierdź klawiszem **Enter**.

8. Tunel został zestawiony.

Nawiązanie połączenia przez klienta Oracle

1. Uruchom klienta Oracle (np. **Oracle SQL Developer**).
2. Kliknij **New Connection**, aby utworzyć nową konfigurację.
3. Wypełnij pola:
   - **Name** – nazwa połączenia,
   - **Username** i **Password** – dane logowania do bazy,
   - **Hostname** – `localhost`,
   - **Port** – `4455` (port wpisany w PuTTY jako *Source port*),
   - **Service name** – nazwa usługi bazy danych (np. `orcl`).
4. Kliknij **Connect**, aby nawiązać połączenie z bazą danych.

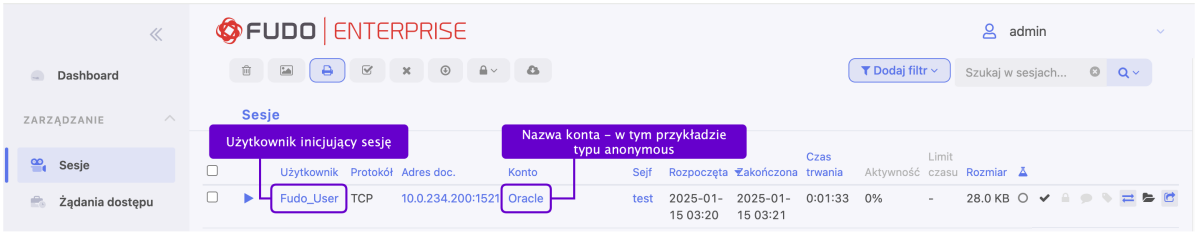


Wygląd listy sesji

Po nawiązaniu połączenia, w zakładce **Zarządzanie** > **Sesje** pojawi się wpis dotyczący sesji zestawionej wewnątrz tunelu. Widoczne będą następujące informacje:

- Nazwa użytkownika Fudo (również jeśli użyto konta typu anonymous),
- Protokół sesji,
- Adres serwera docelowego,

- Nazwa konta użytego do nawiązania połączenia,
- Nazwa sejfu,
- Czas rozpoczęcia i zakończenia sesji,
- Czas trwania sesji.



20.9.1.4 Połączenie do serwera z odwrotnym tunelem przez listener typu Tunnel

Ten scenariusz opisuje przypadek, gdy:

- Listener jest skonfigurowany w trybie *Tunnel*.
- Serwer docelowy używa odwrotnego tunelu SSH (opcja **Użyj tunelu SSH**) wykorzystując **jump host** (serwer pośredniczący), który ma dostęp zarówno do Fudo Enterprise jak i do tego serwera.

Konfiguracja użytkownika

1. Przejdź do *Zarządzanie użytkownikami* > *Użytkownicy* i kliknij + *Dodaj użytkownika*.
2. Podaj nazwę (np. `tunnel_user`) i kliknij *Zapisz*.
3. Wybierz metodę uwierzytelnienia użytkownika:
   - Wybierz np: *Hasło statyczne* z listy rozwijanej *Dodaj metodę uwierzytelnienia*.
   - Wpisz hasło dla tworzonego użytkownika (np: `TestPassw0rd`).
   - Kliknij *Zapisz*, aby zamknąć okno dialogowe.
4. Kliknij *Zapisz i wyjdź*.

Tworzenie gniazda nasłuchiwania

1. Wybierz z lewego menu **Zarządzanie** > **Gniazda nasłuchiwania** i kliknij + **Dodaj gniazdo nasłuchiwania**.
2. Wprowadź unikalną nazwę (np: `SSH_Tunnel`).
3. Przejdź do zakładki **Ustawienia** i w polu **Protokół** wciśnij przycisk **SSH**.
4. W sekcji **Tryb połączenia** wybierz **Tunel**.
5. Z listy **Adres lokalny** wybierz adres IP gniazda nasłuchiwania i port (np: `10.31.135.179` i `3455`).
6. Kliknij **Zapisz**.

Uwaga

W polu **Klucze** widoczne są wygenerowane klucze SSH, TLS i Standard RDP Security oraz certyfikat TLS wymagane do prawidłowej pracy gniazda typu „Tunel".

Konfiguracja serwera RDP z odwrotnym tunelem

1. Wybierz z lewego menu **Zarządzanie** > **Serwery** i kliknij + **Dodaj serwer**.
2. Wprowadź nazwę (np: `RDP_Reverse_Server`).
3. W sekcji **Ustawienia**, wybierz **RDP** jako protokół.
4. Zaznacz opcję *Użyj tunelu SSH* i w polu *Klucz tunelu SSH* wklej klucz publiczny *jump hosta*.
5. Kliknij **Zapisz**.
6. Po zapisaniu serwera skopiuj polecenie wyświetlone w polu *Polecenie do zestawienia tunelu SSH*.

Uwaga

W przeciwieństwie do standardowej konfiguracji serwerów, nie definiujemy adresu IP i portu w sekcji **Miejsce przeznaczenia**, ponieważ serwer będzie dostępny przez odwrotny tunel SSH.

Konfiguracja konta

1. Wybierz **Zarządzanie** > **Konta**, kliknij + **Dodaj konto**.
2. Podaj nazwę (np: `Reverse_Tunnel_Account`).
3. W zakładce **Ustawienia**, w polu **Typ**, wybierz **REGULAR**.
4. W sekcji **Cel**, wybierz serwer `RDP_Reverse_Server`.
5. W sekcji **Dane uwierzytelniające**: - Wprowadź login konta na serwerze docelowym (np: `admin`). - Kliknij przycisk w sekcji **Zastąp tajemnicę**, wybierz np: **Hasło**, i podaj hasło do uwierzytelnienia na serwerze docelowym.
6. Kliknij **Zapisz**, a następnie **Zapisz i wyjdź**.

Konfiguracja sejfu

1. Wybierz **Zarządzanie** > **Sejfy** i kliknij + **Dodaj sejf**.
2. Wprowadź nazwę (np: `Reverse_Tunnel_Safe`), kliknij **Zapisz**.
3. W zakładce **Użytkownicy**, kliknij **Zarządzaj użytkownikami** i zaznacz użytkownika `tunnel_user`.
4. Kliknij **Zapisz**.
5. W zakładce **Konta**, kliknij **Zarządzaj kontami** i zaznacz `Reverse_Tunnel_Account`.
6. Kliknij **Zapisz**.

7. Wybierz `Reverse_Tunnel_Account`, kliknij **Zarządzaj gniazdami nasłuchiwania**, wybierz `SSH_Tunnel`.
8. Kliknij **Zapisz**, a następnie **Zapisz i zamknij**.

Zestawienie tuneli i nawiązywanie połączenia

1. Na serwerze **jump host** uruchom polecenie wygenerowane podczas tworzenia serwera w Fudo Enterprise, aby zestawić tunel. Polecenie zawiera identyfikator utworzonego serwera (`8754997675608244234`), wykorzystywany podczas zestawiania tunelu i nawiązywania połączenia.

   Przykład:

   ```
   ssh -l tunnel -p 65522 -o ExitOnForwardFailure=yes -N -f -R /tunnel/
   ↪8754997675608244234:<target>:<port> 10.31.135.179
   ```

   gdzie należy zastąpić:

   - `<target>` - adresem IP serwera docelowego
   - `<port>` - portem serwera docelowego

2. Na maszynie użytkownika, z której będzie nawiązywane połączenie z serwerem docelowym, zestaw tunel do gniazda nasłuchiwania.

   ```
   ssh -N -l <fudo_username> <fudo_listener_ip> -p <listener_port_tunnel>
   ↪ -L <listener_port_tunnel>:/tunnel/<server_id_on_fudo>
   ```

   Przykład:

   ```
   ssh -N -l 'tunnel_user' 10.31.135.179 -p 3455 -L 3455:tunnel/
   ↪8754997675608244234
   ```

   gdzie:

   - `'tunnel_user'` - nazwa użytkownika w Fudo Enterprise.
   - `10.31.135.179` - adres gniazda nasłuchiwania.
   - `3455` - port gniazda nasłuchiwania typu Tunnel
   - `8754997675608244234` numer ID serwera utworzonego w Fudo Enterprise.

3. Nawiąż połączenie przez tunel, używając nazwy serwera skonfigurowanej w Fudo Enterprise.

   ```
   ssh -l '<fudo_username>#<server_username>#<name_of_server_on_fudo>'␣
   ↪localhost -p <listener_port_tunnel>
   ```

   Przykład:

   ```
   ssh -l 'tunnel_user#admin#RDP_Reverse_Server' localhost -p 3455
   ```

4. W zależności od protokołu serwera docelowego (w tym przypadku RDP), uruchom odpowiedniego klienta natywnego i nawiąż połączenie z adresem `localhost:3455`.

Tematy pokrewne:

- *Nawiązywanie połączenia SSH*
- *Dodawanie serwera SSH*

ROZDZIAŁ 21

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

Uwaga

- 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. Sesja zostanie zakończona, jeśli ustawiona jest odpowiednia polityka AI.

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 *AI - Analiza behawioralna sesji*.

ROZDZIAŁ 22

Słownik pojęć

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).

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.

A

Active Directory, **816**
AD, **816**
administracja
    aktualizacja systemu, 464
    import/eksport konfiguracji, 475
    pierwsze uruchomienie, 41
    ponowne uruchomienie, 580
    przywracanie poprzedniej wersji, 578
AI, 510
API
    użytkownicy, 189
ARP, **816**
Azure, **816**

B

blokowanie
    serwery, 282
broker połączeń RDP, 608, **816**

C

CERB, **816**
certyfikat CA, **816**
Czułość, **816**

D

DHCP, **816**
DNS, **816**
    konfiguracja, 499
dodawanie
    serwery, 237
DoS (*Denial of Service*), **817**
dostęp SSH, **817**
DUO, **817**

E

Efficiency Analyzer/Productivity Analyzer, **817**

F

FPR, **817**

G

gniazda nasłuchiwania
    HTTP, 326
    konfiguracja, 315
    Modbus, 330
    MS SQL, 338
    MySQL, 332
    RDP, 320
    SSH, 317
    TCP, 337
    Telnet, 341
    Telnet 3270, 343
    Telnet 5250, 345
    VNC, 323
gniazdo nasłuchiwania, **817**
grupa redundancji, **817**

H

Hasło statyczne, **817**
heartbeat, **817**
hot-swap, **817**
HTTP
    gniazda nasłuchiwania, 326
    protokoły, 10
    protokół, 10
    serwery, 237

I

import
    serwery, 280

K

Kerberos, **817**
Klucz publiczny, **817**
konfiguracja
    AI, 505

gniazda nasłuchiwania, 315
model danych, 32
powiadomienia, 502
serwery, 237
synchronizacja użytkowników, 568
ustawienia sieciowe, 488, 497
użytkownicy, 187
konto, **817**

L

LDAP, **817**

M

Modbus
gniazda nasłuchiwania, 330
protokoły, 11
protokół, 11
serwery, 241
model danych
serwer, 32
użytkownik, 32
modyfikator haseł, **818**
modyfikowanie
serwery, 282
MS SQL
gniazda nasłuchiwania, 338
serwery, 244
MS SQL (*TDS*)
protokoły, 11
protokół, 11
MySQL
gniazda nasłuchiwania, 332
protokoły, 12
protokół, 12
serwery, 247

N

notacja CIDR, **818**

O

OATH, **818**
OCR, **818**
odblokowanie
serwery, 284
Odcisk Palca, **818**
odwrotny tunel SSH
przypadek użycia, 279
Okta, **818**
OpenID Connect, **818**

P

polityka, **818**
polityka czasowa, **818**
PostgreSQL
protokoły, 12
protokół, 12
serwery, 251
Prawdopodobieństwa zagrożenia, **818**
protocol
secret, 23
protocols
secret, 23
protokoły
HTTP, 10
Modbus, 11
MS SQL (*TDS*), 11
MySQL, 12
PostgreSQL, 12
RDP, 13
SSH, 16
TCP, 23
Telnet, 21
Telnet 3270, 20
Telnet 5250, 21
VNC, 22
X11, 23
protokół
HTTP, 10
Modbus, 11
MS SQL (*TDS*), 11
MySQL, 12
PostgreSQL, 12
RDP, 13
SSH, 16
TCP, 23
Telnet, 21
Telnet 3270, 20
Telnet 5250, 21
VNC, 22
X11, 23
przypadek użycia
odwrotny tunel SSH, 279
tunel do tunelowanego serwera, 807
PSM (*Privileged Session Management*), **818**

R

RADIUS, **818**
RDP, **818**
gniazda nasłuchiwania, 320
protokoły, 13
protokół, 13
serwery, 254
repozytorium haseł, **818**

retencja, **818**
Reverse Proxy
    konfiguracja, 477

S

scenariusze wdrożenia
    bastion, 26
    proxy, 25
    wymuszony routing, 24
secret
    protocol, 23
    protocols, 23
sejf, **819**
sejf anonimowy, **819**
serwer, **819**
Serwery, **819**
serwery
    blokowanie, 282
    dodawanie, 237
    HTTP, 237
    import, 280
    konfiguracja, 237
    Modbus, 241
    modyfikowanie, 282
    MS SQL, 244
    MySQL, 247
    odblokowanie, 284
    PostgreSQL, 251
    RDP, 254
    ssh, 257
    TCP, 274
    Telnet, 260
    Telnet 3270, 264
    Telnet 5250, 267
    usuwanie, 285
    VNC, 270
sesje, 138
    dołączanie do trwającej sesji, 153
    eksportowanie, 159
    filtrowanie, 140
    komentowanie, 156
    odtwarzanie i podgląd, 144
SMS, **818**
SSH, **819**
    gniazda nasłuchiwania, 317
    protokoły, 16
    protokół, 16
ssh
    serwery, 257
SSH reverse tunnel
    use case, 279
SSO, **819**
synchronizacja użytkowników, 568
    konfiguracja, 568
Syslog, **819**

T

TCP
    gniazda nasłuchiwania, 337
    protokoły, 23
    protokół, 23
    serwery, 274
Telnet
    gniazda nasłuchiwania, 341
    protokoły, 21
    protokół, 21
    serwery, 260
Telnet 3270
    gniazda nasłuchiwania, 343
    protokoły, 20
    protokół, 20
    serwery, 264
Telnet 5250
    gniazda nasłuchiwania, 345
    protokoły, 21
    protokół, 21
    serwery, 267
tunel do tunelowanego serwera
    przypadek użycia, 807
tunnel to tunneled server
    use case, 807

U

use case
    SSH reverse tunnel, 279
    tunnel to tunneled server, 807
ustawienia sieciowe
    ARP, 500
    etykiety adresów IP, 497
    konfiguracja interfejsów, 488
    Reverse Proxy, 477
    serwery DNS, 499
    trasa routingu, 498
usuwanie
    serwery, 285
użytkownicy, 187
    API, 189
    konfiguracja, 187
    prawa dostępu, 189
    role, 189
użytkownik, **819**

V

VLAN, **819**
VNC, **819**
    gniazda nasłuchiwania, 323
    protokoły, 22
    protokół, 22
    serwery, 270

W

WWN, **819**

X

X11
    protokoły, 23
    protokół, 23

Z

zewnętrzny serwer uwierzytelnienia, **819**
znacznik czasu, **819**